10 kiberbiztonságra veszélyes szokás

2022. január 04. 14:21 - Csizmazia Darab István [Rambo]

Amikről legjobb, ha 2022-re leszokunk. Ha statisztikákat olvasgatunk, azt látjuk, **az új esztendő első napjaiban a haveibeenpwned.com oldal 11.7 Mrd kiszivárgott jelszót tartalmaz, az Avtest.org tanúsága szerint az egyedi kártékony kódok száma pedig már meghaladja az 1.3 Mrd-ot.**

Az IBM 2021-es jelentésében azt olvashatjuk, hogy **tavaly volt a legmagasabb költsége az adatsértéseknek, az előző éves átlag 3.8 millió dollárhoz képest 2021-ben ez 4.2 millió USD volt**. Az ESET Threat Report számolt be arról, hogy 1**58%-kal megnőtt az Android banki rosszindulatú programok észlelési szintje**, és hogy a **Kaseya elleni ransomware támadás hozta el minden idők legmagasabb, 70 millió dolláros váltságdíj** követelését. Mindeközben a Verizon 2021. jelentése szerint **a social engineering támadások jelentették a legsúlyosabb fenyegetést a közigazgatásra, ezek tavaly az összes incidens 69%-át** tették ki.

Akkor a változások és az újévi fogadalmak jegyében **lássuk azt a tíz rossz szokást, amivel biztonságunk érdekében érdemes lesz mielőbb leszámolni.**

1. Elavult szoftverek használata
Az operációs rendszerek, böngészők és egyéb alkalmazói szoftverek sebezhetőségei a PC-ken és egyéb mobil eszközökön az egyik legfontosabb módja annak, ahogy a kártevők és a számítógépes bűnözők támadhatnak.

Csak 2020-ban több ilyen hibát fedeztek fel, mint előtte bármikor korábban: több, mint 18 ezret. Ez naponta több, mint 50 új szoftver sérülékenységet jelent. A jó hír az, hogy az automatikus frissítési funkció bekapcsolásával máris sokat tehetünk a hibajavító foltok mielőbbi letöltése és futtatása érdekében.

2. Rossz jelszó-higiénia
A jelszavak védik a hozzáféréseinket, belépéseinket. Amit elronthatunk, hogy gyenge, és/vagy több helyen is ugyanazt a jelszót használjuk. A gyenge jelszavak szótáralapon, bruteforce segítségével másodpercek alatt feltörhetők.

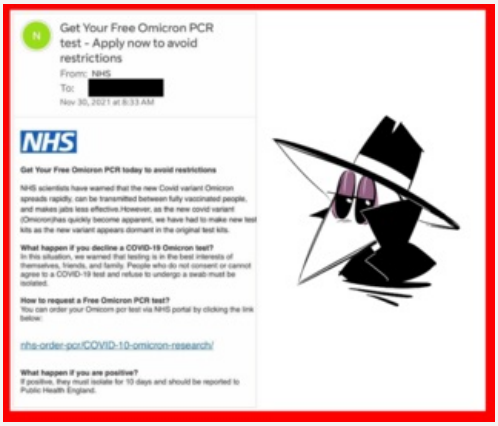
Mindenhol legyen egyedi, erős azaz betűket, számokat és szimbólum karaktereket is tartalmazó hosszú jelszavunk. Ahol csak lehetséges, alkalmazzunk többtényezős hitelesítést: biometrikus (pl. arc, ujjlenyomat) azonosítást, egyedi SMS küldést, vagy egyéb dedikált hitelesítő alkalmazást.

3. Nyilvános wifi használata
A nyitott, nyilvános wifi hálózatok használata egy folyamatosan velünk lévő kísértés, ám a biztonságunk érdekében próbáljuk meg ezek használatát inkább elkerülni, hiszen lehallgathatják a forgalmat, ellophatják a bizalmas adatainkat.

A biztonságos netkapcsolat mindig kiemelt fontosságú, de különösen így van ez vásárláskor, pénzügyeink intézésekor. Erre a célra mindig inkább az otthoni saját internetes elérésünket, vagy mobileszközünk saját adatforgalmát célszerű használni. Nyitott wifi esetében - ha esetleg mégis erre kényszerülnénk, a VPN azaz a Virtual Private Network megoldások segíthetnek a titkosított és biztonságos adatforgalom biztosításában.

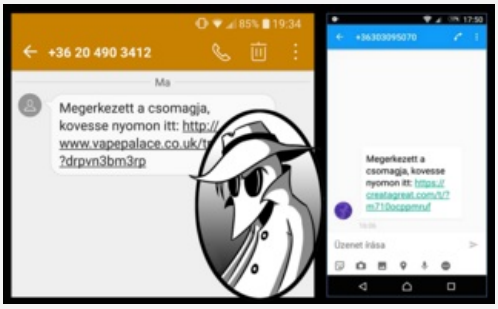
4. Kattintás gondolkodás nélkül
Az adathalászat az egyik leggyakoribb és a támadók szemszögéből egyben a legsikeresebb kiberfenyegetés. A social engineering, azaz megtévesztéses technikát használja ki, ahol a támadó megpróbálja rávenni az áldozatát, hogy rákattintson egy rosszindulatú linkre, vagy nyisson meg egy kártékony mellékletet.

Ahhoz, hogy megakadályozhassuk ezeket a támadásokat, mindig gondolkodjunk kattintás előtt. Ellenőrizzük a feladót, a tartalmat, hihető-e, legitim-e. Sose hagyjuk magunkat sürgetni, mert akkor hajlamosabbak vagyunk kapkodni, hibás döntést hozni.



5. Nem használni biztonsági megoldást minden eszközünkön
A kiberfenyegetések minden számítógépen és internetre kötött mobil eszközön megjelenhetnek. Ahogy a sebezhetőségek, sérülékenységek is mindenhol jelen vannak, úgy érdemes Windows, Linux, Macintosh rendszerünket, Androidos telefonunkat, táblagépünket is megfelelő védelmi programmal ellátni.

A kutatások azt mutatják, hogy évente közel 5000 órát töltünk a mobileszközeinkkel, ennek ellenére sokan ezeket kihagyják a védelemből, ami nagy hiba. Rengeteg lehetőség van ugyanis arra, hogy ott is rosszindulatú alkalmazásokkal és kártékony webhelyekkel találkozzunk.



6. Nem biztonságos webhelyek használata
A HTTPS-webhelyek titkosítást használnak a webböngészőből az adott webhelyre irányuló forgalom védelmére.

Egyrészt láthatjuk, hogy a weboldal valódi, nem pedig adathalász site, másrészt biztosítja, hogy a számítógépes bűnözők ne tudják észrevétlenül lehallgatni, ellopni a webes kommunikációt, pl. jelszavakat. Bár ez önmagában még nem 100%-os garancia arra, hogy semmi rossz nem fog történni, de érdemes mindig figyelni a lakat ikont, ellenőrizni a tanúsítvány érvényességét.

7. A munka és a magánélet keveredése
A tartós homeoffice lassan már két éve velünk van a pandémiás helyzet miatt. Sokan közülünk otthonról dolgoznak, és a korábbi világosan elkülönülő határvonal, ami munkánk és a személyes életünk között volt, összemosódott. Érdemes tudatosan kezelni ezt a helyzetet, céges gépről, e-mailről ne intézzünk privát ügyeket, sose használjuk ugyanazokat a jelszavakat mind a két helyen, mert adatlopás, adatszivárgás esetén ebből komoly kiberkockázat állhat elő.

Mivel egyre gyakoribb a vállalati fiókok elleni támadás, érdemes komolyan venni a vállalati előírásokat, és az árnyékinformatikai kockázatokat is elkerülni. A nem védett, és nem engedélyezett személyes eszközök, postafiókok, felhős tárhelyek, fájlmegosztók használata a munkához extra kitettséget jelent, amiről ráadásul a céges IT csapat nem is értesül.

8. Személyes bizalmas adatok megadása telefonon keresztül
Vishing szintén social engineering technikákat használja a felhasználók becsapására. Ez újabban egyre népszerűbb módja annak, hogy személyes és pénzügyi információkat csaljanak ki az áldozatoktól.

A bankok sosem kérik el tőlünk a banki adatainkat, kártyaszámunkat, lejárati dátumot, PIN kódunkat, 3 jegyű CVV biztonsági kódunkat, internetes banki belépési név-jelszó párosunkat telefonon keresztül, ez legyen egy örök érvényű figyelmeztetés az agyunkban. Ilyet kizárólag adathalász támadók tesznek. A legjobb ökölszabály az, hogy sose adjunk ki érzékeny információkat telefonon keresztül.

9. A biztonsági mentések hiánya
Bár a biztonsági mentések mindig is kulcsfontosságúak voltak - elsősorban persze vállalati környezetben, de

magánfelhasználóként is lényeges lenne - a nagyobb hangsúly az utóbbi négy évben lett érezhető. Ennek oka pedig nem más, mint a zsarolóvírusok tömeges megjelenése és elterjedése. A mentés elkészítésének a legmegfelelőbb ideje az a pillanat, amikor még egyáltalán nincs rá szükség :-)

Emellett egy másik fontos jellemzője is van: csak a kipróbált, letesztelt mentés ér egyáltalán valamit. A ransomware elleni védekezéshez, megelőzéshez egyszerre több dolgot is tenni kell: a naprakész vírusvédelem mellett az operációs rendszer és az alkalmazói programok hibajavító frissítéseinek futtatása, rendszeres külső adathordóra történő mentés, emellett pedig mind a vírusvédelem, mind az operációs rendszer, mind a hálózat biztonság beállításainak felülvizsgálata.

10. Védetlen okosotthon
Végül, de nem utolsósorban az okos-otthonok jelentős része is sebezhető. Az európai házak közel egyharmada már valamilyen intelligens IoT eszközzel van felszerelve, mint a hangasszisztensek, az okos tv-k, termosztátok vagy biztonsági kamerák. Ám azáltal, hogy a netre kapcsolódnak, ezek az eszközök egyre vonzóbb célponttá válnak a bűnözők számára is. Ezeket feltörhetik, eltéríthetik és botnetekké alakíthatják, hogy támadásokat indítsanak mások ellen, vagy átjáróként használhatók a többi belső eszközünk felé.

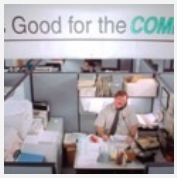
A biztonság megőrzése érdekében érdemes ezeket az eszközöket szeparált hálózaton üzemeltetni, az alapértelmezett jelszavakat lecserélni, a rendszeres hibajavító frissítéseket mielőbb letölteni és futtatni. Csak olyan gyártót válasszunk, aki hangsúlyt fektet a biztonságra, legyen titkosítás, hitelesítés, brute force elleni védelem, és legyenek rendszeres hibajavító frissítések is az eszközhöz.

3 komment
Címkék: frissítés jelszó tippek védelem megelőzés mentés antivírus kiberbiztonság biztonságtudatosság welivesecurity.com

Ajánlott bejegyzések:

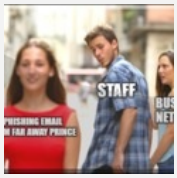

10 gyakori IT biztonsági hiba


10 alaplépés a biztonsághoz



Karácsonyi vásárlás biztonságosabban


Kiberbiztonsági útikalauz diákoknak



10 gyakori ok, amiért bedőlünk a csalásoknak

Kommentek:

Head Honcho 2022.01.04. 14:42:50

Az 1. ponthoz tartoznak azok, akiknek megvan a véleményük a későbbi Windowsokról, és még mindig mániákusan ragaszkodnak a 7-hez.

Válasz erre

Bitfaragó 2022.01.04. 15:49:52

7? Van aki büszkén hangoztatja, hogy csakis az XP. Természetesen letiltott frissítésekkel. És egyébként is, ő okos, soha nem nyit meg olyat ami veszélyes.

Válasz erre

Head Honcho 2022.01.04. 16:16:33

Ő aztán csuda okos lehet.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Sör-Bitcoin menet

2022. január 06. 13:03 - Csizmazia Darab István [Rambo]

Ki bírja tovább? Nem Bud Spencer a főszereplő, és sajnos nem is vidám a dolog. Egy oregoni családi tulajdonban lévő, 1974-es alapítású kézműves sörfőzde, kocsma és szállodalánc, a McMenamins cég **a Wikipédia szerint az Egyesült Államok 50 legnagyobb kézműves sörfőzdéje közé tartozik, ám tavaly decemberben viszont bekaptak egy súlyos ransomware támadást.**

A doxing szó remélhetőleg már senkinek nem jelent újdonságot, ennek segítségével turbózták fel a bűnözők az eredeti klasszikus zsarolóvírus támadásokat. **Ha volt mentése az áldozatnak, és nem érdekelte, hogy váltságdíjért feloldókulcsot kapjon saját állományai helyreállításáért, akkor hátha fizet azért, hogy a titkosítás előtt még el is lopott bizalmas dokumentumai ne kerüljenek nyilvánosságra, töltsék fel azokat publikusan az internetre.**

Ez a zsarolási modell sajnos túl jól működik, ezt láthattuk például tavaly a Colonial Pipeline esetében is.

A McMenamins ugyan sokkal kisebb cég, ám cégmérettől függetlenül egy ilyen támadás még KKV-k esetében is katasztrofális következményekkel járhat. A vállalkozás 55 telephellyel rendelkezik, és több tucat szállodát, bárt, mozit, koncerthelyszínt, éttermet működtetnek az északnyugati parton. Sajnos itt is súlyos dolgok történtek, olyan **bizalmas adatok szivárogtak ki, mint a munkavállalók részletes adatai, név, lakcím, telefonszám, születési dátum, állampolgárság, fogyatékossági státusz, valamint olyan további érzékeny információk, mint a társadalombiztosítási számok, bankszámlaadatok, egészségbiztosítási helyzet, jövedelemösszeg és a dolgozó fegyelmi megjegyzései.**

Az ezekkel való esetleges visszaélés, ezek nyilvánosságra hozatala, vagy más bűnözőknek való továbbadása, eladása komoly veszélybe sodorhatja mind a vállalkozást, mind az egyes embereket. **A cég szerint körülbelül 15-30 ezer dolgozó adata kerülhetett ily módon illetéktelen kezekbe.**

Emellett a támadók hozzáfértek a munkavállalói adatokon kívül **a vállalati üzleti nyilvántartásokhoz, bérszámfejtési adatfájlokhoz is az 1998 és 2010 közötti időszakból, és ezeket titkosították. A vállalati mentésekben sajnos csak a 2010-2021 időszakra vonatkozó adatok szerepeltek, így az ennél korábbi adatokat végleg elveszíthetik.**

A cég értesítette a hatóságokat, az FBI-t és a dolgozóit is tájékoztatta a december 12-i incidensről. A vállalat emellett felbérelt egy kiberbiztonsági céget, hogy segítsen nekik a helyreállítási folyamatban. **Az incidens miatt a**

szállodáikban a szobafoglalási, a hitelkártya-feldolgozás, és a fizetési rendszer átmenetileg leállt.

A McMenamins **eddigi hivatalos nyilatkozatai szerint ügyfél adatok nem érintettek az incidensben. Mivel a munkavállalói hitelkártya és társadalombiztosítási adatok viszont biztosan veszélyben vannak, emiatt a cég egy éves identitás- és hitelvédelmi szolgáltatást biztosít** a dolgozóknak, valamint egy külön segélyvonalat is létrehoztak a helyzet kezelésére.

A Bleeping Computer értesülése szerint a Conti bűnözői csoport állhat a támadás hátterében, amely **több mint 400 ransomware támadást hajtott már végre különböző amerikai szervezetek és nemzetközi vállalkozások ellen.**

3 komment
Címkék: usa étterem váltságdíj adatlopás sörfőzde ransomware szállodalánc doxing McMenamins

Ajánlott bejegyzések:


Fordulat ransomware fronton

Van másik!

Fizess vagy einstandoljuk a kőolajvezetékedet!


Nem szállunk rendelkezésére II.

LockBit vs. olasz adóhivatal

Kommentek:

Head Honcho 2022.01.06. 15:23:26

Miért kell ilyen adatokat online elérhetően tárolni?

Válasz erre

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2022.01.06. 16:30:39

Hát ja, jogos a kérdés.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.

VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Beváltak-e a 2021-es jóslatok?

2022. január 10. 15:40 - Csizmazia Darab István [Rambo]

Megkezdjük a 2022-es esztendőt, és **régi hagyományunk szerint a tavalyi évre jósolt kártevő trendeket, támadási vektorokat nézzük meg abból a szemszögből, vajon mennyire voltak találóak az akkori előrejelzéseink.**

"*A jövő esztendőben is sajnos egyre több zsarolóprogrammal és fájl-nélküli kártevővel kell majd szembenéznie a vállalkozásoknak és az egyéni felhasználóknak.*" Hát ez a tétel sajnos nagyon is bejött, és nem csak mennyiségileg volt sok a ransomware, hanem olyan világméretű támadásoknak is tanúi lehettünk, mint például a Colonial Pipeline csővezetékrendszer elleni incidens.

Illetve a Kaseya ügy hozta el minden addigi idők legmagasabb, 70 millió dolláros váltságdíj követelését. A Colonial eset is tartogatott azért vaskos meglepetéseket, egyrészt hatalmas anyagi veszteséget és hetekig elhúzódó üzemanyaghiányt hozott az USA keleti partján, másrészt a 4.4 millió dollárnyi váltságdíj kifizetése sem hozta el a megoldást, ugyanis a cserébe kapott visszafejtő eszköz olyannyira lassú volt, hogy **helyette inkább mégis saját korábbi biztonsági mentéseikből állították helyre a rendszert.**

"*A távoli munkavégzés számos előnnyel járt a munkavállalók számára, de ezzel párhuzamosan a vállalatok hálózatait is fokozottan sebezhetővé tette a támadásokkal szemben.*" A különféle támadások a fentieken kívül olyan neves cégeket is komoly próbatétel elé állított, mint a JBS a világ egyik legnagyobb húsfeldolgozó vállalata, vagy az Acer.

De súlyos incidens volt **a Microsoft Exchange rendszereket érintő, több különböző sebezhetőséget kihasználó támadássorozat is, amely világszerte komoly adatszivárgásokat** okozott, és amelynek jelentősége a korábbi SolarWinds esethez volt mérhető.

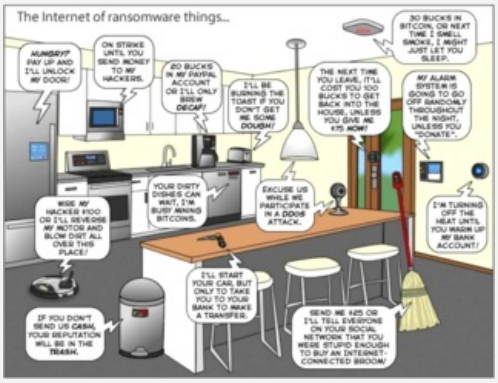
"*Zsarolóprogramok csavarral - ha nem fizetünk, az adataink kiszivárognak*". Ez a fenti esetek jó részét is érintette, a lényeg, hogy **a cégek elleni ransomware támadások esetében már szinte mindig alkalmazzák ezt a**

stratégiát, azaz a doxinggal kiegészülő fenyegetést. Emlékezetes, hogy a Colonial Pipeline incidensnél 100 GB bizalmas adatot sikerült ellopniuk az elkövetőknek, amelyet később részben fel is töltöttek a darknetre.

De nem volt jó éve a T-Mobile-nak sem, ahol egy darknetes fórumbejegyzés tanúsága szerint **egy ismeretlen hacker 100 millió, az ő szerverükről lopott ügyféladatot bocsátott áruba, és 6 Bitcoint, azaz körülbelül 80 millió forintnak megfelelő összeget kért az adatbázisért.** Később a T-Mobile megerősítette, hogy valóban támadás áldozatai lettek, és illetéktelenek jogosulatlanul hozzáfértek az adataikhoz.

Ugyancsak szerepelt a jóslatok közt ez is: **"*A fájl nélküli fenyegetések gyorsan fejlődnek, és várhatóan 2021-ben ezeket a módszereket még gyakrabban fogják használni az egyre összetettebb és erőteljesebb támadásokban.*"**

Nos a PowerShell alapú támadások valóban gyakoribbá váltak, és az ilyen típusú incidensek mennyisége a korábbi, 2020-as esztendőhöz képest duplázódott.



Végül, de nem utolsósorban az IoT eszközök is szóba kerültek: "***Az IoT (Internet of Things), azaz internetre csatlakozó okos-eszközök és alkalmazások általában hatalmas adatvédelmi és biztonsági kihívásokkal járnak.***" Ebben a témában azt láthattuk, hogy 2021-ben itt is masszívan nőtt az internetes okos-eszközök elleni támadások mértéke.

A statisztikák szerint a támadók elsősorban kriptovaluta bányászatra, elosztott szolgáltatásmegtagadási (DDoS) támadások kivitelezésére használták a kompromittált rendszereket, amelyeknél leggyakrabban a telneten keresztül próbálkoztak. **Vagyis elkönyvelhetjük, összességében elég pontosan beváltak a tavalyi évre vetített jóslatok, előrejelzések.**

2 komment
Címkék: fenyegetés trend jóslat riport előrejelzés iot kiberbiztonság beválás ESET welivesecurity.com 2021.

Ajánlott bejegyzések:

A nemzetközi helyzet egyre fokozódik


Kiberkockázatok - miért nehéz velük lépést tartani?


VPN appok Androidra vagy mégsem?


10 alaplépés a biztonsághoz


Oroszország lett a fő kibercélpont

Kommentek:

gigabursch 2022.01.10. 20:36:39

Elnézve ezt a vicces grafikát, vajon ki az a hülye, aki okosotthonban akar élni?

Válasz erre

GyMasa 2022.01.12. 12:17:32

@gigabursch:
Ja, nekem a hideg futkos a hátamon az IoT hallatán...
Pedig annyira egyszerű lenne a megoldás:
- Egy QR kód a cuccra, ami addig nem csinál semmit, amíg az ember meg nem ad neki egy biztosnágos user/password párost.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Dutyi dili

2022. január 13. 13:05 - Csizmazia Darab István [Rambo]

Számos helyen találkoztunk már zsarolóvírussal: rendőrkapitányságon, ügyvédi irodában, kórházakban, iskolákban, kormányhivatalokban, multicégeknél, húsfeldolgozó hálózatnál, felhős távmenedzsment szolgáltatónál, vagy éppenséggel kőolaj vezetéket üzemeltető vállalat hálózatában. Mindenhol sikerült zavart kelteni, kárt okozni, de **eddig még nem láttunk olyan hírt, amelynél egy börtön intézmény lett volna a célpont. Egészen mostanáig.**

Az Egyesült Államok New Mexico területén fekvő Bernalillo megyei intézményben történt eset január elején. A beszámolók szerint a Metropolitan Fogvatartási Központot lezárták, miután ismeretlen támadók kiütötték a börtön informatikai rendszerét, leállt az internet, elérhetetlenek lettek az adatbázisok és a biztonsági kamerák.

A ransomware támadás ugyan nem okozott automatikus ajtónyitást, és hollywoodi filmekben látható tömeges fogolyszökést, **de totális káoszt annál inkább.**

Az incidens miatt és a megfigyelő kamerák elérhetetlensége miatt egyelőre minden fogvatartottnak folyamatosan a cellájában kell tartózkodnia, kivéve amikor éppen szükségük van orvosi ellátásra. A börtön vezetősége korlátozta a mobiltelefon használatot és bizonytalan ideig szüneteltette az összes látogatást is.

A kibertámadás előtt a meghallgatásokat Zoomon keresztül internetes videókonferencia keretében folytatták le, ezenkívül a vádlottak és az ügyvédek négyszemközt is beszélhettek egy szeparált szobában vagy egyeztethettek egy külön telefonvonalon keresztül. Most ideiglenesen ez is **megszűnt, 15 perces vezetékes telefonos fülkés hívásokkal bonyolítják le mindezeket.**


Bernalillo County notice of emergency Contributed by The Verge (Vox.com)

Case 6:95-cv-00024-JB-KBM Document 1516 Filed 01/06/22 Page 1 of 7

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

JIMMY (BILLY) McCLENDON, et al.,
Plaintiffs,
vs. CIV 95-24 JB/KBM
CITY OF ALBUQUERQUE, et al.,
Defendants,
vs.
E.M., R.L., W.A., D.J., P.S., and N.W. on behalf of themselves and all other similarly situated,
Plaintiff-Intervenors.

DEFENDANT'S NOTICE OF EMERGENCY
PURSUANT TO PARAGRAPH 14 OF THE SETTLEMENT AGREEMENT

Document 1 of 7

A börtön alkalmazottak is alkalmazkodni kényszerültek, **az email rendszer hiánya miatt telefonvonalas beszélgetéseken zajlik az ügyintézés, egyeztetés, ám a túlterheltség miatt ezek gyakran megszakadnak. A korábbi jelentések tartalmához sem férnek hozzá - pl. fogvatartottak adatai, magaviseleti aktái, orvosi feljegyzések, stb. Mivel január 5-e óta az automatikus központi ajtóvezérlés használhatatlanná vált, ez azt jelenti, hogy a személyzetnek minden egyes alkalommal kulcsokat kell használnia a létesítményajtók kézi kinyitásához.**

Bár a támadás után január 10-én egyes rendszerek már részlegesen üzemeltek ugyan, de a korábbi rend még korántsem

állt teljesen helyre. **A helyzet fonákságához tartozik még, hogy ezek a rendkívüli helyzet miatti időleges korlátozások elvileg törvénysértőek, ám bevezetésük mégis elkerülhetetlen volt.**

A támadás technikai mikéntjéről egyelőre nem jelentek meg részletek, például hogy melyik bűnözői csoport hajtotta azt végre, milyen malware változat szerepelt az incidensben, loptak-e el tőlük bizalmas adatokat, pontosan milyen adatok lehettek veszélyben, követeltek-e tőlük valamilyen formában váltságdíjat, ha igen egyáltalán fizetett-e végül a támadóknak az intézmény, és ha igen, milyen összegben.

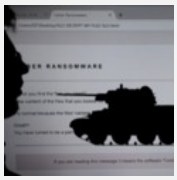
1 komment
Címkék: biztonság usa börtön incidens ransomware zsarolóvírus

Ajánlott bejegyzések:


Apa kezdődik!


Felkészül: USA kritikus infrastruktúra

Netwalker tag menni 6 év börtön


Ez most vajon akkor milyen ware?

Tesz-e Oroszország a ransomware ellen?

Kommentek:

gigabursch 2022.01.14. 11:01:45

Ügyes...

Válasz erre

keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.

VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Addig jár a REvil a kútra...

2022. január 18. 09:38 - Csizmazia Darab István [Rambo]

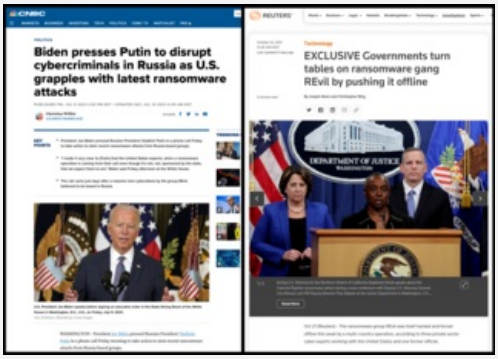
Igen sokszor írtunk arról, hogy megint újabb támadás történt valahol a világban, és sajnos csak igen **ritkán adatik meg az a kedvező lehetőség, hogy éppen egy nemzetközi számítógépes bűnbanda letartóztatása legyen az aktuális téma. Nos most végre ismét egy ilyen várva várt esemény történt.**

A korábbi emlékezetesebb esetek között volt például, amikor 2015-ben egy közös nemzetközi hadművelet keretében a hatóságok nagy erőkkel lecsaptak a Zeus és Spyeye **banki trójait terjesztő hálózatra**. Ugyancsak letartóztatással zárult 2020-ban az a csalássorozat is, amelyben indiai elkövetők az amerikai adóhatóság (Internal Revenue Service, IRS) munkatársainak kiadva magukat egy illegális telefonos központot üzemeltettek, **amely olyan személyeket igyekezett megzsarolni, akik az Egyesült Államokban telepedtek le.**

És hogy a közelmúltból is szerepeljen egy példa, tavaly ősszel az Europol és az olasz Eurojust aktív közreműködésével 106 gyanúsított letartóztatása történt meg, miután **lefülelték azt jól szervezett bandát, amelynek központja Tenerifén üzemelt, és több száz áldozatot károsítottak meg SIM kártyacserés csalásokkal.**

És akkor ugorjunk is a mostani eseményhez, a REvil csoporthoz, akik számos komoly leállásokkal járó zsarolóvírus incidensért felelősek. Hogy csak egy közelmúltbeli címlapos sztorit idézzünk fel, tavaly nyáron nagyszabású támadást intéztek a Kaseya felhős távmenedzsment szolgáltató ellen, amelynél **70 millió dollárnak megfelelő kriptovalutát követeltek az üzemeltetőktől váltságdíjként**, de állhatna itt a Colonial Pipeline incidens is, ahol a DarkSide a REvil szoftverét használta.

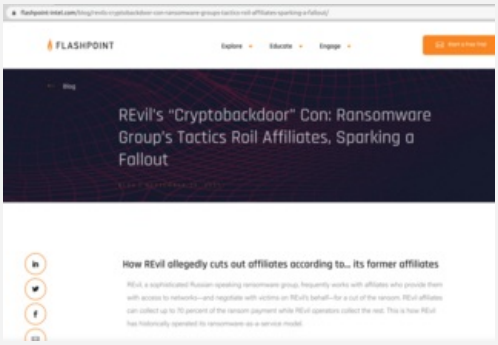
Ezek után felvetődött és nem először, hogy **vajon elegendő energiával üldözik-e Oroszországban az ilyen bűnözőket,** mert sokak szerint nem igazán tesznek meg mindent, ez pedig konkrétan szóba került Biden-Putyin megbeszélésén is.



Közben annyival is érdekesebb lett a história, hogy **kiderült, a REvil csapat a RaaS azaz Ransomware as a Service**

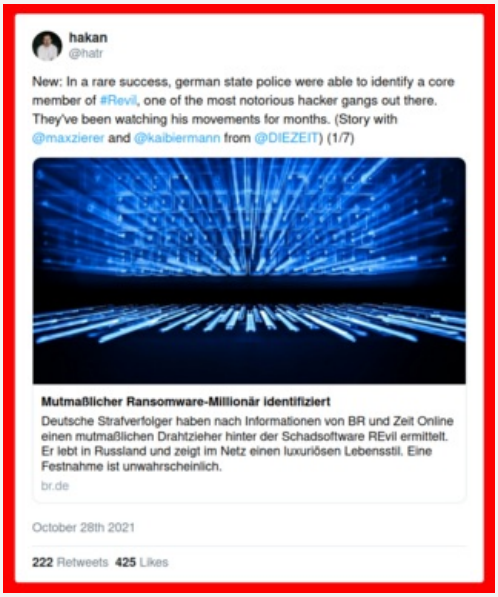
formájában is bérbe adott ransomware szolgáltatásába elrejtett egy titkos hátsóajtó alkalmazást is, amelynek segítségével a fizetős bérlőik ransomware tárgyalásait észrevétlenül figyelemmel kísérhették.

Mohóságukra jellemző, hogy amennyiben potenciálisan nagy összegű váltságdíjjal kecsegtetett egy ilyen bérlő által intézett támadás, egyszerűen közvetlenül felvették a kapcsolatot az áldozatokkal, és ők maguk kasszírozták be a feloldó kulcsért járó összeget kizárva így saját bérlőiket.



Mindenesetre **a nyomás több irányból is fokozódott irányukban, és amikor 2021. októberében váratlanul elnémult a híres-hírhedt REvil bűnözői csoport**, október 17-étől elérhetetlenné váltak, és elindultak az ezzel kapcsolatos találgatások.

Mint kiderült, a leállás oka az volt, hogy a bűnüldöző szerveknek sikerült hozzáférniük nemcsak a korábbi Happy bloghoz, hanem a REvil számítógépes hálózati infrastruktúrájához is, és ezen szerverek felett részleges irányítást tudtak szerezni.

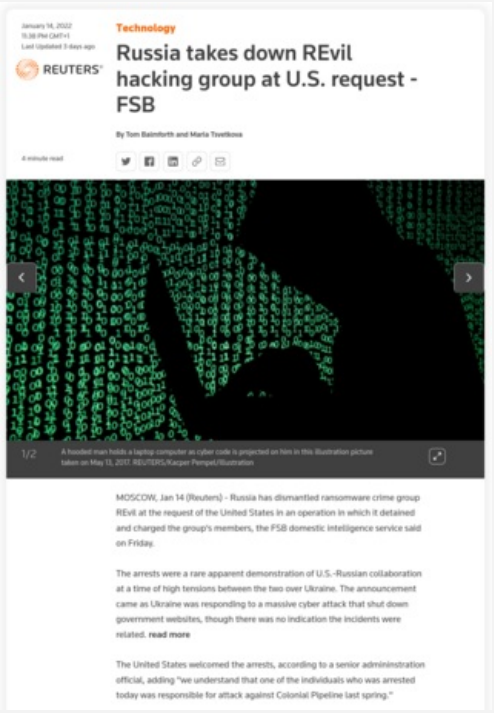


Izgalmas folyománya volt a velük kapcsolatos híradásoknak, hogy korábban **két német újság, a Bayerische Rundfunk és a Zeit Online riporterei hónapokat töltöttek el a REvil digitális nyomainak felkutatásával. Ezalatt találtak például olyan érintett kriptovaluta számlát, amelyre a vizsgált időszak alatt hat részletben több mint 400 000 eurót (144 millió forintnyi összeget) utaltak Bitcoinban.**

Egy a bűnöző csapat vélelmezett tagjáról, egy bizonyos Nikolay K-ról kiderült, hogy az áldozatoktól befolyó váltságdíjaknak hála elképesztő pénzszórással élte az életét, ötcsillagos szállodákban fordult meg Dubajban, a Maldív szigeteken vagy éppen a törökországi Antalyán. **A gyanúsított még az interneten is büszkélkedett vagyonával, ahol kriptovaluta befektetőnek adta ki magát.**

És az események végül felgyorsultak, ugyanis az orosz FSZB (Szövetségi Biztonsági Szolgálat) bejelentette, hogy amerikai kérésre lekapcsolták a REvil hackercsoportot. A rendőrség összesen **25 helyszínen tartott házkutatást, és 14 embert vettek őrizetbe. Az FSZB beszámolója szerint az akció során 426 millió rubelt (kb. 17. milliárd forint), 600 ezer dollárt, 500 ezer eurót, különféle számítástechnikai eszközöket és 20 luxusautót foglaltak le.**

A moszkvai bíróság két gyanúsítottat, Roman Muromskyt és Andrej Bessonovot két hónapra előzetes letartóztatásba helyezett.



Emlékezetes, hogy **2021. novemberében az Egyesült Államok bejelentette, hogy 10 millió dolláros jutalmat ajánl fel olyan információkért, amelyek a DarkSide és REvil csoportban kulcsfontosságú pozíciót betöltők azonosításához vagy tartózkodási helyéhez vezetnek.** Egy a mostani letartóztatási ügyet ismerő forrás azt mondta az Interfaxnak, hogy a csoport orosz állampolgársággal rendelkező tagjait biztosan nem fogják átadni az Egyesült Államoknak.

Mindenesetre az FSZB nyilatkozat szerint a csoport letartóztatott tagjait vád alá helyezték, és végül akár hét év börtönt is kaphatnak. Meglátjuk, hogy hosszútávon mindez mennyit segít majd rajtunk.

Szólj hozzá!
Címkék: bíróság oroszország letartóztatás vádemelés fszb váltságdíj darkside revil ransomware zsarolóvírus

Ajánlott bejegyzések:

[Váltságdíjat kínálnak a váltságdíjszedő bandáért]

[Netwalker tag menni 6 év börtön]

[Kik, hol és mire költik a beszedett váltságdíjainkat?]

[Offline mennyország - egy rövid időre]

[Amikor a hóhért akasztják...]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Mit tehetünk a kriptovaluta csalások ellen?

2022. január 20. 10:35 - Csizmazia Darab István [Rambo]

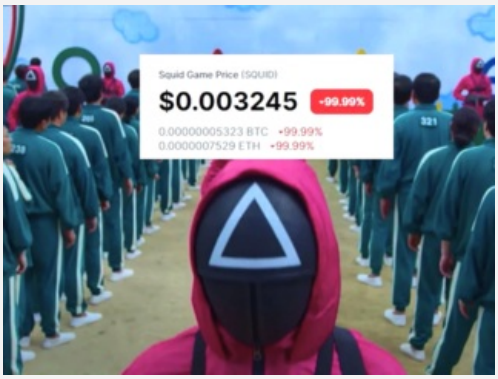
Szezonja van a különféle Bitcoinos és egyéb virtuális valutákkal kapcsolatos átveréseknek, befektetési csalásoknak. Ha már ide tart a korszellem, hogyan védekezhetünk, ismerhetjük fel a gyanús jeleket, **miként előzhetjük meg a bajt, mielőtt áldozattá válnánk és elbuknánk a pénzünket?**

A velünk élő spamek sajnos nem ritkulnak, hiába ígérte meg annak idején 2004-ben ezek kihalását maga a nagy Bill Gates. **Ha időszakokat, kiemelt tematikákat vizsgálunk az időben, láthatjuk, hogyan voltak különféle jellegzetes korszakok, amelyek mindig egy adott dolgot próbált meg népszerűsíteni:** kezdetben hamisított Rolex, fizetős pornográf oldalakhoz való ingyenes hozzáférést, warez programokat.

Később a hamis antivírus korszak évekig tartotta magát nagyjából 2008 és 2010 között volt ennek a horizontja, majd később jöttek a hamis szerzői jogi fenyegetések, amelyeknél szintén a pénzünket akarták kicsalni. **Pár éve viszont a kriptovalutás csalások szezonja tart, ez tematizálja a postaládánkba beeső kéretlen tartalmak zömét**. A tavalyi esztendőben jó pár ilyen eset került a címlapokra.

Ha a statisztikákat nézzük, 2020. októbere és 2021. májusa között az amerikaiak becslések szerint körülbelül 80 millió dollárt (25 milliárd forint) kárt szenvedtek el a kriptovalutás csalás miatt a Szövetségi Kereskedelmi Bizottság (Federal Trade Commission, FTC) szerint. **Az Egyesült Királyságban ez a szám még ennél is magasabb: rendőrségi adatok alapján az áldozatok több mint 146 millió fontot (kb. 62 milliárd forint) veszítettek el a tavalyi, 2021-es év első kilenc hónapjában**.

A csalások fő oka, hogy **sok országban még szabályozatlan ez a tényked**és, **sok számítógépes kártevő használja a fertőzött gépeket Bitcoin bányászatra, az email spamek ingyen és hatalmas számú emberhez képesek eljuttatni bármilyen hamis ajánlatot, és persze a közösségi oldalakon is zajlik ez a fajta** "hogyan gazdagodjunk meg öt egyszerű lépésben pár nap alatt" típusú megtévesztés.



Nézzük akkor, milyen ajánlatokkal bombáznak minket. Vonzó befektetéseket kínálhatnak kéretlen üzenetekben, ahol hamis információkkal akarják rávenni az áldozatot arra, hogy kevéssé ismert, vagy totálisan ismeretlen kriptovaluta

cégekben részvényeket vegyenek. **A legutóbbi ilyen esetben Squid Games tokenekkel kereskedtek, és rövid idő alatt sikeresen fel is verték az árat, majd az egekből lezuhanva hirtelen 99.99%-ot vesztett az értékéből.**

Ez az úgynevezett Ponzi séma, ahol az új befektetők pénzéből fizetik ki a korábbiakat törvényszerűen összeomlásra van ítélve, ám mégis mindig akadnak olyan balekok, akik naivságból, tájékozatlanságból vagy nyereségvágyból beleesnek a csapdába.

A blogban mi is foglalkoztunk már a híresség nevében elkövetett csalásokkal, ahol Elon Musk vagy Warren Buffett ír nekünk, hogy megduplázhatjuk vagy megtriplázhatjuk a pénzünket. Előbb küldjük el neki, ő meg persze majd háromszor adja vissza mint Ludas Matyi.

Hát aki ezt elhitte, az utána gazdagabb lett - egy tapasztalattal: ha valaki úgy ígér pénzt, hogy előbb mi fizessünk neki, érdemes tehát gyanakodni.

Hasonló elven működik az az átverés, amelynél egy hamis kriptotőzsde hatalmas nyereséggel kecsegtető állítólagos Bitcoin befektetési platform ígéretével csalja ki az áldozatok hitelesítő adatait. Aki ezt megadja, szintén csalódik az adott szó szentségében, mert a számláját pillanatok alatt kiürítik.

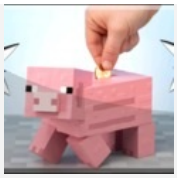
Emellett még számtalan adathalász kísérlet, legitim cégek nevével visszaélve hamis sajtóközlemények terjesztése, amely azonnali tőzsdemozgásokat okoznak, és hasonló trükkök lapulnak a csalók tarsolyában.

Végezetül foglaljuk össze röviden, hogyan védekezzünk. **Soha ne adjuk meg személyes adatainkat olyan szervezeteknek, amelyek kéretlen üzenet útján kerestek meg bennünket e-mailben, sms-ben, vagy a közösségi médiában. Klasszikus az idézet, de változatlanul igaz: ha valami túl szép ahhoz, hogy igaz legyen, az általában átverés. Kezeljünk minden új befektetési rendszert egészsége gyanakvással, ne kapkodjunk, alaposan tájékozódjunk. Kriptovaluta fiókunkhoz kapcsoljuk be a kétfaktoros hitelesítést, így a név-jelszó páros illetéktelen kezekbe kerülése esetén sem férnek hozzá a számlánkhoz.**

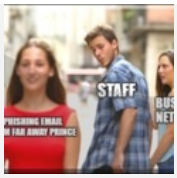
Soha ne utaljunk előre későbbi nyereséget remélve ismeretleneknek, és minden számítógépünkre, mobileszközünkre telepítsünk megbízható vírusvédelmi alkalmazást, továbbá a rendszeres hibajavító frissítéseket is futtassuk el időben. A biztonságtudatos hozzáállás pedig gyakorlatilag nélkülözhetetlen skill a mai világban.

Szólj hozzá!
Címkék: csalás átverés megelőzés virtuális védekezés bányászat valuta welivesecurity.com kriptovaluta

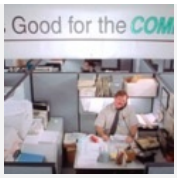
Ajánlott bejegyzések:



[A csalások már a spájzban vannak]



[10 gyakori ok, amiért bedőlünk a csalásoknak]



[Karácsonyi vásárlás biztonságosabban]

[Fiatal vagy? Ezekre az online csalásokra figyelj!]

[VPN appok Androidra vagy mégsem?]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

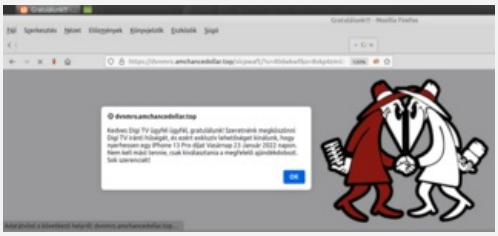
accountz

Belépés
Regisztráció

Ingyen iPhone csak itt, csak most, csak nekünk

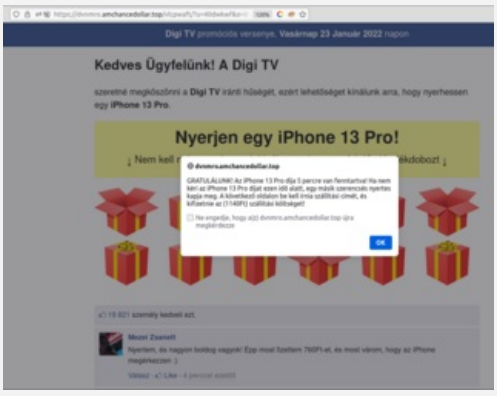
2022. január 24. 10:11 - Csizmazia Darab István [Rambo]

"#vótmá" - ezzel a címkével jelzik szlengesen a kommentelők a különféle topikokban, hogy megint egy ismétlődő dolog újraemlítéséről van szó. Való igaz, a hasonló átveréseknek már itt a blogon belül is vaskos előzményei vannak, de a mai esetünkkel **nemcsak azt szeretnénk megmutatni, hogy ezek a trükkök sajnos egyáltalán nem haltak ki, hanem azt is, hogy extra ügyvédi rafinériával megfűszerezve néha nem is annyira egyszerű ezektől a csalásoktól megszabadulni.**



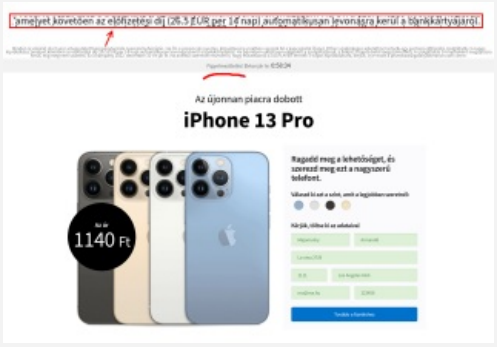
Mai munkadarabunkat nagyon köszönjük kedves olvasónknak. Itt egy **böngészés közben felugró ablak azzal az örömhírrel, hogy mint hűséges internet-előfizető ügyfél nyerhetünk egy iPhone 13 Pro készüléket**. Ehhez nem is kell mást tenni, mint 3 kattintásból rálelni a nyerő dobozra.

Ezer százalék, hogy ez mindenkinek összejön, hiszen ez a csali a terv része. Milyen színűt szeretnénk? - ezt is kiválaszthatjuk a szemgyönyörködtető pasztellszínek közül.



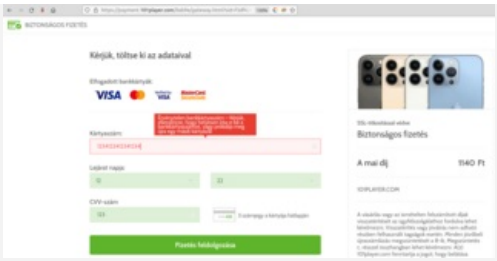
Ám az akárhányadik click után, hogy így szerencsésen "nyertünk", akkor **jönnek szépen sorban a klasszikus átverési elemek: mindössze 5 percünk van intézkedni (sürgetés), lesz egy előrefizetendő úgynevezett szállítási díj (419-es pénzkicsalási trükk), és bekérik a személyes adatainkat. Elsőként jöhet a teljes név, e-mail fiók, telefonszám és pontos lakcím (adathalászat).**

És mindez megtámasztva kamu értékelésekkel is, ahol az állítólagos Mezei Zsanett azt írja, "*Nyertem és nagyon boldog vagyok!*". Nem baj, ez nem fog túl sokáig tartani ;-)



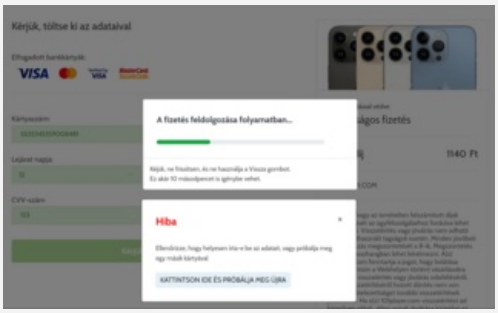
És **végül a banki adatainkat is elkérik a "biztonságos" fizetéshez. Kártyaszám, lejárati idő és természetesen a 3 jegyű CVV biztonsági kód is szükséges.** Ehhez persze hozzávehetjük, hogy szerencsére számos banknál a netes vásárlásoknál jelentkező a fizetési kérelmeket (terhelés) már egyedileg kell engedélyeznünk és jóváhagynunk, de ez persze a bizalmas banki adatok ellopását sajnos nem akadályozza meg.

A **lap alján szereplő ciprusi cím azért szintén besorolható a nagy-nagy intő jelek** közé.



Ha a csalók jogi csűrcsavarral is igyekeznek körbebástyázni kétes üzelmeiket, akkor ez egy igen halálos kombináció - emlékezzünk csak a Kaspersky 2007-ben zajló, évekig tartó perére a Zango nevű (180Solutions) hírhedt reklám-program-terjesztő ellen. **De hasonló próbálkozások, fenyegetések tömegesen fordulnak elő, például az ESET-et a szintén kétes hírű eMediaCodec terjesztői is feljelentéssel fenyegették, ha a trójaiként való észlelést nem távolítják el az adatbázisukból.**

Emiatt **a mai esetünk kapcsán is érdemes a tisztánlátás végett még az alábbi cikket is alaposan átfutni.**



Ugyanis itt nem lopták el a kártyaadatainkat (ezt a pert simán elveszítenénk), hanem megtévesztéssel ugyan, de általában **mi saját magunk adtuk meg, pl. a fenti állítólagos nyeremény postázási díja, vagy fájl letöltés, társkereső szolgálat "ingyenes próbaidejére", ahol ezzel "észrevétlenül" és figyelmetlenül, de különféle rendszeres fizetős szolgáltatásokra is feliratkoztunk.** Ekkor a bankkártya letiltása esetén nem is fognak igazat adni nekünk, hiszen ott a bizonyíték a mi kártyaadatainkkal általunk végzett "megrendelés".

Az egyedüli út lemondani a szolgáltatást, leiratkozni a felesleges, csalárd módon létrejött megrendeléseinkről. Szóval odafigyelés, óvatos biztonságtudatosság, vírusvédelmi beállításoknál a "Kéretlen alkalmazások keresésének engedélyezése" és az egészséges gyanakvás, na meg egy jó olvasószemüveg az apró-betűs részekhez - ezek nagyban segíthetnek rajtunk.

3 komment
Címkék: iphone csalás átverés nyeremény megtévesztés adathalászat 101player.com

Ajánlott bejegyzések:

Ismét csomagunk érkezett - vagy mégsem?

Banki meló

Nagy pénz, nagy foci, nagy átverések

Gratulálunk - mihez is?

Tagsági kérdések - vagy mégsem?

Kommentek:

Head Honcho 2022.01.24. 10:39:03

1.140 ft egyszer, további 26.5 eur kéthetente. Ravasz.

Válasz erre

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2022.01.24. 18:29:09

Hali :-)

Jaja, a jó kis apróbetűs.

"Érted? Nem! De remélted!
A távcsövet a boltban te kérted."

Válasz erre

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2022.01.25. 17:58:14

Egy csomó egyéb másik domainről is megy ez a játék, pl. tone.birdforframe.com oldalról

whois.domaintools.com/amchancedollar.top

whois.domaintools.com/birdforframe.com

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

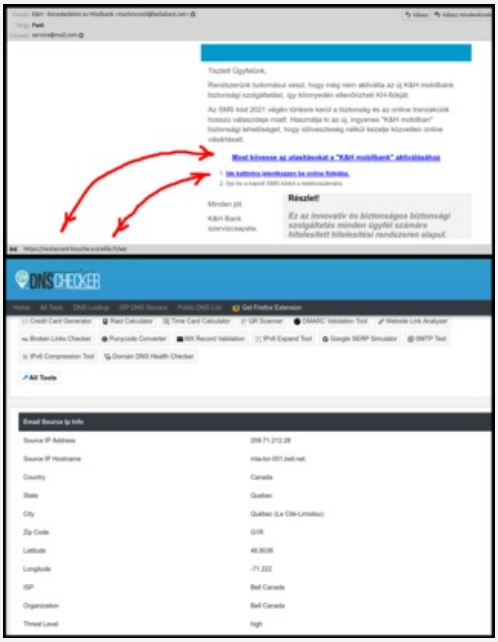
K&H mobilbank biztonsági szolgáltatás - vagy mégsem?

2022. január 27. 11:23 - Csizmazia Darab István [Rambo]

A pandémia lassan két éves alatt egyre több időt töltünk online, tanulással, munkával, kikapcsolódással, vásárlással, bankolással. Még több neten tárolt személyes és bejelentkezési hitelesítő adatunk keletkezik, amelyeket a kiberbűnözők részben az üzemeltető szervezetektől, részben tőlünk igyekeznek ellopni. **Ezúttal egy banki próbálkozás került a látóterünkbe.**

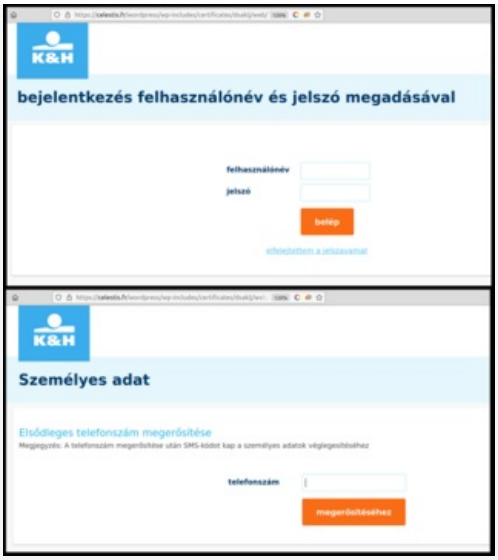
Az átverések hiába magyarul érkeznek, még mindig döcögősen fogalmazott, Tuskó Hopkins és Fülig Jimmy szerelemgyermeke némi Google Translate nyers-fordítói segítséggel fűszerezve. **"*Rendszerünk tudomásul veszi, hogy még nem aktiválta az új K&H mobilbank biztonsági szolgáltatást, így könnyedén ellenőrizheti KH-fiókját:*".**

A fenti a hivatalosság látszatát imitáló mondat azért elég árulkodó. A csapatmunkába Török Szultán is láthatóan bekéredzkedett: **"*Ez az innovatív és biztonságos biztonsági szolgáltatás minden ügyfél számára hitelesített hitelesítési rendszeren alapul.*"** A klasszikus szófordulattal élve: persze hogy tudtuk, csak nem sejtettük.



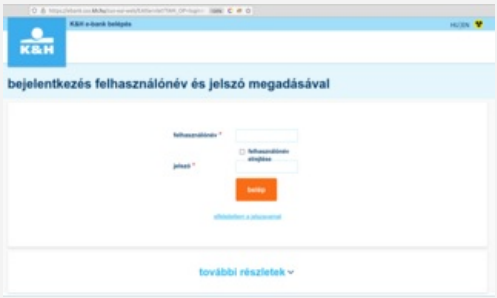
A zsenge nyelvi képességek mellett **érdemes egy pillantást vetni magára a feladóra is**, amely nem annyira tűnik egy hivatalos küldőnek: "K&H - Kereskedelmi es Hitelbank <markmcneil KUKAC bellaliant PONT net>".

De még ha esetleg ügyfelek is lennénk, és nemcsak így hasraütés szerűen küldték volna ki ezt egy rakat ismeretlennek, a mellékelt linkek akkor is megálljt parancsolna a figyelmes tekinteteknek: **nehogy már a bank linkje egy francia Wordpressel létrehozott oldalra mutasson**. Szóval hemzsegnek itt a kamuszagú intő jelek, csak a strigulákat kell húzogatni.



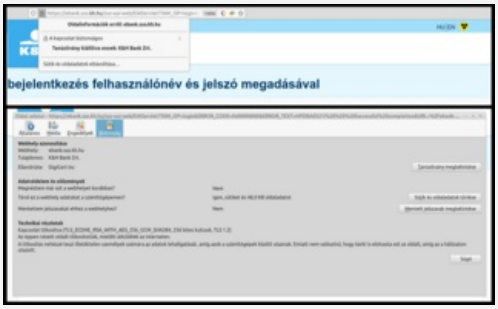
Ha az áldozat rákattint a **"*Most kövesse az utasításokat a "K&H mobilbank" aktiválásához*"** vagy az **"*Ide kattintva jelentkezzen be online fiókjába.*"** link valamelyikére, úgy egy adathalász oldalon találja magát. Eredetileg egy francia cég weboldala a link, amelynek egy manipulált aloldala jelenik meg mint K&H bank belépési oldal. Pár órával későbbi újabb próbálkozás után már egy francia étterem Wordpress oldala tűnik elő.

Emlékezetes, hogy a tavaly májusi csomagküldős átverés is valamilyen Wordpress sebezhetőség tömeges kihasználásával indult, itt is hasonló lehet az ok. A banki hasonmás oldal pedig személyes adatokat kér tisztelettel: szabad neki begépelni **a felhasználónév és jelszó párost, valamint a telefonszámunkat is szeretnék megkapni.**

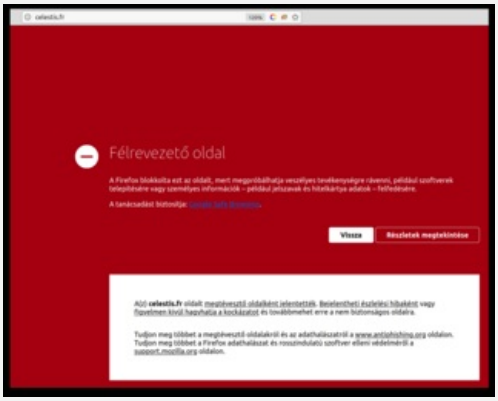


Érdemes lehet ilyenkor egy kört futni a tanúsítvány ellenőrzéssel is, amiből sok minden látszik, még ha a csaló oldalon https kapcsolatról is van szó, lakattal a fedélzeten.

Jól látható, hogy bank igazi weboldalán nemcsak az URL van rendben, hanem a digitális tanúsítvány is érvényes és hiteles.



Az email trace tanúsága szerint ezúttal **Kanadából küldték ezt a spam levelet**, egy lehetséges utánanézési lehetőség erre, ha az üzenet fejlécét megjelenítve (CTRL + U) annak elejét bemásoljuk pl. a DNSChecker weboldal erre szolgáló ablakába. Hűha, akkor talán mégsem a bank küldte ;-)



A weboldalt azóta letiltották, nyilván közben a bűnözők tíz másik helyen viszont továbbra is próbálkoznak.

Reméljük, már sokkal többen mosolyogva szórakoznak, semmint megijednek vagy áldozatul esnek az ilyen erősen színvonaltalan átverési próbálkozásoknak.

6 komment
Címkék: bank csalás átverés k&h adathalászat adatlopás

Ajánlott bejegyzések:


Továbbra is célkeresztben a banki adataink

Banki meló


A bankos mindig kétszer csenget...

Ismét csomagunk érkezett - vagy mégsem?


Viva la Revolut

Kommentek:

Head Honcho 2022.01.27. 19:58:45

Sajnos joggal alapoznak arra, hogy az egyszeri egyorrú user azt se tudja, mi az az url. Kérdés, iskolában vajon mit oktatnak informatika órán, már ha létezik ilyen? Mert ha nem, igény az volna rá!

Válasz erre

Sinkapeter 2022.01.27. 21:02:56

A K&H-tól érkező e-mailekben a megszólítás után zárójelben egy ideje ott az ügyfél telefonszáma (persze a közepén csillagozva). Így talán a kevésbé informatikai vénájúak is meg tudják különböztetni az igazit a csalástól.

Válasz erre

Androsz • http://wikipedia.blog.hu/ 2022.01.27. 22:26:37

@Head Honcho: Elmondjuk a gyerekeknek, hogy kattintás előtt ellenőrizzék a linket, de ötből csak három figyel oda rá, csak egy jegyzi meg, és pár év múlva ő is elfelejti. Ráadásul a böngészők mobiltelefonokon nem kezelhetők úgy, mint számítógépen, nincs egérmutató, amelyet kattintás előtt ráviszünk a linkre, a státuszsor sem mindig látható, néha az oldalak még a címsort is eltüntetik. Ez a szélhámosság nem teljesen hülyeség, sajnos, kevés embernek van meg a rutinja ezek megfigyeléséhez.

@Sinkapeter: Hát ez nem valami izmos segítség. Nem úgy hangzik, mint aminek azonnal riadót kellene fújnia az átlagfelhasználó átlagfejében.

Válasz erre

Sinkapeter 2022.01.28. 07:22:21

@Androsz: Lehet, hogy nem a legtökéletesebb, de egyszerűbb egy alapszintű tudással bíró embernek azt megjegyezni, hogy akkor valódi a levél, ha ott a neve és a száma, mint megnézni a linket, a valós feladót, esetleg a forrást.

Válasz erre

IamTwo 2022.01.28. 20:58:37

@Head Honcho: ezen szörnyülködök én is évek óta. Tanulják a rövidítéseket LAN, WAN, HDD. Tudnak Wordben boldra formázni (bár a 16space és a 2 tab közötti különbséget nem tudják). Scratchben bohóckodnak néhány órát. Nálunk 5. - 9. évfolyamon nagyjából ennyi történt. Az iskolában.
Nem tudom hol tanít Androsz, de biztosan nem ott, ahova az én gyerekeim járnak :(

Válasz erre

IamTwo 2022.01.28. 21:00:36

Amúgy jó ez a sok ellenőrzés, de felesleges.
Egyszerűen: soha semelyik bank nem küld ilyen email-t.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Fogyókúra automata üzemmódban

2022. január 31. 13:03 - Csizmazia Darab István [Rambo]

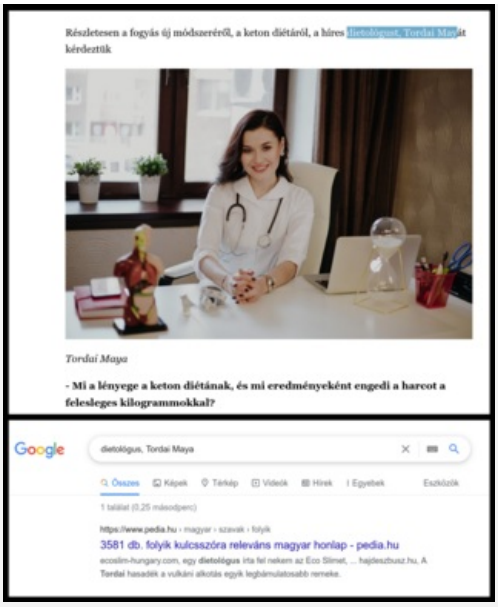
Nincs új a nap alatt, csodás fogyókúra tematikánk korábban már többször is szerepelt a posztok között, az egyik legemlékezetesebb talán a Fogyjunk le csokival kezdetű átverés volt. Mivel a probléma örök, sőt a pandémiás időszak sokaknál még a kevesebb mozgást indukált, folyamatosan ömlenek ránk a kéretlen ajánlatok, amik közül most egy újabbnak járunk utána.

Az vagy, amit elhiszel - facsarhatnánk ki az eredeti mondást úgy, hogy még így is maximálisan igaz maradjon, sőt.

Idézzük fel előzetesen, miket szoktunk figyelni egy kéretlen üzenet, adathalászati próbálkozás kapcsán: **csali ígéret, amivel hihetetlenül jól járunk majd, helyesírási és ékezet hibák a szövegben, közeli rokonság a Google Translate nyers-fordított nyelvezetével, és persze akciós ár.** Ezek itt mind szépen sorakoznak mai munkadarabunknál, amelynek címe **"*Nem fogyni nem lehet!*".**

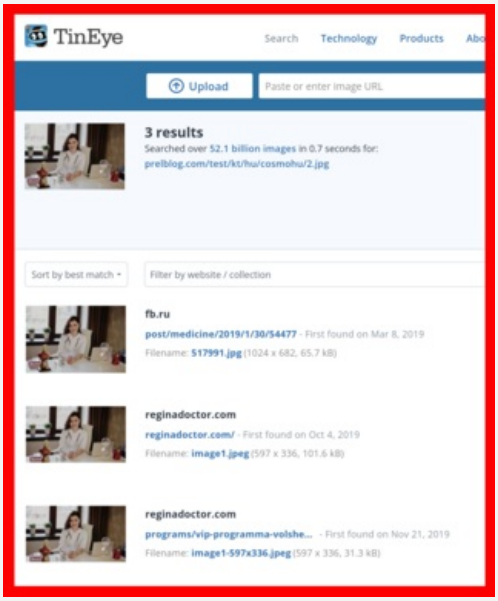
Kezdjünk is pár jellegzetes idézettel, milyen zseniális segítséget kaphatunk: **"*A közismert táplálkozási szakember egy új, fogyás trendről beszélt - el keton étrendről, amely belső zsírt éget egy teljesen automatikusan.*"** Aztán van ilyen is: **"*Az új módszer segítségével nem lehet nem lefogyni, mivel a bőr alatti zsírral biokémiai folyamatok szintjén folyik a harc.*".**

Sőt hogy milyen egyszerű az úgynevezett módszer, arról megtudhatjuk, hogy: **"*Teljesen automata üzemmódban megy végbe. Maga az ember semmilyen negatív hatást nem érez, nem kell sportolnia a fogyáshoz, nem kell éheznie. Ha megszokásból minden nap a mérlegre áll, akkor a keton szedésekor minden nap a testsúly csökkenését fogja tapasztalni.*"**



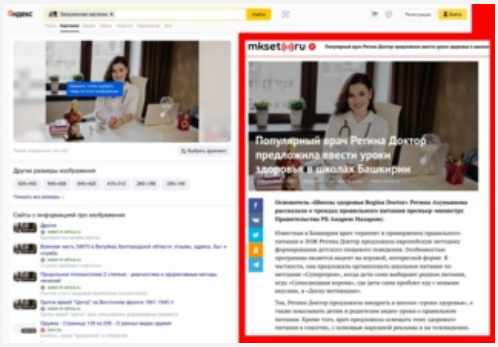
Az európai ember türelmetlen, megszokta, hogy mindent azonnal akarjon, csak befizeti a pénzt, és máris erőfeszítés nélkül jöjjön az eredmény: instant leves, megvilágosodást ígérő tábor, 48 óra alatt elsajátítható profi nyelvtudás és hasonlók.

A gyors eredmény ígéretet itt is megkapjuk, ezt írják az oldalon: **"*Részletesen a fogyás új módszeréről, a keton diétáról, a híres dietológust, Tordai Mayát kérdeztük*".**



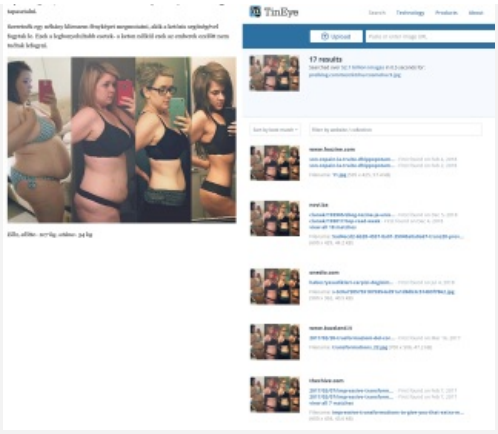
Akkor most táplálkozástudományi szakismeretek nélkül, faék egyszerűséggel csak és kizárólag az igazmondás irányából nézzük meg, ki ez a híres Tordai Maya dietológus. Vagy elég rosszul menedzseli SEO-ját, vagy nem publikál eleget a világhálón, a Google kereső a nevére nem igazán bőbeszédű.

Ám aki emlékszik, hogyan boncoljuk fel az ilyen csalásokat, emlékezhet a fordított képkeresésre, induljunk hát el erre, nézzük meg Tordai Maya "Magyarországon világhírű" dietológus fotójára mit köp ki TinEye szolgáltatás. Ez utóbbi böngésző kiegészítőként is elérhető, és kényelmesen használható.



Nos hát ez felettébb érdekes, itt **a képen Tordai Maya helyett Regina Akhunyanova szerepel, egy orosz Regina Doktor klinikáról néz velünk szembe mosolyogva**. Most vagy egypetéjű ikrek, akiket két különböző országban fogadtak örökbe, vagy esetleg hamis a kép - tanácstalanok vagyunk.

Akkor nézzünk meg most néhányat Tordai "doktornő" páratlan eredményei közül.

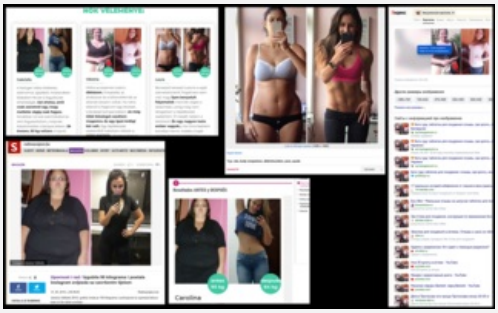


"Szeretnék egy néhány kliensem fényképet megmutatni, akik a ketózis segítségével fogytak le. Ezek a legbonyolultabb esetek- a keton nélkül ezek az emberek ezelőtt nem tudtak lefogyni. Ella, előtte- 107 kg, utána- 54 kg".

Jöjjön a rutinszerű képkeresés, és az eredményekből az látható, a magyar Ella török és orosz weblapokon is látható, esetleg nem is Ella?

Éva fotóinak keresése pedig Maria Quinones néven ad találatokat.

Ezek után meg sem lepődünk, hogy Maria, aki **"*előtte- 105 kg, utána- 55 kg*"** szintén számos orosz oldalon szerepel, felvetve az a nyugtalanító dilemmát, hogy a két képen itt sem ugyanazt a személyt láthatjuk esetleg netalántán.



Szerencsére van link az oldalról az igazi egyetlen hiteles, korrekt és egységes, tévedést kizáró "hivatalos" webhelyhez is, amely további látványos sikereket mutat. **Viktóriából egész oroszországi arzenált láthatunk a keresési eredményekben. Gabriellára rákeresve a találatokból kiderül, máshol ő valójában már Jessica Valitutto, esetleg megint máshol mint Carolina szerepel, ki érti ezt?**

Laura pedig Kayla Itsines néven köszön vissza a képkeresés után - egyedül talán az ő képei után látszik hihetőnek legalább az a rész, az előtte-utána fotók azonos személyről készülhettek.

Szintén van tapasztalatom a KETO DIET szedésében és szintén pozitív. 98 kg voltam, most 81 kg. Meg vagyok elégedve.
Bárány Tamás

Részletesen elolvastam mindent a KETO DIET-ről. Végre valahára, a tudósok valami érdemlegeset is felfedeztek!
Viki

Ez tényleg valami nagyon jó dolog! Nem nagyon bíztam benne, hogy ez a készítmény segít nekem. Mert a többi sem segített, de már 3 kg fogytam! Mindössze 4 napja szedem a KETO DIET-et. Az étrendemet nem módisítottam
R. Mária.

Ilyen készítményt akarok! Szaladok, hogy amíg készleten van meg tudjam rendelni.
Kovács Rebeka

Együtt a férjemmel fogytunk. Amint a készítmény megjelent az ismerős dietológusunk javasolta. Most már vékonyak vagyunk, ketten együtt 41 kg dobtunk le, most már egészséges életmódot folytatunk. Vékonynak lenni, ez valami gyönyörűség!
Valéria

Az össze barátnőm csak a KETO DIET-ről beszél. Segítségével sokan közülük lefogytak. Ez egy valódi hit a barátnőimnél
L. Éva.

Köszönet. Ez egy nagyon jó hír
Nagy János

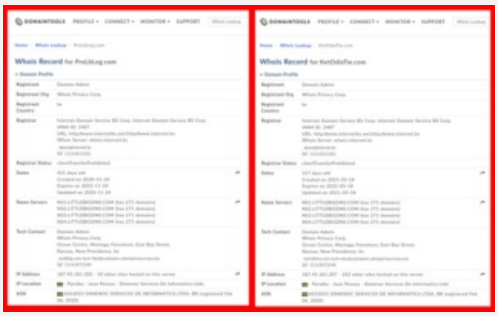
Én szintén fogytam a KETO DIET segítségével!!! 18 kg 7 nap alatt. Eddig, ilyen mértékben még soha nem fogytam. Sok köszönet a cikkért!!!
Ildi

Megrendeltem. Akcióban még van készítmény, de már nagyon kevés maradt
D. Fanni.

A KETO DIET hivatalos honlapja Magyarország

A visszajelzések, értékelések minősége, hihetősége is megér egy misét. **"*Ilyen készítményt akarok! Szaladok, hogy amíg készleten van meg tudjam rendelni. - Kovács Rebeka***" vagy **"*Köszönet. Ez egy nagyon jó hír - Nagy János*".**

De van itt ilyen is: **"*Én szintén fogytam a KETO DIET segítségével!!! 18 kg 7 nap alatt. Eddig, ilyen mértékben még soha nem fogytam. Sok köszönet a cikkért!!! - Ildi***" Szóval hitelesség tekintetében valahogy a tízes skálán inkább a mínusz egyhez közelítőnek tűnik számunkra.



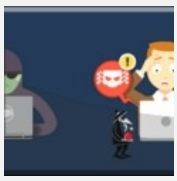
Képekből, értékelésekből ennyi éppen elég, nézzünk akkor még rá érdekességképpen a domainekre is, ki foglalta le azokat. **A .bs végződés a Bahama-szigetek internetes legfelső szintű tartomány kódja, onnan regisztrálták a Brazíliában üzemeltetett oldalt**. A "hivatalos" weboldalnál is ugyanez a felállás, csak ott 2021-es a bejegyzés dátuma.

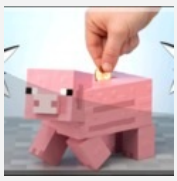
Itt a vége, fuss el véle. Ha még emlékszünk a minden évben karácsony tájékán felelevenített hogyan és honnan vásároljunk biztonságosan posztot, ott többek között **olyanok szerepelnek, mint meglévő adatvédelmi szabályzat, magyarországi telephely és hivatalos elérhetőség, biztonságos fizetés, leinformálhatóság, érvényes megbízható tanúsítvány, korrekt visszajelzések, ilyesmik.** Hát ezeknek itt nem sok nyomát lehetett találni, szóval **addig is marad a diéta és a sok testmozgás, sőt inkább életmód változtatás, ahol valóban várható változás. Igaz nem azonnal és a munkát, odafigyelést is bele kell fektetni az egyik oldalon, hogy kijöjjön az eredményesség a másikon.**

Fakenews sújtotta korunkban mind a híreket, mind a reklámok hihetőségét érdemes fontolóra venni, több forrásból ellenőrizni, józan paraszti ésszel és biztonságtudatos hozzáállással kezelni, hogy kevesebb csalódásban legyen részünk.

2 komment
Címkék: csalás átverés hamis fogyokúra

Ajánlott bejegyzések:


Üzleti e-mail hamisítás


A csalások már a spájzban vannak


VPN appok Androidra vagy mégsem?

Nagy pénz, nagy foci, nagy átverések


Csupasz pisztoly hívja felhasználót, vétel!

Kommentek:

Péter 2 2022.01.31. 17:20:50

"Ha honlapján személyes adatokat, jelszavakat, bankkártya információkat kér be, akkor semmiképp ne válasszon ingyenes SSL tanúsítványt."

A többi stimmel, de ilyen ökörséget hol tetszett olvasni? :-) Az ilyet elhinni kábé ugyanannyit ér, mint az ilyen fogyókurás ajánlatokat elhinni.

Válasz erre

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2022.01.31. 18:09:59

Szia Péter 2!

Igen, jogos az észrevétel:
www.forpsi.hu/ssl/

Köszi a kommentet.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.

VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

A nemzetközi helyzet egyre fokozódik

2022. február 02. 10:36 - Csizmazia Darab István [Rambo]

Összegyűjtöttük azokat a statisztikákat, melyek segítenek **2022-ben is naprakésznek maradni a legújabb támadási trendekkel kapcsolatban.**

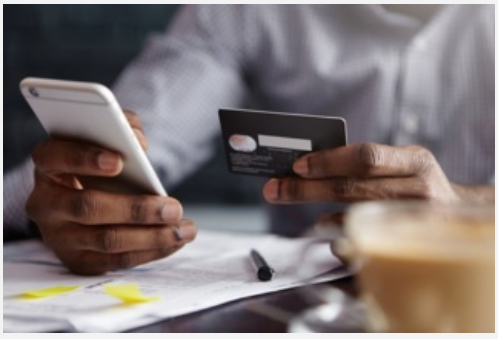
Annak érdekében, hogy idén is felkészülten nézhessünk szembe az internetes fenyegetésekkel, az alábbi statisztikai adatokat érdemes a következő hónapokban is észben tartanunk biztonságunk és adataink védelme érdekében.

A listával az ESET szakemberei azt szeretnék érzékeltetni, hogy a kiberbiztonság áthatja a digitális életünk minden szegletét, ezért semmiképp sem érdemes sokadrangú szempontként kezelni. **Íme a 12 legfontosabb és legérdekesebb statisztikai információ.**

1. 17 éves csúcsot döntött az adatvédelmi incidensek költsége 2021-ben: az átlag költség mértéke évi 3.86 millió dollárról 4.24 millió dollárra emelkedett. Ez 1.07 millió dollárral volt magasabb azokban az esetekben, ahol a távmunka is szerepet játszott az adatsértésben.

Az adatvédelmi incidensek mögött álló leggyakoribb indíték a felhasználói adatok ellopása volt. (Forrás: az IBM 2021-es adatsértések költségeit vizsgáló riportja)

2. Az adatsértések 36%-a adathalász-támadásokhoz kapcsolódott, ami 11%-os növekedést jelent - ez részben a koronavírus-járványnak tudható be. Ahogy az várható volt, a kiberbűnözők mindig az aktuális hírekre, az embereket leginkább foglalkoztató témákra építették az adathalász kampányaikat. (Forrás: a Verizon 2021-es adatsértés riportja)



3. 2021-ben erőteljesen megnőtt a mobilbankos kártevők észlelése az Android eszközökön. Az év első harmadában drasztikus, 158.7%-os növekedés volt észlelhető, a második harmad pedig további 49%-os növekedést hozott. Kifejezetten aggasztó tendenciáról van szó, hiszen a mobilbankos trójai kártevők hatalmas anyagi károkat

okozhatnak az áldozatoknak. (Forrás: az ESET 2021. második harmadéves vírusriportja)

4. A kriptovalutákra épülő befektetési csalások sajnos továbbra is rendkívül gyakoriak. 2020. októbere és 2021. májusa között több, mint 80 millió dollárt csaltak ki ezzel a módszerrel az áldozatoktól. A tényleges összeg vélhetően még ennél is magasabb, mivel sokan szégyellik bevallani, hogy átverték őket. (Forrás: az USA Szövetségi Kereskedelmi Bizottsága)

5. Az úgynevezett "social engineering" azaz az emberi megtévesztésre építő támadások jelentik a legnagyobb veszélyt a közigazgatási szervezetek számára, ugyanis a 2021-es közigazgatási adatsértések 69%-át éppen ezek tették ki. (Forrás: a Verizon 2021-es adatsértés riportja)

6. A Log4Shell, a Log4j naplózó segédprogram súlyos sebezhetőségének 2021. decemberében történő nyilvánosságra kerülése után az ESET több százezer támadási kísérletet észlelt és blokkolt, amelyek többsége az Egyesült Államokban és az Egyesült Királyságban történt. (Forrás: ESET kutatás)

7. Az elmúlt években a kiberbűnözők elkezdtek áttérni az egyszerű zsarolóvírusról a dupla zsarolásra (doxing), vagyis azzal fenyegetőztek, hogy a váltságdíj fizetés elmaradása esetén eladják vagy nyilvánossá teszik a titkosítás során megszerzett adatokat. Az ilyen jellegű fenyegetések száma drasztikusan megnőtt: 2020-ról 2021. második negyedévére 8.7 százalékról 81 százalékra ugrott. Ezzel együtt pedig jelentősen növekedtek a zsarolóvírus-támadások elhárításának összköltségei is. (Forrás: ENISA 2021-es vírusriport)

8. 2021 közepén az IT-menedzsment szoftverszolgáltató Kaseya rendszereit megtámadták a Sodinokibi zsarolóprogrammal, az elkövetők 70 millió dolláros váltságdíjat kértek - ez lett minden idők eddigi legnagyobb váltságdíj követelése. (Forrás: az ESET 2021. második harmadéves vírusriportja)

9. A szolgáltatásokat ellehetetlenítő túlterheléses DDoS-támadások száma is emelkedő tendenciát mutat, részben a koronavírus-járványnak köszönhetően. 2020-ban több, mint 10 millió ilyen támadás történt, amely 1.6 millióval több, mint az előző évben. (Forrás: ENISA 2021-es vírusriport)

10. Négy évvel az első észlelés után a WannaCryptor (másik ismert nevén WannaCry) továbbra is globális fenyegetést jelent. A május és augusztus közötti zsarolóvírus-észleléseknek még mindig a 21.3 százalékát tette ki ez az EternalBlue sebezhetőséggel rendelkező gépeket támadó trójai kártevő. (Forrás: az ESET 2021 második harmadéves vírusriportja)

11. Globális szinten még mindig hiány van: a kiberbiztonsági munkaerőnek 65%-kal kellene növekednie ahhoz, hogy elegendő számú szakember jusson a szervezetek legfontosabb eszközeinek hatékony védelmére. (2021-es kiberbiztonsági munkaerő riport)

12. Az idősek aránytalanul nagy mértékben esnek áldozatul a kiberbűnözésnek: az összes családhoz kötődő pénzveszteség 28%-át a 60 év felettiek szenvedték el. Ez 2020-ban körülbelül 1 milliárd dolláros veszteséget jelentett e korcsoport számára. (Forrás: IC3 2020 Elder Fraud Report)

Ezek a statisztikák csak a jéghegy csúcsát jelentik, amikor az egyéneket és a szervezeteket fenyegető veszélyekről van szó. De talán ennyiből is jól érzékelhető, milyen hatalmas mértékű és **elképesztő nagyságrendű a kiberfenyegetések folyamatos fejlődése, és hogy az ellenük történő védekezést minden szereplőnek nagyon komolyan kell vennie, és minden eszközön érdemes gondoskodnia a megbízható védelemről, megelőzésről.**

Szólj hozzá!
Címkék: statisztika fenyegetés eset adathalászat kiberbiztonság welivesecurity.com 2022. tigris-éve

Ajánlott bejegyzések:


Oroszország lett a fő kibercélpont


Beváltak-e a 2021-es jóslatok?

Kis- és középvállalkozások adatvédelmi incidensei


Ezer százalékkal nőtt, maradhat?


Durva ransomware statisztikai adatok

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Antivírusblog
245 követő

Oldal követése Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

Esemény utáni teendők

2022. február 07. 10:31 - Csizmazia Darab István [Rambo]

Írtunk már korábban egy olyan posztot, amely a feltört postafiók helyzettel, vagy ennek gyanújával foglalkozott. Ebben **összefoglaltunk pár olyan szükséges lépést**, amit a további visszaélések elkerülése érdekében tanácsos volt elvégezni. Mivel közben már **több hasonló kérdés is érkezett - közösségi oldali account, levelező fiók, vagy ellopott kriptovaluta problémával, összeállítottunk egy hosszabb checklistet, amely tanácsaival a védelmi teendők mellett az incidens okainak felderítésében is segíthet.**

Milyen lépéseket érdemes megtenni, illetve miket érdemes ellenőrizni, végiggondolni, ha valakinek feltörték a levelezését, illetéktelenek beléptek a közösségi oldali fiókjába, vagy a biztonságosnak hitt virtuális tárcájából ellopták a kriptovalutáját? Kérdőjel halmozó posztunk következik...

A kárvallott tulajdonos oldaláról ezek a felteendő kérdések:

- a tulajdonos egyedül rendelkezett a wallet jelszavával, vagy megismerhette-e azt rajta kívül más harmadik személy is?

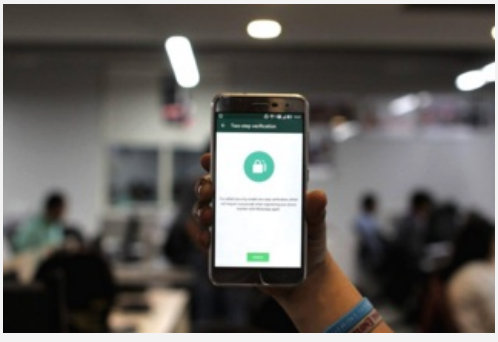
- milyen eszközön kezelték a fiókot, tárcát: mobileszköz, számítógép, esetleg mindkettő, vagy több gépről is?

- fizikailag hozzáférhetett-e illetéktelen az eszközökhöz (családtag, alkalmazott, takarító, idegen)?

- volt-e az eszközö(kö)n naprakész vírusvédelmi alkalmazás (sok kártevő képes észrevétlenül adatokat, jelszavakat lopni)?

- megtörténtek-e időben a számítástechnikai eszközökön a rendszeres hibajavító frissítések (a javítatlan, foltozatlan hibákon, sebezhetőségeken támadnak a kiberkártevők)?

- kattintottak-e a közelmúltban gyanús kéretlen levélben érkező linkre, e-mail mellékletre?



- hívta-e őket bank, vagy más hivatal nevében és diktáltatott-e be a károsult "ellenőrzésképpen" személyes adatokat telefonban (ez is a csalók egyik kedvelt módszere)?

- volt-e a tárcához kétfaktoros autentikáció (többtényezős hitelesítés), amely kizárja a sima név-jelszó lopása esetén az illetéktelen hozzáférést? Ha volt, ez be volt-e kapcsolva?

- volt-e olyan lehetőség, hogy a Google, Facebook, LinkedIn fiókok védelméhez hasonlóan azonnali értesítést kérjen, ha valaki illetéktelenül megpróbál bejelentkezni a fiókjába? Ha volt, ez be volt-e kapcsolva?

- ha mobiltelefon is érintett volt, Apple vagy Android rendszerű?

- ha androidos telefon, milyen alkalmazások voltak telepítve, ezeknek milyen engedélyek voltak megadva?

- az otthoni netes router adminisztrációs jelszava meg lett-e változtatva a vásárláskor, beszereléskor? sok eszköz az alapértelmezett (default) jelszót használja, amit támadók egyszerűen kiolvasnak egy adatbázisból, és máris átvehetik az irányítást, vagy illetéktelenül hozzáférhetnek a netes forgalomhoz

- az otthoni netes router wifi jelszava meg lett-e változtatva a vásárláskor, beszereléskor?

- a wifi titkosítása legalább WPA2-PSK szintű volt?

- A fiókhoz, vagy kriptotárcához és a wifihez való jelszó teljesen egyedi volt, vagyis sehol máshol nem használták ugyanezt a jelszót? Ha egyforma jelszót használnak, akkor egy harmadik helyszín feltörésével megszerzett jelszavakat a támadók végig szokták próbálni az összes lehetséges szolgáltató webhelyén, hátha szerencsével járnak, és sajnos gyakran ez a helyzet.

- erős volt-e a használt jelszó? Legalább 12 karakter hosszú, kis és nagybetűket, számokat és speciális karaktereket egyaránt tartalmazott és nem könnyen kitalálható szótári szó volt?

- kapcsolódtak-e korábban nyitott, jelszó nélküli wifi hotspot hálózathoz? Ilyenkor könnyen ellophatják az adatokat, korábbi jelszavakat.

- megjegyeztették-e a név-jelszó párost a böngésző jelszókezelőjével? Onnan sajnos sokkal egyszerűbb ellopni, mint egy speciális jelszószéf (Bitwarden, Enpass, stb.) célalkalmazásokból.

- felvehette-e kamera illetéktelenül a fiókba, vagy wallet tárcába való belépést, kifigyelve a jelszót?

- állhatott-e ismeretlen, illetéktelen személy a háta mögött, a fiókba, wallet tárcába való belépéskor, kifigyelve a jelszót?

- ismerhette-e illetéktelen személy az otthoni wifi elérési jelszavát (barát, szomszéd, vendég, alkalmazott, stb.)

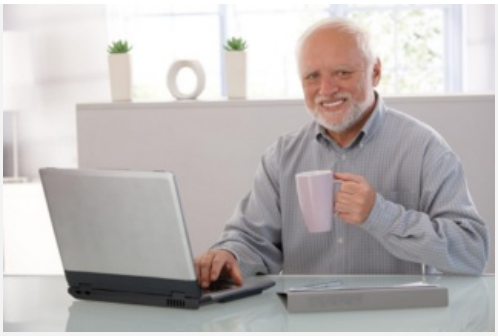
Az igénybe vett szolgáltatás üzemeltetőit is érdemes megkeresni, kárvallott tulajdonos oldaláról ezek a felteendő kérdések:

- történt-e hivatalosan írásbeli kérdés, panaszbejelentés a szolgáltató felé, kriptovaluta esetén az eltűnt összeg miatt?

- sajnos időnként feltörnek ilyen jellegű szolgáltatókat is, pl. itt egy hasonló eset a sok közül: https://www.vice.com/en/article/ywkw9j/etherscan-l337-hack

- érdemes megtudakolni tőlük, hogy ezzel egy időben több ügyfelet is érintett-e a dolog, mert akkor nagyobb lehet arra esély, hogy kompenzálni fognak bennünket. Ennek az interneten is utánanézhetünk.

- végig futni még az általunk korábban elfogadott EULA-t, hogy mit írnak az ilyen esetekre.



A fentiek fényében a szükséges lépések megtétele, bank, szolgáltató, hatóságok, miegymás.

- alapos vírusvédelmi ellenőrzést futtatni a telefonon, tableten, számítógépen, nincs-e rajta vírus, kémprogram

- haveibeenpwned.com weboldalon a kiszivárgott jelszavak közt ellenőrzést végezni

- ellenőrizzük az össze többi fiókunkat is

- fontosabb fiókjainkban is azonnal cseréljünk jelszót

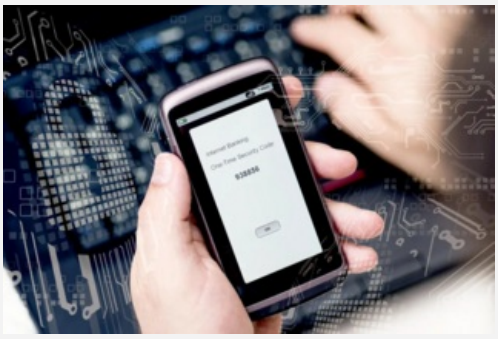
- fontosabb fiókjainkban ismételten ellenőrizzük le a biztonsági beállításokat

- értesítsük barátainkat, ismerőseinket az incidensről, nehogy a nevünkben esetlegesen posztolt üzenetekkel megtévesszék őket

- bankszámlát is érintő csalás esetén a bank azonnali értesítése, szükség esetén a számla/kártya letiltása

- SIM kártyát érintő csalás esetén a mobilszolgáltató azonnali értesítése

- minél több konkrét technikai részlet, képernyőkép melléklettel a kerületi rendőrkapitányságon feljelentést tenni

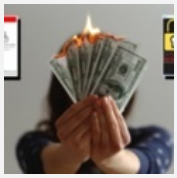


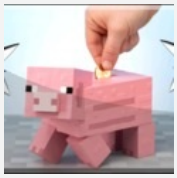
Ezt az alap (és még a végtelenségig bővíthető) checklistet lehet első körben végiggondolni, ellenőrizni, megtenni. Ha valakinek a fentiekhez hozzáfűzni valója lenne, természetesen kommentelni ér :-)

1 komment
Címkék: jelszó incidens megelőzés felderítés feltörés hitelesítés védekezés jelszólopás teendő kárelhárítás kétfaktor kéttényezős

Ajánlott bejegyzések:


Ha nincs az a baj, ha van akkor az a baj


Fejemen olvad a vaj, engem nem érhet baj


A csalások már a spájzban vannak

Még gyengébb a jelszavad


10 gyakori IT biztonsági hiba

Kommentek:

gigabursch 2022.02.07. 13:31:33

Ez a cím...

Rögtön eszembe jutott egy találós kérdés:
- Mit tesz az erdész esemény utáni védekezésként?
- ???
.
.
.
- Lelövi a gólyát!

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

- RSS 2.0
  bejegyzések, kommentek
- Atom
  bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

Netwalker tag menni 6 év börtön

2022. február 09. 12:31 - Csizmazia Darab István [Rambo]

A kicsit Boratos cím ellenére komoly dologról van szó: **sajnos igen-igen ritka esemény, hogy elkapni és bíróság elé lehessen állítani olyan bűnözőket, akik ransomware bűnbandában tevékenykednek.**

Bizonyíthatóan tizenhét különböző megcélzott szervezet ellen intézett zsarolóvírusos támadást az ottawai Sebastien Vachons-Desjardins, akit a hatóságok most februárban hat év nyolc hónap börtönbüntetésre ítéltek. A férfi nemcsak aktív támadásokban közreműködött, de más bűnelkövetők betanításában is részt vett, tanítványokat is képzett.

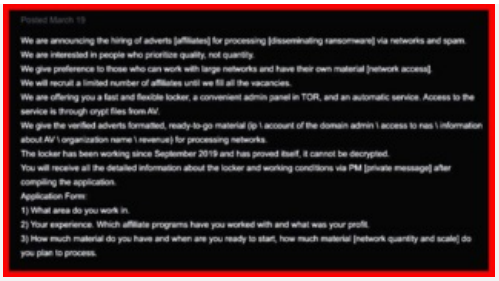
A letartóztatására tavaly év végén került sor, és az FBI azzal gyanúsította meg, hogy a vélhetően orosz gyökerű Netwalker banda tagjaként 27 millió dollárnyi váltságdíj zsarolásában vett részt.

A Netwalker (más néven Mailto) egy fejlett támadóeszköz, a 2019. óta ismert Windows alapú kártevőt az elemzők szerint elsősorban vállalati hálózatok, kormányszervek, oktatási intézmények ellen vetik be. A fertőzések leggyakrabban VBS (Visual Basic Script) fájlokkal, vagy rosszindulatú EXE fájlokkal terjedtek.

A kártevő a doxingot is alkalmazza, vagyis azt az utóbbi időben elterjedt módszert, hogy az adatok titkosítása előtt el is lopja azokat, így a váltságdíj követelés nemcsak arra terjed ki, hogy feloldó kulcsot kínáljon cserébe, hanem azzal is, hogy **nemfizetés esetén a lopott bizalmas adatokat feltöltik publikusan az internetre.**

Mint ismeretes, **a Netwalker a darknetes fórumokon RaaS (Ransomware as a Service), azaz bérelhető szolgáltatásként is elérhető volt**, vagyis a bérlőknek a zsarolóvírus támadásokért cserébe jutalékot fizettek.

Itt a blogon is írtunk többször már ilyen incidensekről, például a CWT Business Travel Management Company ügyéről, amely egy Minnesotában található utazási társaság és miután **2020-ban a hálózatukból 30 ezer számítógép állományait lopták és kódolták el, megszerezve mintegy 2 TB bizalmas céges adatot, végül kifizették a 4.5 millió dolláros váltságdíjat.**



A Lockbit csapathoz hasonlóan **ők is igyekeztek közvetlenül sértett munkavállalókat, bennfenteseket toborozni, és pénzjutalmat ígértek azoknak, akik saját céges RDP, VPN, levelező szerver, és egyéb belső vállalati rendszereikhez hozzáférést, jelszavakat** adnak ki a bűnözőknek. A most elítélt elkövető a **2020. májusa és 2021. januárja közötti kilenc hónapos időszak alatt több, mint 2000 BTC összegű (kb. 27mrd HUF) bevételhez jutott a ransomware támadásokból befolyó váltságdíjakból.**

A házkutatás során 600 ezer dollár készpénzt, 400 ezer dolláros bankbetétet foglaltak le nála, amelyet a bíróság az áldozatul esett szervezetek kárpótlására kíván fordítani, többek közt egy helyi főiskola, egy biztosító társaság, autókereskedés, és egyéb intézmények.


Handelsblatt

Cyberangriff legt Oiltanking-Tanklager deutschlandweit vollständig lahm – Tankwagen-Beladung außer Betrieb

Zwei Tochterunternehmen des Hamburger Konzerns Marquard & Bahls sind Opfer von Hackern geworden. Mittelständische Tankstellen, aber auch Konzerne wie Shell sind betroffen.

Az Egyesült Államok kérelmezte a bűnelkövető kiadatását, ez még további fejleményeket hozhat az ügyben. **Sajnos a különféle ransomware támadások általánosságban folyamatosan napirenden vannak, pár napja a svájci reptéren történt ilyen incidens, ahol késéseket, járatkimaradásokat okozott az eset.**

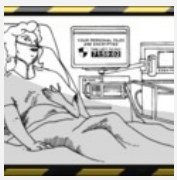
De a emellett például két németországi olajszállítót is megtámadtak, ami miatt a Shell arra kényszerült, **hogy más raktárakba irányítsa át az olajszállítást.** Szóval zajlanak az események.

Szólj hozzá!
Címkék: börtön bíróság kanada ítélet váltságdíj ransomware zsarolóvírus netwalker

Ajánlott bejegyzések:


Addig jár a REvil a kútra...


Összeomlás


Nem csitulnak a kórházak elleni támadások


Emelkedő ransomware károk


Nem szállunk rendelkezésére II.

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Swatting - új köntösben

2022. február 11. 13:52 - Csizmazia Darab István [Rambo]

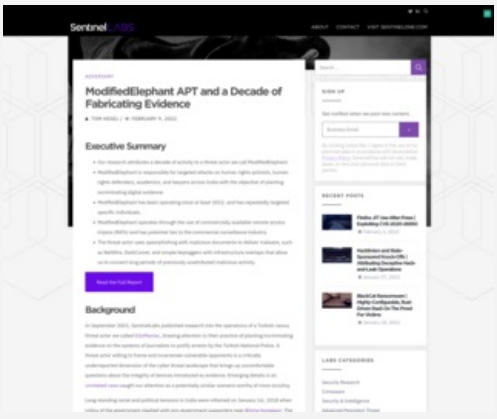
A klasszikus "átverés", amely néha halálos áldozattal is jár **azon alapul, hogy valaki ki akar tolni egy másik emberrel, és ezért segélyhívás keretében hamisan arról értesíti a rendőröket, hogy az illető az illető fegyveres, közveszélyes, például épp az imént végzett egy családtagjával, és hogy a terrorelhárítók jöjjenek ki azonnal, adjuk a címet.**

Ilyenkor - a hamis bombariadóhoz hasonlóan - mivel minden bejelentést ellenőriznek, jó esetben csak rárúgják az ajtót és rájönnek, hogy vakriasztás volt. Rosszabb esetben megszégyenítő gyanúsítás, letartóztatás lesz a vége, vagy az ijedtség miatt szívroham, esetleg egy suta félreérthető mozdulat miatti agyonlövetés. Sajnos mindegyikre láttunk már példát, sokszor ehhez elég egy online játékban kikapni valakitől, de az **ilyen aljadék bosszú elérte már a világhírű biztonsági szakértőt, Brian Krebset is.**

Mivel előtte leleplezett egy bűnbandát a blogján, bosszúból spam és gyermekpornó anyagok terjesztésével vádolták meg névtelenül, és **észak-virginiai otthonában igen hamar felfegyverzett rendőrökkel találta magát szembe - szerencsére végül kiderült a hamis vád.**

Mindez azért került most elő, mert a TheRegister egy friss cikke foglalkozik egy "ModifiedElephant" nevű kártevővel, amely nemcsak kémprogram, amely észrevétlenül megfigyelni, ellopni képes bizalmas adatokat az áldozat számítógépéről, de **2013. óta bizonyíthatóan arra is többször használták, hogy kompromittáló adatokat, fájlokat - például terrorizmus, gyermekpornográfia - töltsenek fel az áldozatok eszközére.**

Akiket aztán feljelentve a házkutatáskor tényleg megtalálják a keresett "bizonyítékokat" - akárcsak a Tanú című Bacsó Péter filmben **a mindig már jó előre odakészített leltári dollár bankjegy zajos felfedezése.**



Az emlegetett ModifiedElephant kártevőt már évek óta használják, például indiai célpontok ellen többször is bevetésre

került, és ott letartóztatással, börtönbüntetéssel végződtek a történetek. Súlyosbítja a dolgot, hogy mindezt már nemcsak számítógépen, hanem immár androidos telefonon is véghez tudják vinni. **Technikailag egy kéretlen üzenetben egy fertőzött linket csatolnak, vagy pedig a levél melléklete egy sebezhetőséget kihasználó kártékony .doc, .pps, .docx vagy .rar fájlt hordoz.** Az egyik hivatkozott incidensben a megfigyelt Rona Wilson gépén 22 hónapig eleinte csak kémkedtek.

A módszer ellen **nehéz a védekezés, ráadásul reménytelen helyzetből bizonyítani is kellene a tervszerű összeesküvést.** Ezeknél az eseteknél pedig élesen felvetődik a fejlesztők, forgalmazók erkölcsi felelőssége is - emlékezhetünk például az Egyiptomban bevetett FinSpy (Finfisher) angol-német állami kémprogramra is, **amelynek számláit csak véletlenül találták meg jóval később civilek.**

A végére egy régi, de ebből a szempontból érdekes hasonló esetet érdemes megemlíteni. 2008-ban egy Michael Fiola nevű minisztériumi munkatársra azért figyeltek fel a főnökei, mert a céges számítógépén az átlagos internet forgalom négy és félszerese futott keresztül. A gépét ellenőrizve azon gyermekpornó anyagokat találtak, **emiatt meghallgatás nélkül azonnal kirúgták, és feljelentették ezek birtoklása miatt, ennek büntetési tétele akkor 5 év börtön volt.**

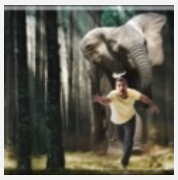
Közben névtelen halálos fenyegetéseket is kapott, az autója kerekeit rendszeresen kiszúrták, korábbi barátai, ismerősei kiközösítették. Feleségével hosszan harcoltak az ártatlanságot hangoztatva, ennek azonban hatalmas ügyvédi költségei (250 ezer dollár) voltak, így emiatt jelzálogot is kénytelenek voltak felvenni a házukra.

Kilátástalan történetükben végül az hozta meg a szerencsés fordulatot, hogy **egy Tami Loehrs nevű törvényszéki szakértő egy igen alapos elemzés után arra a következtetésre jutott, hogy egy olyan számítógépes kártevő fertőzte meg a számítógépet, amely percenként automatikusan és egyben teljesen életszerűtlenül 40 különböző pedofil oldalt látogatott meg. A vádat aztán ennek alapján 11 hónap után ejtették**, ami megkönnyebbülés volt, ám a férfi és családja életét eléggé tönkretették ezek az események.Vélhetően a bűnözők meg azóta már olyan kártevőt is írnak, amely csak 2 percenként lép át új oldalra.

Jó adalék egy ilyen hamis vád érzelmi terhének illusztrálására a kizárólag erős idegzetűeknek való Vadászat című 2012-es dán mozifilm, amely igen szemléletesen bemutatja, hogy **még egy esetleges felmentés után is hosszan, talán örökre megmarad a közegben gyanakvó légkör, a lincselő közhangulat, és az egzisztenciális bezuhanás sem marad el.**

Szólj hozzá!
Címkék: india hamis kémkedés bizonyíték feltöltés swatting kémprogram rat ModifiedElephant

Ajánlott bejegyzések:


Módosított elefánt a felhasználók porcelánboltjában


Hazugságok: messzebbre és gyorsabban


Nem szállunk rendelkezésére

Fogyókúra automata üzemmódban

Hol jársz, hová mész?

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Banki meló

2022. február 14. 10:21 - Csizmazia Darab István [Rambo]

Vagy mégsem rovatunkba azóta is áramlanak a próbálkozások, hogy nem is olyan régen a K&H mobilbank biztonsági szolgáltatással kapcsolatos átverésről írtunk. Azóta volt már hasonló a Takarékbank nevével visszaélve, és **most épp egy hamis CIB-es levél próbálkozik hasonló a megtévesztéssel.**

Itt a korábbi K&H bankoshoz képest is silányabb kivitelezést láthatunk, a szokásosnak mondható "Fontos" subject itt már "Fw:Fontos!" tárgysorral szerepel, felvetve a kérdést, ha valóban a bank írna nekünk, akkor legalább direktben tenné mindezt, nem továbbküldözgetve valamit.

A feladó leplezésére minimális erőfeszítést sem tettek itt sem, ír nekünk hivatalosan a CIB bank, közben a küldő helyén meg a "colin PONT macinnis KUKAC ns PONT sympatico PONT ca" cím szerepel. **Az aktiválás linkje pedig egy francia doménre mutat. Szinte nem is érdemes innen már továbbmenni.**

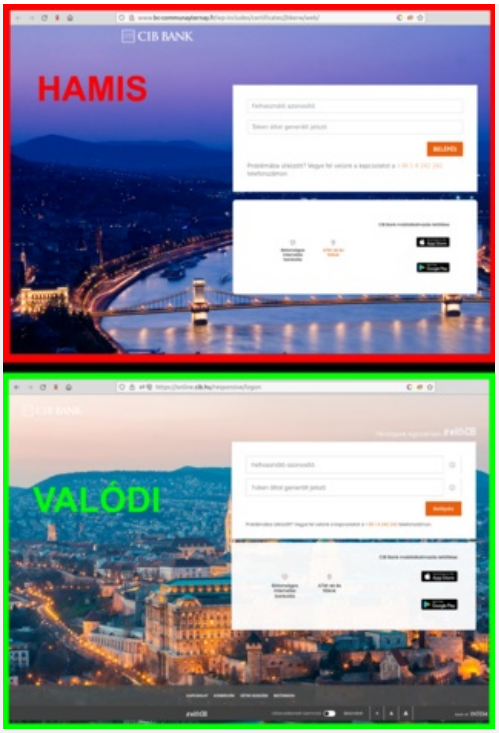
Az üzenet szövege a szokásos Tisztelt Ügyfelünk megszólítással kezdődik, és itt is kattintásra, nevezetesen mobilbank biztonsági szolgáltatás állítólagos aktiválására próbálnak minket rávenni:

"*Rendszerünk észleli, hogy Ön még nem aktiválta új biztonsági szolgáltatásunkat, a CIB Mobile -t, így könnyedén kezelheti CIB BANK számláját:*

Az SMS-ben kapott KÓD 2022. február végén törlésre kerül, mert az elektronikus tranzakciókra való reagálás hosszú ideig tart. Használja most az új ingyenes biztosítást"

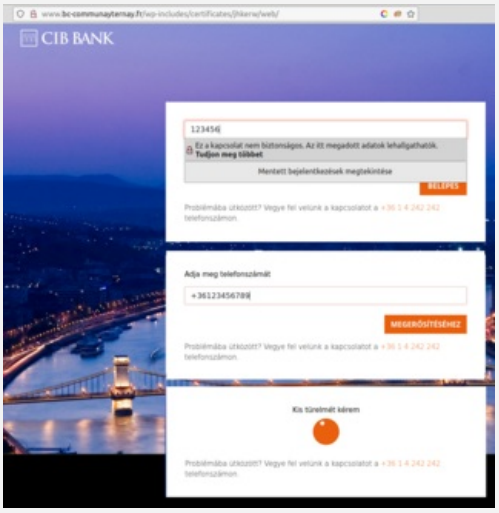
CIB Mobile , hogy azonnali online vásárlásait időveszteség nélkül kezelje.

Aktiválja a "CIB Mobile" alkalmazást most az utasításokat követve."



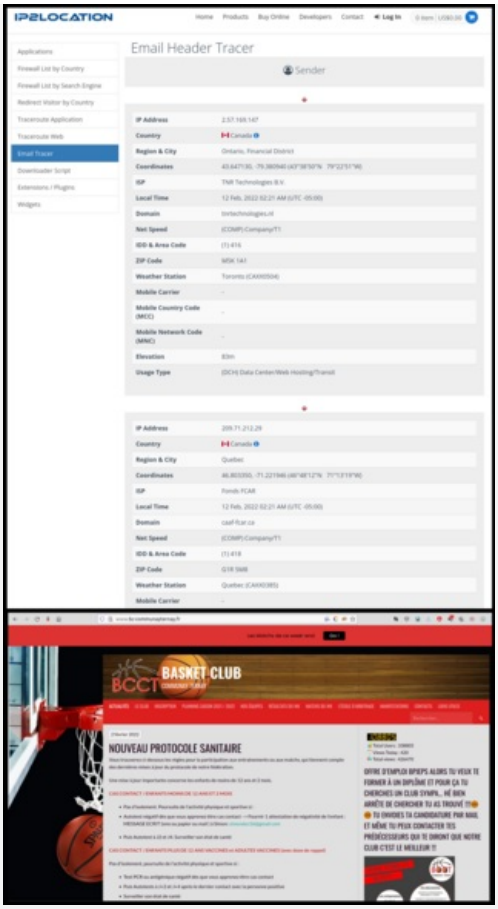
A cél mint mindig, most is **a személyes ügyféladatok, banki jelszavak begereblyézése, ellopása**. A hamis bekérő oldal a budapesti panorámával hasonló, mint a hivatalos weboldal, ám az URL cím nagyon nem hasonlít sem a CIB, de semmilyen legitim bank címéhez. Megint azt láthatjuk, hogy tömeges Wordpress-es oldalak feltörésével terjesztik a csalást, ahogy azt például a tavaly márciusi FedEx-es csomagküldős átverésben is történt.

Jól láthatóan még SSL sincs hozzá, itt még erre sem fordítottak figyelmet. A telefonszámot azért még egy külön ablakban bekérik, **aztán egy végtelen cikluson át türelmünket kérik.**



Itt vagy egy frissen felfedezett, még javítatlan zeroday sebezhetőségről van szó, amit gyorsan kihasználnak a bűnözők, vagy egy már korábban ismert, és kibocsátott javítással is rendelkező sérülékenységről, amit a lusta, feledékeny felhasználók tömegei nem foltoztok be azóta sem. Itt mind a keretrendszer, **mind a Wordpress kiegészítők frissítése igen fontos lenne az ilyen helyzetek megelőzése szempontjábó**l.

A most végigzongorázott oldal tegnap még működött, ma már lelőtték, valószínűleg jeleztek feléjük, hogy gond van. **Eredetileg ez a második Wordpress link egy BCCT nevű kosárlabda klub weboldala, amit a távoli támadók sikeresen megfertőztek, és felhasználtak az adathalász átveréshez.**



Érdemes lehet ránézni a kapott spam fejlécadataira, mit mond rá az e-mail trace: valóban Quebec, azaz Kanada a feladó szerinti térség, **nyilván a magyar CIB bank nem innen levelezne velünk.**

A végső tanulság, amit nem lehet elégszer mondani, nem változott: Soha semmilyen bank nem küld nekünk ilyen e-mailt, ezt fontos lenne mindenkinek megjegyezni.

Szólj hozzá!
Címkék: bank wordpress csalás átverés megtévesztés adathalászat cib adatlopás

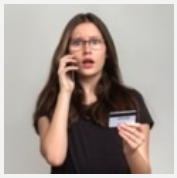
Ajánlott bejegyzések:

Ismét csomagunk érkezett - vagy mégsem?

K&H mobilbank biztonsági szolgáltatás - vagy mégsem?

A bankos mindig kétszer csenget...

Fogják a pénzünket és futnak



Továbbra is célkeresztben a banki adataink

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

Közösségi média VS munkahely

2022. február 16. 09:37 - Csizmazia Darab István [Rambo]

Gyakran posztolunk a közösségi médiában a munkánkról, a főnökünkről vagy a kollégáikról? Íme 4 hasznos tanács az ESET-től a biztonságosabb közösségi média használathoz.

Egy friss felmérés szerint a legtöbb kisvállalkozó tisztában van azzal, hogy a munkavállalóik által használt közösségi médiás alkalmazások kiberbiztonsági kockázatot jelentenek. Ezek hatással lehetnek a munkáltatókra, a kollégákra vagy akár magára az egyénre, akinek a legrosszabb esetben ezzel még a munkaviszonya is veszélybe kerülhet.

Jó hír azonban, hogy a **megfelelő hozzáállással a kockázatok csökkenthetők. Az alábbi szabályok betartásával elkerülhetjük, hogy szükségtelen veszélyeknek tegyük ki magunkat vagy munkáltatónkat.**

1. Ismerjük meg a munkahelyünk szabályzatát!

Sokan előszeretettel osztják meg a közösségi oldalakon a vállalatuk referenciáit és sikereit, akár a cég jó hírének, akár a saját imázsunk építése érdekében. Habár lehet, hogy jó szándék vezérli őket, a poszttal azonban kárt is okozhatnak - és még az is lehet, hogy ezzel megszegik a vállalat szabályzatát.

Ha a munkánkról vagy a munkáltatónkról szeretnénk posztolni, **célszerű először átnézni a vállalat közösségi médiára vonatkozó irányelveit és szabályzatát**. Abban az esetben, ha nem találunk ilyet, és nem vagyunk biztosak abban, hogy mit szabad és mit nem, **keressük fel a HR osztályt, ahol biztosan tudnak nekünk felvilágosítást adni a vállalat üzletszabályzatáról.**

2. Legyünk fokozottan óvatosak, ha magáncélra használjuk a céges eszközeinket!

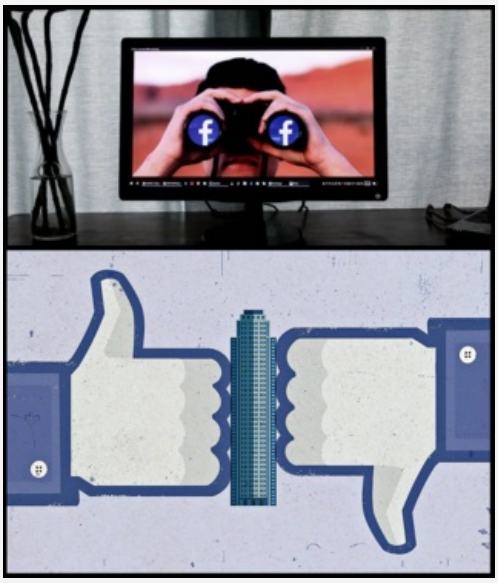
A vállalati eszközökön a munkáltatók gyakran engedélyezik a magánjellegű használatot is. **Azonban ez nem jelenti azt, hogy azt csinálhatunk a munkaeszközökkel, amit akarunk.** Nem szabad elfelejteni, hogy a vállalat rendszergazdáinak felügyelete alatt állnak és a vállalati hálózatra vannak rácsatlakozva, úgyhogy könnyedén ellenőrizhetik a tevékenységünket. A munkaeszközök biztonságáért elsősorban a vállalat és az IT csapat felelnek. Tehát a legjobb kiberbiztonsági gyakorlatokat kell bevezetniük, megbízható biztonsági megoldásokat kell alkalmazniuk, és megfelelő védelmi, megelőzési stratégiával kell rendelkezniük.

Azonban nekünk, munkavállalóknak is tennünk kell a kibertámadások elkerülése érdekében. Többek között rendszeresen frissítenünk az eszközeinket, valamint ismernünk kell a népszerű közösségi médiaplatformokon, például a Facebookon vagy az Instagramon előforduló leggyakoribb átveréseket. **Ha áldozatul esünk egy adathalász kísérletnek vagy rákattintunk egy ártalmas linkre, az egész vállalati rendszert kitesszük a zsarolóvírusok, kémprogramok vagy más típusú kártevők támadásainak.** A legjobb esetben ezért figyelmeztetést kapunk,

legrosszabb esetben pedig akár ki is rúghatnak.

3. Ne osszunk meg túl sok és részletes információt - akkor sem, ha jó szándék vezérel!
Az ESET tapasztalatai szerint gyakran felmerülő téma **a közösségi médián történő túlzott kitárulkozás, a munkánkkal kapcsolatos információk részletekbe menő megosztásával pedig akaratlanul is veszélybe sodorhatjuk** magunkat és a munkáltatónkat egyaránt.

Például, ha fényképeket osztunk meg a munkahelyünkről, az lehetővé teheti a potenciális támadók számára, hogy jól megismerjék a terepet, ha esetleg tesztelni akarnák a vállalatunk fizikai védelmét. A személyes adataink túlzott megosztásával pedig megkönnyítjük a személyazonosságunkkal való visszaélést, vagy segítjük az esetleges célzott támadások testreszabását.



Hogyan csökkenthetjük ezeket a kockázatokat? **Ne tegyünk közzé olyan fényképeket vagy bizalmas információkat, amelyek túl sokat elárulnak akár rólunk, akár a munkáltatónkról és az irodáról.** Ellenőrizzük a posztjaink láthatóságára vonatkozó beállításokat: nem kell mindent megosztanunk a széles nyilvánossággal, korlátozhatjuk csak azokra az emberekre, akiket közelről ismerünk, és akikben megbízunk.

Az adatvédelmi beállítások rendszeres ellenőrzése szintén fontos. A szakértők szerint ezeket a lépéseket célszerű az egész online jelenlétünk során rendre alkalmazni, vagyis nemcsak a munkahelyi posztjainkkal kapcsolatban.

4. Ne bánjunk gondatlanul a munkahelyi fotókkal!
Az irodai fotók - beleértve a home office-t is - kiemelt népszerűségnek örvendenek a közösségi médiában, mivel az emberek szeretik megosztani, hogyan és milyen környezetben dolgoznak. Azonban ezek a fotók túlságosan is árulkodóak lehetnek. Érdemes szemügyre venni például, hogy mi látszódik az asztalunkból a fényképen.

Egyetlen fotó bizalmas információk tárházát jelentheti: az asztalon például olyan dokumentumok is feltűnhetnek, amelyek **a munkaadó szellemi tulajdonát képezik, esetleg vállalati titkot lepleznek le; egy cetlin szerepelhet a munkáltató belépési azonosítója, a számítógép képernyőjén egy ügyfél bizalmas adatai, belépőkártya, igazolvány**. Ez adatvédelmi jogszabályokat is sérthet, ami súlyos szankciókkal jár a munkáltatóra nézve.

A legkézenfekvőbb megoldás eleve nem is posztolni a munkaasztalunkról képet. Ha viszont minden áron szeretnénk megosztani egy ilyen fotót, akkor előbb nézzük át alaposan az asztalt és mérjük fel, szem előtt van-e bármilyen biztonsági kockázatot jelentő információ. Ha találunk ilyet, távolítsuk el, fedjük le vagy takarjuk el valamilyen képszerkesztő alkalmazás segítségével.

A kiberbűnözők minden eddiginél kreatívabb stratégiákkal próbálnak átverni minket és megfertőzni az eszközeinket rosszindulatú szoftverekkel. A tét pedig egyre nagyobb, hiszen lelkesen osztjuk meg a napunk minden mozzanatát, beleértve a munkával kapcsolatos élményeinket is. Ez pedig olyan veszélyforrást jelent, amit a támadók örömmel használnak ki.

A kockázatok mérséklése nem lehetetlen feladat - a legfontosabb, hogy tartsuk szem előtt a fenti tanácsokat, és viszonyuljunk egészséges mértékű gyanakvással a közösségi médiában szembejövő dolgokhoz.

Legyünk tisztában a vállalati irányelvekkel és mindig tartsuk be az IT csapat által bevezetett kiberbiztonsági előírásokat! A mindennapjaink megosztásakor pedig ne feledjük: a kevesebb néha több - a közösségi oldalakon is.

Szólj hozzá!
Címkék: média adatvédelem policy szabályzat közösségi munkahely megosztás biztonságtudatosság

Ajánlott bejegyzések:


Fakenews fék - vajon hol a pedál?


Mindent IS visz...


10 gyakori IT biztonsági hiba


Ezer százalék lett, maradhat?


Csomagja érkezett - sokadik menet

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Antivírusblog
245 követő

Oldal követése Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

Linkeskedő linkek

2022. február 18. 11:28 - Csizmazia Darab István [Rambo]

A támadók egyre többször használják a Microsoft Teams programot arra célra, hogy rosszindulatú programokat terjesszenek. A havonta mintegy 270 millió aktív felhasználót magának tudható platform **beszélgetéseibe kerülnek bele a kártékony linkek, havonta több ezer ilyen támadást regisztráltak biztonsági kutatók.**

Az elsősorban vállalati konferencia beszélgetésekre használatos eszköz **a pandémia kitörése óta még gyakrabban használt Microsoft program, amely a 2020-as járvány miatti lezáráskor is sokkal biztonságosabb céges megoldásnak számított, mint például a rengeteg hibával, sebezhetőséggel és bizonytalan működéssel rendelkező Zoom alkalmazás.**

Emlékezetes, hogy például eredetileg end-to-end titkosítást ígértek, ami viszont mégsem volt igaz, csak szerver oldali volt, könnyen illetéktelenül bele lehetett trollkodni mások beszélgetéseibe, és az sem volt világos, zajlik-e kínai cenzúra a szervereken.


BLEEPINGCOMPUTER

Hackers slip into Microsoft Teams chats to distribute malware

By Ionut Ilascu — February 17, 2022 — 09:00 AM — 2

Security researchers warn that some attackers are compromising Microsoft Teams accounts to slip into chats and spread malicious executables to participants in the conversation.

More than 270 million users are relying on Microsoft Teams every month, many of them trusting the platform implicitly, despite the absence of protections against malicious files.

Simple but efficient method

Researchers at Avanan, a Check Point company that secures cloud email and collaboration platforms, found that hackers started to drop malicious executable files in conversations on Microsoft Teams communication platform.

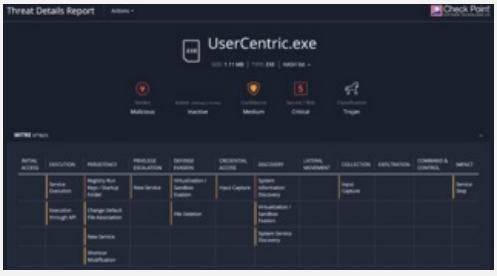
The attacks started in January, the company says in a report today, and the threat actor inserts in a chat an executable file called "User Centric" to trick the user into running it.

Once executed, the malware writes data into the system registry installs DLLs and establishes persistence on the Windows machine.

"In this Teams attack, hackers have attached a malicious Trojan document to a chat thread. When clicked on, the file will eventually take over the user's computer" - Avanan

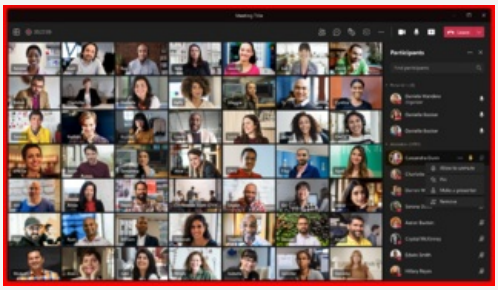
A mostani jelzések viszont azt mutatják, hogy a céges felhasználók már jórészt megtanulták gyanakodva kezelni **a kéretlen e-maileket, az adathalász próbálkozásokat, ám a Teams felhasználókban hajlamosabbak automatikusan megbízni.**

Jeremy Fuchs biztonsági szakértő tapasztalatai szerint **például a Teamst használó kórházakban az orvosok gyakorlatilag korlátozás nélkül osztják meg a betegek orvosi információit ezen a platformon. És ugyan az egészségügyi személyzet általában ismeri a biztonsági szabályokat, és e-mailben nem is osztanak meg ilyesmit, de a szabályokat hajlamosak figyelmen kívül hagyni, amikor az MSTeamsről van szó.**



A most jelzett egyszerű, de hatékony támadási módszerben **a beszélgetési csetekbe kerülnek bele kártékony futtatható (például .EXE kiterjesztésű) trójai állományok. Kritikus esetben ezek olyan sérülékenységet is kihasználhatnak, ami által a távoli támadók képesek lehetnek átvenni a teljes jogú irányítást a megfertőződött számítógép felett**. 2022 januárjában figyeltek fel a szakemberek a tömegessé váló próbálkozásokra.

A Teams fiókokhoz való illetéktelen hozzáférés pedig történhet például Microsoft 365 hitelesítő adatainak adathalászattal való ellopásával is.



A védekezéshez, megelőzéshez **érdemes óvatosnak lenni a más vállalatoktól érkező meghívókkal, és nem gondolkodás nélkül, automatikusan elfogadni ezeket.** Itt is bárki könnyen ki tudja adni magát másnak, akár cégen belüli, akár cégen kívüli kontaktokról van szó.

És persze a szokásos jótanácsok is élnek: **használjunk naprakész vírusvédelmi megoldást, haladéktalanul futtassuk a már megjelent hibajavító frissítéseket, és kapkodás helyett kezeljük biztonságtudatosan a Teams kommunikációs platform körül zajló eseményeinket.**

Szólj hozzá!
Címkék: microsoft konferencia csevegés kártevő platform msteams fájlmelléklet

Ajánlott bejegyzések:


Hogyan ne jussunk 10-ről 11-re?


Támadás 1,2,3 - Industroyer újratöltve

Sikeres brandek az adathalászatban


Ezer százalék lett, maradhat?


10 alaplépés a biztonsághoz

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Xenomorph kalandjai GooglePlay országban

2022. február 22. 12:51 - Csizmazia Darab István [Rambo]

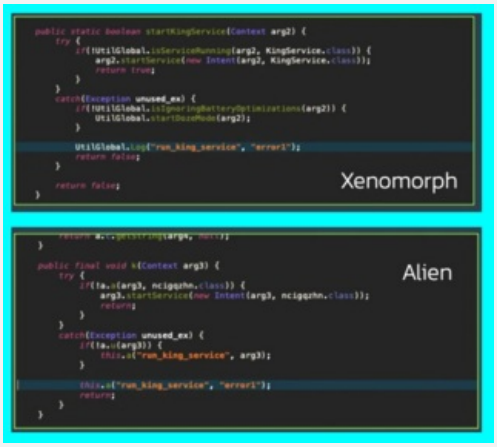
Nem egy jó felütés, ha valakiről az az első lényegi megosztható információ, hogy ő az Alien rokona, legalábbis forráskód alapján. Jelen esetben a besorolás **egy banki trójai adatlopó kártevő** családfára utal, ami talán csak egy fokkal jobb, mintha a Nostromo űrhajó fedélzetén lenne igazi szörnyeteg. De persze **a hivatalos androidos piactérre való észrevétlen beszivárgás is lehet adott esetben ijesztő kockázat.**

Fast Cleaner néven jelent meg az az alkalmazás a Google hivatalos áruházában, amely azt állította magáról, hogy az androidos eszközök teljesítményét növelik - itt akár deja vu érzésünk is lehet, hasonlókat már átéltük Windows esetében is. Ezek vagy hamis antivírusok voltak, vagy valamilyen memória vagy teljesítmény többszörözést ígérő kamu programok.

Mindenesetre az akkori tanulság a mai korra áttranszformálva biztosan hasznos még ma is: "*Soha ne használjunk és ne telepítsünk olyan programot, amelyre rákeresve a Google szinte összes találata 'How to remove...' szófordulattal kezdődik.*"

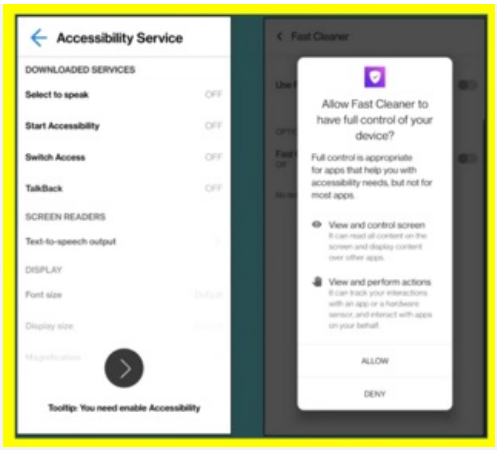
Szóval ez a Fast Cleaner android app **elsőre teljesen tiszta, és kiállta az elsődleges ellenőrzést a piactérre való feltöltéskor, ugyanis a kártékony funkciókat csak a későbbi frissítéskor tölti le az eszközökre.**

A rosszindulatú program onnantól képes figyelni az értesítéseket, az SMS üzeneteket, így például már megszerezheti a bankszámlák védelmére használt kétfaktoros hitelesítő adatokat és az egyszer használatos (OTP) jelszavakat is.



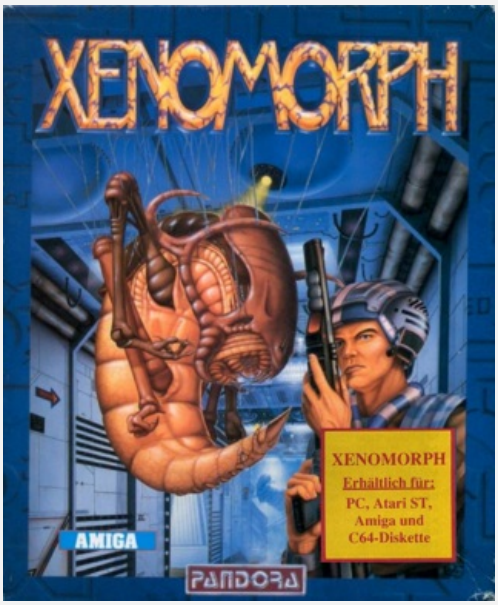
Az engedélyek között megtaláljuk a 2021. márciusában elhíresült FedEx-es csalásnál is használt akadálymentesítési szolgáltatás engedélyeinek kérését is (Accessebility Service), amely **abban segít a kártevőnek, hogy észrevétlenné tegye a rosszindulatú működést, teljes jogosultságot ad a támadóknak az eszköz felett**, és a későbbi mentesítést, uninstallt is megnehezíti.

A kártékony alkalmazást a beazonosítás előtt már **több, mint 50 ezren töltötték le.**



A Bleeping Computer cikke szerint a ThreatFabric szakértői f**olyamatos fejlesztés nyomait látják a Xenomorph kártevő kódjában, ami a mostani 56 európai bankra jelentett alacsonyabb kaliberű veszély körét tovább tágíthatja**, és ebbe beleérthetjük a későbbiekben akár hazai bankok elleni modulok megjelenését is.

Egy sajnos biztos, hogy nem utoljára bukkant fel ez **a kártevő, továbbfejlesztett új verziói más, szép ígéreteket hordozó újabb trójai alkalmazásokban még** sok borsot fognak törni a gyanútlan és felkészületlen felhasználók orra alá.

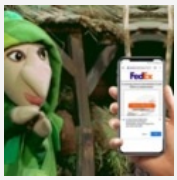


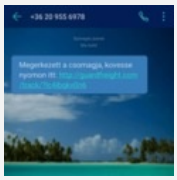
Védekezés, megelőzés terén nem tudunk újat mondani, csak a szokásos régi okosságokat újra felsorolni. A Maginot-vonalat, azaz a legerősebb védelmi falat ma is **egy korszerű és hatékony vírusvédelmi alkalmazás adhatja meg. Ezenfelül lehet, sőt kell a naprakész rendszeres rendszer és alkalmazás frissítéseket alkalmazni.** A sok kétes és noname alkalmazás áruház, és letöltési piactér mellett a hivatalos Google Play változatlanul tanácsos, noha önmagában ez nem elég az üdvösséghez.

És emellé kell még a **biztonságtudatos alkalmazástelepítés is, ami részben a tudatos program kiválasztást jelenti, beleértve az értékelések, visszajelzések figyelését, valamint a kért és megadott engedélyek alapos átgondolását, felülvizsgálatát is.**

4 komment
Címkék: google play alien trójai android áruház kártevő kártékony banki adatlopás piactér xenomorph

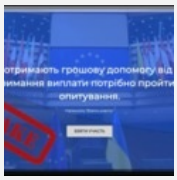
Ajánlott bejegyzések:


Sárkány ellen sárkányfű


Megérkezett a csomagja - vagy mégsem?


VPN appok Androidra vagy mégsem?


Igazgató-e vagy?


Adathalászok lakat alatt

Kommentek:

kéki béla 2022.02.23. 12:21:54

"A Maginot-vonalat, azaz a legerősebb védelmi falat ma is egy korszerű és hatékony vírusvédelmi alkalmazás adhatja meg"

Ha kicsit félretesszük, hogy "hazabeszélsz", androidon, ha csak google playről telepítesz alkalmazást, mi értelme a víruskeresőnek?
A play ellenőrzi a felkerülő kódokat, ha van benne kereső által felfedezhető malware, azt megtalálja. Ha nem, akkor jó eséllyel a mobilra telepített kereső sem veszi észre.
Akkor meg minek?

Válasz erre

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2022.02.23. 13:50:51

Szia.

A vírusirtónak van a legnagyobb értelme, legyen szó adathalászatról, távoli rosszindulatú USSD kódokról, trójaikról, például a Fedexes incindesnél azonnal blokkolta a kártevőt a védelem.

Itt éppen arról van szó, hogy a piactéri feltöltés előtti engedélyhez szükséges ellenőrzés azért nem vette észre, mert akkor még nem is volt benne a későbbi kártékony frissítés. De később bármikor is "mérgezik" meg az appot, nálad az AV azonnal ráugrik és detektálja, blokkolja, megvéd téged. Ez az értelme.

Válasz erre

kéki béla 2022.02.23. 14:15:53

@Csizmazia Darab István [Rambo]: bocs, lehet, hogy félreertettem, de ez az eset nem úgy lett felderítve, hogy az ezzel foglalkozó szakemberek fedezték fel a letöltött kártevőket és nem a lokális víruskeresők?

Válasz erre

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2022.02.23. 14:42:51

Gondolom a bankoknál is lehetett gyanús tevékenység, amit jelentettek, és közben egyes felhasználóknál kár keletkezett vagy beriasztottak náluk a különböző víruskeresők és tudni akarták, hogy ez most vakriasztás vagy komoly. És mikor kielemezték, úgy tűnik komoly lett:

www.threatfabric.com/blogs/xenomorph-a-newly-hatched-banking-trojan.html

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.

VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Ransomware a spájzban

2022. február 24. 13:44 - Csizmazia Darab István [Rambo]

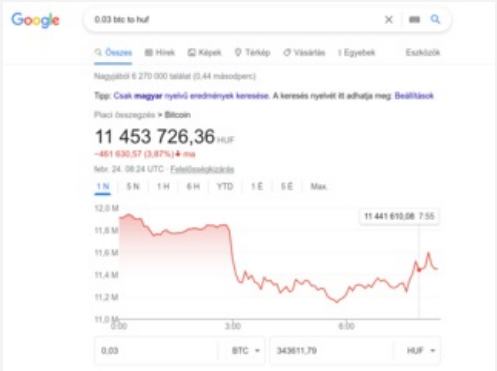
A napokban az Asustor NAS tulajdonosok futottak bele a Deadbolt nevű zsarolóvírusba. Az elérhetetlenné kódolt .deadbolt kiterjesztésű fájljaik mellett egy üzenet fogadta őket: **0.03 Bitcoint váltságdíjat kell fizetniük**, különben az állományaiknak reszeltek. Emellett ránézünk még a 2021-es év ransomware statisztikáira is.

Az aktívan támadott eszközökön követelt **nagyjából 340 ezer forintnak megfelelő (945 euro) váltságdíj fejbekólintotta a póruljárt tulajdonosokat, akik nyilván mentésre is használták a neten lógó NAS tárolójukat** - igaz a zsarolóvírus ellen elengedhetetlenül fontos az offline tárolt rendszeres mentés.

A gyártó gyorsan lelőtte a myasustor.com DDNS szolgáltatást, és azt javasolja a felhasználóknak, hogy módosítsák az alapértelmezett portokat, **tiltsák le az EZ Connect szolgáltatást, illetve kapcsolják le a terminál/SSH valamint az SFTP szolgáltatásokat.**

Áttérve a tavalyi számokra, a Veeam jelentése egészen extrém mértékű támadásokról árulkodik. Elképesztő módon a 2021-es esztendőben **a megkérdezett szervezetek háromnegyede szenvedett el zsarolóvírus incidenst.**

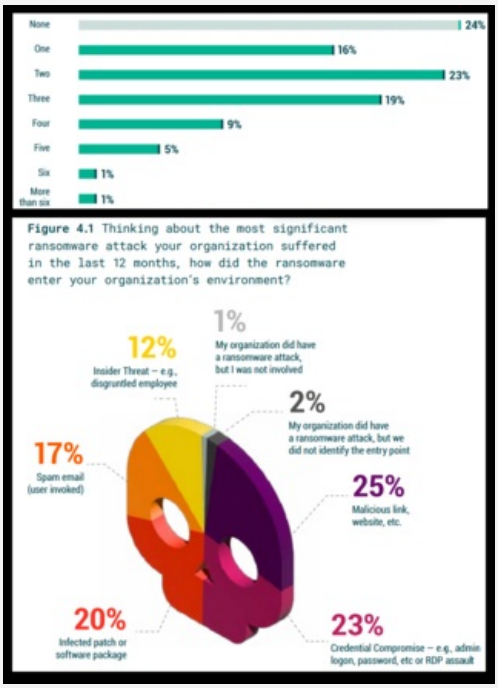
A támadási vektorok eloszlása is beszédes: nagyjából egynegyed-egynegyed arányban osztozik a nyitott RDP port, feltört jelszó és hasonlók valamint a kártékony linkekre való kattintás is ezzel pariban van.



Van még 20% trójai vagy egyéb kártékony szoftver frissítés, illetve telepítés, és 17%-ban a kéretlen spam levelek is meghozzák az óvatlan felhasználók kattintása miatt a fertőzést. Tíz százalék feletti az úgynevezett belső munka, ahol egy munkavállaló valamilyen részt vállal a támadásban. Ami nem is feltétlen jelent folyamatos aktív részvételt, hanem lehet ez olyan sértett munkavállaló, aki bosszúból vagy a bűnözőktől kapott pénzért ad el bizalmas adatokat, hozzáféréseket, jelszavakat a céges hálózathoz, ehhez a ransomware bandák rendszeresen szoktak belsős munkatársakat toborozni.

Ilyenkor jelentős pénzjutalmat ígérnek azoknak, akik cégük RDP, VPN, levelező szerver, és egyéb belső

vállalati rendszereikhez hozzáférést, jelszavakat adnak a bűnözőknek. A toborzók a pénz mellé teljes anonimitás ígérnek a besúgónak.



További érdekes adat, hogy **a kárt szenvedett szervezetek átlagosan csak az adataik nagyjából 64%-át tudták helyreállítani, ami egyúttal azt jelenti, hogy az adatok több mint harmada általában helyrehozhatatlanul elveszik.** A megkérdezett 1376 szervezet válaszadói közül 36 százalék volt csak ennél valamivel sikeresebb, ott a helyreállítás után sikeresen visszanyerték adataik több, mint 80 százalékát, ami azért még mindig tartalmaz egy jelentős gap-et.

Ha pedig belevesszük mindebbe, hogy a doxing miatt a fenyegetés jóval nagyobb kockázat, mint az adatok puszta elvesztése, úgy már még inkább látszik, hogy igen jelentős a veszély, KKV-tól kritikus infrastruktúrákat üzemeltető nagy cégekig mindenhol.

Szólj hozzá!
Címkék: statisztika fertőzés nas váltságdíj adatlopás ransomware zsarolóvírus asustor

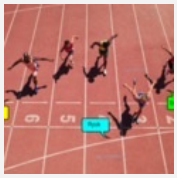
Ajánlott bejegyzések:


Emelkedő ransomware károk


Durva ransomware statisztikai adatok


Fordulat ransomware fronton


Ransomware helyzetjelentés


Világrekord, aminek mégsem örül senki

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Antivírusblog
245 követő

Oldal követése Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

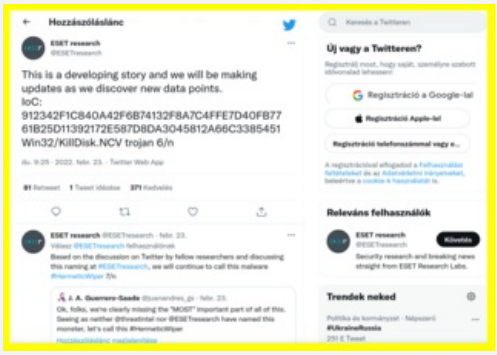
A kibertér is hadszíntér

2022. február 28. 07:25 - Csizmazia Darab István [Rambo]

Több száz számítógép került veszélybe Ukrajnában néhány órával azután, hogy **egy célzott túlterheléses támadássorozatot követően számos ukrán weboldal elérhetetlenné vált** az elmúlt héten.

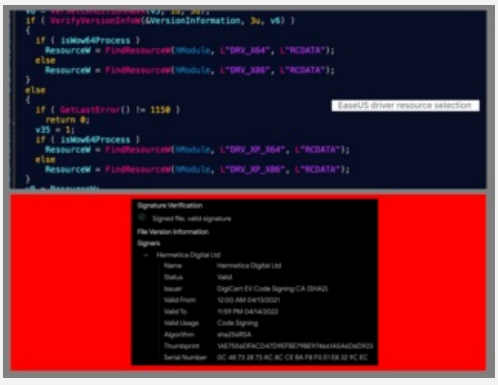
Ukrajnában számos szervezetet ért kibertámadás, melynek hátterében **egy HermeticWiper nevű adattörlő kártevő (wiper) áll**, állapították meg az ESET kiberbiztonsági kutatói. A támadás az ESET telemetriája szerint **néhány órával azután történt, hogy egy túlterheléses támadássorozat (DDoS) több fontos webhelyet elérhetetlenné tett az országban.**

Biztonsági kutatók Win32/KillDisk.NCV néven február 23-án helyi idő szerint 17 óra előtt észlelték első alkalommal a Wipert. A kártevő adatainak vizsgálatából az derült ki, hogy azt két hónappal ezelőtt hozhatták létre, de az eddigi információk alapján a múlt hét szerdán vetették be először.

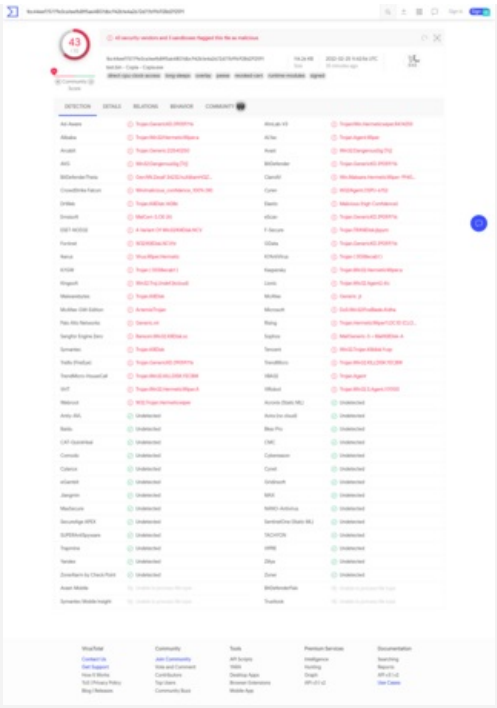


A Hermetic Wiper képes letörölni a megfertőzött rendszer minden adatát, a célba vett hálózat számítógépeinek teljes tartalmát és azokat semmilyen módon nem lehet később visszaállítani. Más rosszindulatú kártevőkkel szemben a HermeticWiper valódi célja nem az adatlopás és így az anyagi haszonszerzés, hanem a puszta rombolás: véglegesen megsemmisíteni az adatokat, illetve a szabotázsakció révén leállítani a működő infrastruktúrákat.

Az adattörlő **visszaél az EaseUS Partition Master szoftver illesztőprogramjaival,** megsemmisítve annak adatait. A kártevő elnevezése abból ered, hogy **a támadók egy olyan digitálisan aláírt legitim szoftvert használtak, melynek hivatalos tanúsítványát a ciprusi székhelyű Hermetica Digital nevű cégnek állították ki.** Úgy tűnik, hogy legalább egy alkalommal a kiberbűnözők hozzáférhettek a cég hálózatához, mielőtt szabadon engedték a rosszindulatú programot.



Szerdán számos ukrán weboldalt lekapcsoltak a DDoS támadások újabb hullámában, amelyek már hetek óta célozzák az országot, köztük kulcsfontosságú kormányzati oldalakat,az ukrán parlamenti, a külügyminisztériumi illetve emellett különböző banki weboldalakat támadtak.



Korábban **már egy másik adattörlő kártevő is végigsöpört Ukrajnán idén január közepén**. Az akkori támadásban szereplő kártevő **a WhisperGate nevű adattörlő zsarolóvírusnak álcázta magát, és erősen emlékeztetett a NotPetya támadásra,** amely 2017 júniusában sújtott le Ukrajnára, mielőtt hatalmas pusztítást okozott volna az egész világon.

A kutatók szerint azonban **a most azonosított új Wiper kártevő ennél sokkal nagyobb veszélyt jelent, mert több módszer egyidejű alkalmazásával teszi tönkre a megtámadott gépeket, és állítja le ezzel a megcélzott szolgáltatásokat.**

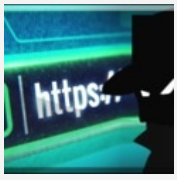
Szólj hozzá!
Címkék: ukrajna eset kártevő kibertámadás wiper hermetic

Ajánlott bejegyzések:

Támadás 1,2,3 - Industroyer újratöltve

Kis- és középvállalkozások adatvédelmi incidensei

Oroszország ott a fő kibercélpont



Böngészés - kockázatok és mellékhatások

Durva ransomware statisztikai adatok

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Antivírusblog
245 követő

Oldal követése Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

- RSS 2.0
  bejegyzések, kommentek
- Atom
  bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

Tinder + Svindler = Tinder Svindler

2022. március 02. 17:14 - Csizmazia Darab István [Rambo]

A közelmúlt egyik érdekes filmje a Netflixen a fenti film, de sok más igazi csalóról is készülnek mozik, sorozatok - például Az örökösnő álarca mögött című sorozat, amely Anna Delvey álörökösnő New York-i üzelmeit mutatja be testközelből. Visszatérve **a tinderes témára, eléggé felkapott lett a sztori, ám több rétege is van mindennek, na meg tanulsága is lehetne bőven.**

Először jöjjön akkor az alaptörténet, amelyben **egy Shimon Hayut, vagy másik álnevén Simon Leviev egy milliárdos izraeli gyémántkereskedő fiának adja ki magát, és a Tinderen üzemszerűen keresett párt.**

Itt nem feleséget, élettársat vagy barátnőt kell érteni, hanem **tudatosan, ravasz módon behálózott 30-40 körüli jól szituált nőket, akikkel többnyire csak néhány alkalommal találkozott**, ám akikkel ennek ellenére sikeresen elhitette, hogy köztük a kötődés ennek ellenére mély.

A férfi igazi szociopata, sikeresen manipulálja az áldozatait, akiket lenyűgöz a látszat: drága szállodai szobák, magánrepülőgép, sportkocsik, jólét, látványos költekezés. A sztorit - amely valós eseményeket mutat be - több helyen is elemezték, például **a Tangó és Kes - Túl nagyra fújta a lufit a Tinder-svindler című podcastban, de igen érdekes, és több szempontú megközelítések születtek a témáról az Önkényes mérvadó #232 adásában is.**

Az a megközelítés, hogy ha nem is profi aranyások a pórul járt áldozatok, de azért mindenképpen jól akartak járni kétségkívül igaz, és **a látszat alaposan megtévesztette őket. Ami 90%-ban egy már előre elkészített, luxuséletet villantó Tinder és Insta oldal volt, ami mögé mindenki odaképzelte az álmait, a vágyait.**

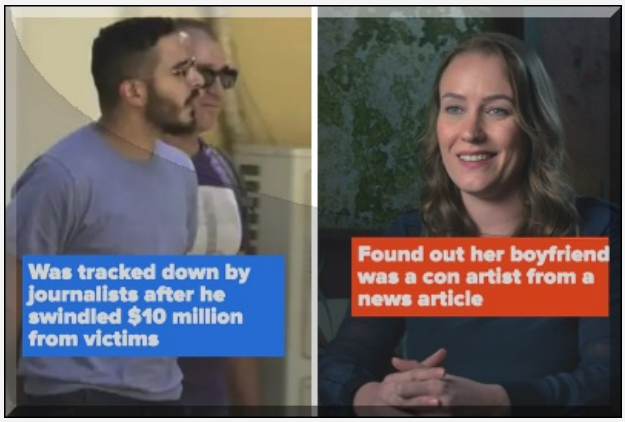
Ha valaki erre felkapja a fejét, és a romantikus csalás kategóriájú átverések jutnak az eszébe, az korántsem véletlen,

ezekről már többször is szó volt itt a blogposztok között is. **A csalónk igen profi módon válogatta ki az áldozatait, és gyaníthatóan időben is egyszerre szédítette őket: a már megismert áldozatoktól kért kölcsönökből finanszírozta a rá következő hölgy meghódítását, szállodát, utazást, ajándékokat, vacsorákat.**

A már éppen anyagilag kihasznált nőktől időt kért állítólagos sürgős üzleti ügyei, utazásai ürügyén, illetve egy szintén előre elkészített felvételsorozattal - amelyben ő és a testőre megsérült, és egy mentőben ülnek - rejtélyes fenyegetés miatti menekülésre hivatkozva kért kölcsön pénzt, vagy rendelt repülőjegyeket a naiv áldozatoktól.

Az is **profi módszer volt, hogy az állítólagos életveszélyre hivatkozva azt kérte az áldozatoktól, hogy saját biztonságuk érdekében azonnal töröljék közösségi oldalaikat, hiszen ezzel a számára kompromittáló közös képek is eltűntek, és zavaró tényezők nélkül jobb eséllyel tudott rástartolni a soron következő randijaira**. Felicity Morris filmjét mindenkinek érdemes megnéznie, aki jobban bele szeretne látni az ilyen társkeresős csalások rejtelmeibe. Érdekes része volt a filmnek, hogy bár az elkövetőt már 2011. óta körözték Izraelben, végül a 2019-es elfogásakor és kiadatásakor mégis mindössze 15 hónapos börtönre ítélték közokirat hamisításért, amiből csak 5 hónapot ült le, és azóta is aktív a Tinderen, csapatával ott folytatta, ahol abbahagyta.

Kicsit a Wall Street farkasai filmhez hasonlóan, utána ő is egy tanácsadó céget alapított - reméljük nem a fenti módszereket tanítja ott a jelentkezőknek. Egy pert most idén mindenesetre kapott a nyakába az igazi Leviev családtól, miután a filmből kiderült, hogy visszaélt a nevükkel.



Végül a jótanácsok hasznos rész, ami fájóan kimaradt a Netflixes filmből, pedig szintén fontos. Ehhez felidézzük egy korábbi posztunkat, amelyben már sok mindent összefoglaltunk ezzel kapcsolatban. **Idegeneknek sose adjuk ki részletes személyes adatainkat, igazolvány számainkat, igazolványaink fotóját. Soha ne utaljunk előre ismeretlen személyeknek, akik a valódi, offline találkozást ettől a pénztől teszik függővé. De ugyanez áll azokra is, akiket csak rövid ideje ismerünk, vagy csak úgy gondoljuk, hogy ismerünk.**

A filmben többen is 2-3 személyes találkozó után banki hiteleket vettek fel azért, hogy odaadják a csalónak. Banki adatainkat - megtakarításaink mértékét, bankszámlaszámunkat, stb. - szintén kezeljük bizalmasan, mert ez is pénzügyi visszaélésekre adhat lehetőséget.

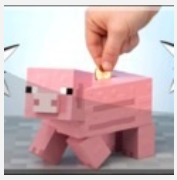
Az ismétlődő, egyre agresszívabb pénzkövetelés mindenkor keltsen kételyt, és jól tesszük, ha esetleg már belesodródtunk volna egy ilyen történetbe, akkor feljelentést teszünk a hatóságoknál. Hasznos ötlet az inverz képkeresés is, például a TinEye időnként életmentően hasznos észrevételeket tud tenni, a hirdető félről itt sok minden, akár egy csomó más személyazonosság is kiderülhet.

És persze az is hasznos, ha a biztonságtudatosságunk mellett a hozzáállásunkat is felülvizsgáljuk, és hasznos elgondolkodnunk azon, ha például hét év alatt még nem találtuk meg az áhított nagy őt, akkor esetleg a saját elvárásainkkal is lehet valami túltolás, és talán mégsem egy milliárdos herceg fog majd eljönni értünk fehér lovon.

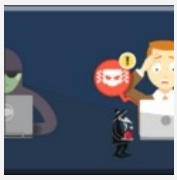
Szólj hozzá!
Címkék: társkeresés csalás átverés romantikus 419 dating tinder svindler

Ajánlott bejegyzések:

Modern románc, holdfény és tánc


A csalások már a spájzban vannak

Celeb vagyok, fizess nekem!


Üzleti e-mail hamisítás


VPN appok Androidra vagy mégsem?

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

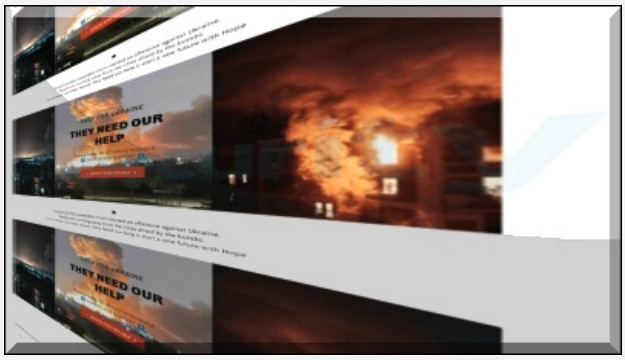
Jótékonysági csalások Ukrajna nevében

2022. március 07. 09:02 - Csizmazia Darab István [Rambo]

Már a pandémia ideje alatt is megtapasztalhattuk, hogy a válságot kihasználva jelentős mértékben megugrott az online térben elkövetett bűncselekmények száma. **Most az orosz-ukrán háború alakulását követve láthatjuk, hogy az etikus hackerek segítő szándéka mellett egyre több pénzsóvár csaló próbálja hamis adományozási felhívással kihasználni a válságos időszakot.**

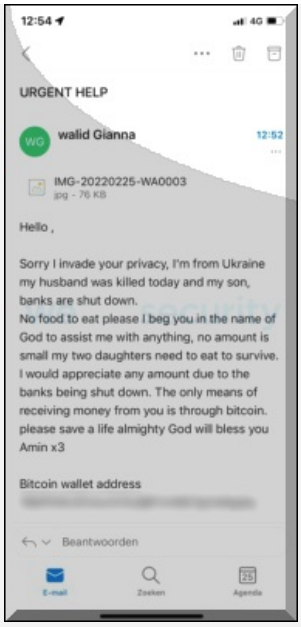
Az elmúlt napok történései sokakból együttérzést és segítő szándékot váltottak ki, **sajnos azonban jó pár olyan kétes szervezet is felbukkant, amely az emberek jóhiszeműségét kihasználva aljas módon próbál pénzhez jutni.** Az ESET kutatói rengeteg olyan weboldalt fedeztek fel, melyek jótékonysági célokra hivatkozva próbálnak pénzt kicsalni a jóhiszemű netezőktől.

Ezek a weboldalak az aktuális események tükrében erőteljesen **az érzelmekre ható, ugyanakkor hamis felhívásokat intéznek a látogatók felé, az ukrán néppel való együttérzés jegyében.**



Az adott honlapok jellemzően nem teljesen egyértelműen, kissé ködösen fogalmaznak a „segély” felhasználási módjára vonatkozóan. **Alaposabban megvizsgálva ezeket, az is világossá válik, hogy egyikük sem képvisel legitim hivatalos szervezetet**. A szakértők összegyűjtöttek pár ilyen példát:

- *help-for-ukraine[.]eu*
- *tokenukraine[.]com*
- *supportukraine[.]today*
- *ukrainecharity[.]gives*
- *ukrainesolidarity[.]org*
- *ukraine-solidarity[.]com*
- *saveukraine[.]today*

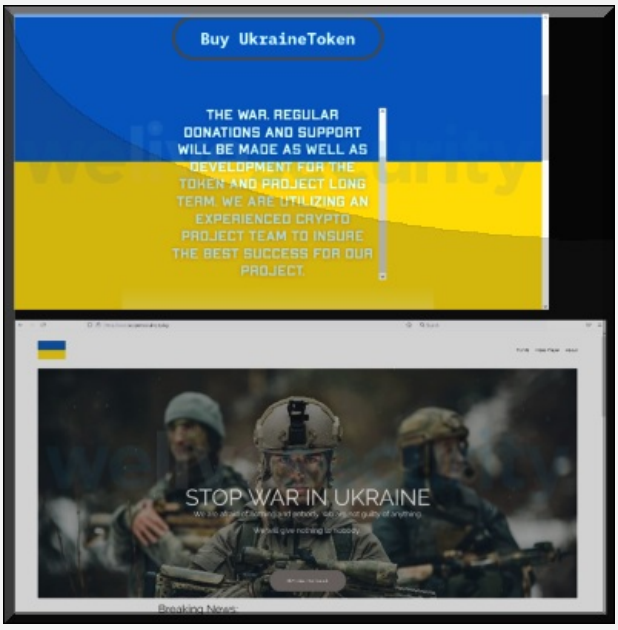


A kibertámadók közvetlen formában e-mailen keresztül is megkereshetnek bennünket, jellemzően kéretlen e-mailen keresztül.

Egy Reddit-felhasználó osztotta meg az alábbi, hamis adománykérő levelet:

„Szia,

Elnézést a zavarásért! Ukrán vagyok, megölték ma a férjem és a fiam, a bankok pedig bezártak.
Nincs mit ennünk, könyörgöm Neked Isten nevében, hogy segíts rajtam bármilyen összeggel. Most semmi sem kevés, mert a két lányomnak muszáj ennie a túlélésért. Bármilyen összegért hálás vagyok, hiszen a bankok bezártak. Az egyetlen módja a segítségnek, ha Bitcoint küldesz nekem. Kérlek, ments meg egy életet, a mindenható Isten meg fog áldani ezért.
Amin”



Több más, ehhez hasonló trükk kering még a különböző közösségi média felületeken, melyek célja, hogy Bitcoint szerezzenek a jóhiszemű felhasználóktól. Egy olyan korban, amikor mindennaposak az online fiókok feltörései, és folyamatos kibertámadások érnek ukrán célpontokat, nehéz a „kizárólag digitálisan” elérhető információkat ellenőrizni.

Míg a válságok idején a közösségi oldalak nagy szerepet játszanak abban, hogy tájékoztassanak a segítségnyújtás lehetőségeiről, ugyanakkor a csalásoknak is rendívül jó táptalajt jelentenek.

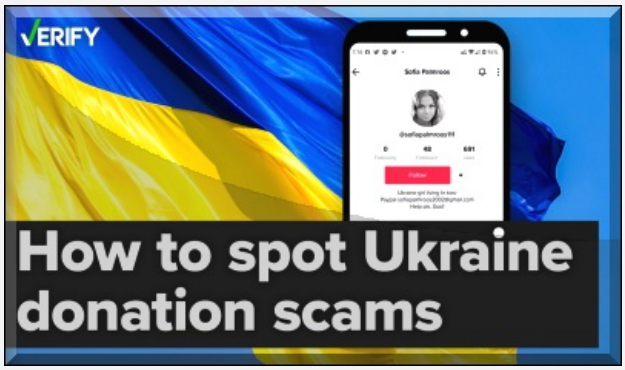
Hogyan kerülhetjük el a jótékonysági csalásokat?
Ha adományozni szeretnénk, érdemes megfogadni az alábbi jó tanácsokat a saját biztonságunk megőrzése érdekében.

- Gondosan ellenőrizzük adakozás előtt, hogy pontosan milyen alapítványt, vagy szervezetet támogatunk. A legjobb, ha ragaszkodunk azokhoz a jól ismert, nagy múltú megbízható szervezetekhez, amelyek valamilyen formában vagy akár partnereiken keresztül jelen vannak Ukrajnában.

- Adományozzunk közvetlenül a webhelyükön keresztül, vagy forduljunk egyenesen az adott jótékonysági szervhez útmutatásért.

- Legyünk óvatosak a pénz átutalására vagy ajándékutalványok küldésére vonatkozó kérelmekkel kapcsolatban.

- Legyünk óvatosak az ismeretlen feladóktól származó kéretlen e-mailekkel és közösségi média üzenetekkel. Ezeknél kerüljük a mellékletek letöltését, vagy a linkekre való kattintást, mert akaratlanul is rosszindulatú programot tölthetünk le az eszközünkre.



- Még a látszólag megbízható forrásokból érkező üzenetekkel is érdemes vigyázni, és alaposan ellenőrizni azok hitelességét. Vegyük fel a kapcsolatot közvetlenül a feladóval más csatornákon is, például telefonon vagy e-mailen keresztül.

- Legyünk szkeptikusak a jótékonysági szervezeteket népszerűsítő közösségi média tartalmakkal, amíg nem ellenőriztük, hogy valóban legitim szervezetről van szó. Nem tudhatjuk, hogy az ismerősünk, aki megosztotta, elvégezte-e előtte ezt a kutatómunkát, és a poszt alatti lájkok száma sem hitelesíti annak valóságtartalmát.

- Ne engedjünk az indokolatlan pszichológiai nyomásnak, bűntudatkeltésnek, hiszen a csalók éppen ez a sürgetést használják fel arra, hogy minél előbb átgondolatlan adakozásra késztessenek minket.

Mivel az ukrán humanitárius válság továbbra is a címlapokon szerepel a világ minden táján, a csalók folyamatosan keresik az újabb módszereket, hogy saját hasznukra fordítsák a háború által érintett, kiszolgáltatott emberek helyzetét.

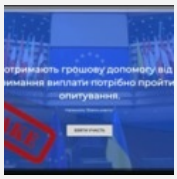
A hamis jótékonysági átverések esetén ráadásul áldozatként nem csak minket ér kár, de a rászorulók helyett a csalók zsebében landol a jóhiszemű adományunk.

2 komment
Címkék: orosz ukrajna háború jótékonyság csalás ukrán adománygyűjtés welivesecurity.com

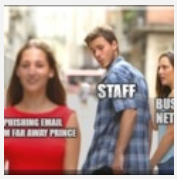
Ajánlott bejegyzések:


Támadás 1,2,3 - Industroyer újratöltve


VPN appok Androidra vagy mégsem?


Adathalászok lakat alatt


Oroszország lett a fő kibercélpont



10 gyakori ok, amiért bedőlünk a csalásoknak

Kommentek:

Head Honcho 2022.03.07. 09:07:26

Igazán patkány húzás a szerencsétlen sorsúakkal visszaélni.

Válasz erre

kuszkusz1 2022.03.07. 12:04:37

Erre sajnos számítani lehetett. Ezért perkáltam én a Vöröskeresztnek. De ha már vírus, meg hacker, kaptam ma egy e-mailt amelyben 1200 dollárt kérnek azért hogy ne tegyék ki a netre a kínos videóimat amelyen felnőtt tartalmak böngészése mellett helytelen cselekedetek láthatóak rólam. Nem a smucigság beszél belőlem - mi az az 1200 dollár egy nyugdíjasnak, nem igaz - de nincs a számítógépemen webkamera. Ez egy régi gép. :) Ami a felnőtt tartalmakat illeti, nem cáfolom, a Hírkereső híreit tényleg nem ajánlom serdülő ifjaknak. :)

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez

5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.

VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Felkészül: USA kritikus infrastruktúra

2022. március 09. 13:36 - Csizmazia Darab István [Rambo]

De persze nemcsak ott, hanem világszerte indokolt a fokozott kibervédelem. Bár éppen nagyban folyik a hibrid háború Oroszország és Ukrajna között **mind a fizikai, mind pedig a kibertérben, emellett a célzott ransomware támadások harmadik felek ellen is erőteljesen megszaporodtak.**

Az amerikai Szövetségi Nyomozó Iroda (FBI) riasztást adott ki annak kapcsán, hogy 2022. januárja óta legalább 52 USA-beli szervezetet céloztak meg támadók, amelyek kritikus infrastrukturális - beleértve ebbe a kritikus gyártási, energetikai, pénzügyi szolgáltatási, kormányzati és informatikai szektorban működő szervezeteket is - ágazatban működnek.

A támadások a gyaníthatóan **orosz eredetű RagnarLocker ransomware csoporthoz köthetők**. Az FBI felszólította az áldozatokat, hogy azonnal jelentsék a ransomware támadásokat a helyi területi irodájuknak.


TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

7 MARCH 2022

FLASH Number

CU-000163-MW

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This alert is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actors of cyber crime. This FLASH was coordinated with DHS/CISA.

This FLASH has been released TLP:WHITE

WE NEED YOUR HELP! If you identify any suspicious activity within your enterprise or have related information, please contact your local FBI Cyber Squad immediately with respect to the procedures outlined in the Reporting Notice section of this message.

*Note: By reporting any related information to FBI Cyber Squads, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.

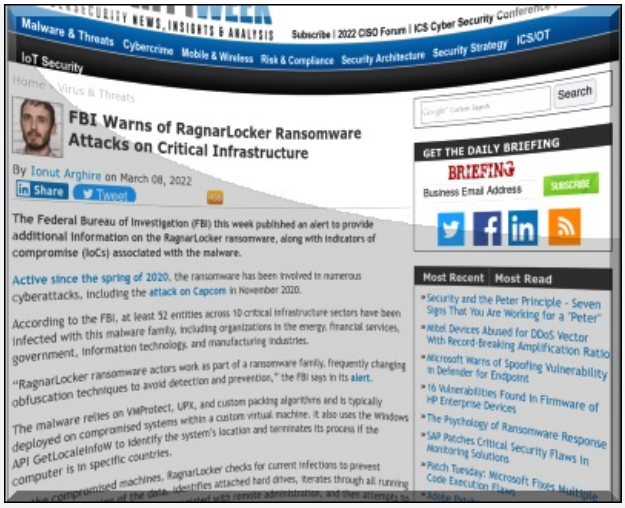
RagnarLocker Ransomware Indicators of Compromise

Summary

The FBI first became aware of RagnarLocker in April 2020 and subsequently produced a FLASH to disseminate known indicators of compromise (IOCs) at that time. This FLASH provides updated and additional IOCs to supplement that report. As of January 2022, the FBI has identified at least 52 entities across 10 critical infrastructure sectors affected by RagnarLocker ransomware, including entities in the critical manufacturing, energy, financial services, government, and information technology sectors. RagnarLocker ransomware actors work as part of a ransomware family[1], frequently changing obfuscation techniques to avoid detection and prevention.

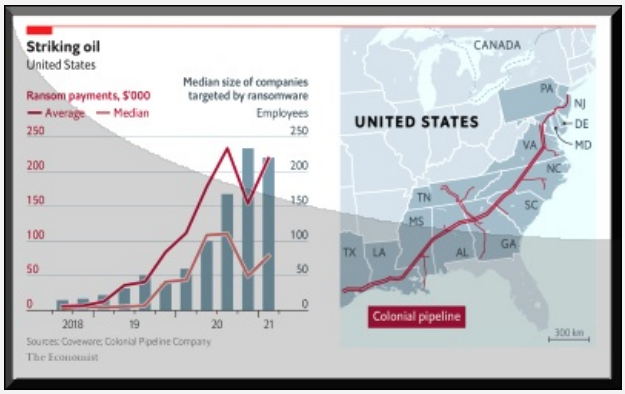
Mint ismeretes, ez a zsarolóvírus (is) ellenőrzi a támadás kezdetén az áldozat lokációját (például Windows API GetLocaleInfoW), és ha a fertőzendő gép helye azerbajdzsáni, örmény, fehérorosz, kazahsztáni, kirgizisztáni, moldvai, tádzsikisztáni, orosz, türkmenisztáni, üzbegisztáni, ukrajnai vagy grúziaiként azonosító, akkor a ransomware fertőzés folyamata automatikusan megszűnik, el sem indul.

Ezt korábban már más ransomwarek esetén is láthattuk, emlékezzünk csak **például mondjuk a Cerberre**. Ha a korábbi Putyin-Biden egyezségre gondolunk, amely az erőteljesebb orosz fellépést szorgalmazta az ottani ransomware bandákkal szemben, **akkor a mai helyzetben ezt sajnos el is lehet felejteni, sőt most lesz csak felfutóban igazán.**



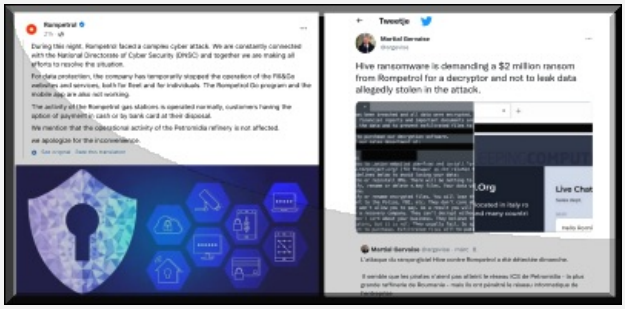
A ransomware támadások technikailag a 2013-as CryptoLocker megjelenése óta rengeteget fejlődtek. Hihetetlen gyorsan képesek végigfutni az elkódolással a fájlokon, például úgy is, hogy csak az első x bájtot kódolják el, azzal is gallyra lehet már vágni a titkosított állományok használatát. **Folyamatosan kutatnak shadow copy és egyéb visszaállítást, helyreállítást segítő rendszermentések után, és azokat is megsemmisítik, valamint minden felcsatlakoztatott meghajtón (fizikai, netes, felhős) is végigmennek, és ott is elvégzik a pusztítást.**

Nagyjából 2020. óta már az adatok ellopása is megelőzi a rombolást, **így ha valamelyik áldozat nem fizet azért, hogy feloldó kulcsot kapjon, mert van neki mentése, akkor majd fizessen váltságdíjat azért, hogy a bizalmas adatok ne landoljanak a publikus neten. És azt látjuk, folyamatosan egyre jelentősebb célpontok kerülnek sorra világszerte.**



A szofisztikált működés emellett jó ideje abba az irányba is elindult, hogy optimalizálva a támadási időt, kihagyják a felesleges mappákat a titkosításból, ennek egyértelmű jeleit lehet látni már a RagnarLockerben is.

Kihagyásra kerülnek többek közt a Windows, Windows.old, Mozilla, Mozilla Firefox, Tor browser, Internet Explorer, $Recycle.Bin, Program Data, Google, Opera, Opera Software, stb. mappák. Emellett a Windows működéséhez szükséges állomány kiterjesztések szintén nem kerülnek elkódolásra, például a .db, .sys, .dll, .lnk, .msi, .drv és a futtatható .exe típusú fájlok.



A tavalyi Colonial Pipeline után már egyre több kritikus infrastruktúra ellen jelentkezik támadás más országokban is, például pár napja **a romániai Rompetrol szenvedett el egy ilyen incidenst**, ahol a weblapjaik mellett **a kieső Fill&Go rendszerük leállása miatt a benzinkutak is működésképtelenné váltak.**

Az itteni elkövetők **a HIVE csoport nevében 2 millió dolláros váltságdíjat követeltek annak fejében, hogy átadják a helyreállításhoz szükséges egyedi dekódoló kulcsot, valamint hogy ne szivárogtassák ki nyilvánosan az innen ellopott bizalmas adatokat a HiveLeaks Tor webhelyén.**

9 komment
Címkék: usa infrastruktúra erőmű kritikus váltságdíj ransomware kibertámadás olajvezeték zsarolóvírus

Ajánlott bejegyzések:

A nyugtalanság tengere

Apa kezdődik!

Tesz-e Oroszország a ransomware ellen?

Fizess vagy einstandoljuk a kőolajvezetékedet!

Nem csitulnak a kórházak elleni támadások

Kommentek:

Head Honcho 2022.03.10. 00:48:20

Nem kell publikus netre engedni ezeket a kritikus területeket, ennyi.

Válasz erre

Who111 2022.03.10. 06:55:47

copy *.* C:\Windows.old
Egyébként meg igaz az előző...

Válasz erre

nemecsekerno_007 2022.03.10. 09:07:26

Háborút provokáltak. Megkapták.
Mi már hamarabb megkaptuk.
Ne csak Európa szopjon.

Válasz erre

Head Honcho 2022.03.10. 10:03:36

Kik provokáltak háborút?

Válasz erre

nemecsekerno_007 2022.03.10. 11:29:12

@Head Honcho: Ezt komolyan kérdezed?
Keress rá arra, hogy Monroe-elv.
Illetve nézd meg George Friedman 2015-ös sajtótájékoztatóját:
m.youtube.com/watch?v=gGdcQMaLinE

2015 február, nyáron jött a migránsválság, ősszel a dízelbotrány. Németország kipipálva.

Válasz erre

steery 2022.03.10. 15:10:01

Ez után a hír után mindenki a /Windows és /Mozilla mappákba fogja eldugni az értékes adatait .db vagy .dll kiterjesztéssel álcázva a cuccot.

Válasz erre

Head Honcho 2022.03.12. 11:06:10

@nemecsekerno_007: Konteós hülyeségeken kívül gondoltam, de csalódnom kellett. Olyanról tetszett hallani, hogy az ukránoknak is van önrendelkezésük, és ők saját jogon döntöttek, hogy kívánnak tartozni?

Válasz erre

Head Honcho 2022.03.12. 11:07:04

*hova

Válasz erre

nemecsekerno_007 2022.03.13. 12:00:31

@Head Honcho: Sárga és hápog, de véletlenül se kacsa, mivel az konteo lenne.
Igaz, hogy az oroszok is nyomják a propagandát de az USA-hoz képest amatőrök. Az USA elérte, hogy a haladó Hópihék ukrán nácikat támogassanak és véres szájjal küldjék vágóhídra a civileket.

A önrendelkezési jog annyit ér amennyit meg tud belőle valósítani.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Antivírusblog
245 követő

Oldal követése Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Fakenews fék - vajon hol a pedál?

2022. március 16. 10:06 - Csizmazia Darab István [Rambo]

Manapság a print és a sugárzott televízió adások tömegfogyasztásának erőteljes gyengülése közben **egyre inkább az internetről is tájékozódunk**. Nagyszüleink korában sokan gondolhatták, igaz hiszen bemondta a rádió és megírta az újság. Szüleink korában sokan gondolhatták, igaz hiszen láttuk a TV-ben. **A mi korunkban pedig sokan gondolják, igaz hiszen a saját szememmel láttam a neten. Sajnos ennél azért bonyolultabb a dolog.**

Ha az iskolai biztonságos internet tematikából kikeressük, mit tanítunk a gyerekeknek az álhírekről, akkor nagyjából így foglalható össze a lényeg. Sok káros tartalom található a neten, ezek egy része az életkoruknak nem megfelelő (pl. erőszakos; veszélyes pl. netes kihívások), anyagi haszonszerzésre irányuló csalás, vagy hamis információ. **Ez utóbbiak lehetnek tévedések illetve szándékos félrevezetések, ez utóbbi megtévesztésekre használják gyakran az álhír vagy fakenews kifejezést is.**

Sajnos manapság sokszor az is látható, hogy ezt akkor is használják, ha például a hamis hír terjesztőjét szembesítjük az igazsággal: a lapos Föld hívő ekkor, ha látja is gömböt formázó űrhajós bolygófelvételeket, kikéri magának és fakenewst, hamisítást kiált.

Mi most viszont inkább azt szedtük össze, hogy ismerhetjük fel könnyen a valótlan híreket, információkat, mikre érdemes figyelni. Ezek a hamis hírek **bármilyen platformon megjelenhetnek, nyomtatott, televízión sugárzott vagy internetes környezetben egyaránt.** Érdemes azt is megjegyezni, hogy a statisztikákból még mindig az látszik, hogy átlag napi 3-4 óra televíziós képernyőidő jut a magyar fogyasztókra, és ebben benne van az is, hogy az alacsony státuszúak az átlaghoz képest fél órával többet tévéznek - leegyszerűsítve, aki szegény, többet tévézik.

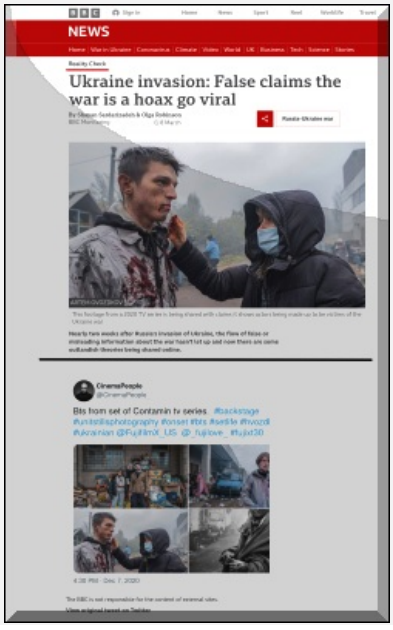
A netes tartalmak azonban **mára a legjellemzőbb információforrásnak számítanak, és sokan csak a saját "vélemény buborékjukból" tájékozódnak, ahol az ugyanazon nézetet vallók mindig azt és csak azt a véleményt kapják, amit hallani akarnak.**

Mik a fő tippek? **Ellenőrizzük, ki hozta létre az adott weboldalt, ki írta a cikket! Gondolkodjunk reálisan, a címsorok sokszor túlzóak, hazugok, hogy sokan kattintsanak rá. Több párhuzamos és hiteles forrásból tájékozódjunk**, és hasonlítsuk össze az információkat azzal, amit magunk, családtagjaink, barátaink közvetlenül tapasztaltunk. Ellenőrizzük a cikk megjelenési dátumát és külön a képeket is, pl. TinEye inverz képkeresővel vagy a Google Imagesearch funkciójával, hogy láthassuk, ezenkívül hol, mikor és mire használták fel azokat!

Sose dőljünk be a manipulációknak, hangulatkeltésnek, és az is hasznos szokás, ha vannak olyan mértékadó hiteles szakemberek, médiaszemélyiségek, akiknek adott témában rákereshetünk a véleményére, szerintük hihető-e az éppen keresett hír vagy információ! Legyünk tudatában annak is, hogy egy hihetetlen dolog lehet mém, photoshop vicc, vagy ártalmatlan szatíra is, ezt viszont illik feltüntetni.

Szerencsére sok hasznos összefoglaló létezik, amely ezt a hiteles tájékozódást, eligazodást nagyban segíti, mindennek persze első lépése, hogy egyáltalán mi magunk felismerjük, hogy szükséges ez a forráskritika. Az orosz-ukrán háborúval kapcsolatban is számos hamis hír jelenik meg, kezdve attól, hogy az orosz állampolgársággal is rendelkező Steven Seagal egy filmjelenetből kivágott fotóját arra használták fel, hogy elhitessék, az orosz oldalon ő maga is beszállt fegyverrel harcolni.

De felbukkantak olyan állítólagos orosz háborús felvételek is, amelyek **eredetileg egy 2020-as Contamin című ukrán televíziós sorozatból valók, ahol a színészek arról posztoltak, hogy a filmfelvételen hogyan kenik szét az arcukon a művért a hitelesebb moziélmény bemutatása miatt.**



Emellett a Welivesecurity weboldal is összeszedte azokat a legfontosabb jellemzőket, amikre érdemes figyelni az álhírek kapcsán. **Tony Anscombe biztonsági szakértő tanácsai közt szerepel, hogy több forrásból is igyekezzünk tájékozódni, és legyünk gyanakvóak a szenzációhajhász címeknél,** posztoknál, híreknél. **Egy másik alapos összefoglaló olvasható a Corvinus blogon, amely kifejezetten a háborúval kapcsolatos dezinformációval kapcsolatban ad gyakorlati útmutatást.**

És végül egy olyan cikk is elérhető, amely **az INVID nevezetű böngésző kiegészítő segítségével mutatja meg, hogyan leplezhető le, ha egy manipulációs céllal összevágott híradós anyag több, különböző és nem is az adott témában, adott időben, adott országban felvett videókat tartalmaz összekeverve.**

Két frappáns ontopic idézettel zárjuk a mai posztunkat.

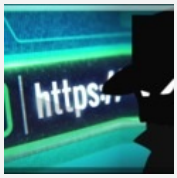
"*1018-ban az emberek nagyjából tudták, hogy milyen lesz 1050, tudták, hogy nagyjából azokra a skillekre lesz szükségük a gyerekeiknek, mint amiket ők is megtanultak: parasztoknak földművelés és csöndben levés; leányoknak háztartási praktikák; nemeseknek vadászgatás, kardozás, menedzsment, ilyesmi. Manapság fogalmunk sincs nem csak arról, hogy milyen lesz 2050, de azt sem tudjuk, milyen lesz 2023: mikor jön valami forradalmi technológia vagy katasztrófa, ami felforgatja a világot és alapjaiban változtatja meg az életünket. Ami szinte biztos, hogy sok változás előtt állunk.*"
(Yuval Noah Harari: 21 lecke a 21. századra)

"*Az interneten a tartalom gazdag és széles, mindenki azt fogyaszt, amit akar, és ugyanígy el is kerülheti a szennynek érzett tartalmakat. Ezt meg kell tanulni, ez médiafogyasztási higiénia kérdése.*"
(Stefan)

5 komment
Címkék: média fake trükkök news tippek álhír biztonságtudatosság fakenews

Ajánlott bejegyzések:


10 gyakori IT biztonsági hiba



Böngészés - kockázatok és mellékhatások


10 alaplépés a biztonsághoz


Kiberbiztonsági útikalauz diákoknak

Közösségi média VS munkahely

Kommentek:

különvélemény 2022.03.17. 05:55:00

Az átlag ember úgy sem fog semmilyen "lépéseken" átmenni, sőt gyakran csak a főcímet olvassa, ezért is szokták a cikk aljára tenni, hogy már cáfolták a hírt, még a legnagyobb hírportálok is eljátsszák ezt minden nap.
Ma már szinte mindenki nyomja az álhírt, emlékezzünk csak a Bloomberg kamu kínai lehallgató csipjére az alaplapon, amit szinte azonnal cáfoltak szakemberek, hogy ez így nem működhet, majd a gyártó is, majd a szakma is, akinek volt ilyen alaplapja és senki sem találta az állítólagos csipet. Érdekelt valakit is? Nem.
De itt a wuhani biolab, amiről kiderült, hogy mégiscsak finanszírozta az USA, vagy a legújabb ukrán biolab, amit először egymást taposva minősítettek propagandának a "Fact Checkerek", majd kiderült, hogy mégis csak vannak, de csak vakcinákat fejlesztenek, majd az újabb magyarázat a volt szovjet vegyi fegyverek megsemmisítését végzik (17 éve), majd a pentagon még rátett a lapáttal egy szalmabáb érveléssel, hogy nincs amerikai tulajdonban és nem is üzemeltet az USA biolabot Ukrajnában, amit senki sem állított, csak azt, hogy támogatták/finanszírozták.
Szóval mindenki folyamatosan hazudik, a mainstream media nézettsége is a béka segge alatt van, mert annyiszor megbuktak már, hogy senki sem hisz senkinek.

Válasz erre

Motorogre 2022.03.17. 07:42:39

A leírtak kb. helytállóak (saját vélemény, ellenőrizd a forrást !!!) de mindennek az elvégzése a hírszerkesztők feladata lenne. Sajnos nem, a netes cikkeknél a megjelenés dátuma is sokszor hiányzik. Olvasod hogy március 1-től díjtalanul szállíthatsz kerékpárt a 77-es villamoson --- aztán megbüntet az ellenőr, mert ilyen akció 2016-ban volt egyszer. De gyógyszerek használati leírásai is hibásak - hogy honnét tudni: két de eltérő anyag is található a neten.
A könyviadásban főleg szakkönyveknél a Lektor meg az OlvasóSzerkesztő szerepe igen fontos volt - Ők nem költöztek át a netre. Kár ...

Válasz erre

Ekrü 2022.03.17. 09:12:06

Az én álhírem a valóság, a te álhíred megvetendő,mert becsapod az embereket...Kb,így működik az összes média. Amúgy meg mindenkinek joga van abban hinni amiben akar. Ha valaki olyan hülye,hogy nem néz utána az általa olvasott hír valóságtartalmának ,akkor az megérdemli a sorsát.

Válasz erre

rabelais · nacifacebook.blog.hu 2022.03.17. 09:29:02

Azt utálom az ilyen fake newsról szóló blogokban, hogy kurvára egyik se bírja összeszedni azokat az elveket, amelyek a fake news kiszűrését elősegítenék, mert ahhoz hülyék. Mindegyik csak okoskdoik, de fingja nincs arról, hogy mi a racionális gondolkodás, mik lennének a racionális gondolkodás elvei, és, hogy általánosságban hogyan is lehet eldönteni azt, hogy mi fake news.

Válasz erre

MaxVal BircaMan KözÍró · http://bircahang.org 2022.03.17. 11:14:04

Alapból minden fakenews, amit nem Soros hálózata adott közre.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

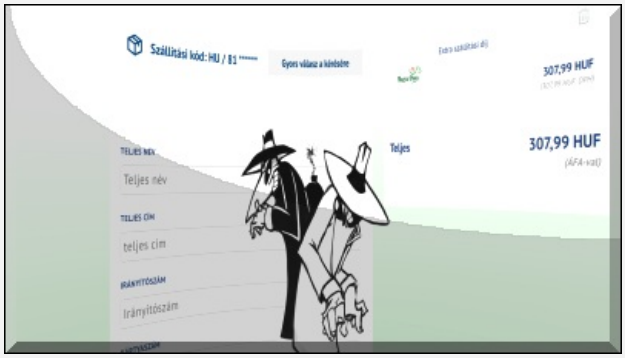
accountz

Belépés
Regisztráció

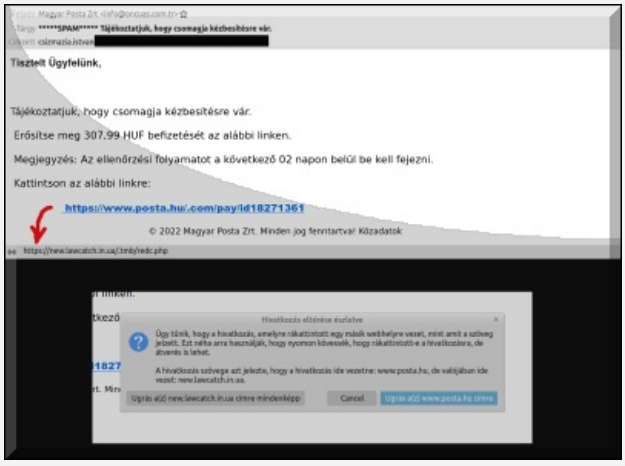
Magyar Posta csomagunk jött - vagy mégsem?

2022. március 18. 12:53 - Csizmazia Darab István [Rambo]

Elpusztíthatatlan vagy mégsem rovatunkban ezúttal egy olyan kéretlen e-mail üzenet szerepel, amely **a Magyar Posta nevében igyekszik begyűjteni a banki adatainkat**. Az is látható, hogy ez is egy Wordpress sebezhetőséget kihasználva terjed a neten.

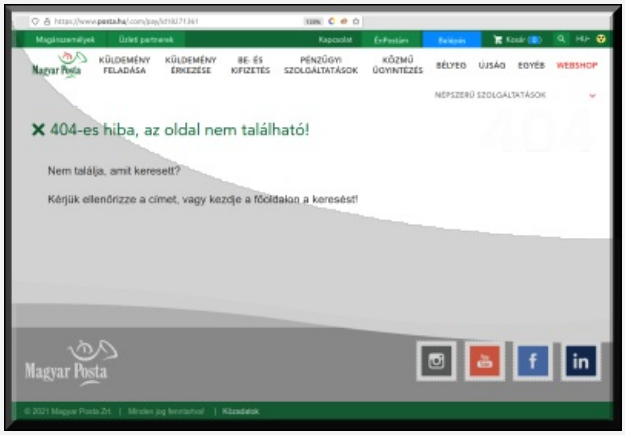


"*Tisztelt Ügyfelünk,*
Tájékoztatjuk, hogy csomagja kézbesítésre vár.
Erősítse meg 307,99 HUF befizetését az alábbi linken.
Megjegyzés: Az ellenőrzési folyamatot a következő 02 napon belül be kell fejezni.
Kattintson az alábbi linkre:
https://www.posta.hu/.com/pay/id18271361"



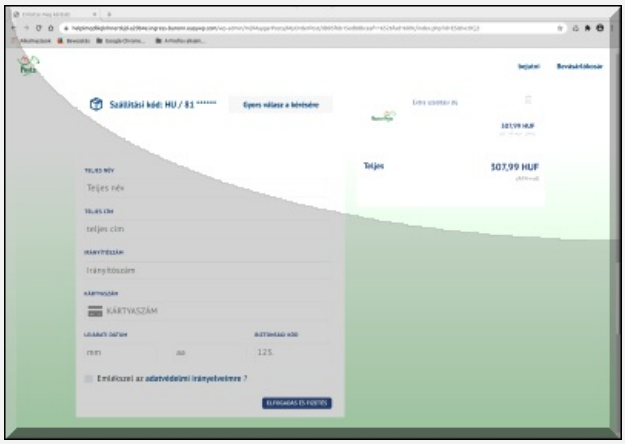
A kamu levél linkje csak a megjelenésében tartozik a postához, valójában ha az egérkurzort fölé mozgatjuk, először egy ukrán link látható, amiről aztán a kaliforniai easywp.com egy olyan aloldalára érkezünk, amely **ékes magyar nyelven kér bennünket, ugyan utaljunk már át 307 forint 99 fillért a mellékelt űrlap segítségével extra szállítási díj címén.**

Nem egy óriási címlet, és persze nem is ez a zsákmányszerzés lényege, hanem a kártyaadatok.

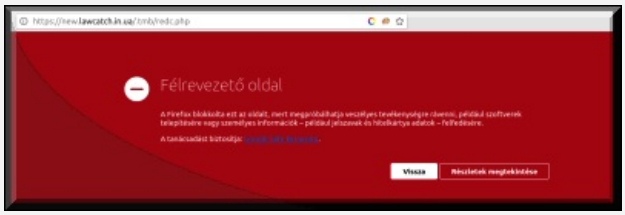


Persze nem javít a helyzeten az sem, ha a szöveget bemásoljuk kattintás helyett, a **figyelemelterelés a**

".com/pay/stb." csak valódi link látszatát hivatott mutatni, és senki nem fogja kattintás helyett a címet másolgatni, ami természetesen nem vezet sehova, bár az adathalász weboldalt sikeresen el lehet így kerülni.



Azt azért megjegyezhetjük, hogy aki egy ilyen weblapon, ami a posta.hu helyett "loxcawahynagrwa-a20b4e PONT ingress-erytho PONT easywp PONT com" bizalmas banki adatokat gépel be, annak a kezére lehetne ütni a figyelmetlenségéért. Na mi viszont szándékosan kattintunk, hogy **lássuk miket kér be tőlünk: teljes név, teljes cím, irányítószám, bankkártya száma, lejárati dátum és tadaaaam!, naná, hogy a 3 jegyű CVV biztonsági kódunk is érdekli a csalókat.**



A lap alján látható **"Emlékszel az adatvédelmi irányelveimre ?" csak egy kamulink, ide rákattintva mindössze újra betöltődik az adott oldal,** és semmilyen adatvédelmi nyilatkozat nem jelenik meg, nem irányít el bennünket sehova.

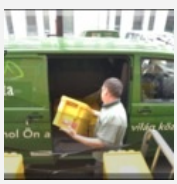
Érdekes módon **a kártékony adathalász link még mindig működik, igaz a Google és a Netcraft rendszere már szépen belistázta a rosszindulatú webhelyek közé.**

Bár az egész próbálkozás jóval fapadosabb, mint amilyen a tavaly márciusi, pont egy éves FedExes átverés volt, azért az maradhat tanulság, hogy **érdemes óvatosan kezelni a kéretlen üzeneteket, figyeljünk oda a linkekre, gondolkozzunk, mielőtt utalnánk, és gyanakodjunk bátran**, ha a Magyar Posta Zrt. nevében az info KUKAC oncuas PONT com PONT tr" törökországi címről értesítenek bennünket állítólagos csomagunkról.

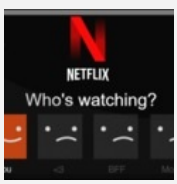
5 komment
Címkék: magyar posta csomag e-mail adatok csalás átverés adathalászat banki vagymégsem

Ajánlott bejegyzések:

Ismét csomagunk érkezett - vagy

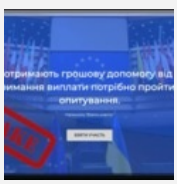


Csomagja kézbesítésre vár! Vagy mégsem?



Tagsági kérdések - vagy mégsem?

Viva la Revolut



Adathalászok lakat alatt

[mégsem?]

Kommentek:

MaxVal BircaMan KözÍró · http://bircahang.org 2022.03.18. 23:10:02

Nekem csak a múlt héten 26 csomagom jött. Mindnek kifizettem a költségét, s várom, mikor lesz a kiszállítás.

Válasz erre

Flowey 2022.03.19. 14:11:09

Ez vicces, hogy van aki ennek bedől. A másik kedvencem e-mail SPAM fiók következetes "I'm the Chinese software engineer who hacked into your device OS." kezdettel és olyan oldalakkal akar zsarolni, amiken az életben nem jártam (insta meg twitter) és szerinte le is kameráztak, ami megint csak egy érdekes dolog, mert nincs webkamerám vagy ilyesmi. De persze küldjek csak nekik 0,mittoménmennyi bitcoint. Nice try, mint régen a nigériai herceg, ami amúgy nincs is.

Válasz erre

geegee · http://eszakonelunk.blog.hu 2022.03.19. 23:24:34

@Flowey: Van már ilyenből magyar nyelvű is sajnos, és fejlődőképesek, mert egyre szebben használják kies nyelvünket.Már nincsenek központozási hibák, meg váltott tegezés-magázás, valszeg egy originál magyar megfogalmazta rendesen a szöveget és eladta a mocskos csalóknak.Nekem van webkamerám, de "tejfölöspohár" van rajta, meg egyébként is el van forgatva alapból a plafon felé; úgyhogy nálam is besz*pták a dolgot.Nem is igazi netező az, aki nem kapott már vagy öt darab ilyen levelet.
:-))

Válasz erre

Billy Hill 2022.03.19. 23:24:51

@Flowey: Azóta van egy update, ti. most már Ukrajnából kell ott rekedt diplomatát (és természetesen a tetemes pénzét) kimenteni, a héten már kaptam egy ilyet is...

Válasz erre

Billy Hill 2022.03.19. 23:29:22

@Billy Hill: Kedvencem ebből a stílusból a (még régi) szarul fordított, amikor az idős, 70 feletti nő (valamilyen asszony) ír nekem "egy humanitárius föld alatt" (gondolom "on humanitarian grounds" volt az eredetiben), hogy segítsek neki néhai nagyon jóember férjének millióit "kimenteni", majd az aláírásban ott van, hogy "Joselyn kisasszony". Na most akkor mámika vagy bébike? :-)

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

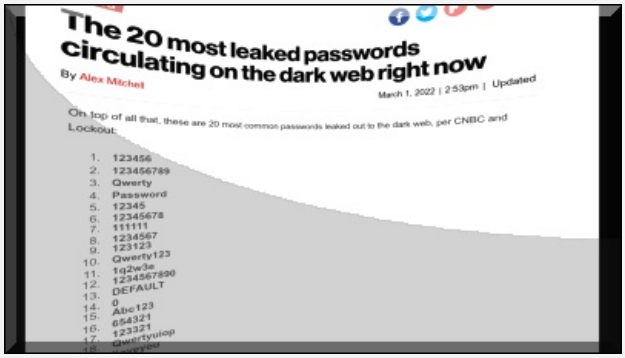
Gyenge, gyengébb, leggyengébb

2022. március 22. 17:54 - Csizmazia Darab István [Rambo]

Megjelent egy friss lista, amiben **a dark weben található ellopott, kiszivárgott leggyakoribb jelszavak szerepelnek.**

A jelszavakról már sokszor volt szó, arról is, hogy miket lehet használni helyette és mellette, és arról is, hogy mikre érdemes figyelni a jelszó választáskor, hogy lehetőség szerint az erős, biztonságos lehessen.

Ezenkívül **rendszeresen írtunk a Worst Password és hasonló válogatásokról,** amiknél a leggyengébb jelszavak elrettentő listáját tették közzé.



Vajon látszik-e most 2022-ben a fentiek fényében lényeges változás, gigászi előrelépés, hihetetlen módon megerősödött biztonságtudatosság a felhasználói szokásokban? Spoiler alert - sajnos ilyesminek szabad szemmel a leghalványabb nyoma sem látható. Íme a top 20-as lista:

01. 123456
02. 123456789
03. Qwerty
04. Password
05. 12345
06. 12345678
07. 111111
08. 1234567
09. 123123
10. Qwerty123
11. 1q2w3e
12. 1234567890
13. DEFAULT
14. 0
15. Abc123
16. 654321
17. 123321
18. Qwertyuiop
19. Iloveyou
20. 666666

Hát ünneplésre nincs sok okunk. **A kellően erős jelszó választáshoz többször is adtunk már e hasábokon tanácsokat, legutóbb például ebben a posztban**. Ebben többek közt azt írtuk, hogy használjunk egyedi és erős jelszavakat, bízzuk a munkát a jelszógenerátorra, kerüljük a jelszavak újrafelhasználását, éljünk a többfaktoros hitelesítés lehetőségével, legalább negyedévente cseréljünk jelszót a legfontosabb fiókjainkban.

Ha pedig incidens áldozatai lettünk, akkor az alábbi teendőket érdemes végigvenni, és alaposan átgondolni.

Szólj hozzá!
Címkék: toplista jelszó password tippek gyenge worst darkweb

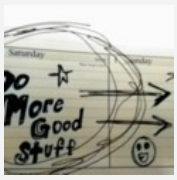
Ajánlott bejegyzések:

Nem életrevalók

Még gyengébb a jelszavad

C mint CEO, P mint password


Az elveszett jelszavak fosztogatói



10 kiberbiztonságra veszélyes szokás

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.

VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Eljött az emelt szintű biztonság ideje

2022. március 25. 12:31 - Csizmazia Darab István [Rambo]

Az ukrajnai konfliktus világszerte növeli a kibertámadások kockázatát. **Mit tehetnek a vállalkozások, szervezetek a kibervédelmük javítása érdekében?**

A szomszédunkban zajló események következtében számíthatunk-e a kibertámadások növekedésére? Ez az egyik leggyakoribb kérdés, amit feltesznek Oroszország ukrajnai offenzívája óta. Az ESET kiberbiztonsági szakértői szerint válasz egyszerű: igen. **Konfliktusok során a szokásos menetrend része a kommunikáció és az információs csatornák megzavarása.**

Számos hírt olvashattunk például arról, hogy fontos ukrajnai webhelyek ellen indítottak szolgáltatásmegtagadási (DDoS) támadásokat.

Az Ukrajnával szolidaritást és támogatást kifejező országokban működő vállalkozásokat és szervezeteket a kormányok és kiberbiztonsági ügynökségeik - köztük az Egyesült Államok Kiberbiztonsági és Infrastruktúrabiztonsági Ügynöksége (CISA) - folyamatosan figyelmeztetik a kibertámadások számának várható növekedésére. Van erre esély? Válasz egyértelműen igen.

Egyértelműen fennáll annak a veszélye, hogy **tovább nő a dezinformáció, az álhírek és az adathalász e-mailek száma, amelyek megpróbálják a címzetteket olyan hamis oldalakra irányítani, amelyek látszólag ukrán menekültek számára gyűjtenek adományt, hitelesnek álcázott hírekre és szervezetekre hivatkozva.**

Az ESET kutatócsoportja már közzétett néhány példát, amelyek a kiberbűnözők éberségét és képességét mutatják arra, hogy gyorsan és hatékonyan indítsanak kampányokat a pénzszerzés érdekében. Voltaképpen bármilyen krízishelyzet lehetőséget ad az átverésekre, gondoljunk csak a világjárványra, amikor azt tapasztaltuk, hogy hamis kontaktus-nyomkövető alkalmazások, adathalász e-mailek és védőfelszereléseket kínáló webhelyek jelentek meg.

A jelenlegi ukrajnai helyzet is bizonyítja, hogy a vállalatoknak jobban fel kell készülniük a kiberbiztonsági incidensek kivédésére és kezelésére. A tavalyi év kétségtelenül a ransomware zsarolások csúcsra járatásának éve volt, olyan kiemelkedő esetekkel, **mint a Colonial Pipeline 4,4 millió dolláros, a CNA Financial 40 millió dolláros váltságdíja vagy a Kaseyától követelt 70 millió és a Media Markt-tól követelt 240 millió dollár.**

A ransomware támadások is számos súlyos sebezhetőségre derítettek fényt, amely erősítette ugyan a tudatosságot, de ezért nagy árat kellett fizetni. És mivel az ördög nem alszik, jó, ha újra és újra ellenőrizzük szervezetünk biztonsági folyamatait és működését.

Íme néhány fontos lépés, amit mindenképpen érdemes megtenni a vállalkozásunk biztonsága érdekében:

1. Frissítsük (vagy készítsük el) az üzletmenet folytonosságát biztosító tervet. Tervezzük meg, hogyan működhet a vállalkozás folyamatosan egy esetleges kibertámadás alatt, abban az esetben is, ha a rendszerekhez való hozzáférés korlátozottá válik.

2. Készítsünk gyakorlati krízisforgatókönyvet. Győződjünk meg róla, hogy mindenki ismeri a szerepét és a vele szemben támasztott elvárásokat egy ilyen kiélezett helyzetben.

3. Frissítsük a vészhelyzeti forródrót listáját - Ki kit fog értesíteni probléma esetén?

4. Mérlegeljük a krízisterv készítésénél, hogy a **partnercégeink ellátási láncában hol szerepel a mi vállalatunk.**

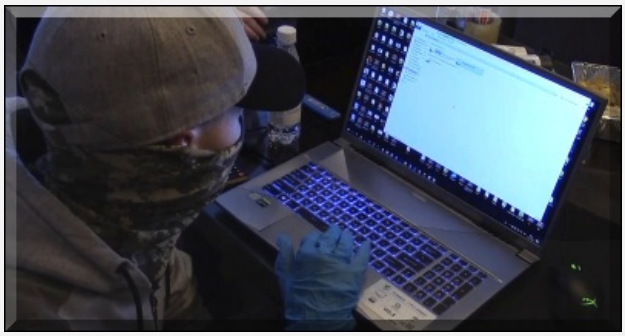
5. Mind a vertikális, mind a horizontális vállalati kapcsolatokban ajánlatos **összehangolni a kiberbiztonsági szabályzatokat**, hogy azok összhangban legyenek egymással.

6. Erősítsük meg kiberbiztonsági csapatunkat és a fordítsunk kiemelt figyelmet a kulcspozíciókban lévőkre. Előfordulhat, hogy egy incidens esetén nagyon gyorsan kell reagálni, ezért kritikus, hogy a megfelelő emberek legyenek a megfelelő pozíciókban.

7. Kísérjük figyelemmel a gyanús és szokatlan hálózati történéseket. Javasoljuk az EDR, XDR megoldás bevezetését, hiszen a korai riasztási rendszer segít a csapatoknak a kritikus incidensekre összpontosítani.

8. Ha a cégen belül nem állnak rendelkezésére a szükséges erőforrások egy jelentősebb incidens kezelésére, **szervezzük ki ezt a kritikus feladatot.** Fontoljuk meg, hogy erre a tevékenységre külső szolgáltató támogatását vesszük igénybe.

9. A kiberbiztonsági kockázatok tudatosítása érdekében **tartsunk oktatást, tréninget minden alkalmazott számára,** amely során újra emlékeztetjük őket arra, hogy ne nyissanak meg mellékleteket, és ne kattintsanak ismeretlen vagy gyanús hivatkozásokra. Ez segíthet abban, hogy minden alkalmazottunk naprakész és biztonságtudatos legyen.



Emlékeztetőül: néhány alapvető kiberbiztonsági követelmény

1. Erős és biztonságos jelszavak - vagy ami még jobb, az erős összetett jelmondatok alkalmazása. Lehetőleg minden fiókban, de kiemelten a pénzügyi tranzakciós felületeken használjunk egyedi, eltérő jelszavakat. Ebben segítségünkre lehet egy jelszókezelő alkalmazás.

2. Kétfaktoros hitelesítés alkalmazása minden admin felületen és minden rendszergazdai jogosultsággal rendelkező fiókban. Ez a szenzitív vállalati adatokhoz hozzáféréssel rendelkezők esetében is kritikus fontosságú.

3. Telepítsük haladéktalanul a frissítéseket és a hibajavításokat rendszeresen annak érdekében, hogy a lehető legkisebb eséllyel váljon sebezhetővé a rendszerünk.

4. Teszteljük a biztonsági mentéseket és a katasztrófa utáni helyreállítási rendszereket. Ügyeljünk arra, hogy offline és a felhőben is készítsünk biztonsági másolatokat.

5. A felhasználói hozzáférések auditálása: csökkentsük a kockázatot a szolgáltatásokhoz, szoftverekhez és adatokhoz való hozzáférés szabályozásával úgy, hogy minden munkavállaló csak azt érje el, ami a feladatai elvégzéséhez szükséges.

6. Zárjuk be azokat a portokat és állítsuk le azokat szolgáltatásokat, amelyeket nem használunk, mert ezek biztonsági rést hagyhatnak a visszaélésekhez.

7. Az elavult technológián alapuló régebbi rendszereket, amennyire lehet, **válasszuk le a hálózat többi elemétől és a nyilvános internethálózatról is.**

8. És természetesen ügyeljünk arra, hogy **minden végpontot, szervert, mobileszközt és más digitális eszközt folyamatosan frissített és teljesen működőképes biztonsági szolgáltatással védjünk.**

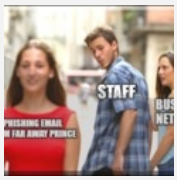
Egy kibertámadás számos negatív következménnyel járhat a vállalatok számára - beleértve a munkavállalókat, a gazdasági mutatókat és az egész szervezet működését - ezért elengedhetetlen, hogy alaposan felkészüljünk. Ne feledjük: **a fenyegetések mennyisége és kifinomultsága folyamatosan emelkedik és fejlődik.**

Szólj hozzá!
Címkék: ukrajna oroszország háború tippek megelőzés védekezés kiberháború kiberbiztonság

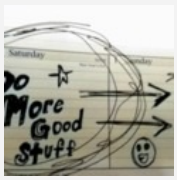
Ajánlott bejegyzések:


10 alaplépés a biztonsághoz


10 gyakori IT biztonsági hiba



10 gyakori ok, amiért bedőlünk a csalásoknak



10 kiberbiztonságra veszélyes szokás


Fiatal vagy? Ezekre az online csalásokra figyelj!

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Antivírusblog
245 követő

Oldal követése Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

- RSS 2.0
- bejegyzések, kommentek
- Atom

bejegyzések, kommentek

accountz

Belépés
Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

Fedett pályás titkosítási bajnokság

2022. március 29. 11:34 - Csizmazia Darab István [Rambo]

Elképesztő, hogy nem csak a számítógépes vírusok történelme **is már 36 esztendős, de szinte hihetetlen, hogy a mai klasszikusnak számító ransomware első tipikus szereplője, a CryptoLocker is 2013-ban bukkant fel, azaz ez a támadási módszer is már 10 éves.**

A napokban olvashattunk arról, hogy 2021-ben az átlagos váltságdíj már 2.2 millió dollárnak megfelelő összegre emelkedett a Palo Alto Unit42 beszámolója szerint, és ez az előző évihez képest 144%-kal nőtt. Több tucat híres-hírhedt csoport fejleszt-terjeszt zsarolóvírus fertőzést, és a Ransomware as a Service (RaaS), azaz a bérelhető szolgáltatásként igénybe vehető ransomware üzletág is **már évek óta pörög a darkneten.**

A felkínált elemek közt olyan **extrákat találhatunk, mint 7/24 support, nyelvi támogatás nyújtása, váltságdíj-tárgyalások kezelése, a megszerzett doxing adatok tárolása-közzététele, direkt telefonhívások az áldozatoknak, vagy éppen DDoS támadás indítása vonakodó fizetés esetén.**

A ransomwarek száma már több ezres nagyságrendű, rendkívül elterjedtek, és **technikai fejlődésük-fejlesztésük is töretlen**: rámennek a backupokra, árnyékmásolatokra és törlik ezeket, képesek a hálózatban terjedni, jogosultsági szintet tudnak emelni, szótáralapú támadást intéznek a primitív hálózati jelszavakra, és az erős egyedi gyors elkódolást is egyre ügyesebb algoritmusok végzik.

Ezek sok esetben ügyesen kikerülik a Windows rendszerállományait, és az értékes pótolhatatlan felhasználói dokumentumokra, fájlokra fókuszálnak, gyakran ezeknek is csak az első pár ezer bájtját hazavágva **tényleg rekordidő alatt darálnak le hatalmas merevlemezeket, hálózati vagy felhős tárolókat, sőt egész hálózati szegmenseket.**

Family	Median Duration
LockBit	00:05:50
Babuk	00:06:34
Avaddon	00:13:15
Ryuk	00:14:30
Revil	00:24:16
BlackMatter	00:43:03
Darkside	00:44:52
Conti	00:59:34
Maze	01:54:33
Mespinoza (PYSA)	01:54:54
Average of the median	**00:42:52**

Most egy olyan teszt eredménye jelent meg, ahol a Robot Wars vetélkedőhöz hasonlóan a **ransomware programok**

mérték össze egymással az erejüket az arénában, ami egy 53GB méretű válogatott teszt adatmennyiséget jelent, benne 98 ezer pdf, doc, xls, és hasonló tipikus Office és egyéb felhasználói állománnyal. Vajon ki képes hamarabb ledarálni ezt a nem kevés mennyiséget: ez volt a jelen kihívás lényege, és a versenyben a jelentősebb zsarolóvírus családokból több, különböző verzió is a startmezőre állhatott.

A vizsgálatot a Splunk információbiztonsági kutatói végezték **Windows 10 és Windows Server 2019 rendszereken, összesen 400 titkosítási tesztet 10 különböző kártevő családból, családonként tíz-tíz mintával.**

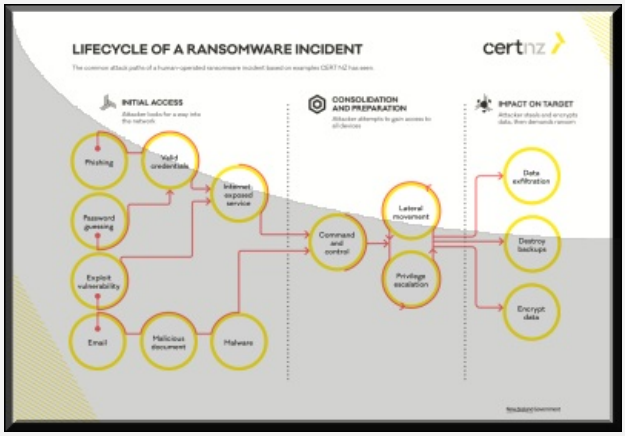
Encryption speed comparative table for some ransomware

PC for testing: Windows Server 2016 x64 | 8 core Xeon E5-2680@2.40GHz | 16 GB RAM | SSD

Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 357472)
LOCKBIT 2.0	6 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130	110468
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 29M	No	253	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 29M	No	902	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115	111002
RansomEXX	14 Dec,2020	138 MB/s	12M	20H	No	156	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91	81081
Ranzy	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17	109842
Sekhmet	30 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	364	random extension
Sun Crypt	26 Jan, 2021	104MB/s	16M	1D 2H 40M	No	1422	random extension
REvil	8 Apr, 2021	98 MB/s	17M	1D 4H 20M	No	121	109789
Conti	22 Dec, 2020	98 MB/s	17M	1D 4H 20M	Yes	186	110220
Ryuk	21 Mar, 2021	92 MB/s	18M	1D 6H	Yes	274	110784
Zeppelin	8 Mar, 2021	92 MB/s	18M	1D 6H	No	813	109963
DarkSide	1 May, 2021	83 MB/s	20M	1D 9H 20M	No	30	100549
DarkSide	16 Jan, 2021	79 MB/s	21M	1D 11H	No	59	100171
Nephilim	31 Aug, 2020	75 MB/s	22M	1D 12H 40M	No	3061	110404
DearCry	13 Mar, 2021	64 MB/s	26M	1D 19H 20M	No	1292	104547
MountLocker	20 Nov, 2020	64 MB/s	26M	1D 19H 20M	Yes	200	110367
Nemty	3 Mar, 2021	57 MB/s	29M	2D 0H 20M	No	124	110012
MedusaLocker	24 Apr, 2020	53 MB/s	31M	2D 3H 40M	Yes	661	109615
Phoenix	29 Mar, 2021	52 MB/s	32M	2D 5H 20M	No	1930	110026
Hades	29 Mar, 2021	47 MB/s	35M	2D 10H 20M	No	1909	110026
DarkSide	18 Dec, 2020	45 MB/s	37M	2D 13H 40M	No	17	114741
Babuk	4 Jan, 2021	45 MB/s	37M	2D 13H 40M	Yes	31	110760
REvil	7 Apr, 2021	37 MB/s	45M	3D 3H	No	121	109790
BlackKingdom	23 Mar, 2021	32 MB/s	52M	3D 14H 40M	No	12460	random extension

Az eredmény hirdetés alapján **a vitathatatlan győztes a LockBit lett 5 perc 50 másodperces eredményével, ami egyfelől elképesztő gyorsaság és hatékonyság,** másfelől például olyan neves szereplőknek, mint a jól ismert DarkSide vagy a Conti - számukra érdekes módon mindez több, mint tízszer annyi időbe tellett: 44 és 59 perc. Csalódást okozott a hírhedt Maze, hiszen számára majdnem két órára, 1 óra 54 percre volt szüksége ugyanehhez.

Az élmezőnyben végzett még a Babuk, Avaddon, Ryuk és a REvil is, ezek a programok nagyon gyors pusztítási képességeket tudtak villantani. Az első helyezett LockBit kiemelkedő teljesítményét úgy is megfogalmazhatjuk, hogy 25 ezer fájl percenkénti titkosítására volt képes.



Számunkra a látványos technikai érdekességen túl mindez azért is lehet tanulságos figyelmeztetés, mert jól láthatóan **drasztikusan lerövidült az az időablak, ami a szokatlan, gyanús tevékenység felismerése és az azt követő reagálás között marad a felhasználói-védekezői oldalon.**

Mindez még az összes ransomware szereplőt figyelembe vevő átlagolt eredménynél is csak mindössze 43 perc, és ez a fajta zsarolási modell sajnos túl jól és eredményesen működik.

Szólj hozzá!
Címkék: teszt titkosítás sebesség váltságdíj gyorsaság ransomware zsarolóvírus elkódolás lockbit splunk

Ajánlott bejegyzések:

[Még többet, még gyorsabban]

[LockBit vs. olasz adóhivatal]

[Kulcs a túléléshez]

[Rossz gondolatok a könyvtárban]

[Nem csitulnak a kórházak elleni támadások]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Kórházprogram

2022. április 04. 11:29 - Csizmazia Darab István [Rambo]

Észak-kaliforniai **egyik legnagyobb nonprofit egészségügyi szolgáltatókhoz kapcsolódó szervezete, a Partnership HealthPlan of California a napokban jelentős zsarolóvírus támadást** szenvedett el. Az incidens kezdete még március végére tehető.

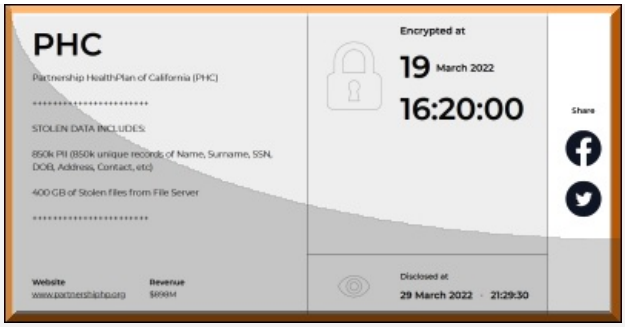
A ransomware támadásban **a Hive csoport több, mint 850 000 ember személyes adatait lopta el, valamint 400 GB bizalmas adatot is megszereztek a szervezet szervereiről**.

Az egészségügyi intézmények elleni akció sajnos korántsem egyedi, hiszen 2021-ben a Hive már legalább 28 más hasonló szervezetet támadott meg, köztük az Ohióban és Nyugat-Virginiában működő Memorial Health System-et is, és a sorozat az idén tovább folytatódott több amerikai kórház elleni zsarolóvírus támadással.

A Memorial tavaly augusztusban végül ki is fizette a váltságdíjat, mert leállt 800 szervere és 3000 internetes gépe, eszköze miatt minden sürgős sebészeti és radiológiai vizsgálatot törölniük kellett, emellett pedig 210 ezer páciensük adata is illetéktelen kezekbe került.

A mostani ransomware támadásban **a kiszivárgott 400 giga részletes betegadat komoly ütőkártya lehet a bűnözők kezében, hiszen a fenyegetés a klasszikus titkosítás és a hetekig tartó leállás mellett a doxing módszerével is fenyeget, azaz a LiveLeaks oldalán** keresztüli publikussá tétel ígérete is nyomást helyez az áldozatra.

Statisztikailag a ransomware támadások egyre nagyobb veszélyt jelentenek a közszférában, több száz állami vállalat és önkormányzat ellen követtek el hasonló támadásokat az Egyesült Államokban.



A HealthPlan már az incidens elején felvette a kapcsolatot és segítséget kért a Szövetségi Nyomozó Irodától (FBI).

A feltört és ellopott adatok betegenként változtak, de sajnos érzékeny részleteket tartalmaznak, így teljes nevet, elérhetőségeket, születési dátumot, beteg azonosító és bankszámlaszámot, vezetői engedély számokat, kórházi vagy orvosi kódokat, orvosi nyilvántartási számokat, egészségbiztosítási adatokat, tesztelési, diagnosztikai és kezelési információkat, valamint kárigényi adatokat.

Sajnos úgy tűnik, [a Hive csoport célzottan ráment az egészségügyi intézmények elleni sorozatos támadásokra](#).

A 898 millió dollárnyi (300 milliárd forintos) váltságdíj követelés viszont nyitó próbálkozásnak még így is nagyon erős.

Szólj hozzá!
Címkék: kalifornia kórház váltságdíj ransomware hive zsarolóvírus doxing

Ajánlott bejegyzések:


Nem csitulnak a kórházak elleni támadások


Emelkedő ransomware károk


Nem szállunk rendelkezésére II.


LockBit vs. olasz adóhivatal


Baljós árnyak: fekete macska Karintiában

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

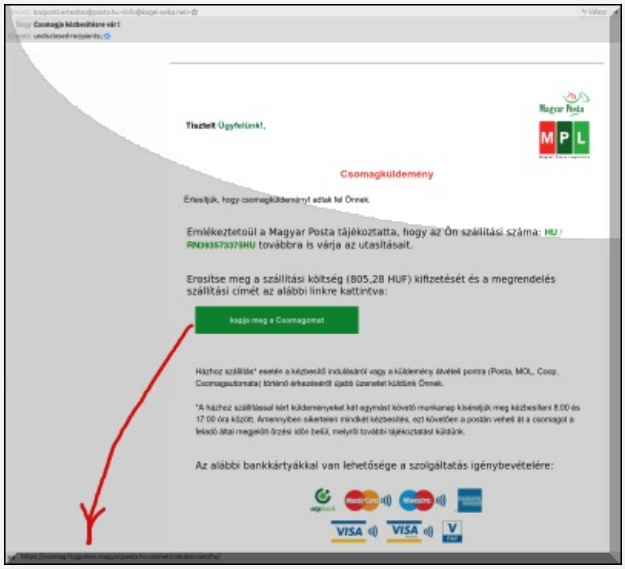
Csomagja kézbesítésre vár! Vagy mégsem?

2022. április 08. 11:39 - Csizmazia Darab István [Rambo]

Csalás csalás után érkezik földön, vízen levegőben. **Ezúttal látszólag csomagküldeményünk érkezett a Magyar Posta hivatalos logóját felmutató e-mail szerint**. Vajon jó egy évvel a FedEx-es sztori után ezúttal sikerül a tökéletes átverés?

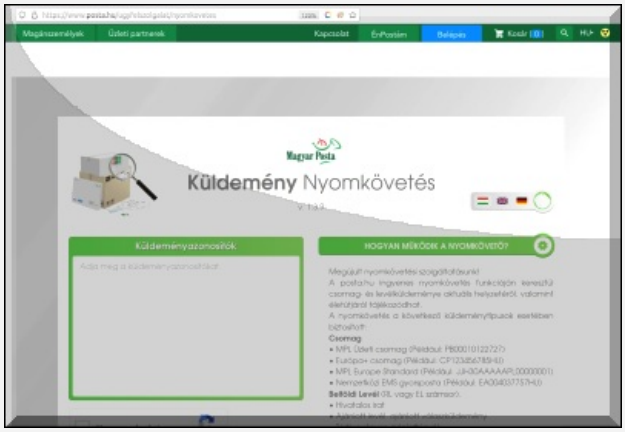
Spoiler alert: nem. Nézzük is az erre utaló jegyeket! Ki a feladó? Látszólag "*kozponti.ertesites@posta.hu*" de mellette meg ezt olvashatjuk: "*<info@kogei-seika.net>*". Hát ez nem igazán látszik hitelesnek.

De folytassuk, ha valóban mi kapnánk értesítést, mi lennék a címzettek. Mit találunk a címzettnél? "*undisclosed-recipients:;*" - ami **arra utal, hogy a csalók látatlanba kiszórtak egy rakat ilyen kéretlen levelet, és most várják, mennyien dőlnek be a próbálkozásnak.**



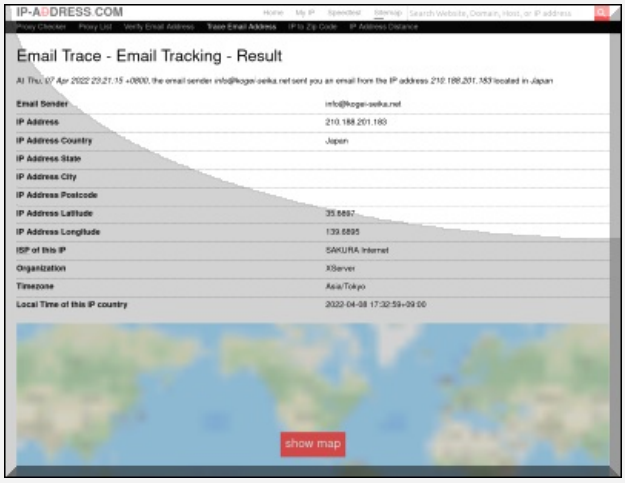
Jöhet a jó édes anyanyelvünk és **a magyar helyesírás alaposabb vizsgálata**, ebben is szépen ott vannak az intő jelek: "*Emlékeztetoül a Magyar Posta tájékoztatta, hogy az Ön szállítási száma: HU / RN393573375HU továbbra is várja az utasításait.*"

Ékezetek hibája pipa, suta fogalmazás pipa, kattintani kell pipa, pénzt kérnek pipa.



Haladó csoportos ellenőrzés, ha a levél header részét megetetjük valamilyen e-mail trace checker weboldallal, és megnézzük, honnan érkezett az üzenet. Itt még véletlenül sem a Magyar Posta jön a képbe, **hanem Tokyo, Japán IP cím a feladó lokációja.**

Valóban van olyan, hogy postai küldemények nyomkövetése, de annak az igazi hiteles weboldalnak egészen más a címe és kinézete. Nem is beszélve arról, hogy a valós link "www.posta.hu" kezdetű. Már eddig 4:0 ide, és még nem értünk a végére.



És akkor nézzük meg azt a linket, amit az állítólagos internetes fizetéshez kínálnak a csalók: "*hxxps://csomag.fuggoben.magyar.posta.hu.cosmeticsdubai.com/hu/*". Szerencsére ebben is van elütés, így ezúttal nem vezet semmilyen valódi helyre, és **szerencsére már meg sem jelenik az adathalász weboldal.**

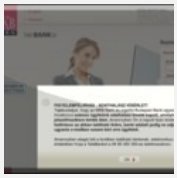
Ám ha csak a doménnév utolsó részét nézzük, **a "*cosmeticsdubai.com*" egy WordPress alapú weboldal, amit valószínűleg egy sebezhetőséggel feltörtek**, és egy aloldalát maszkírozták át postai fizető landing pagenek.

A mai gyenge spam próbálkozás gyanús külső jegyei **remélhetőleg már mindenkinek felkeltenék a biztonságtudatos figyelmét, és nem csak azért nem gyalogolnak bele egy ilyen átverésbe, mert a weblaphivatkozás ezúttal éppen nem működik.**

Szóval jönnek szépen sorban a magyar nyelvű csalási kísérletek, érdemes mindenkinek továbbra is figyelmesen kezelni a kéretlen üzeneteket.

1 komment
Címkék: spam magyar posta wordpress csalás átverés kéretlen adathalászat

Ajánlott bejegyzések:


MKB adathalászat szigonnyal, horoggal, hálóval


Magyar Posta csomagunk jött - vagy mégsem?

Ismét csomagunk érkezett - vagy mégsem?


Igazgató-e vagy?

Banki meló

Kommentek:

Head Honcho 2022.04.09. 15:29:39

Amatőr próbálkozás a pénzkaszára. Sajnos azok még amatőrebbek és figyelmetlenek, akik körében mégis képes aratni.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

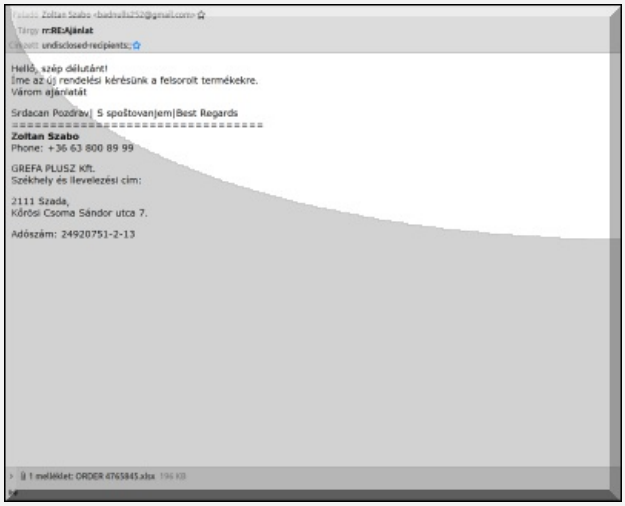
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

Bárhol bármikor bárkivel

2022. április 12. 10:08 - Csizmazia Darab István [Rambo]

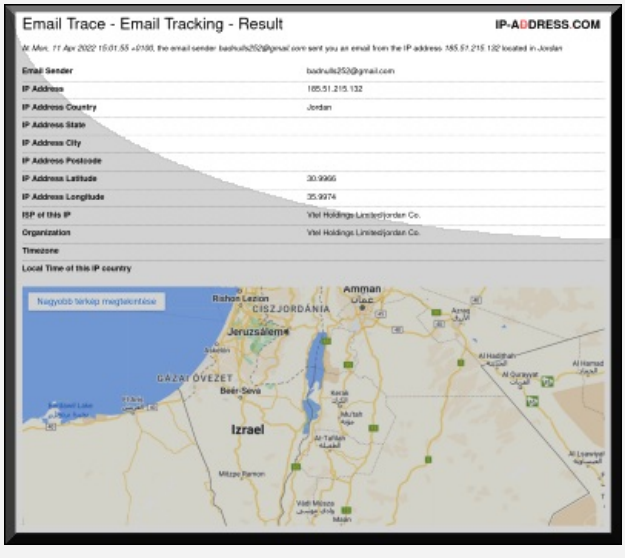
Amikor hamis számlát, csomagértesítőt, banki üzenetet, vagy amikor a Magyar Kormány nevében kapunk olyan levelet, amelyben állítólag 150 ezer forint kártérítéshez juthatunk a koronavírus miatt, **minden ilyen átveréskor visszaélnek valamilyen cég, szervezet nevével. Sajnos bárkinek, még a kisebb vállalkozások nevét is felhasználhatják hasonló célra gátlástalan csalók.**

Vagy mégsem rovatunkban már több tucatnyi példát hoztunk, amikor mégsem a FedEx értesít csomagról, amikor mégsem a koronavirus.gov.hu a valódi feladója a levélnek, amikor nincsenek ingyen Rolling Stones jegyek, vagy amikor látszólag Telekom számla érkezik, de csalók várják a túloldalon, hogy bedőljünk a próbálkozásuknak.

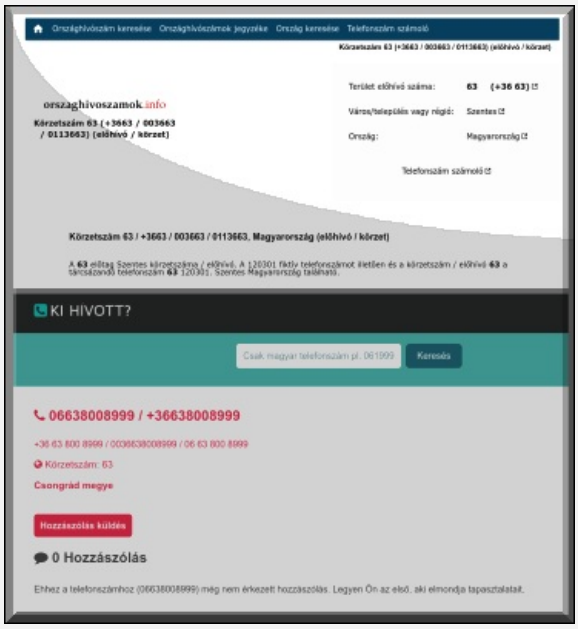


Ezúttal egy olyan kéretlen e-mail érkezett, amely **egy legitim magyarországi cég nevében válaszol egy olyan ajánlatra, amit nem is kértünk.**

A gyanús jelek itt is hosszú tömött sorban mutatkoznak meg: feladó egy olyan állítólagos "Zoltan Szabo", aki még **a magyar ékezetekkel is hadilábon áll, de a levél feladója valójában badnulls252 KUKAC gmail PONT com.**

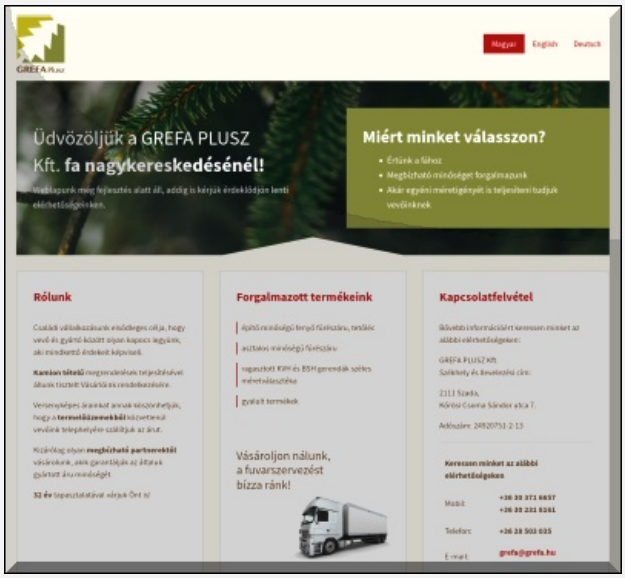


Rövid e-mail trace kapirgálás után az is látható a fejlécből, hogy Jordániából jött az e-mail, ami egy valódi magyar vállalkozásnál elég unortodox megoldásnak számítana.

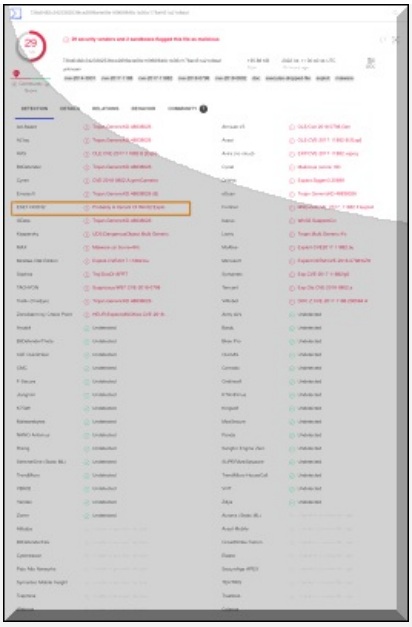


Az állítólagos válasz az ajánlatkérésünkre (Tárgy: "rr:RE:Ajánlat") **a magyar nyelvvel sem boldogul túl jól** - például: "*Íme az új rendelési kérésünk a felsorolt termékekre*." Akkor most mi van, ki kért és mit, nagyon nem világos ezek alapján.

És persze az igénytelenség fokozható, **nem mi kaptuk a levelet, hogy kedves mélyen tisztelt Gipsz Jakab, hanem csak a sima körleveles "*undisclosed-recipients:;*" a címzett.**

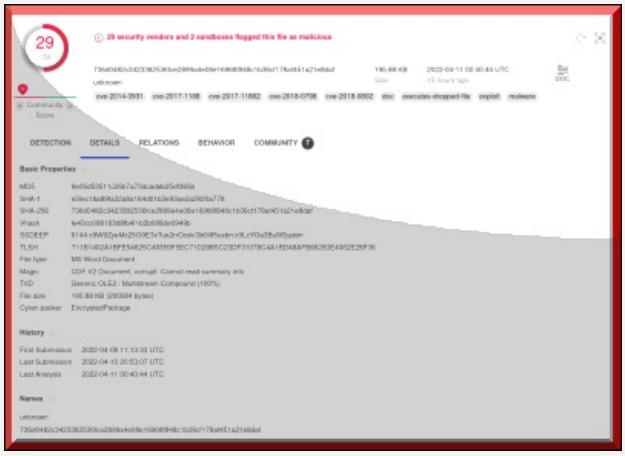


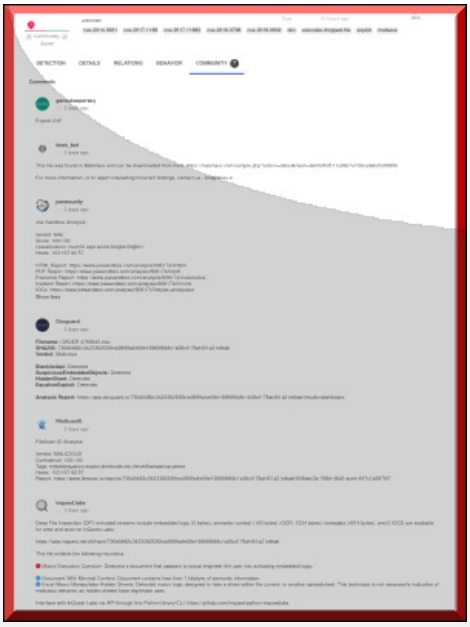
Rákeresve **a cég igazi honlapjára jól látszik, hogy az e-mailben jelzett telefonszám és a cég valódi telefonos elérhetősége nem egyezik**, a csalók mindenesetre egy 63-as körzetes szentesi számot tettek a levélbe.



Ennyi már bőven elég lenne ahhoz, hogy olvasatlanul direkt-véletlenül rákönyököljünk a Delete gombra, ha már a spamszűrő nem fogta meg. Ám a levélnek van csatolmánya is, amit ha feltöltünk a VirusTotal oldalára, akkor a vizsgálati eredmény bizony nem igazán mutat szép képet. **A látszólag "ORDER 4765845.xlsx" nevű állomány valójában egy olyan 196 KB méretű MS Word dokumentum, amely egy sebezhetőséget kihasználó kódot (exploit) tartalmaz.**

Ha valaki a mellékletre rákattint és a szükséges hibajavítások hiányoznak a gépéről, akkor megfertőződik a rendszere.





A [CVE-2017-11822-ről azt lehet tudni, hogy a jó 5 éves magas besorolású sérülékenységet](#) kihasználó preparált kóddal át lehet venni a teljes vezérlést a fertőzött gép felett.

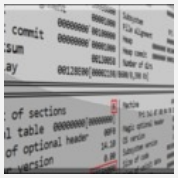
Vagyis azon a támadó ezután tetszőleges programokat telepíthet, bármilyen adatok megtekinthet, módosíthat vagy törölhet, de akár teljes felhasználói jogokkal rendelkező új fiókokat is létrehozhat.

Mi segíthet még a fenti intő jelek biztonságtudatos felismerésén felül? A naprakész vírusvédelmen természetesen felkoppan a kártékony kód, emellett szintén nem szabad elhanyagolni a hibajavító frissítő foltok telepítéseit sem.

És sajnos jól látható, nem kell ahhoz egy nagy multinak, vagy a WHO-nak, NAV-nak lenni ahhoz, hogy valakinek a nevével csalárd módon visszaéljenek a rosszindulatú bűnözők. Az érintett céget mindenesetre már értesítettük a jelen csalási kísérletről.

[Szólj hozzá!](#)
Címkék: [dokumentum](#) [csalás](#) [átverés](#) [visszaélés](#) [exploit](#) [sebezhetőség](#) [sérülékenység](#) [kártevőterjesztés](#) [offic](#)

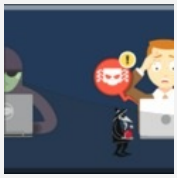
Ajánlott bejegyzések:


[Lenovo laptopok a pácban](#)


[Log4j sebezhetőség - hogyan tovább?](#)


[Exchange szerverek tűz alatt](#)


[Egyedül nem megy](#)


[Üzleti e-mail hamisítás](#)

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

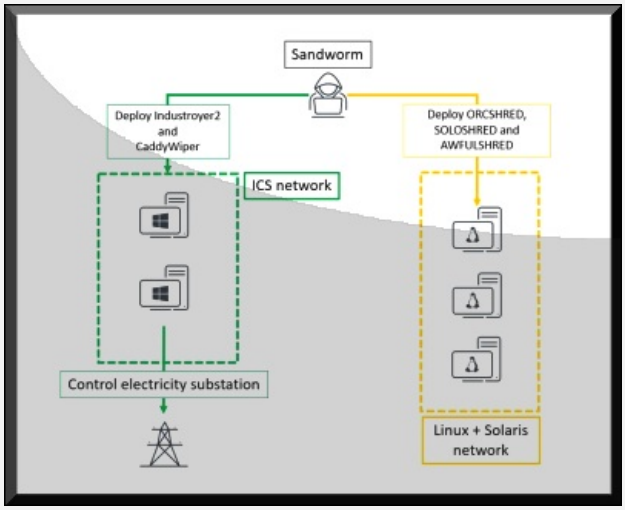
Támadás 1,2,3 - Industroyer újratöltve

2022. április 14. 16:37 - Csizmazia Darab István [Rambo]

Az öt évvel ezelőtti ukrán energetikai vállalatok elleni támadás volt az első, amely a Sandworm Industroyer kártevőjét használta. **Ennek segítségével 24 órás áramkimaradások alakultak ki 2016. év végén.**

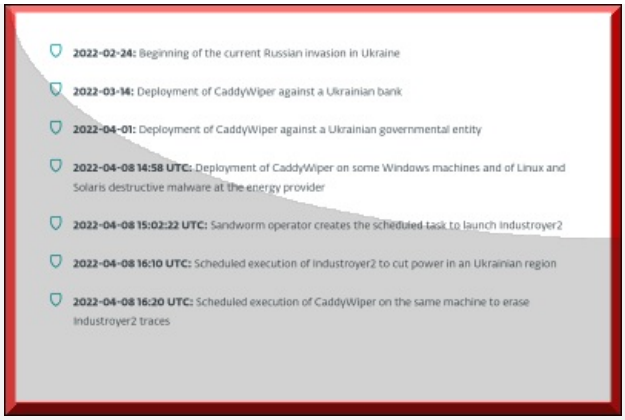
A Sandworm néven ismert hírhedt orosz hackerek 2016. karácsonya előtt egy héttel vettek célba egy elektromos átviteli állomást Kijevtől északra, és az automatizált támadókód segítségével közvetlenül kapcsolatba léptek az állomás megszakítóival, és **lekapcsolták az áramot.**

Az Industroyer ugyanis azért nagyon veszélyes, mert képes közvetlenül irányítani a villamosenergia-alállomás kapcsolóit és megszakítóit. Ehhez olyan ipari kommunikációs protokollokat használ, amelyeket más ellátó infrastruktúrákban, szállításirányítási rendszerekben és más kritikus hálózatokban (víz, gáz) is világszerte alkalmaznak.



Az ipari vezérlőrendszerek eme rosszindulatú programját azóta nem látták - **egészen mostanáig. Oroszország brutális ukrajnai inváziója közepette a Sandworm a jelek szerint újra elővette régi trükkjeit.**

Kedden az ukrán Computer Emergency Response Team (CERT-UA) és a szlovák ESET kiberbiztonsági cég figyelmeztetést adott ki, hogy **a Sandworm hackercsoport - amelyről megerősítették, hogy az orosz GRU katonai hírszerző ügynökség 74455-ös egysége - nagyfeszültségű elektromos alállomásokat vett célba Ukrajnában**.

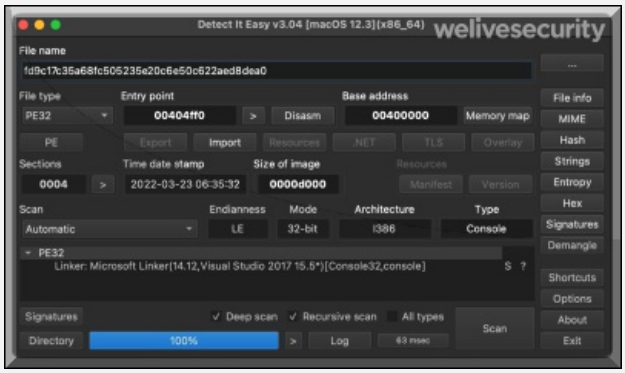


Az energiaszolgáltató hálózatában a támadók a CaddyWiper adattörlő kártevő új verzióját telepítették. Emlékezetes, hogy **a CaddyWiper első verzióját az ESET kutatói fedezték fel Ukrajnában 2022. márciusában, amikor azt egy ottani bank hálózatába telepítették**. Egy másik adattörlő kártevő, a HermeticWiper pedig 2022. februárjában próbálkozott szabotázsakció révén leállítani Ukrajnában működő infrastruktúrákat.

Az adattörlő kártevők alapvető célja szemben a zsarolóvírusokkal nem az adatlopás és az anyagi haszonszerzés, hanem a rombolás, azaz véglegesen megsemmisíteni az adatokat, működésképtelenné tenni az informatikai rendszereket.

A mostani akcióban megcélzott energiavállalat hálózatán további **rosszindulatú adattörlő programokat is találtak, amelyek célzottan Linuxot és a Solaris-t futtató rendszerekhez készültek**. Az ukrajnai CERT azt állítja, hogy **a támadást még idejében észlelték, és azt sikeresen leállították, mielőtt tényleges áramszünetet válthattak volna ki a támadók, illetve az adattörlést is el tudták kerülni.**

A Sandworm incidens feltárása több bizonyítékot szolgáltat arra vonatkozóan, hogy Oroszország Ukrajna elleni inváziójáért az ország hálózatait és kritikus infrastruktúráját érő kibertámadások új hulláma kísérte, bár ezúttal csak vegyes sikerrel.



Az incidens elhárításában **az ESET és a Microsoft szakemberei közösen akadályozták meg az ukrán villamosenergetikai hálózat leállítását.** Jean-Ian Boutin, az ESET kiberszakértője szerint igen jelentős ez a fenyegetés, hiszen az derült ki, hogy **ez a bűnözői csoport azóta is használja és karbantartja ezt az az ipari vezérlőrendszerek elleni támadó eszközt.**

Ez pedig lehetővé teszik számukra, hogy ténylegesen beleavatkozzanak más országok olyan kritikus infrastruktúráiba, mint az elektromosság és az energiaellátás. **Emiatt az ilyen típusú támadások határozott fenyegetést jelentenek a világ összes többi országaira is.**

1 komment
Címkék: microsoft orosz ukrajna hacker eset kártevő cert szabotázs villamosenergia wiper sandworm welivesecurity.com adattörlés industroyer

Ajánlott bejegyzések:

[A kibertér is hadszíntér]

[Jótékonysági csalások Ukrajna nevében]

[10 alaplépés a biztonsághoz]

[Oroszország lett a fő kibercélpont]

[Hogyan ne jussunk 10-ről 11-re?]

Kommentek:

gigabursch 2022.04.14. 19:58:51

Ennek a hírnek kapcsán felmerült bennem, hogy az elfoglalt atomerőművek vajon milyen tanulofazist hozhattak be. Hmmmm...

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Hogyan ne jussunk 10-ről 11-re?

2022. április 19. 13:15 - Csizmazia Darab István [Rambo]

A Windows10 utódként megjelenő immár csak 64 bites rendszereket támogató 11-es változatú Microsoft operációs rendszer már itt kopogtat az ajtónkon, és **ez a felfokozott érdeklődés egyúttal persze remek lehetőséget ad a kártevőterjesztőknek is.**

A frissítési szándékot kihasználva olyan átverések jelentek meg, amelyek kéretlen levelek linkjeivel vagy felbukkanó ablakokban olyan nemhivatalos és **kártékony weboldalakra vezetnek, amelyek aztán komoly veszteséget okoznak a gyanútlan felhasználóknak.**

Ezek a hamis frissítési lehetőségek olyan rejtett kártevőket telepítenek, amelyek ellopják a böngészési adatokat, a vágólap (Clipboard) tartalmát, és a kriptovaluta tárcákban őrzött pénzt is.

Chrome	opera	Chromex86	Chromium	BraveBrowser
amigo	Vivaldi	orbitum	MailRuatom	Kometa
Torch	Comodo	Slimjet	360Browser	Maxthon3
Sputnik	Nichrome	CocCocBrowser	uCozMediauran	Chromodo
edgeChromium	ChromePlus	iridium	7Star	CentBrowser
elementsBrowser	Sleipnir6	Citrio	liebaoBrowser	Coowon
epicPrivacyBrowser	ComodoDragon	K-Meleon	Chedot	QiPSurf

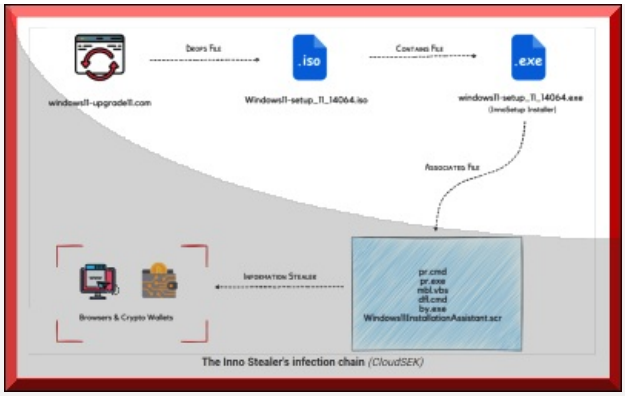
Web browsers targeted by Inno Stealer (CloudSEK)

wallet-backup\\	wallet-unenc-backup\\	mbhd.wallet
\wa\corewallet	WalletWasabi	\wa\WalletWasabi
owallet	\wa\owallet	\wa\exodus.wallet
\wa\YoroiWallet	\wa\RoninWallet	\wa\CloverWallet
\wa\MathWallet	\wa\UWallet	\wa\NiftyWallet
\wa\GeroWallet	\wa\GuardaWallet	\wa\GuildWallet
\wa\LeafWallet	\wa\SaturnWallet	\wa\EqualWallet
\wa\BraveWallet	wallet.dat	electrum_data\\wallets\\
Electrum-DASH\\wallets\\	\.wallet.aes	\\Coinomi\\wallets\\
\\wallet-backup\\	\\wallet-unenc-backup\\	\\mbhd\.wallet
WalletWasabi\\Client\\Wallets\\	\\WalletBackup\\	\\BackupWallet\\
Bisq\\btc_mainnet\\wallet\\	\\wallet\.dat	\\atomex\.wallet
\.tezwallet	\\default_wallet	\\backups\\wallet\\

Crypto wallets targeted by Inno Stealer (CloudSEK)

A kártékony weboldalak a Microsoft logójával és nevével visszaélve olyan "Letöltés most" linket tartalmaznak, amely az Inno Stealer nevű kártevőt telepíti az áldozat számítógépére. **A CloudSEK biztonsági szakemberei visszafejtették a rosszindulatú programot, és a részletes technikai elemezés eredményét is megosztották** nyilvánosan a BleepingComputer weboldalán.

Számos böngészőkliens - **Opera, Edge, Chrome, Chromium, Vivaldi - és sokféle kriptovaluta tárca érintett a támadásban. Az ellopott adatokat egy PowerShell szkript segítségével továbbítja** a távoli támadók szerverére.



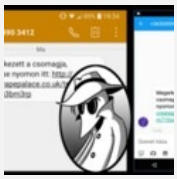
The Inno Stealer's infection chain *(CloudSEK)*

Ha biztonságosan akarunk frissíteni, akkor erre vannak precíz hivatalos útmutatók, ám ha mégsem ezt az utat választjuk, például a gépünk esetleg nem felel meg az elvárt paramétereknek, akkor erre is van biztonságosabb manuális lehetőség.

Nyilván ez utóbbi esetben egy hivatalos www.microsoft kezdetű oldalról fogjuk letölteni az eredeti ISO fájlt, nem pedig egy pár hónapja Reykjavíkban regisztrált ismeretlen weboldalról a kártevővel fertőzött preparált kártékony változatot.

2 komment
Címkék: microsoft windows frissítés telepítés upgrade trójai kártevő biztonságtudatosság kriptovaluta

Ajánlott bejegyzések:


Csak a felszín más: csomagküldés helyett frissítés


10 alaplépés a biztonsághoz


Igazgató-e vagy?


Támadás 1,2,3 - Industroyer újratöltve


Xenomorph kalandjai GooglePlay országban

Kommentek:

Head Honcho 2022.04.20. 05:24:07

Elképesztő, mi mindenre kiterjed a kártevőterkesztők figyelme...

Válasz erre

Head Honcho 2022.04.20. 05:25:11

*kártevőterjesztők

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.

VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Colonial Pipeline után a mindennapi kenyerünk

2022. április 22. 08:25 - Csizmazia Darab István [Rambo]

A kritikus infrastruktúrák és ellátási láncok elleni támadások tucatjai kerültek már eddig is a címlapokra. **2021. májusában egy célzott ransomware incidens az USA keleti partján hetekig tartó üzemanyaghiányt és hatalmas anyagi veszteséget okozott. Pár hónap múlva a Kaseya távmenedzsment szolgáltató elleni hasonló támadás világszerte 800 és 1500 közötti vállalkozást bénított meg, köztük a svéd Coop-szupermarketnek kellett bezárnia, mert a pénztárgépeik nem működtek.**

Számos értékelés, gazdasági előrejelzés látott napvilágot az orosz-ukrán háború hatásairól, de abban mindegyik elemzés hasonló, hogy extrém mértékben növekszik az infláció, és hosszútávon az élelmiszer-ellátás az egész világon nehéz kihívások előtt áll.

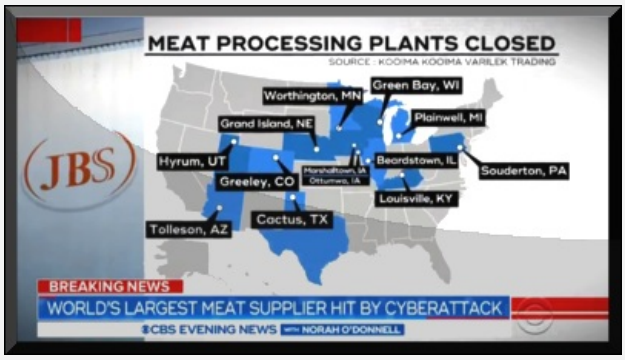
Részben a kieső mezőgazdasági területek miatt, részben a szankciók hatása révén, illetve nyilván az elszálló olaj- és üzemanyagár az áruszállításban és a mezőgazdasági gépek használatában is komoly gondokat okoz.

Ebben a helyzetben figyelmeztette most az FBI az élelmiszer- és mezőgazdasági vállalatokat, hogy készüljenek fel arra, hogy ebben az amúgy is kritikus helyzetben nagyobb valószínűséggel lehetnek célzott ransomware támadások célpontjai. A mezőgazdaság nagyon kiszolgáltatott lehet az ilyen incidenseknek, és **ezek hatása nem csak lokálisan egy adott országban, vagy régióban jelentkezhet, hanem világméretű negatív következményei is lehetnek.**

A korábbi csővezeték-hálózatos támadás kapcsán pedig jól látszott, hogy még az elképesztő nagyságú (1.27 Mrd HUF) váltságdíj kifizetése sem oldotta meg azonnal a problémát, **részint mert a kapott helyreállítókulcs olyan rettentő lassú volt, hogy mégis inkább mentésekből történt a munka, másrészt pedig a hetekig elhúzódó hiányt, válságot még így fizetve sem tudták elkerülni.**

Emlékezetes, hogy a múltbeli incidensek között volt már hasonló, igaz ezt csak távolról láttuk, ez volt tavaly júniusi JBS elleni támadás. A JBS a világ egyik legnagyobb húsfeldolgozó vállalata, amelynek székhelye ugyan Brazíliában található, ám világszerte több, mint 250 000 alkalmazottja van, és komoly szereplőnek számít a piacon.

A JBS USA részlege elismerte, hogy célzott és szervezett kibertámadás áldozatai lettek, és **emiatt vészhelyzet, káosz, áruhiány alakult ki az észak-amerikai és ausztrál informatikai rendszerek kiesése révén. A kifizetett váltságdíj itt elképesztően magad volt, 11 millió dollárnyi (akkori átváltási áron körülbelül 3.17 milliárd forintnak megfelelő) kriptovaluta.**



Most, amikor a kibertérben jelenleg két jól körülhatárolható érdek mentén zajlik a támadások jelentős része, az élelmiszer ellátás biztonságát veszélyeztető gyaníthatóan orosz eredetű kibertámadások valós kockázatnak számítanak, és **a szereplőknek nagyon komolyan kell venniük ezt a fenyegetettséget.**

Szólj hozzá!
Címkék: fenyegetés fbi mezőgazdaság figyelmeztetés élelmiszeripar ellátás váltságdíj ransomware zsarolóvírus

Ajánlott bejegyzések:


Emelkedő ransomware károk

Közeleg a tél, érzékeny ponton támadnak a zsarolóbandák


Apa kezdődik!


Váltságdíjat kínálnak a váltságdíjszedő bandáért

Ha szólsz a rendőröknek, akkor véged!

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Antivírusblog
245 követő

Oldal követése Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

- RSS 2.0
- bejegyzések, kommentek
- Atom

bejegyzések, kommentek

accountz

Belépés
Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

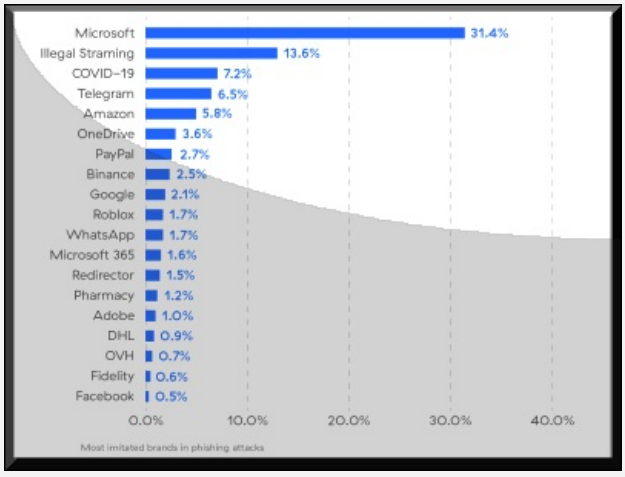
Az adathalászatot megölni nem kell félnetek

2022. április 26. 10:03 - Csizmazia Darab István [Rambo]

Az egyik leggyakoribb és egyben a legsikeresebb eredményességi rátát felmutató támadási módszer a kibertérben. Befigyelt persze közben **két év covidos bezártság, homeoffice, karantén viszonyok, és talán ennek is lett az eredménye, hogy a kereskedelem területén több mint 400%-kal nőtt az adathalász támadások száma.**

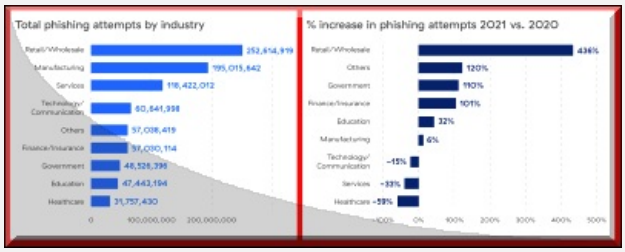
A tavalyi évet elemző, ezt a területet felölelő biztonsági jelentésben a Zscaler részletes statisztikákat mutat a világszerte bekövetkezett változásokról, és **ezalatt a változások alatt sűrűbb támadási gyakoriságot, nagyobb kockázatot kell érteni.**

Adataik alapján az adathalász támadások száma globálisan mintegy 29%-kal nőtt, összesen 873 millió ilyen incidenst regisztráltak az elmúlt esztendőben.



A szektorokat tekintve **a kis- és nagykereskedelem volt a legcélzottabb iparág, itt az elmúlt 12 hónapban több, mint 400%-kal nőtt az adathalász támadások száma.**

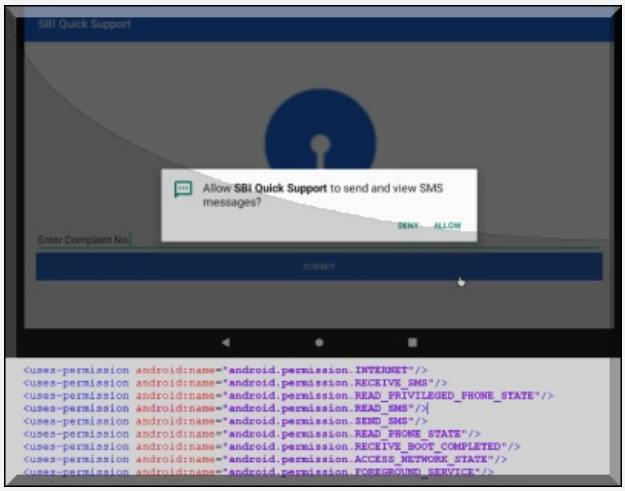
Ha célországokra fókuszálunk, akkor az Egyesült Államokat, Szingapúrt, Németországot, Hollandiát és az Egyesült Királyságot célozták meg leggyakrabban ezek az adathalász csalások.



Kiemelhetjük, hogy bizonyos alakulóban lévő módszerek esetén, mint például **az egyre gyakoribb SMS adathalászat, itt a számok lényegesen gyorsabban növekednek**, mint más hagyományos klasszikus technikák esetén. A smishing az adathalász támadások olyan formája, amely a szöveges SMS üzenetküldést kihasználja ki a mobileszközökön.

Bár a smishing már 2006. óta létezik, mégis az elmúlt években drámai módon megnőtt a gyakorisága: 2020-

hoz képest 300%-os növekedést, 2021 első hat hónapjához képest pedig 700%-os növekedést mutat az utolsó negyedévben észlelt esetek száma, és ennek az is lehet az oka, hogy a végfelhasználók jelentős része a gyanús e-mailekkel szemben már óvatosabb.



A támadók gyakran magukat cégvezetőnek álcázva kísérlik meg átverni az áldozataikat, illetve az is bevált módszerük, hogy megbízható márkák, bankok vagy mobiltelefon-szolgáltatók, hivatalos szervezetek nevével visszaélve történik.

Ha az áldozatok nem vigyáznak, és rákattintanak a kéretlen üzenetben kapott adathalász linkekre, akkor gyorsan kompromittálhatják a név-jelszó párosukat, ha nem tartozik ehhez valamilyen kétfaktoros vagy többfaktoros autentikációs védelmi réteg.

És hogy a helyzet még bonyolultabb legyen, a növekvő adathalász tevékenység egyik oka, hogy a zsarolóvírusoknál ismert RaaS, vagyis Ransomware as a Service módozathoz hasonlóan itt is létezik a bűnözőket közvetlenül kiszolgáló adathalászat mint szolgáltatás.

Ennek segítségével előre elkészített támadási eszközökkel könnyítik meg a bűnözők az adathalász támadásokkal foglalkozók dolgát, a szolgáltatásaikat pedig egyszerűen a sötét weben értékesítik, ezzel minimális technikai ismerettel is biztosítani tudják ennek a csalási formának a piacát.

Az adathalászat mindig is az egyik leggyakoribb kiberfenyegetés volt arra, hogy különböző módszerekkel a személyes adatainkat ellophassák. **Egy átlagos méretű szervezet naponta több tucat adathalász e-mailt kap**, emiatt a munkavállalók biztonságtudatossági képzése elengedhetetlen.

Legyünk gyanakvóak a kéretlen üzenetekkel, figyeljünk fel a gyanús feladóra, ismerjük fel a szabvány általános körlevél formában terjesztett tömeges SPAM leveleket, vegyük észre a hamisított hiperhivatkozások és webhelyek címében a hibákat, elütéseket, ellenőrizzük a mellékelt linket még kattintás előtt az egérkurzor segítségével (hover), tűnjön fel azonnal a hibás, helytelen helyesírás és nyelvhasználat, és sose kattintsunk gyanús mellékletekre, még akkor sem, ha sürgetni vagy fenyegetni próbálnak bennünket. És persze a naprakész vírusvédelem és a rendszerünk hibajavításokkal történő rendszeres frissítése is lényeges segítség mindehhez.

1 komment
Címkék: statisztika védelem megelőzés phishing adathalászat smishing

Ajánlott bejegyzések:


Mai szavunk pedig: biztonsági fásultság


Nagy pénz, nagy foci, nagy átverések


10 gyakori IT biztonsági hiba


Iskolák a kiberbűnözők célkeresztjében

Sikeres brandek az adathalászatban

Kommentek:

Who111 2022.04.27. 21:04:24

Ahogy a Fonográf megénekelte: "Kár, hogy a magyar nyelvet nem érti senki..." Elképesztő magyartalanságok vannak ezekben az adathalász levelekben, rendkívül könnyű felismerni. Főleg a ragozás okoz nehézséget. :-) Ez jelent nekünk némi védelmet, már aki nem teljesen sík hülye. Pont tegnap kaptam egy elképesztő akcióról levelet, ahol egy ismert fúrógép márka volt 99%-al leakciózva. Már a fénykép is Photoshoppolt volt, ráadásul valami ilyesmi ár volt: 78.00Ft Namármost: Már régen nincs fillér, így árat Magyarországon nem írnak ki. Másrészt pontot használ tizedes vesszőnek. Angolszász környezetben fel sem merül, hogy valahol más szeparátort használnak. Másrészt egy kérdőívre vitt a link, holott azonnali kedvezményt írtak. (Konkrétan, bemész a boltba és megveszed ennyiért.) Szóval járjunk nyitott szemmel, ne vakítson el a könnyű haszonszerzés lehetősége. Egyik bolt, bank, stb. sem Róbert bácsi. Akkor írnak neked, ha hasznot remélnek belőled. Nem neked akarnak jót, hanem maguknak.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus

- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

- RSS 2.0
  bejegyzések, kommentek
- Atom
  bejegyzések, kommentek

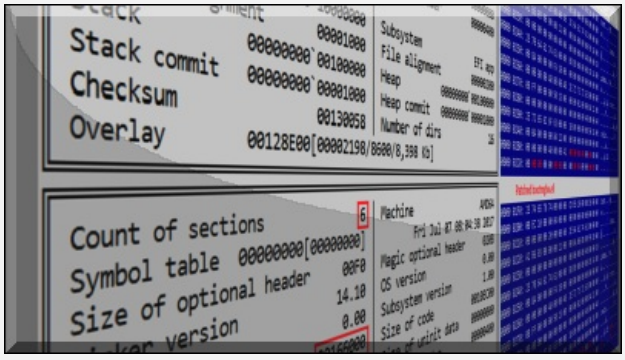
accountz

- Belépés
- Regisztráció

Lenovo laptopok a pácban

2022. április 29. 09:29 - Csizmazia Darab István [Rambo]

Az ESET kutatói **három olyan sebezhetőséget fedeztek fel és elemeztek ki, amelyek a Lenovo gyártmányú laptopokat érintik.** Az ESET 2021. októberében az összes felfedezett sérülékenységről tájékoztatta a Lenovót. Az érintett eszközök **listája több, mint száz különböző laptopmodellt tartalmaz, amelyek világszerte több millió felhasználót érintenek.**

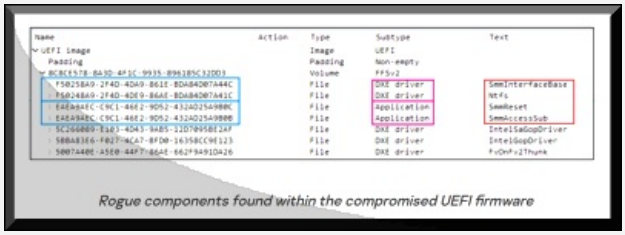


E sebezhetőségek lehetővé tehetik a támadók számára, hogy olyan UEFI-t (a BIOS utódja) támadó kódokat telepíthessenek, mint például az SPI Flash memóriát érintő LoJax, vagy a most felfedezett, UEFI bootkithez kapcsolódó ESPecter kártevő.

Az UEFI-kártevők rendkívül alattomosak és veszélyesek lehetnek. Ezek még **a rendszerindítási folyamat elején kezdenek működni, mielőtt átadnák a vezérlést az operációs rendszernek, ami azt jelenti, hogy ezáltal számos, operációs rendszer szinten futó biztonsági intézkedést meg tudnak kerülni**. - mondta a sebezhetőségeket felfedező Martin Smolár, az ESET kutatója. Felfedezésük azt mutatja, hogy **bizonyos esetekben az UEFI-kártevők észrevétlen telepítése sajnos nem is olyan nehézkes, mint azt korábban tapasztalták, és az elmúlt években felfedezett új UEFI fenyegetések növekvő száma arra utal, hogy a támadók is kihasználják ezt.**

Az elmúlt években felfedezett valamennyi korábbi UEFI-fenyegetésnek - LoJax, a MosaicRegressor, a MoonBounce, ESPecter, a FinSpy kártevő - meg kellett kerülnie vagy ki kellett kapcsolnia a biztonsági mechanizmusokat ahhoz, hogy telepíteni és végrehajtani lehessen.

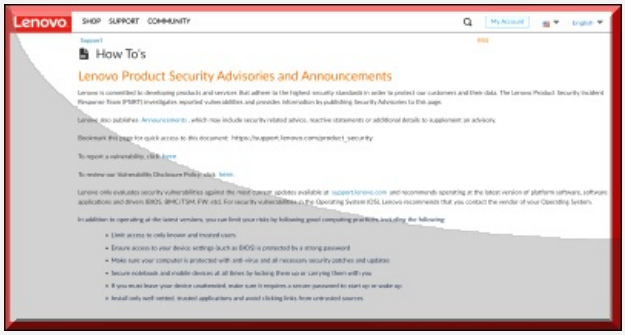
Az UEFI rendszerindítási és működtetési szolgáltatásai biztosítják azokat az alapvető funkciókat és adatstruktúrákat, amelyek szükségesek az illesztőprogramok (driver) és alkalmazások működése érdekében, például a különféle protokollok telepítéséhez, a már meglévő protokollok kereséséhez, vagy a memóriafelosztáshoz. **A biztonsági rések közül az első kettő - CVE-2021-3971, CVE-2021-3972 - az UEFI firmware meghajtókat érinti, amelyeket eredetileg csak a Lenovo notebookok gyártási folyamata során használtak volna.**



Sajnos tévedésből a gyártási BIOS-ba is bekerültek, anélkül, hogy megfelelően deaktiválták volna őket. Ráadásul a vizsgálat során az ESET felfedezett egy harmadik sebezhetőséget is: az SMM memória (System Management Mode) sérülését.

Ez a biztonsági rés illetéktelen olvasást/írást tesz lehetővé az SMRAM-ban, ami rosszindulatú kód futtatásához vezethet

SMM jogosultságok birtokában, illetve lehetővé teszi kártékony modulok SPI flash-re való telepítését.



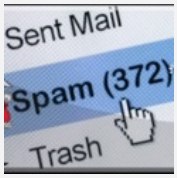
A különböző firmware-implementációk nagy száma és ezek összetettsége miatt sajnos valószínűleg a jövőben is felbukkanhatnak hasonló, jelenleg még felfedezetlen sérülékenységek. **Az ESET kutatói határozottan azt tanácsolják a Lenovo laptopok tulajdonosainak, hogy mindenképpen nézzék át az érintett eszközök listáját, és a gyártó utasításait követve haladéktalanul frissítsék firmware-üket.**

További részletes technikai információkat az ESET angol nyelvű WeLiveSecurity blogján olvashatunk.

Szólj hozzá!
Címkék: frissítés lenovo firmware bios exploit sebezhetőség sérülékenység uefi welivesecurity.com

Ajánlott bejegyzések:


Exchange szerverek tűz alatt



Bárhol bármikor bárkivel


Log4j sebezhetőség - hogyan tovább?


Egyedül nem megy


Okoskodás: okos-e az okosjáték?

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

A mesterséges intelligencia véd, a felhasználó megkerüli

2022. május 03. 09:43 - Csizmazia Darab István [Rambo]

A SecWorld 2022. konferencián jártunk, ahol a szakemberek azt a témát járták körül, vajon mennyire lehet automatizálni a védelmet, eljött-e, eljöhet-e a "robotzsaruk" ideje?

Az előadások között arra kerestük a választ, mennyire gyenge láncszem ebben a humán faktor. A mesterséges intelligencia véd, a felhasználó megkerüli - ez volt a cím, és ebben szó esett arról is, hogy alig egy évvel a nulla kilométer kőnek nyilvánított 1986-os Brain vírus megjelenése után 1987-ben megalakult az ESET vírusvédelmi cég, amely **régóta alkalmazza az adatgyűjtést, osztályozást, 1995-től pedig tudatosan támaszkodik gépi tanulásra, a védelemben és a víruslaborban pedig többféle AI is dolgozik.**

A prezentációban a jelenlegi helyzet támadói és védelmi oldalról való bemutatása **után a felhasználói hibákról, a célzott felhasználói támadásokról hangzottak el friss adatok**.

Itt a mesterséges intelligencia mind a két oldal eszköztárában szerepel, ami egyre fejlettebb megoldásokkal rukkol elő.

Például támadói oldalon 2019-ben DeepVoice hangszintetizálás segítségével ismeretlen elkövetők egy brit energetikai cég német igazgatója hangján, az ő nevében felhívták a brit igazgatót, és egy azonnali, de bizalmas 220 ezer euró összegű pénzátutalást kért egy magyar alvállalkozó magyar bankszámlájára, amiről utólag derült csak ki, hogy csalás volt.

Az előadás videófelvételét ezen a linken lehet megnézni, illetve az ezt követő, ezt a tematikát feszegető kerekasztal beszélgetést is vissza lehet nézni, **ahol pedig jobbára a védekezés, a megelőzés volt a fókuszban.**

1 komment
Címkék: prezentáció előadás konferencia eset 2022 itbiztonság secworld

Ajánlott bejegyzések:

Kis- és középvállalkozások adatvédelmi incidensei

Böngészés - kockázatok és mellékhatások


Durva ransomware statisztikai adatok


Kiberbiztonsági útikalauz diákoknak


Hazugságok: messzebbre és gyorsabban

Kommentek:

steery 2022.05.05. 20:44:10

A felhasználók jó okkal kerülik meg a különféle védelmeket és beépített akadályokat. Mert használni akarják a rendszert, nem állandóan falakba ütközni, kudarcot vallani és semmit el nem érni. Senki sem szeret állandóan azzal szembesülni, hogy ezt se tehetem, azt se tehetem, így se tehetem, úgy se tehetem, ezért nem tehetem, azért nem tehetem. Ezért a védelmet úgy kellene fejleszteni, hogy azonnali megoldásokat nyújtson a felhasználó számára a szándékozni kívánt dolog megtételéhez. Nem elég azt mondani az embernek, hogy ezt ne tedd. Azt is meg kell mondani, ha meg akarod tenni, így meg úgy tedd és akkor oké lesz.
Újabban sok honlap tartalma nem jelenik meg. Helyette felvillant egy üzenetet, hogy a felhasználó reklám blokkolót használ, kapcsolja ki, ha látni akarja a tartalmat. Ezt a hozzáállást kell mindenhol máshol is alkalmazni. És akkor a felhasználó vagy lemond a tartalomról vagy lesz olyan hülye, hogy kikapcsolja a reklámblokkolót, aztán meg anyázik a következmények miatt. Hacsak... fel nem ajánlja automatikusan a böngésző a blokkolás kijátszó megoldást: ami során úgy tesz, mintha megjelenítené a reklámokat, de valójában mégse.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.

VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Rossz gondolatok a könyvtárban

2022. május 05. 10:30 - Csizmazia Darab István [Rambo]

Kibertámadásokkal sajnos már eddig is tele volt a padlás, aztán jött a Covid miatti homeoffice, ez is tovább emelte a számukat, és persze az orosz-ukrán háború is felpörgette a kritikus infrastruktúrák, és minden más ellen is a ransomware és egyéb támadásokat. Megsemmisíteni egy könyvtári gyűjteményt azonban inkább a Fahrenheit 451 című filmre hajazó primitív barbárságnak tűnik.

Ha csak felsorolni akarnánk, mi mindent támadtak meg már zsarolóvírussal, kilométeres lenne a lista vége, **ügyvédi irodától rendőrőrsig, kórházaktól kőolajvezetékig, húsfeldolgozó multicégtől utazási irodáig, egyetemektől önkormányzatokig** volt már itt minden a 2013-as CryptoLockertől évek óta ránk záduló ransomware áradatban.

"*Van, akit nem várnak, csak érkezik*" - ahogy az LGT anno énekelte, és ez szó szerint sajnos tényleg így volt.

Megküzdési stratégiában is széles palettán mozogtak az áldozatok: az incidens szimpla letagadása, a nyíltan vagy titokban való váltságdíj fizetés, a hatóságok azonnali értesítése, saját nevükben való alkudozás a pénzen vagy éppen külön felkért ransomware szakértő specialista tusztárgyalása, fizetés után kapott használhatatlan helyreállítókulccsal való szenvedés, kifejezetten ransomware elleni biztosítás megkötése, és sajnos sokkal ritkábban idejekorán elkészített kiberbiztonsági akcióterv, védekezés, rendszeres mentés, erőforrások megelőzésre fordítása.

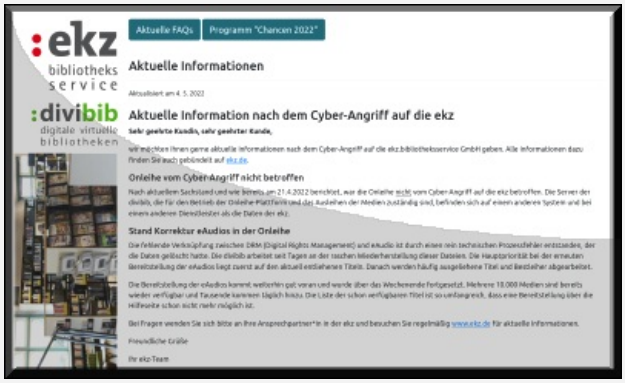
A mostani eset a németországi EKZ könyvtár szolgáltatót érte, akiket a Lockbit ransomware csoport célzott meg még április 18-án. Az e-audió streaming és letöltési szolgáltatásokat biztosító könyvtár a támadás után

komoly leállásokkal küzdött. A vállalat számos ország felé tette lehetővé, hogy a felhasználók több, mint 200 könyvtárból kölcsönözzenek ki online e-könyveket, elektronikus újságokat, magazinokat, hangoskönyveket és zenéket.

A felhasználók döntő többségben Németországban voltak, de emellett Ausztriában, Svájcban, Olaszországban, Liechtensteinben, Dániában, Belgiumban és Franciaországban is biztosították az elérést. Az Onleihe alkalmazást számos európai egyetem és a nemzetközi Goethe-Intézet is használja, és Németországban ez az összes e-könyv fogyasztásának mintegy 40% -át teszi ki.

A cég május 4-i közleményében arról tájékoztatta az érdeklődőket, hogy a kibertámadás az audió és videó anyagokat érinti leginkább, ezért most minden erőforrást arra fordítanak, hogy ezeket a hangoskönyveket és filmeket saját biztonsági mentéseikből helyreállítsák. A cég büntetőfeljelentést tett a helyi németországi bűnüldöző szerveknél, és saját informatikai csapata mellett külső szakértőket is megbízott a helyreállítási munkákra, ez jelenleg is folyamatban van.

A kimaradás az ekz.de, ekz.at, ekz.fr, valamint a divibib.com weboldalakra volt hatással, május 3-án kedden pedig Németországban és Ausztriában már újraindították a megrendelések kiszállítását. **Azt viszont nem tudták megmondani, hogy személyes adatokat is elloptak-e a támadás során.**



A BleepingComputer értesülései szerint **valószínűleg megtagadták a váltságdíj kifizetését a LockBit 2.0 csapatnak, ugyanis mivel a támadás egy doxinggal kombinált**, azaz nem fizetés esetén az ellopott adatok kiszivárogtatásával fenyegető akció volt, így időközben a lopott bizalmas adatok 100%-a felkerült már a ransomware banda Tor adatszivárgási webhelyére.

Szólj hozzá!
Címkék: németország könyvtár váltságdíj ransomware e-könyv zsarolóvírus doxing lockbit

Ajánlott bejegyzések:

LockBit vs. olasz adóhivatal


Nem szállunk rendelkezésére II.


Baljós árnyak: fekete macska Karintiában

Fordulat ransomware fronton


Kórházprogram

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

Apa kezdődik!

2022. május 09. 11:02 - Csizmazia Darab István [Rambo]

Sajnálatos módon csak kevesen olvasták azt a közelmúltban megjelent posztunkat, amelyben arról számoltunk be, hogy az FBI célzott ransomware támadási kockázatra figyelmeztette **az élelmiszeripari- és mezőgazdasági vállalatokat.**

A mezőgazdaság már a Covid helyzet alatt is nehéz helyzetben volt, **ám a mostani hibrid háborús környezet tovább növelte azokat a fenyegetéseket, amelyek az élelmiszeripari ellátási láncokra összpontosítva kiemelten képesek lehetnek világméretű károkat okozni.**

Sajnos nem is kellett sokat várni, hogy az első ilyen "fecske" megjelenjen, **a múlt héten az amerikai AGCO Corp mezőgazdasági berendezéseket gyártó vállalat jelentett be, hogy egy ransomware támadás miatt néhány termelési létesítményük működése leállt, illetve a mostani tavaszi kritikus ültetési szezonban a traktorok értékesítése is elakadt.**

Az AGCO a John Deere cég egyik versenytársa, és beszámolójuk szerint május 5-én csütörtök óta több napos leállásra kényszerültek. **A mezőgazdasági cégeknek a tavasz az év legfontosabb és legforgalmasabb időszaka, így érzékeny veszteséget kénytelenek elszenvedni.**

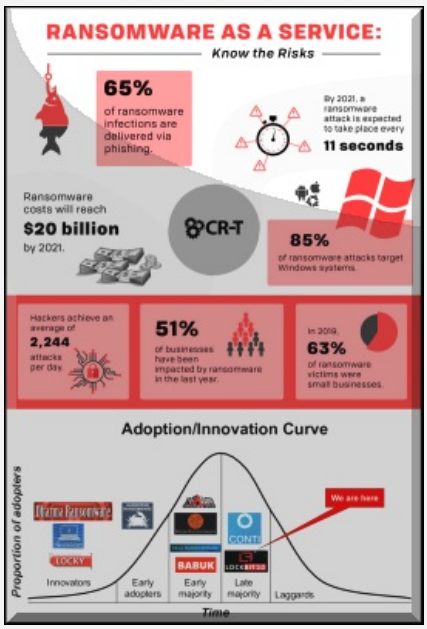
A Duluthban székelő AGCO nem hozta nyilvánosságra a támadásban érintett üzemegységeik pontos nevét, **illetve azt sem, hogy az incidens során elloptak-e bármilyen bizalmas adatot. A támadás a weboldalukat is érinti, így a tájékozódás mellett az alkatrészek rendelése is leállt, szünetel.**

Az AGCO 1810 észak-amerikai márkakereskedéssel rendelkezik, illetve további 42 országban van jelen világszerte. A vállalat állítása szerint már vizsgálják a támadás mértékét, ami a teljes nemzetközi rendszerüket érinti és közben gőzerővel dolgoznak a rendszerek helyreállításán.

Ennél bővebb, és részletesebb tájékoztatást nem lehetett megtudni az esetről, **így azt sem, pontosan melyik ransomware kártevő okozta a kiberincidenst, mennyi váltságdíjat kértek, fizettek-e támadóknak, illetve béreltek-e fel külsős kiberbiztonsági tanácsadókat. Az AGCO részvényei a támadás hírének bejelentésére 6%-kal csökkentek a múlt hétvégére.**

Zárásképp egy érdekes és pontos elemzést ajánlunk azoknak, akik kíváncsiak a ransomware elleni harc jelenlegi állására.

Ebben az összefoglalóban kitérnek arra, hogy **a kritikus infrastruktúrák egyre nagyobb veszélyben vannak, illetve hogy a RaaS, azaz a Ransomware as a Service kártékony elterjedése miképpen fokozta a vállalati rendszerek kitettségét.**



A darkneten bérelhető szolgáltatásban **nem csak magát a ransomware-t kínálják, hanem ma már olyan extrákat nyújtanak a bérlőknek, mint a 7/24 supportot, adott nyelvi támogatást, direkt telefonhívási lehetőséget, a váltságdíj-tárgyalások kezelésében jártas szakembereket, pénzmosási szolgáltatásokat, tárhelyet a megszerzett adatok tárolásához, sőt nem fizetés esetén felületeket ezek közzétételére, valamint igen részletes recepteket, tanácsokat, forgatókönyveket a hatékony zsarolásokhoz.**

3 komment
Címkék: usa traktor mezőgazdaság támadás váltságdíj ransomware zsarolóvírus agco

Ajánlott bejegyzések:


Nem csitulnak a kórházak elleni támadások

Közeleg a tél, érzékeny ponton támadnak a zsarolóbandák


Colonial Pipeline után a mindennapi kenyerünk


Felkészül: USA kritikus infrastruktúra

Tesz-e Oroszország a ransomware ellen?

Kommentek:

Bandibacsi34 2022.05.10. 01:24:09

Nem tudom miért kellene sajnálni ezeket a p.. fejeket, hogy akik az emberi munkát ki akarják váltani távirányítású traktorokkal. Remélem a dilerek máskor is le fognak rájuk csapni!!

Válasz erre

Bandibacsi34 2022.05.10. 01:32:19

pcforum.hu/hirek/24620/oriasi-szivasba-futottak-bele-az-oroszok-az-ukrajnabol-ellopott-okostraktorokkal
Vagy mégsem?

Válasz erre

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2022.05.10. 07:50:16

@Bandibacsi34: Köszi szépen a linket, érdekes volt, különösen a kommentek...

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.

VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

A nevem halász, adathalász

2022. május 12. 11:32 - Csizmazia Darab István [Rambo]

Nem volt eseménytelen a kibertér az Egyesült Királyságban, **friss statisztikák szerint 2.7 millió online csalást indítottak útnak a tavalyi esztendőben, ebben pedig híres emberek illetve ismert cégek nevével való visszaélés, Covid-19 világjárványhoz kapcsolódó zsarolási kísérlet**, és még számos egyéb trükk szerepelt.

Az egyik eset azonban bővebb említést is megérdemel, ebben **az ismeretlen elkövető magát az Egyesült Királyság fő kiberbiztonsági ügynökség (NCSC) vezetőjének, Lindy Cameronnak kiadva próbált meg személyes adatokat ellopni. A csaló egy e-mailt küldött, amelyben azt állította, hogy a szervezetük épp az imént akadályozta meg az áldozat 5 millió fontjának ellopását, és hogy az állítólagos összeget visszaküldje, ehhez részletes személyes adatokat kért.**

Annyi azért érdekes, hogy hány olyan visszaküldő lehetett, akinél valóban reális esélye lehetett volna egy ekkora összegű lopásnak, és hány olyan, aki csak kapzsiságból, nyereségvágyból bepróbálkozott az ingyen pénzért, mint a 409-es csalások közül a nigériai örökös típusú átverésnél.

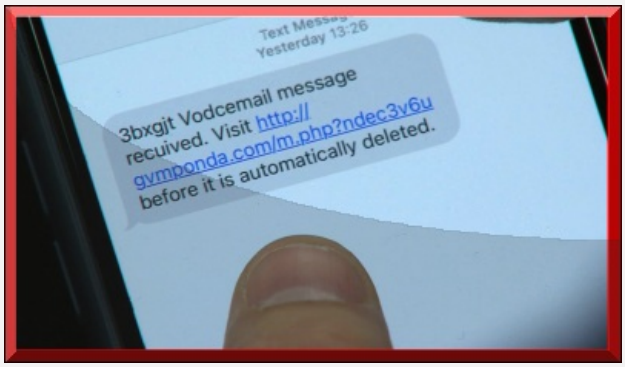
Az adathalászat mindenesetre világszerte egyre növekvő méretben jelentkező kockázat, **az NCSC szerint tavaly több, mint 1400 adathalász kísérletet regisztráltak, amelyek a brit közegészségügyi szolgálathoz kapcsolódtak.**

Az egészségüggyel kapcsolatos ilyen csalások száma az előző, **2020-as évhez képes megtízszereződtek**. Az okok között természetesen a homeoffice, és a világjárvány miatti lakossági aggodalmak is komoly szerepet játszhattak.

Érdemes még a statisztikai adatokból azt is megemlíteni, hogy az NCSC **többek között 1.2 millió olyan domaint is blokkolt, amelyek az Android Flubot kártékony programmal kapcsolatosak.** Emlékezetes, hogy ez a kártevő játszott főszerepet a tavaly márciusi FedEx csomagküldő szolgálat nevével visszaélő csalássorozatban, ennek az átverésnek Magyarországon is számos áldozata volt.

Fő jellemzője, hogy többnyire **szöveges üzeneteken keresztül terjed, azt állítva, hogy sikertelen volt az első**

kézbesítési próbálkozás, és ahhoz, hogy nyomonkövethessük az állítólagos küldeményünket, kattintani kell a mellékelt linkre, telepíteni egy ismeretlen alkalmazást, annak minden használati engedélyt megadni, illetve a személyes adatainkat is bekérték.



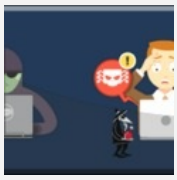
Védekezés, megelőzés témában már sokszor körbejártuk az adathalászattal kapcsolatos legfontosabb ajánlott teendőket, ezért ehhez most csak belinkeljük az egyik ilyen friss összefoglalónkat.

Szólj hozzá!

Ajánlott bejegyzések:


Összeomlás


Kellemes Karácsonyi Ünnepeket!


Üzleti e-mail hamisítás


VPN appok Androidra vagy mégsem?


Emelkedő ransomware károk

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

10 gyakori ok, amiért bedőlünk a csalásoknak

2022. május 17. 13:04 - Csizmazia Darab István [Rambo]

Már régóta vártunk már egy ilyen hangzatos címre, mint például "5 dolog amit nem tudtál erről és erről", vagy "a 3 legfontosabb akármi, amitől megváltozik az életünk". De a tétet ennek ellenére tartjuk, és **valóban tíz olyan kockázati tényezőt fogunk felsorolni, ami miatt gyakran beleeshetünk a különféle csalók csapdájába.**

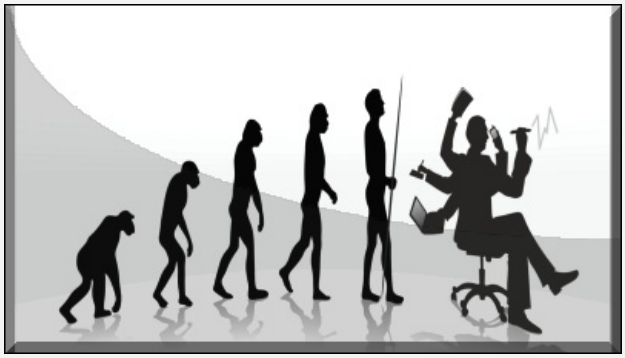
2008-ban volt egy fordulópont, amikor **az USA-ban a számítógépes bűncselekmények több pénzt hoztak a szervezett bűnözők konyhájára, mint a drogkereskedelem, ez akkor 105 milliárd dollár volt.**

Azt láthatjuk, hogy azóta teljes mértékben átalakult a bűnözés, és **a hagyományos, nagyobb lebukási rátával rendelkező klasszikus bűncselekményeket ha nem is felváltották, de jól kiegészítették**, és lekörözték a nagyobb anonimitással kecsegtető online számítógépes csalások, átverések. Vegyük akkor végig az említett tízes listát!

01. A csalások egymásra épülően fejlődnek

A mém szót Richard Dawkins-i értelemben véve minden megtörtént támadási incidens már egy lehetséges gyakorlati példaként lebeg a többi bűnöző előtt, akik ráadásul nem csak leleményesek, hanem **tanulnak is saját és más bandák módszereiből és elkövetett hibákból, emiatt a csalások még fejlettebbek, profibbak és egyre inkább testre szabottak.**

A kipróbált technikák egyre kifinomultabban bukkannak fel, gondoljunk például a FedEx-es csomagküldős átverésre, amely több országban is tarolt. **A jó hír, hogy mindeközben nekünk is kumulatívan egymásra épülhet a tapasztalatunk, biztonságtudatosságunk, és idővel egyre hatékonyabban ismerhetjük fel a gyanús jeleket.**



02. Sok értékes információ morzsát hagyunk a digitális lábnyomainkban

Már többször is volt szó arról, hogy nem érdemes túlzottan kitárulkozónak lenni az interneten, hiszen nem tudhatjuk,

hogy a fotó, az információ végül kikhez kerül, így **például semmiképpen nem érdemes előre bejelenteni a közösségi oldalon, hogy most indulunk nyaralni.**

Mivel a tömeges spam kampányok mellett egyre gyakrabban fordulnak elő tudatos és célzott támadások, ahol **az ellopott, kiszivárgott vagy publikusan hozzáférhető adatokból hatásosabban lehet megtéveszteni az áldozatokat.**

03. A csalók leleményesek és ügyesek a megtévesztésben
Sok szélhámos ténykedik a neten, gondoljunk például a profi csalókra a társkereső oldalakon. **Hamis profilokat használnak, kész forgatókönyvük van az áldozatok behálózására, bevált formulákkal kerülik el a felelősségrevonást, és igen hatékonyan tudják kiválasztani azokat a sérülékeny célpontokat, akiket aztán anyagilag megkárosítanak**. Igen jó adalék ehhez a témához a Tinder Svindler film, illetve az Örökösnő álarca című Netflix sorozat.

Jó iránytű lehet itt, ha valami túl szép ahhoz, hogy igaz legyen, akkor ott rendszerint valami hátsó szándék van a háttérben.

04. A csalók sürgetnek, mi pedig sietünk, kapkodunk
Amikor az intő jeleket szedjük csokorba, akkor a rossz helyesírás mellett a sürgetés is általában megjelenik. A sürgetés lehet olyan, hogy épp most törik fel a bankszámlánkat, és ha nem akarjuk, hogy ellopják a pénzt, zárolják a számlát, kattintsunk azonnal. Lehet olyan, hogy egy fantasztikusan hangzó kedvezmény csak korlátozott ideig áll rendelkezésre és limitált darabszámban, így ha valaki "jól akar járni", sietnie kell.

A sietség pedig kéz a kézben jár az óvatlansággal, figyelmetlenséggel, és gyakoribb a hibázás az áldozatok részéről. Érdemes megállni és gondolkodni, mielőtt bármilyen döntést hoznánk, kattintanánk, bizalmas személyes adatokat megadnánk.

05. Mindenki szereti az ingyen ebédet
Szeretünk jól járni, ingyen iPhone, örökélet, ingyen sör, vagy hogy a közelmúltból egy konkrét csalást is említsünk, a Covid időszak alatt a magyar kormány nevében érkezett egy olyan üzenet, amely a WHO-ra hivatkozva állítólagos pénzügyi segítséget ajánlott fel. **A részletes személyes és banki adatok kitöltése után 150 ezer forintot ígértek, amihez a Bitcoines pénztárcánk számát is meg kellett volna adni, ám átverés volt az egész.**

Ha kivételes hozammal kecsegtető befektetést ajánlanak, Bill Gates állítólag felajánlja a vagyonát, és hasonló remek

ajánlat érkezik, érdemes résen lenni, és gyanakodni.

06. Az emberek többsége igyekszik megfelelni, engedelmeskedni felfelé
Az emberek hajlamosak bízni azokban, akik hatalmi pozícióban vannak. A csalók gyakran olyan embereknek adják ki magukat, akik valamilyen szakértelemmel rendelkeznek, vagy hatalmuk révén függhetünk tőlük: kormányzati ügyintéző, adósságbehajtással foglalkozó ügyvéd, egy adott vállalati vezető vagy egy adott terület szakértője.

Kelet-Európában ehhez még a poroszos iskolarendszer is hozzájárult, ahol a felnőttnek, a tanárnak, a főnöknek, az eggyel több csillaggal rendelkezőnek automatikusan igaza van - erre kondicionáltak bennünket. **Ám ha ezekkel a tekintély személyek, vagy szervezetek nevével internetes csalásokban visszaélnek, akkor jogosan gyanakodjunk, és legyünk figyelmesek.**

07. Jó időzítéssel elvonják a figyelmünket
Ha az év végi hajrá közepette érkezik egy hamis villanyszámla, akkor lehet, **hogy hajlamosak leszünk gyorsan letudni, és egy közepes összeg esetén gondolkodás nélkül gyorsan átutalni**.

Hasonló gondolat mentén figyelhető meg például céges támadásoknál, hogy **gyakran ezt ünnepi, vagy hétvégi időszakra időzítik a bűnözők arra számítva, hogy csökkentett létszám, kevesebb figyelem, vagy a hétvégi munkaszünet** alatt több idejük és lehetőségük lesz a támadásra, és csak később veszik észre a behatolást, feltörést, adatlopást.

08. A csalók saját járt utukat járják, flowban vannak
A támadók gyakran előnyben vannak, míg az védelem csak reagál az eseményekre. Ha érkezik egy váratlan üzenet, vagy telefonhívás, nekünk ez egy nem várt és zavaró tényező, a bűnöző pedig a saját útját járja, bőséges tapasztalattal odakoncentrálva igyekszik becserkészni az áldozatát.

Fel kell készülni a váratlan helyzetekre, ahol nem hagyjuk magunkat sürgetni, átgondoljuk, vagy megbeszéljük a környezetünkkel a helyzetet, és egészséges gyanakvással élni a különféle szituációkban, teljes figyelmünkkel "jelen lenni", és ezután döntést hozni, vagy reagálni ha kell, illetve akár egyszerűen megszakítani a kommunikációt, ha gyanakszunk.

09. Szeretünk segíteni
A segítségkéréseket tartalmazó üzenetek sajnálatot, empátiát keltenek bennünk, például ha személyes tragédiákról vagy vészhelyzetekről hallunk. **Számos hamis jótékonysági adománygyűjtésről számoltunk be itt a blogon is**, például az orosz-ukrán háború kapcsán, vagy egy régebbi esetet is említhetünk, ahol gyermekrákra és babaszívműtétekre hivatkozva jelentek meg visszataszító csalások a Facebookon.

A csalók rájöttek, hogy az emberek szeretik hasznosnak érezni magukat, például a székükből fel sem kelve egy telefonhívással segíteni az árvízkárosultakon, **ám érdemes mindig figyelmesnek lenni, és alaposan ellenőrizni a felhívások hitelességét.**

10. A csalók figyelmesek, ráhangolódnak az áldozatukra
Ez nem igazi empátia, inkább a **szociopata viselkedés jellemzője, hogy igyekszenek elnyerni az áldozat bizalmát, figyelmet színlelnek a céljuk érdekében, csalikat használnak, erőltetett kedvességet vetnek be**. A romantikus csalás tipikus terepe ennek, ahol **elsősorban idősebb és jól szituált egyedülálló nőket vesznek célba**, és a magányosságot, hiszékenységet kihasználva sablon átverésekkel operálnak.

Ezekben külföldön szolgáló megözvegyült katona, fúrótornyon dolgozó jól kereső olajmunkás jelentkezik, aki váratlanul

bajba kerülve átmeneti kölcsönt kér a frissen megismert online párjától. **Érdemes megismerni a tipikus csalásokat, átveréseket, és ezzel a tudással felvértezve máris jobb helyzetbe kerülhetünk.**

És végül jöhet egy kis tanulság. Minden tipikus példa végén igyekeztünk a megelőzés, védekezés módjait is felvázolni, de ezen felül is említést érdemel **az erős és egyedi jelszavak használata, olyan naprakész vírusvédelem alkalmazása, amely az adathalászat kiszűrésére is alkalmas.**

Ha pedig becsapnak bennünket, vagy kárt okoznak nekünk, **haladéktalanul tegyünk feljelentést, lépjünk azonnal kapcsolatba a bankunkkal. Online fiókjaink kompromittálódása esetén pedig késedelem nélkül kövessük az ilyenkor szükséges megteendő lépéseket.**

Szólj hozzá!
Címkék: csalás tippek átverés megelőzés tanácsok védekezés adathalászat adatlopás welivesecurity.com

Ajánlott bejegyzések:

Nagy pénz, nagy foci, nagy átverések

Mit tehetünk a kriptovaluta csalások ellen?

Ha eljön a személyiségtolvaj


Ingyenes Omikron teszt vagy mégsem?


Fiatal vagy? Ezekre az online csalásokra figyelj!

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

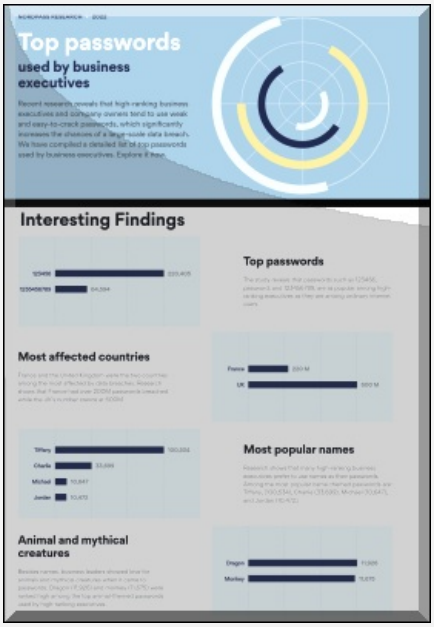
C mint CEO, P mint password

2022. május 23. 13:38 - Csizmazia Darab István [Rambo]

Évről évre tördeljük a kezünket látva a szokásos összesítéseket a felhasználói jelszavakról. Miközben 11.8 milliárd ellopott, kiszivárgott jelszót jegyeznek a haveibeenpwned.com weboldalon, **a használt jelszavak minősége rendre marad a pocsék szinten. Vajon a cégek vezetői jobbak ebben?**

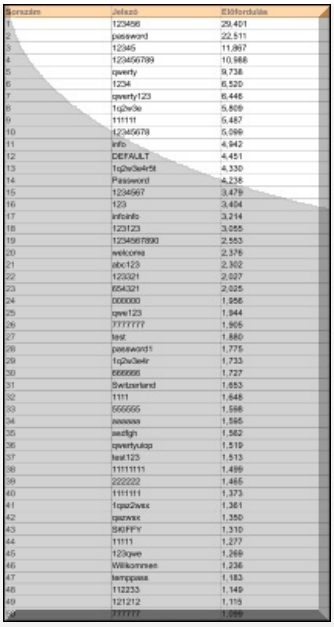
Itt a NordPass friss nemzetközi statisztikája a jelszavakról, ebből a forrásból már többször is szemléztük az aktuális helyzetet, legutóbb éppen tavaly év elején.

Akkor még egy jópofa ábra is illusztrálta, hogy **a számok, nevek, születési dátumok, qwerty típusú karakterláncok, sport, és egyéb univerzumok mekkora halmazt birtokolnak a primitív jelszavakból**.



A mostani friss beszámoló arról tanúskodik, hogy **a világ magas beosztású üzleti vezetőinek és cégtulajdonosoknak a hozzáállása sem különb** sokkal, ugyanis a legutóbbi felmérés kifejezetten rájuk fókuszált. A jelszavak listáját a kiberbiztonsági incidensek kutatására szakosodott független kutatókkal együttműködve úgy állították össze, hogy az eredményeket négy külön csoportba sorolták.

Ezek a vállalati vezérigazgatók, a különféle C-szintű (COO Chief Operating Officer, CFO Chief Financial Officer, stb.) vezetők, a cégtulajdonosok, valamint a vállalati menedzsmentbe tartozó vezetői tagok jelszavait vizsgálták. **A kutatás számos iparágra, így többek közt ipari, technológiai, egészségügyi, vendéglátóipari, média, marketing, ingatlanos, tanácsadói, nonprofit, építőipari területre is kiterjedt.**



Sorszám	Jelszó	Előfordulás
1	123456	29.401
2	password	22.511
3	12345	11.997
4	123456789	10.968
5	qwerty	9.738
6	1234	6.520
7	qwerty123	6.448
8	1q2w3e	5.809
9	111111	5.487
10	12345678	5.096
11	info	4.942
12	DEFAULT	4.451
13	1q2w3e4r5t	4.330
14	Password	4.238
15	1234567	3.479
16	123	3.404
17	infoinfo	3.214
18	123123	3.055
19	1234567890	2.553
20	welcome	2.376
21	abc123	2.302
22	123321	2.027
23	654321	2.025
24	000000	1.956
25	qwe123	1.944
26	7777777	1.906
27	test	1.880
28	password1	1.775
29	1q2w3e4r	1.733
30	666666	1.727
31	Switzerland	1.653
32	1111	1.648
33	555555	1.596
34	aaaaaa	1.585
35	asdfgh	1.582
36	qwertyuiop	1.519
37	test123	1.513
38	11111111	1.499
39	222222	1.465
40	1111111	1.373
41	1qaz2wsx	1.361
42	qazwsx	1.350
43	SKIFFY	1.310
44	11111	1.277
45	123qwe	1.269
46	Willkommen	1.236
47	kenpawa	1.183
48	112233	1.149
49	121212	1.115
50	777777	1.099

És akkor tadaaaam!, jöjjenek a megállapítások. Érdekes módon **az "123456" ebben a klubban is roppant népszerűnek bizonyult. Feltörhető és fel is tört jelszavak tekintetében a felmérés szerint Franciaország és az Egyesült Királyság jár az élmezőnyben.**

A keresztnevek közül a "Tiffany" nyerte a versenyt, **az állatok közül a sárkány és a majom feszült egymásnak döntetlen közeli állapotban. Mellékeljük a 290 millió tétel elemzéséből keletkezett top 50-es listát is, benne sok-sok régi "ismerőssel".**

A doxing sajnos egy nagyon elterjedt jelenség ma már a ransomware világában, de úgy tűnik, **sok cégvezető alulbecsüli azt a veszélyt, ha a fiókjának vagy belépésének feltörésével ellophatják, publikálhatják a bizalmas anyagait.**

Sokféleképpen eshet el egy jelszó a csatában: túl egyszerű, több helyen használják, begépelik egy adathalász oldalon, nyitott wifin lépnek be vele, kukkolnak a hátunk mögül, SSL nélküli weboldalt használnak, és még estig folytatható a sor.

A megelőzéshez, védekezéshez sem lehet kizárólag egyetlen dolgot említeni, itt is több teendőnk van.

Erős, egyedi jelszó használata, jelszószéf (jelszó menedzser program) alkalmazása, átfogó és rendszeres kötelező kiberbiztonsági képzések tartása segíthet. És vajon ez utóbbira elmenne-e a főnök?

Ám a fő kérdés még így is nyitva marad: **vajon mer-e bárki szólni egy főnöknek, egy politikusnak, egy államfőnek, ha az nyilvánvalóan hibázik vagy mulaszt security téren?**

Erre viszont már nem ad választ nekünk a fenti NordPass tanulmány.

Szólj hozzá!
Címkék: statisztika jelszó primitív password gyenge vezetők főnökök nordpass feltörhető

Ajánlott bejegyzések:

Még gyengébb a jelszavad

Nem életrevalók


Gyenge, gyengébb, leggyengébb


Az elveszett jelszavak fosztogatói

Kis- és középvállalkozások adatvédelmi incidensei

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.

VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Nem szállunk rendelkezésére

2022. május 25. 19:16 - Csizmazia Darab István [Rambo]

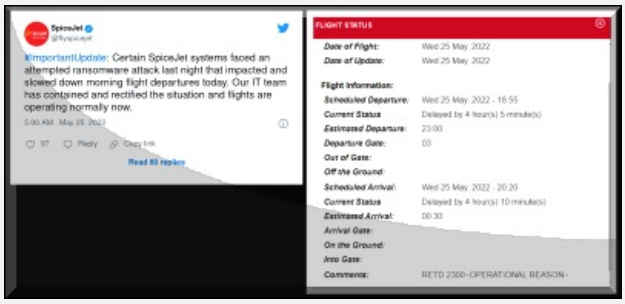
A ransomware nem válogat, illetve nagyon is jól céloz be kritikus területeket. Ha már repülés, akkor emlékezhetünk arra a korábbi esetre, mikor **2018-ban egy brit repülőtéren egy menetrenden kívül érkező ransomware fertőzés miatt filctollal irkálták tacepaókra a repülési menetrendet.**

Ebben az előző történetben, melyben a Bristol Airport zsarolóvírusos támadást szenvedett el, emiatt bő két napon keresztül nem működtek a kijelzők a reptéren. **Az utasok ezalatt kézzel írt papír listákról olvashatták le az aktuális járat információkat.**

Akkor az angliai reptér szóvivője akkor megerősítette, hogy **nem fizettek váltságdíjat a támadóknak, és személyes adatok, illetve kritikus biztonsági rendszerek nem kerültek veszélybe** az incidens miatt, és járatokat sem kellett törölni emiatt.

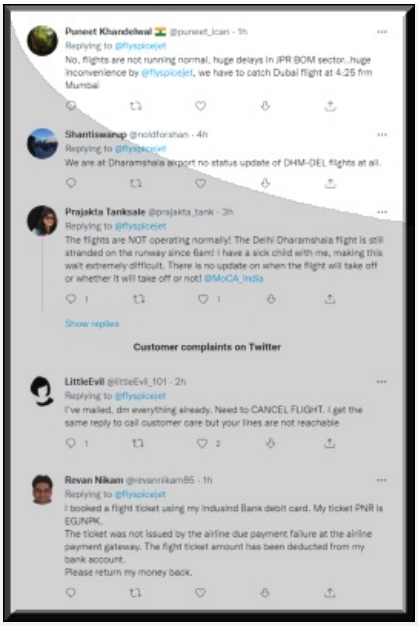
A mostani friss esetnél a **SpiceJet nevű indiai fapados légitársaság ma arról tájékoztatta ügyfeleit, hogy egy ransomware támadási kísérlet miatt leállások voltak a rendszerükben, és ez késéseket okozott a tegnap esti és ma reggeli járatok indulásában**. A SpiceJet India második legnagyobb légitársasága, 102 repülővel 60 célállomást szolgál ki, 14 ezer alkalmazottat foglalkoztat.

A vállalat közösségi oldalon megjelentetett hivatalos közleménye szerint az informatikai csapatnak végül sikerült megakadályoznia a támadást, és **állításuk szerint minden visszatért a normál működési állapotba.**



A Twitter és Facebook oldalakon azonban az látszott, hogy a bejelentés ellenére az ügyfelek azóta is problémákra panaszkodnak, így a járatkésések nem szűntek meg, a telefonon keresztüli ügyfélszolgálat nem érhető el, és a számítógépes foglalási rendszer továbbra sem működik.

A Bleeping Computer ma reggeli beszámolója arról írt, hogy bár a hivatalos SpiceJet weboldal látszólag él és **be is töltődik, a mögötte lévő rendszer azonban továbbra sem működőképes. A késések nyilván a leállások miatt halmozódtak, és 2-5 órás csúszásokra számíthattak az utasok.**



A SpiceJet szóvivői közleményben elismerte a ransomware támadás tényét, ami **főképp éjszaki járatok törlésével, illetve további járatok késésével járt.**

Megerősítették, hogy az informatikai csapat a tegnapi napon felismerte és igyekezett orvosolni a helyzetet, de **a helyreállítás érdekében külsős biztonsági szakértőkkel is együtt dolgoznak, valamint a kiberbűnözéssel foglalkozó hatóságok is bekapcsolódtak a nyomozásba.** Követelt vagy kifizett váltságdíjról, illetve adatlopásról viszont nincs hír, ezek a részletek egyelőre nem ismertek.

Szólj hozzá!
Címkék: india késés menetrend reptér repülőtér repülőgép ransomware zsarolóvírus spicejet

Ajánlott bejegyzések:


Összeomlás


Nem csitulnak a kórházak elleni támadások


Emelkedő ransomware károk

Venus ransomware támadja az egészségügyet


Nem szállunk rendelkezésére II.

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás

Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

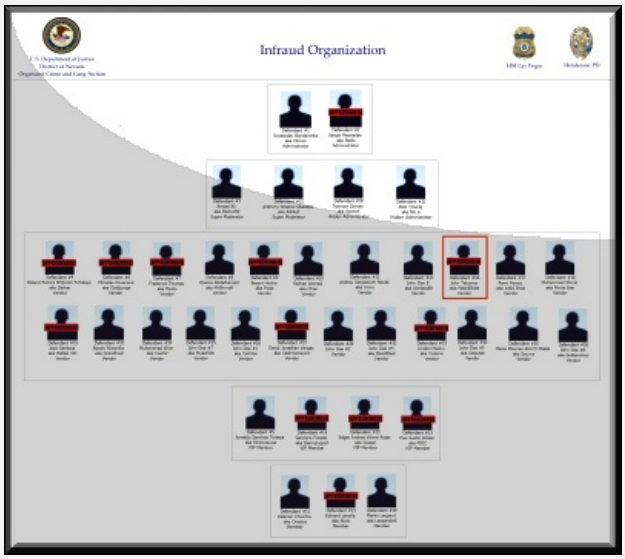
Összeomlott kártyavár

2022. május 30. 11:03 - Csizmazia Darab István [Rambo]

Igen hosszú ideig volt aktív az **Infraud Organization bűnszervezet, amelynek fő tevékenysége pénzügyi információk, ellopott személyazonosító adatok, bankkártyák, hamis dokumentumok, személyazonosításra alkalmas adatok, bankszámla- és hitelszámla-információk** megszerzése és értékesítése volt.

Igazi nemzetközi bűnszervezetként működtek, a 2018-ban az őrizetbe vett vádlottak között orosz és amerikai állampolgár is volt, a 13 letartóztatás pedig részint az Egyesült Államokban, és további hat másik országban zajlott: Ausztrália, az Egyesült Királyság, Franciaország, Olaszország, Koszovó és Szerbia voltak érintve ebben.

Bár ez az őrizetbevétel fontos lépésnek számított, ám fontos megjegyezni, hogy a teljes szervezeti taglétszám jóval tízezer feletti volt. **A mellékelt szervezeti felépítés alapján látható, hogy még a vezérkarból is sok csuklóról hiányzik egyelőre a bilincs. Az "In God We Trust"-hoz hasonlóan az "In Fraud We Trust" szlogen alatt hirdették több mint 7 éven át alvilági szolgáltatásaikat.**

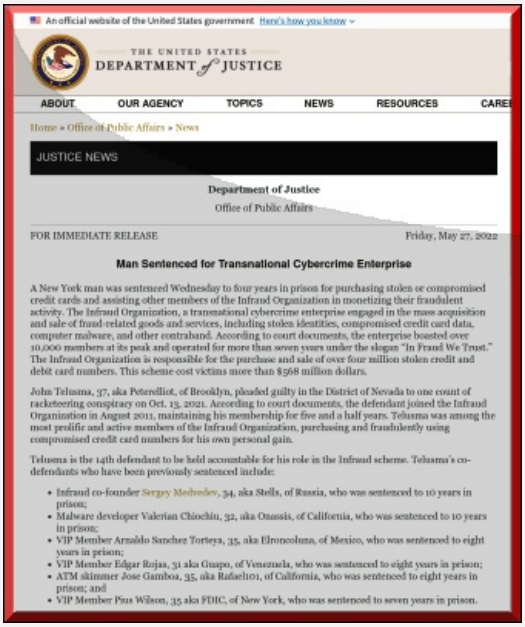


A 2010-ben Szvjatoszlav Bondarenko által alapított Infraud Organization banda weboldala a .cc az ausztráliai Kókusz-szigetek, valamint a .ws azaz Nyugat-Szamoa doménjein is üzemelt, később aztán más címekre költözött. **Az Infraud tagjai több mint 4 millió ellopott hitel- és betéti kártya megvásárlásáért és illegális eladásáért voltak felelősek, amivel összesen több, mint 568 millió dolláros veszteséget okoztak magánszemélyeknek, vállalkozásoknak és a pénzügyi intézményeknek.**

A bűnözők a banki adatlopás és feketekereskedelem mellett **kémkedésre, adatlopásra alkalmas rosszindulatú számítógépes programok értékesítésében és terjesztésében is vétkesek voltak.**

Ezek alapján a mostani ítélet szerint **John Telusmát, egy 37 éves New York-i férfit ítélték négy év börtönre, mert bűnrészes volt lopott hitelkártyák adásvételében az infraud kártyaportálon**. Telusma egyike annak a 36 személynek, akiket az amerikai hatóságok még 2018. februárjában vádoltak meg a nemzetközi bűnszervezetben játszott szerepük miatt.

A szervezet tagjai a nickneveken felül személyesen nem ismerték egymást, hogy az esetleges lebukás esetén elkerüljék a kapcsolattartás miatti következményeket.



An official website of the United States government Here's how you know

THE UNITED STATES DEPARTMENT of JUSTICE

ABOUT OUR AGENCY TOPICS NEWS RESOURCES CAREE

Home » Office of Public Affairs » News

JUSTICE NEWS

Department of Justice
Office of Public Affairs

FOR IMMEDIATE RELEASE Friday, May 27, 2022

Man Sentenced for Transnational Cybercrime Enterprise

A New York man was sentenced Wednesday to four years in prison for purchasing stolen or compromised credit cards and assisting other members of the Infraud Organization in monetizing their fraudulent activity. The Infraud Organization, a transnational cybercrime enterprise engaged in the mass acquisition and sale of fraud-related goods and services, including stolen identities, compromised credit card data, computer malware, and other contraband. According to court documents, the enterprise boasted over 10,000 members at its peak and operated for more than seven years under the slogan "In Fraud We Trust." The Infraud Organization is responsible for the purchase and sale of over four million stolen credit and debit card numbers. This scheme cost victims more than $568 million dollars.

John Telusma, 37, aka Peterelliot, of Brooklyn, pleaded guilty in the District of Nevada to one count of racketeering conspiracy on Oct. 13, 2021. According to court documents, the defendant joined the Infraud Organization in August 2011, maintaining his membership for five and a half years. Telusma was among the most prolific and active members of the Infraud Organization, purchasing and fraudulently using compromised credit card numbers for his own personal gain.

Telusma is the 14th defendant to be held accountable for his role in the Infraud scheme. Telusma's co-defendants who have been previously sentenced include:

- Infraud co-founder Sergey Medvedev, 34, aka Stells, of Russia, who was sentenced to 10 years in prison;
- Malware developer Valerian Chiochiu, 32, aka Onassis, of California, who was sentenced to 10 years in prison;
- VIP Member Arnaldo Sanchez Torteya, 35, aka Elroncoluna, of Mexico, who was sentenced to eight years in prison;
- VIP Member Edgar Rojas, 31 aka Guapo, of Venezuela, who was sentenced to eight years in prison;
- ATM skimmer Jose Gamboa, 35, aka Rafael101, of California, who was sentenced to eight years in prison; and
- VIP Member Pius Wilson, 35 aka FDIC, of New York, who was sentenced to seven years in prison.

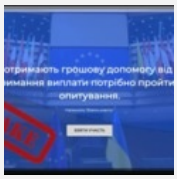
A bírósági dokumentumok szerint Telusma 2011. augusztusában csatlakozott az Infraud szervezethez **"Peterelliot" álnéven, és összesen öt és fél évig volt aktív csapattag. Az egyik legtermelékenyebb bandatagnak számított, rendszeresen és nagy tételben szállította a lopott banki adatokat.**

Az Egyesült Államokban már korábban is születtek ítéletek ez ügyben, többek közt például Szergej Medvegyevet, az Infraud másik társalapítóját 10 év börtönre ítélték, Valerian Chiochiu malware fejlesztőt szintén 10 évre, Arnaldo Sanchez Torteya és Edgar Rojas VIP-tagokat nyolc évre, az ATM csalással foglalkozó Jose Gamboát nyolc, míg a Pius Wilson VIP-tagot hét év börtön büntetésre ítélték.

Szólj hozzá!
Címkék: bűnözés ítélet adat bankkártya lopott szervezett bűnszervezet bűnbanda banki organization infraud

Ajánlott bejegyzések:


Drágán add a bankkártyád!


Adathalászok lakat alatt


Magyar Posta csomagunk jött - vagy


Xenomorph kalandjai GooglePlay

Netwalker tag menni 6 év börtön

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

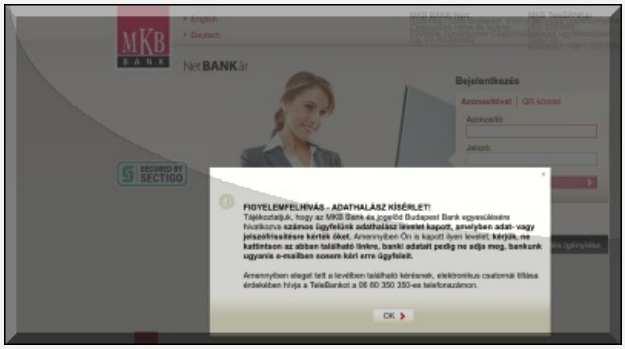
accountz

Belépés
Regisztráció

MKB adathalászat szigonnyal, horoggal, hálóval

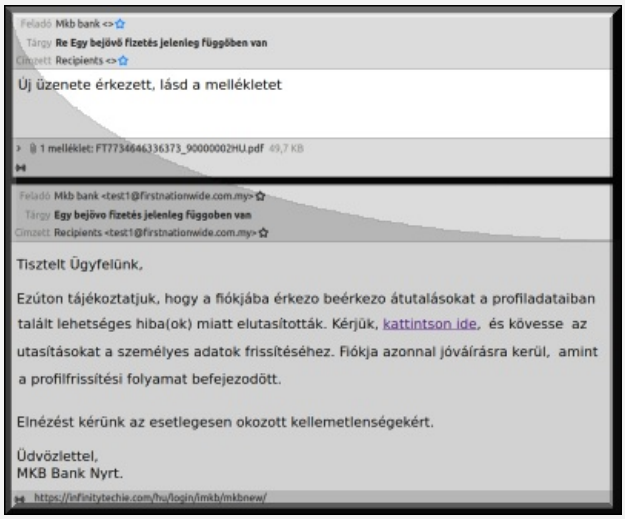
2022. június 01. 11:56 - Csizmazia Darab István [Rambo]

Szinte nincs nap, hogy **valamelyik magyarországi bank ellen ne indulna phishing támadási kísérlet. Ezúttal a Magyar Külkereskedelmi Bank került célkeresztbe**, de Déri Jánossal szólva szerencsére a gyenge minőségű adathalász próbálkozásért akár járhatna a Pocsék Áruk Fóruma díj.



Két kéretlen levél is érkezett a postafiókunkba, az első még a gagyi szintet is csak alulról próbálta meg súrolni, tegyük hozzá sikertelenül. Ebben az e-mail trace alapján egy németországi IP címről (Hessen, Frankfurt am Main) írtak mindössze annyit egy "*Re Egy bejövő fizetés jelenleg függőben van*" tárgysorú levélben, hogy: "*Új üzenete érkezett, lásd a mellékletet*".

Megszólítás nuku, aláírás nuku, a címzettnél látszik, hogy tömegesen kiküldött körlevélről van szó, a mellékletében pedig egy .PDF kiterjesztésű állomány, amelyre a VirusTotal 71 motorja közül egyik sem riasztott.



Így ez nem is érdemel több figyelmet, rátérhetünk a második üzenetre, a mesterbűnözők szemlátomást igyekeztek javítgatni a tákolmányukat. Ebből született immár a mai, most már nyárinak számító júniusi levél, **"*Egy bejövo fizetés jelenleg függoben van*" tárgysorral.**

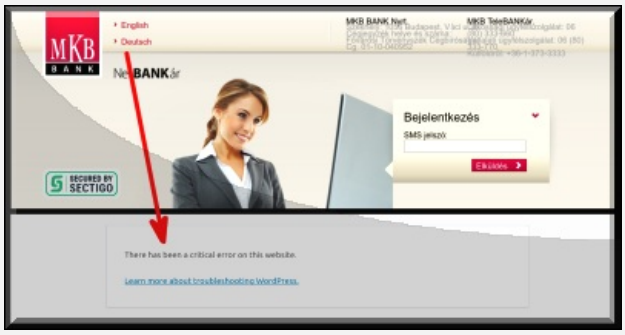
Gyenge magyarság, hiányzó ékezetek, és megint csak tömeges terjesztésre utaló "*Recipients*" szerepel a címzett mezőben. Itt már láthatóan több lektori figyelem jutott az üzenet helyesírására, esetleg egy magyar bandatag segítségével, ennek ellenére az ékezetek itt sem lettek tökéletesek.

"*Tisztelt Ügyfelünk,*

Ezúton tájékoztatjuk, hogy a fiókjába érkezo beérkezo átutalásokat a profiladataiban talált lehetséges hiba(ok) miatt elutasították. Kérjük, kattintson ide, és kövesse az utasításokat a személyes adatok frissítéséhez. Fiókja azonnal jóváírásra kerül, amint a profilfrissítési folyamat befejezodött. Elnézést kérünk az esetlegesen okozott kellemetlenségekért.

Üdvözlettel,
MKB Bank Nyrt."

Ezúttal egy holland IP címtartományból érkezett az e-mail, ahol a kattintható link erre az URL-re mutat: "https://infinitytechie.com/hu/login/imkb/mkbnew/". Nem igazán néz ki hivatalos banki oldalnak.



Az adathalász oldal erős, de **nem tökéletes hasonlósággal [másolja az MKB eredi NetBankár oldalát](#)**, amely naprakészen már egy figyelmeztető ablakot is feldob, amelyben az éppen aktuális adathalász kísérletről tájékoztatja az ügyfeleket. Fekete-öves versenyzőknek **nem csak a domén név eltérése tűnhet fel, de ha valaki veszi a fáradságot, és ellenőrzi a biztonsági tanúsítványt is**, ott is ordít róla, hogy átveréssel állunk szemben.

Ha a másolt csaló weblapon **kattintunk a német vagy angol nyelv linkre, egyből kiderült, hogy megint egy valamilyen kihasznált sebezhetőség révén feltört Wordpress oldal szolgált kamu banki aloldalnak** - ahogy ez például a FedEx-es Flubot esetben is történt.

Az adathalász oldal bekéri a banki azonosítót és a jelszót, és nagy trükkösen az SMS kódot is, tehát ha valaki ezt benézi, akkor ezzel bukta a saját belépését. Remélhetőleg idáig már senki nem jut el, mert patentül idejében felismert minden ide vonatkozó gyanús intő jelet. Azért az vicces lett volna, ha még az adathalászatra figyelmeztető ablakot is idemásolták volna.

A cikk írása közben a pshishing oldalt is sikeresen lelőtték, de gyaníthatóan másik feltört Wordpress oldalakon még nagy valószínűséggel többször is találkozhatunk majd vele.

4 komment
Címkék: spam magyar link bank levél csalás átverés üzenet phishing mkb kéretlen adathalászat külkereskedelmi

Ajánlott bejegyzések:


Csomagja kézbesítésre vár! Vagy mégsem?

Egyre gyakoribb a banki adathalászat


A bankos mindig kétszer csenget...


Üdvözlünk Sin City-ben

Vakcinás csalások, szevasztok

Kommentek:

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2022.06.01. 17:42:17

MKB Bank. Nem Magyar Külkereskedelmi Bank.
Hogy ki volt az a címeres ökör, aki kitalálta, hogy tartsák meg az MKB nevet, de dobják a bank eredeti nevét, arra már nem emlékszem.
Még Erdei Tamás volt a vezér a névcsere idején, szóval nem ma volt.
Vagy azóta újra külkereskedelmi?

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2022.06.01. 17:44:17

J, holland IP -> jó eséllyel protonvpn.

Válasz erre

Hívő hitetlen 2022.06.02. 10:44:11

Nem pshishing, hanem phishing.
Ha már .

Válasz erre

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2022.06.02. 17:44:22

Csak elütés volt, de köszi szépen a jelzést :-)

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

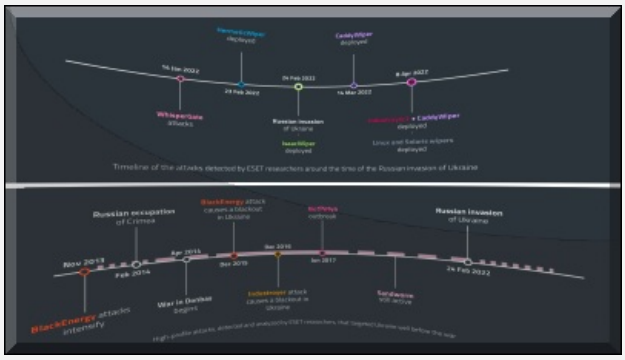
Oroszország lett a fő kibercélpont

2022. június 07. 09:02 - Csizmazia Darab István [Rambo]

Az ESET közzétette az idei első vírusriportját, amely többek közt **bemutatja az Ukrajnában zajló, a kutatók által kielemzett és elhárított, a háborúhoz köthető kibertámadásokat. Ezek közé tartozik a hírhedt Industroyer malware feltámadása, ami nagyfeszültségű elektromos állomásokat vesz célba.**

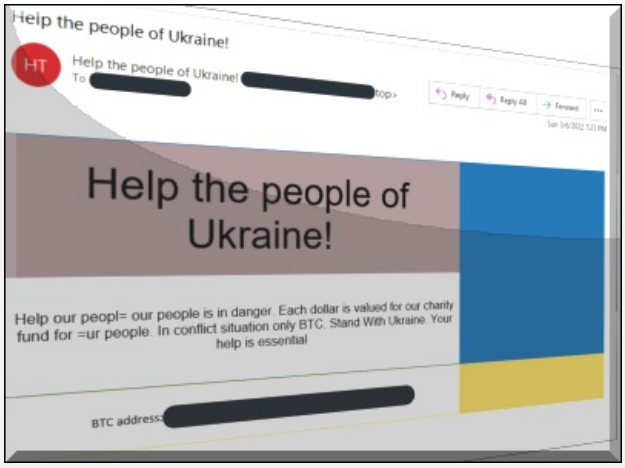
Röviddel az orosz invázió előtt az ESET telemetriai adatai a Távoli Asztali Protokoll (Remote Desktop Protocol, RDP) támadások jelentős, 43 százalékos csökkenését mutatták. A támadások számának visszaesése két évnyi folyamatos növekedés után következett be - a vírusriport szerint ez is összefüggésben lehet az ukrajnai háborúval. A csökkenés mellett **megfigyelhető, hogy a 2022. első harmadában észlelt RDP-támadások közel 60%-át Oroszországból indították.**

"*A világ különböző részein számos konfliktus dúl, de számunkra mást jelentenek az ukrajnai események.* ***Közvetlenül Magyarország és Szlovákia keleti határainak közelében ukrán emberek az életükért és a szuverenitásukért harcolnak*****" - emelte ki Roman Kováč kutatási igazgató** annak kapcsán, hogy a jelentés a háborúval kapcsolatos kiberfenyegetettségre összpontosít.



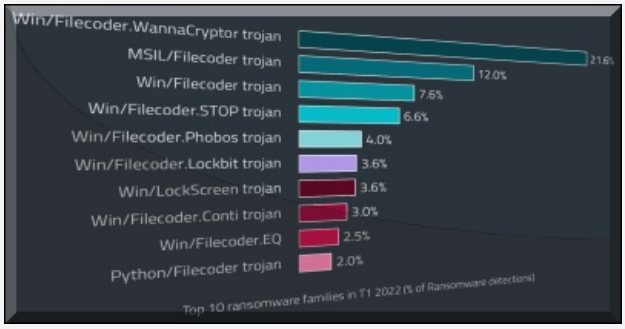
A háború másik mellékhatása, hogy míg korábban a zsarolóvírus-fenyegetések általában elkerülték Oroszországot, a háború kitörése óta Oroszország a kibertámadások legkedveltebb célpontja lett. Elemzők olyan Lock-Screen, azaz az okostelefonok képernyőzárát megkerülő vírust is találtak, amelyek az ukrán nemzeti üdvözlést használják, miszerint "*Slava Ukraini!*", *vagyis* "*Dicsőség Ukrajnának!*" Az invázió kezdete óta megnőtt az amatőr zsaroló- és adattörlőprogramok száma is. Ezek készítői gyakran a harcoló felek egyike mellett foglalnak állást, és a támadásokat személyes bosszúként állítják be.

Nem meglepő módon a háborúban a spam és az adathalász fenyegetések is megjelentek. Közvetlenül a február 24-i események után **a csalók elkezdték kihasználni az Ukrajnát támogatni próbáló embereket, fiktív jótékonysági szervezetek és adománygyűjtő akciók által.** A statisztikai adatok már az invázió első napján is a spamek nagymértékű megugrását mutatták.

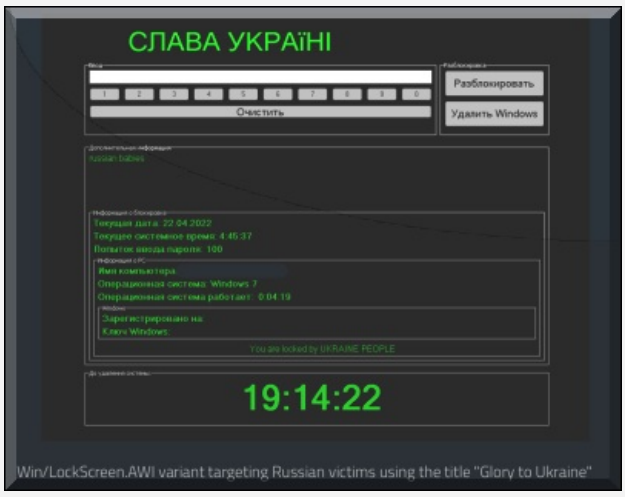


2022. márciusában és áprilisában az Emotet üzemeltetői magasabb fokozatba kapcsoltak, és tömeges spam-kampányokat indítottak **Microsoft Word dokumentumok felhasználásával, ami miatt az Emotet észlelések száma 113-szorosára emelkedett.** Az Emotet kampányai megjelentek az e-mail fenyegetések között is – ezek 2022 első harmadában 37 százalékos emelkedést mutattak. A kiberbiztonsági vállalat telemetriai mérései számos más, az orosz-ukrán háborúhoz nem kapcsolódó fenyegetést is észleltek. A biztonsági kutatók megerősítették, hogy az Emotet – a hírhedt malware, amely elsősorban spam e-maileken keresztül terjed – **a tavalyi törlési kísérletek után visszatért, és újra felbukkant telemetriájukban.**

Az Emotet működtetői az év első harmadában **az egyik spamkampányt indították a másik után, és támadási kísérleteik több mint százszorosára nőttek**. A vírusriport ugyanakkor megjegyzi, hogy a rosszindulatú makró szkriptekre épülő kampányok talán az utolsók voltak ebből a fajtából, **mivel a Microsoft nemrégiben úgy döntött, az Office programokban alapértelmezés szerint letiltja az internetről elérhető makrókat. A változást követően az Emotet üzemeltetői más támadási vektorokat kezdtek tesztelni.**

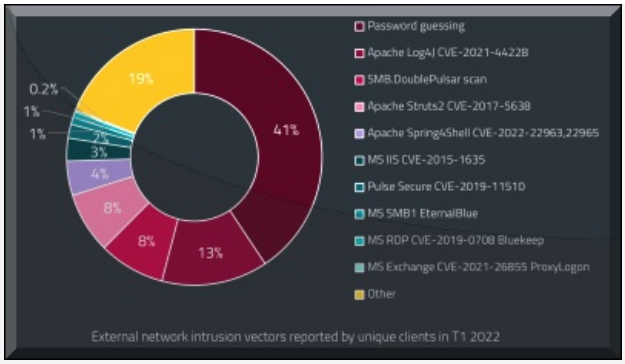


Az első harmadéves vírusriport legfontosabb megállapításai között olyan észlelések is szerepelnek, mint a kernel-illesztőprogramok sebezhetőségével való visszaélések; **a nagy kockázatú UEFI sebezhetőségek; az Android és iOS eszközöket célzó kriptovaluta kártevők; egy, a DazzleSpy macOS malware-t telepítő, ám egyelőre nem azonosított kampány, valamint a Mustang Panda, a Donot Team, a Winnti Group és a TA410 APT csoport akciói.**



Az ESET kutatói a vállalat éves konferenciáján a vírusriport mellett **a hírhedt Lazarus APT csoport védelmi és repülőgépipari vállalkozókat célzó támadásait is ismertették. A Lazarus a közelmúltban a LinkedIn és a WhatsApp használatával szedte áldozatait.** A csoport álláshirdetésnek álcázott megkeresésekkel igyekezett bizalmat építeni a hamis toborzók és a gyanútlan jelentkezők között, végül kártékony programokat küldött a mit sem sejtő áldozatoknak.

A célpontjaik itt főként európai, illetve közel-keleti és latin-amerikai internetezők voltak. Az amerikai kormány szerint a Lazarus kapcsolatba hozható az észak-koreai rezsimmel.



A legfrissebb kiberbiztonsági hírekért érdemes bekövetni a szakértőket a Twitteren. A teljes, angol nyelvű riport az alábbi linken olvasható.

Szólj hozzá!
Címkék: statisztika oroszország háború infrastruktúra virus riport kritikus eset kibertámadás welivesecurity.com

Ajánlott bejegyzések:


Sötét jelen: agresszív zsarolóvírusok, tömeges bruteforce


Kormányzatok célkeresztben

Kis- és középvállalkozások adatvédelmi incidensei


Felkészül: USA kritikus infrastruktúra

A nemzetközi helyzet egyre fokozódik

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.

VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

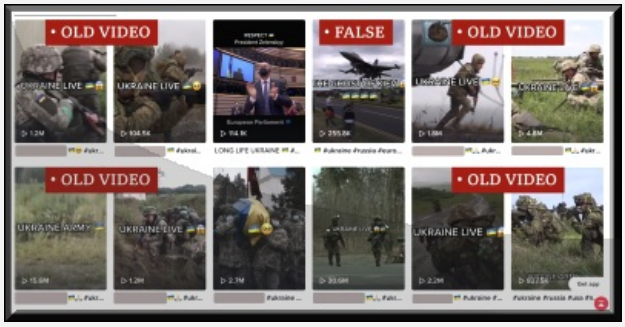
Hazugságok: messzebbre és gyorsabban

2022. június 10. 09:28 - Csizmazia Darab István [Rambo]

Miért hisszük el az álhíreket? **Kutatások szerint a hazugság nem csak gyorsabban és messzebbre terjed az igazságnál, de a valótlanságokra sokkal több reakció is érkezik a közösségi médiában.** Az ESET szakértői összegyűjtötték, miért terjedhetnek olyan gyorsan az álhírek és **mi az oka, hogy oly sokan hisznek ezeknek.**

Minden nap hírek áradata versenyez a figyelmünkért: a végtelen mennyiségű és széles körű információ könnyen túlterhelővé, nyomasztóvá válhat számunkra. Korábban nem látott részletességgel követhetjük például az Ukrajnában zajló háború történéseit, **amely nem véletlenül kapta az "első TikTok háború" elnevezést.**

Az ukrajnai lakosok a TikTok, a Twitter és az Instagram segítségével tudják megmutatni a világnak, hogy min mennek keresztül. **Azonban a háborúban részt vevő mindkét félnek hozzáférése van ezekhez a platformokhoz, amelyek így digitális csatatérré válnak, emberek millióinak tudatát befolyásolva világszerte.**



Azt már mindenki megtapasztalhatta, hogy amiben hiszünk, az néha nem feltétlenül valós. **Napjainkban az ipari méretű félretájékoztatás azonban a társadalmat sújtó egyik legnagyobb probléma. Az MIT (Massachusettsi Műszaki Egyetem) 2018-ban publikált kutatása a Twitteren megosztott híreket elemezte, és arra jutott, hogy a hazugság jelentősen messzebbre, gyorsabban, mélyebben és szélesebb körben terjed, mint az igazság, még akkor is, ha a botokat eltávolítják, és csak a valódi emberi interakciókat veszik figyelembe.**

Az eredmények olyannyira feltűnőek, hogy az MIT következtetése szerint a vizsgált bejegyzések esetében **a valótlanságokat 70 százalékkal nagyobb valószínűséggel retweetelték, mint az igazságot.**

A probléma hátterében a **kognitív torzítások állhatnak, aminek mindannyian áldozatai vagyunk: minden vagy semmi gondolkodás, túláltalánosítás, pozitívumok diszkvalifikálása, címkézés.** Bár ez a mindennapi életünkben hasznos lehet, mert lehetővé teszi számunkra, hogy emlékezzünk a korábban megtanult folyamatokra és felismerjük az ismerős helyzeteket, mégis hajlamossá tehet minket mentális vakfoltokra.

Jól példázza ezt **egy beszélgetés két olyan ember között, akik az ukrajnai háború ellentétes oldalán állnak: mindkét fél úgy gondolja, hogy racionálisan cselekszik, a másikat vádolva azzal, hogy elfogult és nem érti a valóság összetettségét.** Innentől kezdve mindketten nyitottabbak lesznek az olyan hírek fogyasztására, amelyek megerősítik saját nézőpontjukat - még akkor is, ha a hír valótlan.

Általában olyan emberekkel vesszük körül magunkat, akikkel azonos a világnézetünk, és ez a tendencia a közösségi médiában még hangsúlyosabb: online egy szűrt valósággal találkozunk, amelyet egy olyan algoritmus épít fel, amely megerősít bennünket, bármilyen elképzeléseink is vannak. **A közösségi médiában a saját buborékunkban vagyunk, ahol mindig nekünk van igazunk. Ezzel viszont kamrákba (echo chambers), vélemény buborékokba záródva torzul a világképünk. Az elfogultak számára csak fekete vagy fehér létezhet, és sosincs egyrészt-másrészt típusú érvelés, nézőpont váltás.**

A Nature magazin 2018-ban megjelent egyik cikke az 1918-as világjárvány tapasztalatairól, valamint egy jövőbeli járvány kitörésének kockázatairól szólt. A szerző, Heidi Larson, a London School of Hygiene and Tropical Medicine **antropológus professzora azt jósolta, hogy a következő nagy járvány nem a megelőző technológiák hiánya miatt fog kitörni, hanem az ellentmondásos információk, a félretájékoztatás és a manipulált információk áradata miatt zajlik majd a közösségi médiában.**

Amikor Larson 2018-ban a téves információk terjesztéséről írt, **egy olyan kifejezést használt, amellyel mindannyian megismerkedtünk az utóbbi időben: szuperterjesztők, akárcsak a vírusok esetében.** Egy kifejezés, amely megmagyarázza, hogy az internetes trollok hogyan okoznak pusztítást azzal, hogy szándékosan ellentmondásos és lázító hozzászólásokat tesznek közzé. De míg egyesek közülük csak unatkozó, az internet láthatatlanná tévő köpenyét

használó egyének, **addig mások ezt napi munkaként végzik, felhergelve a közvéleményt, megzavarva a társadalmi és politikai folyamatokat. Ez volt az egyik következtetése annak a két oxfordi kutatónak is, akik több példát is találtak arra, hogy a kormányok, illetve a magánvállalatok hogyan irányítják a szervezett kibercsapatokat.**

Ne etessük a trollokat! - az egyik legfontosabb tanács, amelyet be kell tartani, amikor online találkozunk velük, ha nem így teszünk, akkor csak olajat dobunk a tűzre és pontosan azt adjuk nekik, amire vágynak - figyelmet. **Az érvek süket fülekre találnak, hiszen a trollok nem akarnak vitatkozni, csak dühöt és szorongást akarnak kiváltani.**

Szóval akkor hogyan kezeli ezt a közösségi média? A The New Yorker 2019-ben azt írta, az elmúlt évtizedben **a Facebook elutasította azt a nézetet, hogy a közösségi oldal lenne a felelős a tartalom szűréséért,** ehelyett a platformot egy üres térként kezelte, ahol az emberek megoszthatják az információkat. Azóta az álhírek nemcsak választási eredményeket befolyásoltak, hanem a való életben is jelentős kárt okoztak az embereknek.

A félrevezető tartalmakkal kapcsolatos hozzáállásuk miatt éles bírálatokat kapott már a Twitter, a Telegram és a YouTube is. Egyes kormányok nagyobb felelősséget követelnek, sőt, **azt fontolgatják, hogy szabályozást vezetnek be ezekre a szolgáltatásokra a tiltott tartalmak vagy a hamis, szélsőséges eszmék terjesztése miatt.**

2022. januárjában tényellenőrző weboldalak a világ minden tájáról nyílt levélben fordultak a YouTube-hoz, amelyben felszólították a világ legnagyobb videómegosztó portálját, hogy tegyen határozott lépéseket, elsősorban kontextusok megadásával és cáfolatok felajánlásával ahelyett, hogy egyszerűen törölné a videós tartalmakat.

A levél kitért arra is, hogy a visszaeső jogsértőkkel szemben fel kell lépni, és ezeket az erőfeszítéseket az angoltól eltérő nyelveken is alkalmazni kell.

Mit lehet tenni? Ellenőrizzük, ki hozta létre az adott weboldalt, ki írta a cikket! Gondolkodjunk reálisan: a címsorok sokszor túlzóak, torzítottak, hogy minél többen kattintsanak rá. **Több párhuzamos és hiteles forrásból tájékozódjunk, és hasonlítsuk össze az információkat azzal, amit magunk, családtagjaink, barátaink közvetlenül tapasztaltunk!**

Ellenőrizzük a cikk megjelenési dátumát és külön a képeket is egy inverz képkeresővel, hogy láthassuk, az adott híren kívül hol, mikor és mire használták fel azokat! **Hasonlítsuk össze a kérdéses információt a fősodratú fakenews terjesztők híreivel, és ha megegyezik, akkor jó eséllyel egy szándékosan terjesztett megtévesztéssel állunk szemben!**

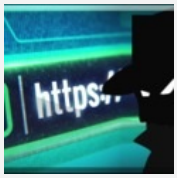
Itt jönnek képbe **a tényellenőrző platformok, amelyek megvizsgálják és értékelik a hírek vagy a közösségi médiában terjedő posztok információinak minőségét.** Azonban még ezeknek a forrásoknak is megvannak a maguk korlátai. Mivel a valóság nem mindig egyértelmű, a legtöbb ilyen weboldal egy barométer-szerű mutatót követ, amely a "hamis", "többnyire hamis", "többnyire igaz" és az "igaz" között mozog. **Sőt sajnos újabban a fakenews terjesztők hamis tényellenőrző oldalakat is üzemeltetnek, vagyis itt is fontos, hogy minőségi és megbízható platformot válasszunk.**

Nekünk magunknak is van szerepünk abban, hogy különbséget lehessen tenni a valódi és a hamis információk között: egy háborúban ez az egyéni munka még nagyobb jelentőséget kap, de békeidőben és **általában véve is érdemes fenntartásokkal kezelni, amit tényként állítanak egyesek.** A legfrissebb kibertéri hírekért érdemes bekövetni az ESET kiberbiztonsági kutatóit a Twitteren, a mellékelt linken pedig **a 2019-es III. Ethical Hacking Day konferencián elhangzott "Médiahekk, Social engineering, Photoshop, Deepfake, Fakenews" előadás videófelvételét lehet megtekinteni.**

1 komment
Címkék: hírek hamis eset deepfake fakenews tényellenőrzés

Ajánlott bejegyzések:

Kis- és középvállalkozások adatvédelmi incidensei



Böngészés - kockázatok és mellékhatások


Durva ransomware statisztikai adatok


Kiberbiztonsági útikalauz diákoknak


Oroszország lett a fő kibercélpont

Kommentek:

ulpius66 2022.06.12. 15:00:12

Most már csak az a kérdés, hogy ez a cikk valóság, vagy álhír?

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.

VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

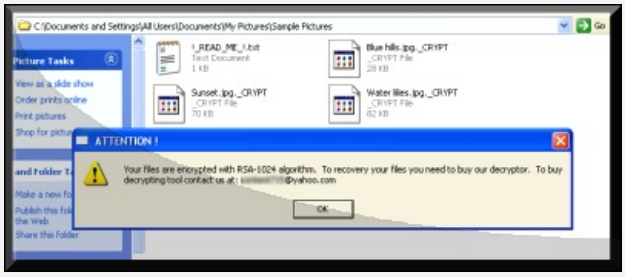
Evolúció, ami számunkra nem csodálatos

2022. június 14. 11:15 - Csizmazia Darab István [Rambo]

Folyamatos fejlődésen megy át az az új generációs zsarolóvírus, amelynek első klasszikus képviselője a még 2013-ban felbukkant CryptoLocker volt. A ransomware jó tíz éve tarolja le a gépek adatait, és láthatóan **mindig megjelenik benne valami olyan újabb csavar, ami még ijesztőbbé teszi az amúgy is komoly kockázatú kártevőt.**

Egy történelmi elődöt azért említsünk meg, ez pedig nem más, mint a Windows XP és Vista korszakban 2008-ban megjelent GPCode kártevő, amely erős, 1024 bites RSA titkosítással kódolta el a felhasználó dokumentum adatait (például .DOC, .JPG, .PDF), majd letörölte azokat és némi készpénz fejében felajánlotta a titkosítást feloldó kulcsot.

A módszer **ekkor már szinte kész volt, igaz a GPCode ekkor még elvérzett azon, hogy az antivírus cégek összefogásával sikerült durva hibákat találni a kártevőben és ennek segítségével fizetésmentesen** a zsarolást szerencsésen megúszva visszaállítani az elkódolt fájlokat.



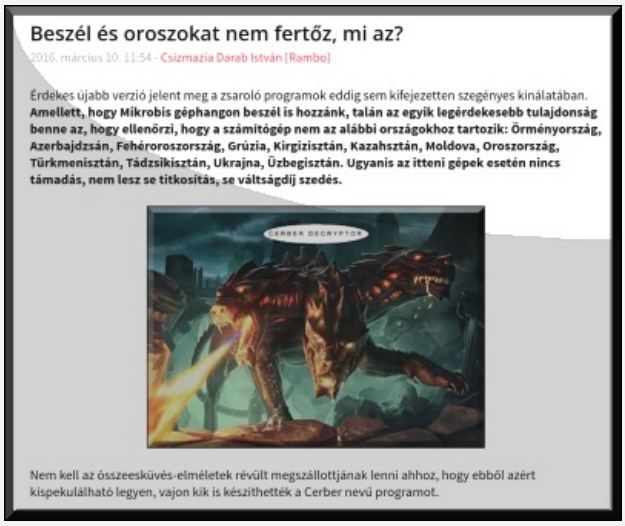
Az alapműködés, vagyis az 1024-2048 bites egyedi aszimmetrikus RSA kulcs (más kulcs a titkosításhoz, más a feloldáshoz), később az RSA-nál erősebb Elliptical Curve Cryptography (ECC) alkalmazása, jellemzően 24-48 órás rövid határidő, és Bitcoinban vagy más kriptovalutában követelt váltságdíjon felül **eleinte csak apró kis lépésekben gyülekeztek a felhők.**

A zsarolók lehetőséget adtak például 5 darab fájl ingyenes teszthelyreállítására, hogy bizonyítsák, fizetés esetén működik az "üzleti" modell, ám hamarosan **megjelent például az is, hogy a határidő lejárta után duplázódott a váltságdíj összege.**

Aztán **jöttek a további baljós jelek: maga a zsarolóvírus, vagy a vele együttműködő kártevők célzottan törölték a helyi backup, a rendszer-visszaállítási pontokat, valamint az úgynevezett lokális Shadow Copy fájlokat is, hogy mentés híján ezzel is megnehezítsék a helyreállítást. 2015. óta aztán újabb fellegek**

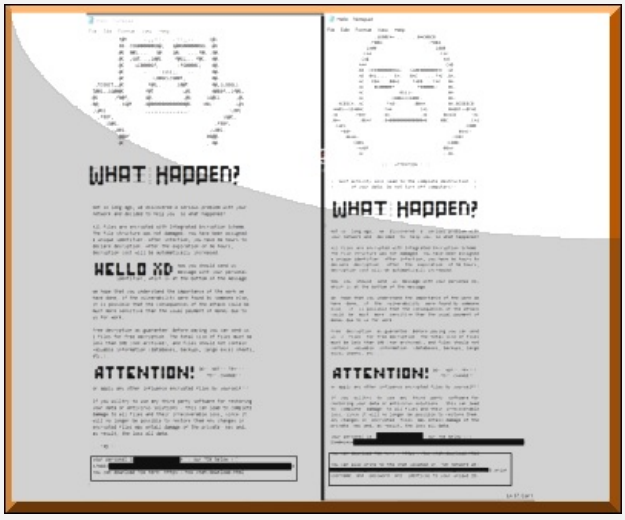
érkeztek: a Windows rendszerek mellett megjelentek a Macintosh, Linux és Android platformokon futó változatok is, igaz a Windows fősodornál kisebb mennyiségben.

Ám a fizetési hajlandóságra az mért egy igazán jelentős csapást, amikor a Chimera 2015-ben a titkosított állományokat már nemcsak zárolta, hanem **nemfizetés esetén fel is töltötte egy nyilvános weboldalra, így ha volt is biztonsági mentés, sokan az adatszivárgás elkerülése miatt így is fizettek.** Azóta ez a doxingnak nevezett módszer mára már a cégeket támadó zsarolási recept egyik állandó kelléke lett.



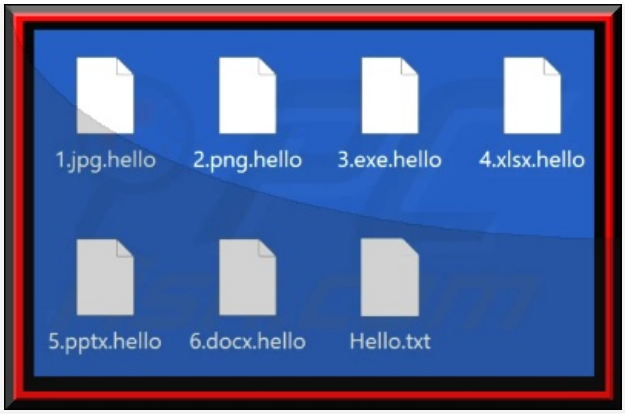
A bűnbandák ontották a különféle zsarolóvírusokat, így a Cerbertől, CryptoWall-tól kezdve WannaCryptoron át Locky-t, CTBLocker-t, NotPetya-t, Ryuk-ot, TeslaCrypt-et, Clop-ot, Hive-t, RagnarLocker-t a REvil-ig rengeteg verzió jelent meg, **és egy idő után testet öltött a RaaS, azaz a Ransomware as a Service bérelhető szolgáltatás is.**

Már korábban is egyre olcsóbban lehetett ransomware kódot vásárolni, ám ez a szisztéma 24/7 supporttal, felkínált nyelvi modulokkal, különféle affiliate konstrukciókkal elképesztő módon elterjedt. Ma már olyan szolgáltatásokat is ajánlanak, mint **vonakodó fizetés esetén DDoS támadás indítása, a megszerzett-ellopott doxing adatok tárolása-közzététele** vagy a váltságdíj-tárgyalások kezelése.



A most felbukkant **Windows és Linux környezetben futó Hello XD ransomware egy beépített hátsóajtót is tartalmaz, amelyet a támadók a veszélyeztetett rendszerben való navigáláshoz, az értékes felhasználói fájlok kiszűréséhez, tetszőleges távoli parancsok végrehajtásához és az árulkodó nyomok törléséhez használhatnak, illetve folyamatosan figyelemmel kísérhetik a titkosítás folyamatát is.**

A Unit42 elemzéséből nemcsak az derült ki, hogy ebben a kártevő változatban a MicroBackdoor nevű nyílt forráskódú hátsó ajtót alkalmazták, hanem hogy **a Hello XD valószínűleg a korábban kiszivárgott Babuk forráskódjára épült, és vélhetően az X4KME nevű orosz anyanyelvű bűnöző műve lehet.**



A beépített hátsóajtó segítségével a ransomware csoportok könnyen azonosíthatják a célba vett áldozatot, és képesek nyomon követni a hozzáférésen keresztül, amint az rendelkezésre áll. Érdekes, hogy az immár 36 éves vírustörténelemből ismert, a rosszindulatú futtatható fájlok tömörítéséhez használt UPX is felbukkant a történetben. Az elemzés szerint a Hello XD egy új, korai verziónak látszik, ám a képességei alapján alighanem sajnos még biztosan fogunk vele találkozni.

Végül egy elgondolkoztató tény: az IBM X-Force új tanulmánya azt mutatja, hogy **a vállalati ransomware támadások átlagos időtartama - azaz a kezdeti illetéktelen hozzáférés és a ransomware telepítése közötti idő - 2019. és 2021. között 94%-kal csökkent, vagyis több, mint két hónapról mindössze alig 4 napra.**

Szólj hozzá!
Címkék: statisztika orosz hello xd backdoor váltságdíj hátsóajtó ransomeware zsarolóvírus

Ajánlott bejegyzések:


Amikor a hóhért akasztják...


Emelkedő ransomware károk


Durva ransomware statisztikai adatok


Ransomware a spájzban


Ransomware helyzetjelentés

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

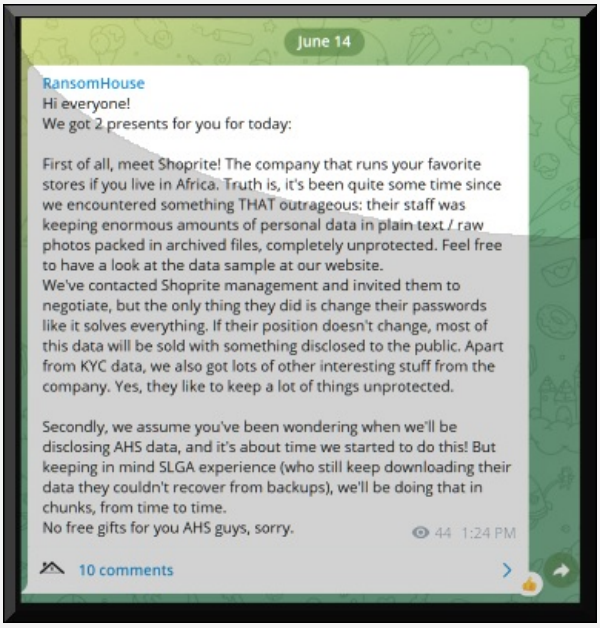
Ransom in da House

2022. június 16. 12:51 - Csizmazia Darab István [Rambo]

Afrika legnagyobb szupermarketláncát támadták meg zsarolóvírussal a múlt héten. **A Shoprite csaknem háromezer üzletet üzemeltet a kontinens tizenkét országában**, ügyfelek millióit szolgálja ki Dél-Afrikában, Nigériában, Ghánában, Madagaszkáron, Mozambikban, Namíbiában, Kongóban, Angolában és további más országokban.

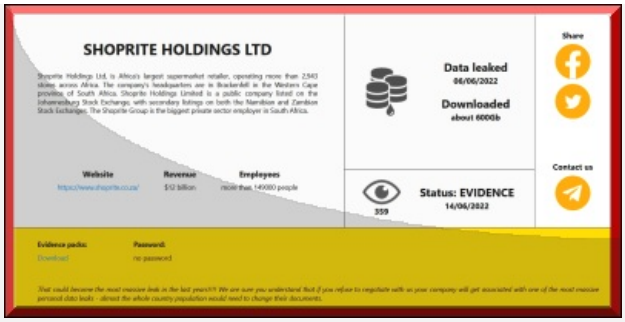
Főleg Európából és az Egyesült Államokból érkeznek a beszámlók különféle kibertámadásokról, pedig ezek mindenhol előfordulnak. A mostani esetnél a vállalat hozta nyilvánosságra, hogya múlt pénteken biztonsági incidenst szenvedtek el, ami miatt vásárlól személyes adatai is veszélybe kerülhettek. **A kiszivárgott, ellopott adatok neveket és azonosító számokat tartalmaznak, de pénzügyi információk vagy bankszámlaszámok állítólag nem szerepeltek benne.**

Valójában nehéz eldönteni, tényleg így történt-e vagy ez csak a bevett kríziskommunikációs elem. Mindenesetre **a cég figyelmezettet az ügyfeleit, hogy azonnal változtassanak jelszót, és óvatosan járjanak el, ha a közeljövőben illetéktelenek e-mailben, SMS-ben vagy telefonon megkeresik őket személyes banki adatok állítólagos egyeztetésére való hivatkozással.**



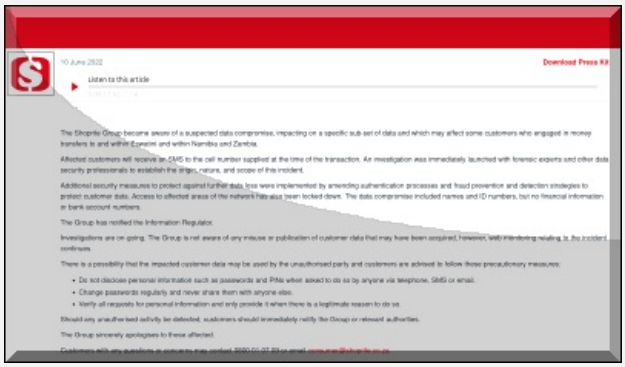
A BleepingComputer beszámolója szerint az elkövető a RansomHouse banda volt, akik 2021. decemberében tűntek fel, és szakértők szerint közreműködőként a White Rabbit csoporthoz tartoznak. Az ellopott doxing adatok nyilvánosságra hozatalához egy külön webhelyet hoztak létre, és azon egy **600 GB méretű adatmintát is közzétettek a váltságdíj nyomatékosításához.**

A Telegram csatornájukon közben egy olyan közleményt jelent meg, miszerint **a Shoprite biztonsági állapota csapnivaló volt, érzékeny adatokat tartottak a szervereken plain text formában, és emellett egyéb érdekes, zsarolási szempontból értékes adatokat is megszereztek, amivel nyomást tudnak helyezni a menedzsmentre.**



A RansomHouse gyakorlata, hogy az áldozataikat nyilvánosan hibáztatják a gyenge biztonsági gyakorlatokért és a nem megfelelő védelemért.

Azok, akik akik nem válaszolnak a zsarolási felhívásra vagy nem fizetnek nekik, ott az ellopott adatokat további más kiberbűnözőknek adják el, vagy ha mégsem akad rá vevő, akkor a csoport ingyenesen közzéteszi azokat az Onion webhelyén.



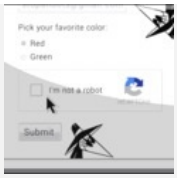
A szupermarket közleménye szerint **az incidens óta számos biztonsági intézkedést hajtottak végre (hát jókor...) a további adatvesztés elkerülése érdekében**, erősítettek a hitelesítési folyamatokon, illetve természetesen elnézést kérnek az ügyfeleiktől. A nyilatkozatból csak annyi derül ki, hogy zajlik a nyomozás az ügyben, de se a váltságdíj mértékéről, fizetési hajlandóságról, esetlegesen bevont külső szakértőkről nem beszélnek.

Az ügyfélből potenciális áldozat módszer pedig tovább szedi áldozatait, így tanulságként az erős egyedi jelszó, a többtényezős hitelesítés és az ismeretlen megkeresésekkel szembeni erőteljes gyanakvás említhető, hiszen ez utóbbi tényleg elképesztő mértékben támad bennünket bankok, hivatalok, vállalatok nevében.

A szupermarketek is vonzó célpontok a zsarolóvírus bandáknak, emlékezhetünk a Kaseya elleni támadásra, ahol járulékosan ugyan, de **a svédországi Coop hálózat 800 üzlete állt le emiatt, de említhető az idén áprilisban Trinidaban történt incidens is, ahol egy másik szupermarket, a Massy Stores szenvedett el hasonló zsarolóvírus támadást.**

1 komment
Címkék: afrika szupermarket adathalászat ransomware stores massy zsarolóvírus shoprite ransomhouse

Ajánlott bejegyzések:



[Mai szavunk pedig: reCAPTCHA]

[Összeomlás]

[Nem csitulnak a kórházak elleni támadások]

[Emelkedő ransomware károk]

[Venus ransomware támadja az egészségügyet]

Kommentek:

midnight coder 2022.06.17. 09:38:13

Mondjuk ezeket nem tudom miért nem lehet ugyanúgy elkapni mint mondjuk a pedofilokat és leültetni úgy, mintha mondjuk bankrablást követtek volna el?

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Módosított elefánt a felhasználók porcelánboltjában

2022. június 21. 11:52 - Csizmazia Darab István [Rambo]

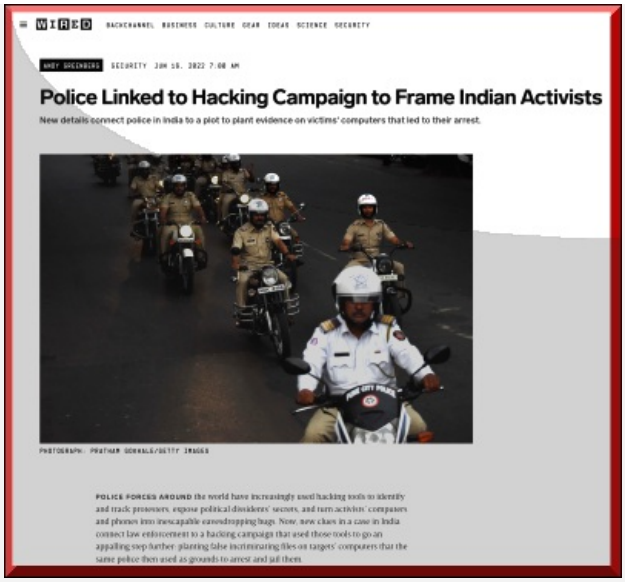
Sok éve már, hogy a kártevő fajták között feltűntek a politikai célú vírusok is. **Ezek eleinte csak üzeneteket jelenítettek meg, később viszont már célzottan támadtak konkrét személyeket vagy kémkedtek adott célpontok ellen**, de bosszúból rá lehet hívni bárkire a SWAT kommandót, sőt egyes államilag fejlesztett kártevő arra is képes volt, hogy az iráni busheri atomerőműben leégessen Siemens centrifugákat. **Most sajnos újabb területen látunk hasonló motivációt.**

Fakenews és deepfake sújtotta jelenünkben már az is nehézséget okoz, hogy kiszelektáljuk a hiteles, értékes és érvényes tartalmakat a szeméttől, a hamistól, a propagandától, a kártékonytól. Ez egy élethosszig tartó figyelmet, tanulást is igényel, ami nem mindenkinek terepe, igénye. Ám az internet mint az ötödik hadszíntér arra is lehetőséget ad, hogy ott kiberháborút vagy hibrid hadviselést folytassanak, **illetve politikai ellenfelek elleni kémkedésre is alkalmas.**

Emlékezetes lehet például a Potao incidens, ahol egy oroszországi weboldal olyan trójait terjesztett a TrueCrypt legitim szoftvert módosított változatában, **amivel ukrán tisztviselők és újságírók után kémkedtek.**

Ám a mostani eset ennél jóval tovább ment, itt már a hatalom szerint nemkívánatos személyek lejáratásában a hatóságok durván elvetették a sulykot, bűncselekményeket követtek el céljuk érdekében. **Egy friss indiai ügyben úgy néz ki, hogy gyaníthatóan maguk az állami bűnüldöző szervek követhettek el illegális hacker támadásokat, amelynek keretében a gyanúsítottak számítógépére hamis terhelő fájlokat töltöttek fel, ezzel bizonyítékot hamisítva.**

Az így "megtalált" Microsoft Office fájl bizonyítékok alapján a rendőrség aztán letartóztatásokat hajtott végre, ahol a vétlen felhasználókat börtönbüntetésre ítéltek, közülük az egyik a Covid vírusos időszakban azóta már meghalt a börtönben.



WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

ANDY GREENBERG SECURITY JUN 16, 2022 7:00 AM

Police Linked to Hacking Campaign to Frame Indian Activists

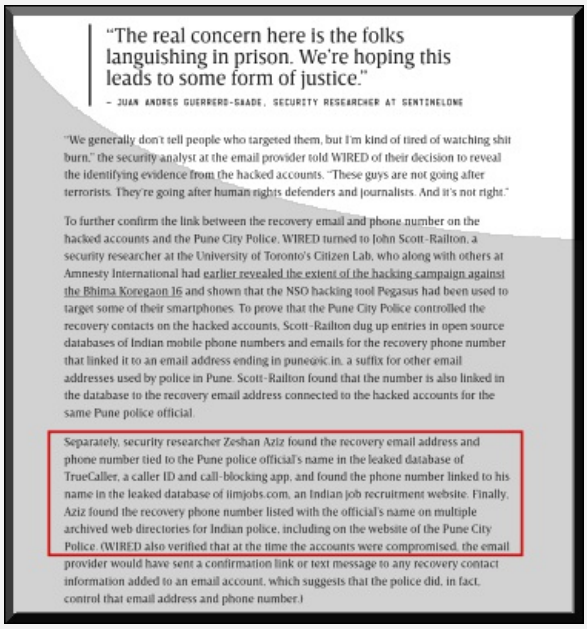
New details connect police in India to a plot to plant evidence on victims' computers that led to their arrest.

PHOTOGRAPH: PRATHAM GOKHALE/GETTY IMAGES

POLICE FORCES AROUND the world have increasingly used hacking tools to identify and track prosecutors, expose political dissidents' secrets, and turn activists' computers and phones into inescapable eavesdropping bugs. Now, new clues in a case in India connect law enforcement to a hacking campaign that used those tools to go an appalling step further: planting false incriminating files on targets' computers that the same police then used as grounds to arrest and jail them.

A szakértők szerint az illegális akció **egyértelműen politikai célzatú volt, ahol emberi jogi aktivisták és újságírók voltak az áldozatok. A Modified Elephant fedőnéven futó kampány keretében a NetWire nevű távoli adminisztrációs eszközt (RAT) használták**, amely lehetővé teszi a távoli támadók számára, hogy átvegyék a teljes vezérlést Windows, Mac OSX vagy Linux gépeken, vagyis tetszőleges fájl olvassanak, letöltsenek, töröljenek vagy oda feltöltsenek.

Ezzel a módszerrel **olyan kompromittáló dokumentumokat csempésztek be észrevétlenül a gyanúsítottak gépére, amik a szakértők véleménye alapján biztosan nem az adott számítógépen készültek.**



"The real concern here is the folks languishing in prison. We're hoping this leads to some form of justice."

– JUAN ANDRES GUERRERO-SAADE, SECURITY RESEARCHER AT SENTINELONE

"We generally don't tell people who targeted them, but I'm kind of tired of watching shit burn," the security analyst at the email provider told WIRED of their decision to reveal the identifying evidence from the hacked accounts. "These guys are not going after terrorists. They're going after human rights defenders and journalists. And it's not right."

To further confirm the link between the recovery email and phone number on the hacked accounts and the Pune City Police, WIRED turned to John Scott-Railton, a security researcher at the University of Toronto's Citizen Lab, who along with others at Amnesty International had earlier revealed the extent of the hacking campaign against the Bhima Koregaon 16 and shown that the NSO hacking tool Pegasus had been used to target some of their smartphones. To prove that the Pune City Police controlled the recovery contacts on the hacked accounts, Scott-Railton dug up entries in open source databases of Indian mobile phone numbers and emails for the recovery phone number that linked it to an email address ending in puneguic.in, a suffix for other email addresses used by police in Pune. Scott-Railton found that the number is also linked in the database to the recovery email address connected to the hacked accounts for the same Pune police official.

Separately, security researcher Zeshan Aziz found the recovery email address and phone number tied to the Pune police official's name in the leaked database of TrueCaller, a caller ID and call-blocking app, and found the phone number linked to his name in the leaked database of timjobs.com, an Indian job recruitment website. Finally, Aziz found the recovery phone number listed with the official's name on multiple archived web directories for Indian police, including on the website of the Pune City Police. (WIRED also verified that at the time the accounts were compromised, the email provider would have sent a confirmation link or text message to any recovery contact information added to an email account, which suggests that the police did, in fact, control that email address and phone number.)

Az elemzés arra is rávilágított, hogy **az egyik gyanúsítottat 2018. áprilisában egy adathalász támadással tévesztették meg**, ami után a postafiókját fel tudták törni, illetve azt azóta is folyamatosan képesek voltak megfigyelni.

A szakértők azt is észrevették, hogy **mindhárom ilyen feltört postafiók jelszó helyreállítási e-mail címe és telefonszáma egyértelműen a helyi rendőrséghez volt köthető, és azt a TrueCaller kiszivárgott adatbázisában is megtalálták és beazonosították.**

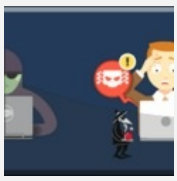
A biztonsági kutatók most azt remélik, hogy újabb részletes eredményeik segíthetnek a hamisan megvádolt gyanúsítottak szabadon bocsátásában. A TheRegister cikke alapján egyértelmű, hogy **az említett Modified Elephant-ot bizonyíthatóan már többször is arra használták, hogy kompromittáló adatokat, fájlokat - például terrorizmus, gyermekpornográfia - töltsenek fel áldozatok különféle eszközére.**

Virág elvtárs már 1969-ben megmondta: "*A kémek nem úgy dolgoznak, hogy gyanút keltsenek. Épp ellenkezőleg. De pont az bennük a gyanús, hogy nem gyanúsak. Érti már, Pelikán elvtárs?*"

3 komment
Címkék: india eszköz hamisítás bizonyíték kémprogram távoli rat adminisztrációs potao ModifiedElephant adm

Ajánlott bejegyzések:


Swatting - új köntösben


Üzleti e-mail hamisítás


Kulcs a túléléshez


Nem szállunk rendelkezésére

Kommentek:

gigabursch 2022.06.21. 12:22:31

Ügyes!

Válasz erre

Bitfaragó 2022.06.21. 14:02:54

Állítólag van ország ahol államilag, valami szárnyas lóval figyeltek meg újságírókat és aktivistákat...

Válasz erre

Kovacs Nocraft Jozsefne 2022.06.22. 12:47:45

@Bitfaragó:

Használd a többes számot: vannak olyan országok...

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

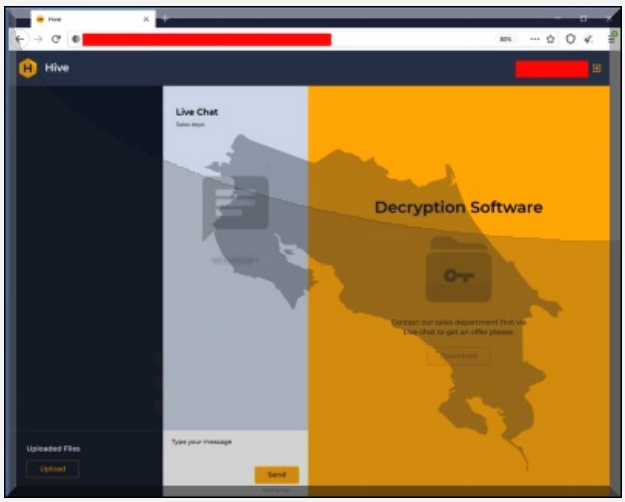
accountz

Belépés
Regisztráció

Felhasználó, kórház, olajvezeték után egy egész ország

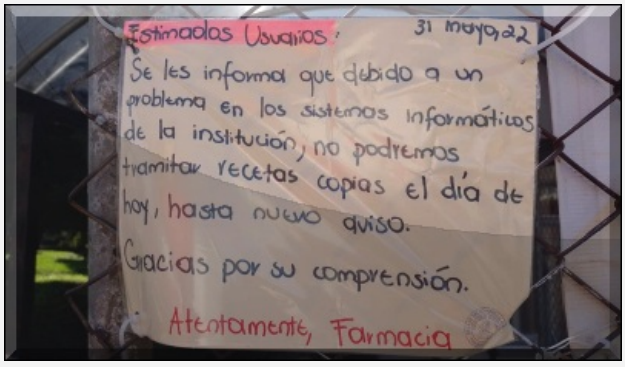
2022. június 23. 14:01 - Csizmazia Darab István [Rambo]

Egyre nagyobb tétekben zajlik a ransomware csata. Eleinte mentés-nélküli hétköznapi felhasználók estek el a fronton, aztán szép lassan ügyvédi irodák, rendőrőrsök, vállalkozások, cégek, közhivatalok, kórházak, repterek, utazási irodák, felhős távmenedzsment szolgáltató, üzlethálózatok, olajvezeték üzemeltetők szenvedték el a következményeket. **Most egy ország került a célkeresztbe és furcsa módon politikai üzenetek is előkerültek a támadók részéről.**



Costa Rica ellen indított zsarolóvírus támadást a hírhedt, Oroszországhoz köthető Conti és Hive bűnbanda, látszólag összedolgozva. Számos állami intézményt, többek közt a pénzügyminisztérium hálózatát, adó- és vámhivatalokat, kereskedelmi központokat, közműveket, egészségügyi intézményt ért kiterjedt ransomware incidens. A megtámadott célpontok hosszú ideig kényszerültek leállni, a mellékelt képen például a Costa Rica-i közegészségügyi központ egy kézzel írt táblán tájékoztat arról, hogy **a kibertámadás miatt rendszerkimaradás várható.**

A hivatalos tájékoztatás szerint 1,500 kormányzati szerverből legalább 30 megfertőződött, a helyreállítás időpontjára egyelőre még becslések sincsenek. Emlékezetes, hogy 2021-ben számos egészségügyi intézmény szenvedett el hasonló támadásokat az Egyesült Államokban a Conti csoport részéről.

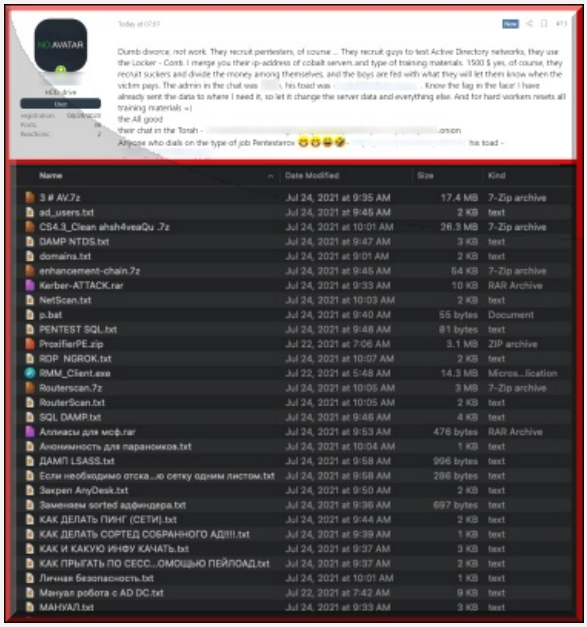


A pénzügyminisztériumi támadás után 10 millió dollárnak megfelelő váltságdíjat követeltek a bűnözők, amelynek megfizetését megtagadták. Ennek következtében a doxinggal, vagyis a titkosítás előtt a bizalmas adatok ellopásával kombinált támadás részeként bosszúból nyilvánosságra hoztak 672 GB megszerzett adatot.

A Conti szivárogtató webhelye további intézményeket is felsorolt, amelyek szintén érintettek egy hasonló támadásban, és ahol nemfizetés esetén ugyanígy nyilvánosságra hozzák majd az ellopott érzékeny adatokat.

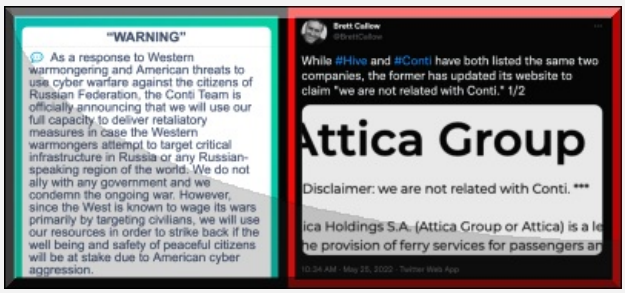
Többek közt érintett a Munkaügyi és Társadalombiztosítási Minisztérium, a Szociális Fejlesztési és Családi Támogatások Alapja, de egyetemek is szerepelnek a listán.

A BleepingComputer előzetes elemzése azt mutatja, hogy nincs szó blöffről, a forráskód és az SQL adatbázisok valóban kormányzati webhelyekről származnak.



Érdekes történés volt 2021. nyarán, amikor egy a Conti csoportnak dolgozó alvállalkozó elégedetlen volt a számára kifizetett részesedéssel, és bosszúból nyilvánossá tette a Conti banda képzési anyagait, stratégiáját és az egyik üzemeltetőjével kapcsolatos információkat is. Ennek ellenére a tevékenységük folyamatos, és **a két oroszországi csoportot az jellemzi, hogy az orosz-ukrán háborúban egyértelműen Oroszország mellett állnak ki,** és mindenkit, aki a támadó agresszor felé diplomáciai, gazdasági megszorító intézkedéseket foganatosít, ellenségnek tekintenek a kibertérben.

Az FBI adatai szerint a Conti csoport elképesztő bevételeket realizált az elmúlt két év alatt, az összeget 150 millió dollárra (57 Mrd HUF) becsülik.



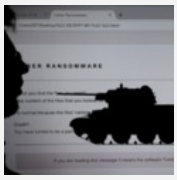
A Costa Rica elleni incidens korábban sosem látott mértékű és irányultságú támadás, ez az első alkalom, ami ilyen fenyegetést hozott egy konkrét ország ellen. Üzeneteikben a kormány megdöntésére szólítanak fel, állítólagos beépített belsős kormányzati embereikről is beszélnek. Független elemzők a kormány megdöntését a súlyos helyzet ellenére sem tartják reálisnak.

Sok latin-amerikai ország nem rendelkezik elegendő technikai eszközzel, szakértelemmel és kiberbűnözés elleni törvényekkel, emiatt nehéz kezelni az állami szektorban az ilyen fenyegetéseket. Igaz, nincs támadhatatlan rendszer, de az biztos, hogy minden szervezetnek egyre erősebb erőfeszítéseket kell tenni, hogy a "*Don't react, prevent!*" szlogen által megfogalmazott elvhez legalább közelíthessenek.

1 komment
Címkék: oroszország politikai támadás rica costa conti ransomware hive zsarolóvírus

Ajánlott bejegyzések:


Kulcs a túléléshez


Ez most vajon akkor milyen ware?


Nem csitulnak a kórházak elleni támadások


Emelkedő ransomware károk

Venus ransomware támadja az egészségügyet

Kommentek:

gigabursch 2022.06.24. 09:24:02

Hmmm
Vajon az offshore paradicsomok bankjai mikor kapnak "átkönyvelést"?

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Fordulat ransomware fronton

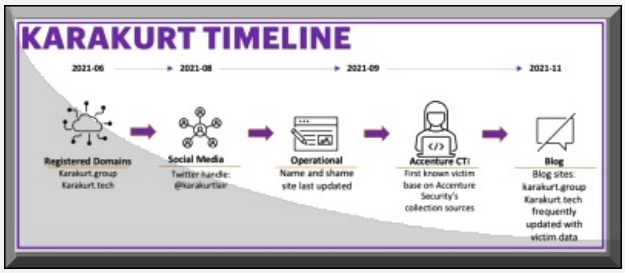
2022. június 27. 11:10 - Csizmazia Darab István [Rambo]

Igen, ezerszer volt már terítéken a téma, sok szempontból körbejártuk, viszont az egyetlen állandó dolog itt is maga a változás. Ami most eléggé gyökeresnek tűnik.

Épp a közelmúltban vettük végig a zsarolóvírusok evolúcióját, amely a 2013-as klasszikus CryptoLockerrel rúgta be az ajtót, és 1024 vagy 2048 bites RSA kulccsal történő titkosítással, váltságdíj követeléssel szorította sarokba a felhasználókat. **Az alapképlet a felhasználó adatok elkódolásából, majd határidős pénzkövetelés kriptovalutában lépésekből állt, igaz a feloldókulcs küldése a váltságdíj fizetését követően vagy megvalósult vagy nem.**

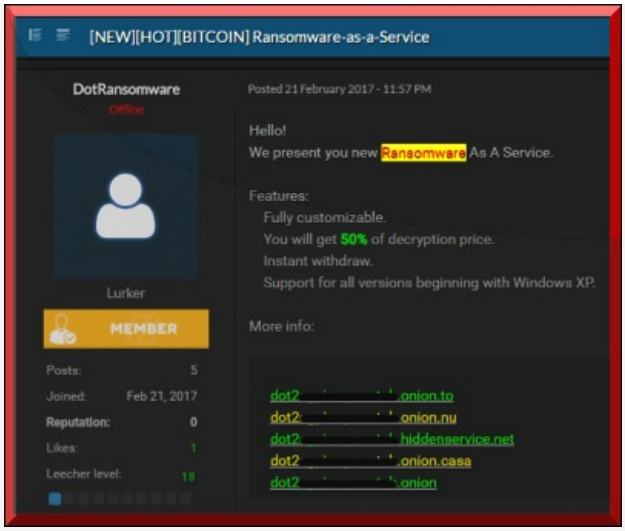
Erre rakódott rá aztán később sok minden: backupok, árnyékmásolatok célzott törlése, agresszív terjeszkedés a belső hálózaton brute force segítségével. Majd egy idő után jött a doxing, vagyis a bizalmas adatok ellopása a titkosítás előtt, és fenyegetés a publikálással.

Ez változott meg a szakértők szerint pár hónapja, ugyanis látszólag **már nem bíbelődnek a támadók titkosítással, elkódolással,egyedi feloldó kulcsokkal, hanem ezeket az elemeket teljesen kihagyva elsősorban direktben az adatlopás és a nyilvánosságra hozással való fenyegetés az új zsarolási irány, ahol egy kis rész mintát rögtön fel is tesznek a netre, a váltságdíjat pedig azért követelik, hogy minden ellopott adat ne kerüljön fel ugyanígy a kiszivárogtatási oldalakra.**



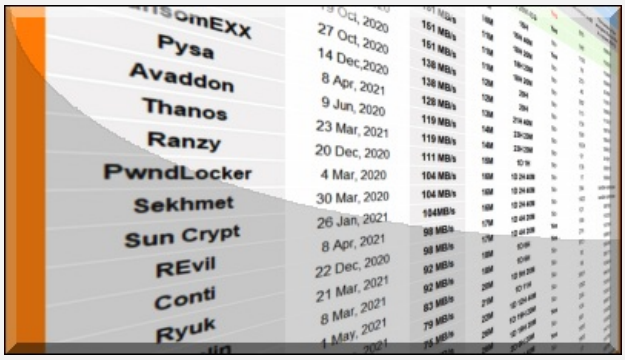
Ennek a vonalnak **az egyik szereplője a Karakurt csoport, amely látszólag nem céloz meg egyetlen konkrét ágazatot vagy iparágat sem, ám az új módszer alapján az áldozatok egyetlen dokumentumát sem titkosították.** Ehelyett a csalók azt állítják, hogy ellopták a bizalmas adatokat, képernyőképeket és fájl másolatokat töltenek fel bizonyítékként, és azzal fenyegetnek, hogy eladják vagy nyilvánosan kiszivárogtatják a teljes adatállományt, ha nem kapják meg a követelt összeget.

Az FBI szerint a váltságdíj követelések összege 25 ezer és 13 millió dollár értéknek megfelelő Bitcoin között mozognak, és Karakurt banda általában egyhetes határidőt tűz ki a fizetésre.



A Ransomware as a Service modell sajnos egyre inkább terjedőben van, és a kifinomultabb, a felhasználóra mind nagyobb pszichés nyomást helyező taktikák, technikák megjelenését hozták a nyakunkra.

Egy korábbi posztban már volt egy olyan ransomware sebességteszt, amelyben ezek a kártékony programok mérték össze egymással a tudásukat egy 53 GB méretű adatmennyiségen. A 2022. márciusi eredmények alapján **az abszolút győztes a LockBit lett, egészen elképesztő 5 perc 50 másodperces eredményével. Ami a "leggyengébb" szereplőnek is 40-50 percbe telt**, és sajnos még ezek is nagyon gyorsak.



Addig is **marad a megelőzés, védekezés területén a rendszeres hibajavító frissítések letöltése, futtatása, hiszen az egyik leggyakoribb fertőzési módszer a már ismert, de foltozatlan sebezhetőségek aktív kihasználása, és nem a zeroday sérülékenységek vásárlása**.

A hálózati és technikai védelmen felül szükséges még a munkavállalók rendszeres biztonságtudatossági képzése (adathalászat, shadow it, stb.), valamint kiberbiztonsági szabályozás, vészhelyzeti protokoll, krízis kommunikáció, és hasonló elemek, mert a helyzet egyre jobban eszkalálódik.

Szólj hozzá!
Címkék: zsarolás váltságdíj publikálás adatlopás adatszivárgás ransomware zsarolóvírus doxing

Ajánlott bejegyzések:

Van másik!

"Illetéktelen fél korlátozott ideig hozzáférhetett fájlokhoz"


Persze hogy tudtam, csak nem sejtettem...

Járulékos következmények szevasztok


Nem szállunk rendelkezésére II.

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei

Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

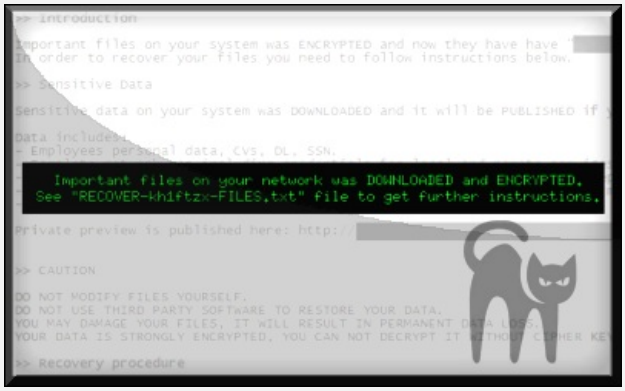
Belépés
Regisztráció

Baljós árnyak: fekete macska Karintiában

2022. június 30. 16:09 - Csizmazia Darab István [Rambo]

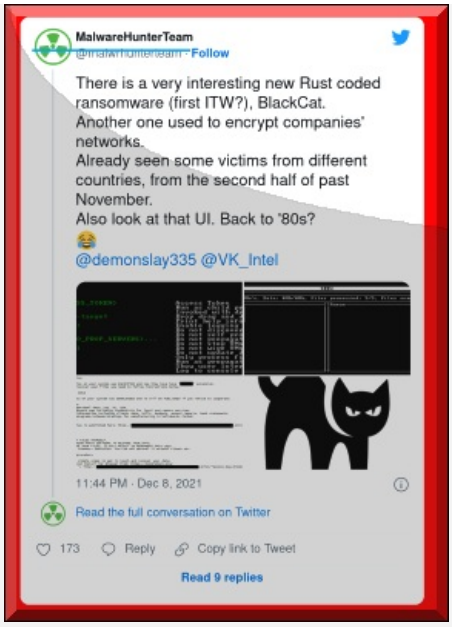
Alig pár nap telt csak el Costa Rica elleni zsarolóvírus támadás óta, máris újabb incidens debütált a láthatáron. Közvetlen szomszédunk, Ausztria a helyszín, és a szövetségi tartományok közül ezúttal Karintia került a célkeresztbe.

Az incidens még a múlt hét kedden történt, és a tartomány honlapja, valamint a teljes számítógépes rendszer leállt. A támadást a BlackCat (alias ALPHV) csoport vállalta magára, és váltságdíjként 5 millió dollárnak (kb. 1.9 mrd forint) megfelelő összeget követeltek egy olyan visszafejtő eszközért, amellyel állítólag rövid idő alatt helyreállhatna a működés. Értesülések szerint ennek megfizetését Karintia megtagadta.



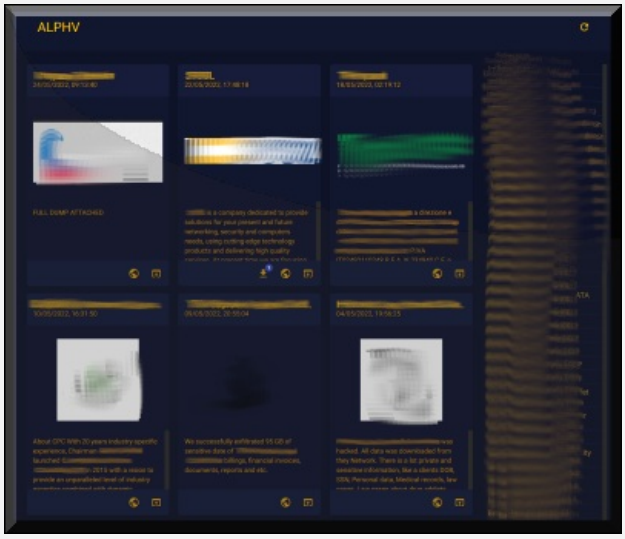
Jelenleg több ezer munkaállomás volt kénytelen leállni, a hivatalos weblap mellett működképtelen az e-mail szolgáltatás, és a teljes adminisztráció, így például **szünetel a COVID-19 tesztek feldolgozása, útlevélkiadás, közlekedési bírságok és egyéb hivatalos ügyek intézése.**

A Bleeping Computer cikke szerint **jelenleg nem találhatók ellopott és nyilvánosságra hozott adatok a banda szivárogtatási webhelyén, ami jelentheti az is, hogy a doxing, vagyis az adatlopás nem volt sikeres, de az is lehetséges, hogy a háttérben esetleg folyik egyfajta alku, ami még nem zárult le.**



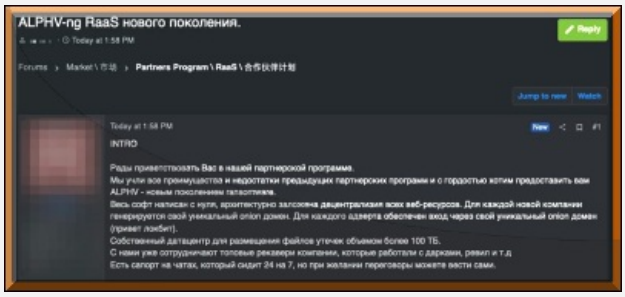
A 2021. novemberében megjelent, és azóta erőteljesen feltörekvő BlackCat csoportnak hosszú bűnlajstroma van, **több tucat zsarolóvírus támadást hajtottak már végre**, amikben Bitcoinban és Moneroban követeltek pénzt.

A kártevőt a szokásos C/C++ helyett Rust nyelven programozták, és mertek nagyot álmodni, mert a célbavett rendszerek között találjuk nem csak a Windows, hanem a Linux és VMWare ESXi platformokat is.



Hogy mennyire kifinomult kártevőről van szó, azt jól mutatja az az információ, ami egy fórumbejegyzésben olvasható. Eszerint **az elkódolás, titkosítás több különböző módon történhet.** A fájl teljes titkosítása nyilván számukra a legbiztonságosabb, de egyben a leglassabb is. A gyors módszert más bandák is alkalmazzák, ahol az első N megabyte titkosítása történik meg, de ezzel is sikeres a károkozás, és roppant gyors. Nem ajánlott használni, a lehető leginkább bizonytalan megoldás, de a leggyorsabb.

Az úgynevezett DotPattern módszeren kívül létezik még **az automatikus mód, ahol pedig a fájl típusától és méretétől függően választják ki a legjobb stratégiát a sebesség/biztonság szempontjából**. Ez azt mutatja, hogy ez a banda mennyire fejlett más bűnözői csoportokhoz képest.



Bár **még nem tudni, hogy az osztrák Karintia szövetségi államot megcélzó BlackCat támadás célzott vagy véletlenszerű volt-e**, az ilyen jellegű, kritikus adatokkal dolgozó állami hivatalok általában szerényebb biztonsági költségvetéssel rendelkeznek, mint a magánszektor.

Így **elképzelhető, hogy egy tárgyalási folyamat végén hajlandóak lesznek kifizetni a követelt váltságdíjat, különösen ha az adatlopás sikeres volt, és nem csak a hosszabb kiesést és adatvesztést nem akarják kockáztatni, hanem az adatok nyilvánossá tételét is el akarják kerülni.**

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: ausztria követelés váltságdíj államigazgatás karintia ransomware blackcat zsarolóvírus doxing alphv

Ajánlott bejegyzések:

Nem szállunk rendelkezésére II.

Közeleg a tél, érzékeny ponton támadnak a zsarolóbandák

LockBit vs. olasz adóhivatal

Fordulat ransomware fronton

Rossz gondolatok a könyvtárban

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

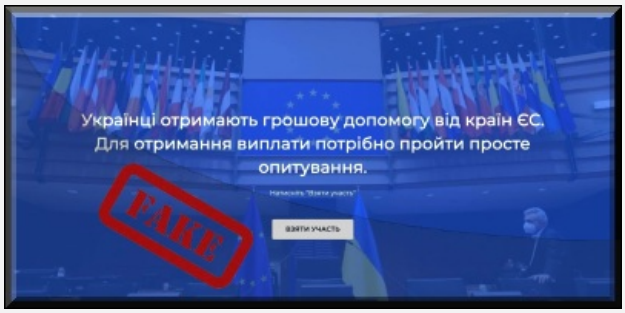
accountz

Belépés
Regisztráció

Adathalászok lakat alatt

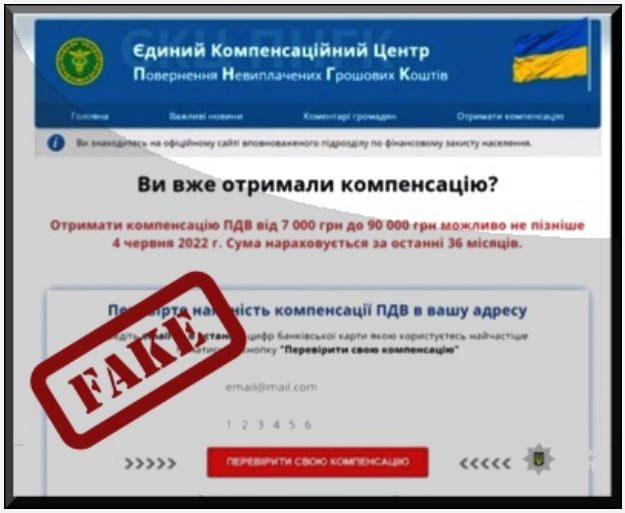
2022. július 05. 09:51 - Csizmazia Darab István [Rambo]

Az adathalászat amúgy is egy komoly bűncselekmény, ám igazán visszataszító formája az a mód, amikor szerencsétlen, kiszolgáltatott, bajban lévő emberek megsegítését ígérik a csalók, ám ehelyett a segélyre várók számláit ürítik le.



Az orosz-ukrán háború még inkább felpörgette a kibertámadásokat, mert ezt megelőzően is volt belőlük jócskán.

Már a háború kezdetén, márciusban is írtunk azokról az átverésekről, visszaélésekről, amelyben hamis adományozási felhívásokkal igyekeztek kihasználni a csalók a jóhiszemű felhasználók segítőkészségét, együttérzését, sajnálatát.

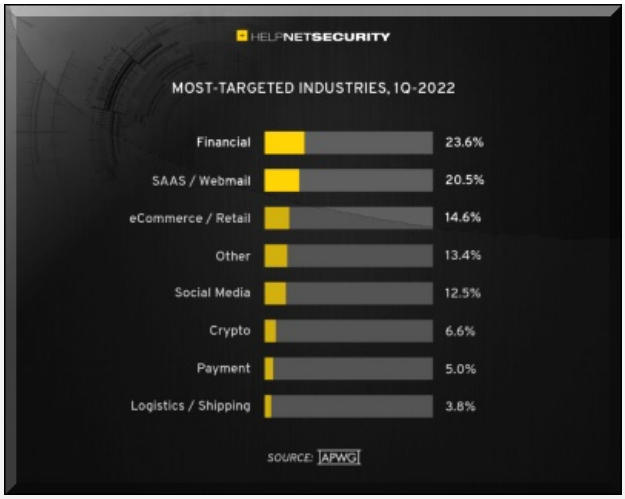


Ezúttal **az ukrán kiberrendőrség ütött rajta egy olyan bűnbandán, amely több, mint 400 adathalász oldalt** hozott létre. Ezeken azt hazudták, hogy a weboldalak célja, hogy **az EU nevében pénzügyi segítséget nyújtsanak a háborús helyzet miatt rászoruló ukrán állampolgároknak. Valójában az adakozók pénzügyi adataira utaztak, és a megszerzett személyes és bankkártya adatok birtokában megkárosították a felhasználókat.**

A teljes kárt 100 millió hrivnya, vagyis **nagyjából 1.3 milliárd forintnak megfelelő összeget loptak el a számlákról, a károsultak száma pedig meghaladja az ötezret**. A kártékony weboldalakra mutató linkeket e-mail spamként, SMS üzenetben terjesztették, de a közösségi médiákban is, hamis reklám bannerekkel, illetve keresési találatok mérgezésével is terítették ezeket.

A 9 személy letartóztatásáról a rendőrség videófelvételt is közölt a legnagyobb videómegosztó oldalon, ahol számítógépeket, mobiltelefonokat, bankkártyákat és készpénzt foglaltak le a gyanúsítottaktól. Jevgenyij Doroganov, a Kiberrendészeti Osztály egyik vezetője szerint **az elkövetők akár 15 év börtönt is kaphatnak.**

Külön érdekessége a felvételnek, ahogy **egy több ponton záródó fém biztonsági ajtót nyitnak fel, mint egy halkonzervet, de az is meghökkentő, milyen spártai, lepukkant lakásban** dolgoztak a bűnözők.



Az adathalászat mértéke egyébként folyamatosan növekvő tendenciát mutat, és természetesen a pénzügyi területet célzó átverések vezetik a listát. A korábbi posztunk végén összefoglaltuk azokat a fontos tudnivalókat, amelyekkel megelőzhetjük, hogy ehhez hasonló módszerekkel átverhessenek bennünket.

Röviden ehhez óvatosság, biztonságtudatosság és egészséges gyanakvás is szükséges, és az ott leírt ma is aktuálisan érvényes részletes jótanácsokat pedig érdemes jól az eszünkbe vésni, na meg a netes tranzakciókhoz kizárólag virtuális kártyát használni.

Szólj hozzá!
Címkék: ukrajna csalás átverés segély phishing adathalászat banki adatlopás

Ajánlott bejegyzések:


A bankos mindig kétszer csenget...


Ingyenes Omikron teszt vagy mégsem?

Ismét csomagunk érkezett - vagy mégsem?

Tagsági kérdések - vagy mégsem?


Viva la Revolut

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.

VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

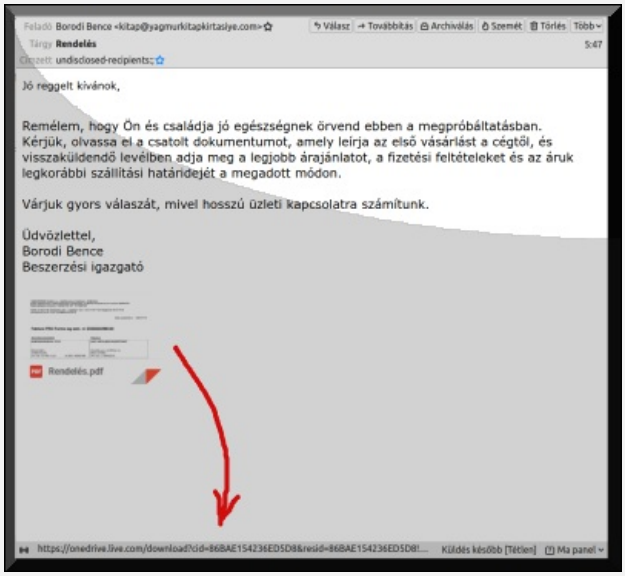
Igazgató-e vagy?

2022. július 07. 09:39 - Csizmazia Darab István [Rambo]

Régebben eseményszámba ment, ha valódi magyar, vagy csak "hunglish" nyelvű spam érkezett a postafiókunkba. A Fülig Jimmy-s és Tuskó Hopkins-os fogalmazásoknak már lassan tényleg vége, ám furcsa próbálkozások azért néha még most is felbukkannak.

Egy új átverés szerint rendelnének tőlünk, erről maga Borodi Bence, beszerzési igazgató tájékoztat egy kéretlen e-mailben, remek hír, jaj de jó. Ráadásul úgy tűnik volt neki gyerekszobája, és nem a ló nézett be rajta, mert elsőként köszön, sőt még a családunk egészsége felől is illendően tudakozódik. **Saját magával kapcsolatban azonban már eléggé szűkszavú, például azt sem tudjuk meg, pontosan melyik cégtől is keres bennünket.** Hogy mit is rendelnének, azt is homály fedi.

Bár a feladó címe "kitap KUKAC yagmurkitapkirtasiye PONT com", de **az e-mail trace szerint a németországi Falkensteinből írtak nekünk. A feladó domain adatai viszont ezzel szemben egyértelműen Törökországra** utalnak. Azért a rend kedvéért azt is vegyük észre, hogy **nem mi vagyunk itt a mélyen tisztelt és nagyra becsült egyedüli címzettek, hanem sima körlevélként az "undisclosed-recipients:;" szerepel**, vagyis ez egy tömegesen terjesztett spam kampány részének látszik.



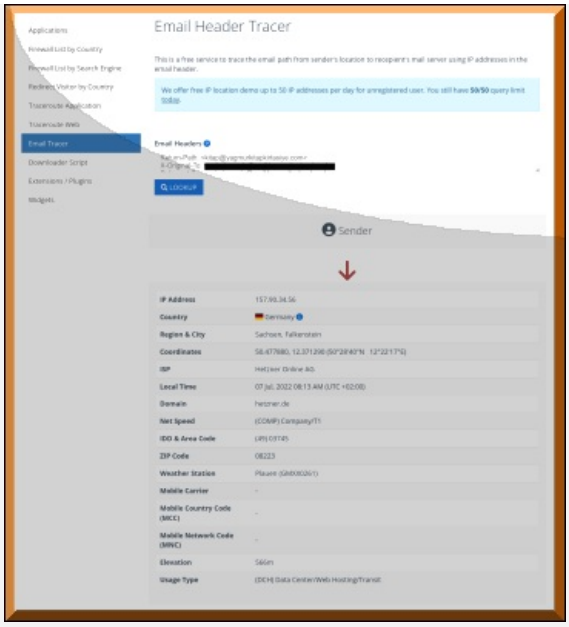
A levél teljes szövege a következő:

"*Jó reggelt kívánok,*

Remélem, hogy Ön és családja jó egészségnek örvend ebben a megpróbáltatásban.
Kérjük, olvassa el a csatolt dokumentumot, amely leírja az első vásárlást a cégtől, és visszaküldendő levélben adja meg a legjobb árajánlatot, a fizetési feltételeket és az áruk legkorábbi szállítási határidejét a megadott módon.

Várjuk gyors válaszát, mivel hosszú üzleti kapcsolatra számítunk.

Üdvözlettel,
Borodi Bence
Beszerzési igazgató"

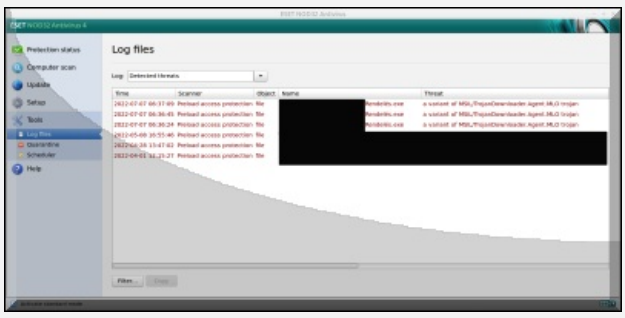


Szép alliteráció: Borodi Bence Beszerzési. **A melléklet viszont, ami a képernyőképen hamisan PDF-nek, azaz hordozható dokumentum formátumnak van ábrázolva, nem valós információ**, ugyanis az valójában a "Rendelés.tgz" fájlra mutat egy valószínűleg feltört OneDrive fiókban.

Ebben pedig egy szintén ékezetes nevű "Rendelés.exe" bontható ki. Na és vajon mit küldött ebben nekünk az állítólagos török-német nagyságos igazgató úr? Hát nem árajánlat kérést, annyi biztos, ez itt már a spoiler helye.

Ha feltoljuk ezt a Windows alatti futtatható .exe állományt a VirusTotal oldalra, **akkor már látható, hogy egy trójai letöltő kártevőt próbáltak meg ránk sózni.** A ma reggeli állapot szerint egyelőre csak 12 AV motor detektálta a kártékony kódot.

Az eredete talán az lehet, hogy egy angol nyelvű, vállalkozásokat segítő legitim próbálkozást igyekeztek a csalók magyarra átültetni, és a Covid19 valamint az orosz-ukrán háború gazdasági mellékhatásaiban megroggyant KKV-k számára **egy reménnyel kecsegtető rendelést, hosszú távú együttműködést csalinak belengetni.**



Volt akkor itt minden szokásos trükk, hogy kattintásra bírják a címzetteket: a látszólag PDF fájltípussal kapcsolatos megtévesztés, hamis feladó, tömegesen kiszórt üzleti levél, reménybeli megrendelés, és kártékony melléklet, aminél persze **a naprakész vírusvédelem szerencsére rögtön felismer, blokkol, töröl.**

A 4xx forintos euró válságos időszakából sajnos nem az ilyen kamu beszerzési igazgatók fognak kihúzni bennünket a

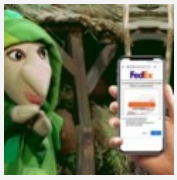
recessziót egy állítólagos zsíros megrendeléssel. Tegye fel a kezét, aki ezen komolyan meglepődött! **Viszont reméljük, ennyi gyanús intő jel mellett már nem kattintott rá senki.**

5 komment
Címkék: spam magyar igazgató csalás átverés trójai kártevő virustotal beszerzési

Ajánlott bejegyzések:


MKB adathalászat szigonnyal, horoggal, hálóval


Csomagja kézbesítésre vár! Vagy mégsem?


Sárkány ellen sárkányfű


Üdvözlünk Sin City-ben


VPN appok Androidra vagy mégsem?

Kommentek:

Head Honcho 2022.07.09. 07:30:52

Én kérek elnézést, Saul Goodman egy becsületes zugügyvéd. :)

Válasz erre

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2022.07.09. 07:55:04

Szívemből szóltál kedves Honcho, én is roppant mód szeretem :-)

Válasz erre

Head Honcho 2022.07.10. 09:18:34

(Jó volna látni szinkronosan az utolsó évadot, de a hárombetűs kanálisnak "hála", se híre - se hamva ennek eddig.)

Válasz erre

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2022.07.10. 11:58:06

A 6-ost még nem is néztem, de az addigiak nagyon rendben voltak.

Ha nincs a 3 betűsön, nézd meg az 5 betűsön ;-)

Válasz erre

Head Honcho 2022.07.10. 20:57:05

Az AMC-re gondoltam, és hát ők rendelik a szinkront, már ha egyáltalán. De roppant következetlen, hogy az eddigieket leszinkronizálták és sugározták is (mindezt az amerikai premierhez képest rendre mindössze pár napos eltéréssel), most pedig szó sincs róla...

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Antivírusblog
245 követő

Oldal követése Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

Kiberbiztonsági útikalauz diákoknak

2022. július 12. 11:28 - Csizmazia Darab István [Rambo]

Egy friss felmérés szerint csak minden ötödik magyar diák érzi magát biztonságban neten. Az eredmények alapján a fiatalok az adathalászattól, személyazonosság-lopástól és profil feltöréstől tartanak a leginkább.

A szünidő beköszöntével a diákok a szokásosnál is több időt töltenek az interneten, ahol számos veszély leselkedhet rájuk. Egy friss felmérés szerint **a magyar fiatalok túlnyomó többsége az adathalászattól, személyazonosság-lopástól és a profiljai feltörésétől tart a neten.**

Európa egyik vezető kiberbiztonsági vállalata, az ESET adatai szerint **a diákok harmada úgy gondolja, hogy kifejezetten tájékozott a kiberbiztonságot érintő kérdésekben, kétharmaduk pedig ismerni véli a főbb veszélyeket és védekezési módokat.** Sajnos a bűnözők egyre kreatívabb módszerekkel keresik meg a diákokat, ezért az alábbiakban sorra vesszük a fiatalokra leggyakrabban leselkedő veszélyeket és tippeket adunk a biztonságosabb netezéshez.

A felmérés szerint csak minden ötödik magyar diák érzi magát biztonságban neten. **A legtöbben (78%) az adathalászattól, személyazonosság-lopástól és profil feltöréstől tartanak. A diákok többsége (54%) fél a kártékony programoktól, kéretlen levelektől és rosszindulatú appoktól, és minden második diák tart attól, hogy online vásárlás miatt kerülhet bajba.**

A felmérésben résztvevő diákok amiatt is aggódnak, hogy bizalmas információk, képek szivárognak ki róluk a közösségi médiában (43%), cyberbullying, azaz online zaklatás és gyűlöletkeltés áldozatává válnak (35%), vagy online ragadozók környékezik meg őket (28%).

A gyerekek - és persze a felnőttek is - **minden olyan eszközön ki vannak téve a kiberbűnözőknek, amely**

internetkapcsolattal rendelkezik. Itt nem elég a számítógépre, tabletre és az okostelefonra gondolni, hiszen az okosóráktól kezdve a játékkonzolokig számos egyéb eszköz is internetkapcsolattal működik.

A kiberbűnözők célja pedig az, hogy az eszközök biztonsági réseit, illetve a felhasználók óvatlanságát kihasználva olyan bizalmas adatokhoz jussanak, amelyekkel meglophatják, megkárosíthatják, megzsarolhatják az áldozatokat.

A bűnözők előszeretettel szerzik meg a fiatalok jelszavait, azonosító számait, hitelkártya-, vagy társadalombiztosítási adatait, hogy azokat **a legkülönbözőbb törvénytelen célokra használják, például hiteligénylésre, vagy nagy értékű internetes vásárlásra.**

A csalók gyakran keresik meg a fiatalokat olyan - nem létező - luxustermékekkel, amelyeket hamis webáruházakban "árulnak", illetve **csali állás- és ösztöndíjajánlatokkal, melyekért részletes személyes adatokat, sőt ezen felül akár állítólagos "regisztrációs vagy feldolgozási díjat" is kérnek.**

A korosztály nem csak az anyagi, hanem **a lelki természetű veszélyeknek is ki van téve, elég csak az online zaklatásra, azaz a cyberbullyingra gondolni. Ilyenkor jellemzően rosszindulatú, sértő, lejáró üzeneteket osztanak meg egy fiatalról a közösségi oldalakon, chat alkalmazásokban, fórumokon, vagy akár online játékok csevegőiben, ami az egyik, legnehezebben kezelhető pszichés kihívás.**

Szintén kifejezetten veszélyesek a "szerelmi csalók" és "bizalmas barátok", akik gyakran a közösségi médiában adják ki magukat olyan társkereső személynek, aki a kiszemelt áldozatnak - a róla elérhető információk alapján - valószínűleg tetszeni fog. **Ha sikerül a kapcsolatfelvétel, privát üzenetekben igyekeznek bizalmas viszonyba kerülni, hogy pénzt csaljanak ki, vagy ami még veszélyesebb, hogy személyes találkozókra** vegyék rá a fiatalokat.

Az alábbi trükkökkel túljárhatunk az online csalók eszén.

- Használjunk otthoni, iskolai hálózatot, vagy mobilnetet, vagy virtuális magán hálózatot (VPN), ami titkosítani fogja az összes adatot. Kerüljük a jelszóval nem védett nyilvános Wi-Fi kapcsolatokat.

- Ne tegyük nyilvánosan elérhetővé a saját, illetve az ismerőseink személyes adatait a közösségi médiában, legyen szó nevekről, születési dátumokról vagy földrajzi elérhetőségről.

- Gyanakodjunk, ha e-mailben személyes információkat kérnek tőlünk, hiszen a bankok, szolgáltatók nem így szokták felvenni az adatainkat.

- Alapszabály, hogy a neten, ami túl szép ahhoz, hogy igaz legyen, az általában átverés. Igaz ez olcsó termékekre, irreálisan jól fizető állásokra és túlságosan könnyen megszerezhető ösztöndíjakra is.

- Ha online zaklatnak minket, ne reagáljunk indulatból, hanem készítsünk mentéseket, képernyőképeket a bántó üzenetekről, hogy a későbbiekben bizonyítani tudjuk az online zaklatás tényét. Fordulhatunk szüleinkhez, tanárainkhoz, a szolgáltató ügyfélszolgálatához vagy tegyünk bejelentést a Nemzeti Média- és Hírközlési Hatóság oldalán.

- Ha egy idegen chatüzenetekben próbál kapcsolatba lépni velünk és rövid időn belül szerelmet is vall, vagy mély barátságról számol be, akkor ott valami nagyon gyanús, legyünk óvatosak! Akár egy gyors, kép alapján történő inverz kereséssel is kiderülhet, hogy valós, vagy esetleg közismerten veszélyes személlyel van-e dolgunk.

- Gondoljuk meg alaposan, kivel osztjuk meg a webkameránk képét, és ha nem használjuk, mindenképp takarjuk le és/vagy kapcsoljuk ki.

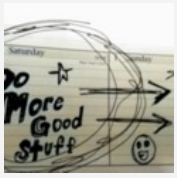
- Ha okosórát veszünk, járjunk utána, hogy a gyártó garantálja-e a titkosított kommunikációt az eszköz és a szerverei között!

- Használjunk olyan internetbiztonsági megoldást, amely szoftveres szinten képes védeni az eszközeinket, ilyen például az ESET Internet Security, amelyet ingyenesen is ki lehet próbálni.

Az ESET kifejezetten a diákok számára kiberbiztonsági kisokost is összeállított, amely innen letölthető. Az összefoglaló nem csak a diákok, hanem a szülők és pedagógusok számára is hasznos segítség lehet az internetes biztonságot érintő kérdésekben, legyen szó védekezésről vagy megelőzésről.

Szólj hozzá!
Címkék: iskola diák összefoglaló útmutató tippek fiatalok eset veszélyek kiberbiztonság biztonságtudatosság

Ajánlott bejegyzések:



10 kiberbiztonságra veszélyes szokás


10 gyakori IT biztonsági hiba


Iskolák a kiberbűnözők célkeresztjében

Böngészés - kockázatok és mellékhatások


10 alaplépés a biztonsághoz

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

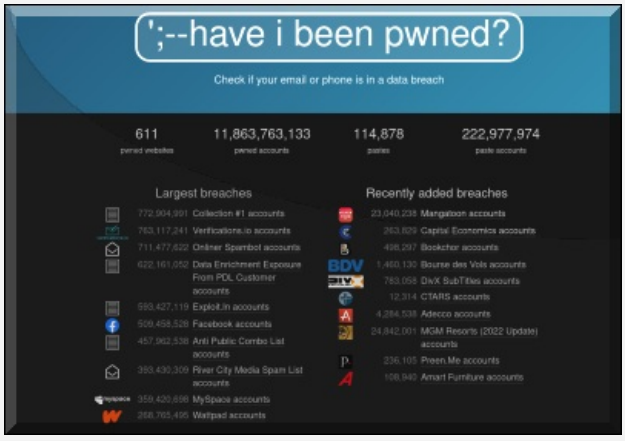
Drágán add a bankkártyád!

2022. július 14. 08:40 - Csizmazia Darab István [Rambo]

Bemutatunk néhányat **a leggyakoribb módszerek közül**, amelyekkel a hackerek megszerezhetik a bankkártyánk adatait, egyúttal **tippeket adunk arra is, hogyan védhetjük ki** ezek a támadásokat.

A kiberbűnözés egy olajozottan működő gépezet, amely évente dollárbilliókban mérhető károkat okoz. A bűnüldöző szervek és a legtöbb felhasználó elől rejtett módon, **a darkweben működő oldalakon a kiberbűnözők nagy mennyiségű lopott adatot, valamint az ezek megszerzéséhez szükséges hackereszközöket adnak-vesznek.**

Feltételezések szerint jelenleg 24 milliárd illegálisan megszerzett felhasználónév és jelszó kering ezeken az oldalakon. **A legkeresettebbek közé tartoznak a friss kártyaadatok, amelyeket a csalók nagy tételben vásárolnak meg, hogy személyazonossággal való visszaélést kövessenek el.**



Azokban az országokban, ahol Chip and PIN, más néven EMV biztonsági rendszert vezettek be, nehéz a bűnözőknek az adatokat klónozott kártyákká alakítani. **Ezért leggyakrabban online használják azokat, kártyát nem igénylő (CNP) támadásokhoz. A csalók gyakran luxuscikkeket vásárolnak az adatok segítségével vagy nagy mennyiségben vesznek ajándékutalványokat** – ez is egy népszerű módja a jogellenesen szerzett pénzek tisztára mosásának.

Nehéz pontosan felbecsülni az ilyen kártyák piacának méretét. **A világ legnagyobb alvilági piacterének üzemeltetői viszont nemrégiben nyugdíjba vonultak, miután becslések szerint 358 millió dollárt kerestek.**

Az ESET kutatói bemutatják **az 5 leggyakoribb módszert, amelyekkel a hackerek megszerezhetik a kártyaadatokat**, és tanácsokat is adnak arra vonatkozóan, **hogyan lehet kivédeni, megelőzni a kártyaadatok megszerzéséért indított támadásokat:**

1. Adathalászat
Az adathalászat a kiberbűnözők egyik legnépszerűbb adatlopási módszere. A legegyszerűbb trükk, amikor a hacker egy legitim szervezetnek (például banknak, e-kereskedelmi cégnek vagy műszaki vállalatnak) adja ki magát, hogy rávegye a felhasználót a személyes adatok megosztására vagy rosszindulatú szoftverek letöltésére. **Gyakran arra ösztönzik áldozatukat, hogy kattintsanak egy linkre vagy nyissák meg a csatolmányt.** Ezáltal a felhasználó egy adathalász oldalra juthat, ahol személyes és pénzügyi adatok megadására kérik. Az adathalászat 2022 első negyedévében minden eddiginél magasabb szintet ért el a statisztika szerint.

444

Az ESET adatai alapján ezek az átverések az elmúlt években továbbfejlődtek. **Manapság már előfordulhat, hogy e-mail helyett egy kártékony sms-t kap az áldozat a hackertől, aki egy futárszolgálatnak, kormányhivatalnak vagy más megbízhatónak tűnő szervezetnek adja ki magát.**

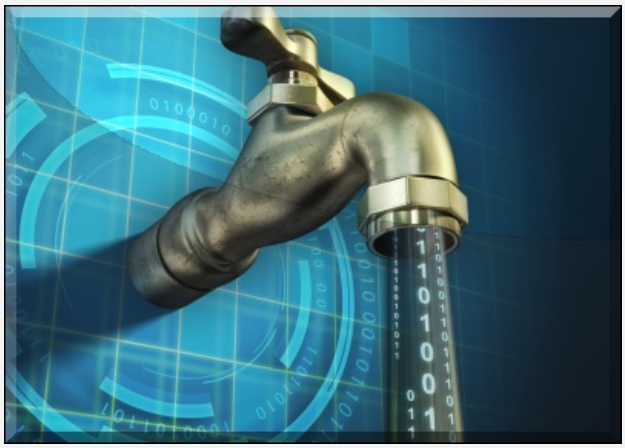
A csalók akár fel is hívhatják az embereket, hogy megerősítsék, valóban megbízhatóak, és így próbálnak kártyaadatokat megszerezni az áldozatoktól. Az sms-ben történő adathalászattal (smishing) összefüggő esetek száma 2021-ben több mint kétszeresére nőtt az azt megelőző évhez képest, míg a hangalapú adathalászat (vishing) szintén jócskán megugrott egy felmérés szerint.

2. Kártevő szoftverek
A kiberbűnözői alvilág hatalmas piac, nemcsak az adatok, hanem a kártevő szoftverek tekintetében is. Az évek során különböző típusú kártékony programokat fejlesztettek ki információlopásra. **Ezek közül néhány a billentyűleütéseket rögzíti – például amikor a kártyaadatokat gépeljük be egy webshopban vagy banki oldalon.** Hogyan telepítik a bűnözők ezeket az eszközöket a felhasználók gépeire?

Az adathalász e-mailek vagy sms-ek népszerű módszernek számítanak, ahogyan a kártékony online hirdetések is. Más esetekben népszerű weboldalakat fertőznek meg, és megvárják, hogy a felhasználók felkeressék azokat. Ezek a Drive-by-download típusú kártevő szoftverek azonnal települnek az eszközökre, amint valaki meglátogatja a fertőzött weboldalt. **Az információtolvaj szoftverek pedig gyakran valódinak és megbízhatónak tűnő, de valójában rosszindulatú mobilalkalmazásokban is megtalálhatóak.**

3. Digitális "lefölözés"
Az ESET figyelmeztetése szerint előfordul az is, hogy **a hackerek kártékony szoftvereket telepítenek az e-kereskedelmi cégek fizetési oldalaira.** Ezek láthatatlanok az áldozat számára, de képesek megszerezni a bankkártya-adatokat azok beírásakor.

A felhasználók itt látszólag nem sokat tehetnek adataik biztonsága érdekében, azon túl, hogy csak nagynevű márkáktól és neves weboldalakon vásárolnak, amelyek valószínűleg biztonságosak. **A digitális "lefölözéses" (digital skimming) esetek száma 150 százalékkal nőtt 2021 májusa és novembere között.**



4. Adatsértések
Olykor a kártyaadatokat közvetlenül azoktól a vállalatoktól lopják el, amelyektől a felhasználó vásárol, legyen szó egészségügyi szolgáltatóról, e-kereskedelmi áruházról vagy éppen utazási irodáról.

A hackerek szempontjából ez egy **költséghatékony módszer, mivel egyetlen támadással hatalmas adathalmazhoz juthatnak hozzá.**

5. Nyilvános Wi-Fi
Utazás közben **csábító lehet ingyenesen használni a világhálót a nyilvános Wi-Fi hotspotokon keresztül a repülőtereken, szállodákban, kávézókban és más közösségi terekben**. Viszont még akkor sem lehetünk biztosak abban, hogy a kapcsolat biztonságos, hogyha fizettünk azért, ugyanis hackerek is használhatják a hozzáférést, hogy kémkedjenek az adatok után, miközben a felhasználó beírja azokat az eszközébe.

Hogyan tartsuk biztonságban kártyaadatainkat? Szerencsére számos módja van annak, hogy csökkentsük az adatlopások kockázatát. Mindenképp érdemes az alábbiakat figyelembe venni:

- Maradjunk éberek: soha ne válaszoljunk kéretlen e-mailekre, ne kattintsunk az abban szereplő linkekre, és ne nyissuk meg az ilyen e-mailek csatolmányait. Könnyen lehet, hogy kártevő szoftvereket tartalmaznak, vagy olyan hitelesnek tűnő adathalász oldalakra vezethetnek, ahol az adatok megadását kérik.

- Ne osszunk meg információt idegenekkel, akkor sem, ha a beszélgetőpartner meggyőzőnek hangzik. Kérdezzük meg, honnan hívnak bennünket, majd keressük fel az említett szervezetet, hogy ellenőrizhessük a hívás valódiságát. Ne használjuk az ismeretlen által megadott elérhetőségeket.

- Ne használjunk nyilvános Wi-Fi hálózatot, különösen virtuális magánhálózat (VPN) nélkül. Amennyiben muszáj csatlakoznunk, ne csináljunk semmi olyat a hálózaton, amihez kártyaadatokat kell megadni (például online vásárlás).

- Ne mentsük el a kártyaadatokat online vásárlás során, még akkor sem, ha ezzel időt takarítanánk meg a későbbi tranzakciók esetében. Így csökkenthető annak az esélye, hogy megszerezzék bankkártyaadatainkat, amennyiben az adott cég fiókját feltörik vagy megtámadják.

- Töltsünk le minden számítógépünkre és eszközünkre (például mobiltelefonokra vagy táblagépekre) **kártékony programok és adathalászat elleni védelmet** egy megbízható és elismert biztonsági szolgáltatótól.

- Használjunk kétfaktoros hitelesítést bizalmas fiókjainknál. Ez csökkenti annak az esélyét, hogy hackerek lopott jelszavakkal feltörjék azokat.

- Csak megbízható alkalmazásokat árusító boltból töltsünk le applikációkat (Apple App Store, Google Play)

- Amennyiben online vásárolunk, csakis HTTPS protokollal rendelkező oldalakon keresztül tegyük azt (ez esetben a böngésző címsorában az URL-cím mellett egy lakatnak kell megjelennie). Így kisebb az esélye annak, hogy adataink illetéktelen kezekbe kerülnek.

Végül pedig jó módszer, ha figyeljük az összes bank- és kártyaszámlánkat. Ha gyanús tranzakciót észlelünk, azonnal értesítsük bankunk vagy kártyaszolgáltatónk csalással foglalkozó munkatársait. Egyes alkalmazások már lehetővé teszik, hogy befagyasszuk minden kiadásunkat bizonyos kártyákon, amíg meg nem bizonyosodunk arról, hogy valóban történt-e biztonsági incidens.

Rengeteg módja van annak, hogy a bűnözők megszerezzék kártyaadatainkat, de mi magunk is sokat tehetünk azért,

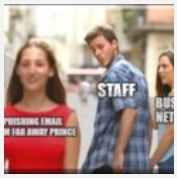
hogy megállítsuk őket.

Szólj hozzá!
Címkék: biztonság bank bankkártya megelőzés védekezés adathalászat pénzintézet utalás

Ajánlott bejegyzések:


A bankos mindig kétszer csenget...


10 alaplépés a biztonsághoz



10 gyakori ok, amiért bedőlünk a csalásoknak


7 tipp a mobilunk védelméhez


Mai szavunk pedig: biztonsági fásultság

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook


Antivírusblog
245 követő

Oldal követése Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.

VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

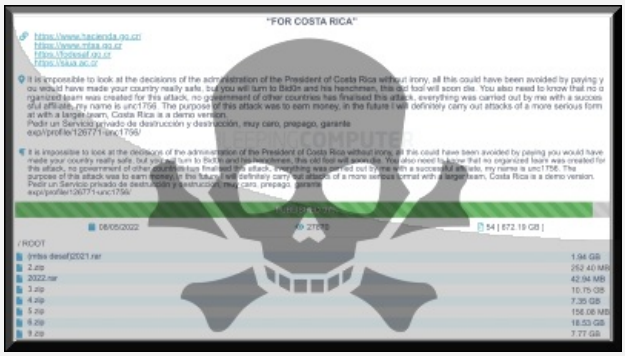
accountz

Belépés
Regisztráció

Kulcs a túléléshez

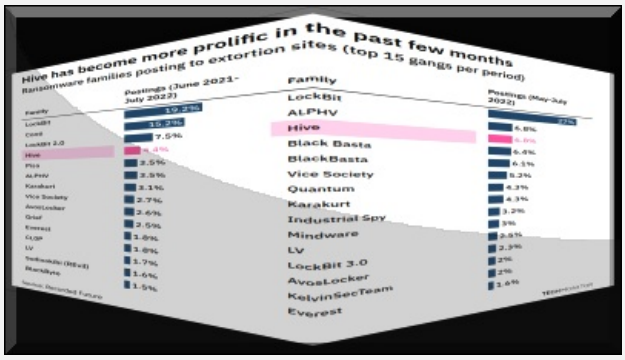
2022. július 19. 10:45 - Csizmazia Darab István [Rambo]

Ország, város, iskola, kórház, közüzem, kritikus infrastruktúra - ezek a fő célpontjai az Oroszországhoz köthető Conti és Hive bűnbandának, ahol zsarolóvírus támadásokat indítanak és váltságdíjat követelnek. Legutóbb például Costa Rica ellen láthattunk ilyet, ahol a bűnözők állami intézményeket, bankokat, minisztériumi hálózatokat, **közműveket, egészségügyi intézményeket bénítottak meg.**



A Hive csapat **az elmúlt hónapokban jelentős támadásokat hajtott végre, különösen az egészségügyi szervezeteket célozva meg**. Emiatt májusban az Egyesült Államok Egészségügyi és Humánszolgáltatási Minisztériuma (US Department of Health and Human Services) a 2022-es év első negyedéves statisztikája alapján az öt legjelentősebb számítógépes bűnözői banda egyikeként nevezte meg őket, ahol **a Hive a támadások 11%-áért volt felelős.**

De már az előző, 2021-es évben is több, mint 350 vállalatot támadtak meg.



Az incidensek miatt tucatnyi kórház, vállalat, vállalkozás állt le kényszerűen hosszabb-rövidebb időre, ami például a betegellátásban, a pénzügyi szektorban komoly fennakadásokkal járt. **Az új rosszindulatú kártevő verziót a BlackCat-hez hasonlóan már itt is GoLang helyett Rust nyelven programozták, amelyet sokkal nehezebb visszafejteni, és ennek a programozási nyelvnek a segítségével egy nehezebben detektálható, valamint egyúttal egy összetettebb titkosítási módszert használó vírust tudtak készíteni a támadók.**

Szakértők szerint ez a közös kódolási nyelvhasználat arra utalhat, hogy mindkét csoport az orosz Conti tagja.

Ezúttal viszont [egy "reecDeep" nevű ismert malware elemző a GitHub oldalon tette közzé nyilvánosan a visszafejtő programjának a legújabb változatát](), amely Hive V5 titkosítás feloldására alkalmas. A HiveRansomwareV5-keystream_decryptor kizárólag haladócsoportos felhasználók számára ajánlott, ugyanis működése a próbálgatásos (brute force) technikára épülve igyekszik kinyerni a helyreállító titkos kulcsot.

Bár **használata nem next-next-finish egyszerűségű egy átlagfelhasználó számára, ám [a bajbajutott cégek, vállalkozások feketeöves biztonsági szakembereinek viszont mégis reményt és profi segítséget]() adhat az elveszett adatok visszanyeréséhez az eszköz.**

Szólj hozzá!
Címkék: eszköz titkosítás segédprogram conti ransomware github hive rust zsarolóvírus elkódolás visszafejtő reecdeep

Ajánlott bejegyzések:


Felhasználó, kórház, olajvezeték után egy egész ország


Fedett pályás titkosítási bajnokság


Emelkedő ransomware károk


Még többet, még gyorsabban


A nyugtalanság tengere

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Antivírusblog
245 követő

Oldal követése Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog

Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

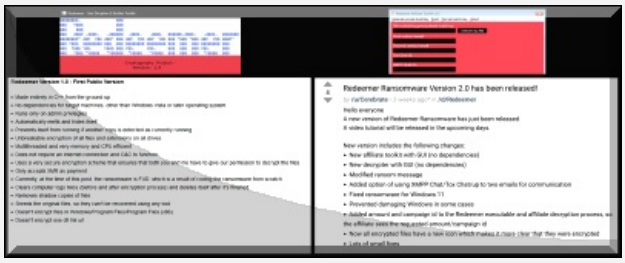
Fej vagy gyomor?

2022. július 21. 16:46 - Csizmazia Darab István [Rambo]

Ha valaki még emlékszik, volt már korábban egy Redeemer 1.0 zsarolóvírus, és ahogy más ransomware kártevők esetében, sajnos itt is folyamatosan egyre újabb riasztó fejlesztések történnek. Minden okunk meg lehet a pesszimizmusra.

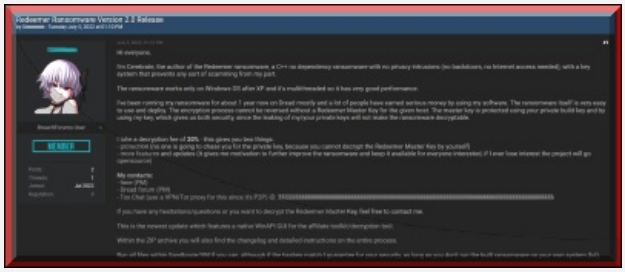
Szó sincs nyári uborkaszezonról, ugyanis beszámolók szerint **hacker fórumokon megjelent a Redeemer 2.0 (Megváltó 2.0) ransomware készítő ingyenesen elérhető alkalmazás.** Mivel ez még az egyébként elég olcsón elérhető RaaS modellhez képest is kedvezőbb, bárki könnyen alkalmazhatja, ami felhasználók számára ismét egy újabb fenyegetést jelent.

A leírás szerint a C++ nyelven készült program **Windows Vistától egészen a legfrissebb Windows 11 rendszerig működik, és grafikus interfésszel segíti a kezelőjét. Bárki letöltheti, bárki használhatja, indíthat saját támadást**, a következmények pedig ismertek.



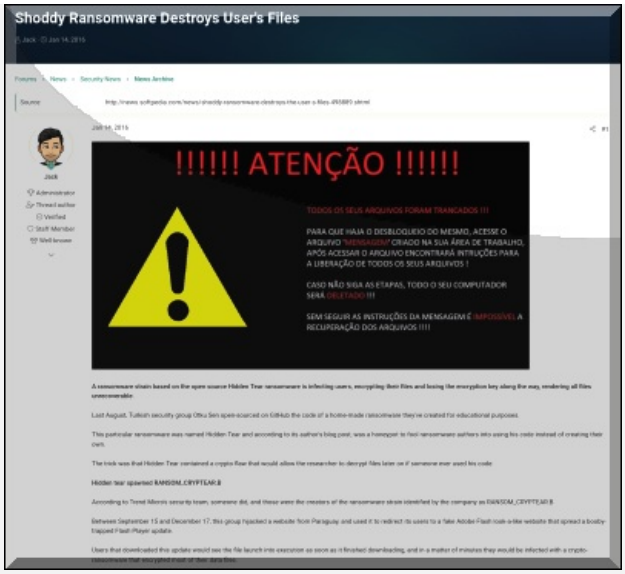
Ahogy az előző verzió, ez is rendszergazdai jogosultság megszerzésére törekszik, és a titkosítás előtt a visszaállítási pontokat, valamint a shadow copy másolatokat megsemmisíti.

A Bleeping Computer tesztje szerint viszont egyelőre nem tökéletes a működése, **például a titkosítás után nem törölte az összes fájlt, illetve nem képes minden antivírus alkalmazás elől elbújni.**



Sajnos várhatóan ezek a kezdeti gyermekbetegségek biztosan javításra kerülnek, és mivel **az affiliate modellben folyamatosan biztosítva van a szerző anyagi haszonszerzése, valamint a terjesztők ingyen juthatnak hozzá, így még biztosan sok kellemetlenséget fog okozni ez a kártékony program.**

És ehhez társul még egy **további fenyegetés is, miszerint a szerző, ha úgy érzi, már nem érdeklődnek elegen a projektje iránt, kilátásba helyezte, hogy közzéteszi a forráskódot**, amint ez 2021. júniusában a Redeemer 1.0 esetében is megtette.



Korábban is volt már több [nyílt forráskodú ransomware, említhetjük például az ArisLockert](), amit bárki letölthetett a darkwebről. De [ide sorolhatjuk a HiddenTear esetét](), ami nem csak amiatt okozott galibát, hogy boldog-boldogtalan hozzáfért a kódjához, hanem amiatt is emlékezetes volt, hogy **valaki összegányolt belőle egy hibásan működő kódot, aminél az áldozat még ha ki is csengette a pénzt a fájljaiért, [akkor sem volt esélye a helyreállításra, ugyanis a kódban a szerző még azelőtt törölte a titkosítási kulcsot, előbb elküldte volna a C&C szervereknek]().**

Nyilván itt inkább a pénzre és a zsarolásra mentek rá, de így lehetetlen helyzetbe hozták még a fizető áldozatokat is.

Mindenesetre komor jövő elé tekinthetünk, **akár a hibák javítása történik meg, akár a beígért forráskód publikálás, egyik sem kedvező forgatókönyv számunkra. Akárcsak az Utolsó cserkészben a Joe Hallenbecket játszó Bruce Willis kérdése: "Head or gut"?**

Szólj hozzá!
Címkék: ingyenes nyílt forráskód váltságdíj kit ransomware redeemer zsarolóvírus

Ajánlott bejegyzések:


Nem csitulnak a kórházak elleni támadások


Emelkedő ransomware károk


Nem szállunk rendelkezésére II.


Durva ransomware statisztikai adatok


A nyugtalanság tengere

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Antivírusblog
245 követő

Oldal követése Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

- RSS 2.0
- bejegyzések, kommentek
- Atom

bejegyzések, kommentek

accountz

Belépés
Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

LockBit vs. olasz adóhivatal

2022. július 26. 18:02 - Csizmazia Darab István [Rambo]

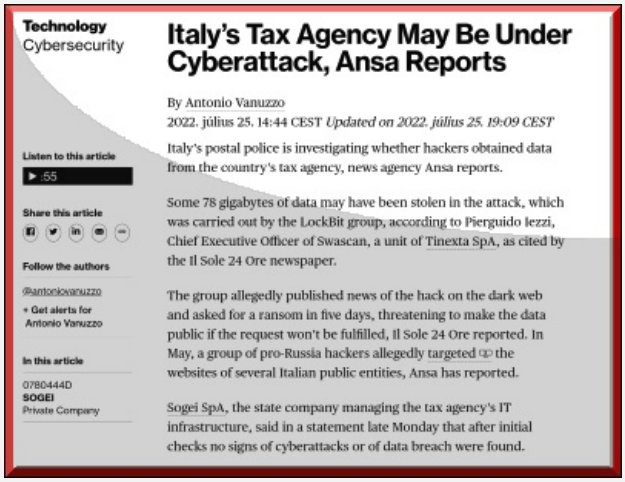
Elindult egy újabb csörte, ezúttal a tét az, hogy valóban sikerült-e a zsarolóvírus bandának az adatlopási és titkosítási akció. Ha igen, azt július 31-ig megtudjuk.

Szinte nem is múlik el hét, hogy valamilyen illusztris célpont ellen ne indulna ransomware támadás, a "szokásos" hivatalos szervezetek, kórházak, minisztériumok, közművek mellett még Costa Rica is feltűnt az áldozatok között.

Ezúttal viszont a LockBit csapat jelentette be, hogy újabb nagy skalpja van, ami nem más, mint az olasz adóhivatal, és az onnan zsákmányolt 78 GB érzékeny bizalmas adat, beleértve a vállalati dokumentumokat, szkennelt iratokat, belső pénzügyi jelentéseket és szerződéseket. Úgy tervezik, hogy bizonyítékul hamarosan néhány képernyőképet tesznek közzé az ellopott fájlokról.

Egyelőre nem ismeretes, mennyi valóságalapja van a hírnek, de **ha tényleg igaz, ez lehet az olasz kormányhivatalok történetének legsúlyosabb incidense.**

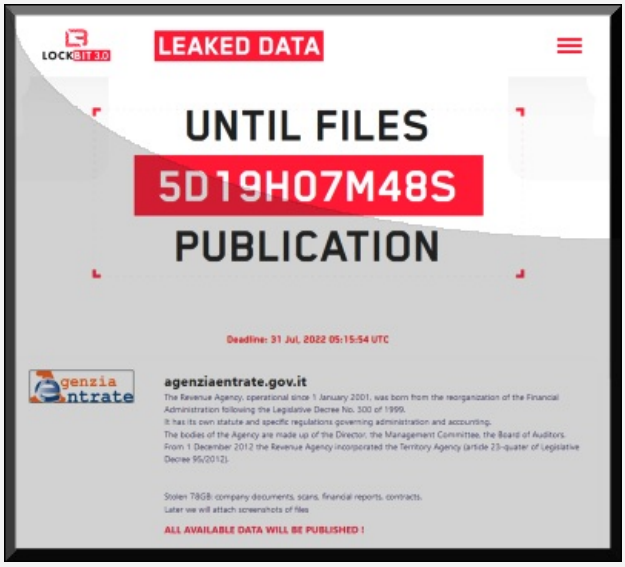
Nem tudni, hogy a darkwebes közleményen túl a bűnöző felvették-e a kapcsolatot más módon is a hivatallal, illetve történt-e már konkrét váltságdíj követelés.



Közben kijött a hivatalos sajtóközlemény is az állítólagos kibertámadással kapcsolatban, amelyben arról tájékoztatnak, hogy az első elvégzett elemzések alapján **szerintük egyáltalán nem is történt semmifajta incidens, illetve adatlopás az adóhivatali információs rendszerből.** Mindenesetre tovább vizsgálódnak, és a nyomozásban a rendőrség és a Nemzeti Kiberbiztonsági Ügynökség segítségét is kérték.

Hát mindenesetre érdekes egy helyzet, hiszen egyszerre nem lehet igaza mindkét félnek, így maradt a július 31-i határidő kivárása.

A LockBit banda egyébként már 2019. óta keseríti meg a felhasználók életét. Emlékezetes lehet, hogy **a 2.0-ás verzióban már direktben toboroztak sértett munkavállalókat, hogy bosszúból vagy pénzért adjanak el bizalmas céges adatokat, hozzáféréseket, jelszavakat.**



Nemrég pedig, **alig egy hónapja jelent meg a legfrissebb, 3.0-ás változat, amelyben további új zsarolási taktikákkal, Zcash fizetési móddal és egyéb újdonságokkal bővült a repertoár.**

Például egyedülálló módon **hibavadász (Bug Bounty) felhívást is hirdettek, amelynek keretében állítólag 1000 és 1 millió dollár közötti összeget fizetnek** annak, aki valamilyen hibát talál a programjukban.

Szólj hozzá!
Címkék: olasz váltságdíj adóhivatal ransomware zsarolóvírus doxing lockbit

Ajánlott bejegyzések:


Rossz gondolatok a könyvtárban


Nem szállunk rendelkezésére II.


Baljós árnyak: fekete macska Karintiában

Fordulat ransomware fronton


Kórházprogram

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei

Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

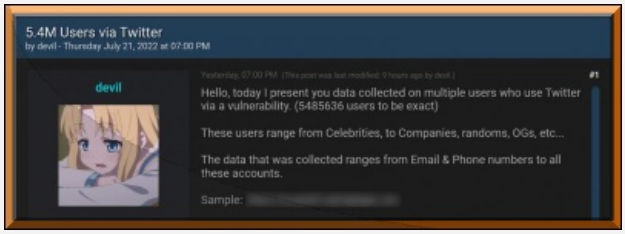
Elvitte az ördög

2022. július 28. 13:12 - Csizmazia Darab István [Rambo]

Esetünkben ez most nem egy irodalmias szófordulat, hanem maga a valóság. Az utóbbi időben a Twitter egymás után kapja a kemény csapásokat, **előbb Elon Musk mégsem akarja felvásárolni őket ;-)**, most pedig **egy csomó kiszivárgott, ellopott adat került illetéktelen kezekbe.**

Egy Devil nevezetű hacker 5.4 millió Twitter fiók adatot kínált eladásra egy darknetes fórumban. Az adatcsomagot, amely e-mail címek mellett például telefonszámokat is tartalmaz, állítása szerint egy korábbi sebezhetőség kihasználásával tudta megszerezni.

Az érintett felhasználók különféle kaliberűek, a hétköznapi júzerektől a celebeken át vállalati fiókok is vannak a felkínált egész pontosan 5,485,636 account között.



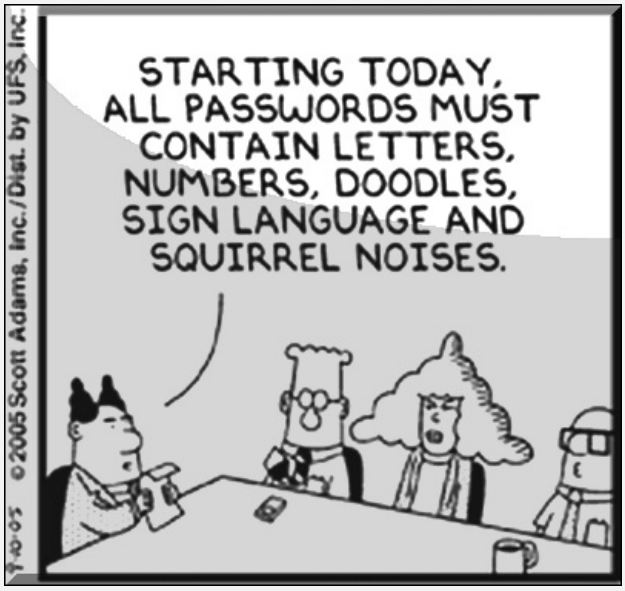
A csomag ára 30 ezer dollárért cserélhet gazdát. A Bleeping Computer kapcsolatba lépett az eladóval, aki úgy nyilatkozott, hogy egy 2021. decemberi Android platformon szereplő sérülékenység kihasználásával jutott az elkövető ezekhez az adatokhoz, és **már kapott is érdeklődéseket potenciális vásárlóktól.**

A hivatkozott sebezhetőségről a **HackerOne oldalán 2022. január 1-én beszámoló "zhirinovskiy" nevű biztonsági szakember bejegyzése szerint ez lehetővé tette, hogy illetéktelenek hitelesítés nélkül szerezzenek meg azonosítókat,** és a Bug Bounty program keretében ő ezért a felfedezésért 5 ezer dollárt kapott.

Devil az üzenetváltásban viszont **tagadta, hogy bármilyen kapcsolatban állt volna a fenti biztonsági szakértővel, vagy hogy a HackerOne-ról értesült volna a dologról.** A Twitter végül **január 13-án befoltozta ezt a fórumban**

is említett hibát, ám a most megjelentetett adatcsomaggal kapcsolatosan nem ismerte el, hogy ez a jelentős adatsértés emiatt valóban bekövetkezett volna. **Az eladó által mutatott részleges minta alapján azonban az adatok valósnak és érvényesnek látszanak.**

A Twitter felhasználók viszont eközben azt **sérelmezik, hogy nem kaptak semmilyen hivatalos figyelmeztetést a szolgáltatótól** emiatt a kihasználható, és a helyzet szerint ki is használt sebezhetőséggel kapcsolatban.



Mi most mindenesetre figyelmeztetünk mindenkit, rendszeresen frissítsen, legyen óvatos a Twitter bejelentkezésnél, **kapcsolja be a kétfaktoros autentikációt, és számítson rá, hogy a közeljövőben különféle testre szabott adathalász támadások érkezhetnek attól, aki ezt az adathalmazt birtokolja, megvásárolja.**

Érdemes lehet azonnal jelszót változtatni, és ha valaki ugyanazt az azonos jelszót használta több, különböző szolgáltatásnál, akkor itt az ideje egyedi és erős jelszavakat választani. Ezek megjegyzésében segíthet például a KeePass vagy a BitWarden jelszómenedzser.

Szólj hozzá!
Címkék: hack devil twitter adatlopás adatszivárgás darknet zhirinovskiy

Ajánlott bejegyzések:


100 millió helyett "csak" 40 lett, maradhat?

Van másik!

Járulékos következmények szevasztok


Viva la Revolut


Fordulat ransomware fronton

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.

VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

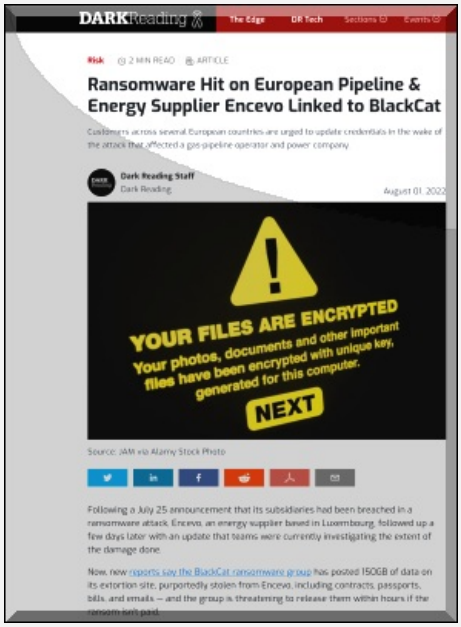
Közeleg a tél, érzékeny ponton támadnak a zsarolóbandák

2022. augusztus 02. 11:50 - Csizmazia Darab István [Rambo]

Miután világszerte rendkívüli helyzetet okoz az energia ellátás, és mindenhol sok bizonytalanságnak nézünk elébe **a földgáz, kőolaj és egyéb energiahordozók egyre drágúló árával és rendelkezésre álló mennyiségével kapcsolatban, a bűnözők sebészi pontossággal használják ki mindezt.**

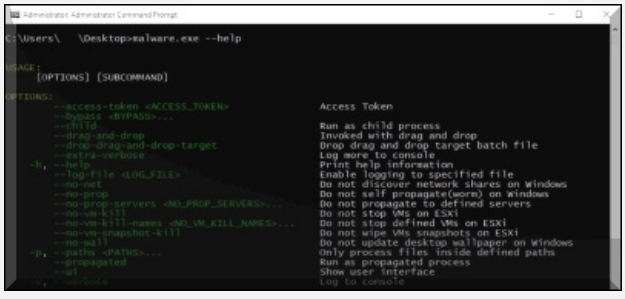
Már a Covid időszak alatt is drámai hatása volt a DarkSide banda Colonial Pipeline csővezeték hálózat elleni támadásnak, melynek következtében több hetes leállás, és üzemanyag hiány lépett fel az USA keleti partján.

Most az orosz-ukrán háború következtében kialakult energia válságot kihasználva egy luxemburgi székhelyű Enveco energiaszolgáltató hálózat ellen indítottak zsarolóvírusos támadást.



A hírhedt **BlackCat ransomware csapat mostani akciója a földgázvezeték-üzemeltető Creos és az Enovos energiaszolgáltatót érintette.** Az Enveco úgy nyilatkozott, hogy **az incidens egyelőre nem okozott semmifajta földgáz és villamos energia ellátási problémát, csak a számítógépes hálózatban történtek leállások július 22-e óta, de még vizsgálják a támadás pontos körülményeit, és a kiszivárgott adatok lehetséges körét.**

A doxing-gal kombinált incidensben - melynél az adatok titkosítása mellett bizalmas adatokat is lopnak - 150 GB érzékeny adatot tudtak zsákmányolni a bűnelkövetők, ebben pedig különféle személyes és útlevél adatok, céges szerződések, vállalati levelezés, illetve számlázási adatok is szerepelnek.



A BlackCatről (alias AlphV) kutatók úgy vélik, hogy az a mára már megszűnt korábbi DarkSide ransomware

csoport tagjaiból alakulhatott. A mostani támadásnál az energiaszolgáltató ügyfélportálja még mindig nem érhető el, és arról sincsenek nyilvános információk, mekkora követeléssel léptek fel ellenük, illetve fizettek-e váltságdíjat.

Ám az sajnos már most borítékolható, hogy a tél közeledtével az energia szolgáltató szektor és az élelmiszer ellátó hálózatok kiemelt kockázatokkal nézhetnek majd szembe, hiszen **a folyamatos ellátás miatt a bűnözők úgy kalkulálnak, hogy nagyobb lesz a fizetési hajlandóság, mint más egyéb általános támadásoknál.**

Szólj hozzá!
Címkék: szolgáltató energia támadás ellátás váltságdíj célzott ransomware blackcat zsarolóvírus

Ajánlott bejegyzések:


Nem csitulnak a kórházak elleni támadások


Baljós árnyak: fekete macska Karintiában


Apa kezdődik!


Colonial Pipeline után a mindennapi kenyerünk

"Illetéktelen fél korlátozott ideig hozzáférhetett fájlokhoz"

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi

vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.

VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

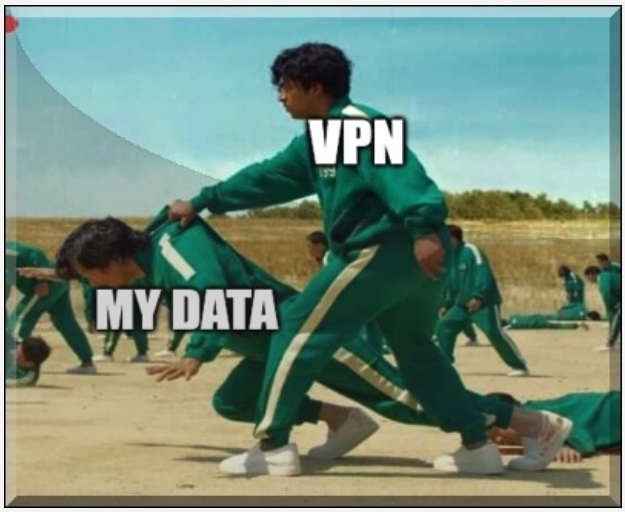
accountz

Belépés
Regisztráció

VPN-t a VPN boltból

2022. augusztus 05. 12:00 - Csizmazia Darab István [Rambo]

Virtuális magánhálózatok: mik az előnyei, mire használhatjuk? Íme a leggyakoribb kérdések a VPN megoldásokkal kapcsolatban.



Alaposan megfizethetünk a digitális világban a másokkal megosztott privát adatainkért: a magánéletünk lehet az ára. **Az általunk meglátogatott weboldalak, költéseink, tartózkodási helyünk és az, hogy milyen bankkártyával fizetünk, csak néhány azok közül az információk közül, amelyeket mások gyűjtenek és pénzzé tehetnek. Háborús helyzetben a veszély még ennél is sokkal nagyobb:** az adatokkal olyan módon élhetnek vissza, ami a virtuális és valós életünkre nézve is káros lehet.

Az ukrajnai háború kezdete óta a virtuális magánhálózatok (VPN megoldások) iránti kereslet Ukrajnában és Oroszországban is több száz százalékkal megugrott. Az ESET kutatói összegyűjtötték a VPN-ekkel kapcsolatban leggyakrabban feltett kérdéseket, és bemutatják **miben nyújthatnak védelmet számunkra az online tevékenységeink során.**

A VPN-re úgy is gondolhatunk, mint az IP-címünk láthatatlanná tévő eszközére, amely áthelyezi a kapcsolatot egy általunk kiválasztott országban működő szerverre, és egy onnan származó IP-címet mutat. Egyfajta védőrétegként működik, titkosítja az összes adatot, amely áthalad rajta, és erősíti az online adatvédelmet. A felhasználók adatai, tartózkodási helye és böngészési előzményei elérhetetlenek lesznek bárki számára, aki megpróbálja azonosítani és nyomon követni azokat. Egy nyilvános Wi-Fi használatakor sokkal kevésbé biztonságos hálózathoz csatlakozunk, ami tökéletes lehetőséget ad a hackerek számára, hogy illetéktelenül hozzáférést nyerjenek más felhasználók eszközeihez.

A VPN biztosítja, hogy a kapcsolatunk titkosított és védett legyen a támadókkal szemben, akik a személyes adatainkra, jelszavainkra vagy banki adatainkra vadásznak. Otthon a legtöbb ember úgy gondolhatja, biztonságos hálózatot használ, de ez nem feltétlenül van mindig így. Egyáltalán nem biztos, hogy az otthoni hálózati jelszó biztonságos, és azt sem tudhatjuk, hogy feltörték-e hálózati eszközünket vagy kiszivárgott-e a jelszavunk egy korábbi adatszivárgás során.

Mik a VPN használat előnyei?

- **Védi a személyes adatokat.** Megosztott adatainkat az általunk választott országban lévő szervereken tárolják, így azok nem hozhatók kapcsolatba velünk. A legitim VPN-szolgáltatások nem rögzítik a keresési előzményeket, amely különösen fontos, ha valaki olyan országban él, ahol korlátozott a szólás- és sajtószabadság.

- **Elrejti a böngészési információkat.** A VPN segítségével rejtve marad IP-címünk a webhelyek és alkalmazások elől. A közösségi médiaplatformok előtt viszont nem titkolózhatunk, ha be vagyunk jelentkezve fiókjainkba – vagyis ott a VPN nem képes teljes anonimitást biztosítani a felhasználóknak.

- **Lehetővé teszi a blokkolt weboldalak elérését.** Ha egy weboldal nem érhető el lakóhelyünkön – a BBC például blokkolva van Oroszországban –, bizonyos korlátozásokat megkerülhetünk, a VPN használatával ugyanis úgy működik az internetkapcsolatunk, mintha egy másik országban lennénk.

- **Több tartalmat tesz elérhetővé a streaming platformokon.** Miután IP-címünk földrajzilag egy adott helyen van, a VPN segítségével olyan műsorokat is láthatunk, amely a platformon korlátozások miatt elvileg csak más területi régiókban lenne elérhető.

- Végső soron pénzt takaríthat meg, mivel sok online kereskedő a magasabb jövedelmű régiókban megemeli a helyi területi árait.

Elegendő-e a VPN a magánélet védelméhez? Kiberbiztonsági szakértők szerint önmagában természetesen nem elegendő, de hasznos, néha egyenesen nélkülözhetetlen kiegészítő számos adatvédelmi és biztonsági aggályra.

Jó pár vállalat kínál VPN megoldásokat, vagyis **választhatunk az igényeinknek megfelelőt, ám fontos néhány szempontot mérlegelni a VPN kiválasztása előtt. Például ha a szolgáltató ígérete ellenére mégis mindent naplóz, és közben szemérmetlenül eladja harmadik félnek az adatainkat, akkor a vélt biztonságunknak annyi.**

- A kapcsolat egy **másik szerverre történő átirányítása miatt az internet sebessége lassabb lehet**. A szolgáltatók különböző maximális sebességgel rendelkező szervereket kínálnak, **a gyorsabb jobb, és általában nem ingyenes. Használatuk pénzbe kerül, viszont érdemes rájuk költeni**, pl. ExpressVPN, NordVPN, Surfshark NET, stb.

- A vállalatok székhelyei **különböző országokban találhatóak, és az adott ország adatvédelmi követelményeitől**

függően eltérő szabályokat és törvényeket követnek. Nem minden VPN-t kínáló vállalat olyan megbízható, mint amilyennek látszik.

- **A VPN-t használni néhány országban kifejezetten illegális,** főként olyan államokban, ahol erre lenne szükség a hírközlő médiát sújtó tiltó korlátozások megkerüléséhez. Bizonyos országokban ugyan nem illegális, de a kormányok titokban szisztematikusan próbálják megakadályozni a VPN szolgáltatásokhoz való hozzáférést.

- Amennyiben a VPN használata közben bejelentkeztünk valamely közösségi média fiókunkba, **onnantól tevékenységünk már nem marad rejtve az adott közösségi média platform előtt.**

- Egyes VPN-ek az adatvédelemre, mások pedig az összetettebb biztonsági funkciókra helyezik a hangsúlyt. **Semmilyen VPN sem nyújt teljes biztonságot, a vállalatok, az internetszolgáltatók és egyes kormányok pedig megpróbálhatják letiltani ezeket.**

- **Érdemes annak is utánajárni, hogy van-e az adott szolgáltatónál lehetőség anonim regisztrációra, pontosan mit naplóz a szolgáltató, és vajon eladja-e a felhasználói adatokat, böngészési előzményeket harmadik félnek, például hirdetőknek.**

666

Hogyan használható profi módon a VPN? Minden eszközünkre VPN-t telepíteni, valamint azt állandóan ki- és bekapcsolni kivitelezhető, de elég körülményes. Ahelyett, hogy külön-külön csatlakoznánk, engedélyezhetjük a VPN opciót az otthoni routeren, amennyiben az kínál ilyen lehetőséget.

Ezáltal a hálózatunkhoz csatlakozó összes eszköz forgalma a VPN titkosított csatornáján keresztül halad át, így még az olyan eszközök is nagyobb biztonságban vannak, amelyek nem támogatják az alkalmazásokat. Igaz, ez a módszer kevésbé felhasználóbarát, de a szolgáltatók el tudják magyarázni, hogyan telepíthetjük a VPN-t, amelynek használata nagyobb biztonságot kínál.

777

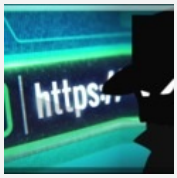
Tényleg szükség van VPN-re? Olyan világban élünk, ahol nem árt azzal tisztában lennünk, hogy adataink értékesek a vállalatok számára, akik minél részletesebb információkat akarnak szerezni az érdeklődési körünkről, valamint tartózkodási helyünkről, amennyire azt az algoritmusok csak lehetővé teszik.

Ugyanakkor a VPN-ek adataink nagyobb védelmén túlmenően biztonságosabbá tehetik a konfliktus sújtotta régiókban élők digitális életét is. A virtuális magánhálózatok ablakot nyitnak a világra azoknak, akik olyan kevésbé szerencsés régiókban élnek, ahol a szabad hozzáférést a politika vagy a technológia megakadályozza.

Szólj hozzá!
Címkék: private adatvédelem privátszféra network virtual vpn

Ajánlott bejegyzések:


Az online térben hagyott személyes adataink



Böngészés - kockázatok és mellékhatások

Közösségi média VS munkahely


Mindent IS visz...


Kémek krémje

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

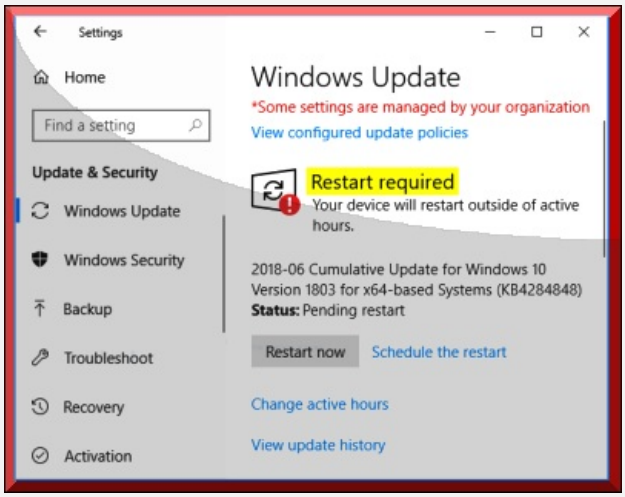
10 alaplépés a biztonsághoz

2022. augusztus 08. 13:49 - Csizmazia Darab István [Rambo]

Minden pillanatban számtalan **fenyegetés érkezik felénk a kibertérből: adathalászat, rosszindulatú hirdetések, kártékony linkek és fájlok formájában.** Sok más ilyen hasonló tízes listát lehetne még összeírni, de az alapok tekintetében talán ezek a legfontosabbak. Jöjjön egy kis rövid könnyed nyári ismétlés!

01. Automatikus frissítések alkalmazása.
Nincs hatékony védelem naprakész, lefuttatott hibajavító frissítések nélkül, a kártékony kódok legtöbbször javítatlan réseken keresztül fertőznek.

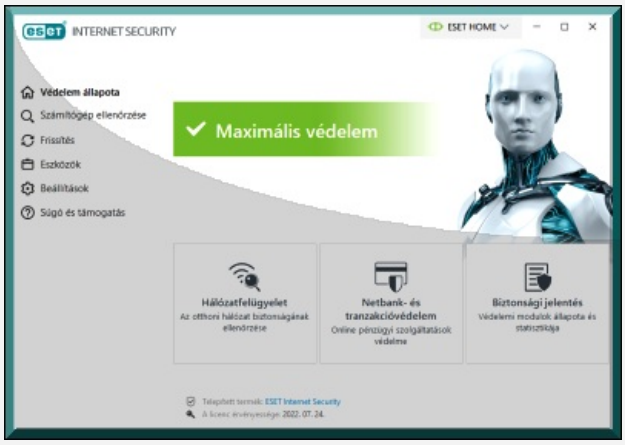
Számos antivírus alkalmazás képes figyelmeztetni az elmaradt Windows frissítésekre, hiszen ezekkel sebezhetőségeket, sérülékenységeket zárunk be, ami a felhasználó védelmében egy nagyon hasznos dolog. Ne felejtsük a szükséges újraindításokat sem!



02. Távolítsuk el a PC-kkel gyakran gyárilag mellékelt bloatware-eket!
A kéretlen, előtelepített programok **lassítják, feleslegesen használják a netünk és az eszközünk erőforrását, adatokat gyűjthetnek és szivárogtatnak**, de néha egy időkorlát átlépése után fizetős változat megvásárlására is buzdíthatnak.

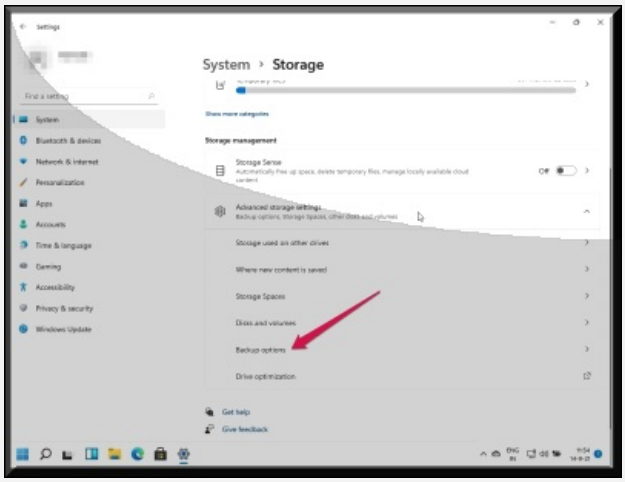
Voltak ilyen jellegű programok korábban a gyári Lenovo laptopokon, illetve androidos telefonokon is, kukába velük.

03. Telepítsünk neves védelmi programot, és tartsuk azt naprakészen!
Ma már nem is vírusirtónak, hanem sokkal inkább internetbiztonsági alkalmazásnak nevezhetőek ezek a korszerű komplex védelmi alkalmazások, amelyekben különféle integrált modulok dolgoznak - **többek közt Exploit Blocker, Botnet Protection, hálózati támadások elleni védelem, biztonságos bankolási felület, webkamera védelem és természetesen a zsarolóprogram elleni modul** sem hiányzik a programba beépített védelmi eszköztárból.



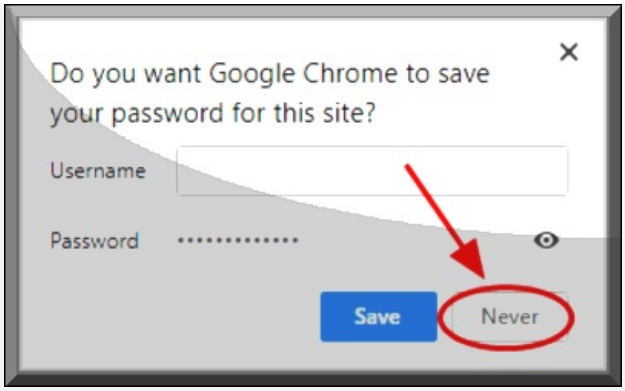
04. Gondoskodjunk a rendszeres biztonsági mentésekről!
Ezt a feladatot is lehet sőt kell automatizálni, a saját munkák mellett jó, ha az operációs rendszernél is helyreállító pontok kerülnek mentésre.

A 2013. óta velünk élő ransomware már kellően megijesztett mindenkit, de adatvesztés bekövetkezhet akár fizikai meghibásodás, vagy lopás miatt is, szóval a külső adathordozóra történő rendszeres mentés tényleg létfontosságú.



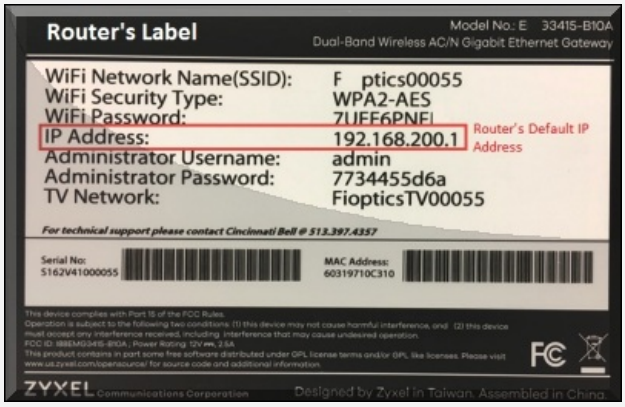
05. Állítsuk be a böngészőnket biztonságosra!
Részint ezt az alkalmazást is frissítsük rendszeresen, másrészt a biztonsági beállításoknál tegyük meg a szükséges lépéseket!

Mindig szabályosan lépjünk ki a webes szolgáltatásokból, és sose mentsük el a jelszavainkat a böngészővel, mert illetéktelenek távolról hitelesítve hozzáférhetnek! Használjunk különféle biztonságos kiegészítőket: pl. AdBlocker, HTTPS Everywhere, NetCraft, TrackMeNot, stb. Szükség esetén a profilozást, adatgyűjtést is mellőző DuckDuckGo keresőre is válthatunk.



06. Fusson a tűzfal, és a router is legyen rendben.
Az otthoni útválasztó eszközök jelentős része nincs biztonságban. Ennek legfőbb okai a gyenge jelszóválasztás, a gyári alapértelmezett jelszó használata, az eszközökön futó szoftverek sebezhetőségei, illetve hogy a megfelelő védelem hiányában a külső hálózatokról is hozzáférhetőek hálózati szolgáltatások.

Válasszunk erős egyedi jelszót mind az admin felülethez, mind a wifi eléréshez, frissítsük a firmware, amikor ez szükséges!



07. Ahol csak lehet, használjunk többtényezős hitelesítést!
A haveibeenpwned.com oldalon kis híján 11.9 milliárd ellopott, kiszivárgott jelszó van. **Pedig az erős egyedi jelszó használaton felül lehetne javítani a helyzeten, csak használni kéne a 2FA/MFA megoldásokat.**

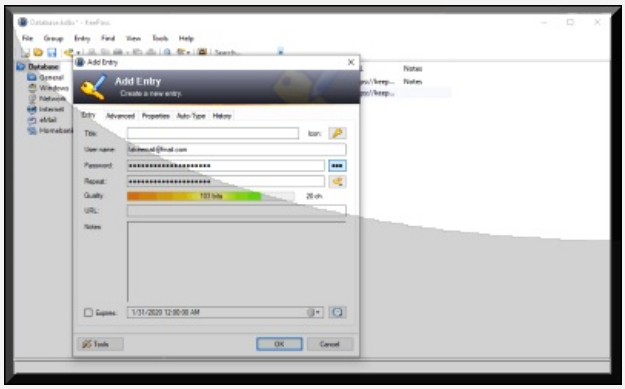
Ezek az SMS, a hitelesítő USB kulcseszköz, az egyszer használatos OTP (One Time Password), vagy valamilyen dedikált hitelesítő külső alkalmazás a mobileszközünkre.

08. Legyünk óvatosak az ismeretlen USB eszközökkel!
Idegen USB kulcsoknál, tárolóknál mindig végezzünk vírusellenőrzést, és ez alól a talált eszközök se legyenek kivételek!

Itt mindenféle külső eszköz gyanús lehet, fényképezőgéptől kezdve az áruházi fotókidolgozást végző nyilvános gépig.

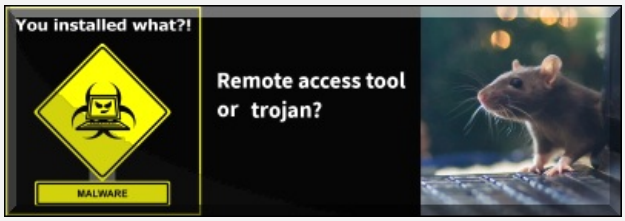
09. Használjunk jelszókezelőt!
Mindenképpen szükséges az erős, egyedi és rendszeresen cserélt jelszavak használata a legfontosabb belépési helyeinket. A sok jelszót megjegyezni viszont nehézkes, így sokaknál a PostIt, papírfecni, textfájl tárolja ezeket. A legjobb kiváltó megoldás a password menedzser program használata.

Egyes védelmi megoldásokban (pl. ESET Smart Security Premium) gyárilag található ilyen, ez képes generálni, megvédeni, tárolni, és a weboldalakon automatikus kitölti az űrlapokat. Külső alkalmazások is használhatóak, mint a KeePass, vagy a a multiplatform Bitwarden.



10. Csak megbízható forrásokból töltsünk le alkalmazásokat/fájlokat!
A kétes telepítések gyakori kockázatot jelentenek minden platformon, legyen az Windows vagy Android. Tavaly májusban tarolt a FedEx-es csomagküldő nevével visszaélő androidos FluBot vírus, ahol **sokan az SMS-ben kapott ordítóan idegen linkre simán kattintottak, feltelepítettek egy ismeretlen alkalmazást, gondolkodás nélkül megadva neki minden létező engedélyt.**

Pedig a védekezés, megelőzés, a biztonságos környezet egyik alappillére továbbra is a biztonságtudatos alkalmazás választás és telepítés.

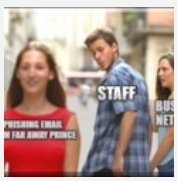


Szólj hozzá!
Címkék: microsoft windows biztonság trükkök tippek megelőzés védekezés kiberbiztonság welivesecurity.com

Ajánlott bejegyzések:


10 gyakori IT biztonsági hiba


7 tipp a mobilunk védelméhez



10 gyakori ok, amiért bedőlünk a csalásoknak


Eljött az emelt szintű biztonság ideje

10 kiberbiztonságra veszélyes szokás

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

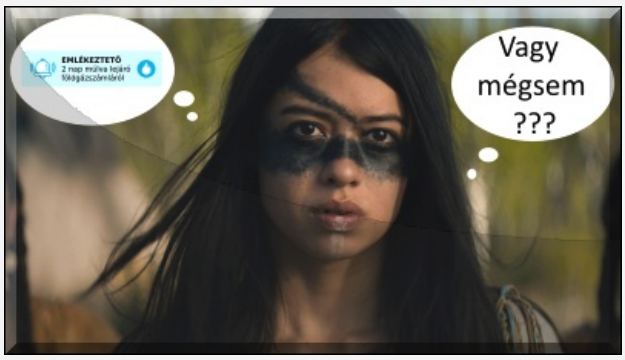
accountz

Belépés
Regisztráció

2 nap múlva lejáró MVM gázszámla vagy mégsem?

2022. augusztus 10. 07:51 - Csizmazia Darab István [Rambo]

Sokat látott "vagy mégsem" rovatunk újabb epizódja következik, benne a 700%-os gázáremelés miatti **amúgy is ideges időszakban érkező állítólagos tartozás. Vajon be kell fizessük a látszólag tavalyról maradt kiegyenlítetlen számlát?**

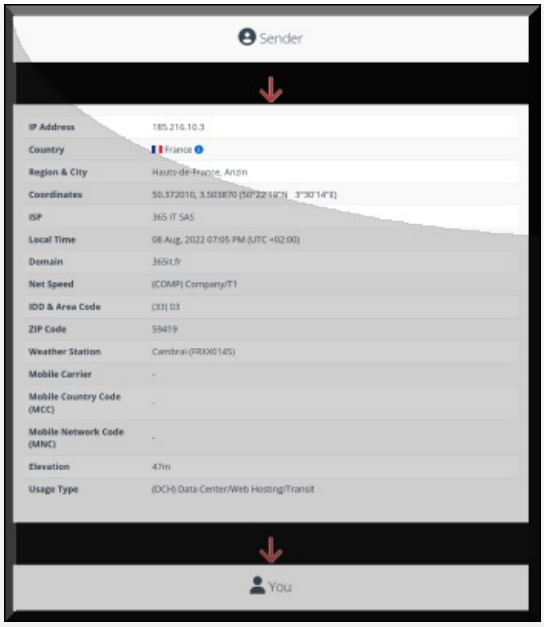


Röviden összefoglalva: amatőrök próbálkoznak. Bővebben pedig, **kapunk egy "EMLÉKEZTETO 2 nap múlva lejáró földgázszámláról" tárgysorú e-mailt látszólag az MVM Next-től, de a levél azért sok sebből vérzik**. Nem elég hivatalosnak lenni, hivatalosnak is kell látszani - **ezt a tételt máris bukta a küldő, aki a "support KUKAC decayeuxlasecurite PONT fr" címről lőtte fel a küldeményét az űrbe.**

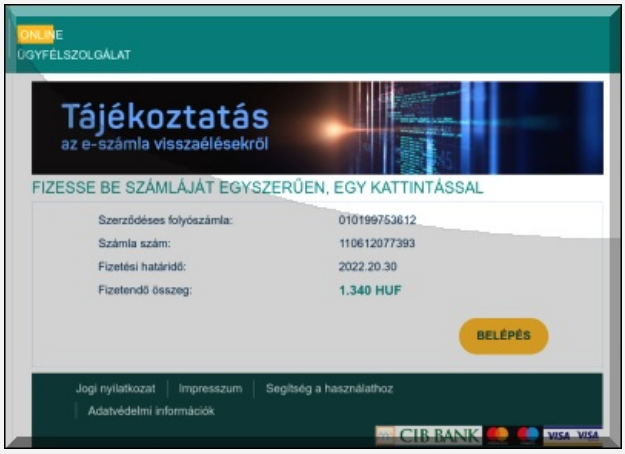
Mellesleg az e-mailtrace is arra jutott, nem volt itt sem túlagyalás, **valóban a franciaországi Anzinból küldték a levelet**. Bár az ékezetek szinte teljesen rendben vannak az egész levélben, egyedül a subject sorban nem sikerült a mutatvány a nagybetűs karaktereknél.

A mellékelt megjelenített számlaszám viszont legalább valóban az NKM Földgázszolgáltató Zrt. Gázdíjhoz tartozik, igaz nagy jelentősége nem lesz, szerepe itt csak formaság, hiszen bankkártyás fizetést várnak tőlünk. Az összegre mondhatjuk hogy viszonylag jól megválasztott, nem olyan hatalmas, hogy mindenki azonnal gyanakodjon.

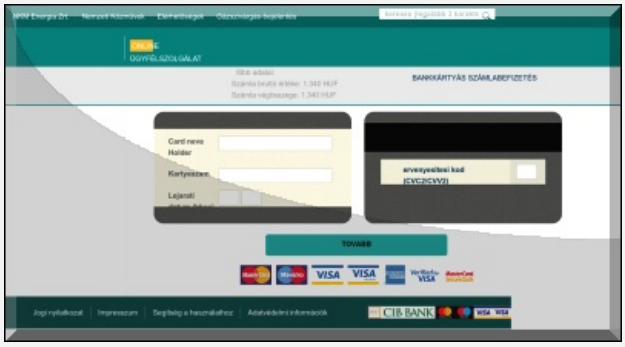
Szerződéses folyószámlaszámra és számla sorszámra kockadobással be van írva valami random érték, nem pedig az igazi saját, valahogy kiszivárgott valódi adatokkal vettek minket profin célba. És persze a **"Befizetem bankkártyával" sor itt a leglényegesebb link, amely vajon hova mutat? A "creativewebmind PONT com PER en" weboldalra,** hát így ebben a formában ez sem kerül majd bele az adathalászat nagy aranykönyvébe.



És akkor itt most már kőkeményen **a bankkártya adatok bekérése jön, úgy mint kártyabirtokos neve, kártyaszám, lejárati idő és a háromjegyű CVV biztonsági kód. Vegyük észre, hogy az e-mailben kért eredeti 14,541.- forint helyett valamiért itt már "csak" 1,340.- forint szerepel.** Barion, SimplePay vagy egyéb alternatív lehetőséget nem ajánlanak fel, csak a kártyaadatok bamba begépelését várják.



Ha valaki elég paranoid, és minden netes számláját virtuális (unembossed) kártyával fizeti, amire amúgy sem tölt fel összegeket, csak közvetlenül a vásárlás előtt, az viszonylag nyugodt lehet, sőt sok banknál már az ilyen kártyával történő tranzakciók is csak egyedi visszaigazolás után élesednek, magyarán jóvá kell hagyni őket egyesével. **Ennek ellenére ilyen kamu helyekre sose gépeljünk be még ilyen adatokat sem.**



Egészen vicces még, hogy a különben elég jó magyarsággal, és majdnem helyes ékezettel érkező spam külön figyelmeztetést mellékel számunkra, amelyben csalókra figyelmeztetnek minket. Vajon kik lehetnek ezek?

"*FIGYELMEZTETÉS ADATHALÁSZATRA!*
Vigyázzon adataira, ne dőljön be az MVM vagy az NKM nevével visszaélő csalóknak!
Bővebb tájékoztatás: www.mvmnext.hu/Adathalaszat"

Miközben a mellékelt link viszont ugyanúgy az ő adathalász oldalukra mutat.

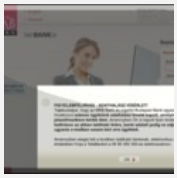
Jól láthatóan a mostani csalási próbálkozás egy tavalyi hasonló spam felmelegítése, aktualizálása, hiszen most mindenki mérgezett egérként mérőórát jelent, kapkodva befizet még a korábbi "rezsicsökkentett" áron.

A kampány a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézetnek azonnal lejelentve, azóta ezt az oldalt már sikeresen lelőtték, de persze **további előfordulása más domén címekről még azért bárhol előfordulhat, tehát érdemes figyelni.**

1 komment
Címkék: magyar számla mvm phishing adathalászat gázszámla vagymégsem

Ajánlott bejegyzések:

Tagsági kérdések - vagy mégsem?


MKB adathalászat szigonnyal, horoggal, hálóval


Magyar Posta csomagunk jött - vagy mégsem?


Ingyenes Omikron teszt vagy mégsem?

Sikeres brandek az adathalászatban

Kommentek:

Head Honcho 2022.08.10. 09:42:11

Annyira sükebókának tartom a "zembereket", hogy a csalók biztos kaszálnak így is.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

Havi 10 terabájt lett, maradhat?

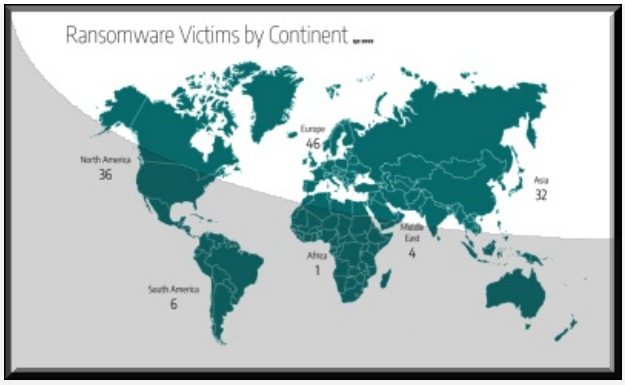
2022. augusztus 15. 11:15 - Csizmazia Darab István [Rambo]

Két érdekes statisztika is foglalkozik a ransomware támadások mértékével, gyakoriságával, hatékonyságával. **Ezekből válogattunk pár érdekes és egyben tanulságos adatot.**

A Dragos által gyűjtött adatok összefoglalója szerint folyamatosak az ipari rendszerek elleni nagyszabású támadások, például az idén júniusban **a mexikói Foxconn gyár elleni támadásban 1,200 szervert titkosított LockBit csoport** több hetes leállást okozva. **A Black Basta banda pedig egy tavaly májusban szintén hetekig tartó olyan incidensért tehető felelőssé, amelyet az AGCO nevű mezőgazdasági berendezéseket gyártó cég ellen hajtottak végre.**

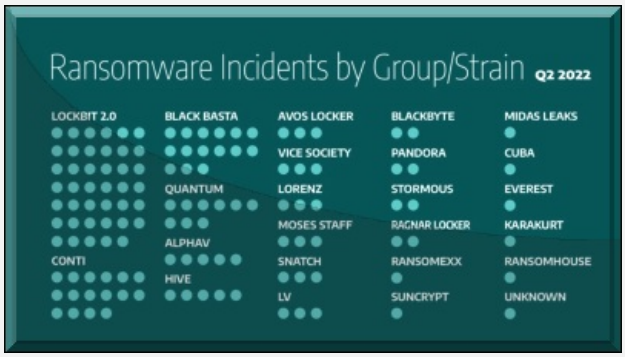
A biztonsági cég **43 különböző ransomware szereplőt követ nyomon, amelyből a második negyedévben 23 volt aktív. A vizsgálatban 125 különböző zsarolóvírus támadást** elemeztek ki.

A második negyedévi részletes adatok szerint **az ipari szervezetek és infrastruktúrák elleni támadások többsége, majdnem 40%-a európai célpontok ellen zajlott**, Észak-Amerika került a második helyre 36 jegyzett incidenssel, míg Ázsiában valamivel kevesebb, 32 eset történt, és a maradék támadások dél-amerikai, közel-keleti és afrikai célpontok ellen történtek.



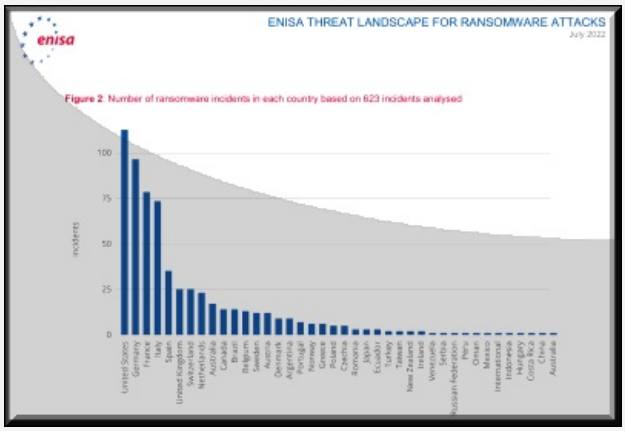
A LockBit 2.0 által indított támadások messze a leggyakoribbak, az összes eset 33 százalékáért ez a banda a felelős. A szoros verseny élmezőnyében találjuk még a Conti, a már említett Black Basta, a Quantum és az AlphaV (másnéven Black Cat) csoportot is.

A vizsgált adatok azt támasztják alá, hogy **a bűnözők az év hátralévő részében is gyaníthatón növekvő aktivitást fognak mutatni az ipari rendszerek elleni műveletekben.**



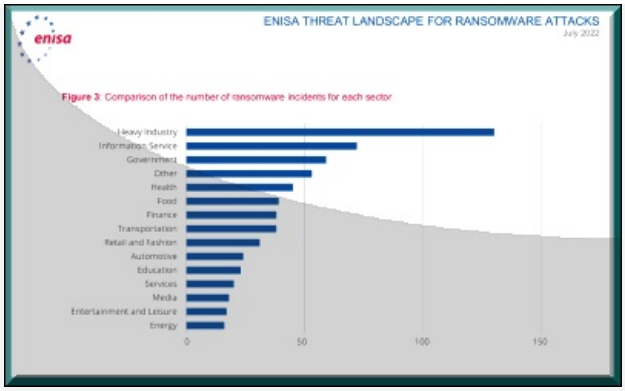
Ezt képet árnyalja kissé az európai **ENISA fenyegetettségi helyzetről szóló jelentése, amely szerint a jelentett és nyilvánosságra került esetek igazából csak töredéke a valós számoknak**. Az egyéves időtartamot átfogó elemzés adatai 2021 májusa és 2022. júniusa közti időszakra vonatkozóan összesen **623 zsarolóvírus-incidenst elemzett világszerte.**

A vizsgált vállalatok igen **széles körből kerültek ki, mind változatos üzleti profiljuk, mind cégméretük szerint a legkisebbektől egészen a multinacionális nagyvállalatokig** szerepelnek a merítésben. A statisztika szerint ebben az időszakban **havonta mintegy 10 terabájtnyi adatot loptak el a ransomware fenyegetés szereplői. Az ellopott adatok 58%-a a munkavállalók személyes adatait tartalmazta.**



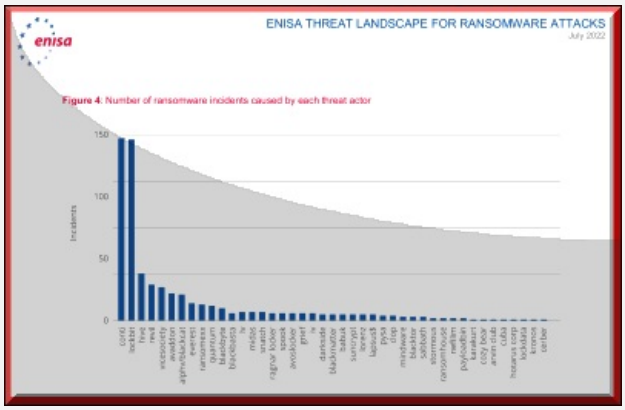
A doxing - vagyis az ellopott adatok nyilvánossá tételével való kombinált fenyegetés - miatt nőtt a nyomás az áldozatokon. **Az incidensek 94%-ánál nem került nyilvánosságra, hogy az adott vállalat végül kifizette-e a váltságdíjat vagy sem.** Gyakori eset azonban, hogy nem fizetés esetén a bűnözők beváltják a fenyegetést, és a sikertelen egyeztetés után az incidensek közel **38 százalékában a bandák elérhetővé teszik a zsákmányolt bizalmas adatokat a weboldalukon.**

Ebből pedig egyenesen következik, hogy a fennmaradó 62%-nál vagy kamu volt az adatlopás, vagy pedig a háttérben sikerült valahogy megállapodni a támadókkal.



Mivel a látencia hatalmas, emiatt ezek a számszerűsített adatok csak a jéghegy csúcsát jelentik. Nehezíti a célzott vállalatok helyzetét, hogy **2018. óta egyre komplexebb támadások zajlanak, jól működő üzleti modellé vált RaaS (Ransomware as a Service), állandó szereplő lett a doxing.**

Emellett nem fizetés esetén DDoS támadással is fenyegetőznek a támadók, amely az üzletmenet folytonosság szempontjából jelentős kockázat, és **a célzott támadásokban sajnos szerepe lett az olyan jellegű módszereknek is, amelyeknél belsős információkért pénzt ígérve sértett munkavállalókat toboroznak saját cégük elleni támadáshoz.**



Végül érdemes a védekezéshez, megelőzéshez történő szokásos ajánlások közül kiemelni párat. Nyilván a naprakész biztonsági másolat készítése az üzleti fájlokról és a személyes adatokról már alapnak számít, de ebben is van például olyan 3-2-1 elnevezésű best practice módszer, **amely a 3 példány, 2 különböző adathordozó, és 1 másolat a helyszínen kívül jelentőségét emeli ki jogosan.**

Támadás esetén hasznos ötlet a No More Ransom Project weboldalára ellátogatni, **amely az Europol kezdeményezésére jött létre, valamint célszerű értesíteni a helyi kiberbiztonsági hatóságot is**, és lehetőség szerint nem fizetni, nem tárgyalni a bűnözőkkel.

Szólj hozzá!
Címkék: statisztika jelentés elemzés összefoglaló adatok enisa ransomware zsarolóvírus dragos látencia

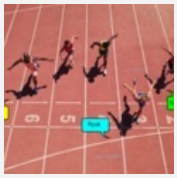
Ajánlott bejegyzések:


Ransomware helyzetjelentés


Emelkedő ransomware károk


Durva ransomware statisztikai adatok


Ransomware a spájzban


Világrekord, aminek mégsem örül senki

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei

Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

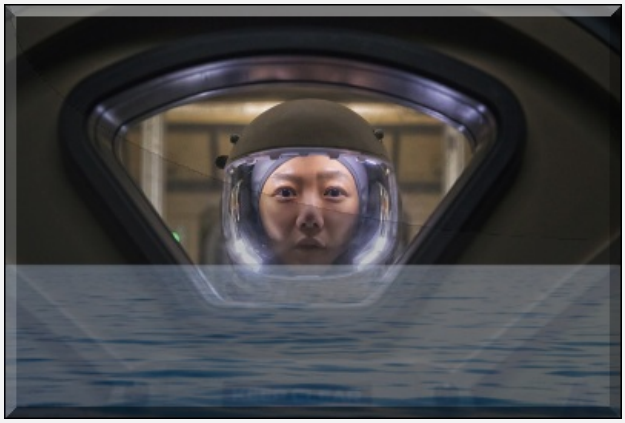
accountz

Belépés
Regisztráció

A nyugtalanság tengere

2022. augusztus 17. 11:26 - Csizmazia Darab István [Rambo]

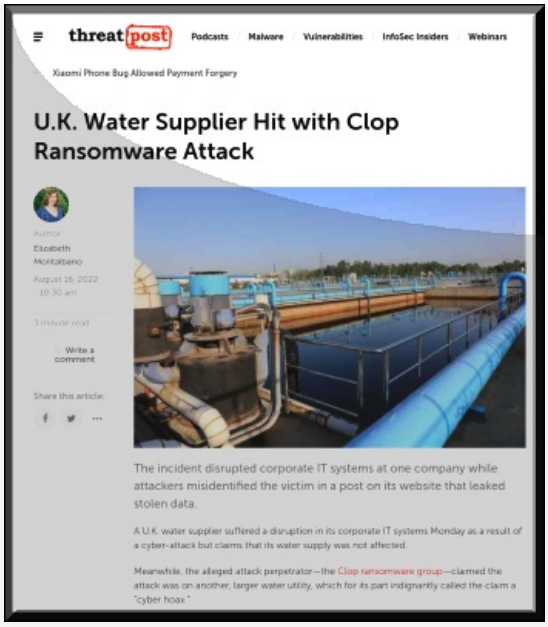
A Conti csoport esete az Egyesült Királyság vízügyi társaságaival is lehetne a cím, melyben immár sokadjára ért ransomware támadás valamilyen kritikus közművet. Azonban az események folytatása a szokásos mederből ezúttal kissé félresiklott, és kiderült, hogy ami majdnem az, az nem az.



Kapcsolgatják a villanyt Ukrajnában? Lelövik az USA keleti partjának üzemanyag-ellátását a Colinial Pipeline csővezeték elleni zsarolóvírustámadással? Kórházakban műtétek maradnak el és válik lehetetlenné a munka? Mezőgazdasági gépgyártó termelése bénul le? Kibertámadással mattot adnak egy komplett országnak?

Ezeket sajnos már mind átélhettük, szerencsére például atomerőművek távoli illetéktelen piszkálása eddig nem fordult elő, vagy legalábbis nem került nagyobb nyilvánosságra.

Ezúttal azonban a South Staffordshire nevű brit vízszolgáltató céget érte ransomware támadás, amelyet a vállalat nyilvánosan is elismerte. Ehhez nagyjából azt kell tudni, hogy ez a vízszolgáltató **nagyjából 1.6 millió fogyasztó ügyfelet lát el**, tehát egy viszonylag kisebb terület ellátásáért felelős. Amint vízügyi vállalatnál észlelték a fennakadásokat az informatikai hálózatban, azonnal megtették a szükséges intézkedéseket, ám a beszámolók szerint **az incidens nem befolyásolta a biztonságos vízellátást a hozzájuk tartozó Cambridge Water és South Staffs Water ügyfeleknek.**



Nagyjából ugyanekkor viszont **nem őket, hanem tévesen a jóval nagyobb, 15 millió ügyfelet ellátó Thames Water szolgáltatót kezdte el fenyegetni a Clop ransomware csoport**, és a váltságdíjat nem csak a titkosított állományok feloldásáért követelte, hanem a doxing keretében ellopott bizalmas és állítólag titkosítás nélkül tárolt adatok nyilvánosságra kerülésének megelőzésére, amelyből **5 TB mennyiséget a kérésük nyomatékosítása miatt publikussá is tettek.**

A Bleeping Computer értesülései szerint viszont az látszik, hogy a kisebb South Staffordshire cégtől lopott dokumentumok nyilvánosságra hozatalával próbálták a nagy, Thames Water szolgáltatót megzsarolni, nagyobb skalppal dicsekedtek, mint ami volt.

A támadók egyúttal azt is állították, hogy nemcsak az adatokat lopták el, de hozzáfértek a SCADA rendszerhez, és tetszés szerint képesek felette távolról átvenni az irányítást, ez szerencsére szintén nem bizonyult valósnak. **Ebben a súlyosan aszályos időszakban nagyon jól irányzott érzékeny csapásnak látszik ez az akció, és jól mutatja, hogy sikeresen választják ki és veszik célba a nehéz helyzetben lévő vállalatokat, szolgáltatókat.**

Időközben a támadók pontosították a követelésüket, és a 355 ezer dollárnak megfelelő összeget immár a valódi célponttól, a South Staffordshire-től kérik.

Mindkét szolgáltató gyorsan reagált, és kivizsgálta az incidenst, elmondásuk szerint **nem állt fenn a hosszabb kimaradások kockázata**. Emlékezetes, hogy **egy éve egy floridai vízszolgáltató informatikai rendszerébe betörtek, és a kiberbűnözők távolról megemelték a folyékony lúg, a Natrium-hidroxid szintjét, amely beláthatatlan katasztrófát idézhetett volna elő, ha a helyi üzemeltetők nem észlelik időben az illetéktelen beavatkozást**.

Ám ezek az esetek is jól mutatják, alapvetően milyen sérülékenyek lehetnek az ellátási rendszerek, és sajnos abban is biztosak lehetünk, nem ez a mostani volt az utolsó ilyen jellegű, **az aktuális nehéz helyzetet kihasználó támadás.**

2 komment

Címkék: infrastruktúra kritikus víz egyesült királyság váltságdíj conti ransomware közművek vízhálózat zsarolóvírus

Ajánlott bejegyzések:

Felkészül: USA kritikus infrastruktúra

Nem csitulnak a kórházak elleni támadások

Emelkedő ransomware károk

Nem szállunk rendelkezésére II.

Durva ransomware statisztikai adatok

Kommentek:

Head Honcho 2022.08.17. 21:57:02

Még mindig nem értem, hogy az ilyen érzékeny rendszerek miért nem hermetikusan zártak a külvilág felé.

Válasz erre

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2022.08.18. 08:50:53

A Conti állítása szerint észrevétlenül hónapokig bent volt a rendszerben, gyalázatosan gyengének minősítette a védelmet, és közben 5 TB adatot töltöttek le a hálózatból. Annyira kevés pénzt ajánlott fel a tárgyalások során a cég, amit nevetségesen kevésnek ítéltek. Állításuk szerint igenis hozzáfértek és manipulálhatták volna a vízminőséget, de ezt mégsem tették.

Viszont most biztos, hogy egy alapos kód elemzés, hálózat átnézés és forensic vizsgálat kell, mert maradthattak bent még időzített eldugott kellemetlenségek, rejtett kódok, módosítások.
www.itpro.co.uk/security/ransomware/368808/uk-water-supplier-confirms-hack-by-cl0p-ransomware-gang

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Egyre gyakoribb a banki adathalászat

2022. augusztus 23. 10:38 - Csizmazia Darab István [Rambo]

Muszáj mindenkinek komolyan venni a jelenséget, ami bár külföldön gyakoribb módszer ugyan, de **nincs olyan hazai bank, amelynek nevében az évek során hetente-havonta ne próbálkoznának a csalók magyar** nyelvű levelekkel, SMS-ekkel, direkt telefonhívással.

Szingapúrban a napokban tartóztattak le négy embert, akiket azzal gyanúsítanak, hogy banki ügyfeleket célzó adathalász csalásokban vettek részt. A módszerük az volt, hogy **az áldozatoknak kéretlen SMS-eket küldtek arról, hogy bankkártyáikat állítólag ideiglenesen felfüggesztették.**

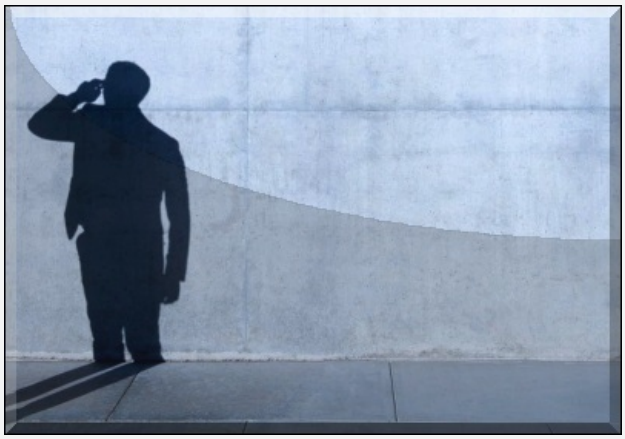
Az SMS arra utasította őket, hogy **jelentkezzenek be és ellenőrizzék személyazonosságukat a mellékelt linken keresztül, ami valójában egy hamisított internetes banki bejelentkezési oldalhoz vezetett**. Aki az adathalász lapon begépelte a név jelszó párosát, és pluszban még a kéttényezős hitelesítéshez használt egyszeri (OTP, One Time Password) kapott kódját is, annak a csalók hozzáfértek a pénzéhez.

A fenti bűncselekmény nem volt egy óriási volumenű visszaélés, és szerencsére kevés számú áldozatot sikerült megtéveszteni a nyomozás gyorsasága és a korai letartóztatás révén. Mondhatnánk, hogy Szingapúr meg amúgy is messze van, mégis mit lehet, sőt kell mindebből megtanulni itt és most?

A fenti vagy ahhoz nagyon hasonló módon bármelyik országban bárkihez érkezhet olyan megkeresés, amelyben számlájának állítólagos feltöréséről tájékoztatja valaki látszólag a bank nevében. Adunk pár tippet, mikre érdemes ilyenkor figyelni, és pénzünk biztonsága érdekében mit ne tegyünk semmiképpen?

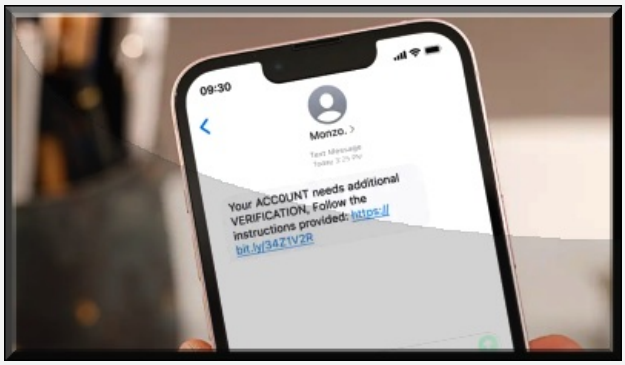
A fenti videóban a magyartalan, akcentusos beszéd és az ostoba viselkedés gyorsan ellentmondásokba kergette a próbálkozó csalót, de nyilván vannak ennél színvonalasabb kísérletek is.

E-mailes adathalászatnál mi is milliószor írtunk már a gyenge helyesírás, a Fülig Jimmy és Tuskó Hopkins nyelvezetű üzenetekről, tehát **ez is egy intő jel lehet a sok közül**. Igaz, évről évre egyre jobb minőségű, és helyes magyarsággal írt levél is megjelenik.



Egyáltalán ügyfelek vagyunk az adott szolgáltatónál? Ha nem bank, hanem csomagküldő szolgálat nevével élnek vissza, ott sokkal hatékonyabban sikerülhet az átverés, csomagot ugyanis bárki kaphat, még ha nem is vár éppen konkrét helyről - erről szólt a tavaly márciusi FedEx nevével visszaélő FluBot vírusos SMS üzenetek esete. **Ott azt volt érdemes megjegyezni, hogy kéretlen SMS üzenetben érkező linkre nem kattintunk, onnan semmilyen alkalmazást nem telepítünk, nem is adunk meg neki semmilyen engedélyt, és igen jót teszünk magunkkal, ha naprakész vírusvédelmi megoldást használunk a mobilunkon.**

Érdekes módon a teljesen idegen, a szolgáltatóra nem is hasonlító linkre tömegesen kattintottak az emberek, ilyet sem érdemes elkövetni.

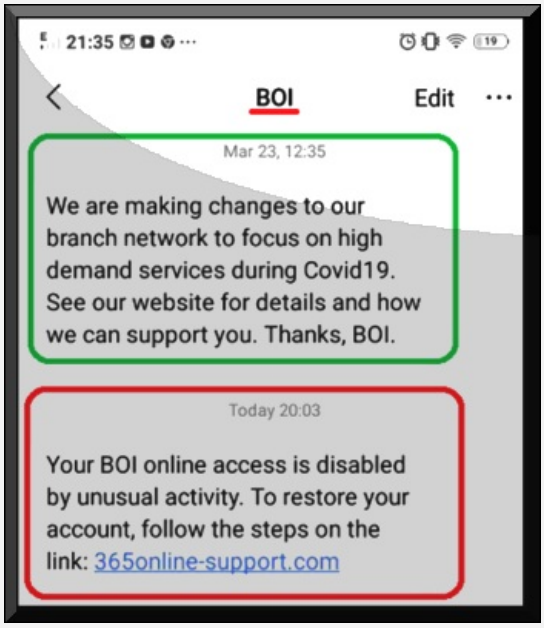


A bevezetőben leírt esetnél volt még egy érdekesség, ami más csalásoknál is előfordul. **Sosem szabad kétlépcsős azonosítási kódokat idegeneknek, ismeretleneknek megadni, elküldeni, bediktálni, megosztani**. Ezek a kódok a mi biztonságunkat szolgálják, de csak addig, amíg nem kerülnek illetéktelen kezekbe, mert onnantól már tudtunk és beleegyezésünk nélkül megszemélyesíthetnek vele bennünket. **A banki tisztviselők soha nem fogják SMS-ben elkérni a banki adatainkat vagy az egyszeri megerősítő jelszavainkat**.

A mit ne tegyünk listára kívánkozik még, hogy legyünk gyanakvóak, biztonságtudatosak, óvatosak. **Ha nem értjük a szituációt, ne hagyjuk magunkat sürgetni, kérjünk a környezetünktől segítséget, szakítsuk meg a hívást, és hívjuk fel mi a bankunkat, hogy tisztázzuk a helyzetet.**

Hazai eset volt, amikor autó, illetve egy lakás eladás kapcsán a csalók elérték azt, hogy az áldozat hajlandó volt egy mellékelt linkről ismeretlen programot feltelepíteni a számítógépére.

Ilyet sem szabad engedni, megtenni, **a fenti esetekben 30, illetve 50 millió forintot loptak el a csalók, ugyanis olyan hátsóajtó szoftvert sikerült feltelepíteniük, amelynek segítségével tetszőleges fájlokhoz, például céges aláírási címpéldányhoz is hozzájutottak.**

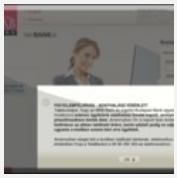


És végül a külföldi és hazai banki csalásoknak **ugyancsak eleme lehet az is, amikor az állítólagos banki ügyintéző éppen zajló visszaélésre, feltörésre hivatkozva azt kéri az áldozattól, biztonsága érdekében azonnal utalja át ideiglenesen az összes pénzét egy a csaló által bediktált, védettnek mondott számlaszámra.**

Aki ennek bedőlt, az keresztet vethetett a pénzére, és ami még szomorúbb, ezekben az esetekben mivel az ügyfél hibázott, a pénzintézet nem téríti meg a károkat. Érdemes tehát óvatosnak lenni minden hasonló megkeresésekkel, és betartani a fenti óvintézkedéseket.

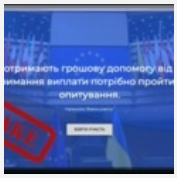
1 komment
Címkék: bank csalás átverés phishing adathalászat

Ajánlott bejegyzések:


MKB adathalászat szigonnyal, horoggal, hálóval


A bankos mindig kétszer csenget...

Tagsági kérdések - vagy mégsem?


Adathalászok lakat alatt

Banki meló

Kommentek:

RocketDoll · https://somagyarkaszino.com 2022.08.23. 14:02:30

Nemrég én is kaptam ezt az üzenetet. Nem tudom, honnan szerezték az információimat.

Válasz erre

keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

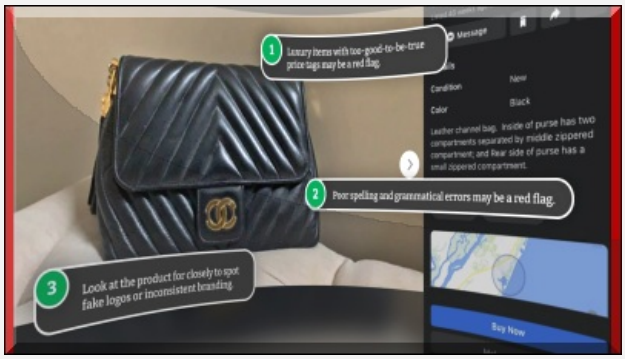
Átverések az online piactéren

2022. augusztus 25. 12:11 - Csizmazia Darab István [Rambo]

Tavaly a Facebook Marketplace felhasználóinak száma átlépte az egymilliárdot. Az egymás közötti adásvételt lehetővé tévő **platform ingyenes és könnyen használható**, a felhasználók pedig biztonságosnak érzik, mivel az eladók profilját is meg tudják nézni. Sajnos azonban ez a biztonságérzet gyakran hamis, mivel **a Marketplace is rengeteg csalót vonz.**

Egy közelmúltban készült felmérés **résztvevőinek hatoda (17%) volt már csalás áldozata az Facebook Marketplace-en**, a Facebook pedig nehezen tudja kiszűrni a csalókat. Olykor túlbuzgón blokkolja a szabályosan hirdető felhasználókat, miközben más esetekben akaratlanul is lehetővé teszi, hogy csalók kikerülhessék az automatikus ellenőrzést és a platform adminisztrátorait.

Mivel **a hamis hirdetések a lakáseladásokat és az autóvásárlásokat is érintik, a tét ott már elég nagy.** Ezért nagyon fontos, hogy a felhasználók megismerjék az online csalók tipikus trükkjeit, és megtudják, hogy mit tehetnek biztonságuk érdekében.



A megélhetési költségek növekedésével **egyre több magyar felhasználó fordul az olyan online platformokhoz, mint a Facebook Marketplace, hogy eladóként gyorsan pénzhez juthasson, vagy vevőként minél alacsonyabb áron vásárolhasson termékeket.** Ezzel párhuzamosan viszont sajnos a csalók is egyre nagyobb számban jelennek meg az online piactereken, ezért a biztonságtudatosság és az óvatosság továbbra is kiemelten fontos.

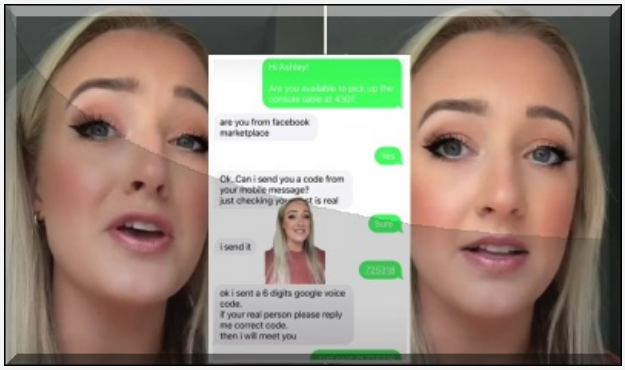
Akárcsak az adathalászatnál, **az intő jelek korai felismerése - gyanúsan alacsony ár, magyartalan nyelvhasználat, sürgetés - itt is megóvhat minket az áldozattá válástól**. Az alábbiakban az ESET kiberbiztonsági szakértői **nyolc, a Facebook Marketplace-en leggyakrabban előforduló csalást mutatnak, és tanácsokat adnak arra vonatkozóan, hogyan lehet kivédeni ezeket.**

1. Hibás termékek
Az eladók hirdethetnek olyan terméket, amely a közzétett **fotó alapján jó állapotúnak tűnik** ugyan, de amint megkapjuk, kiderül, hogy törött vagy nem működik. Ez **különösen az elektronikai cikkek esetében lehet igaz, amelyek összes funkcióját ebben a formában nem tudjuk kipróbálni vásárlás előtt**. Mindez ugyanolyan valószínűséggel történhet egy gátlástalan eladó vagy egy hivatásos csaló részéről is.

2. Hamisítványok
Ha nem törött, akkor lehet, hogy **hamis termékről van szó. A designer ruhákat, parfümöket, ékszereket és kozmetikumokat különösen gyakran hamisítják**, egy fotó alapján viszont gyakran nehéz megállapítani az áru valódiságát. Bár mindenki az akciós árakat keresi, itt is igaz az állandó szabály: ha egy ajánlat túl jónak tűnik ahhoz, hogy igaz legyen, valószínűleg csalásról van szó.

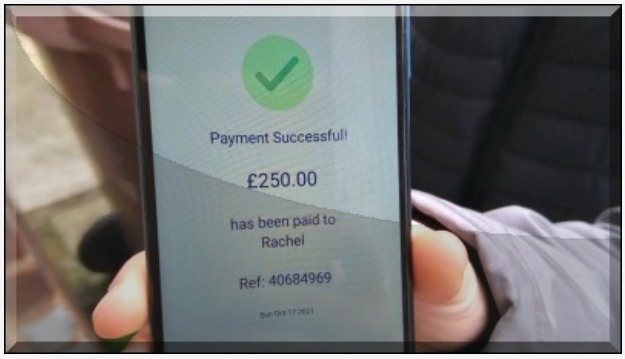
3. Google Voice átverések
A Facebook Marketplace-t más típusú csalásokra is használják. Tegyük fel például, hogy a csaló beleegyezik egy termék megvásárlásába. Ezek után viszont a beszélgetést egy másik, nem ellenőrzött platformra, **például a WhatsAppra tereli, ahol arra kéri az eladót, hogy hitelesítse magát egy ellenőrző kóddal.**

Valójában viszont az eladó telefonjára érkezett kód egy Google Voice által küldött, a csaló által kezdeményezett kétfaktoros hitelesítési kód. **A hitelesítés után a csalók képesek a nevünkben fiókot létrehozni az eladó telefonszámával, amelyet mások átverésére is felhasználhatnak.** Egyéb információ birtokában pedig megpróbálhatnak további új profilokat létrehozni az áldozat nevében vagy hozzáférhetnek a meglévőkhöz.



4. Állítólagos túlfizetés
A csalók az eladókat is átverhetik a Facebook Marketplace-en. Például amikor **azt állítják, hogy többet fizettek egy adott termékért a megadott árnál, és közzétesznek egy képernyőfotót, amelyen az állítólagos tranzakció látható**, követelve a különbözet visszatérítését.

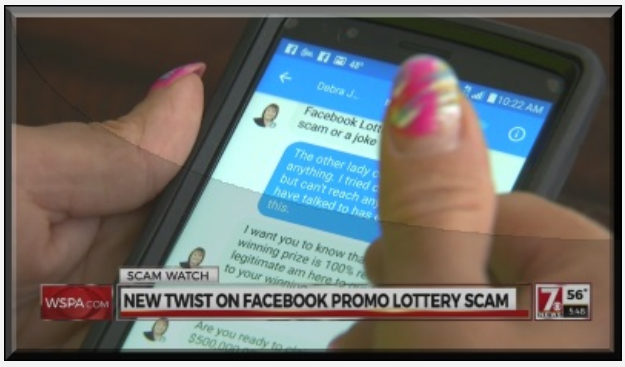
5. Szállítás elmaradása
Klasszikus trükknek számít, hogy **eladnak egy terméket, elkérik a pénzt, de a termék mégsem érkezik meg** a vevőhöz, vagy csak egy tégla van a csomagban Xbox helyett.



6. Hamis nyereményjátékok
Az információk megszerzésének egy másik módja a hamis nyereményjátékok közzététele a Facebook Marketplace-en. **A gyanútlan felhasználó mindössze egy linkre kattint, ahol személyes adatokat ad meg magáról abban a**

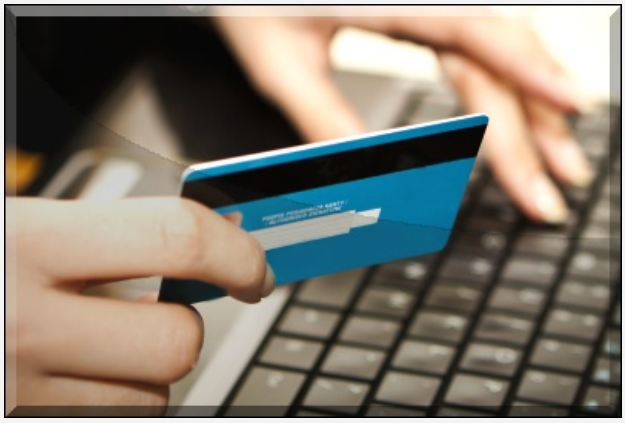
hitben, hogy ingyenes luxuscikkeket, kriptodevizát vagy más különleges ajándékot kaphat.

A csalók viszont kizárólag a személyes adatokat akarják megszerezni, hogy azokkal további személyazonossággal kapcsolatos csalást vagy lopást kövessenek el.



7. Biztosítási csalás
A drága árucikkeket közzétevő eladókkal is gyakran kapcsolatba lépnek szélhámosok. A csalók vállalják, hogy kifizetik a szállítási költséget, ennek bizonyítékául egy hamis számlát küldenek. Emellett **az eladótól előre egy biztosítási díjat is kérnek: mivel az összeg viszonylag kicsi az eladásra szánt tárgy értékéhez képest, az eladók gyakran belemennek az ilyen állítólagos díj kifizetésébe.**

8. Beetetés, figyelemfelkeltés
A csalók gyakran kiváló minőségű terméket hirdetnek nagyon kedvező áron. **Amikor a vásárló szeretné megvásárolni az akciós terméket, az eltűnik a rendszerből, a csalók pedig vagy egy hasonló terméket ajánlanak** fel magasabb áron vagy egy rosszabb alternatívát.



Hogyan lehet kiszúrni a Facebook Marketplace átveréseket? **Az alábbi tíz tipp segíthet abban, hogy biztonságosan használhassuk a Facebook Marketplace felületét:**

- Vásárlás előtt **ellenőrizzük az árucikkeket, és csak helyi** eladóknál vásároljunk.

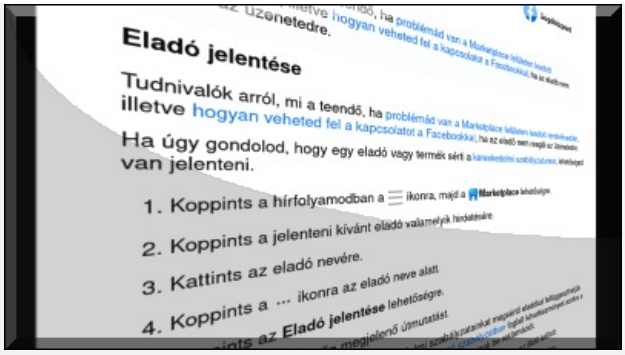
- Mindig nyilvános helyen történjen **az átadás-átvétel**, lehetőleg jól megvilágított helyen, a nappali órákban. A benzinkutak, bevásárlóközpontok további előnye, hogy ott biztonsági kamerák is működnek.

- Ellenőrizzük az **eladók/vásárlók profiljait, a felhasználói értékeléseket**, és gyanakodjunk, ha a profilokat csak nemrég hozták létre, vagy túl rövid idő alatt gyanúsan sok pozitív értékelést látunk.

- **Keressünk rá a termékek eredeti árára**, és ha ennél jelentősen alacsonyabb áron kínálják a Marketplace-en, legyünk gyanakvóak, mert az árucikk hamisítvány, lopott vagy hibás lehet.

- Óvakodjunk a **nyereményjátékoktól, és ezen a címen soha ne adjuk ki személyes adatainkat!**

- Válasszunk **biztonságos fizetési módokat (PayPal, Facebook, Checkout),** mivel ezek lehetőséget biztosítanak a visszatérítésre. Az ajándékkártyákat, átutalásokat, és az olyan fizetési szolgáltatásokat, mint a Venmo vagy a Zelle, előszeretettel használják a csalók.



- **Csak a Facebookon egyeztessünk** - a csalók szeretik átterelni a beszélgetést egy másik platformra, ahol könnyebben átverhetik az embereket, és esetleg megakadályozhatják, hogy vitassák a tranzakciókat. Ha maradunk a Facebookon, akkor minden kommunikáció itt naplózódik, ami később jól jöhet bizonyítékként.

- **Soha ne adjunk fel csomagokat előre, az ellenérték kifizetése előtt**. Kivétel itt a Foxpost és egyéb hasonló pénzkezelő csomagautomatás megoldások, amelyek garantálják, hogy a vevő csak a sikeres fizetés után veheti át a csomagunkat.

- **Vevőként figyeljünk a termék listaárának változásaira, valóban akciós-e az akciósnak mondott ár.**

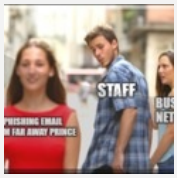
- **Soha ne küldjünk kétlépcsős azonosítási kódokat állítólagos leendő vásárlóknak, idegeneknek, ismeretleneknek. Ezek a kódok a mi saját biztonságunkat szolgálják, csak ránk tartoznak, ezért tilos azokat bediktálni, továbbküldeni, másokkal megosztani.**

Ha mégis bekövetkezik a legrosszabb, és csalást gyanítunk, jelentsük az eladót a Facebook felé.

3 komment
Címkék: facebook csalás tippek átverés megelőzés marketplace piactér

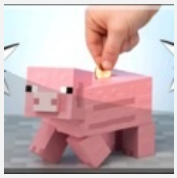
Ajánlott bejegyzések:

Nagy pénz, nagy foci, nagy átverések



10 gyakori ok, amiért bedőlünk a csalásoknak


Fiatal vagy? Ezekre az online csalásokra figyelj!


A csalások már a spájzban vannak

Gratulálunk - mihez is?

Kommentek:

para_noir 2022.08.26. 08:40:38

Az ilyen primitív csalásokkal csak a hülyéket lehet megvezetni. Sokkal gázabb, hogy a rohadt marketplacre nem lehet felrakni normálisan márkás, eredeti terméket, mert automatiksuan hamisítványnak veszi, és jön a fenyegető üzenet, hogy még egy ilyen, és korlátoznak.

Válasz erre

BOAR 2022.08.26. 12:29:46

Bullshit.
Idézetek a közhelyszótárból c. műsorunkat hallhatták...

Válasz erre

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2022.08.27. 15:34:48

Ezek MAGYAR adatok, ahol adathalász oldalra léptek be, vagy állítólagos banki ügyintézőknek válaszolgattak az

áldozatok:

"A Pénzügyi Békéltető Testülethez (PBT) 2018. január 1. és 2022. május 15-e között 343 „jóvá nem hagyott fizetési művelettel” kapcsolatos fogyasztói jogvita került – ezek közül 231 volt bankkártyával kapcsolatos visszaélés, 112 pedig fizetési számlához kapcsolódó tranzakció. Ezekből 295 zárult le – 227 eljárás végződött megszüntetéssel, többnyire azért, mert az ügyfél szolgáltatta ki az adatait, biztosított hozzáférést eszközeihez, illetve maga végezte a műveleteket vagy hagyta jóvá azokat. "

24.hu/fn/gazdasag/2022/08/27/eletuk-megtakaritasa-lenyulas-telefonos-banki-csalok-nyugdijas-par/

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

Durva ransomware statisztikai adatok

2022. augusztus 30. 12:41 - Csizmazia Darab István [Rambo]

Tovább emelkedhetnek a kiberbiztosítási díjak, ugyanis **olyan mennyiségű incidens történik elsősorban az állami szféra által üzemeltetett rendszerekben, amelyek a mostani feltételekkel már komoly veszteséget okoznak a biztosítóknak**.

A biztosítók egy része a széles körben elterjedt támadások jelentette fenyegetések miatt **ebben a konstrukcióban már egy ideje nem is hajlandó a váltságdíj kifizetésre, így döntött például tavaly az AXA.**

A manchesteri székhelyű NCC Group információbiztosítási cég adatai azt mutatják, hogy **2022. júliusban 45%-kal nőtt a ransomware támadási események száma az előző év azonos időszakához képest.** Bár a zsarolóvírus bandák ténykedésében történtek hullámzásszerű visszaesések és emelkedések - például a Conti és a LockBit 3.0 visszatérésével - **az előző hónaphoz képest is 47%-os ijesztő növekedést regisztráltak.**

Az AtlasVPN közleménye pedig arról árulkodik, hogy **2022-ben 320 incidens során eddig már 30 TB érzékeny adatot sikerült a bűnözőknek ellopniuk. A latencia miatt ez szám sokkal nagyobb is lehet**, hiszen csak az esetek egy része kerül bejelentésre és nyilvánosságra.

Emlékezetes, hogy többek közt az Nvidia is elszenvedett ilyen támadást, ahol **1 TB zsákmányolt bizalmas adatért cserébe 1 millió dolláros váltságdíjat követeltek.**

Riasztó számok jelzik a váltságdíjak globális mértékének alakulását is. A kutatások kimutatták, hogy a **követelt összeg 105%-kal nőtt az előző, 2021-es értékekhez képest**. A támadási próbálkozások **gyakorisága is elképesztő, a 2021-es évben átlagosan másodpercenként 20 kísérletet jelent.**

Ezen belül is az Egyesült Államok volt leginkább a célkeresztben, egymaga lényegesen több ransomware fenyegetést (421.5 millió) szenvedett el, mint bármely más ország. **Az összes támadás 48%-a irányult az USA ellen, a szektorokat tekintve pedig az ipari és energetikai, kiskereskedelmi és pénzügyi vállalkozások tartoztak a legveszélyeztetettebb ágazatok közé.**

A Veeam 2022. Ransomware Trends Report szerint **a megtámadott szervezetek 73%-a szenvedett el kettő vagy ennél is több ransomware támadást az elmúlt 12 hónap során.**

Ebben az is közrejátszhat, hogy egyrészt **a doxing miatt nagyobb a fizetési hajlandóság a cégeknél**, másrészt a behatolás során a támadók a már feltört hálózatokban sokszor igyekeznek rejtett hátsóajtót telepíteni, hogy később újra lehessen fertőzni a fizetőképes vállalatokat.

A statisztikai számmágia még olyan adatokat is kimutat, hogy állítólag a japán és holland székhelyű vállalkozások fizetik a legmagasabb váltságdíj összegeket a zsarolóvírus támadásoknál. A japán cégek átlagosan 4.3 millió dollár értékben (1.7 mrd HUF), míg a hollandok átlagosan 2m USD, azaz nagyjából 811 millió forintnyi összegű kriptovalutát utalnak át elkódolt adataikért és a lopott adatok nyilvánosságra kerülés megelőzésének reményében.

Végül zárásképpen pedig belinkeljük azt az összefoglaló tudástárat, amelyben minden fontos információ megtalálható védekezés és megelőzés témakörben.

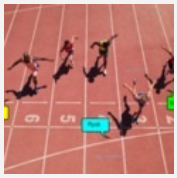
Szólj hozzá!
Címkék: statisztika tudástár biztosítás eset váltságdíj ransomware zsarolóvírus

Ajánlott bejegyzések:

Ransomware helyzetjelentés


Emelkedő ransomware károk


Ransomware a spájzban


Világrekord, aminek mégsem örül senki

A ransomware-nek nincs No-go zóna

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Antivírusblog
245 követő

Oldal követése Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker

2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.

VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

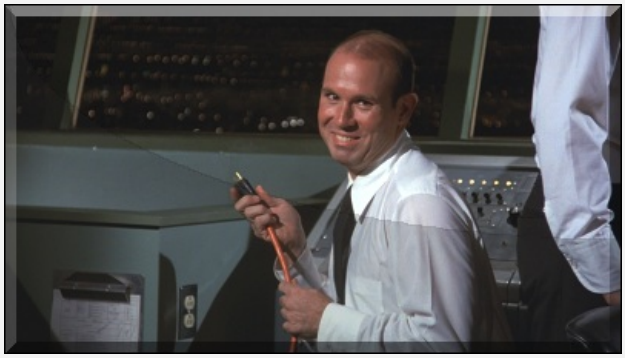
accountz

Belépés
Regisztráció

Nem szállunk rendelkezésére II.

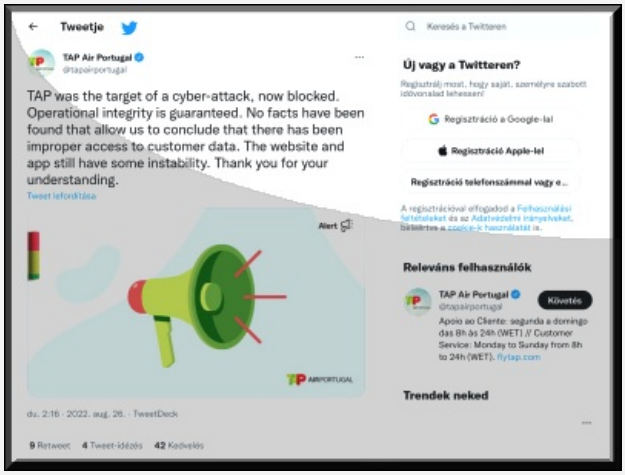
2022. szeptember 01. 13:18 - Csizmazia Darab István [Rambo]

Brit repülőtér már szerepelt a történetünkben, ahol **jó négy éve zsarolóvírusos támadás miatt két napon keresztül számítógépes kijelzők híján filctollal írt papír listákról olvashatták le az utasok az aktuális járat információkat.** Idén májusban pedig I**ndia második legnagyobb légitársasága, a SpiceJet szenvedett el zsarolóvírus incidenst, ami késéseket, járatkimaradásokat okozott. És akkor most felkészül TAP Air Portugal.**



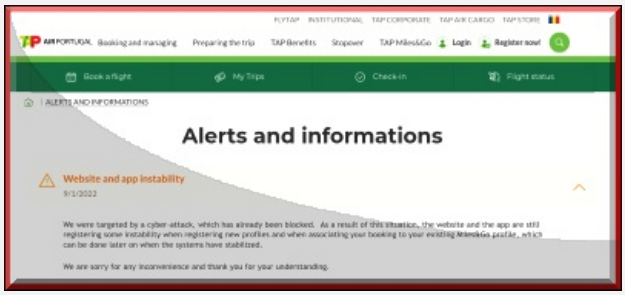
A **Ragnar Locker banda bejelentette, hogy augusztus utolsó napjaiban sikeres támadást intézett Portugália legnagyobb légitársasága**, a TAP Air Portugal ellen.

A vállalat ezzel szemben azt állítja, hogy a próbálkozást blokkolták, és hozzátették, nem talált bizonyítékot arra, hogy a támadók hozzáfértek volna az érintett szervereken tárolt érzékeny ügyféladatokhoz. **Twitter bejegyzésükben cáfolták a kibertámadás sikerét, szerintük a működéssel minden rendben, az garantált.**



Mai, azaz **szeptember 1-i figyelmeztetésükben azt jelzik, hogy a hivatalos weboldal és a járatfoglalás nem elérhető a múlt csütörtöki kibertámadás** miatt.

Egyúttal elnézést kérnek a kellemetlenségekért, és köszönik a szíves megértést.



Ám innentől aztán kicsit már a LockBit VS. olasz adóhivatal csörtéhez hasonlít az ügymenet, ahol a két fél különbözőt állít, ám a kettő egyszerre nem lehet igaz.

Ugyanis **a Ragnar Locker időközben több száz GB ellopott adatról beszélt, és ennek bizonyítására egy képernyőképet is megosztottak egy olyan táblázatról**, amely látszólag a TAP szervereiről ellopott ügyféladatokat tartalmazza, beleértve olyan érzékeny ügyféladatokat, mint név, születési dátum, e-mail elérés és lakcím.

Az incidensről hírt adó Bleeping Computer megkereste a légitársaságot a kérdéseivel, ám egyelőre nem kapott ezekre választ.

A Ragnar banda **korábbi skalpjai között olyan cégek szerepelnek, mint az Energias de Portugal (EDP) portugál multinacionális energiavállalat, a Capcom japán videojáték-gyártó cég, az ADATA számítógépes félvezetőgyártó és a Dassault Falcon repülőgépgyártó vállalat.**

Szólj hozzá!
Címkék: portugália légitársaság váltságdíj ransomware locker tap zsarolóvírus ragnar doxing

Ajánlott bejegyzések:

Ha szólsz a rendőröknek, akkor véged!

LockBit vs. olasz adóhivatal


Baljós árnyak: fekete macska Karintiában

Fordulat ransomware fronton


Rossz gondolatok a könyvtárban

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.

VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

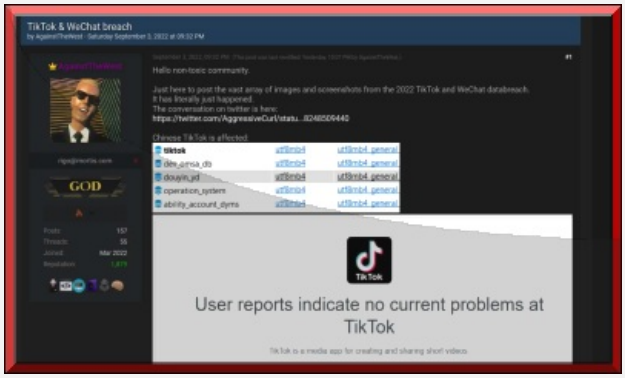
TikTok VS. AgainstTheWest

2022. szeptember 06. 12:33 - Csizmazia Darab István [Rambo]

Bejelentkezett egy támadó csoport, hogy **állítólag sikeresen feltörték az igen népszerű TikTok és a WeChat rendszerét,** ennek bizonyítására pedig képernyőképeket is nyilvánosságra hoztak az adatbázisokról.

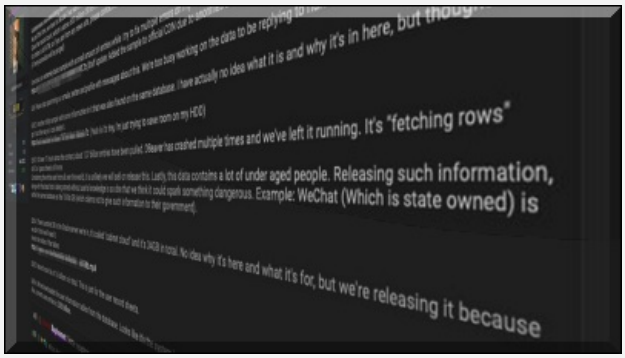
Az AgainstTheWest hackercsoport nevével ellentétben nem a nyugati országok megbüntetését tűzte ki célul, hanem sokkal inkább ezek védelmét a keletről érkező támadások ellen, így ellenfeleik közé sorolják Kínát, Oroszországot, Észak-Koreát és Iránt.

Jelen esetben a kínai TikTok és WeChat volt a célpontjuk, és **weboldalukon szeptember 3-án azt állították, sikeres feltörés után egy 2 milliárd rekordot tartalmazó 790 GB méretű adatbázist sikerült zsákmányolniuk a TikTok rendszeréből** egy Alibaba felhős rendszeren keresztül. Ennek illusztrálására a Breach Fórumon részleteket is bemutattak az említett adatállományból.



A támadók **felhasználói adatokat, platformstatisztikákat, cookie-kat, hitelesítési tokeneket, szerverinformációkat is megkaparintottak, sőt állítólag még forráskódokat is.** Ezzel szemben a TikTokot üzemeltető ByteDance azt állítja, **semmilyen bizonyítékot nem találtak az adatsértésre, a fórumon megosztott forráskód sem része a rendszerüknek**, ami lehet egy szokásos sablon válasz és szintén lehet akár igaz is.

Az adatállománnyal kapcsolatban is **úgy nyilatkoztak, kizárt, hogy közvetlen feltörés útján sikerült volna valakinek begyűjtenie ezeket az adatokat**. Az újságírók megkeresték a WeChat-et üzemeltető Tencent vállalatot is, ám a cikk megírásáig nem kaptak választ tőlük.



Ahogy a ransomware+doxing támadásoknál is előfordul, van olyan eset, amikor a támadók pusztán csak bepróbálkoznak azzal, hogy sikeresen elloptak ügyféladatokat, ám ez időnként nem mindig fedi a valóságot.

Jelen esetben az adatbázisban szereplő adatokról **több szakértőt is megkérdeztek**, akik szerint ezek legitim

adatoknak látszanak ugyan, de mivel ezeket nyilvános adatbázisokból is össze lehet szedni, úgy nyilatkoztak, **pusztán ez alapján még nem látszik bizonyítottnak a feltörés. Többek közt [Troy Hunt, a Have I been Pwned weboldal üzemeltetője is így vélekedett.]**

Amit egy **hétköznapi felhasználó tenni tud egy szolgáltatót ért valóságos feltörés esetén, vagy ennek kockázatát megelőzendő, minden lényeges belépési helyen erős és egyedi jelszót használjunk, a böngészőkkel sose jegyeztessük meg a jelszavainkat, inkább használjunk jelszó széfet. Mindezt támogassuk meg kétfaktoros autentikációval, és adott időközönként változtassuk is meg a jelszavainkat.**

Emellett érdemes figyelemmel kísérni **a szolgáltatók jelzéseit is, akik bizonyított incidens esetén jó esetben figyelmeztetik erre ügyfeleiket.** Ám egy korábbi statisztika szerint a felhasználók ötöde (18%-a) simán figyelmen kívül hagyja az incidensek miatti azonnali jelszócsere figyelmeztető jelzéseket. Bár ez több éves statisztikai adat, sajnos nincs okunk azt gondolni, hogy ez most 2022-ben sem okoz senkinél problémát.

Szólj hozzá!
Címkék: incidens feltörés tiktok tencent wechat bytedance doxing againstthewest

Ajánlott bejegyzések:

Esemény utáni teendők

GoDaddy - apák a pácban

Még gyengébb a jelszavad

GTA6 - Ellopták a lopós játékot


Nem szállunk rendelkezésére II.

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

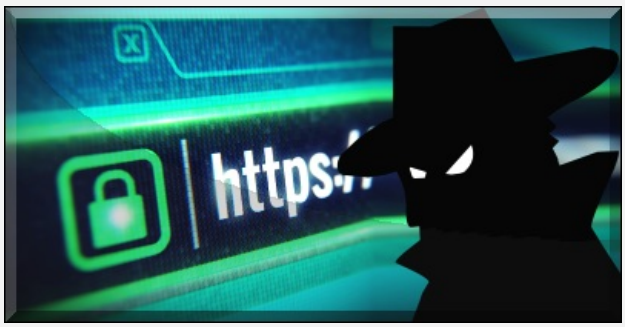
accountz

Belépés
Regisztráció

Böngészés - kockázatok és mellékhatások

2022. szeptember 08. 08:38 - Csizmazia Darab István [Rambo]

Hirdetők és más szereplők a böngészőn keresztül hozzájuthatnak személyes adataikhoz és nyomon is követhetik azokat. A böngészők az évek során a **hitelesítő adatok, cookie-k, webes keresések, szokásaink és más hasznos információk tárházává váltak**, amelyek a kiberbűnözők közkedvelt célpontjai is lehetnek.



A támadások által akár távolról is irányítani tudják számítógépünket és hozzáférhetnek a hálózathoz, amelyre csatlakoztunk. A böngészőket érintő legfőbb fenyegetéstípusokat viszont érdemes ismerni.

- A böngészőkben vagy a telepített bővítményekben, kiterjesztésekben található sebezhetőségek kihasználása: ez a taktika alkalmas lehet érzékeny adatok ellopására vagy további kártékony programok letöltésére. A támadások gyakran adathalász e-maillel, üzenettel vagy egy veszélyes webhely meglátogatásával kezdődnek, amelyet a támadó felügyel (drive-by-download típusú támadás).

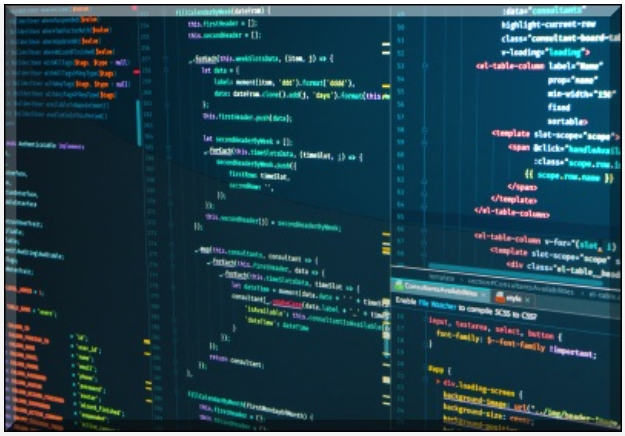
- Kártékony bővítmények: Több ezer bővítmény létezik, amelyeket a felhasználók letölthetnek a böngészési élmény fokozása érdekében. Sok plug-in viszont jogosult a böngészőhöz való hozzáférésre. Ez azt jelenti, hogy a legálisnak tűnő, de valójában kártékony bővítményeket adatlopásra, további malware-ek letöltésére és más rosszindulatú célokra is felhasználhatják.

- DNS-mérgezés: A DNS az internet címjegyzéke, amely az általunk beírt domainneveket IP-címekké alakítja át, hogy a böngészőink megjeleníthessék az általunk meglátogatni kívánt oldalakat. A számítógép által tárolt DNS-bejegyzések vagy maguk a DNS-kiszolgálók elleni támadások azonban lehetővé tehetik a támadók számára, hogy a böngészőket kártékony domainekre, például adathalász oldalakra irányítsák át.

- A munkamenet eltérítése: A munkamenet-azonosítókat a webhelyek és az alkalmazásszerverek adják ki, amikor a felhasználók bejelentkeznek. Amennyiben viszont a támadóknak sikerül ezeket az azonosítókat feltörni vagy ellopni (ha nincsenek titkosítva), akkor álcázva magukat bejelentkezhetnek a nevünkben ugyanazokra az oldalakra, alkalmazásokra. Innen pedig már csak egy lépés az érzékeny, akár pénzügyi adataink ellopása.

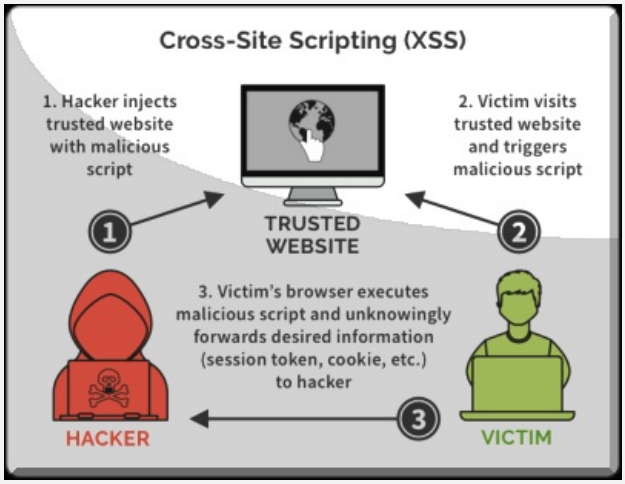
- Közbeékelődéses/böngésző támadás: Ha a támadónak sikerül bejutnia az általunk meglátogatott weboldal és a böngészőnk közé, képes lehet eltéríteni a kommunikációs csatornát – például átirányíthat egy adathalász oldalra, zsarolóprogramot telepíthet vagy belépési adatokat lophat. A kockázat sokszorosára nő a nyilvános Wi-Fi hálózatok használata esetén.

- Webalkalmazások elleni támadás: Az olyan támadások, mint az úgynevezett „cross-site scripting”, amelyek a számítógépen lévő alkalmazásokat célozhatják meg a böngésző helyett, de utóbbit használják a kártékony hasznos tartalmak továbbítására vagy futtatására.
Az adatvédelmi szempontok



A felsorolt esetek mindegyikében szerepet kap egy rosszindulatú harmadik fél. De nem szabad megfeledkeznünk arról a **nagy mennyiségű adatról sem, amelyet az internetszolgáltatók, a webhelyek és a hirdetők nap mint nap gyűjtenek a látogatókról, miközben ők a világhálón böngésznek. A cookie-k (websütik) a webszerverek által generált kis kódrészletek, amelyeket a böngésző egy bizonyos ideig tárol.** Egyrészt olyan információkat tárolnak benne, amelyek segíthetnek személyre szabni a böngészési élményt – például releváns hirdetések megjelenítésében vagy annak biztosításában, hogy ne kelljen többször bejelentkeznie ugyanarra az oldalra.

Másrészt viszont adatvédelmi aggályokat és potenciális biztonsági kockázatot is jelenthetnek, ha a hackerek megszerzik őket, és ezzel hozzáférnek a felhasználói műveletekhez. Az Európai Unióban és néhány amerikai államban szabályozott a cookie-k használata. Amikor viszont egy felugró ablakban megjelennek a lehetőségek, **sok felhasználó egyszerűen rákattint az alapértelmezett sütibeállítások elfogadására, ami leggyakrabban az összeshez való teljes hozzájárulást jelenti.**



Ezek után akkor hogyan böngészhetünk biztonságosabban az interneten? A felhasználók maguk is sokat tehetnek azért, hogy csökkentsék a biztonsági és adatvédelmi kockázatokat az internetes böngészés során.

- Tartsuk naprakészen böngészőnket és annak bővítményeit, mérsékelve a sebezhetőség kihasználásának kockázatát. Távolítsunk el minden elavult bővítményt, hogy tovább csökkentsük a támadási felületet.

- Csak HTTPS oldalakat látogassunk (amelyeknél a böngésző címsorában lakat van), így a hackerek nem tudják egyszerűen megfigyelni a böngésző és a webszerver közötti forgalmat.

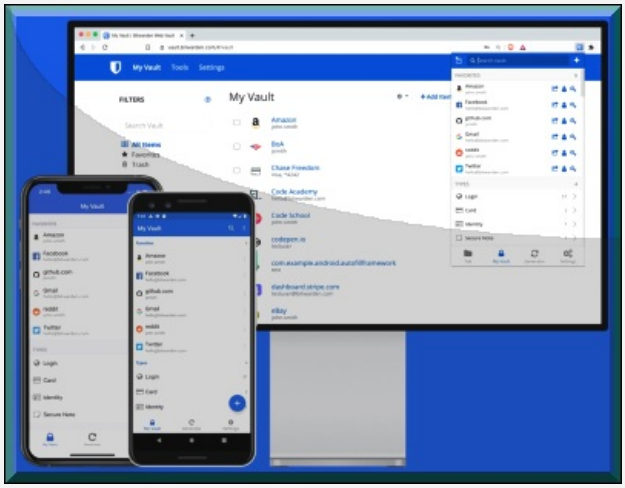
- Legyünk elővigyázatosak, és csökkentsük az e-maileken és online üzeneteken keresztül terjedő fenyegetések kockázatát. Soha ne válaszoljunk kéretlen e-mailekre, és ne kattintsunk rájuk anélkül, hogy ellenőriznénk a feladó adatait. Ne adjunk ki ezekre semmilyen érzékeny információt.

- Gondoljuk át, mielőtt bármilyen alkalmazást vagy fájlt letöltenénk. Mindig használjuk a hivatalos weboldalakat, és csak megbízható programokat, böngészőkiegészítőket telepítsünk.

- Használjunk többfaktoros hitelesítési (MFA) alkalmazást, hogy ezzel is csökkentsük a hitelesítő adatok ellopásával járó kockázatokat.

- Használjunk megbízható szolgáltatótól származó VPN-t. Ez egy titkosított csatornát hoz létre az internetforgalom számára, fenntartva a biztonságot, elrejtve adatainkat illetéktelen harmadik fél elől.

- Szerezzünk be többszintű biztonsági szoftvert egy megbízható vírusvédelmi gyártótól.



- Engedélyezzük az automatikus frissítéseket az operációs rendszeren és az eszköz/készülék szoftverein.

- Frissítsük a böngésző beállításait a megfigyelések megakadályozására, valamint a harmadik féltől származó cookie-k és felugró ablakok blokkolására.

- Kapcsoljuk ki a jelszó automatikus mentését a böngészőben, még annak tudatában is, hogy ez hatással lesz a felhasználói élményre. Ehelyett használjunk inkább jelszószéf alkalmazást.

- Fontoljuk meg egy adatvédelem-központú böngésző és keresőmotor használatát a bizalmas adatok megosztásának csökkentése érdekében, ilyen például a DuckDuckGo.

- Használjuk a privát böngészési beállításokat (inkognitó mód) a cookie-k nyomon követésének korlátozására.

Az ESET fenti tippjei segíthet azoknak, akik aggódnak adataik védelme miatt. Egyes felhasználók viszont hajlandóak elfogadni bizonyos mértékű nyomonkövetést a kényelmesebb böngészési élményért cserébe, de ezek már egyéni döntések.

A fenti biztonsági tippek (például HTTPS, automatikus frissítések, biztonsági szoftverek) azonban elengedhetetlenek ahhoz, hogy hatékonyan csökkenthessük a kiberfenyegetettséget.

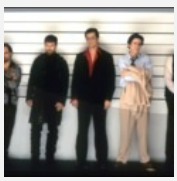
1 komment
Címkék: biztonság adatvédelem trükkök tippek tanácsok böngészés eset

Ajánlott bejegyzések:


7 tipp a


Okoskodás:


10 alaplépés a


Tőrbeejtett

Kis- és

Kommentek:

kolléga · http://radicspeter.hu 2022.09.16. 23:02:13

szerintem az sem árt (ha más nem, a profilozást nehezítendő), ha havonta csinálunk egy teljes böngésző előzmények törlést , max. arra a pár minden nap használt oldalra újból be kell jelentkezni

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Még többet, még gyorsabban

2022. szeptember 13. 18:08 - Csizmazia Darab István [Rambo]

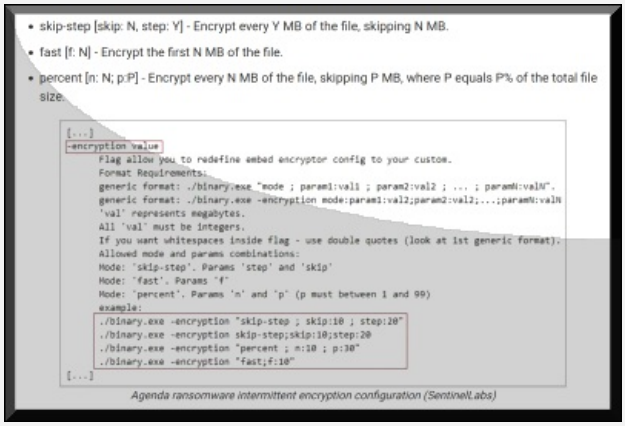
Lassan már a sztahanovista mozgalmat idézi az a fejlődés, amit a lassan tíz éves ransomware pályaíve befut. A kezdeti erős egyedi titkosításhoz társult doxing és büntető DDoS mellett **folyamatosan igyekeztek a bűnözök az elkódolás folyamatát is gyorsítani.** Jelentjük, ismét sikerült.

Pár hónapja volt egy olyan posztunk, amelyben a nevesebb zsarolóvírus családok titkosítási sebességét hasonlították össze.

Az akkori élmezőny már a márciusi mérések alapján is villámgyorsnak nevezhető tempót volt képest felmutatni: **a győztes LockBit egy 53GB méretű válogatott teszt adatcsomaggal - benne 98 ezer pdf, doc, xls, és hasonló tipikus Office és egyéb felhasználói állománnyal - mindössze 5 perc 50 másodperc alatt volt képest leszámolni.**

Most pedig arról lehet olvasni, hogy **az újabb innováció az úgynevezett szakaszos titkosítás lett.** A ransomware kártevő itt már nem a teljes fájlt, hanem "csak" például minden második 16 byte-ot kódol el, így ezzel **egyrészt fele annyi idő alatt végez, másrészt az enyhébb titkosítási folyamat miatt az automatizált védelmi eszközök kevésbé intenzív I/O műveleteket észlelnek, így nagyobb eséllyel tudnak észrevétlenek maradni.**

De **a szakaszolás tetszés szerint beállítható,** lehet egy állomány minden x-edik byte-ját titkosítani, kihagyva eközben tetszőleges y bájtot, lehet csak a fájl első x byte-ját legyalulni, illetve kihagyható az elkódolásból bárhol bármekkora megadott GAP is.

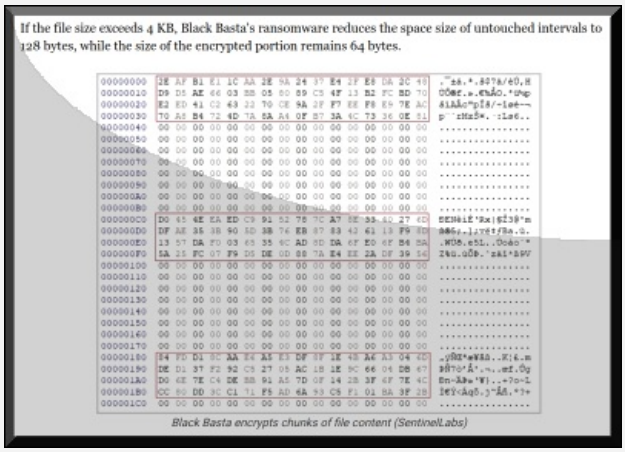


Agenda ransomware intermittent encryption configuration (SentinelLabs)

A SentinelLabs jelentése szerint **a 2021-ben a LockFile által bevezetett gyakorlatot immár tömegesen további bűnözői csapatok is átvették, így a Black Basta, az ALPHV (BlackCat), a PLAY, az Agenda és a Qyick is a követők közé sorolt be.** A szakaszos titkosítási funkciókat beépítve az általuk kínált RaaS (Ransomware as a Service)

üzleti modellbe sokkal hatékonyabb károkozásra lettek képesek a gyorsaság fokozásával.

Az újabb és bonyolultabb technika elterjedésével az ingyenesen elérhető helyreállító segédprogramoknak is fel van adva ezzel a lecke.



A Bleeping Computer véleménye szerint a szakaszos titkosításnak a ransomware bandák számára csak előnyei vannak, valódi hátrányok nélkül.

Még belegondolni is rossz, hogy ha a korábbi győztes LockBit bevezeti az újítást, a versenytársakhoz 20, 30, 50, 90 perces eredményeihez képesti 5 perc még jobban lerövidülve milyen eszeveszett gyors pusztítást lehet képes okozni a céges hálózatokban.

1 komment
Címkék: titkosítás sebesség gyorsaság szakaszos ransomeware zsarolóvírus elkódolás

Ajánlott bejegyzések:


Fedett pályás titkosítási bajnokság


Kulcs a túléléshez


Evolúció, ami számunkra nem csodálatos


Összeomlás


Nem csitulnak a kórházak elleni támadások

Kommentek:

kolléga · http://radicspeter.hu 2022.09.16. 22:33:02

ügyes

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.

VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

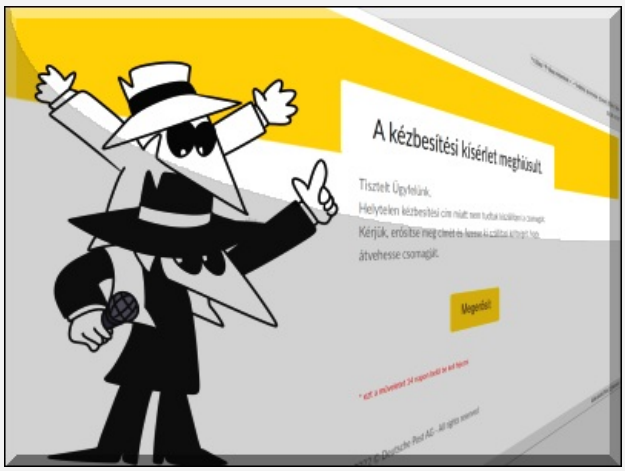
accountz

Belépés
Regisztráció

Csomagja érkezett - sokadik menet

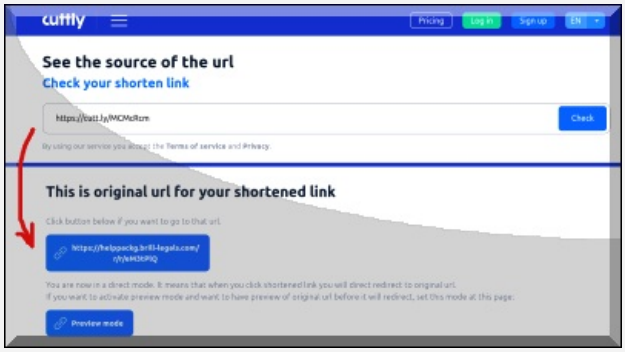
2022. szeptember 15. 13:48 - Csizmazia Darab István [Rambo]

Remélhetőleg mindenki levonta már a tanulságokat a tavaly márciusi FedEx-es átverés után, amely egy FluBot nevű vírus segítségével jó nagy kalamajkát okozott azoknál, **akik elhitték, hogy csomagjuk jött, telepítettek, engedélyeket adtak és a végén pórul jártak**. A csomagküldéssel kapcsolatos csalások azóta is folyamatosak, hetente jönnek újak.



Ezúttal **látszólag a Deutsche Post írt nekünk ékes magyar nyelven** egy titokzatos levelet, amelyből csak annyi derül ki, hogy egy nekünk szánt küldemény kézbesítési kísérlete állítólag meghiúsult. Mi más teendőnk is lehetne, mint kattintani a mellékelt linkre.

És itt már meg is állhatunk, mert szinte **az összes csomagküldéssel foglalkozó hivatal, vállalkozás tipikusan egy saját központi nyomkövető weboldalon intézi mindezt, ahova csak az adott küldemény azonosítót kell csak begépelni. Vagyis kattintani, pláne telepíteni ismeretlen dolgokat legitim esetben abszolút nem szükséges.**

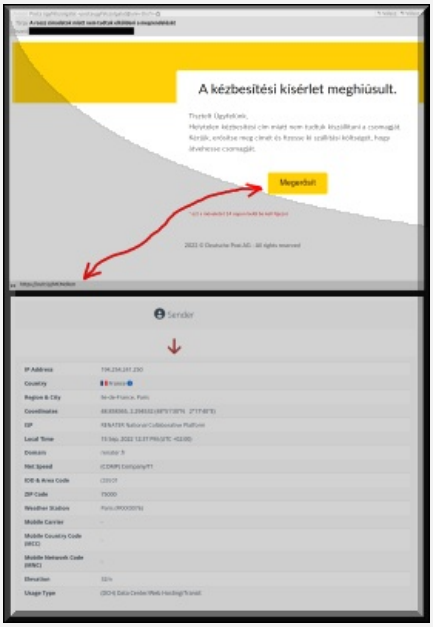


A sok szócséplés után nézzünk rá az egérmutatóval a mellékelt linkre is, ami **egy líbiai hosztolású (.ly) linkrövidítő által generált URL cím, de semmiképpen nem a német posta hivatalos oldalára mutat**. Ezt viszont lehetőségünk van előzetesen kattintás mentesen is kibontani, ami azt az érdekes helyzetet mutatja, hogy **nem egy fix, bedrótozott másik webhelyre mutat, hanem a fastflux DNS manipulációs technikára emlékeztető módon minden alkalommal különböző másik címre irányít.**

Ez egy 2007 óta létező bűnözői technika, amellyel az egyes fix domain címek elleni intézkedéseket, letiltásokat igyekeznek kijátszani.

A türelmes **feloldási próbálkozások ellenére egyetlen Deutsche Post-nak látszó weboldalt nem sikerült preview oldalon kipörgetnünk**, és kártevővel fertőzött webhely sem bukkant fel. Kicsit félkarú rabló feelingje volt a dolognak, ám ezúttal sok kísérletből egyszer sem jött ki egymás mellé a három nyerő ananász.

Egy csomó vélhetően feltört WordPress oldal mellett már nem létező, törölt címek is nagy számban előjöttek.



Ha az email feladóját nézzük (postaugyfelszolgalat KUKAC univ-tln PONT fr), az sem a német posta hivatalos címének látszik, de legalább a gyors e-mail trace alapján valóban francia IP címről küldték a kéretlen levelet.

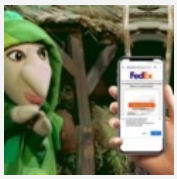
A tanulság nyilván az, hogy folyamatosan fognak érkezni a jövőben is az adathalász próbálkozások, ideje lenne mindenkinek nagyobb figyelemmel kezelni a kéretlen üzeneteket: feladót, linket, mellékletet. És persze antivírus megoldás adathalászat elleni védelemmel, biztonságos böngésző kiegészítők (AdBlocker, uBlock, HTTPS Everywhere, NetCraft, TrackMeNot, NoScript, stb.) alkalmazásával, valamint nélkülözhetetlen a biztonságtudatos hozzáállás is, leánykori nevén egészséges gyanakvás.

1 komment
Címkék: spam kattintás adathalászat adatlopás csomagküldő biztonságtudatosság fastflux phis

Ajánlott bejegyzések:

Ismét csomagunk

Egypálcás adathalász


Sárkány ellen sárkányfű

Sikeres brandek az


Viva la Revolut

érkezett - vagy mégsem?

próbálkozások

adathalászatban

Kommentek:

Head Honcho 2022.09.15. 21:28:47

Felteszem, kaszálnak a net-analfabéták körében továbbra is. Félelmetes különben, hogy a fenti, legitnek látszó weboldalakon hogy nem veszik észre, hogy meg lettek törve, és ilyen malíciózus ügyletekre használják a domainjaikat.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

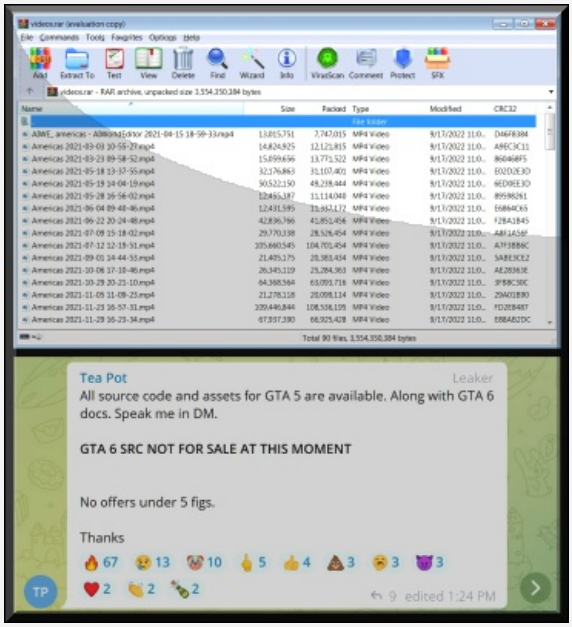
GTA6 - Ellopták a lopós játékot

2022. szeptember 19. 13:07 - Csizmazia Darab István [Rambo]

Informatikai incidens érte a **Grand Theft Auto játékot fejlesztő Rockstar Games rendszerét. A feltörés következtében a tesztelők játékmenet videói, illetve maguk a forráskódok is** illetéktelen kézbe kerültek.

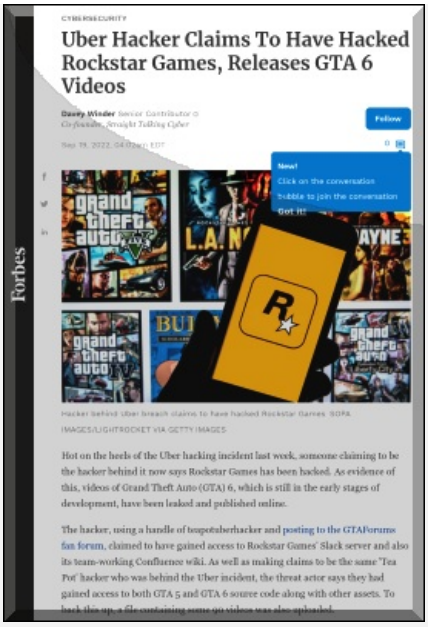
A Tea Pot (teáskanna) nevezetű hacker a GTA fórumon tett elérhetővé bizonyítékként egy olyan RAR linket, amely **90 lopott videofájlt tartalmazott.**

Ezeket a nem publikus belső videókat a fejlesztők készítették saját maguknak teszteléshez, hibakereséshez.



A Grand Theft Auto V egy olyan látványos autótolvaj tematikájú videójáték, amely még **majdnem tíz évvel ezelőtt, 2013-ban jelent meg PC-re, PlayStation és Xbox konzolokra.**

A játékprogram igazi különlegességnek számított a maga idejében, 265 millió dollárból készült - ami kb. egy akkori hollywoodi film költségvetése - ebből 100 millió USD csak a marketing volt. A játékmeneten 300 szakember dolgozott 5 éven keresztül, 240 licencelt slágert tartalmaz, és erősen épített a jutalmazó gamificationra. A befektetett energia viszont bőségesen megtérült, hiszen a megjelenésekor már az első napon 800 milliós bevételt hozott.

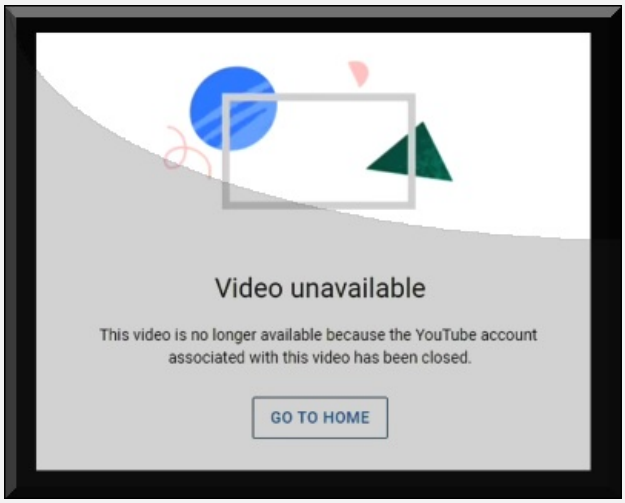


A folytatást, a GTA 6-ot évek óta ígérik a fejlesztők, így hatalmas várakozás előzi meg az idáig még meg sem jelent játékot. A Bleeping Computer értesülési szerint a hacker azt is állította, hogy a már említett játékmenet videók mellett a GTA 5 és a GTA 6 forráskódjához is hozzáfért, így ezeket is ellopta.

Az 5-ös verziónál 10 ezer dollár feletti árajánlatot tart elfogadhatónak váltságdíjként, a 6-ost egyelőre nem bocsátotta áruba.

A Rockstar Games megerősítette az incidensről szóló híreket, és eltávolítási kérelmeket adott ki a YouTube és egyéb megosztó oldalakon szereplő kiszivárgott anyagokra. **A 90 lopott videó összesen körülbelül egy órányi játékidőt mutat be. Ezek idő előtt lelövik a meglepetéseket, ám a forrás kód kikerülése viszont már olyan problémát is okozhat, ami további késésekhez**, vagy akár a projekt meghiúsulásához is vezethet.

Korábban a Cyberpunk 2077 játék esetében volt hasonló nehézség, ahol **a rajongók eleinte a nagy késéseket nehezményezték, itt a fejlesztők több halálos fenyegetést is kaptak.** A megjelenés után viszont a hibák miatt voltak igen mérgesek a vásárlók.



A GTA feltörés technikai részleteiről egyelőre sajnos nincsenek konkrét információk.

A támadó azt állítja magáról, hogy korábban az Uber rendszerébe sikerült bejutnia, ahol social engineering technikával egy megtévesztett alkalmazotton keresztül jutott olyan belsős információkhoz, ami aztán az ottani sikeres támadást lehetővé tette.

Szólj hozzá!
Címkék: games gta feltörés váltságdíj adatlopás szivárgás rocktar gta5 teapot gta6

Ajánlott bejegyzések:

[Járulékos következmények szevasztok]

[Fordulat ransomware fronton]

[Ransomware a spájzban]

[Sör-Bitcoin menet]

[GoDaddy - apák a pácban]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

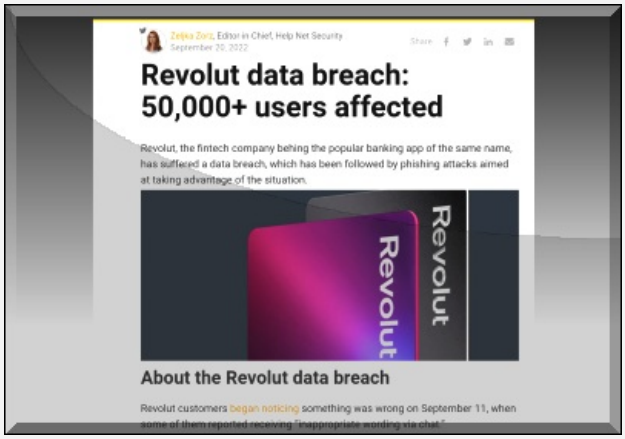
Viva la Revolut

2022. szeptember 22. 14:21 - Csizmazia Darab István [Rambo]

Rossz hírek érkeztek a **litván fintech startup Revolut háza tájáról is, feltörték őket, és ennek során az ügyfél adatok** egy részéhez is hozzáfértek illetéktelenek.

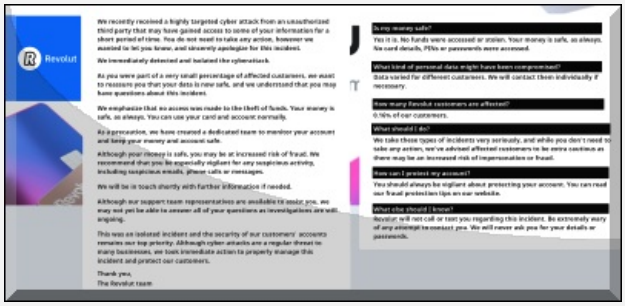
A cég nyilatkozó illetékes szóvivő, Michael Bodansky szerint az ügyfelek 0.16 százalékát érinti az az adatlopás, amelyet még **szeptember 11-én késő este fedeztek fel a rendszerükben. A célzott támadás azonosítása után azonnal felvették a kapcsolatot az érintett ügyfeleikkel.**

Ez egy e-mailes értesítést jelent, magyarán csak azok kaptak ilyet üzenetet, akik beletartoznak az incidenst elszenvedő csoportba. A cég nyilatkozata szerint **50 ezer ügyféladatot loptak el, ebből 20 ezer európai illetőségű.**



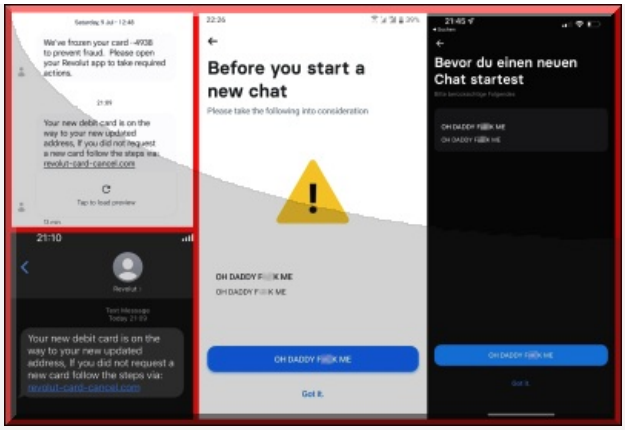
Ebben arról írnak, hogy egyrészt elnézést kérnek, másrészt tájékoztatni akarnak az incidens részleteiről. **Hangsúlyozzák, hogy pénzeszközökhöz a támadók állítólag nem fértek hozzá, mindenki pénze biztonságban van, ám a személyes adatok ellopása miatt nagy a kockázat a testre szabott adathalász, csaló támadásoknak.**

Az illetéktelenek által megszerzett adatok ugyanis e-mail címek, ügyfél nevek, posta címek, telefonszámok, és egyes ügyfelek esetében pluszban fiók és kártyaadatok is.



Izgalmas mellékszál, hogy **egyes banki felhasználók arról számoltak be, hogy a támogatási csevegésben szexuális tartalmú üzeneteket kaptak a hivatalos chatablakban.**

Nem tudni, hogy ennek az eredeti támadáshot volt-e köze.



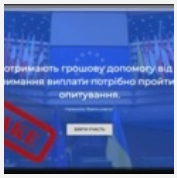
A Revolut a levélben arra figyelmezteti az ügyfeleket, hogy készüljenek fel arra, hogy a bűnözők az ellopott adatok birtokában az adathalász kampányokat indíthatnak a végfelhasználók ellen. Ne felejtsük el, hogy soha egyetlen bank sem küldene SMS-eket, vagy hívná fel a fióktulajdonosokat amiatt, hogy bejelentkezési adatokat vagy hozzáférési kódokat kérjen tőlük, ez sajnos egy bevett csalási forma, tehát érdemes vigyázni, gyanakodni.

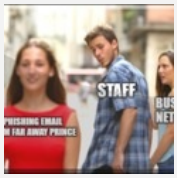
A tájékoztatás szerint az incidenstől függetlenül viszont minden ügyfél továbbra is a szokásos módon használhatja a számláját és a bankkártyáját.

1 komment
Címkék: sms e-mail csalás átverés testreszabott adathalászat adatlopás adatszivárgás revolut

Ajánlott bejegyzések:

Ismét csomagunk érkezett - vagy mégsem?


Adathalászok lakat alatt



10 gyakori ok, amiért bedőlünk a csalásoknak


Magyar Posta csomagunk jött - vagy mégsem?

Banki meló

Kommentek:

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu
2022.09.24. 07:54:36

CityPolice confirm 17-year-old arrested over hacking incident; source says the crime is related to intrusion on Rockstar Games and possibly Uber Technologies.
twitter.com/MatthewKeysLive/status/1573298480520404992

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.

VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Ez történik a weben egy perc alatt

2022. szeptember 27. 15:22 - Csizmazia Darab István [Rambo]

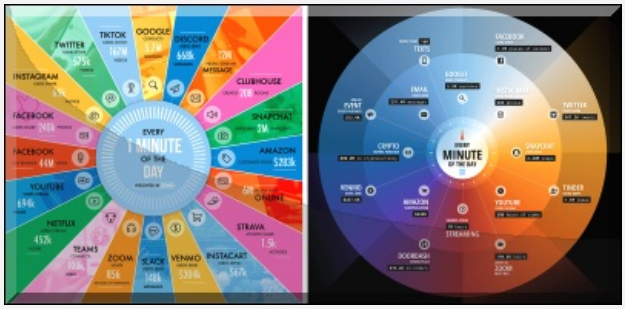
Itt a legújabb, immár **10.0 Data Never Sleeps infografika, lássuk mi minden zajlik a neten mindössze 60 másodperc leforgása alatt.**

A legfontosabb látnivaló az, hogy korábban mintha pedánsan ügyeltek volna arra a készítők, nehogy véletlenül is hasonló szerkezetű, ezáltal túl egyszerűen összehasonlítható legyen a régebbi változatokkal az aktuális statisztika.

Ezúttal viszont szerencsére vannak párhuzamos átfedések a kategóriákban, kezdjük is akkor ezekkel a könnyen nyomon követhető és párhuzamba állítható adatokkal.

A Google keresések száma a 2021-ben megjelent 9.0 verzióhoz képest a mostani 2022. szeptemberi mértéke 5.7 millióról 5.9 millióra nőtt, míg az Insta fotómegosztások is csak minimálisan változott, 65 millió után ez most 66 millió lett. A percenkénti YouTube stream letöltés mértéke 694 ezer volt korábban, most 500 órányi feltöltést tudunk ezzel szembeállítani. (Thanks to Geegee :)

A Snapchat is felfutóban volt, itt 2 millió után a 10-es ábrán 2.43 milliós számot találhatunk. **Az Amazon költések viszont láthatóan meglódultak, a korábbi 283 ezer dollárról 443 ezer USD-re ugrott ez fel. A Venmo mobilfizetési szolgáltatás is jól teljesített, itt az előző 304 ezres érték 437 ezerre duzzadt.**



Nézzük akkor, hol látható valamennyi csökkenés, visszaesés. Érdekes módon a a Twitterezési kedv is valamelyest lanyhult: az egy perc alatti 575 ezer tweet ezúttal már csak 347 ezer lett, **persze ez is egy óriási szám a jó 5 milliárd internetező vonatkozásában.**

Összességében **a pandémia alatt felfutó online vásárlás, online konferenciázás, online ételrendelés és kripto műveletek időarányosan növekedtek, ehhez nyilván a részlegesen megmaradt homeoffice is hozzájárult.**

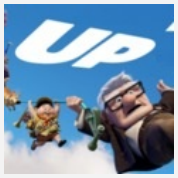
És végül a szokásosnak mondható kártevős, illetve IT biztonsági vonatkozásokat is előrántjuk a korábbi, tavaly júniusban keltezett posztunkból. Az AVTest.org szerint meghaladta az **1.2 milliárdos számot a nyilvántartott egyedi kártékony kódok száma.**

A haveibeenpwned.com pedig a korábbi adatokhoz képest **mára már 11.9 milliárd feltört jelszó található, ez is egy beszédes szám**, remélhetőleg mindenkinek azt mondja, hogy naprakész vírusvédelem, rendszeres operációs rendszer és alkalmazói program frissítés, valamint erős jelszó és kétfaktoros autentikáció hajrá előre.

3 komment
Címkék: statisztika internet net never ez egy alatt perc történik minute domo infografika sleeps

Ajánlott bejegyzések:


Ez történik a weben egy perc alatt



5.2 milliárd netező 1 perce

Kis- és középvállalkozások adatvédelmi incidensei

Még gyengébb a jelszavad


Emelkedő ransomware károk

Kommentek:

geegee · http://eszakonelunk.blog.hu 2022.09.28. 22:18:43

Izé, meg a vaslőcs; a a jutubnál 2021-es 694 az ezer óra (lásd k betű) és streamelés, tehát letöltés.A 2022-es 500 az viszont sima 500 óra (nincs k betű) és feltöltés...És már a sima 500 óra is ultrabrutál mennyiség.
Már elnézést, hogy kötözködök. :D

Válasz erre

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2022.09.29. 05:49:04

@geegee: Köszönöm alássan... :-)

Válasz erre

geegee · **http://eszakonelunk.blog.hu 2022.09.29. 10:01:49**

@Csizmazia Darab István [Rambo]: :D

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

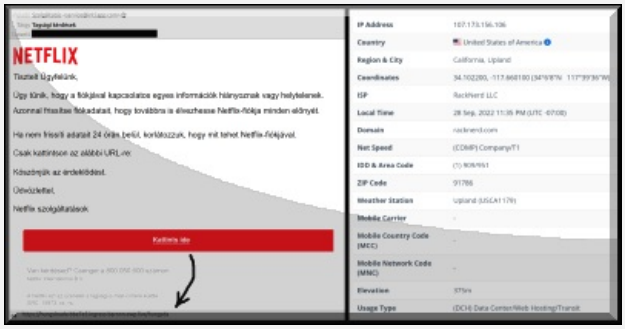
Tagsági kérdések - vagy mégsem?

2022. szeptember 29. 10:11 - Csizmazia Darab István [Rambo]

Írt nekünk a Netflix - függetlenül attól, vajon ügyfelek vagyunk-e - frissítenünk kell a fiókadatokat. Persze remek **phishing linket is kapunk hozzá, hátha lesz aki bedől** ennek az újabb átverésnek.

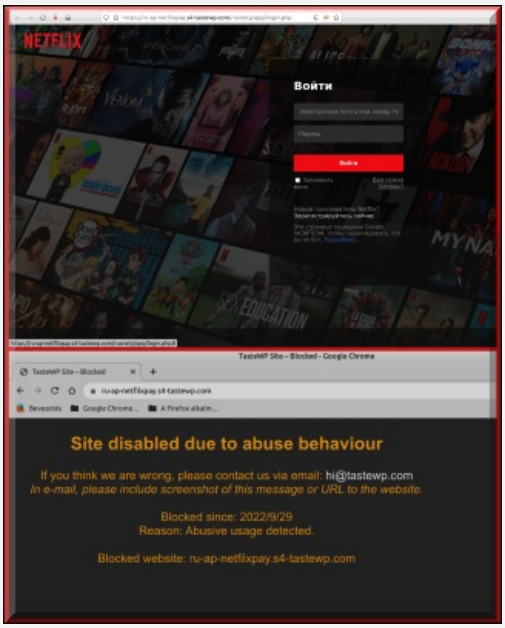
Vagy mégsem rovatunk kifogyhatatlan, csak a bankok nevében érkező üzenetekkel Dunát lehetne rekeszteni, vagy külön tematikus blogot indítani belőlük.

Ezúttal a Netflix nevével éltek vissza ismeretlenek, jön az ősz, mindenki behúzódik a lakásban, ők pedig betakarítják az óvatlan felhasználók streaming platform hozzáférését.



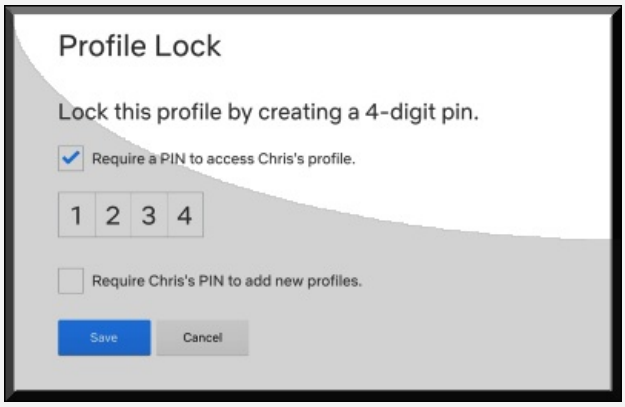
Már a levélről is ordít, hogy semmi köze egy hivatalos megkereséshez, a feladó is eltérő, az IP cím alapján pedig Kaliforniából küldték a magyar nyelvű megkeresést egy olyan valakihez, aki egyébként maga nem is előfizető.

És ha ez nem lenne elég, jön az **árulkodó sürgetés és fenyegetés: "*Ha nem frissíti adatait 24 órán belül, korlátozzuk, hogy mit tehet Netflix-fiókjával. Csak kattintson az alábbi URL-re*".** Kedvenc részünk a tegezős/magázós egyvelegből egyébként ez: "Van kérdésed? Csenget a ... számon" XD



Az üzenet **a tegnapi érkezésekor egy URL egy orosz nyelvű Netflix adathalász oldalra mutatott**, aki ide begépelgette a belépési adatait, az onnantól már nem (csak) az ő fiókja.

Valószínű, hogy sok bejelentés érkezhetett az esetről, mert a **ma reggeli állapot szerint már lekapcsolták a rosszindulatú hasonmás weboldalt.**



A Hulu és az Apple TV Plus szolgáltatásokkal ellentétben a Netflixnek 2022-ben egyelőre nincs támogatva a kétfaktoros autentikációs lehetősége, legalábbis a weboldalán ennek nem volt nyoma ma reggel. A lehetséges profilvédelmi megoldás sajnos egyelőre mindössze a számítógépen (mobilon nem) beállítható négyjegyű gyerekzár használata lehet.

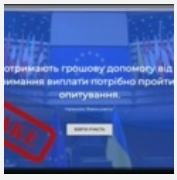
No meg persze az is, hogy egy ilyen **nyilvánvaló adathalász támadásnak nem/sem dőlünk be, mert már biztonságtudatosan régóta odafigyelünk az intő jelekre**. Legalábbis ez már milyen menőség lenne!

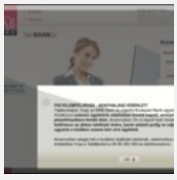
1 komment
Címkék: vagy csalás átverés phishing netflix adathalászat mégsem vagymégsem

Ajánlott bejegyzések:


Ingyenes Omikron teszt vagy mégsem?

Egyre gyakoribb a banki adathalászat


Adathalászok lakat alatt


MKB adathalászat szigonnyal, horoggal, hálóval


Magyar Posta csomagunk jött - vagy mégsem?

Kommentek:

Head Honcho 2022.09.29. 11:30:29

Ilyesmit én is kaptam, azzal a nem elhanyagolható kivétellel, hogy valaki az emailemmel regisztrált fel Netflixre. Telefonálnom kellett, hogy töröljék a regisztrációt. (Akkor ugyanis pont nem fért bele az életembe plusz fizetnivaló.)

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.

VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

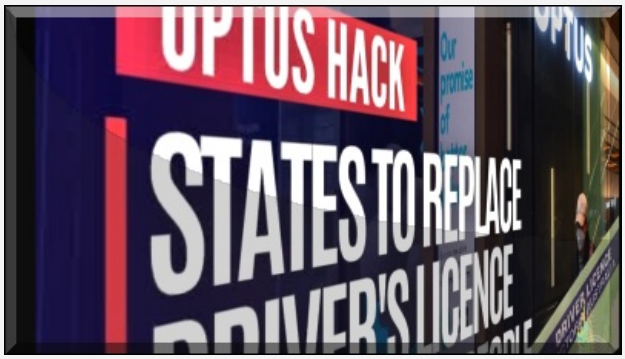
Járulékos következmények szevasztok

2022. október 06. 15:12 - Csizmazia Darab István [Rambo]

Nemrég került nyilvánosságra, hogy a szingapúri tulajdonosi háttérrel rendelkező **ausztrál telekommunikációs vállalat, az Optus olyan informatikai incidenst szenvedett el, melynek során illetéktelenek 9.8 millió ügyfél személyes adatát lopták el** a számítógépes rendszerükből.

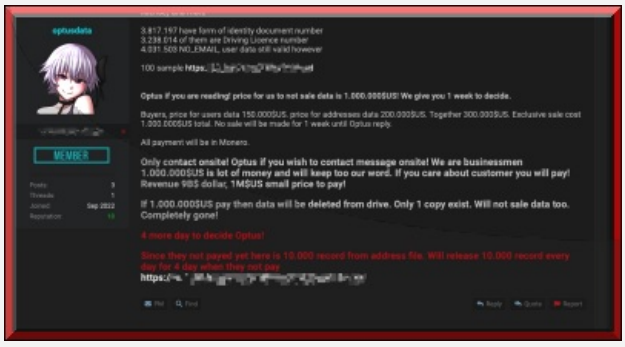
Ehhez hasonló történetet már sajnos sokat ismerünk, ilyenkor a legjobb forgatókönyv az, ha a tagadás helyett nyilvánosan elismerik a támadást, azonnal figyelmeztetik az ügyfeleiket, és azonnali lépéseket tesznek az elhárítás és a felderítés érdekében. A sajtóközlemény szerint 7.7 millió esetben ezek nem tartalmaztak érvényes vagy aktuális okmányazonosító számokat, **vagyis a kivonást elvégezve 2.1 milliónál viszont igen.**

Az Optus emailt és SMS-t küldött az érintett ügyfeleknek, hogy a személyazonosító okmányaik, adataik veszélybe kerültek, ezek között állítólag 900 ezer olyan is szerepelt, akiknek időközben lejárt az igazolványuk érvényességi ideje.



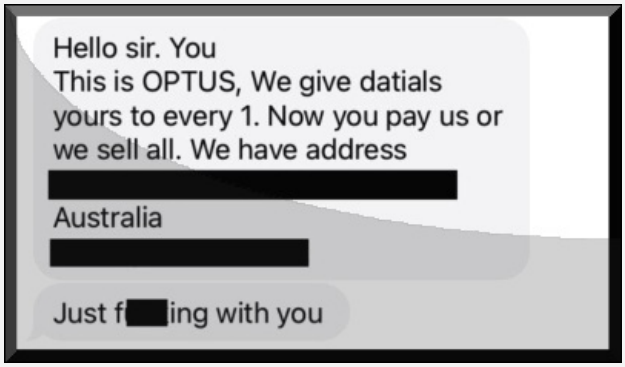
Eddig ez a reagálás, figyelmeztetés is lassan szokványosnak mondható, de például a tavalyi Telekom incidensnél a vállalat mindezt megfejelve két év ingyenes személyazonosság-védelmi szolgáltatást is felajánlott az érintett ügyfeleknek, hogy ezzel is segítsenek biztosítani kompromittálódott személyes adataik védelmét.

Itt ilyenről nem tudunk, de ami inkább érdekes lehet, hogy **ha ezek az adatok kiszivárognak, akkor igen könnyen további veszélybe kerülhetnek az áldozattá vált ügyfelek.**



Ugyanis nem csak az a tankönyvi eset van, hogy maga a behatoló akar ezzel zsarolni, vagy célzott adathalász támadási kampányokat indítani ezen adatok birtokában, hanem gyakran eladják ezeket, sőt akár többször is további bűnözői köröknek. Itt **a valódi támadó eredetileg 1 millió dolláros váltságdíjat követelt az Optustól azért, hogy ne tegye közzé az ellopott adatokat. Mivel nem fizettek neki, bosszúból 10 ezer ügyfél adatot szivárogtatott ki egy fórumoldalon.**

És a nyilvánossá tett adatállományokkal harmadik felek is bepróbálkozhatnak, erre ott vannak a nevek, címek, e-mail címek, telefonszámok, születési dátumok.



Ezúttal éppen ez utóbbi történt, ugyanis **az ausztrál rendőrség letartóztatott egy 19 éves sydney-i fiatalembert, mert állítólag ezeket a kiszivárgott Optus ügyféladatokat használta fel zsaroláshoz.**

SMS üzenetekben fenyegette meg az áldozatokat, hogy ha nem fizetnek neki két napon belül 2000 ausztrál dollárt (mai áron nagyjából 844 ezer forintnak megfelelő összeg), akkor eladja ezeket az adatokat bűnözőknek.

A kezdő csaló 93 embert fenyegetett meg, és egy konkrét bankszámlára követelte a váltságdíjat, amit a rendőrség később beazonosított, és ezek után került sor a letartóztatásra. Az ügyfelek nagyon helyesen nem fizettek, ám feljelentést tettek. **A rendőrség szerint egyértelműnek látszik, hogy a zsaroló nem azonos az Optus megtámadó hackerrel.**

Az ausztrál kormány azt is követeli az Optustól, hogy az igazolvány cserék költségét térítse meg a bajba jutott ügyfeleknek - ahogy például, hogy a 2015-ös Target áruházlánc elleni támadásnál is ez egy jogos igényként merült fel, és végül valóban meg is történt.

Szólj hozzá!
Címkék: ausztrália zsarolás telekommunikáció váltságdíj adatlopás adatszivárgás optus

Ajánlott bejegyzések:

Fordulat ransomware fronton

Van másik!

"Illetéktelen fél korlátozott ideig hozzáférhetett fájlokhoz"


Persze hogy tudtam, csak nem sejtettem...


Viva la Revolut

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Antivírusblog
245 követő

Oldal követése Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

- RSS 2.0
- bejegyzések, kommentek
- Atom

bejegyzések, kommentek

accountz

Belépés
Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

Gratulálunk - mihez is?

2022. október 10. 14:07 - Csizmazia Darab István [Rambo]

Mostanában nincs sok ok a jókedvre, hiszen számos baljós történés beárnyékolja az életünket. Mai hétfői adathalász példánk viszont legalább ironikus - **a terjesztői már annyira túltolták a görcsös igyekezetet, hogy ennek így remélhetőleg már senki sem dőlne be. Vagy mégsem?!**

Az üzenet mintha csak **a korábbi e-mail lottó** **és emellett a Covid vírushelyzet miatti hamis jóvátételi összeggel kapcsolatos** csalások közös szerelemgyereke lenne.

Egybeötvözi a fentieket, és a fogalmazvány Tuskó Hopkins, Fülig Jimmy és Török Szultán kevert nyelvi stílusában és magyarságával **ígér irgalmatlanul hatalmas összeget a meggazdagodni vágyó hétköznapi halandóknak.**

A **Facebook Lottócsapat nevében kapjuk az e-mailt, és nem kevesebb, mint egymillió angol fontot sorsoltak ki. És a szerencse csakugyan ránk mosolygott, hiszen 27 millió e-mail cím közül éppen minket választott ki** Fortuna szerencsecsillaga.

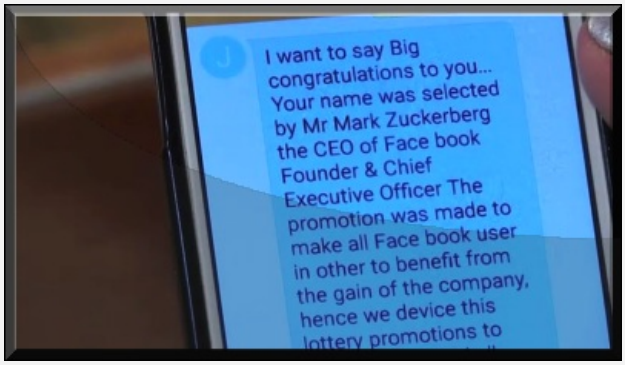
Illetve hát izé, szóval rajtunk kívül még sok millió másik embert is, akik ugyanígy hasonlóan megkapták ugyanezt a forma spamet tömegesen terjesztett körlevélként.

"*Az Ön E-MAIL FIÓKJA egymillió font (1 000 000 GBP) összeget nyert a Facebook folyamatban lévő online díjátadó promóciójában és a koronavírus (COVID-19) segélyezési támogatásban a Facebook Inc. vezérigazgatójától, Mark úrtól. Zuckerberg. Az Ön jegyének száma: 00545 188 564756.*"

Hát igen, impozáns összeg, köszönhetően Önök a szolgálatban szorgosan tevékenykedő Marc Andreessen úrnak, aki hivatása szerint Facebook lottószervező.

Nézzük, pontosan mit is kellene tenni a nyeremény átvétele érdekében, leszámítva azt, hogy már sok banknál lehet mindenfajta további kérdezősködés nélkül simán e-mail címre is pénzt utalni, ha nagyon akarnák.

Személyes adatokat várnak tőlünk, nem is keveset: teljes név, ország, kapcsolattartási cím, telefonszám, családi állapot, foglalkozás, vállalat, életkor. Vajon ha már egyszer nyertük, mi közük van az életkorunkhoz, foglalkozásunkhoz vagy a családi állapotunkhoz? Az élet nagy rejtélye ez.



A feladó egy perui e-mail cím (eespinoza KUKAC regioncallao PONT gob PONT pe), a kapcsolattartó egy bizonyos David M. Wehner, akinek outlokos címe: facebook PONT claimunit KUKAC outlook PONT com, míg a levél aláírója a már említett Marc Andreessen lottószervező.

Az e-mail trace útvonala már csak azért is érdekes, mert néven nevezik, hogy az Egyesült Királyság európai régiójának pénzügyi igazgatója az az személy, akivel majd állítólag kapcsolatba kerülünk.

Kis kereséssel meg is lehet találni az átverés szlovák és egyéb nyelvű pár éves variánsait - és tadaaam, ugyenezzel 00545 kezdetű sorszámmal. A csalás célja egyfelől a személyes adatok begereblyézése, de később már úgynevezett ügyvédi költség címén 56 EUR összeget is kérnek előre a gyanútlan és naiv áldozatoktól.

Remélhetőleg **a sok-sok nulla, és a látszólag könnyen megkapható ingyen pénz ígérete ellenére ez a kísérlet sokkal inkább a vicces, semmint a veszélyes vagy hihető kategória polcát fogja majd gyarapítani** - legalábbis jó lenne ebben hinni.

Szólj hozzá!
Címkék: facebook lottó csalás átverés adathalászat lottery zuckerberg

Ajánlott bejegyzések:


A Ravasz, az Agy és az online átverések


Nagy pénz, nagy foci, nagy átverések


Ismét csomagunk érkezett - vagy mégsem?

Tagsági kérdések - vagy mégsem?


Viva la Revolut

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

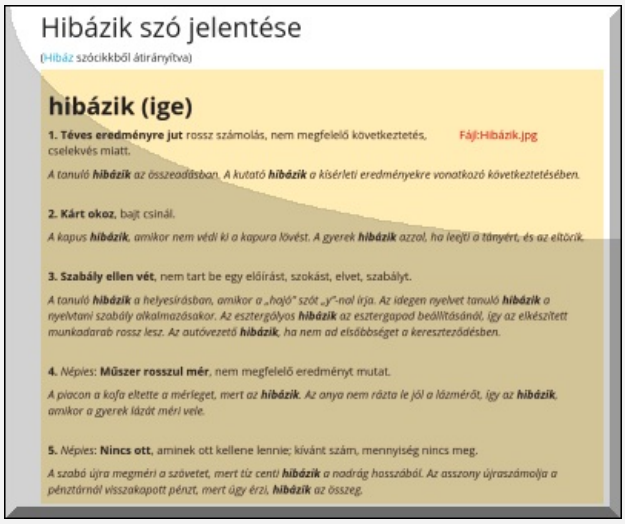
Cselekedettel és mulasztással

2022. október 12. 15:01 - Csizmazia Darab István [Rambo]

Sok feladat, gyors tempó, feszes határidők - ez a körülmény sajnos erősen kedvez a hibázásnak. Néha becsúszhat a kapkodás vagy átgondolatlanság miatt olyan fatális hiba, ami aztán **később nagyon komoly adatvédelmi gondokat okozhat.**

A japán autókat igen sokan szeretik, és ezek közül is méltán népszerű a Mazda vagy a Toyota. Vannak, akik az első ilyen autó után már végig hűségesek maradnak az adott márkához.

Ezúttal a Toyota háza táján történt egy malőr, melynek révén bizalmas ügyfél adatok szivárogtak ki egy nyilvános webfelületen.


Hibázik szó jelentése

(Hibáz szócikkből átirányítva)

hibázik (ige)

1. Téves eredményre jut rossz számolás, nem megfelelő következtetés, cselekvés miatt. Fájl:Hibázik.jpg

*A tanuló **hibázik** az összeadásban. A kutató **hibázik** a kísérleti eredményekre vonatkozó következtetésében.*

2. Kárt okoz, bajt csinál.

*A kapus **hibázik**, amikor nem védi ki a kapura lövést. A gyerek **hibázik** azzal, ha leejti a tányért, és az eltörik.*

3. Szabály ellen vét, nem tart be egy előírást, szokást, elvet, szabályt.

*A tanuló **hibázik** a helyesírásban, amikor a „hajó" szót „y"-nal írja. Az idegen nyelvet tanuló **hibázik** a nyelvtani szabály alkalmazásakor. Az esztergályos **hibázik** az esztergapad beállításánál, így az elkészített munkadarab rossz lesz. Az autóvezető **hibázik**, ha nem ad elsőbbséget a kereszteződésben.*

4. *Népies:* **Műszer rosszul mér**, nem megfelelő eredményt mutat.

*A piacon a kofa eltette a mérleget, mert az **hibázik**. Az anya nem rázta le jól a lázmérőt, így az **hibázik**, amikor a gyerek lázát méri vele.*

5. *Népies:* **Nincs ott**, aminek ott kellene lennie; kívánt szám, mennyiség nincs meg.

*A szabó újra megméri a szövetet, mert tíz cenit **hibázik** a nadrág hosszából. Az asszony újraszámolja a pénztárnál visszakapott pénzt, mert úgy érzi, **hibázik** az összeg.*

A T-Connect ügyféltámogató webhelyre feliratkozott emberek személyes adatai kerültek veszélybe azáltal, hogy **egy szoftverfejlesztő egész egyszerűen feltöltötte a webhely forráskódját egy publikus GitHub oldalra.**

A Toyota elismerte a hibát, amelynek révén közel 300 ezer ügyfél adata kerülhetett illetéktelen kezekbe. **Külön érdesség, hogy a felelőtlen hozzáférési kulcs feltöltése és a hiba észrevételezése között csaknem 5 év telt el.**

A cég közleménye szerint **egy külsős, a T-Connect megvalósításáért felelős fejlesztőjük töltötte fel a kódot még 2017-ben, amit csak most 2022. szeptemberében vettek észre.**

A hivatalos bocsánatkérésükben kiemelték, hogy bár a szerverükre való belépés kompromittálódott, **nem tudták sem megerősíteni, sem cáfolni, hogy ezekhez az SQL hitelesítő adatokhoz hozzáfértek-e bűnözők.**

A Toyota figyelmeztette a T-Connect ügyfeleket, hogy **az esetlegesen ellopott személyes adatok birtokában célzott adathalász támadások várhatóak, emiatt kiemelt figyelemmel kezeljék a cég nevében érkező kéretlen e-mail üzeneteket, vigyázzanak nehogy hamis webhelyre, űrlapra irányítsák őket például jelszó változtatás ürügyén.**

Szólj hozzá!
Címkék: hiba sql kulcs toyota publikus adatszivárgás github t-connect

Ajánlott bejegyzések:

"Illetéktelen fél korlátozott ideig hozzáférhetett fájlokhoz"


10 gyakori IT biztonsági hiba

Járulékos következmények szevasztok


Viva la Revolut


Elvitte az ördög

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei

Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Ezer százalék lett, maradhat?

2022. október 17. 13:24 - Csizmazia Darab István [Rambo]

Adathalászat, személyazonosság lopás, közösségi média fiókok eltérítése, az eredeti tulajdonos kizárása. Ezek a fajta bűncselekmények minden képzeletet felülmúlóan emelkedtek az utóbbi időben - erről számolt az Identity Theft Resource Center összefoglalója.

A beszámoló szerint **az utóbbi 12 hónapban 1000 százalékkal nőtt személyiséglopás mértéke a közösséi oldalakon. Arányaiban az Instagram felhasználók voltak döntően leginkább a célkeresztben, míg az esetek negyede, 25% érintette a Facebook/Meta fiókokat.**

A fiókok eltérítése (zárolás, váltságdíjért való visszaadás, illetve a fiók illetéktelen használata) személyes kellemetlenséget biztosan okoz, ám sok esetben komolyabb következményekkel is szembesülnek az áldozatok. Ezek között említhető az **ismerőseik célzott megtévesztése, vagy a fiók eredeti tulajdonosának nevében lejáratót üzenetek küldése, amelyek egyes profilok esetében anyagi és erkölcsi veszteségeket is okozhatnak: bevétel kiesés, munkahelyi elbocsátás, stb.**

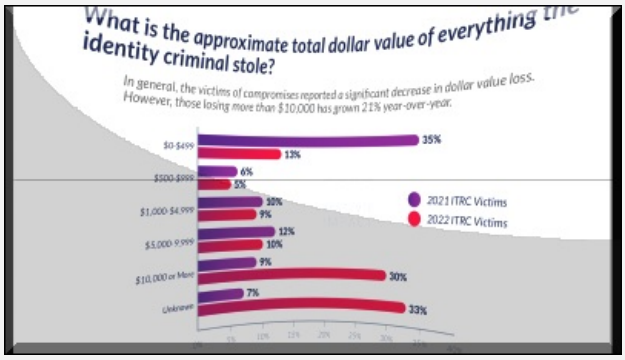
Az ITRC összesen mintegy 1,600 személyesadat-lopás áldozatát kérdezte meg a felmérés során. Az áldozatok közül 40% észlelte, hogy személyes adataikat ellopták, veszélyeztették vagy konkrétan visszaéltek velük a 2021. áprilisa és 2022 márciusa közötti időszakban.

A jelentésből az is látható, hogy az ilyen fajta incidenseknél igen sokszor, esetek **70%-ában véglegesen kizárták az eredeti tulajdonost** a saját korábbi fiókjából, de az is dominánsan, 71%-ban megfigyelhető volt a közösségi fiókok eltérítésénél, hogy **a fiók ismerőseit megkörnyékezték a bűnözők, és különféle csalásokkal, pénzkérésekkel jelentkeztek** a fiók korábbi tulajdonosa nevében.

Az áldozatok mintegy **negyede (27%) számolt be arról, hogy konkrét értékesítési bevételtől eset ki a profil lopás miatt,** különösen jellemző lehet ez influencerek, vagy valamilyen közösség kommunikációs platformja esetében.

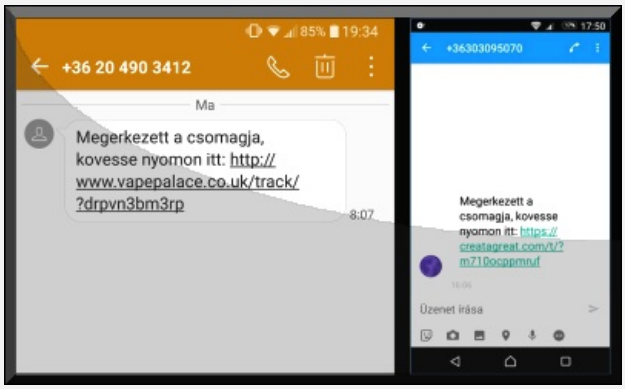
Az influencerek egy Instagram, YouTube vagy a TikTok fiókjuk elvesztése következtében nemcsak egy hosszú idő alatt sikeresen felépített követői közösséget veszít el, de ezzel együtt konkrét anyagi bevétele is kieshet.

Bár az átlagos elvesztett pénz mennyisége jellemzően 500 dollár alatti összeg maradt, **a kifejezetten jövedelmező áldozatokra célzott támadások száma a korábbi 9 százalékról 30%-ra emelkedett.** Egyúttal figyelmeztető dolog az is, hogy a válaszadók 50%-a többször is áldozatul esett már személyiség lopásnak.



Az adathalász támadások közül időnként könnyű kiszűrni a csalásokat, ha például egy olyan bank nevében keresnek meg bennünket kéretlen üzenetben, amelynek nem is vagyunk ügyfelei.

Ám ahogy azt például a Covid lezárási időszakában láttuk, a látszólag a csomagüldő szolgálatok által írt üzeneteknek sokan bedőltek, és ugyanígy a közösségi oldalak nevében történő visszaélések esetében nehezebb a megítélés, hiszen **a többség beregisztrált már ezekre a platformokra, és valóban jelen van.**



Összességében **visszautalunk egy korábbi átfogó posztunkra, amelyben összefoglaltuk, miket érdemes megtenni az adathalászat hatékony elkerülésében, megelőzésében**.

Röviden összefoglalva az erős egyedi jelszavak használata, a több tényezős hitelesítés széleskörű alkalmazása és a biztonságtudatos hozzáállás segíthet ebben a legtöbbet.

Szólj hozzá!
Címkék: statisztika lopás oldal közösségi személyiség theft platform adathalászat személyiséglopás fiókeltérítés indentity itrc

Ajánlott bejegyzések:

Az adathalászatot megölni nem kell félnetek

A nemzetközi helyzet egyre fokozódik

Ha eljön a személyiségtolvaj

Kis- és középvállalkozások adatvédelmi incidensei

Még gyengébb a jelszavad

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei

Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

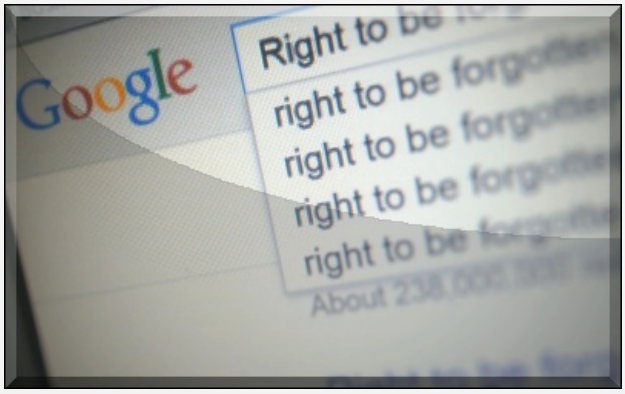
Döntések-következmények: kisebb lábnyom, kevesebb kockázat

2022. október 20. 09:53 - Csizmazia Darab István [Rambo]

Hasznos módszerek, amellyel ellenőrizhetjük digitális lenyomatunkat, és biztonságosabbá tehetjük online jelenlétünket.

Ha valaki **rákeresett már valaha a Google keresővel saját magára, az tapasztalhatta, hogy ez remek módja** annak, hogy felfedezzük a világhálón rólunk tárolt információk egy aprócska szeletét.

Probléma esetén például eldönthetjük, megkérjük-e a Google-t, hogy távolítson el rólunk olyan személyes adatokat, amelyeket nem lehetne nyilvánosan megosztani.



A Google legutóbb 2022 áprilisában módosította irányelveit a személyazonosításra alkalmas adatok eltávolításáról. Ezekbe beletartoznak a kormányzati azonosítószámok, fotók, banki adatok, kapcsolatok, személyes információk vagy például az egészségügyi adatok. Természetesen a Google nem távolítja el a hírekben vagy közhiteles adatbázisokban szereplő személyes adatokat.

A frissítés kiegészíti azt a korábban már létező lehetőséget, hogy **töröltetni lehessen az olyan tartalmakat, amelyek bármilyen módon kárt okozhatnak, ide tartoznak a nem engedélyezett pornográf tartalmak, a gyermekekről készült képek vagy a szerzői jogsértések.** A Google az Európai Unió lakosainak esetében már eleget tett az általános adatvédelmi rendelet 17. cikkelyének, azaz a törléshez való jognak, amely **minden uniós vállalatot arra kötelez, hogy kérésre törölje az érintettek személyes adatait.**

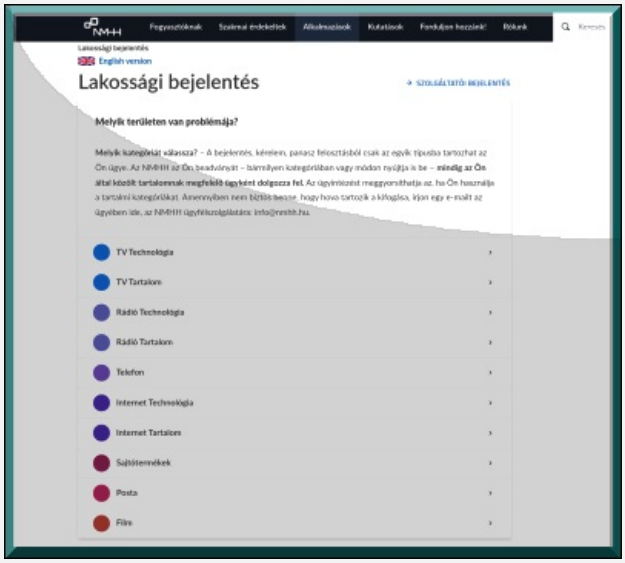
Hogyan próbálhatjuk meg törölni magunkat az internetről? **Ha valami egyszer felkerül az internetre, nincs biztos módja annak, hogy teljesen eltávolítsuk onnan.**

Ám **van néhány dolog, amit mégiscsak megtehetünk azért, hogy legalább minimalizáljuk a kockázatokat és biztonságosabbá tegyük online jelenlétünket.** Nézzük, mik is ezek!

1. Keressünk rá önmagunkra a Google keresőn.
Elsőként érdemes szembesülni azzal, hogy az internet mennyit tud rólunk. Keressünk rá a nevükre és nézzük meg az első öt oldal találatait, kombináljuk a névkeresést telefonszámmal vagy lakcímmel, hogy lássuk, milyen adatok bukkannak fel.

2. Ellenőrizzük az általunk használt szolgáltatások adatvédelmi beállításait.
Egyes platformok, mint például a Facebook vagy a Twitter adatvédelmi beállításaiban van olyan lehetőség, amely által elrejthetjük tartalmainkat és kapcsolatainkat, amelyek így nem jelennek meg nyilvánosan a keresőmotorokban.

3. Vegyük fel a kapcsolatot a weboldalak tulajdonosaival.
Amennyiben egy konkrét említést szeretnénk eltávolítani egy weboldalról, kérjük azt egyenesen a felület tulajdonosától. A legtöbb weboldalon a „Kapcsolat” menüpontban megtalálhatóak az elérhetőségek. Ha nem kapnánk kedvező választ, az NMHH (Nemzeti Média és Hírközlési Hatóság) honlapján is bejelentést tudunk tenni.



4. Töröljük a felesleges, túlzottan kitárulkozó dolgokat.
Sokan túlságosan sok bizalmas személyes információt osztanak meg magukról, családjukról. Ha aggódunk amiatt, hogy mit tud rólunk a nagyvilág, kezdjük azzal, hogy selejtezünk: töröljük a régi Facebook bejegyzéseket, tweeteket, tinédzser korunkból származó előnytelen képeket és bármilyen más, kellemetlen dolgot. Amennyiben kiemelten fontos a magánéletünk, gondoljunk a barátokra, családtagokra is, és töröljünk minden olyan fotót, amelyen ők is szerepelnek velünk.

5. Kérhetjük a Google-t és a Binget személyes adataink eltávolítására.
Használjuk a Google által rendelkezésre bocsátott új lehetőséget személyes adataink eltávolítására a keresési eredményekből. A Bing egyelőre csak a nem megengedett képek vagy sérült linkek és elavult tartalmak eltávolítását teszi lehetővé. Az EU-n belül kérni tudjuk adataink elrejtését a Google keresésből, a Bing esetében pedig kérvényezhetjük a keresés letiltását a rólunk szóló információk esetében.

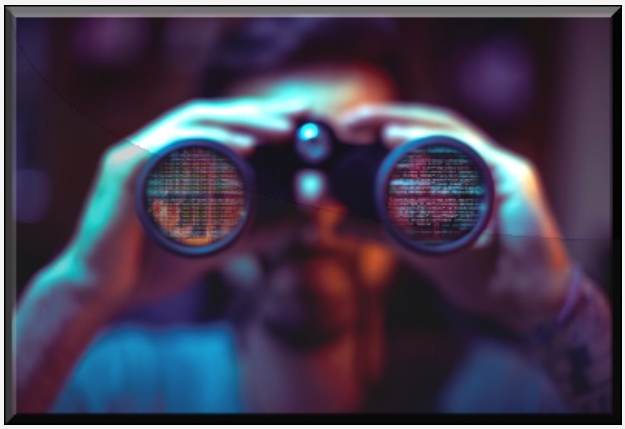
6. Gondoljuk át, érdemes-e megosztanunk valamit.

Az eddigi online jelenlét csökkentése után itt az ideje, hogy a jövőre is gondoljunk. Virtuális életünk nem szűnik meg, sokan ragaszkodnak ahhoz, hogy jelen legyenek az Instagramon, a LinkedInen vagy bármely más közösségi médiaplatformon, és ezzel nincs is semmi gond. Ugyanakkor érdemes felülvizsgálnunk az adatvédelmi beállításokat, korlátozni, hogy ki láthatja bejegyzéseinket és kerülni a felesleges, kockázatos tartalmak megosztását.

7. Használjunk VPN-t.
Ez az extra védelmi szolgáltatás (Virtual Private Network) biztosítja, hogy titkosítva legyen a kapcsolatunk, és láthatatlan legyen a tartózkodási helyünk. Emellett segít megakadályozni, hogy hackerek könnyen hozzájussanak személyes adatainkhoz. Ezt a lehetőséget asztali gépen és mobil eszközünkön is egyszerűen használhatjuk.

Ezek a lépések segíthetnek, de vajon elegendő-e mindez? Erre nincs egyszerű válasz, de valószínűleg nem. **Mindez attól is függ, hogy miként használtuk és használjuk az internetet.** Ha komolyan aggódunk a magánéletünkért, és csak korlátozottan vagyunk jelen a közösségi médiában, úgy valószínűleg könnyebben lesz törölni tudjuk digitális lábnyomunk jelentős részét.

Amennyiben viszont adataink számos platformon megtalálhatóak, a fenti cél elérése valószínűtlen. Ismerőseink biztosan tettek már közzé közös fotókat rólunk a hírfolyamukban, e-mail címünket és telefonszámunkat pedig számtalanszor használtuk már a különböző weboldalakra és alkalmazásokba való bejelentkezéshez, nem is beszélve az online tevékenységünkre vonatkozó összes adatról, amelyet ezek a szolgáltatások, a hozzájárulásunkkal, egy harmadik félnek adnak el az évek során.



Az ESET szakértői szerint azért **arra még mindig van lehetőségünk, hogy legalább részben korlátozzuk, mit találhatnak rólunk az emberek vagy a vállalatok.**

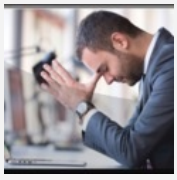
Ez pedig rendkívül fontos nemcsak a magánéletünk védelme érdekében, hanem azért is, hogy elkerüljük azokat az esetleges károkat, amelyek abból származhatnak, ha nyilvánosságra hozzák vallási, politikai, egészségügyi vagy személyes meggyőződésünket, állapotunkat.

Szólj hozzá!

Ajánlott bejegyzések:


Összeomlás


Kellemes Karácsonyi Ünnepeket!


Mai szavunk pedig: biztonsági fásultság


Ezer százalék lett, maradhat?

Cselekedettel és mulasztással

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

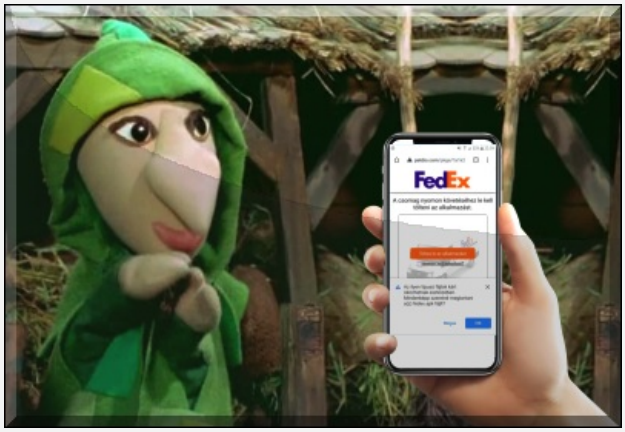
Ismét csomagunk érkezett - vagy mégsem?

2022. október 24. 10:37 - Csizmazia Darab István [Rambo]

Rövid időn belül két különböző csalási próbálkozás is landolt a postafiókunkban. Az egyik a **helytelen kézbesítési cím miatti hibára hivatkozott a német posta nevében, míg a másik a GLS nevével visszaélve próbálja átverni** a gyanútlan felhasználókat.

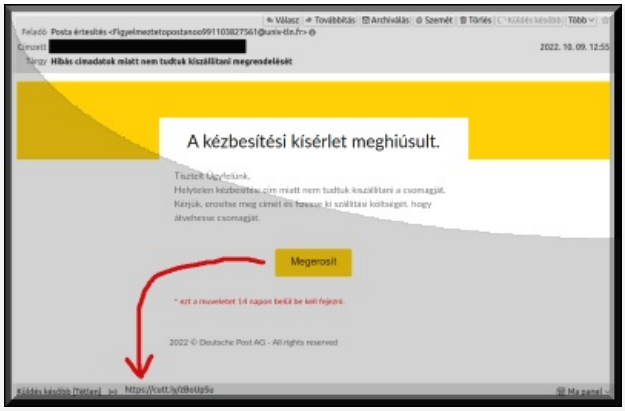
Mindenki emlékezhet rá, hogy a tavaly márciusban tömegesen kiküldött FedEx SMS üzenetek milyen problémákat okoztak sokaknál.

A Flubot vírust tartalmazó kártékony kódot **gyanakvás nélkül igen sokan letöltötték, annak ellenére, hogy nem is vártak csomagot, az üzenet magyartalan volt, szokatlan hogy idegen domainről értesítsenek bennünket, SMS-ben nem szokás külső telepítést kérni, csomag nyomkövetéshez sosem kell extra alkalmazást telepíteni, idegen URL-ről nem ajánlott ismeretlen programot telepíteni, ahogy egy ilyen kétes alkalmazásnak semmiképpen nem adunk meg kritikus fontosságú engedélyeket sem**.



Ám hiába volt megannyi intő jel, ennek ellenére mégis sokan belegyalogoltak a problémába, és áldozattá váltak.

A tömeges fertőzés következtében **személyes adatokat loptak tőlük, néhányan a bankszámlájukon található összeget is elvesztették, illetve a titokban, nevükben észrevétlenül kiküldözgetett SMS üzenetek díjával is** kénytelenek voltak szembesülni a soron következő számlájukon.

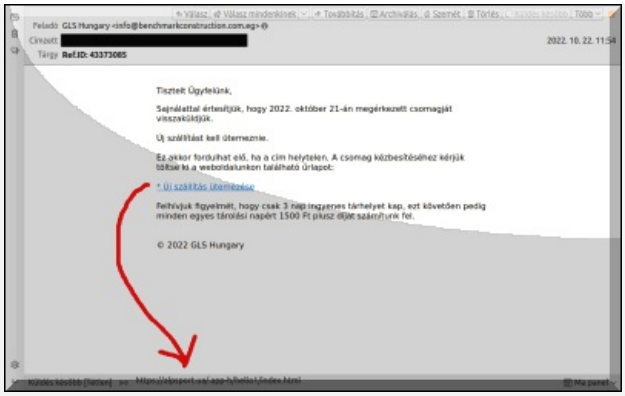


Remélhetőleg ebből mindenki megtanulta a leckét, és az újabb fordulót már biztonságtudatos hozzáállással hárítja, veszteségek nélkül. **Az első üzenet "Hibás címadatok miatt nem tudtuk kiszállítani megrendelését" tárgysorral érkezett, igaz a feladó kacifántos francia e-mailcíme és a hivatkozott Deutsche Post AG közötti ellentmondás** mindenkinek feltűnhetett.

Nem különben **a mellékelt link hivatkozás is**, amely az üzenet szerint arra hivatott, hogy ennek segítségével erősítsük meg fizikai postacímünket, és **előre kifizethessünk egy állítólagos szállítási költségét, amit semmiképpen nem ajánlott megtenni. A sürgetési faktor nem hiányzik a receptből, maximum 14 nap áll rendelkezésünkre a mondvacsinált "megerősítésre".**

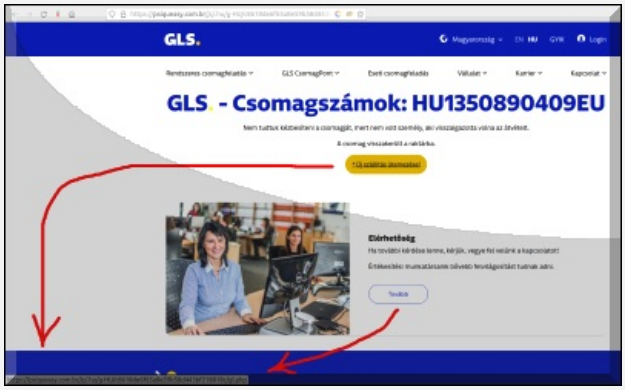
A cut.ly rejtett rövidített link persze nem a Posta, vagy a Deutsche Post webhelyére mutat, hanem egy adathalász oldalra irányít, amit viszont rekordgyorsasággal letiltottak, így ezt már mi sem tudtuk itt bemutatni.

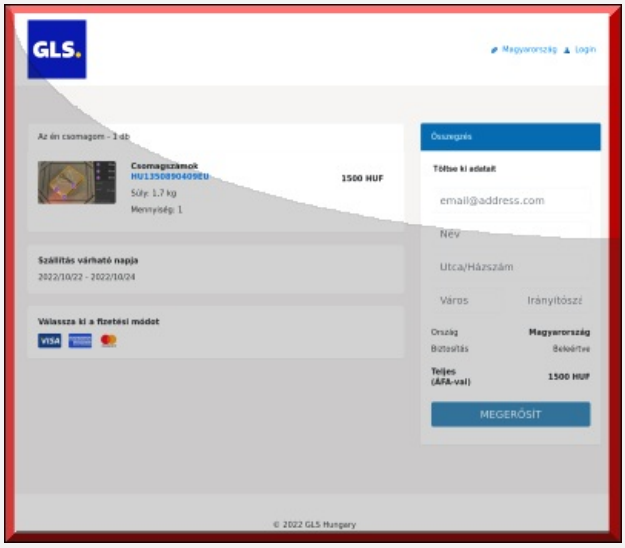
A másik üzenet is hasonló kaptafára készült, de ott látszólag a GLS ír nekünk, a levél tárgysora pedig egy igen hivatalosnak tűnő referencia szám. Ha ránézünk **a feladói címre, az .eg Egyiptom internetes legfelső szintű tartomány kódja, ami már önmagában is elég valószínűtlennek tűnik, ha Magyarországon a GLS Hungary** igazi csomagról akarna értesíteni bennünket.



A román és amerikai szervereken keresztül érkező üzenetben itt is azt írják, hogy **a helytelen cím miatt a csomagunkat visszaküldik, ám az állítólagos címmegerősítésre való kattintást itt azzal is nyomatékosítják, hogy ha nem lépünk azonnal, akkor a hiba miatti tárolásért napi 1500 forint kötbért számítanak majd fel.**

Ha másért nem is, itt azért már ki kellene gyulladnia a képzeletbeli vészcsengőnek mindenki fejében.





A link itt is idegen helyre, ezúttal egy ukrán weboldalról egy brazil URL-re irányít, ahol egy GLS oldalnak látszó felületen a bűnözők megkísérlik begyűjteni a személyes (név, e-mailcím, postacím, valamint bankkártya adatainkat. Ahogy a bankok, és immár a magyar bankok nevében érkező átverések is napi szinten támadnak bennünket, sajnos az ismert csomagküldő szolgálatok és postai szolgáltatást végző cégek nevével is egyre gyakrabban élnek vissza.

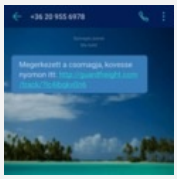
Muszáj mindenkinek felkészülnie, és felvérteződnie az adathalászat elleni védekezésre, és a megelőzésre - erről korábban itt írtunk bővebben, részletes tanácsokkal segítve a felhasználókat.

Szólj hozzá!
Címkék: posta csomag post csalás átverés deutsche megtévesztés adathalászat adatlopás gls csomagküldő

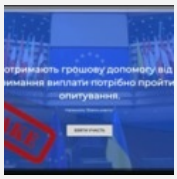
Ajánlott bejegyzések:


Magyar Posta csomagunk jött - vagy mégsem?

Banki meló


Megérkezett a csomagja - vagy mégsem?


Viva la Revolut


Adathalászok lakat alatt

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.

VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

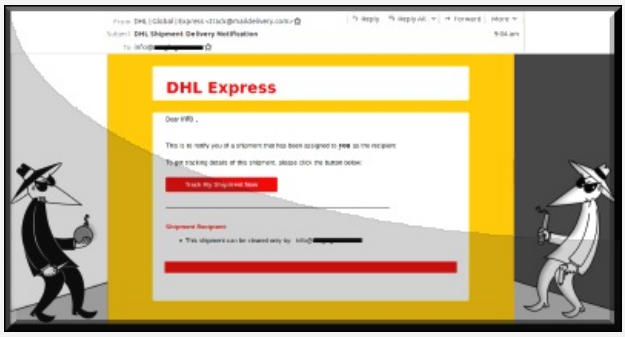
accountz

Belépés
Regisztráció

Sikeres brandek az adathalászatban

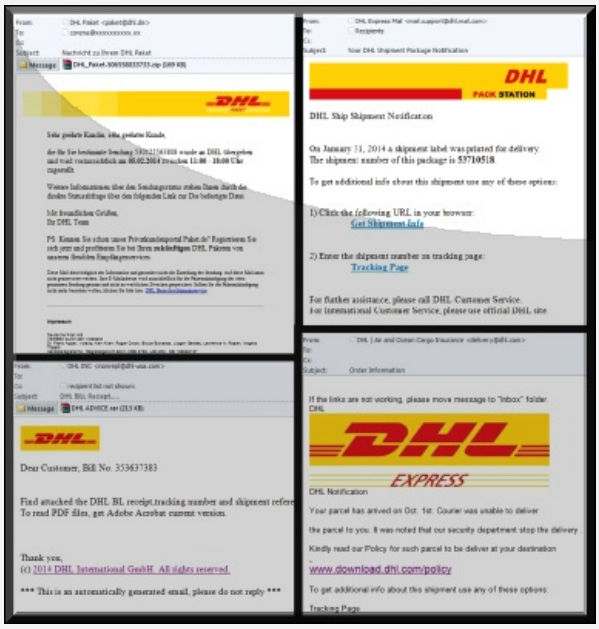
2022. október 26. 09:36 - Csizmazia Darab István [Rambo]

Szerencsére igen sokszor kerül szóba az egyik leggyakoribb, ha nem a leggyakrabban áldozatot szedő csalási forma. Ez pedig az eredeti phishing szóból származó adathalászat.



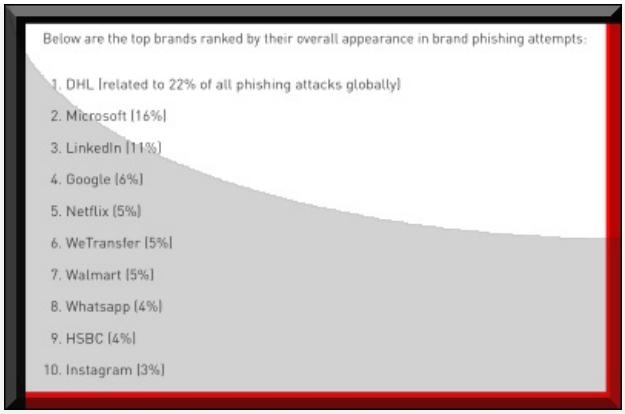
Itt a blogon is szóba került már többször, legutóbb éppen a csomagküldő GLS esete, de ma reggel Index címlapos az **"Így kerülje el, hogy az adathalászok horgára akadjon" című cikk is**.

A Covid ezt is "elintézte" nekünk, hogy a csomagküldő szolgálatok nevében elkövetett visszaélések száma drámain megugrott, talán mindenki emlékszik a tavaly márciusi FedEx-es SMS áradatra.



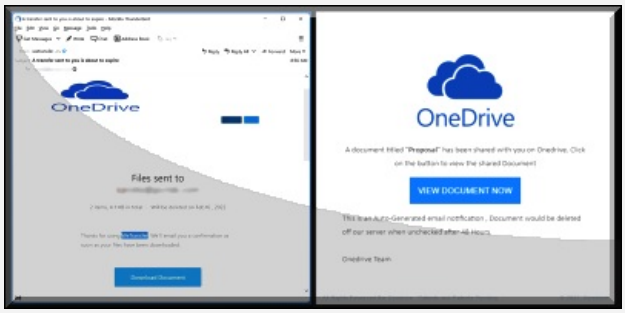
Ezúttal egy olyan toplista készült, amely az adathalászokat leginkább bevonzó márkák, szolgáltatások rangsorát szedte össze 2022 júliusa és szeptembere közötti időszakra vonatkozóan. A gyűjtés adatai alapján a DHL állhat a képzeletbeli dobogóra, 22%-a az összes esetnek az ő nevükkel visszaélve történt. A csalások tömeges e-mail küldésen és számtalan hamisított hasonmás weboldalon alapult, ahol a felhasználók személyes adatain kívül a bankkártya adataikat is igyekeztek eltulajdonítani kézbesítési hibára hivatkozva.

Sajnos a valóságban is többször előfordul hibás címzés, elkallódó csomag, ami miatt hihetőnek tűnhet az ilyen levél.



Második helyezett a Microsoft lett 16%-kal. Itt a módszer egy olyan megosztott csali dokumentum, amelyhez egy hamis OneDrive bejelentkező ablak jelenti a veszélyt - a belépési adatokat begépelve azonnal illetéktelen kezekbe kerülnek a login azonosítók. A LinkedIn áll a dobogó harmadik fokán, az ezzel kapcsolatos visszaélések 11%-ot hasítottak ki az adathalászati tortából.

A számos ismert márkát tartalmazó listát záró tizedik helyre került az Instagram, az ottani incidens is egy jelentős tömeges kampány része volt, amely sok áldozatot szedett.

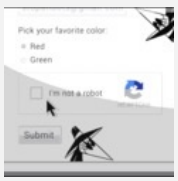


Összességében elmondhatjuk, érdemes óvatosnak és biztonságtudatosnak lenni, amikor személyes adatokat és hitelesítő adatokat kérnek tőlünk alkalmazások vagy weboldalak.

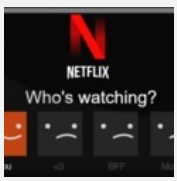
A gyanús kéretlen üzenetekkel is fontos vigyázni, nyilván az említett neves szereplők a leggyakoribb megszemélyesített szolgáltatók, de gyakorlatilag bármilyen toplistán nem szereplő hivatal, cég nevében - pl. adóhivatal, vakcinainfo, VPN szolgáltató, stb. - érkezhet hasonló átverés.

Szólj hozzá!
Címkék: microsoft toplista szolgáltató linkedin phishing dhl adathalászat csomagküldő instagram

Ajánlott bejegyzések:


Mai szavunk pedig: reCAPTCHA


Ismét csomagunk érkezett - vagy mégsem?



Tagsági kérdések - vagy mégsem?


Csomagja érkezett - sokadik menet


Egyre gyakoribb a banki adathalászat

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Antivírusblog
245 követő

Oldal követése Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog

Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Csupasz pisztoly hívja felhasználót, vétel!

2022. október 27. 09:52 - Csizmazia Darab István [Rambo]

Egy csodálatos spamet kaptunk egyik olvasónktól, ezúton is köszönet a remek találatért. Röviden, kapunk egy "Rendőrségi meghívó közlemény"-nek látszó izét, melyben közlik velünk, hogy le fognak bennünket tartóztatni.

A nyersfordítás és a magyartalanság minden építőköve együtt volt ahhoz, hogy mind a levél szövegrésze, mind pedig az oklevél-szerű lényegi értesítés magán hordozza Buzgó Mócsing, Csülök, Fülig Jimmy és Török Szultán sziporkázó stílusát. A bevezetésben egy Maleczk Péter nevében (itt semmi rendfokozat vagy beosztás nem található a neve mellett) írt üzenet **arról tájékoztat minket, hogy állítólag feljelentettek bennünket, nyissuk meg a mellékletet és válaszoljunk, ellenkező esetben jön a letartóztatás.**

Vegyük észre mindeközben, hogy a válaszcímnél viszont már "Maleczky" szerepel, és hogy a címzett nem egy adott személy, hanem a tömegesen kiküldött körlevelekre jellemző: " undisclosed-recipients: ;".

Mielőtt még magára a mellékletre - ami egy ártalmatlan .PNG grafikus fájl, azaz képállomány - rátérnénk, nézzük meg előtte a feladót is. Ez nem tűnik sem a rendőrségnek, sem semmilyen hivatalos magyarországi hatóságnak, esetleg a dijoni mustárhoz lehet annyi köze, hogy azt is Franciaországban gyártják.

Vagyis látható, minimális erőfeszítést sem tettek a terjesztők arra, hogy legalább autentikusnak látsszon a feladó, emiatt valami betűcserés doménnel - typosquatting, vagy egyéb homografikus, azaz nyelvi karakterek hasonlóságával való trükközéssel bajlódjanak.

A 74253. számú meghívó képe itt található, e**bben kapjuk az "Idézést az igazságosságra", de szigorúan csak a kibernetikus beszivárgások lefoglalását követően. Itt már aláírás is található, ebből megtudhatjuk, hogy az említett Maleczky Péter nem más, mint a "Magyar Bűnügyi Rendőrség Hivatal Szövetségi, Fiatalkorúak Védelmi Brigádja, Fiatalkorú Védődandár."**

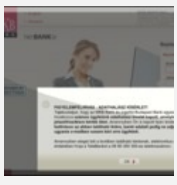
Ezzel a kitalált szervezettel és képzeletbeli titulussal nagyjából le is lepleződik az üzenet, **remélhetőleg senki nem fog szívinfarktust kapni a túlságosan is hihető és a fantasztikusan életszerű fogalmazástól.**

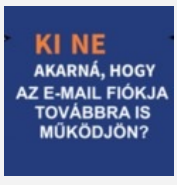
Összefoglalva az ijesztgetés nem túl hatásos, a feladó és a szövegezés árulkodóan primitív, és szerencsére a levél híján van kártékony mellékletnek, valamint rosszindulatú webhelyre sem mellékelnek benne (egyelőre) kattintható linket.

Vélhetően egy angol nyelvterületen már használt, de magyar nyelvre silányan implementált kísérletről lehet szó, vagy talán egy induló új átverésnek az első pilot változata, amelyet később majd vírusokkal, és kártékony linkekkel ékesített verziója fog esetleg követni, meglátjuk. **Mindenesetre még egyszer köszönet a küldőnek, aki elmondása szerint annyira nem is tart a letartóztatástól, mint amennyire szeret néha rákönyökölni a Delete gombra.**

1 komment
Címkék: spam rendőrség csalás átverés scareware

Ajánlott bejegyzések:

Igazgató-e vagy? | MKB adathalászat szigonnyal, horoggal, hálóval | Csomagja kézbesítésre vár! Vagy mégsem? | Elon Musk és Warren Buffett írt nekünk | Egypálcás adathalász próbálkozások

Kommentek:

Head Honcho 2022.10.27. 10:25:10

Manapság már arra is figyelni kell, hogy melyik rendőrség, mert ezeknek a magyar államiságot tagadó konteós szervezeteknek (UCC, MATT, stb.) már külön van. :)

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

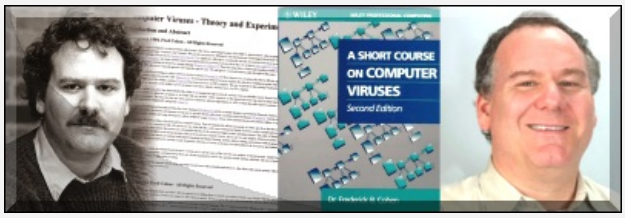
Antimalware Day

2022. november 03. 13:22 - Csizmazia Darab István [Rambo]

Sok mindennek van már világnapja, például a hóembereknek, a nutellának, méheknek, a vakvezető kutyáknak, a TBC elleni küzdelemnek, de van az informatikai biztonságnak (ITBN) is. **November 3-a viszont az Antimalware Day.**

A dolog eredete 1983. november 3-ra vezethető vissza. Emlékezetes lehet talán sokaknak Frederick Cohen neve az első számítógépes vírussal kapcsolatban. **Cohen, a Dél-kaliforniai Egyetem számítógép-tudományi kar hallgatója az első dokumentált kísérletezést végezte el 1983-ban végezte egy Unix alapú VAX 11/750 gépen, a programkód alig nyolc óra alatt íródott.**

A kísérleti vírus aztán olyannyira jól sikerült, hogy egy rendszert átlagosan 30 perc alatt képes volt megfertőzni. Kutatásairól könyvet is írt, ebben részletesen kidolgozta a vírusok viselkedésének matematikai modelljét.

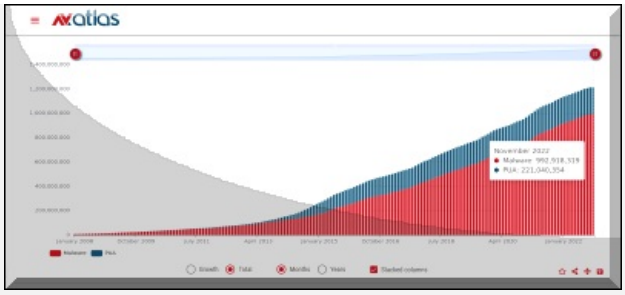


Bár a vírustörténelemben egy másik, jóval korábbról származó dátum is jogosan szerepelhetne, nevezetesen a PDP-10 mainframe gépeken futó, 1971-ben megjelenő Creeper "vírus".

Ez szintén egy PoC, azaz kísérleti kód volt, melyet Bob Thomas nevével kapcsolnak össze - arra törekedett, hogy az akkori ARPANET hálózatban terjedjen gépről gépre. **Kárt egyáltalán nem okozott a terjedésen kívül, csak látványosan kiírta a képernyőre, hogy: "I'm the creeper, catch me if you can!".**

Visszatérve Cohenre, **november 3-a emiatt, Dr. Fred Cohen és Prof. Leonard Adleman munkájának tiszteletére lett az Antimalware Day, azaz a vírusok elleni védekezés világnapja. Ez a nap a "számítógépes vírus" első használatának és a számítógépes vírusok elleni védelemnek és az ellenük irányuló folyamatos keresésnek a napja lett.**

A két számítógépes tudós 1983. november 3-án történelmet írva egy **olyan koncepciót demonstrált, amelyet bármilyen csatlakoztatott rendszer megfertőzésére használhattak volna.** Ezt a prototípust később Prof. Adleman nevezte el számítógépes vírusnak.



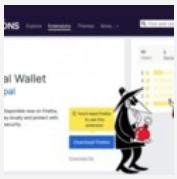
Ez a nap a rosszindulatú programok elleni küzdelem kezdetét is jelenti számunkra, vagyis nem csak a szakmának, hanem minden felhasználónak is. **A kártékony kódok ma már nemcsak klasszikus vírusokat, hanem mindenfajta számítógépes fenyegetést is tartalmaznak. Mára már 1.2 milliárdnál is több egyedi kártékony kód, vírus, féreg, és trójai ellenében egy folyamatosan zajló küzdelemben** igyekszünk megóvni számítógépeink, hálózataink, internetes eszközeink, informatikai rendszereink biztonságát.

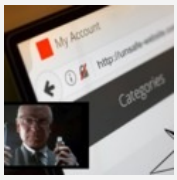
A címlapra még egy fél mondattal visszatérve Adleman számítógépes szakértő volt az 1992. Komputerkémek (Sneakers) című filmnél.

Szólj hozzá!
Címkék: fred day cohen világnap leonard elleni kártékony antimalware kódok adleman

Ajánlott bejegyzések:


Xenomorph kalandjai GooglePlay országban


Bízz embertársaidban, de emeld meg a kártyapaklit!


Biztonságos? Biztonságos?


Az elveszett jelszavak fosztogatói


És ez az a nap!

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.

VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

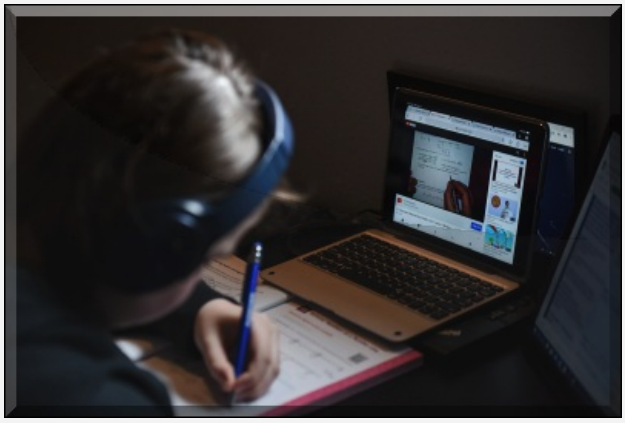
Iskolák a kiberbűnözők célkeresztjében

2022. november 08. 09:09 - Csizmazia Darab István [Rambo]

Az iskolák is egyre jobban ki vannak téve rosszindulatú kibertámadásoknak. Mit tehetnek az intézmények, hogy megerősítsék védelmüket és távol tartsák maguktól az internetes fenyegetéseket?

A világjárvány kezdetekor egyik hétről a másikra tanárok és diákok kerültek át a fizikai tantermekből az online videoplatformok virtuális osztálytermeibe. A könyveket felváltották a táblagépek, a tábla helyett a képernyőmegosztás vált rutinná, az üzenetküldő alkalmazások pedig a szocializáció új színterévé váltak.

Az online oktatásra váltó iskolák számára új kihívások merültek fel az adatvédelmi aggályok, az adatszivárgás és a hackerek jelenléte miatt. **Ez az újfajta oktatási mód azonban velünk maradt azután is**, hogy a tanulók mostanra jórészt visszatértek az iskolaépületekbe.



Minden iskola kockázatot vállal, hiszen számos érzékeny adatot birtokolnak, gondoljunk csak a nevekre, címekre, a diákok egészségügyi adataira és fizetési adatokra. Minden munkahely, így az iskolák és dolgozóik számára érzékeny adatokra pedig kiemelten utaznak a támadók, belekalkulálva azt az esélyt, hogy az iskolák közül sok helyen hiányos, anyagi okok miatt gyengébb védelmet találnak majd.

A napokban derült ki, hogy még szeptemberben érte **kibertámadás a KRÉTA rendszerét, melyet sokan csak mint e-naplót ismerik, ám valójában egy komplett közoktatási informatikai rendszer, rengeteg érzékeny adattal a gyerekekről és a pedagógusokról. Információk szerint valamennyi diák összes, a KRÉTA-ban kezelt adata kiszivároghatott, de nemcsak ezekhez, hanem a cég más adatbázisaihoz és a forráskódokhoz, illetve a fejlesztők belső kommunikációjához is hozzáférhettek.** Adatvédelmi szempontból aggasztó lehet, hogy ezen adatok alapján egészen részletekbe menő profil is megalkotható egy-egy diákról.

Feltörhették a KRÉTA-t, a diákok adatai is kiszivároghattak

TECH BELFÖLD Legfontosabb 2022. november 07. – 10:30

A Köznevelési Regisztrációs és Tanulmányi Alaprendszer (KRÉTA) bejelentkezési oldala egy táblagépen – Fotó: Varga György / MTI

Bolcsó Dániel Másolás 942

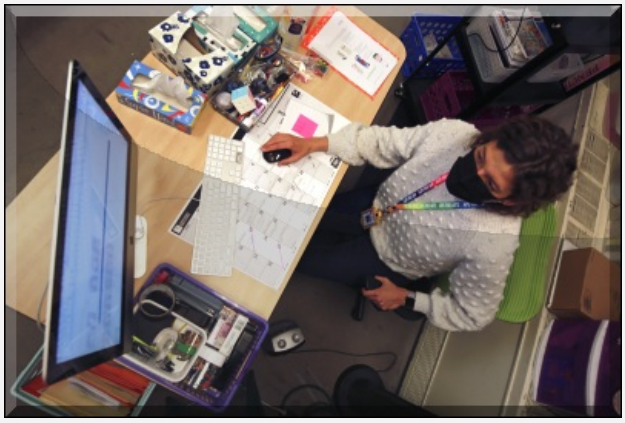
Néhány héttel ezelőtt adathalász támadás érte a Köznevelési Regisztrációs és Tanulmányi Alaprendszer, azaz a KRÉTA fejlesztőcégét, az eKRÉTA Informatikai Zrt.-t.

A támadás sikeres volt, így a támadó illetéktelen hozzáférést szerezhetett a közoktatás minden intézményében kötelezően használt adminisztrációs rendszer adataihoz – értesült a Telex a cégtől független forrásból.

Úgy tudjuk, valamennyi diák összes, a KRÉTA-ban kezelt adata kiszivároghatott, de nemcsak ezekhez, hanem a cég más adatbázisaihoz és a forráskódokhoz, illetve a fejlesztők belső kommunikációjához is hozzáférhettek.

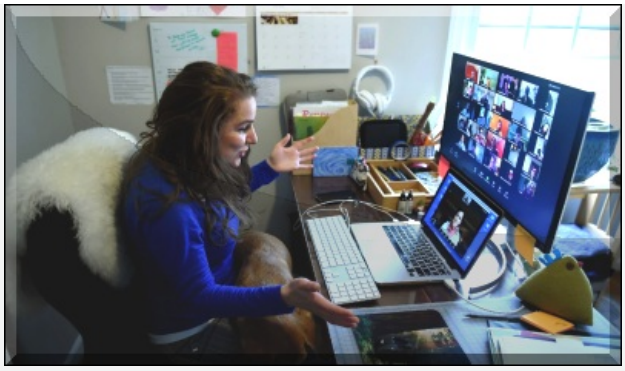
A kiberbiztonság ezáltal az intézményvezetők egyik legfőbb feladatává vált. **A fenyegetések nagyon különböző formákban és forrásokból érkezhetnek, soroljunk fel párat:**

- Hackerek:
A kiberbűnözők automatizált támadásai a leggyakoribb esetek, ezek jelentik a legnagyobb fenyegetést. A hackerek adathalász e-maileket küldenek, amelyek ugyan valósnak tűnnek, de igazából átverések. Céljuk, hogy az iskolákban dolgozó címzettek rákattintsanak a levélben szereplő linkre, és akaratlanul is hozzáférést adjanak a személyes adatokhoz. A birtokukba került információ által a támadók bankszámla adatokat lophatnak, amelyekkel csalást követhetnek el, vagy akár el is adhatják azokat. Valós kockázatot jelentenek a zsarolóprogram-támadások is, amelyekkel a hackerek túszul ejtik az iskola adatait és váltságdíjat követelnek értük.



- Diákok:
Az iskolák saját diákjai is lehetnek támadók, akik megpróbálják feltörni az iskola rendszerét. Néha mindez csak szórakozásból történik, máskor viszont az érdemjegyek megváltoztatása, a diáktársak adatainak megszerzése a cél.

- Iskolai alkalmazottak:
A diákokhoz hasonlóan az intézményben dolgozók is követhetnek el belső kibertámadást. Bár ez ebben a szektorban ritka eset, mégis előfordulhat, hogy szándékosan kárt akarnak okozni, vagy valamilyen bosszú áll a támadás hátterében, emiatt jobb felkészültnek lenni.



Bár a téma összetettnek tűnik, az ESET szakértője szerint a kiberbiztonság lebontható öt egyszerű lépésre, amelyeket egy új stratégia megalkotása és végrehajtása során érdemes követni.

1. Készüljön leltár az eszközökről:
Hány laptopja van az iskolának? Mindegyik megfelelően működik? Telepítettek rájuk biztonsági szoftvert? Az operációs rendszer és az engedélyezett alkalmazások a legújabb verzióra van frissítve? Vegyük sorra az összes eszközt, és írjuk össze, hogy az egyes berendezések **hol találhatóak, ki férhet hozzájuk, és hogy szükség van-e a további** vizsgálatukra.

2. Rendelkezzen az iskola saját informatikai kollégával:
Annak érdekében, hogy tisztában legyünk a leltárba vett eszközök megfelelő működésével, a berendezések naprakészségével, szükség van egy külön felelős informatikusra vagy egy informatikus csapatra. Csak szakember képes az ilyen berendezések megfelelő vizsgálatára és karbantartására. **Az informatikai szakemberek feladata a felhasználói azonosítók beállítása erős jelszavakkal és kétfaktoros hitelesítéssel, valamint annak nyomon követése, hogy ki melyik eszközhöz fér hozzá. Az ő felelősségük emellett egy átfogó és könnyen értelmezhető felhasználói szabályzat bevezetése** az iskola dolgozói, illetve a diákok számára.

3. Szervezzünk kiberbiztonsági workshopokat az iskola munkatársainak:
Kezdjük a nulláról és feltételezzük azt, hogy a dolgozók közül senki nem rendelkezik kiberbiztonsági ismeretekkel. Ezt a tudást érdemes célzott workshopokon keresztül átadni számukra. Tartsunk előadásokat a terület szakértőinek meghívásával, kérjünk támogatást a helyi vezetéstől, és keressünk hasznos online forrásokat. **Győződjünk meg arról, hogy az iskola munkatársai azonosítani tudják a gyanús adathalász e-maileket, megértik, miért nem érdemes megosztani az eszközeiket, kiadni jelszavukat, és miért veszélyes olyan képeket közzétenni, amelyeken érzékeny információk találhatóak.**

4. Ösztönözzük a munkatársakat arra, hogy jelentsék a lehetséges fenyegetéseket:
Mindenki követhet el hibákat, és az ezek bejelentésétől való félelem növelheti az iskola veszélyeztetettségét, kitettségét. Biztosítsuk a munkatársakat, hogy nem éri őket hátrány, ha véletlenül áldozatul estek egy átverésnek. Az a cél, hogy haladéktalanul jelentsék az ilyen eseteket, mert csak így lehet megvédeni őket és az iskolát. A hackerek egyszerű, megtévesztéses (social engineering) módszereket is bevetnek az emberek átverésére, így igazából mindenkiből lehet áldozat.

5. Legyen a kiberbiztonság az iskolai tanterv része:
A tanároknak nem csak az iskolát kell megvédeniük az esetleges fenyegetésektől, de a kiberbiztonság terén is jártasnak

kell lenniük, hogy ezt a tudást is átadhassák diákjaiknak. Még ha van is külön informatikaóra, ahol ezeket a témákat érintik, vagy mélyrehatóan tanítják, fontos, hogy az informatikai oktatás mindenki számára legyen elérhető, tekintve, hogy a laptopok és mobiltelefonok használata ma már a mindennapi életünk része.

Alapvető fontossággal bír, hogy a diákoknak és a tanároknak nem csak a tantermekben kell betartaniuk az online biztonsági szabályokat. A kiberbiztonságnak az iskolán kívül is kiemelt figyelmet kell kapnia, főleg, ha figyelembe vesszük, hogy a kockázatok mennyire jelen vannak az életünkben.

Egy olyan témában, ahol a gyerekek általában tapasztaltabbnak tartják magukat a felnőtteknél **fontos, hogy mind a tanárok, mind a szülők lépést tudjanak tartani a fiatalok online térben szerzett tudásával, és mindhárom szereplő képes legyen biztonságtudatosságát folyamatosan fejleszteni, tanulni, fejlődni.**

Szólj hozzá!
Címkék: oktatás fenyegetés iskola diák tanár védelem megelőzés kockázat intézmény

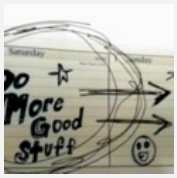
Ajánlott bejegyzések:


Mai szavunk pedig: biztonsági fásultság


10 gyakori IT biztonsági hiba


Kiberbiztonsági útikalauz diákoknak

Az adathalászatot megölni nem kell félnetek



10 kiberbiztonságra veszélyes szokás

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.

VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

10 gyakori IT biztonsági hiba

2022. november 10. 11:49 - Csizmazia Darab István [Rambo]

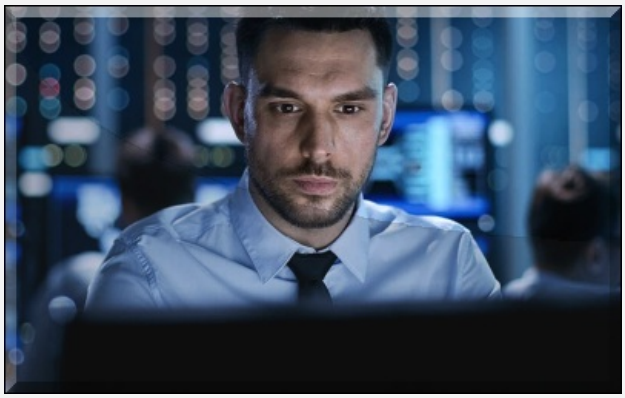
Ma már mindenki megtapasztalhatja, nem kell híres embernek vagy szervezethez tartozónak lenni ahhoz, hogy kibertámadások garmada próbálkozzon behatolni a számítógépünkbe, netes eszközeinkre. **Összegyűjtöttük a tíz leggyakoribb hibát vagy mulasztást, ami a kockázatokat növeli.** Érdemes ezeket elkerülni, megelőzni.

A Covid csak katalizátora volt annak a folyamatnak, hogy egyre inkább online, felhőkben töltsük el időnk java részét. **Egy brit tanulmány szerint a munkaidőt nem számítva napi 5 óra az átlagos képernyőidő**, ami nem kevés.

A 16-24 évesek egyébként is viszik a prímet, például a felmérésbeli évi 2500 órát visszaosztva egyedül csak az Instagramozással átlagosan 6.8 órát töltenek el napi szinten.

Mikre érdemes figyelni, mit érdemes elkerülni ahhoz, hogy javuljon a biztonságunk? Röviden összefoglalva jobban kell kezelnünk a biztonsági kockázatokat és fejlesztenünk kell a biztonságtudatosságunkat. Van is okunk minderre, a már közismert AV-Test nyilvántartás szerinti egyedi kártékony kódok, vírusok száma már elérte az 1.21 milliárdos számot, míg a haveibeenpwned weboldalán 11.9 milliárd ellopott, feltört név-jelszó páros sorakozik.

De említhetjük azt **Digital Shadows által jegyzett kutatást is, miszerint 24 milliárd felhasználónév és jelszó érhető el a dark weben, ami két év alatt 65%-os növekedést jelent**. Következzen akkor pár hasznos tipp.

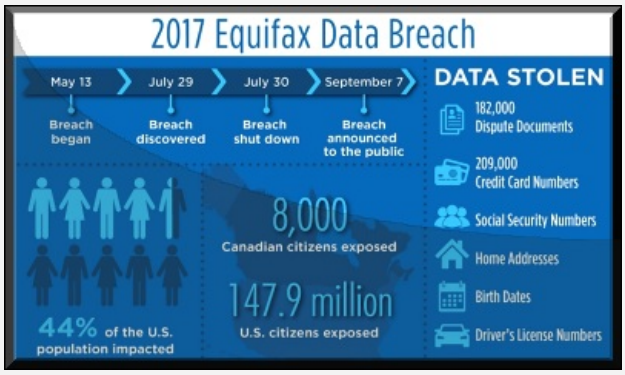


01. A leggyakoribb átverések egyik az adathalászat
Jön a kéretlen üzenet, fedélzetén egy rosszindulatú webhelyre mutató linkkel, vagy egy kártékony fájlmelléklettel, és a felhasználók többsége gondolkodás nélkül kattint ezekre, legutóbb például az eKréta üzemeltetők estek áldozatul ilyen incidensnek. Érdemes óvatosnak, gyanakvónak lenni, hiszen **ez egy nagyon hatékony átverési mód, és pusztító**

következményei lehetnek.

02. Frissítések elmulasztása
Az operációs rendszer, és az alkalmazói programok **rendszeres hibajavító frissítéseket kapnak, hogy ezzel befoltozzák a kártevők által kihasználható sérülékenységeket, sebezhetőségeket**. Érdemes bekapcsolni az automatikus frissítéseket minden eszközünkhöz, szoftvereinkhez, böngészőhöz és operációs rendszerünkhöz.

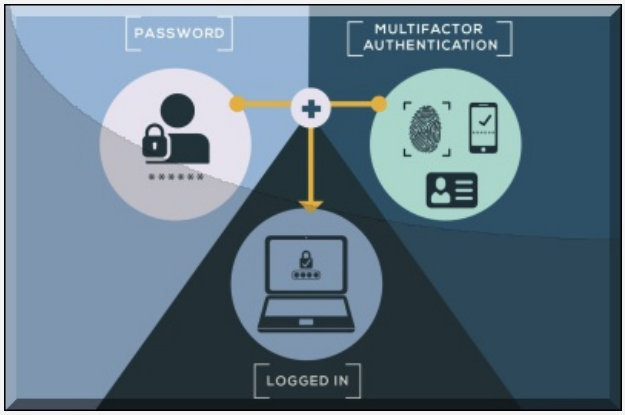
Emlékezetes, hogy 2017-ben az USA egyik legnagyobb hitelminősítő intézete, az Equifax olyan incidens áldozata volt, ahol 143 millió adat szivárgott ki, és összesen 2mrd USD kár keletkezett. **Az utólagos vizsgálatoknál kiderült, nem csak akkor nem frissítettek, de a cégnél nem is létezett szabályozott rendje a hibajavításoknak, és nem is volt kinevezett felelőse sem** ezen feladatok elvégzésének.



03. Ismeretlen USB eszközök csatlakoztatása
Szintén gyakori veszélyforrás a cserélhető adathordozók fertőzöttsége. Érdemes óvatosan kezelni a nem-saját eszközöket, és csatolás előtt alapos vírusellenőrzést végezni rajtuk.

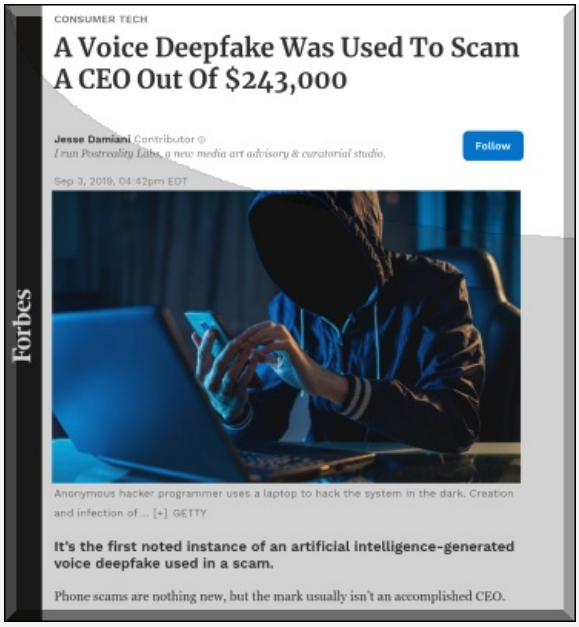
04. Gyenge jelszavak használata és újrafelhasználása
Ez egy örökzöld téma, nem lehet elégszer hangoztatni a fontosságát. **A jelszavaknak, vagy még jobb, ha jelmondatoknak hosszúnak, erősnek és egyedinek kell lenniük. Megjegyzésükhöz, generálásukhoz használjunk jelszókezelőt, jelszó széfet,** hogy biztonságban és könnyen használható legyen.

05. A többfaktoros autentikáció mellőzése
Kapcsolódva a fentiekhez, a két vagy többtényezős hitelesítés egy extra biztonsági réteget ad a belépési folyamathoz, aminél egyszeri SMS kódot, biometrikus azonosítást vagy valamilyen hitelesítő alkalmazás OTP kódját is meg kell adni a sikeres bejelentkezéshez. A vállalatok, szervezetek egyre inkább arra kényszerítik munkatársaikat, hogy ezeket használják minden fiókhoz, ám sajnos sok cégnél még mindig mellőzik. Emlékezetes lehet a Colonial Pipeline 2021-es esete, **ahol a mérnökök távmunkában otthon dolgoztak a pandémia idején, de említhető az eKréta eset is - egyik helyen sem volt kétfaktoros autentikáció,** a következményeket pedig már ismerjük.



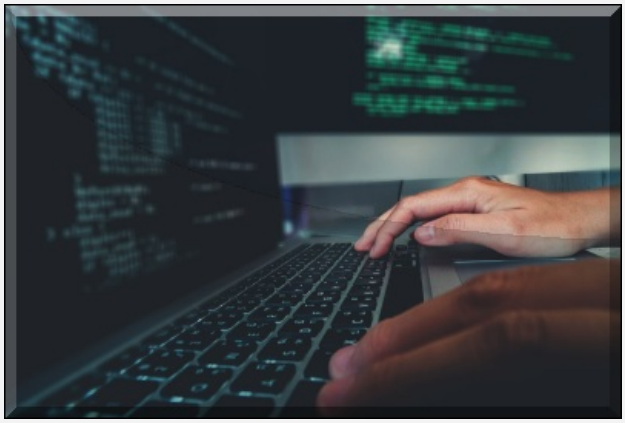
06. Hiányzó biztonsági mentés
Még magánfelhasználóknál is fontos, de vállalati környezetben egyenesen nélkülözhetetlen. Lehet rá szükség rendszerösszeomlás, hardver meghibásodás miatt is, de a lassan tíz éve pusztító zsarolóvírusok miatt még jobban felértékelődött a jelentősége. Ha friss példát kellene említeni, akkor **idén márciusban a Rosaviatsia, vagyis az orosz polgári repülés irányítást feltörték, és 65 TB mennyiségű adatot nem csak elloptak, de töröltek is**. A rendszer leállt, mert nem volt mentésük, elmondásuk szerint mert "nem volt rá költségvetés".

07. Óvatlanság
Egy kimutatás szerint egy átlagos munkaidő alatt egy számítógépen dolgozó felhasználó 150 ezer kattintást végez. A biztonságtudatos felhasználás, az óvatosság tanulható ugyan, de munkahelyi környezetben ezt rendszeres képzéseknek is kell kísérnie, mert ez egy örök probléma. **A túlterheltség, a kapkodás nem kedvez a tudatosságnak, ellenben hihetetlen károkat képes okozni a felelőtlen, átgondolatlan kattintás. Megint csak egy élő példa, 2019. tavaszán egy angol energetikai cég vezérigazgatója 220 ezer eurót utalt át egy ismeretlen magyar beszállító számlájára, ahol a megtévesztésben a vállalat németországi vezetőjének hangját utánozták le sikerrel.** A hanghamisításban a főnök azonnali átutalást rendelt el, és a hangját a csalók annyira jól utánozták le, hogy az akcentus, a beszéd szokásos hanglejtése, sebessége is tökéletes volt. A mintegy 72 millió forintnak megfelelő összeget az ismeretlen elkövetők a magyar számláról azonnal továbbutalták egy mexikói számlaszámra.



08. Munkahelyi eszközök magánhasználata
A Covid időszakban történt lezárásban hirtelen mindenkinek otthonról kellett dolgoznia, amihez megfelelő számú eszközt kellett biztosítani - átcsoportosítani, vásárolni, bérelni - az otthoni munkavégzéshez. Volt ahol ezt sikerült megugrani, és volt ahol nem. **Ám a dedikált munkahelyi eszközök privát használata mindenképpen kockázat,** legyen szó hétköznapi munkavállalóról, vagy vezető beosztású munkatársakról. **Egy korábbi felmérésben például a vezető eszköze azért volt fertőzött volt, 56% adathalász levélre kattintott, 45% átengedte a használatot a családtagjainak, 47% fertőzött USB-t csatlakoztatott, és 40% felnőtt tartalmú weboldalt látogatott.**

09. Hamis biztonságérzet
A biztonság nem egy állapot, hanem egy véget nem érő folyamat, amin mindig dolgozni kell. Robert S. Mueller, korábbi FBI igazgató úgy fogalmazott: "*Két féle cég van, akiket már feltörtek, és akiket még nem.*" Ennél talán közelebb áll a valósághoz John Chambers, Cisco vezérigazgató megközelítése, miszerint "*Két féle cég van, akik már észrevették, hogy feltörték őket, és akik még nem vették észre.*" **Szánjuk időt és energiát a biztonsági beállításokra, és folyamatosan tájékozódjunk a fő kockázatokról, ezek kezeléséről.**

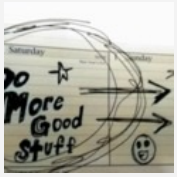


10. Nem minden eszközön használunk biztonsági szoftvert
Ma már nem kérdés, hogy **kártékony kódok, sebezhetőségek minden platformon előfordulnak, legyen az Windows, Macintosh, Linux, Android vagy bármi más.** Gyakori hiba, ha például a mobiltelefont vagy a tabletet kihagyják a védelemből, pedig a kockázat itt is ugyanúgy létezik adathalászat, vírusok, kémprogramok formájában. Érdemes gondoskodni arról, hogy minden számítógép és eszköz védve legyen.

3 komment
Címkék: hiba trükkök tippek védelem megelőzés védekezés mulasztás biztonságtudatosság welivesecurity.com

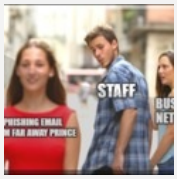
Ajánlott bejegyzések:


10 alaplépés a biztonsághoz

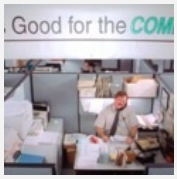


10 kiberbiztonságra


7 tipp a mobilunk



10 gyakori ok, amiért



Karácsonyi vásárlás

veszélyes szokás | védelméhez | bedőlünk a csalásoknak | biztonságosabban

Kommentek:

Mesterséges Geci 2022.11.10. 20:02:15

Kétfaktoros... aha... ez egészen addig jó, míg az ember nem fut bele olyanba, hogy pl. valamiért nem hozzáférhető a 2FA-hoz használt mobilja. És persze ez mindig olyankor történik, amikor a recovery kódok is több száz km-re vannak egy otthoni pendrive-on. Vagy nincs ilyen egyáltalán, lásd pl. az a kib.....tt gúgle, ami sokadjára szopat, hogy nem enged be a postaládámba, mert a mobilom nem elérhető és az egyéb elérhetőségeimre magasról szarik.

Válasz erre

gigabursch 2022.11.11. 07:50:42

A hatodik pont sztorija szerintem féknyúz, de legalább jól hangzik.
Az utolsó is q hihető..

Továbbá nincs ember aki 37 féle jelszót megjegyezzen.

Válasz erre

Mesterséges Geci 2022.11.11. 08:58:57

@gigabursch: a backup egyáltalán nem olcsó dolog. Sajnos nem fake a sztori, simán benne van a hihető kategóriában.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Venus ransomware támadja az egészségügyet

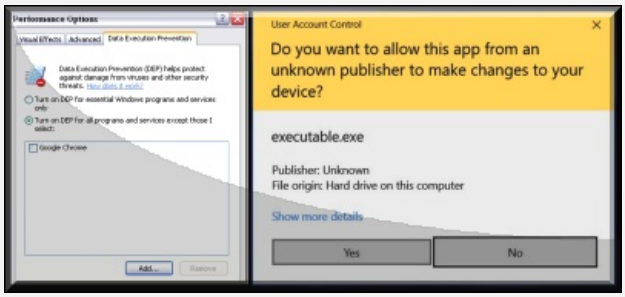
2022. november 17. 12:52 - Csizmazia Darab István [Rambo]

Az Egyesült Államokban hivatalos figyelmeztetést adtak ki, miután a 2022. augusztusában felfedezett **zsarolóvírus számos vállalati rendszert, ezen belül is célzottan kórházakat, egészségügyi létesítményeket támadott meg.**

Ami jellemző erre a kártevőre, hogy Windows gépeket igyekszik megfertőzni, és a nyitott, védetlen RDP (Távoli Asztal Kapcsolat) portján keresztül támad, ami sajnos **gyakorinak nevezhető módszer a zsarolóvírusoknál.**

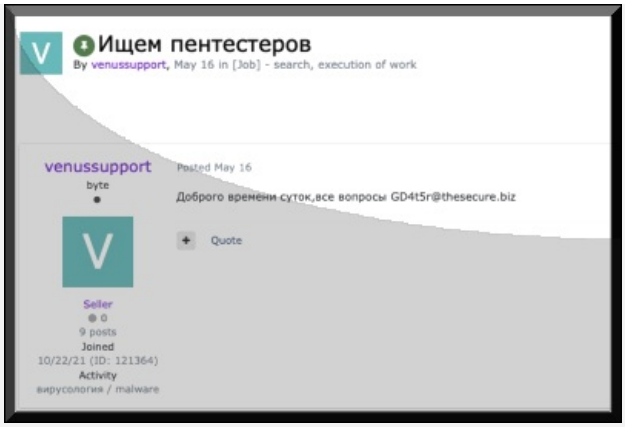
A kártevő hozza a "kötelező köröket": a háttérben megkísérli leállítani az adatbázis és Office alkalmazásokhoz kapcsolódó folyamatokat, **törli az eseménynaplókat és a Shadow Copy másolatokat.**

Valamint **lekapcsolja a kódok engedélyezetlen memóriaterületeken való futtatását felügyelő Data Execution Prevention védelmi technológiát.**



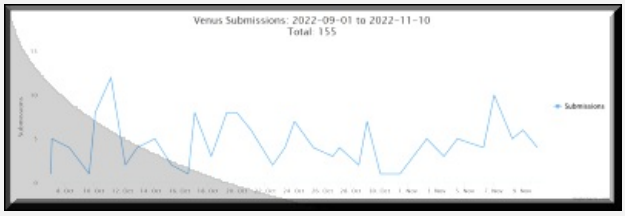
A Venus erős, RSA és AES alapú titkosítást végez, **az elkódolt fájlok végére pedig a ".goodgamer" kiterjesztést illeszti, innen származik a kártevő másik elnevezése (Goodgame).**

A megfigyelések szerint ez **nem a manapság már gyakori RaaS (Ransomware as a Service) üzleti modellt követi, hanem készítői idén május óta a darkneten árulják önálló csomagként**, és nem is tartalmaz hozzáférést nyilvános adatszivárgási webhelyhez, vagy közvetlen kapcsolattartási lehetőséget a Venus üzemeltetőivel.



Sajnos a célzottan kórházak és hasonló intézmények elleni támadások az utóbbi időben nagy mértékben elszaporodtak.

Egy másik vonal, a Quantum ransomware rovására például már több száz hasonló incidenst figyeltek meg az USA-ban.



De korábban mi is beszámoltunk már **több olyan egészségügyi intézményeket ért támadásról, ahol a rendszerek leállása miatt szünetelt az elektronikus kapcsolattartás, és csak személyesen odautazva lehetett leletet átvenni, a kórháznak ideiglenesen vissza kellett állnia a telefon, fax és papíralapú jegyzetelésre, és emellett műtétek maradtak el, valamint bizalmas betegadatok kerültek illetéktelen kezekbe,** a horribilis váltságdíj követelésekről már nem is beszélve.

Szólj hozzá!
Címkék: kórház egészségügy támadás venus intézmény ransomware zsarolóvírus

Ajánlott bejegyzések:


Nem csitulnak a kórházak elleni támadások

A Cerber visszatér


Összeomlás

Közeleg a tél, érzékeny ponton támadnak a zsarolóbandák


Felhasználó, kórház, olajvezeték után egy egész ország

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.

VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Emelkedő ransomware károk

2022. november 21. 12:29 - Csizmazia Darab István [Rambo]

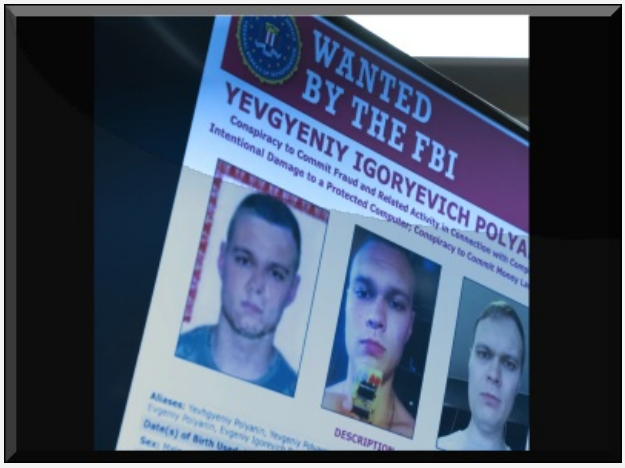
A lassan jó kilenc éve pusztító zsarolóvírusok még várhatóan jó ideig nem tűnnek el életünkből, az okokról pedig már sokszor eltűnődtünk korábban, legutóbb például ebben a posztban. **Az okozott károk mértékéről most friss számok érkeztek.**

Az amerikai bankoknak **1.2 milliárd dolláros kárt okoztak a tavalyi évben a ransomware támadások** - ez szerepel egy friss pénzügyi jelentésben. Ez **188%-os növekedést mutat a korábbi évben tapasztalt értékekhez képest.**

A növekedés több okra is visszavezethető, nyilván **a támadások száma is gyarapodik, de részben annak is betudható**, hogy a hivatalos szervek (pl. Treasury's Office of Foreign Assets Control, OFAC) igyekeztek arra biztatni mindenkit, hogy ne hallgassák el, hanem inkább jelentsék ezeket az eseteket.

Az adott időszakban a bejelentett incidensekben **84 egyedi ransomware-variáns szerepelt, ezek között nagyjából 58%-uk mögött állhat feltételezhetően valamilyen orosz bűnbanda.** Ez abból derül ki, hogy ezek a kártevő változatok orosz nyelvű kódot használtak, kifejezetten úgy voltak kódolva, hogy ne támadjanak célpontokat Oroszországban vagy volt szovjet utód államokban, illetve főleg orosz nyelvű weboldalakon hirdették ezeket.

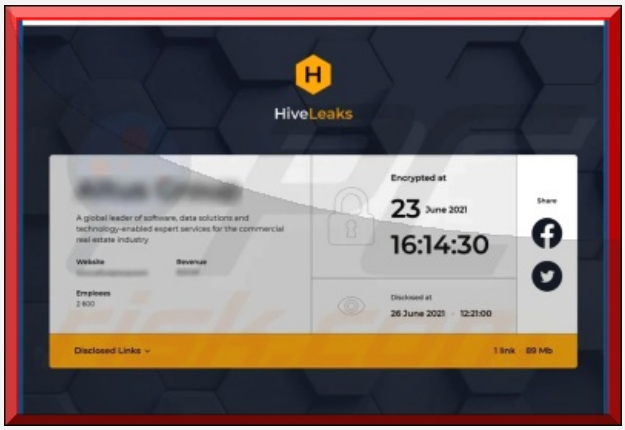
A vizsgált időszakban jelentkezett öt leggyakoribb ransomware-variáns közül négy megfelelt ezen kritériumok legalább egyikének, vagy többnek.



A zsarolóvírusok mezőnyében 2021. nyara óta szereplő Hive is éllovas, akinek Costa Rica is "megvolt". **A Hive csapat ransomware bűnözői világszerte több mint 1,300 vállalatnak okoztak kárt, és az FBI szerint az elmúlt 18**

hónapban mintegy 100 millió dollárnyi váltságdíjat zsaroltak ki áldozataiktól. A csoport komolyan r**ászállt az egészségügyi intézményekre, kórházakra**, és ezeket a kritikus területre mért csapást csak súlyosbította, hogy a titkosítás mellett a szinte már mindenhol alkalmazott doxing is szerepelt.

Ebben **a bizalmas adatok ellopásért és azok nyilvánosságra hozásának elkerüléséért kért váltságdíj sokszor fontosabb szempont,** mint az elkódolt adatok visszanyerés, és a működőképesség, rendelkezésre állás helyreállítása.



A bűnözők a publikálásra a Hiveleaks felületet használják, és ugyancsak **gyakori az a forgatókönyv is, hogy megfelelő védekezés, és megelőzés nélkül a korábbi áldozatok a váltságdíj fizetése után nem sokkal újra megfertőződnek, és újabb zsarolással találják szembe magukat.**

A Hive fő célpontjai az energiavállalatok, az egészségügyi létesítmények, a pénzügyi szolgáltató intézmények és a média vállalatok voltak. **A megelőzés, védekezés témában itt lehet naprakész tippeket, tanácsokat olvasni.**

Szólj hozzá!
Címkék: statisztika fbi váltságdíj ransomware hive zsarolóvírus

Ajánlott bejegyzések:


Durva ransomware statisztikai adatok


Colonial Pipeline után a mindennapi kenyerünk


Kórházprogram


Ransomware a spájzban


Váltságdíjat kínálnak a váltságdíjszedő bandáért

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.

VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Nagy pénz, nagy foci, nagy átverések

2022. november 24. 07:20 - Csizmazia Darab István [Rambo]

A FIFA labdarúgó-világbajnokságra a csalók is készülnek: **hamis jegyek, lottóátverések és más veszélyek is leselkednek a kibertérben a szurkolókra**. Érdemes áttekinteni, hogyan kerülhetjük el, hogy bedőljünk a trükkjeiknek.

Elkezdődött a 2022-es katari FIFA-világbajnokság. Az idei év egyik legfontosabb sporteseménye november 20. és december 18. között több százmillió futballrajongót hoz lázba a világ minden táján. Ahogyan azt korábban már tapasztalhattuk, az online csalók gyakran kihasználják a nagyobb sportesemények körüli felhajtást.

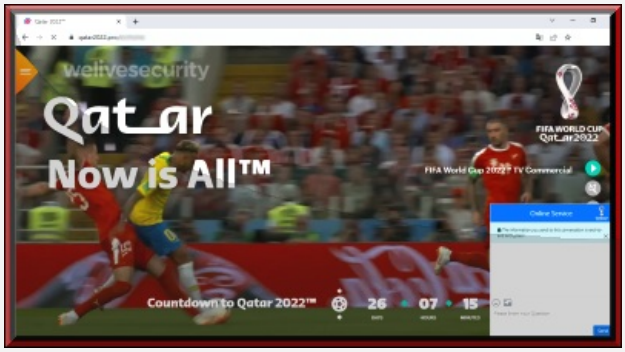
A csalások **egyik jól bevált fajtája, amikor a bűnözők elhitetik az áldozatokkal, hogy készpénzt, jegyet vagy olyan, ellátást is tartalmazó csomagot nyertek, amely személyes részvételt biztosít egy mérkőzésen.** Valódi szándékuk viszont, hogy rávegyék az áldozataikat a személyes adatok átadására, pénz előre utalására vagy rosszindulatú szoftverek letöltésére és telepítésére.

Az **ESET kutatói számos olyan globális adathalász akciót azonosítottak, amelyek megpróbálják elhitetni az emberekkel, hogy állítólag kisorsolták őket.** A "nyeremény" átvételéhez pedig nem kell mást tenniük a célpontoknak, mint kitölteni néhány üres mezőt egy űrlapon, és megadniuk a teljes nevüket, születési dátumukat és telefonszámukat.

Az e-mailes mellékletként érkezett példához hasonlóan a nyereményről szóló értesítés tartalmazhatja egy állítólagos kapcsolattartó nevét, aki segíthet a nyeremény átvételében. Ez a személy egy bizonyos ponton azzal keresi fel az áldozatot, hogy **mielőtt ténylegesen megkaphatná a nyereményét, fizessen be előzetesen valamilyen adót vagy díjat.** Amint az utalás megtörtént, a támadók elérték céljukat: a pénz mellett személyes adatok birtokába jutottak, amelyekkel később további csalásokat hajthatnak végre vagy eladhatják az adatokat más kiberbűnözőknek.

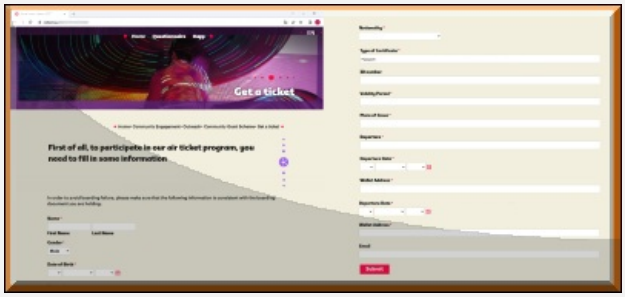
Hamis lottónyeremény-értesítés, amely a világbajnokságot használja csalinak. Az átverés egyik árulkodó jele lehet, hogy általános üdvözléssel indít. **Általában az e-mail tárgya sem túl kreatív, mint például a "Katari világbajnokság 2022 lottónyertes", a "Katar 2022 FIFA lottónyertes" vagy a "Gratulálunk, Ön megnyerte a 2022-es katari labdarúgó-világbajnokság megalottóját".** Másfelől viszont ezek a címek felkelthetik az ember figyelmét és reményt ébreszthetnek.

Megfigyelhető egy másik adathalász e-mailben, hogy a levélbe ágyazott képen egy "Kattintson ide" gomb szerepel, amely azt ígéri, hogy egy klikk után már igényelhetjük is jegyünket a sportesemény nyitómérkőzésére. **A valóság ezzel szemben az, hogy a kattintás után egy olyan felületre kerülünk, ahol személyes adatokat kérnek vagy elindul a rosszindulatú tartalom letöltése a számítógépünkre vagy a mobiltelefonunkra.**



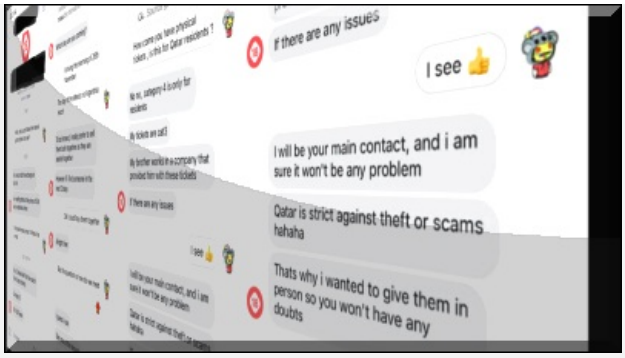
Az adathalász csalások egy meggyőzőbb és veszélyesebb változata, ha olyan rosszindulatú hasonmás weboldalra tévedünk, amely valódinak tűnik. **Az ide vezető linkeket spam e-mailekben, hamis közösségi profilokon keresztül vagy fórum bejegyzésekben terjesztik.**

Függetlenül attól, hogy ezek a weboldalak valós felületeket másolnak le vagy sem, céljuk hasonló: a személyes és pénzügyi adatok, bejelentkezési adatok, illetve egyéb **érzékeny információk megszerzése, illetve kártékony szoftverek telepítése az áldozatok eszközeire.**



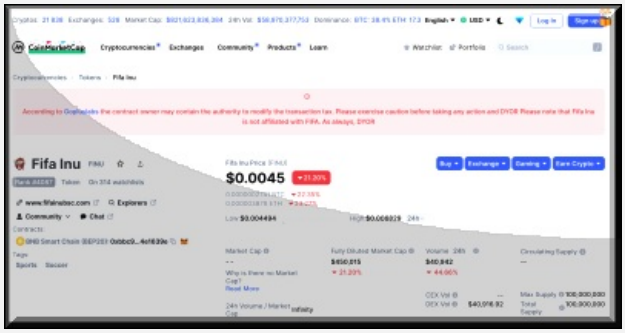
Az alábbi weboldal a labdarúgó-világbajnokság hivatalos weboldalának adja ki magát, ehhez valódi URL-t, a https://www.qatar2022.qa/ címet utánozva, **a különbség mindössze annyi, hogy a csalók a .pro-t használják a domain végén (angolul top-level domain, azaz legfelső szintű tartomány).** A kiberbűnözők egy külön "portált" is létrehoztak, amelyen keresztül az emberek látszólag megvásárolhatják jegyeiket, először azonban személyes adatokat kérnek, amelyekkel visszaélhetnek vagy azonnal eladhatják más csalóknak.

A közelmúltban **többen is beszámoltak arról, hogy a "FIFA képviselői" tárgysorú e-mailben megkeresték őket, és ebben eladó jegyeket kínáltak számukra**. A Redditen pedig felhasználók a hamis jegyeket árusító csalókkal folytatott üzenetváltásokat osztották meg.



Amennyiben szeretnénk jegyet vásárolni valamelyik mérkőzésre, jobb óvatosnak lennünk. **A 2022-es katari tornára kizárólag digitálisan tudunk jegyet váltani, ez alól az egyetlen kivétel az utolsó pillanatban megvásárolt jegy, amelyhez csak személyesen, a katari fővárosban, Dohában található két kijelölt irodában lehet hozzájutni.**

A jegyek engedély nélküli viszonteladása Katarban tilos, a büntetések pedig súlyosak lehetnek. A belépők továbbértékesítésének és megvásárlásának egyetlen legális módja a FIFA hivatalos jegyértékesítési platformján keresztül lehetséges.



Nemrégiben megjelent egy FIFA Inu nevű kriptovaluta, amelyet rövid időn belül sokan átverésnek tituláltak, mivel értéke a folyamatos emelkedést követően hirtelen bezuhant. Az alapítók ezeket a vádakat visszautasították. A pénzünk befektetésekor azonban ajánlatos mindig óvatosnak lennünk. Előfordulhat, hogy a **WhatsApp üzenetküldőn kapunk olyan üzenetet, amelyekben nyereményekkel, ajándékokkal hitegetnek hamis közösségi média profilok felhasználásával, de az üzenetek rosszindulatú hirdetéseket is tartalmazhatnak, amelyek átirányítanak egy csalók által működtetett weboldalra.**

Ezért jobb odafigyelni a gyanús hirdetésekre, kéretlen üzenetekre, nehogy bedőljünk az ilyen átveréseknek. Amint azt már más esetekben is láttuk, a csalók gyakran használják arra a nagyobb eseményeket, aktuális témákat, vészhelyzeteket, hogy ezekre hivatkozva építsék fel a csalásaikat, és világszerte tömeges mennyiségben küldjenek ki átveréssel kapcsolatos leveleket, üzeneteket.

Mit tehetünk az átverések elkerülésére? Az alábbi egyszerű tanácsok észben tartásával nagy eséllyel el tudjuk kerülni az átveréseket:

- Nem nyerhetünk a lottón, ha nem is játszottunk. Ha valaki ennek az ellenkezőjéről próbál meggyőzni minket, nagy valószínűséggel átverésről van szó.

- Ne fizessünk előre azért, hogy valamilyen nyereményt megkapjunk. Amennyiben előleget kérnek tőlünk valamiért cserébe, csak a pénzünket akarják megszerezni.

- Legyünk óvatosak az adathalász támadásokkal. Ne kattintsunk e-mailekben vagy más üzenetekben található linkekre vagy mellékletekre, hacsak nem vagyunk biztosak abban, hogy azok nem jelentenek veszélyt. Különösen igaz ez akkor, ha kéretlen üzenetekről van szó, amelyek a személyes, illetve banki adatainkat kérik.

- Hasonlóképpen vigyázzunk a csaló weboldalakkal. A gyakori nyelvtani hibák, gyanús URL-címek, hiányzó vagy érvénytelen biztonsági tanúsítványok intő jelek lehetnek, főleg, ha az adott weboldal pénzt és/vagy személyes adatot kér tőlünk.

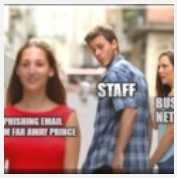
- Ne adjuk ki személyes adatainkat – azokat csalásra használhatják fel vagy eladhatják a dark weben.

- Használjunk erős, egyedi jelszavakat, és kétfaktoros hitelesítést minden fontos fiókunk esetében, amely ezt lehetővé teszi. Különösen, ha a profil érzékeny adatokat tartalmaz. Ezzel csökkentjük annak az esélyét, hogy hackerek könnyedén feltörjék fiókjainkat.

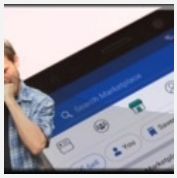
- Használjunk megbízható, többrétegű biztonsági szoftvert, amely rendelkezik adathalászat elleni védelemmel.

Szólj hozzá!
Címkék: foci vb futball csalás tippek átverés katar világbajnokság megelőzés tanácsok adathalászat

Ajánlott bejegyzések:

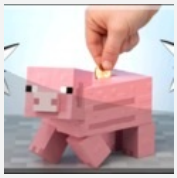


10 gyakori ok, amiért bedőlünk a csalásoknak


Átverések az online piactéren


Fiatal vagy? Ezekre az online csalásokra figyelj!

Az egyik COVID-19, a másik egy híján 20


A csalások már a spájzban vannak

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.

VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Még gyengébb a jelszavad

2022. november 29. 10:38 - Csizmazia Darab István [Rambo]

A NordPass közzétette **2022-es év leggyakoribb jelszavainak listáját, és aki ezen a téren valamiféle látványos javulásra számított, az jól elbukta a feltett zsetonjait.** A jelszó higiéniai állapota látszólag már évek óta változatlan.

Ismétlés a tudás jó édes anyukája - mintha csak ez lenne a mottója a top tízes listára került jelszavaknak, a korábbi évek helyezettjei, az **egymás után következő számok, betűk, azonos karakterek ismételgetése, és hasonlóan gyenge, még szótár nélkül is másodpercek alatt törhető jelszavakat láthatunk az élmezőnyben.**

Néhány itt látható tétel **esetleg azért szerepel előkelő helyen, mert valamilyen netre kapcsolódó eszköznek alapértelmezett**, és a tulajdonos által meg nem változtatott jelszava.

A Nordpass felmérésben 30 ország felhasználóinak adatait vizsgálták. **Különösen a csak számokból álló jelszavaknál szembeötlő a lustaság: "1111111111", "121212", "888888" és hasonlók arról árulkodnak, hogy a jelszóválasztást felesleges nyűgnél érzi az illető, és letudni akarja, nem pedig megoldani. Ugyancsak fantáziátlanságról tanúskodik az "querty", "usr", "football", "monkey", "batman", "oscar" és hasonlóan primitív, rövid jelszavak, amelyek feltöréséhez kevesebb, mint egy másodperc is elég a támadóknak.**

A top 10-es helyezettekről **külön szinte nem is érdemes beszélni, hiszen ez mind a 2019-es, 2020-as helyezettek kicsit megkevert** sorrendjét idézi, vagyis sajnos nem látható e helyütt semmiféle hozzáállásbeli javulás.

Aki mégis abban gondolkodik, hogy a fentieknél erősebb jelszavakat használna, az kalkuláljon **legalább 12 vagy hosszabb karaktersorozatokban, kombinálja a számokat, a kis- és nagybetűket, valamint a speciális karaktereket, vagy használjon erre a célra jelszógenerátort.**

Hasznos szokás emellett a fontos helyeken a rendszeres jelszócsere, a kétfaktoros autentikáció valamilyen SMS, token, biometrikus vagy hitelesítőalkalmazással kiszolgált módja, legyen a jelszó egyedi, valamint figyeljünk a szolgáltatók esetleges jelszócserére figyelmeztető üzeneteire is, ne hagyjuk ezeket figyelmen kívül.

Len	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

A jelszószéf alkalmazás használata ebben a feladatban sok mindent képes számunkra megkönnyíteni, **a jelszavak megjegyzése, előhívása, generálása, offline vagy online tárolása egyaránt megoldható a segítségével.**

6 komment
Címkék: statisztika jelszó primitív password feltörés worst nordpass

Ajánlott bejegyzések:

C mint CEO, P mint password

Nem életrevalók

Gyenge, gyengébb, leggyengébb

Az elveszett jelszavak fosztogatói

Esemény utáni teendők

Kommentek:

Mesterséges Geci 2022.11.30. 11:48:21

István, te értesz ehhez mélyebben?
Bennem minden ilyen írás kapcsán ott motoszkál a kisördög: készítek egy virtuális gépet valami primitívnek mondott jelszóval, aztán szerezzék meg ezt a jelszót!

Tehát nem a rendszer feltörése lenne a lényeg, hanem a jelszó megszerzése.

Elképzelés: a jelszavakat erős kódolással, hosszú+random stringgel "sózva" tárolom, egyirányú kódolással természetesen.
A sózás miatt a szivárványtáblás módszer kiesik.
A login x próbálkozás után letiltja a usert pár perc-pár óra időre.
O.K., DoS-olható a rendszer, de a jelszavak nagyjából biztonságban vannak, nem?

Válasz erre

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2022.11.30. 18:06:37

Sokféle dolog kavarhat be a biztonságnak, még a fenti esetben is, pl. ha kémprogramot telepítenek a gépedre, mindent lehet látni, fizikai hozzáférés kizárárása, stb. A tesztelgetés persze ettől függetlenül jó játék.

Amit én tennék: hosszú egyedi jelszó (>12 kar) emiatt:
www.hivesystems.io/blog/are-your-passwords-in-the-green

Mindenhol használnék 2FA/MFA-t, és a fontos helyeken rendszeresen cserélném, a jelszó széf pedig segíthet. Aki paranoiás, annak érdemes ebben online helyett offline tárolni, hogy semmiképpen ne kerüljön ki semmi.

A brute force elleni védelem nélkülözhetetlen feature, mégis sok helyen hiányzik, pl. az Apple Fappening incidensénél is hiányzott, emiatt a támadók korlátlan alkalommal próbálgathatták a lopott jelszavakat.

Válasz erre

Mesterséges Geci 2022.11.30. 20:14:34

@Csizmazia Darab István [Rambo]: azt hiszem, félreértesz. :)
Pusztán annyi a kérdés, hogy az egyszerű, mondjuk csupa kisbetűből álló, rövid jelszavak egy normálisan konfigurált szerver esetében jelenthetnek-e nagyobb veszélyt, mint a bonyolult, megjegyezhetetlen passwordök?
A keyloggeres verzió más téma, az ellen a nagyon hosszú és bonyolult jelszó sem véd.
Valahogy egyre olyan érzésem van, hogy a szolgáltatók a saját felelősségüket próbálják a userre hárítani amikor megkövetelik a komplex jelszavakat. (Egyik nagybankunk húsz év alatt nem jutott el odáig, hogy engedjen a jelszóban spec. karaktereket, mert azbelső netbanknál annyira rettegtek a SQL injection jellegű támadásoktól :D)

Válasz erre

Mesterséges Geci 2022.12.01. 09:42:18

@Csizmazia Darab István [Rambo]:
www.bleepingcomputer.com/news/security/lastpass-says-hackers-accessed-customer-data-in-new-breach/ - lazán, de kapcsolódik. :(

Válasz erre

Head Honcho 2022.12.01. 21:37:10

@Mesterséges Geci: Ezzel a LastPass-szal már nem ez az első probléma. Jól tudom?

Válasz erre

Mesterséges Geci 2022.12.01. 22:42:20

@Head Honcho: nem tudom, nem használok ilyesmit. Idén ez volt a második, de most az elsőből származó információkat használták fel, ha jól értem.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.

VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

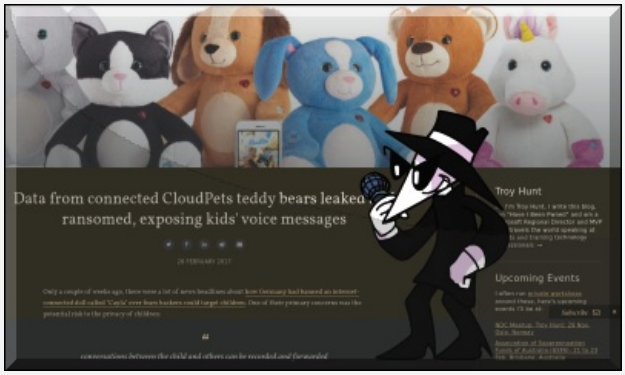
accountz

Belépés
Regisztráció

Okoskodás: okos-e az okosjáték?

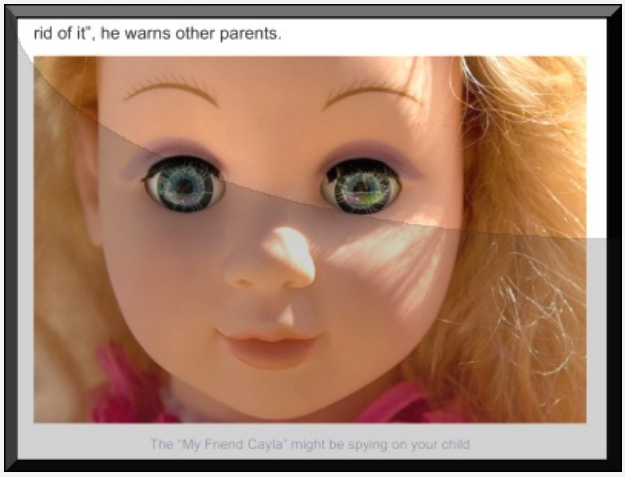
2022. december 01. 10:29 - Csizmazia Darab István [Rambo]

Az **okosjátékok globális piacán két számjegyű százalékos növekedés várható, és 2027-re ez meghaladhatja a 24 milliárd dollárt**. Amikor viszont a hálózati kapcsolat, az adatok és a számítástechnika találkozik, adatvédelmi és biztonsági aggályok is felmerülhetnek, így **a karácsonyi vásárlások kezdetekor érdemes előzetesen is megvizsgálni az ebben rejlő veszélyeket.**



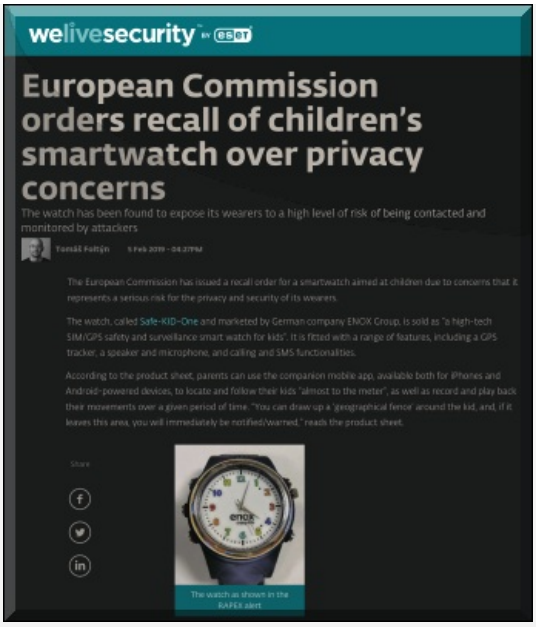
Az intelligens pacemakerektől az okosórákig, a hangasszisztensektől az okos kapucsengőkig a technológia segít életünket egészségesebbé, kényelmesebbé, és szórakoztatóbbá tenni - ez a dolgok internete (Internet of Things - IoT), mely egyúttal lehetővé teszi a gyártók számára, hogy új, izgalmas játékokat dobjanak piacra.

Valószínűleg mindannyiunkban felmerült már a gondolat, hogy beszerzünk gyermekeink számára egy okosjátékot, mely ösztönzi a tanulást és fejleszti a kreativitást. Az ESET kiberbiztonsági szakértői szerint **az adatok és a magánélet védelme (plusz a gyermekek biztonsága!) érdekében érdemes némi előzetes kutatást végeznünk, mielőtt kiválasztjuk a kívánt eszközt.**



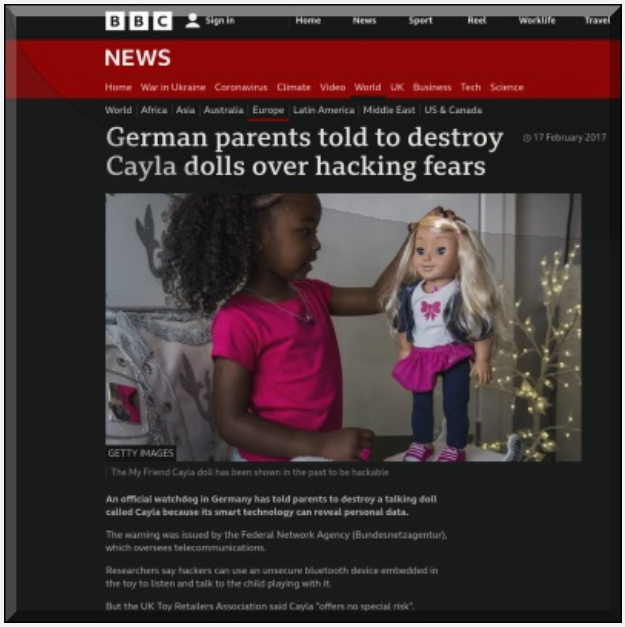
Okosjátékok már évek óta léteznek. Mint minden IoT-eszköz esetében, itt is az a cél, hogy a világhálóra való csatlakoztathatóság és az intelligens eszköz segítségével még magával ragadóbb és interaktívabb élményt nyújtsanak. Ezek a játékok **olyan eszközöket használhatnak, amelyekben mikrofonok és kamerák vannak így alkalmasak videó és hang továbbítására; beépített hangszórók és képernyők, amelyek hangot és videót közvetítenek a gyermekeknek.**

Számos eszköz tartalmaz Bluetooth lehetőséget, amely által a játékot egy mobil alkalmazással kapcsolhatjuk össze, vagy internetkapcsolat az otthoni Wi-Fi routerrel.



Ezek az okoseszközök merőben eltérnek azoktól a játékoktól, amelyekkel legtöbben gyermekkorunkban töltöttük az időt. Képesek arra, hogy az interakcióval bevonzzák a legkisebbeket is, és újabb és újabb funkciókat tudnak elsajátítani az internetről letölthető kiegészítők révén. Sajnos az IT biztonsági szakértők úgy tapasztalják, hogy számos esetben **a gyártók a piacért folyó versenyben spórolnak a biztonsági intézkedéseken.**

Ennek eredményeként **termékeik szoftversebezhetőségeket tartalmazhatnak illetve engedélyezhetik a nem biztonságos jelszavak használatát. Előfordulhat, hogy adatokat rögzítenek, és azokat titokban elküldik egy harmadik félnek, vagy érzékeny adatokat kérnek a szülőktől, amelyeket nem biztonságosan tárolnak.**



Korábban több olyan eset is történt, amikor az okosjátékok veszélyessé váltak:

- **A Fisher Price okos játékmackót 3-8 éves gyermekek számára tervezték, mint "egy interaktív tanuló barátot, amely beszél, figyel, megjegyzi, amit mondanak neki, sőt, válaszol is, ha megszólítják".** A csatlakoztatott okostelefon-alkalmazás hibája azonban lehetővé tette a hackerek számára, hogy jogosulatlanul hozzáférjenek a felhasználói adatokhoz.

- **A CloudPets segítségével a szülők és gyermekeik hangüzeneteket oszthattak meg egymással egy plüssállaton keresztül.** A jelszavak, e-mail címek és üzenetek tárolására használt háttértárat viszont nem biztonságosan tárolták a felhőben. Az adatállomány nyilvánosan, jelszóvédelem nélkül volt elérhető az interneten.

- **A My Friend Cayla egy intelligens technológiával rendelkező játékbaba, amelynek a gyermekek kérdéseket tehetnek fel, és választ is kapnak az internet segítségével.** A kutatók azonban felfedeztek egy biztonsági rést, amely lehetővé teszi a hackerek számára, hogy a babán keresztül kémkedjenek a gyermekek és a szülők után. **Mindez arra késztette a német távközlési felügyeletet, hogy az adatvédelmi aggályok miatt a játék kidobására szólítsa fel a szülőket. Hasonló helyzet állt elő 2019-ben a Safe-KID-One nevű okosóra esetében is.**

Az NCC Group biztonsági cég 2019. karácsonya előtt próbaképpen megvizsgált hét okosjátékot, amelyeknél összesen 20 különböző problémát talált. Ezek közül kettőt magas kockázatúnak, hármat pedig közepes kockázatúnak minősített. A leggyakrabban az alábbi problémákkal találkoztak:

- Nincs titkosítva a fiók létrehozása és a bejelentkezés, így a felhasználónevek és jelszavak nyilvánosságra kerülhetnek.

- Nem lehetséges már meglévő felhasználó fiókot törölni, megszüntetni.

- Gyenge jelszószabályzat, azaz a felhasználók könnyen kitalálható bejelentkezési adatokat választhatnak.

- Homályos adatvédelmi irányelvek, cookie-k és más nyomon követésre alkalmas információk passzív gyűjtése.

- Az eszköz párosítása egy másik játékkal vagy alkalmazással gyakran mindenfajta hitelesítés nélkül történt Bluetoothon keresztül. Ez lehetővé teszi, hogy a hatótávolságon belül bárki sértő vagy felkavaró tartalmakat közvetítsen, illetve manipulatív üzeneteket küldjön a gyermeknek.

- Bizonyos esetekben (például a walkie talkie-n keresztül) egy idegen is képes lehet kommunikálni a környéken lévő gyerekekkel azáltal, hogy egy ugyanolyan játékot vásárol magának.

- Extrém esetben a támadók képesek lehetnek az okosotthonok meghackelésére egy audiofunkciókkal rendelkező intelligens játék (vagy akár robotporszívó) feltörése által, hogy hangüzenetet küldenek az otthoni hangasszisztenseknek (például: "Alexa, nyisd ki a bejárati ajtót").

Hogyan lehetséges minimalizálni az okosjátékokban rejlő adatvédelmi és biztonsági kockázatokat? Mivel az okosjátékok bizonyos fokú biztonsági és adatvédelmi kockázatot jelentenek, **érdemes megfontolni az alábbi gyakorlati tanácsokat ajándékvásárláskor:**

- Tájékozódjunk vásárlás előtt: Ellenőrizzük, hogy találunk-e negatív hangvételű hírt vagy kutatást az adott eszköz biztonságával kapcsolatban.

- Legyen biztonságos az a routerünk. Ez az eszköz az otthoni hálózat központi eleme, és az összes internetre

csatlakoztatott eszközünkkel kommunikál, ezért érdemes ezt erős jelszóval védeni, és a legfrissebb biztonsági hibajavításokkal ellátni.

- Kapcsoljuk ki az eszközöket: Ha nem használjuk a készüléket, a kockázatok minimalizálása érdekében kapcsoljuk ki.

- Ismerjük meg alaposan a játékok működését: Egyúttal gondoskodjunk arról, hogy a kisebb gyermekek csak felügyelet mellett használják az eszközöket.

- Ellenőrizzük a frissítéseket: Ha a játék képes frissítéseket letölteni, győződjünk meg róla, hogy az már a firmware (elektronikai eszközök működését biztosító belső program) legújabb verzióját futtatja.

- Válasszunk biztonságos kapcsolatot: Gondoskodjunk arról, hogy az eszközök a Bluetoothon keresztül történő párosításkor hitelesítést kérnek, és wifin pedig titkosított kommunikációt folytatnak az otthoni routerrel. Erről netes keresésekkel tudunk előzetesen tájékozódni, ha elérhető a részletes felhasználó útmutató, a tapasztalatokat megosztó fórumok oldalain a felhasználók hozzászólásaiból, illetve biztonságtechnikai szakcikkekből.

- Legyünk tisztában azzal, hogy az eszközök pontosan hol tárolják az adatokat, és megbízható híre van-e a játékot forgalmazó vállalatnak a biztonság terén.

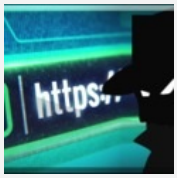
- Használjunk erős és egyedi jelszavakat a fiókok létrehozásakor.

- Csökkentsük minimálisra a megosztott adatok mennyiségét: Ez csökkenti a kockázati kitettséget, ha az adatokat ellopják és/vagy a vállalatot megtámadják.

Az okosjátékok valóban jó eszközei lehetnek a tanulásnak és a szórakozásnak. De csak akkor, ha gondoskodtunk arról, hogy elektronikus eszközeink mindig védve legyenek.

Szólj hozzá!
Címkék: játék vásárlás biztonság gyerek karácsony gyermek tippek tanácsok tájékozódás sebezhetőség sérülékenység iot okoseszköz

Ajánlott bejegyzések:


Böngészés - kockázatok és mellékhatások


Gyermek + okosóra = biztonság?


Amazónia veszélyes ragadozói ;-)


7 tipp a mobilunk védelméhez


Nagy pénz, nagy foci, nagy átverések

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Antivírusblog
245 követő

Oldal követése Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

Nem csitulnak a kórházak elleni támadások

2022. december 06. 11:47 - Csizmazia Darab István [Rambo]

Ahogy egy korábbi bejegyzésben szerepelt, az USA-ban jelentősen megszaporodtak célzott ransomware támadások, amelyek **kifejezetten egészségügyi intézmények hálózataiban tettek kárt**. Ám mindeközben Európa sem lehet nyugodt, ezúttal egy francia kórház kényszerült hasonló okokból leállásra.

A párizsi André-Mignot kórház december 3-án szenvedett el egy zsarolóvírus támadást helyi idő szerint szombat 21 órakor, amelynek hatására megbénult a számítógépes rendszere és telefonhálózata. **A leállások miatt arra kényszerültek, hogy műtéteket, kemoterápiás kezeléseket halasszanak el, illetve irányítsanak át más kórházakba.**

Emellett az újszülött- és intenzív osztályokról betegeket kellett átszállítaniuk más közeli egészségügyi intézményekbe. A vészhelyzetben Francois Braun egészségügyi miniszter szerint teljesen át kellett szervezni az intenzív osztály működtetését.

A kibertámadás közelebbi részletei egyelőre nem ismertek, ám annyi már kiderült, hogy valóban váltságdíj követeléssel álltak elő az ismeretlen támadók.

A 700 ágyas kórház vezetősége úgy nyilatkozott, nem áll szándékunkban kifizetni azt, ehelyett igyekeznek elkülöníteni a fertőzött gépeket, és az ANSSI (francia nemzetbiztonsági és védelmi hatóság) segítségével kivizsgálni az esetet.

A támadásnak esetleg köze lehet egy korábbi másik, szeptemberi Corbeil-Essones beli kórház támadáshoz is, ahol a LockBit 3.0 csoport 10 millió dolláros váltságdíjat követelt, és a kórház a számítógépes rendszerek leállása miatt kénytelen volt visszaállni a papíralapú működésre.

Azt egyelőre nem tudni, hogy az André-Mignot kórház esetében történt-e adatlopás, ami viszont

megnehezítené a helyzetüket, hiszen már nem csak mentésből való helyreállítás lenne a tét, hanem az ellopott bizalmas adatok nyilvánossá tételével való fenyegetés is.

Amint az már közismert, sajnos **több bűnözői csoport is intenzíven támadja világszerte az egészségügyi intézményeket, így a Hive és a Venus banda is rengeteg áldozat elleni incidensért felelős.**

Az FBI szerint a Hive csapat az elmúlt 18 hónapban mintegy 100 millió dollárnyi váltságdíjat zsarolt ki az áldozataiktól.

Szólj hozzá!
Címkék: leállás franciaország kórház egészségügy támadás egészségügyi váltságdíj intézmény ransomware zsarolóvírus

Ajánlott bejegyzések:

Venus ransomware támadja az egészségügyet

A Cerber visszatér

Közeleg a tél, érzékeny ponton támadnak a zsarolóbandák


Apa kezdődik!

Kórházprogram

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

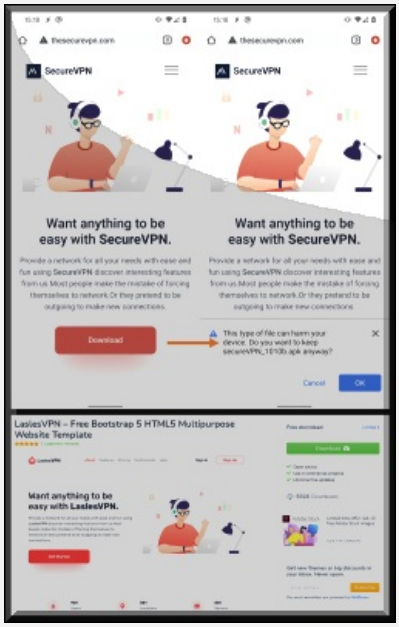
VPN appok Androidra vagy mégsem?

2022. december 08. 10:56 - Csizmazia Darab István [Rambo]

Nem mindegy, hogy mit és honnan töltünk le - mondja az ősi mondás, és **amióta csak létezik net, letöltés, telepítés, mindvégig voltak, vannak és lesznek olyan próbálkozások, amelyekkel igyekeznek becsapni a felhasználókat.**

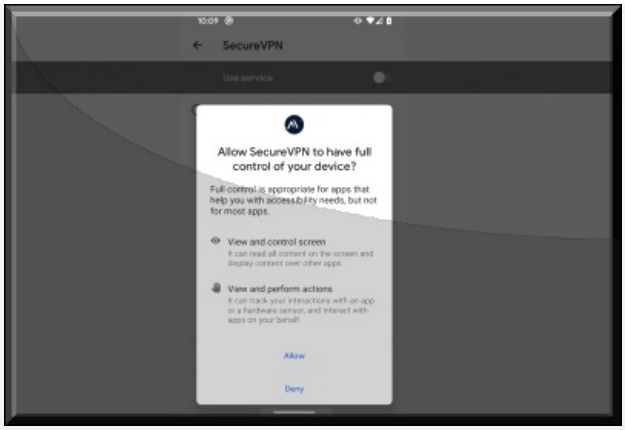
Régi, de releváns posztunk volt ebben a témában a "Hogyan szúrjuk ki a gyanús Android appokat?" évekkel korábbi bejegyzés. Nos az ilyen jellegű átverések azóta is velünk vannak, ezúttal két VPN applikáció nevével éltek vissza.

Az ESET kutatói azonosították azt a rosszindulatú kampányt, amelynek során a SoftVPN és az OpenVPN nevében kínáltak letöltésre kétes applikációkat. Az akció a részletek alapján a Bahamut elnevezésű APT csoport tevékenységére vezethető vissza.



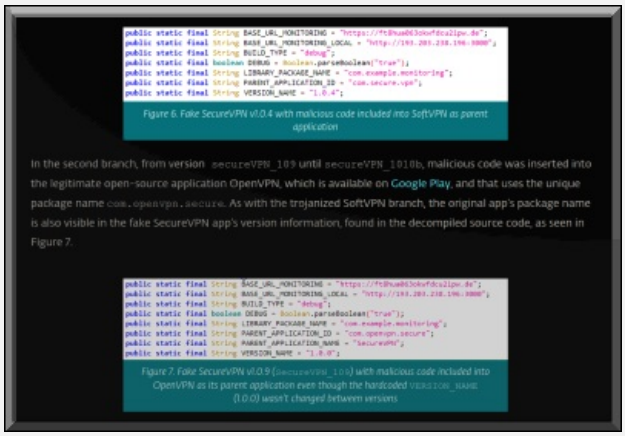
A megfigyelések szerint 2022. januárja óta terjesztik ezeket a hamis alkalmazásokat egy SecureVPN "hasonmás" weboldalán, ami ráadásul egy ingyenes weblap sablonnal operál. A szakértőknek a trójai alkalmazás több, különböző változatát is sikerült beazonosítaniuk. **A manipulált trójai alkalmazások fő célja érzékeny adatok ellopása, valamint az áldozatok üzenetküldő alkalmazásainak lehallgatása, ezek iránti kémkedés volt.**

A hamis alkalmazások nem kerültek fel a Google Play hivatalos piacterére, azokat **csak a fenti weboldal segítségével terjesztették - a gyanú szerint kifejezetten célzottan, szűk körben előre gondosan kiválasztott áldozatoknak, közel-keleti és ázsiai magánszemélyeknek és szervezeteknek küldött testreszabott üzenetekkel, külön aktiválási procedúrával is kiegészítve.**



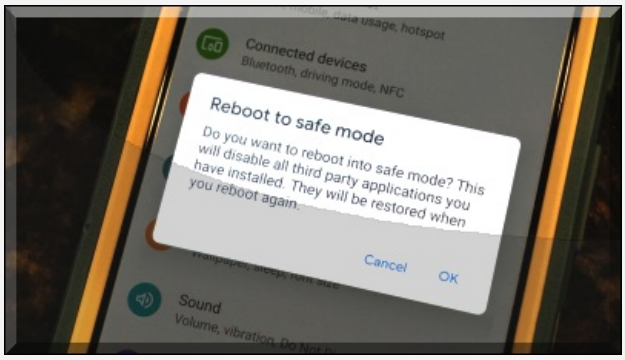
A rosszindulatú alkalmazás működésbe lépve **képes begyűjteni a bizalmas személyes adatokat, például a névjegyeket, az SMS-üzeneteket, a hívásnaplókat, az eszköz fizikai helyzetét, a telepített alkalmazások listáját, részletes eszközinformációt (internetkapcsolat típusa, IMEI, IP, SIM sorozatszám), a külső tárolón lévő fájlok listáját, valamint a rögzített telefonhívásokat.**

Aktívan kémkedhet a népszerű üzenetküldő alkalmazásokon keresztül váltott csevegőüzenetek után is, beleértve a Signal, a Viber, a WhatsApp, a WeChat, a Telegram és a Facebook Messenger alkalmazást is. Az adatok kiszivárogtatása a korábbi FedEx/FluBot vírusnál is ismert módon, **az akadálymentesítési szolgáltatásokkal elfedve rejtetten történik.**



Bár szemlátomást nem vagyunk közel-keleti vagy ázsiai kiemelt célpontok, ám **a gyanús mobil appok elkerülésével kapcsolatban általánosságban azért érdemes alaposan megnézni még azt is, amit a hivatalos piactérről telepítünk.** Időnként ugyanis ott is hemzsegnek a húzónevekkel visszaélve a hasonmás, vagy hasonmás nevű gyanús programok.

De a fenti konkrét esetnél, ahol külön weboldalról kínálták a rosszindulatú alkalmazásokat - akárcsak a tavaly márciusi FedEx/FluBot incidensnél - ott már sokkal inkább **a naprakész vírusvédelem és emellett a megfontolt, gyanakvó, biztonságtudatos hozzáállás adja kezünkben a megfelelő muníciót a védekezéshez, megelőzéshez.**



Ha gyaníthatóan már fertőzött a telefonunk, miközben a futó folyamatok között bármilyen gyanús szervizt találunk, és **ha a hagyományos uninstall segítségével nem sikerül megszabadulni a fertőzéstől, akkor Safe módban kell újraindítani az eszközt, mert ebben csak a gyári alkalmazások élednek fel.**

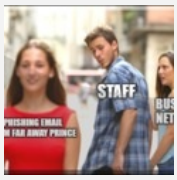
Ekkor pedig már lehetséges lesz bármilyen kártékony, "Accesibility services" által fogott-rejtett ravasz program eltávolítása.

Szólj hozzá!
Címkék: alkalmazás csalás átverés openvpn trójai android app services applikáció accesibility ESET welivesecurity.com bahamut softvpn

Ajánlott bejegyzések:

[Megérkezett a csomagja - vagy mégsem?]

[Igazgató-e vagy?]



[10 gyakori ok, amiért bedőlünk a csalásoknak]

[Mit tehetünk a kriptovaluta csalások ellen?]

[Ingyenes Omikron teszt vagy mégsem?]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

A csalások már a spájzban vannak

2022. december 12. 11:41 - Csizmazia Darab István [Rambo]

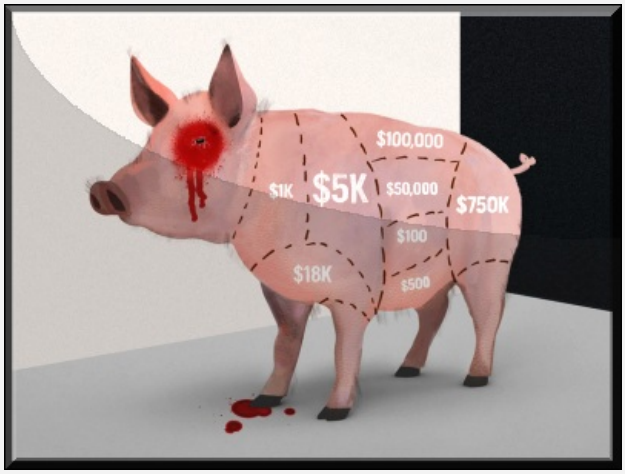
Az átverési kísérletek folyamatosan itt vannak velünk, és ki jobban, **ki kevésbé felkészült ezekkel szemben. Két különféle mostanában futó csalási módszert is bemutatunk**, amelyek elég sok áldozatot szednek.

Az első inkább angol nyelvterületen gyakori, és **már becenevet is adtak a folyamatnak: disznó hentelés. Ez egy olyan manipulációt takar, amelyben ismeretlenek arra vesznek rá embereket, hogy a megtakarításaikat hamis portálokon olyan kripto befektetésekbe fizessék, amelyek állítólag igen nyereségesek**, ám a valóságban nem hogy garantált nyereség nincs, de az áldozatok elveszítik a teljes pénzüket.

Az FBI szerint 2021-ben 429 millió dollárnyi pénzt sikerült így megszerezni a csalóknak, és a trükk egyre népszerűbbé válik a bűnözők körében. Nemrégiben pedig Ausztráliában tartóztattak le egy olyan bandát, amely 100 millió dollárnyi pénzt lopott el ezzel a forgatókönyvvel.

Az elkövetők **kombinálják a már jól ismert romantikus csalást a régebb óta jelenlevő befektetési csalással, és elsősorban a Whatsapp, Tinder és egyéb közösségi vagy társkereső alkalmazásokon tűnnek fel valamilyen vonzó személy profilképével.**

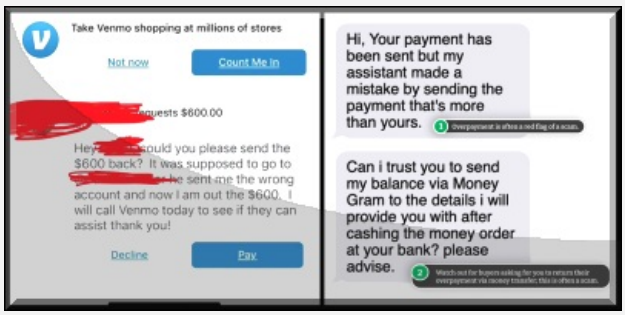
Ahelyett, hogy azonnal nagy összeget kérnének előre, a csalók óvatosak, és csak **lassan csepegtetve dolgoznak** azon, hogy meggyőzzék az ismerkedni vágyó partnert, hogy az általuk javasolt, nem-hivatalos kereskedelmi platformokra irányítsák őket.



Miután kiépítették a bizalmat, jön valamifajta sürgetés, vagy pszichológiai nyomásgyakorlás, hogy az áldozatok nagyobb

összeget helyezzenek el ide. Itt még az is bevett gyakorlat, hogy **egy kezdeti, kisebb összegű "próba befektetésnek" hazudott befizetést egy állítólagos hozammal kiegészítve visszaadnak, hogy ezzel serkentsék őket nagyobb tétben való invesztícióra.** Ám ha valaki már betolt ebbe egy jelentős összeget, hamar csalódnia kell.

Eleinte még azzal hitegetik őket, hogy a befektetés "felszabadítása" egy külön pluszban fizetendő díj vagy adó ellenében hajtható csak végre, **ám nem sokkal ezután egyszerűen nyomtalanul eltűnnek a csalók.** Sosem szabad befektetési tanácsokat elfogadni ismeretlenektől, akár kripto, akár hagyományos területről legyen szó. A netes csalások témájában érdemes megnézni a Tinder Svindler, illetve emellett az Álörökösnő álarca mögött című Netflixes sorozatokat, sokat lehet tanulni más kárából.



A másik átverés is egyre gyakoribb, itt az internetes csalók egy viszonylag új módját választották a pénzszerzésnek. Lopott kártyaadatokat használva egyenleget töltenek fel valamilyen ismert fizetésközvetítőnél nyitott számlájukra - például PayPal, ApplePay, Venmo, Zelle - majd jellemzően 500 dollárnyi pénzt olyan random ismeretlen felhasználóknak utalnak, akiknek kiszivárgott a számlaszáma, és elérhetősége.

Ezután kapcsolatba lépnek vele, és **arra hivatkozva, hogy téves utalás történt, arra kérik az áldozatot, hogy utalják vissza a pénzt egy általuk megadott másik fiókba.**

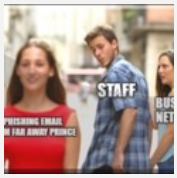
Ha valaki ezt óvatlanul megteszi, elbukja az így elutalt pénzét, ugyanis némi késéssel ugyan, de a lopott kártyaadatok miatt az eredeti tranzakció összegét a bank automatikusan is leemeli, és a csalás miatt visszavonást hajt végre, így az ugyanekkora pluszban intézett kézi utalás összege már végérvényesen elveszik az ügyfél számára. Mivel itt az áldozat megtévesztve ugyan, de mégis saját akaratából "önként" végezte el az átutalást, így **erre sajnos általában már semmilyen banki garancia, jóvátétel vagy kártérítési jogorvoslat nem vonatkozik.**

A jótanács ilyenkor az lehet, hogy **soha ne küldjünk vissza pénzt ilyen esetben**. Az indokolatlanul érkező utalások esetében **azonnal lépjünk kapcsolatba a bankunkkal** és az ügyfélszolgálattól kérjen segítséget, és az ő utasításait megfogadva rendezzük a helyzetet.

Szólj hozzá!
Címkék: befektetés csalás átverés randi megelőzés romantikus védekezés kriptovaluta

Ajánlott bejegyzések:

Mit tehetünk a kriptovaluta



10 gyakori ok, amiért


Fiatal vagy? Ezekre az

Modern románc,

Nagy pénz, nagy foci,

csalások ellen? | bedőlünk a csalásoknak | online csalásokra figyelj! | holdfény és tánc | nagy átverések

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Antivírusblog
245 követő

Oldal követése Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.

VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Kis- és középvállalkozások adatvédelmi incidensei

2022. december 15. 08:52 - Csizmazia Darab István [Rambo]

A KKV-k több százezer eurós kárt szenvedtek el adatvédelmi incidensek miatt az ESET friss felmérése szerint.

Az adatok a 2022-es "SMB Digital Security Sentiment Report" című jelentéséből származnak. Ehhez **1212 IT-biztonsági vezetőt kérdeztek meg** az Egyesült Királyságban, az Egyesült Államokban, Kanadában, Franciaországban, Németországban, Spanyolországban, Olaszországban, Lengyelországban, Svédországban, Csehországban, Hollandiában, Dániában, Norvégiában és Finnországban.

A válaszadók 25 és 500 fő közötti alkalmazottat foglalkoztató, különböző szintű IT-biztonsági fejlettséggel és méretű költségvetéssel rendelkező vállalkozásokat képviseltek.

A jelentés adatai szerint **a kkv-k több, mint kétharmada szenvedett el valamilyen adatbiztonsági incidenst az elmúlt 12 hónapban, amelynek átlagos becsült költsége csaknem 220 ezer euró (közel 90 millió forint) volt**. A kis- és középvállalkozások **29%-a azonban ennek ellenére az adatvesztést tartja** a legnagyobb kockázatnak.

Bár a vezetők **aggódnak egy esetleges kibertámadás és annak következményei miatt, a megkérdezett vállalkozások 70%-a elismerte, hogy a munkarendben bekövetkezett változások (például a hibrid munkavégzés) ellenére mégsem fordítottak kellő összeget és figyelmet a kiberbiztonságra.**

Az ESET legutóbbi vírusriportjának adatai szerint **2022-ben eddig 20 százalékkal több fenyegetést észleltek a tavalyi év azonos időszakához képest.** A megkérdezett vállalkozások 83%-a szerint a kiberháború nagyon is valós fenyegetés, amely bárkit érinthet, ez pedig arra utal, hogy az egyre növekvő kockázatok jelentősen befolyásolják a kkv-k hangulatát, állapotát.

Az észak-amerikai és európai kis- és középvállalkozások **74 százaléka véli úgy, hogy jobban ki van téve a kibertámadásoknak, mint maguk a nagyvállalatok.**

A válaszadók az előttük álló 12 hónapra vonatkozóan leginkább az alábbi kiberbiztonsági kockázatok miatt aggódnak:

- Rosszindulatú szoftverek (összesen 70% tartja reális veszélynek)
- Webes támadások (összesen 67% említette)
- Zsarolóvírus (összesen 65%)
- Harmadik fél által okozott biztonsági problémák (64%)
- Elosztott szolgáltatásmegtagadási (DDoS) támadások (60%)
- Távoli asztali protokoll (RDP) támadások (összesen 60%)

Mindezek alapján nem meglepő, hogy **a kkv-k általános értékelése a kibertámadásokkal szembeni saját ellenálló képességüket illetően alacsony: a válaszadók mindössze 48%-a állította**, hogy közepesen vagy nagyon megbízik saját védelmi felkészültségében. Érdemes megjegyezni, hogy a skandináv országokban megkérdezettek sokkal kevésbé (32%) bíztak saját védelmi-megelőző képességükben, mint Európa más részén és Észak-Amerikában (49-49%).

A felméréséből kiderült továbbá, hogy olyan jelentős globális kihívások ellenére, mint az ukrajnai háború vagy a koronavírus-járvány után is folytatódó home-office, távmunka, **a kkv-k szerint mégis leginkább az alkalmazottak kibertudatosságának hiánya (43%) növeli meg jelentősen a támadások kockázatát.**

A vállalatok szerint további **kiemelt kockázati tényező a nemzetállami támogatású kiberbűnözés (37%), a partneri/beszállítói rendszerek sebezhetősége (34%), a hibrid munkarend (32%) illetve a távoli távoli asztali protokoll szabályozatlan használata (31%).** A kisvállalkozásoknak mindenképpen tisztában kell lenniük azzal, hogy a kiberbűnözők folyamatosan és aktívan támadják a kisebb, gyengébben védett cégeket, vállalkozásokat, beszállító partnereket is.

Bár azt látni, hogy a híradások szalagcímeiben jobbára nagy neves cégek szerepelnek a számítógépes támadások áldozataiként, ennek egyik oka, hogy a kisebb vállalkozásokat ért incidensek egy része észrevétlen marad. **A legnagyobb kockázatot az alkalmazottakkal szembeni célzott támadások jelentik, például az üzleti levélnek álcázott zsarolóvírusok, a céges levelezés feltörése (Business E-mail Compromise, BEC), valamint kiemelt rizikó még az adathalászat is.**

Arról, hogy **mit tehetnének a cégek, hogy ne essenek hackerek áldozatául, az ESET szakértői a most induló IT-biztonsági podcastjükben is beszélnek, sőt számos konkrét támadási esetet is bemutatnak. A "Hackfelmetszők - Veled is megtörténhet!" podcast epizódjaiból** megtudhatjuk, hogy a hazai KKV-k és az otthoni felhasználók mennyire érintettek az online veszélyekben, és hogy mekkora üzleti rizikót jelent, ha nem fordítunk kellő figyelmet a céges eszközeink, hálózatunk védelmére.

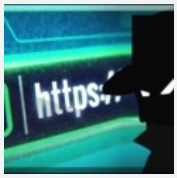
Már elérhető a podcast első adása, amelyből kiderül, hogy kik állnak a hackertámadások mögött, mik az indítékaik, mekkora károkat okozhatnak és egyáltalán, hogyan tudnak bejutni a gépeinkre, a céges hálózatokba? **A podcast az alábbi linken érhető el.**
https://www.eset.com/hu/digitalis-biztonsag/podcast/

Szólj hozzá!
Címkék: statisztika biztonság podcast felmérés kkv cégek eset vállalati cégvezetők kibertámadás

Ajánlott bejegyzések:


Oroszország lett a fő kibercélpont


FinTech: az előretörés ideje



Böngészés - kockázatok és mellékhatások


Durva ransomware statisztikai adatok


A kibertér is hadszíntér

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

Üzleti e-mail hamisítás

2022. december 20. 12:53 - Csizmazia Darab István [Rambo]

A kissé suta magyar elnevezés a **BEC, azaz Business Email Compromise módszert jelöli. Ez egy olyan csalási forma, amelynél egy szervezet levelezését feltörve az abból megismert bizalmas adatokból, levélváltásokból testre szabott célzott adathalász támadások indíthatóak**.

Itt megszemélyesítve a kommunikációban résztvevő felek egyikét arra veszik rá az áldozatokat, hogy valamilyen nagy összegű, gyors átutalást hajtsanak végre. Az **átverés alapulhat azon, hogy a legitim üzleti partner nevében az állítják, egy másik, megváltozott számlaszámra utaljanak, vagy egy korábbi partner nevében nagy volumenű megrendelést adnak le, amit később aztán nem rendeznek.**

De az is gyakran előfordul, hogy valamilyen kémprogramot tartalmazó linket, mellékletet küldenek, vagy egy adathalász oldal segítségével további céges vagy banki azonosítókat szereznek meg a támadók.

Ez a fajta megtévesztéses (social engineering) csalás világszerte szedi az áldozatait, és a felkészült bűnözők jól előkészítve, nagy leleménnyel és pontosan időzítve hajtják végre az ilyen akciókat.

Például 2019-ben a DeepVoice hangszintetizálás segítségével ismeretlen elkövetők egy brit energetikai cég német igazgatója hangján, az ő nevében felhívták a brit igazgatót, és **egy azonnali, de bizalmas 220 ezer euró összegű pénzátutalást kértek egy magyar alvállalkozó magyar bankszámlájára, amiről csak utólag derült ki, hogy csalás volt.**

De a közelmúltban is történt hasonló hazai eset, pár hónapja a Magyar Vízilabda-szövetség (MVLSZ) levelezését törték fel, és **a megismert adatok birtokában egy aktuálisan utalandó Európa-bajnokság szállásköltségeit, valamint**

a Világliga európai selejtezőinek montenegrói hotelfoglalását - összesen 120 ezer euró körüli összeget kértek egy állítólagos "új" számlára átutalni.

Itt ez az átverés több, mint 50 millió forintos kárt okozott a szövetségnek.

Egy friss hír szerint pedig **az FBI is figyelmezteti a kisebb amerikai élelmiszergyártó cégeket, mert ezen a területen megsokasodtak a hasonló csalások. Hamis megrendelések érkeztek korábbi valós ügyfelek nevében, illetve hamis számlaszámokat megadva tömegesen** próbálkoznak csalók az élelmiszereket forgalmazó vállalkozásoknál. **Egy 2021-es statisztika azt mutatja, hogy a céges levelezés meghamisításával végrehajtott csalások gigantikus, 2.4 milliárd dollárnyi hasznot** hajtott a bűnözőknek.

Nagyon fontos tehát, hogy **mind a vevők, mint a beszállítók alaposan ellenőrizzenek minden egyes tranzakciót, és képezzék ki az alkalmazottaikat a csalások korai felismerésére.**

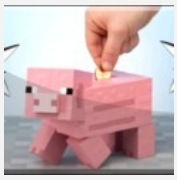
Szólj hozzá!
Címkék: social business üzleti e-mail csalás átverés céges hamisítás engineering bec compromise

Ajánlott bejegyzések:


Mai szavunk pedig: megszemélyesítéses csalás


Viva la Revolut


Magyar Posta csomagunk jött - vagy mégsem?


A csalások már a spájzban vannak


VPN appok Androidra vagy mégsem?

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.

VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Mai szavunk pedig: biztonsági fásultság

2022. december 22. 08:39 - Csizmazia Darab István [Rambo]

Az IT biztonsági részleget gyakran "a nemetmondás osztályának" tartják, és nem nehéz belátni ennek okait. A **fokozódó kockázatok, növekvő támadási felületek és a gyorsan fejlődő kiberbűnözés világában** a biztonsági szakemberek érthető módon igyekeznek minimalizálni a károkat, amelyeket az alkalmazottak okozhatnak. Elvégre elég egyetlen rossz kattintás ahhoz, hogy egy zsarolóvírus áldozataivá váljunk.

Viszont ha az alkalmazottakra túl nagy teher nehezedik a kiberbiztonság terén, nem várt módon reagálhatnak, ami növelheti a szervezet kitettségét. Ezt nevezzük biztonsági fásultságnak, ami meggondolatlan, hirtelen döntésekhez vezethet – ez éppen az ellenkezője annak, amit az informatikai szakemberek szeretnének.

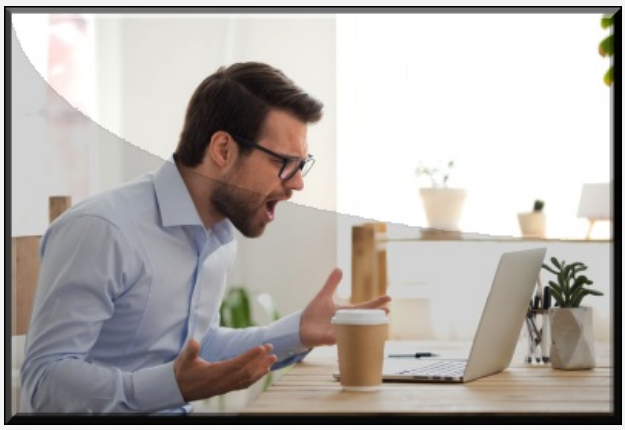
Az ESET szakértői szerint, hogy ez ne történhessen meg, a kiberbiztonságnak zökkenőmentesen kell működnie, korlátozni kell a felhasználói döntések számát, valamint egészséges egyensúlyt kell teremteni a védelem és a hatékonyság között a hibrid munka világában.

Mi az a biztonsági fásultság és mekkora veszélyeket rejt? Az **emberekre gyakran úgy tekintenek, mint a leggyengébb láncszemre a vállalati biztonsági láncban.** Emiatt fordítanak kiemelt figyelmet az IT csapatok arra, hogy csökkentsék az alkalmazottak által jelentett kockázatot. Ebben egyrészről igazuk is van, hiszen egy kutatás szerint 2020-ban a vállalatok 60 százaléka 21-nél is több dolgozói incidenst észlelt, **addig 2021-ben már a vállalatok 67 százaléka észlelt ugyanennyit.**

A károk helyreállítása pedig átlagosan több mint 15 millió dollárba került. Amennyiben viszont a munkavállalók rendszeresen munkahelyi biztonsági figyelmeztetéseket kapnak, szigorúak a szabályok, ráadásul a szabadidejükben is adatvédelmi jogsértésekről és fenyegetésekről szóló hírekkel találkoznak, a kimerültség jelei mutatkozhatnak. A

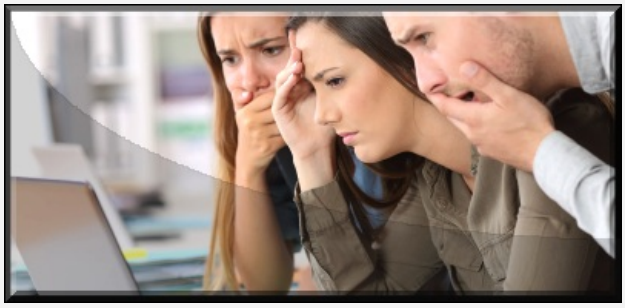
biztonsági fásultságot a tehetetlenség és a kontroll elvesztésének érzése jellemzi.

Az alkalmazottak számára mindez **annyira nyomasztóvá válhat, hogy elzárkózva a vállalati szabályoktól a saját útjukat kezdik járni. Úgy érezhetik, hogy bármit tesznek, a biztonsági incidensek mindenképpen be fognak következni, ezért figyelmen kívül hagyják a biztonsági riasztásokat.**



Ez pedig sajnos sokkal gyakrabban előfordul, mint gondolnánk. Egy 2018-as tanulmány kimutatta, hogy az EMEA (Európa, Közel-Kelet és Afrika) régióban dolgozók több, mint fele (55 százalék) nem törődik rendszeresen a kiberbiztonsággal, közel egyötödük (17 százalék) pedig egyáltalán nem is aggódik miatta.

A tapasztalatok alapján **a fiatalabb munkavállalók még inkább hajlamosak arra, hogy fásulttá-elutasítóvá váljanak** a túlzott biztonsági elvárások miatt. Sajnos mindez komoly destabilizáló hatással lehet a vállalati biztonságra.



A biztonsági fásultság legfőbb jelei, ha az alkalmazottak:

- Úgy döntenek, hogy kíváncsiságból mégis rákattintanak az adathalász e-mailekben szereplő linkekre vagy megnyitják a csatolmányokat.

- Gyenge jelszavakat használnak, vagy több fiókban is ugyanazokat a gyenge hitelesítő adatokat alkalmazzák. Egy nemrég készült kutatás szerint a munkavállalók 43 százaléka megosztja másokkal a belépési adatait, sőt, hajlandó másokra bízni a feladatait, hogy elkerülje a bejelentkezéssel járó stresszt.

- VPN használata nélkül jelentkeznek be vállalati hálózatokba, mivel használata egyes szervezeteknél korlátozott lehet.

- Útközben nem biztonságos, **nyilvános Wi-Fi hotspotokat használnak**, hogy onnan bejelentkezzenek az érzékeny adatokat tartalmazó vállalati fiókokba.

- Nem frissítik rendszeresen eszközeiket, számítógépeiket. Az EY friss tanulmánya szerint a Z és Y generációs munkavállalók az idősebb kollégáknál jóval nagyobb valószínűséggel hagyják figyelmen kívül, és halasztják el a kötelező rendszerjavításokat.

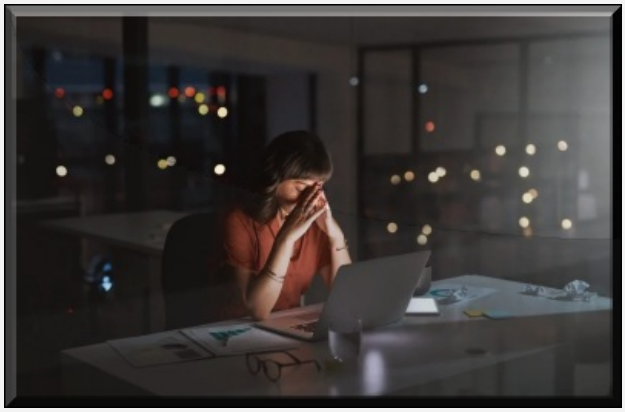
- Nem jelzik azonnal az incidenseket a feletteseiknek vagy az informatikusoknak. Az EY-tanulmányból az is kiderül, hogy a munkavállalók közel egyötöde (16 százaléka) először inkább megpróbálja maga kezelni a feltételezett biztonsági problémát, minthogy értesítene valakit arról.

- A munkaeszközöket privát célokra használják, beleérve az internetes letöltéseket, a játékokat és az online vásárlást. Egy felmérés szerint az alkalmazottak fele személyes tulajdonának tekinti munkaeszközét.

- Megpróbálják kijátszani a biztonsági szabályokat. A 18-24 év közötti irodai dolgozók 31%-a próbálta már megkerülni a biztonsági előírásokat, ezt mutatta ki egy vizsgálat.

És hogyan küzdhető le a biztonsági fásultság? A 2020-ban tapasztalt, tömeges otthoni munkavégzésre való gyors átállásra sok vállalat kapkodva reagált. Az IT-csapatok úgy próbálták csökkenteni a kockázati kitettséget, hogy új, szigorú szabályokat róttak az alkalmazottakra.

Most, hogy a hibrid munkavégzés kezd általánossá válni, **lehetőség nyílik arra, hogy felülvizsgáljuk ezeket a kezdeti szabályokat, különös tekintettel a biztonsági fásultság megelőzésére.**



- Hallgassuk meg a végfelhasználókat, hogy jobban megértsük, miként befolyásolják a biztonsági előírások a munkafolyamatokat és zavarják-e a produktivitást. Próbáljunk meg olyan szabályzatot létrehozni, amely egyensúlyban tartja az alkalmazottak elvárásait és az igényt a kiberkockázat minimalizálására, és valóban betartható.

- Korlátozzuk a döntések számát, amelyeket a felhasználóknak kell meghozniuk. Ez jelenthet automatikus szoftverfrissítést, a biztonsági programok távoli telepítését, illetve a laptopok és más elektronikai eszközök kezelését. Futtassunk háttérben futó észlelési és válasz-szolgáltatásokat, amely megakadályozza a hálózati védelemre irányuló támadásokat.

- Fektessünk hangsúlyt a bejelentkezések fokozott védelmére jelszómenedzserekkel, biometrikus alapú többtényezős hitelesítés és egyszeri bejelentkezési módszer (SSO) használatával.

- Csökkentsük a biztonsági üzenetek számát, amelyeket a felhasználóknak küldünk. A kevesebb több, és nagyobb

figyelmet kap.

- Tegyük szórakoztatóbbá a biztonsági tudatosságról szóló tréningeket rövidebb (10-15 perces), valósághű szimulációkat és játékokat tartalmazó oktatások révén.

Ahhoz, hogy a vállalati védelmi rendszerek megfelelően működjenek, **olyan kultúrát kell teremteni, amelyben minden alkalmazott megérti, hogy ő maga mennyire fontos szerepet játszik a szervezet biztonságának megőrzésében**, és amelyből mindenki proaktívan kiveszi a részét.

Egy ilyen kultúra kiépítése persze időbe telhet. Mindez viszont a biztonsági fásultság okainak megértésével és kezelésével kezdődik, az eredmény pedig megéri.

Szólj hozzá!
Címkék: biztonság védelem emberi megelőzés fásultság tényező hibázás

Ajánlott bejegyzések:


7 tipp a mobilunk védelméhez


10 gyakori IT biztonsági hiba


Iskolák a kiberbűnözők célkeresztjében


10 alaplépés a biztonsághoz


Drágán add a bankkártyád!

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!

Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.
VVV 20.
VVV 21.
VVV 22.
VVV 23.
VVV 24.
VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

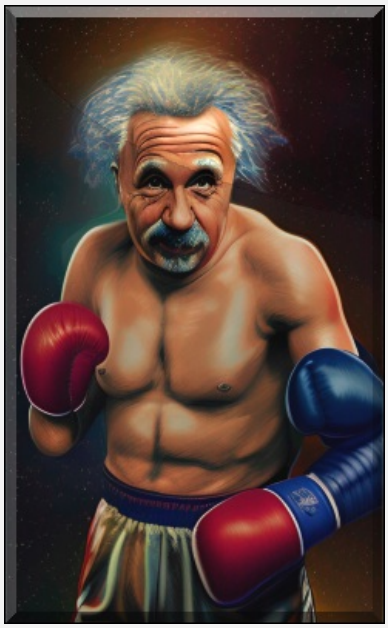
Kellemes Karácsonyi Ünnepeket!

2022. december 26. 16:43 - Csizmazia Darab István [Rambo]

Boldog Karácsonyi Ünnepeket kívánunk blogunk minden látogatójának!

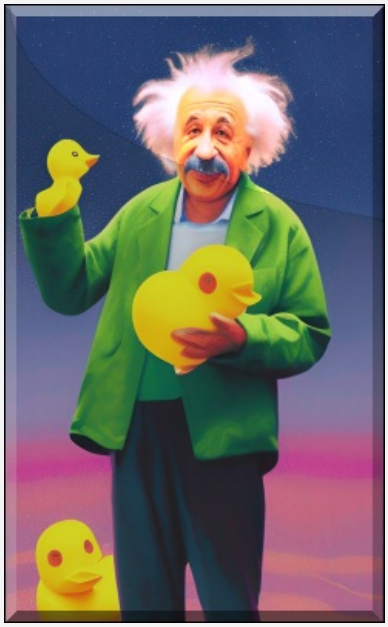
A fenti képekben az a különleges, hogy ezeket **egy olyan AI oldal alkotta, ahol bármilyen szabad szöveget begépelve legenerálódik egy kép**. Különféle stílusok közül lehet válogatni: festészeti irányzatok, street-art, graffiti, stb. Ezek természetesen a "Xmas" szóra érkeztek.

Akkor vágjunk bele valami trükkösebbe: "Einstein boxing..."

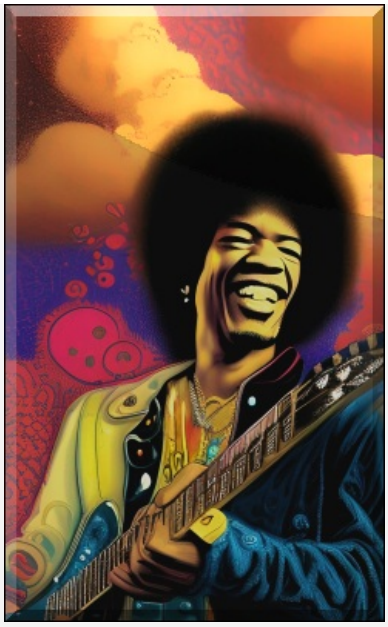


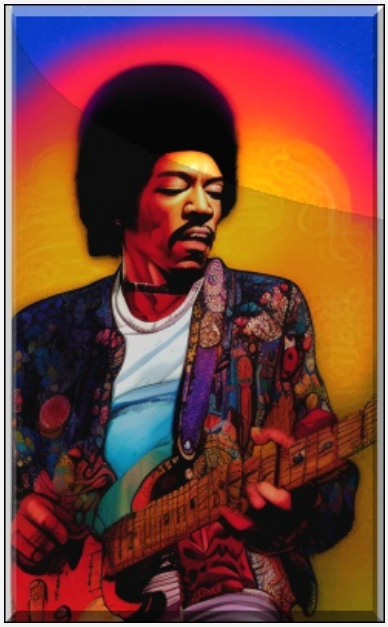
Sima Einstein variációk, keleti stlusban... **Jópofaság, hogy azonos beállításnál akárhányszor lehet generálni, mindig más, különböző végeredménnyel...**

"Einstein with rubber duck"...



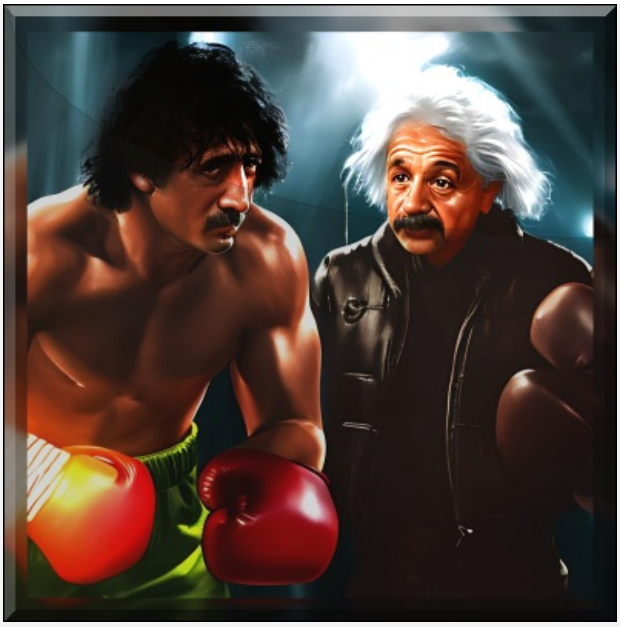
De frankó képeket alkot Jimmy Hendrix nevére is, remélhetőleg még sokan tudják, ki volt ő...

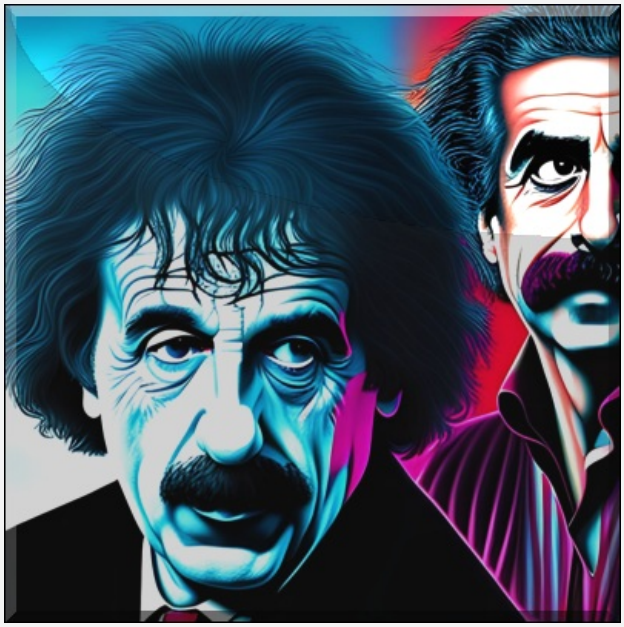




Pár órát eltöltve ezekkel látszanak bizonyos korlátok. Például a tudása kicsit wikipédiás. Ha mondjuk Foxi Maxi (régi amerikai rajzfilm) képeket kérünk tőle, simán kutyás képeket mutat a "Huckleberry Hound" kereső szavakra, **de a mémeket sem igazán ismeri:** "Hide the pain Harold"-ra sem mutat nekünk tetsző találatot, helyette fájós lábú embereket ad ki a Dream.AI. De klasszikus hírességeket ismer, jöhet Johnny Depp, Keanu Reeves, és társai.

Jöjjenek az érdekesebb darabok: "Stallone with Eistein", "Rocky with Einstein", "Frank Zappa with Einstein".





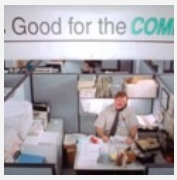
Az alábbi weboldalon találtunk egy gyűjteményt, ahol jó pár ilyen például FOTOR és a regisztráció mentes DREAM.AI típusú izgalmas lehetőséget szedtek össze, de **kommentelni ér, mit tud az AI most 2022. végén: milyen cikket ír, hogy retusál fényképet, tud-e minőségi munkát vagy látványos művészi teljesítményt mutatni, ki ismer más ütősebb cuccokat.**

Szólj hozzá!
Címkék: karácsony xmas boldog 2022.

Ajánlott bejegyzések:


Kellemes Karácsonyi Ünnepeket!

Vírusmentes Boldog Új Évet 2022.



Karácsonyi vásárlás biztonságosabban

Vírusmentes Boldog Új Évet 2023.


Okoskodás: okos-e az okosjáték?

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Antivírusblog
245 követő

Oldal követése Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

- RSS 2.0
- bejegyzések, kommentek

Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

Összeomlás

2022. december 28. 11:42 - Csizmazia Darab István [Rambo]

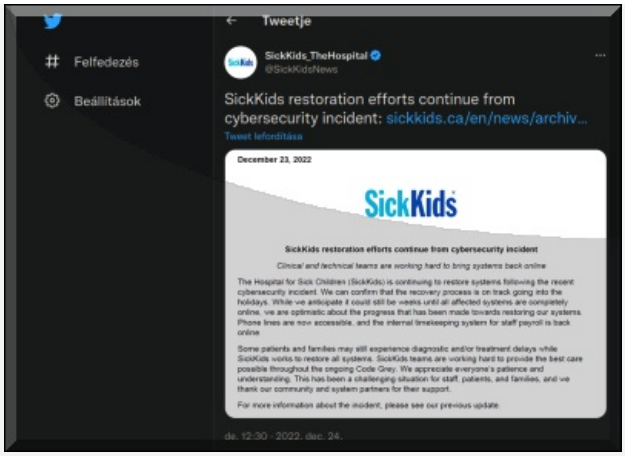
Megint egy kórház küzd a zsarolóvírussal, **ezúttal egy kanadai gyermekgyógyász központot** ért támadás. Ám az ilyenkor szokásos felszínes megállapításokhoz képest - miszerint e-mail helyett mindenki faxol, telefonál, és papírra ír - **sokkal nagyobb a romboló hatása az ilyen jellegű kórházi ransomware incidensnek.**

Nyilván a kommunikáció is megszenvedi a fenti módon, de az a jobbik eset, ha csak részlegesen vagy rövid ideig áll le a betegellátás. **A Torontói Egyetemhez tartozó kórházban még december 18-án kezdődött a pusztítás**, amely a számítógépes hálózatot támadta, ahol a weboldal, a telefonközpont és a belső rendszerek egy része vált azonnal működésképtelenné.

December 23-án egy Twitter bejegyzésben megerősítették a problémát, és a **hivatalos közleményükben hetekre tették azt az időt, mire reményeik szerint helyreállhat a normális működés.** Itt jön képbe tehát a kiesés, a rendelkezésre állás csorbulása. Sajnos **gyakori eset, hogy ilyenkor a betegeket át kell irányítani más intézményekbe, és kemoterápiás kezelések, tervezett műtétek tucatjai maradhatnak el.**

Az információ áramlás leállása az intézményen belül már önmagában is egy komoly csapás, mert így **az orvosok nem férnek hozzá a labor és egyéb képalkotó rendszerek eredményeihez, korábbi belső diagnosztikai jelentésekhez. Ugyanez a helyzet, ha valaki kívülről szeretne laboreredményeket megkapni, a szokásos gyors, kényelmes elektronikus út helyett személyesen autózhat ezekért akár több száz kilométert is.**

De ezen felül **minden más ügyviteli, üzemeltetési munka is leállhat**, vagy sokkal nehézkesebben történik, legyen az a személyzet fizetésének folyósítása, a kötelező jelentések időben történő rendszeres leadása, vagy a számlák, szolgáltatások, közművek külső felek felé történő fizetése, épületvezérlés, és hasonlók. Konkrét váltságdíj követelésről jelenleg nincsenek információk, **a hatóságok bevonásával folyamatosan zajlik a nyomozás és a kárelhárítás.**



Bár **korábban előfordult, hogy egy iskolai vagy kórházi intézmény ransomware támadását az elkövetők sajnálatos véletlennek minősítették**, hiszen esetünkben egy gyermekkórházat (SickKids) célba venni abszolút erkölcstelen tett, ám az FBI nyilatkozataiban azt látni, **sajnos egyáltalán nem példa nélküli a dolog.**

Korábban például iráni bűnözők a bostoni gyermekkórházat bénították le egy hasonló, eléggé el nem ítélhető akcióval. **Korábban mi is írtuk, hogy egyes csoportok kifejezetten egészségügyi intézmények hálózataiban tesznek kárt.**

Állítólag betegadatok itt nem kerültek veszélybe, de ezt nyilván majd végső értékelésnél lehet majd pontosan tudni.

Azoknál az eseteknél, ahol doxing, vagyis adatlopás is történik, súlyosabb a helyzet. Egyrészt fennáll a nyilvánosságra hozatallal való közvetlen zsarolás, másfelől az illetéktelenül megszerzett adatokat eladhatják, vagy a későbbiekben célzott, testre szabott további támadásokban használhatják fel azokat.

Betegnek lenni sosem jó, de egy ransomware által éppen betámadott kórházban betegnek lenni talán még ennél is rosszabb lehet.

Szólj hozzá!
Címkék: kórház kanada gyermekkórház ransomware zsarolóvírus sickkids

Ajánlott bejegyzések:

[Nem csitulnak a kórházak elleni támadások]

[Venus ransomware támadja az egészségügyet]

[Kórházprogram]

[Netwalker tag menni 6 év börtön]

[A Cerber visszatér]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

[Tweets by @antivirusblog]

Facebook

Antivírusblog
245 követő

Oldal követése Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Biztonságos bankolás
- Deliága Éva gyermekpszichológus
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.

VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

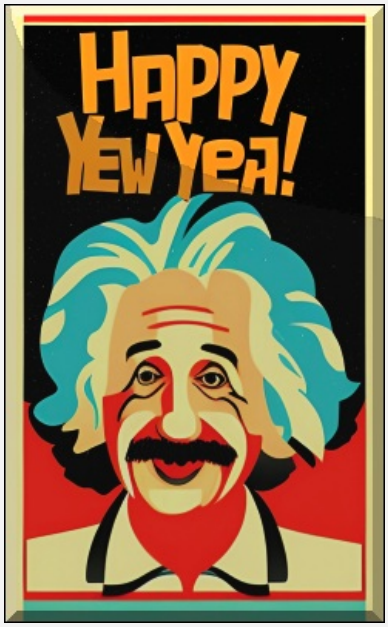
accountz

Belépés
Regisztráció

Vírusmentes Boldog Új Évet 2023.

2022. december 30. 19:18 - Csizmazia Darab István [Rambo]

Az Antivirus.blog nevében Minden Kedves Olvasónknak Egészségben, sikerekben gazdag, feltörés- és adatszivárgásmentes Boldog Új Esztendőt kívánunk!



Megint rajzoltattunk néhány képet az AI motorral, ezúttal "Happy New Year" cimkére.

A generált képeken közös fotóra kértük Einsteint és John McAfeet, és együtt poharazgat itt Bill Gates és Steve Jobs is.

Egy biztos, nem maradunk majd téma nélkül a következő évben sem, a blog megy tovább. **Jó pihenést mindenkinek!**

Szólj hozzá!
Címkék: ünnep szilveszter újév boldog 2023.

Ajánlott bejegyzések:

Vírusmentes Boldog Új Évet 2022.

Kellemes Karácsonyi Ünnepeket!

Kellemes Karácsonyi Ünnepeket!

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Biztonságos bankolás
Deliága Éva gyermekpszichológus

- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász
- NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

- A Vírusok Varázslatos Világa 01.
- VVV 02.
- VVV 03.
- VVV 04.
- VVV 05.
- VVV 06.
- VVV 07.
- VVV 08.
- VVV 09.
- VVV 10.
- VVV 11.
- VVV 12.
- VVV 13.
- VVV 14.
- VVV 15.
- VVV 16.
- VVV 17.
- VVV 18.
- VVV 19.
- VVV 20.
- VVV 21.
- VVV 22.
- VVV 23.
- VVV 24.
- VVV 25.
- VVV 26.
- VVV 27.
- VVV 28.
- VVV 29.
- VVV 30.
- VVV 31.
- VVV 32.
- VVV 33.
- VVV 34.
- VVV 35.
- VVV 36.
- VVV 37.
- VVV 38.
- VVV 39.
- VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció