2000

Csomagot kaptam life...

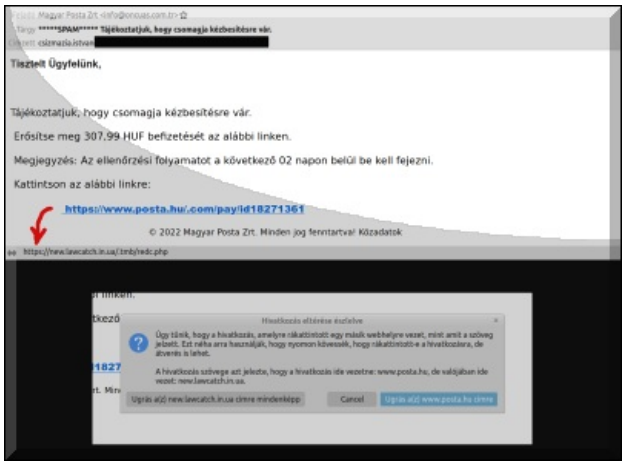
2023. január 03. 09:11 - Csizmazia Darab István [Rambo]

Röviden visszatekintünk az előző év első három legfelkapottabb témájára, akkor az alábbiak váltották ki a legnagyobb érdeklődést, kattintást. Az Opus együttes számának magyar félrehallásához hasonlító cím ("Levelet kaptam life") itt korántsem véletlen, hiszen mindhárom dobogós helyezett éppen ezt a témát karcolgatta.



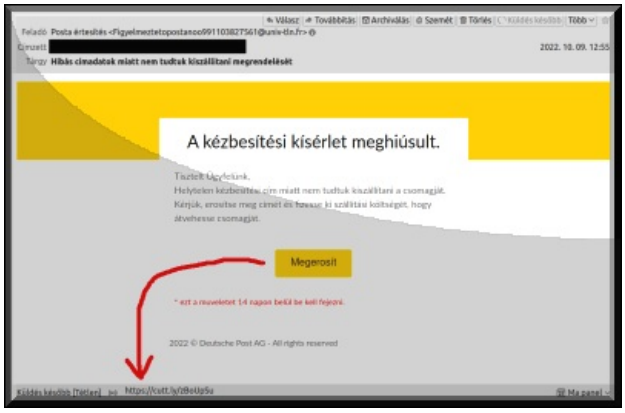
Visszafelé haladva **a harmadik legolvasottabb posztunk az a "Magyar Posta csomagunk jött - vagy mégsem?" című márciusi cikk volt**, amely egy Wordpress sebezhetőséget kihasználva terjedt a neten. A kamu üzenet arról tájékoztatott bennünket, hogy **kézbesítésre váró csomagunk miatt állítólag gyorsan fizetnünk kell pár száz forintot.**

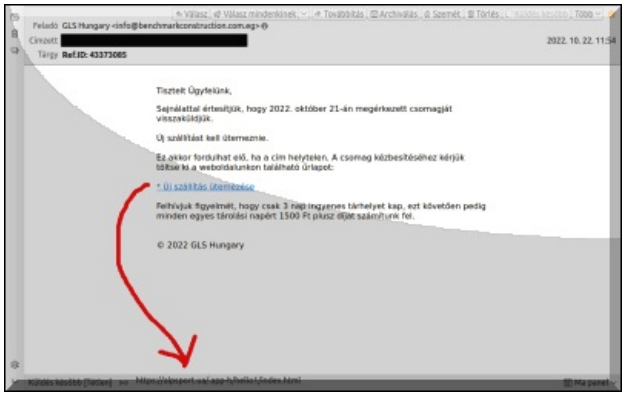
Az átverés nem is nagy összeg miatt érdekes, hanem **megpróbálja kicsalni a személyes és banki adatainkat: teljes név, teljes cím, irányítószám, bankkártya száma, lejárati dátum és a 3 jegyű CVV** biztonsági kód.



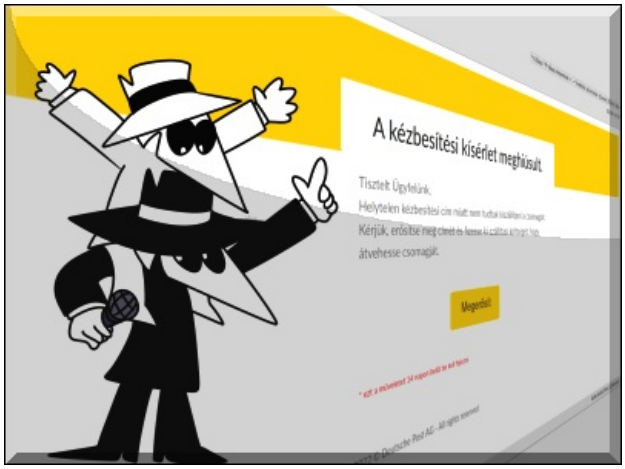
Ezüst érmes második helyezettünk az az októberi beszámoló lett, amelyből kiderülhetett, hogy "Ismét csomagunk érkezett - vagy mégsem?". De inkább mégsem. **Itt az egyik versenyző a Deutsche Post nevével visszaélő e-mail** hasonló logikával, meghiúsult csomagkézbesítésre hivatkozva várt kattintást egy link-rövidített rosszindulatú adathalász weboldalra.

Ezzel egyszerre érkezett **a GLS nevében egy igen hasonló átverés, ahol az adathalász oldal címegyeztetést kért,** amin aztán a bűnözők megkísérelték begyűjteni a személyes és bankkártya adatainkat. Itt **a sürgetés-nyomatékosítás-ijesztgetés arra hivatkozott, hogy ha elmulasztjuk a kért adategyeztetést, akkor napi 1500 forint tárolási díjat számítanak fel**, ami persze nem volt igaz.





És végül a favorit, 2022-es esztendő top #1 befutó bejegyzése a "Csomagja érkezett - sokadik menet" című poszt volt. **Újra a német posta nevében érkezett a próbálkozás**, szóval ez a címegyeztetősdi egy neverending story, tömegesen küldik ki, hátha lesz aki bedől ennek.



Nyilván 2023-ban is folyamatosan fognak érkezni a hasonló adathalász próbálkozások, érdemes tehát mindenkinek nagyobb figyelemmel kezelni a **gyanús kéretlen üzeneteket: feladót, linket, mellékletet csekkolni, helyesírási hibákra figyelni, idegen doméneknél gyanakodni.**

Megosztom tumblr. Tweet Pin it Tetszik 0

3 komment
Címkék: magyar toplista posta csomag post csalás átverés deutsche adathalászat gls csomagküldő 2022.

Ajánlott bejegyzések:



Ismét csomagunk érkezett - vagy mégsem?



Magyar Posta csomagunk jött - vagy mégsem?



Kár érte, kiváló ügynök volt...



Üdvözöljük, csomagja kézbesítésre vár



"NEM TUDJUK KISZÁLLÍTNI A CSOMAGÁT"

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

gigabursch 2023.01.03. 16:32:36

Nekem a magyar posta részéről jött egy levél...

Válasz erre

Head Honcho 2023.01.05. 01:44:48

Az egész a honfitársaink ijesztő technikai világtalanságára épül. Sajnos van mit az átlagmagyarnál megszólni...

Válasz erre

Frakki60 2023.01.05. 13:55:42

Az INTERNETEN folyamatosan érkező nyereményekről már nem is szólva!! Különféle csomagküldő szolgálatok, internetes áruházak, közműszolgáltatók nevében értesítenek arról, hogy egy többszáz-ezer forint értékű okostelefont nyertem, aminek minden költségét (adóvonzatát) állják, "csupán" a csomagolási és posta költségre kell elutalni ELŐRE!!!! 790 forintot. Hogy a bánatos mennykőben van az, hogy ez a - az ajándék/nyeremény értékének töredéke nem fér bele a költségvetésükbe?!?! Aztán miért is nem lehet UTÁNVÉTTEL fizetni??? (Mindenhol máshol ez működik) Gyanítom, hogy nagyon sokan fizetnének UTÁNVÉTTEL lényegesen többet is érte...

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

451

LockBit vs betyárbecsület

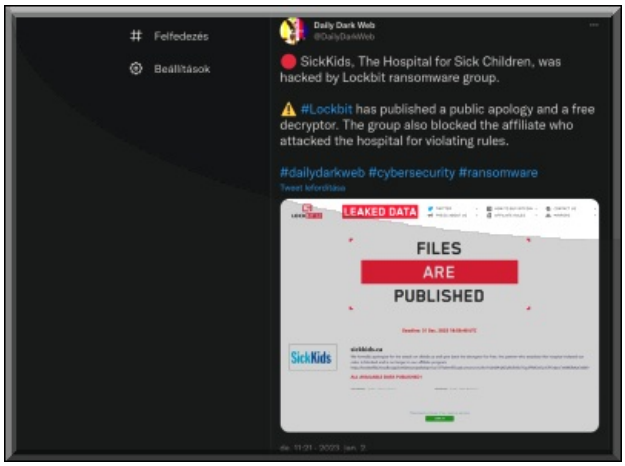
2023. január 04. 11:36 - Csizmazia Darab István [Rambo]

Van-e, lehet-e etikai kódexe egy bűnszervezetnek? Jó kérdés, mondhatnánk erre, és **ezúttal maga a nagybetűs ÉLET is felvetette mindezt egy közelmúltban lezajlott kibertámadás kapcsán.**



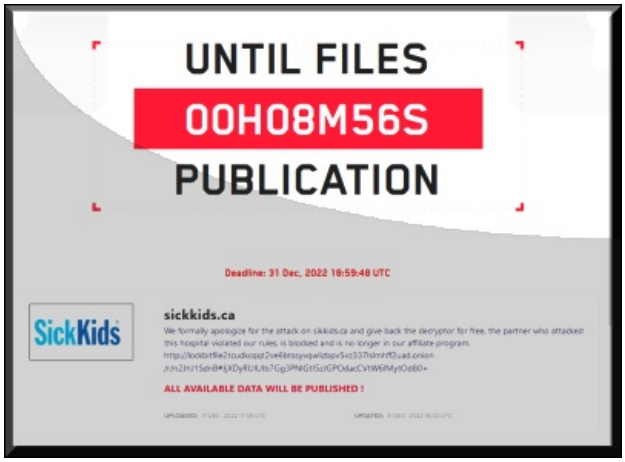
Az erkölcsös hozzáállás állítólag igen fontos a bűnözőknél is, erről bővebben Rejtő Jenő: Az elátkozott part című könyvében is olvashattunk. "*Jámbor ember vagyok, talán azért, mert anyai ágon egy nagybátyám kántor volt, és már kora ifjúságomban magamba szívtam a jó erkölcs törvényeinek tiszteletét. Ezért csak a legritkább esetben szánom rá magamat arra, hogy Márta napján lopjak. Mártának hívták az anyámat, és ez a nap nagy tiszteletben áll előttem.*"

Valamelyik képregény változatban mindez zanzásítva úgy hangzott: "*Márta napján ne lopj, csak ha muszáj!*"



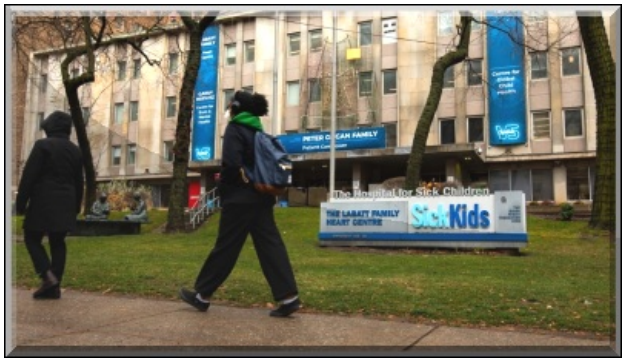
Ezúttal a kanadai SickKids kórház elleni ransomware támadás kapcsán merült fel utólag hasonló erkölcsi felhorgadás a LockBit csoport részéről, bár nem is Márta napon történt a dolog. Történt ugyanis, hogy **a napokban élesen elítélték egyik szerződött bűnözői partnerük korábbi akcióját arra hivatkozva, hogy ezzel a cselekményükkel megsértették a megállapodási feltételeket.**

Hogy ebben pontosan mi áll, nem tudhatjuk, ám valószínűleg nekik sem fér bele az ennyire kiszolgáltatott célpontok támadása. Ami emellett még a bandák közti renoméjukat is megtépázhatja, **de sokkal inkább az ilyen incidensek a hatóságok fokozott érdeklődését is felkorbácsolja az irányukba, ami nyilván nem célja a bűnszervezetnek.**



Minden esetre a LockBit "vezérkar" december 31-én nyilvánosan is elnézést kért partnere baklövése miatt, ebben a hibáztatott társult csoportot állítólag ki is zárták a Ransomware as a Service együttműködésből.

Valamint **egy ingyenes dekódolót tettek közzé az áldozatok számára a fájlok mielőbbi sikeres helyreállításához.**



Mint arról korábban itt a blogon is beszámoltunk, még 2022. december 18-án zsarolóvírus támadás érte a Kanadában található gyermekkórházat, **amely így műtéteket, kemoterápiás kezeléseket volt kénytelen elhalasztani, és betegeket is át kellett helyeznie** más társintézményekbe a belső informatikai rendszer leállása miatt.

Bár **január 1-től a kórház már részlegesen el tudott ugyan indulni hála a külsős szakértők folyamatos munkájának, de nyilván gyorsítani tudja majd** ezt a mostantól hozzáférhető helyreállító eszköz is.



Az incidenssel kapcsolatban viszont még mindig nem tudni, pontosan mekkora váltságdíj követeléssel jelentkeztek a támadók, és **ami talán még ennél is fontosabb, hogyan tudtak bejutni a kórház informatikai rendszerébe, illetve mennyi és milyen adatot lophattak el onnan a támadás során.**

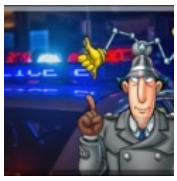
Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: ingyenes kórház kanada gyermekkórház ransomware dekódoló zsarolóvírus lockbit sickkids

Ajánlott bejegyzések:








Összeomlás | 8 kórház, 30 klinika, 2.5 millió betegadat | LockBit piacgazdaság és tervgazdálkodás | Kékfény különkiadás | 9 millió, bizony, dalolva ment...

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

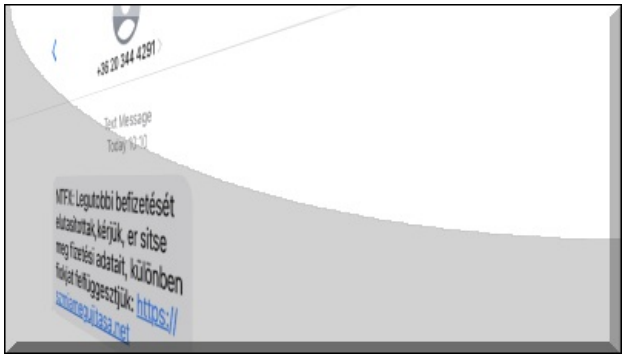
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

1916

2023. első csalásai

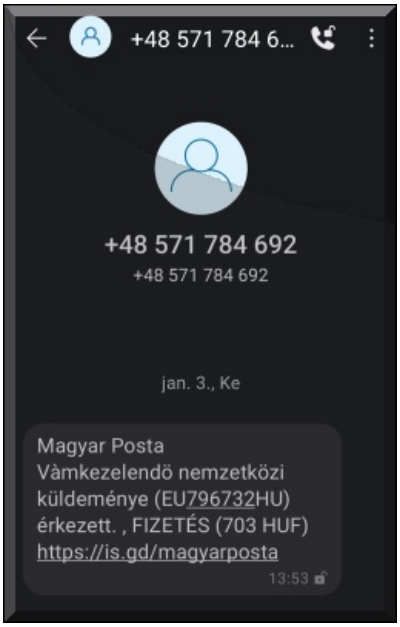
2023. január 10. 12:01 - Csizmazia Darab István [Rambo]

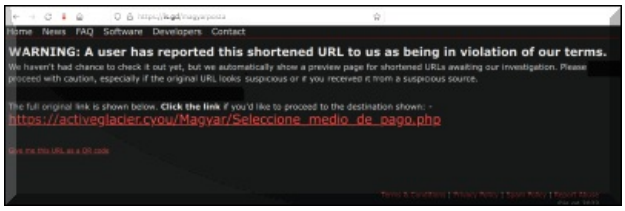
Több próbálkozás is érkezett e-mailben, SMS-ben, amelyek a tavalyi trendeknek megfelelően csomagküldéssel, nyereménnyel, webáruházas rendeléssel voltak kapcsolatosak.



Folytatódnak a klasszikus receptek alapján történő adathalász támadások, amelyek valamilyen futárcég vagy a posta nevében igyekszik megtéveszteni a felhasználókat.

A korábbi évekhez képest sajnos egyre gyakoribb a telefonhívással (például banki ügyintézőnek adják ki magukat a csalók) vagy a FedEx-es támadáshoz hasonlóan az SMS üzenetek is hordozói lehetnek a kártékony linkeknek.





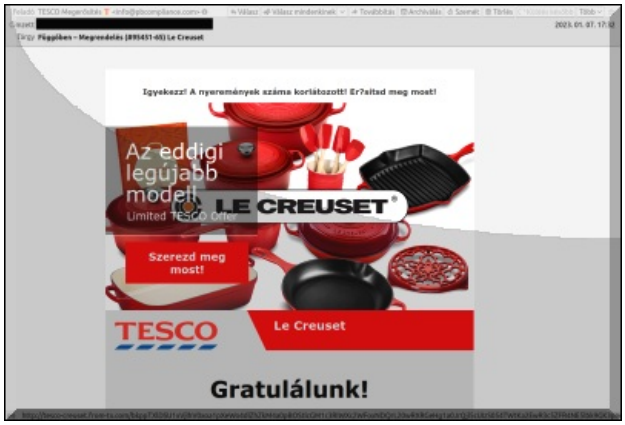
Első munkadarabunk éppen egy ilyen **SMS üzenettel érkezett, amely külföldi postacsomag vámkezelésére hivatkozva igyekszik fizetésre bírni bennünket**. Akár a kíváncsiság vezérli (na vajon mi lehet ez?), akár a düh (mit kell már megint befizetni, ezt nem hiszem el) önti el a gyanútlan felhasználó agyát, mindenképpen rossz választás ad a link.

Bár látható benne a "magyarposta", de **a hivatalos doménhez semmi köze (https://www.posta.hu), és valójában egy rövidített linket látunk, amelynek a feloldása aztán végképp messze áll** mindenfajta hivatalos weboldal címtől. A poszt írásakor az oldal már nem működött, lelőtték időközben.



Nyerni jó, nyerni szép, és ha már a Mikulás nem hozott nekünk sok ezer eurót, akkor reménykedhetünk, ha ilyen ígérettel bélelt üzenet mégis csak beesik az e-mail fiókunkba. **Sajnos a klasszikus csalásokra utaló intő jelek szinte mindegyike ott sorakozik: összevissza című feladó, tipikus tömegesen kiküldött körlevél kinézet, gyatra magyarság és helyesírás toporognak a levélben.**

Nyertünk egy olyan lottón, amelyen nem is játszottunk, és **a nyersfordításnak látszó szöveg szerint állítólag 115 ezer eurónyi összeg (cirka 45 millió HUF) vár bennünket**, ha felvesszük velük a kapcsolatot. Az elköszönés már önmagában is egy mesés darab: **"*Várom te hamarosan*".**



Végül, de nem utolsó sorban egy **olyan e-mail is érkezett, amely egy függőben lévő megrendelésre hivatkozik.** Nyilván itt is arra játszanak, hogy **a delikvens megijed, és gyorsan ki akarja nyomozni, ki és mit rendelt az ő nevében, ami esetleges anyagi veszteséget okozhat**. A levél belsejében aztán már semmiféle függő megrendelés nem látszik, sokkal inkább egy kéretlen spam üzenetnek látszik, amely valamilyen edénykészletet igyekszik ránk sózni.

Egy másik hasonlóban pedig kiválasztottak bennünket a "hü(lye)ségprogramukra" és ezt teljesen ingyenesen. A link már ezeknél a levélnél sem üzemelt, így az **nem derült ki, valóban árultak-e valamilyen terméket, esetleg hamisítványokat, vagy rögtön valamilyen adathalász, vagy kártékony weboldalra került az, aki erre korábban rákattintott.**



Régen régen volt a Hofinak egy vicce: "40 kilós és füvet eszik, mi az? Jövőre te." Valószínűleg nem járunk messze az igazságtól, ha ehhez hasonlóan a "napi több tucat ilyen üzenetet kap, ki az?" kérdésre azt jósolhatjuk, hogy sajnos ezek mi leszünk mindannyian.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: spam magyar posta sms e-mail csalás átverés nyeremény adathalászat

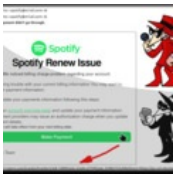
Ajánlott bejegyzések:



[Csomagja kézbesítésre vár! Vagy mégsem?]



[Magyar Posta csomagunk jött - vagy mégsem?]



[Spotify megújítási probléma - vagy mégsem?]



[Üdvözöljük, csomagja kézbesítésre vár]



[Netflix: lejárt a tagságunk. Vagy mégsem?]

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

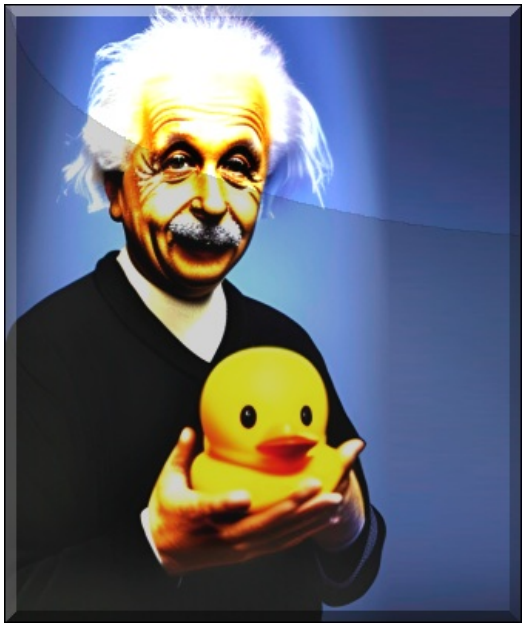
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

545

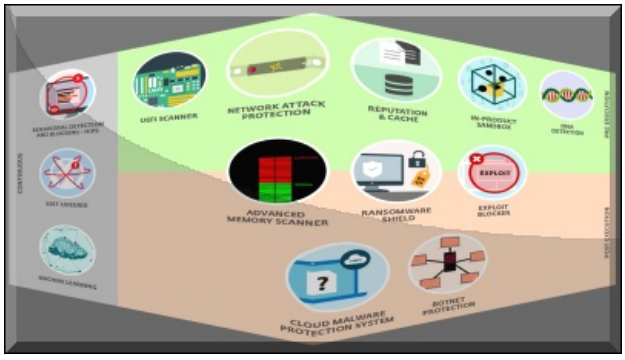
Nyakunkon az AI

2023. január 12. 14:29 - Csizmazia Darab István [Rambo]

Sok posztban foglalkoztunk már azzal, hogy a gépi tanulás és mesterséges intelligencia kétélű fegyver: **használják mind a védelem oldalán, és persze a támadók is élnek vele.**

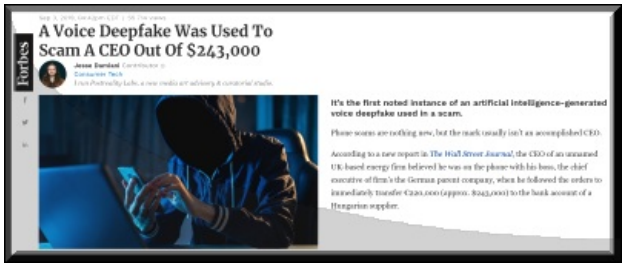


Két idézet is jól rávilágít, mennyire aktuális lett ennek a területnek a felhasználása. Az egyik szerint: *"A mesterséges intelligencia megjelenése miatt a technológiai fejlődés és a társadalmi változások annyira felgyorsulnak, amit a szingularitás előtt élők képtelenek felfogni vagy megbízhatóan kezelni."*. A másik mondás pedig a McKinsey Global Institute kutatóitól származik: "*100 év alatt húszezer évnyi fejlődést hozhat a mesterséges intelligencia*".



A vírusvédelemben is sokan aktívan alkalmazzák a kezdetektől. Például az Esetnél **már 1989-től adatgyűjtés-osztályozás, 1995-től pedig gépi tanulás, és több integrált belső modul is kihasználja**, például a Live Grid, Exploit Blocker, Botnet Protection, Antiransomware, stb.

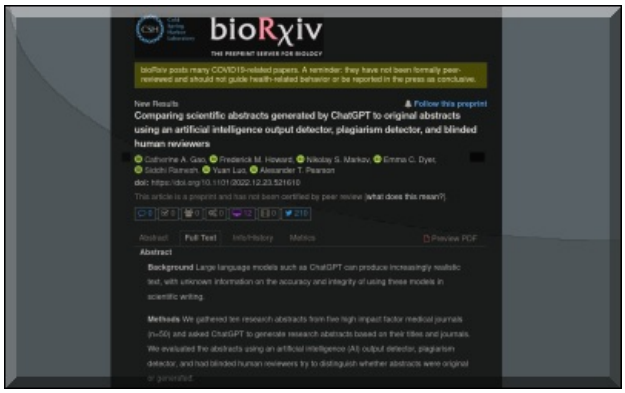
De nem csak a védelemnél dolgozik az AI, hanem a víruslaborokban is régóta működik a kézi elemzés mellett automata feldolgozás, például az **ESET LiveGuard Advanced (Dynamic Threat Defense) is használja a sandbox technológiát és a gépi tanulást.**



Ám a támadói oldal is gőzerővel fejlődik, ehhez beidézhetjük például azt a korábbi esetet, ahol **2019-ben a DeepVoice hangszintetizálás segítségével a RealTalk programmal a támadók a németországi igazgató hangján és nevében felhívták a brit energetikai cég vezetőjét**, és megtévesztve 220 ezer eurós (akkori áron cirka 72m HUF)

azonnali átutalást kértek egy magyar beszállító partner számlájára.

Mire kiderült a csalás, a pénzt már továbbutalták, és a cégnél csak későn vették észre a trükköt.



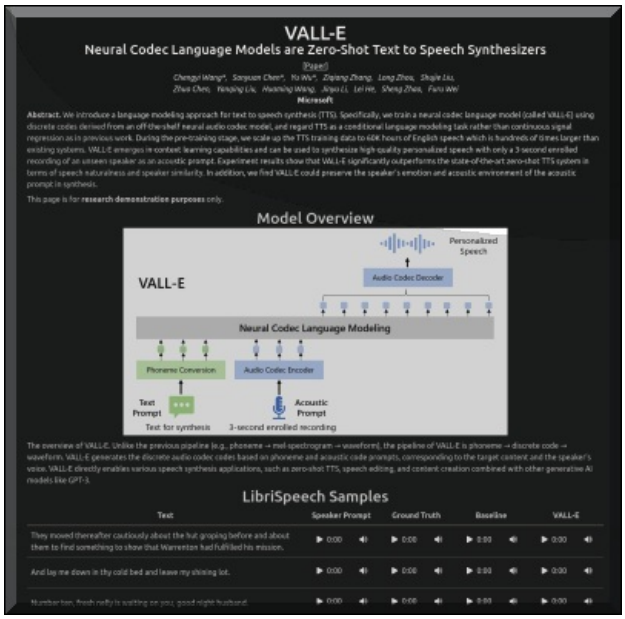
Most több cikk is foglalkozik azzal, hogy a Photoshop-Deepfake-Fakenews tengely után újabb nehezen felismerhető megtévesztések érkeznek, és ezek mind AI alapú fejlesztések eredménye. Kezdhetjük azzal, hogy egy Northwestern University által vezetett kutatócsoport olyan kísérletet végzett, amely **a ChatGPT által generált hamis tudományos értekezések hihetőségét próbálta vizsgálni és tesztelni.** Legeneráltak az OpenAI által fejlesztett eszközzel 50 darab publikációt öt különböző orvosi folyóirat stílusában.

Felvettek négy akadémikust, és **pénzfeldobással eldöntve véletlenszerűen kaptak bírálatra hamis vagy valódi értekezést. A végeredmény rámutatott, hogy az AI anyagok 32%-át valódinak ítélték,** míg a valódi anyagok közül 14%-ot gondoltak hamisnak - vagyis ez a fajta manipuláció nagyon eredményes lehet.



Ha most a valódi kibertámadásokat vesszük, ebben is látunk vészjósló felhőket: miszerint **az AI által generált adathalász e-mailek sokkal meggyőzőbbek, tehát veszélyesebbek lettek.** A GPT-3 modul mind a testre szabott, célzott phishing levelek finomhangolásában, mind a hihető álhírek generálásában jeleskedett. Emiatt jól látható, hogy **az átverés áldozatai számára még nehezebb lesz azonosítani az AI által írt rosszindulatú és hamis tartalmakat.**

Persze AI mentesen is lehet jól célozni csalásokat, **ha például feltörik a céges levelezést (BEC, Business E-mail Compromise) és abban megfigyelik a hierarchiát, a szervezet működését, úgy a külsős és belsős kulcsemberek nevében tudnak olyan megtévesztő üzenetet írni,** ahogy például a Magyar Vízilabda-szövetség berkein belül 120 ezer eurót (kb. 50 mHUF) egy állítólagos "új" számlára kértek utalni a bűnözők.



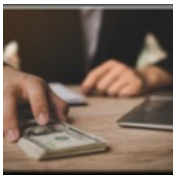
És a hogy a végére is maradjon még érdekesség, a Microsoft kutatói egy olyan szövegfelolvasó (Text To Speech, TTS) modellen dolgoznak, amely mindössze **három másodperces mintával történő betanítás után képes utánozni egy adott személy hangját, és nem is akárhogyan: érzelmekkel és megfelelő intonációval kiegészítve.**

Vagyis már jó ideje nem hihetünk a szemünknek az 1988-ban megjelent 34 éves Photoshop program miatt a képeknek, aztán 2018. óta a Deepfake már a videós tartalmak megbízhatóságát is kérdőjelessé tette, közben mindenütt hegyekben áll a fakenews és lassan az ismerősünk hangja sem lesz már garancia arra, hogy valóban ő maga kér-e tőlünk valamit, vagy egy ismeretlenek által használt VALL-E program. Jól fel van tehát adva a lecke mindenkinek a csalások, átverések felismerése területén, készülhetünk.

Megosztom tumblr. Tweet Pin it Tetszik 0

3 komment
Címkék: kép videó ai hang mesterséges intelligencia gépi tanulás

Ajánlott bejegyzések:


Megváltás-e a váltságdíj?


Na de mit adott nekünk a ChatGPT?


ChatGPT: hogyan használjuk a munkában?

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Head Honcho 2023.01.12. 18:41:35

*Text To Speech

Válasz erre

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2023.01.12. 18:50:01

Köszi. Ezt a cikket nem az AI írta, hanem humán, csak így kerülhetett bele liba ;-)

Válasz erre

Head Honcho 2023.01.14. 08:46:16

@Csizmazia Darab István [Rambo]: Ügyes csel. :)

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

569

Időjárás, vízállás és ransomware előrejelzés

2023. január 17. 13:05 - Csizmazia Darab István [Rambo]

10 éves születésnapját ünnepli a zsarolóvírus modern formája, ami a kezdeti amatőr GPCode és hasonló gyengébb próbálkozások után a 2013-as Cryptolocker megjelenése változtatott meg mindent. Erős egyedi kulccsal való elkódolás után a helyreállításért váltságdíjat kriptovalutában követelő bűnözők mára elárasztották a kiberteret.



Persze soha senki nem jósolt olyasmit, hogy az ilyen kártevők valaha is el fognak tűnni az életünkből, ám **az erős kezdés után a támadók fokozatosan erősítettek, lett doxing, azaz adatlopás előzi meg a titkosítást, lett RaaS azaz Ransomware as a Service, és lett destruktív elkódolás, ahol nem cél a váltságdíj begyűjtése, hanem a szándékos rombolás a fő motiváció.**



Négy vállalható jóslat következik, milyen hatással lehet ránk a folyamatos ransomware kitettség. Az első pont mindjárt az, hogy **egyre célzottabb és kifinomultabb támadások várhatók a közeljövőben.**

Megfigyelhető, hogy a bűnözői csoportok folyamatosan fejlesztenek, **technikailag is egyre professzionálisabb** formákat alkalmaznak, pl. az elkódolás gyorsítása szakaszos titkosítással. **De a social engineering területén is bepróbálkoznak**, például sértett munkavállalók toborzásával, akik pénzért eladják a bűnözőknek a saját céges belépési és hálózati információkat.



A második lehetséges előrejelzés az elsősorban a vállalati szektorra vonatkozik, miszerint elkerülhetetlen, hogy a biztonsági mentésekre egyre nagyobb figyelem összpontosuljon, és ez nem csak azzal jár majd, hogy emelkedő tárterületeket veszünk igénybe, hanem a mentések is egyre inkább célpontjai lesznek a támadásoknak.

Itt láttunk már **számos hiányosságot például hálózati tárolók, routerek biztonsági frissítéseinek elhanyagolását, célzott NAS elleni támadásokat**, így az nagyon valószínű, hogy erre a területre a céges környezetekben komolyabb védelmi megoldások, rétegek kellenek majd.



A harmadik jóslat a zsarolóvírus elleni kiberbiztosításokkal kapcsolatos. Azt már korábban írtuk, hogy a ransomware elleni biztosítással rendelkező cégek, állami hivatalok sokkal engedékenyebben fizetnek váltságdíjat az átlag piaci szereplőkhöz vagy magánemberekhez viszonyítva, és erre a támadók is ráéreztek.

Sok esetben éppen emiatt fokozódott a célzott támadás az állami közintézmények, kórházak, iskolák, önkormányzatok ellen, ahol általában gyengébb a technikai védelem, nincs elegendő számú főállású képzett IT biztonsági szakember, és gyakran a biztonsági területen történő fejlesztések helyett fizetnek inkább váltságdíjat. **Itt a biztosítóknál várhatóan alaposabb elvárások fognak jelentkezni, a kárfizetéseknél több lesz majd az elutasítás, és a biztosítási díj emelkedése is elkerülhetetlennek látszik.**



Végül **az előrejelzés negyedik pontja azt festi fel, hogy az automatizált patchmenedzsment, valamint biztonsági mentési és tárolási rendszerek iránt** várhatóan növekvő lesz az érdeklődés. Ezt persze 2023. év végén visszamenőleg is ellenőrizhetjük majd, mennyire érzékelhető lett ez a tendencia.

Összességében tehát folytatódik a felhasználókra az össztűz, és **annyi már most biztos, hogy a kisebb beszállítóktól kezdve a multicégeken át a kritikus infrastruktúrák üzemeltetőinek is nehéz évük lesz az idei.**

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: trend jóslat biztosítás előrejelzés tendencia váltságdíj ransomware zsarolóvírus 2023.

Ajánlott bejegyzések:


Durva ransomware statisztikai adatok


Ransomware támadás a Nissan ellen



8 kórház, 30 klinika, 2.5 millió betegadat


LockBit piacgazdaság és tervgazdálkodás



Ransomware a One Motelben

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

2690

Mit csinálnak az alkalmazottak a céges gépeken?

2023. január 20. 14:18 - Csizmazia Darab István [Rambo]

A koronavírus járvány egészen új helyzetet teremtett számos cégnél a munkavégzésben. **Az otthon és munkahely határai összemosódtak, ez pedig egészen új kihívásokat jelent a számítógépek és hálózatok védelmét tekintve. Podcast sorozatunk második adásában erről a témáról beszélgettünk.**



A koronavírus miatt egyik napról a másikra kellett átállni az otthoni munkára, ezzel szinte egyik pillanatról a másikra alakult át az otthoni hálószoba, a gyerekszoba, vagy éppen az étkező irodává. **Ilyen gyorsan nem is tudott mindenki felkészülni a megfelelő internetbiztonságra.**

A pandémia miatt elterjedt otthoni munkavégzés tízből kilenc amerikai cégnél negatív hatással volt a csalásmegelőzési intézkedések hatékonyságára, a megfelelőségi kockázatok kezelésére, vagy a kiberbiztonságra - így összegezhetők a 2022-es KPMG Fraud Outlook megállapításai. **Mostani podcast beszélgetésben az volt a fókuszban, hogy hogyan alakítható ki a biztonságos otthoni munkakörnyezet.**



Szinte egyik napról a másikra zárták le az országot, zártak be cégek, álltak le a tevékenységükkel, vagy éppen költözött át a munkavégzés az otthonokba. **Milyen jellegű kibertámadások történtek a covid kitörése idején? Melyek a leggyakoribb hibák, amiket cégek elkövettek az otthoni munkavégzésre való átállás során? Mi volt azokkal a kisebb cégekkel, ahol nem volt külön IT részleg? Ezekre a kérdésekre kerestük a választ a Hackfelmetszők - Veled is megtörténhet! 2. adásában.**



A friss 2-ik adás itt hallgatható meg. A korábbi, első adást, amelyben azt jártuk körül, hogyan jutnak be a kártevők gépeinkre és hálózatainkba - pedig ezen a linken lehet megtalálni, és visszahallgatni.

Megosztom tumblr. Tweet Pin it Tetszik 0

[Szólj hozzá!](#)
Címkék: biztonság podcast eset otthoni munkavégzés pandémia homeoffice covid hackfelmetszők

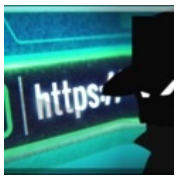
Ajánlott bejegyzések:


Hogyan lehetünk jó digitális szülők?



Kis- és középvállalkozások adatvédelmi incidensei


Black Friday és Cyber Monday járja be Európát


Böngészés - kockázatok és mellékhatások


ChatGPT: hogyan használjuk a munkában?

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

443

Kiberbiztonsági trendek 2023.

2023. január 25. 10:37 - Csizmazia Darab István [Rambo]

Milyen munkavégzést érintő változások várhatóak a biztonságunk és magánéletünk szempontjából, hogyan befolyásolja az online és az offline életünk között húzódó határvonal elmosódása az életünket, milyen kiberfenyegetések próbálkoznak legyűrni bennünket?



Marad a hibrid munkavégzés a maga kihívásaival, a távolról bejelentkező munkatársak és eszközeik jelentette kockázatokkal. Az utóbbi évek változásainak eredményeként egy olyan világ alakult ki, ahol nemcsak a munkahely és az életmódbeli szokásaink, hanem a a munka és a magánélez közötti határvonalak is egyre inkább elmosódtak.

Mivel a támadási vektorok alapján igen gyakori, hogy a kisebb, technikailag kevésbé védett beszállítókon vagy partnercégeken át igyekeznek megtámadni a nagyobb cégeket, ellátási láncokat, emiatt minden vállalkozásnak résen kell lennie. Sajnos az is tapasztalat, hogy sokszor a cégek csak akkor emelik az informatikai költéseket, miután már biztonsági incidens áldozatai lettek.



A 2022. Data Breach Investigations Report szerint **a támadók az esetek 82%-ában a felhasználók valamilyen megtévesztésével - hamis e-mailek, rosszindulatú weboldalak használatával, vagy lopott belépési azonosítókkal - jutnak be a vállalati IT-rendszerekbe**, a betörésekkel okozott **veszteség átlagos értéke pedig 4.3 millió dollár volt 2022-ben.**

Emiatt **fontos lenne a felhasználók biztonságtudatosságának emelése**. Itt nem csak a céges telefonok és vállalati laptopok digitális védelmére van szükség, de azt is tudatosítani is kell a munkavállalókban, hogy ezeket az eszközöket például ne használják magáncélokra. Emellett lényeges, hogy az alkalmazottak ne ugyanazokat a jelszavakat alkalmazzák személyes és munkahelyi fiókjaik esetében, illetve nélkülözhetetlen lenne a többfaktoros hitelesítés teljes körű használata.



Persze mindez az emelt tudatosság nem csak az alkalmazottak esetében lenne fontos: egy közelmúltban készült jelentés

szerint **a cégvezetők négyszer nagyobb valószínűséggel esnek adathalászat áldozatává, mint az irodai dolgozók.**

Emellett 4 vezető beosztásban dolgozó közül 1 könnyen megjegyezhető születésnapot használ a jelszava részeként, sőt beosztottjaiknál ötször nagyobb valószínűséggel osztják meg jelszavukat a vállalaton kívüli emberekkel.



A felhőt sokan leginkább a videókonferenciák során, az együttműködési, fájlmegosztási eszközök, a termelékenységnövelő és hálózatépítési platformok által használják – gondoljunk csak a népszerű Microsoft Teamsre, a Slackre vagy a Zoomra.

Ezek a kommunikációs eszközök azonban veszélyeket is rejtenek magukban. 2021-ben például egy olyan sebezhetőséget fedeztek fel a Microsoft Teamsben, amely lehetővé tette, hogy adatokkal visszaélő bennfentesek e-maileket, Teams-üzeneteket, illetve OneDrive és SharePoint fájlokat lopjanak el. A koronavírus-járvány kezdete idején pedig hackerek több mint 500 ezer Zoom felhasználó adatait lopták el és tették fel a dark webre. **Elgondolkodtató adat, hogy 2020-ban az összes kibertámadás 20 százalékát tették ki felhővel kapcsolatos incidensek.**



Mi várhat még ránk mindezen felül? **Már 2021-től kezdődően megfigyelhető volt az a trend, hogy évi 15%-kal nőttek a kiberbűnözéssel kapcsolatos vállalati költségek, ami idén sem fog megállni, és így várhatóan ezzel együtt drágul és szigorodik majd a kiberbiztosítás is.**

Várhatóan a kriptovaluták területén egyre gyakoribbak lesznek az incidensek, a megfelelő hatósági szabályozások megalkotása elkerülhetetlennek látszik. A sötét oldal viszont továbbra is **használja majd váltságdíjak lekövethetetlen kifizetésére, illetve magánszemélyek és szervezetek számláinak megcsapolása is reális kockázat lesz.**



És a ransomware is velünk marad sajnos. **Ez a 2013. óta, tehát gyakorlatilag tíz éve létező komoly kockázat, ami valóban felrázta a felhasználókat, vállalkozásokat.**

Itt már évek óta a kombinált támadás a jellemző: a titkosítás előtt adatlopás (doxing), és **a zsarolás nem csak a feloldó kulcsról szól, hanem a bizalmas adatok publikálásával való fenyegetésről is, kritikus infrastruktúrák, üzleti vállalkozások esetén pedig nemfizetés esetén pluszban még DDoS-szal (elárasztásos túlterheléses támadással)** való riogatással is.



Összességében **még több figyelmet kell fordítsunk a kiberbiztonságra, és biztonságtudatosabbak legyünk a privát és a szakmai életünkben egyaránt. Tudatos kell törekedni arra, hogy a tipikus leggyakoribb munkavállalói hibákat sikeresen kiküszöböljük. Itt nagyon sok mindent fel lehetne sorolni, az elavult szoftverek használatát, a védetlen hálózatokat, a rossz jelszó-higiéniát, nyilvános wifi használatot, gondolkodás nélküli kattintást, nem használni biztonsági megoldást minden eszközünkön, a BYOD, a Shadow IT, személyes bizalmas adatok felelőtlen megadása telefonon keresztül ismeretleneknek, a biztonsági mentések hiánya, és még hosszú lehetne a lista.**

A helyzet nem könnyű, hiszen mindeközben **egyre súlyosabb gond az IT security területén a szakember hiány.** Jelenleg kb. 3 millió specialista hiányzik, a cégek 70%-nál vannak betöltetlen pozíciók.



Szintén egy jellemző statisztikai adat, hogy **az utóbbi időszakban kiugróan nőtt a smishing, amikor SMS-ben érkezik a kártékony link,** emlékezzünk csak a FedExes történetre, a "csomagja érkezett, kattintson" üzenetre, de **ma már Revolut, Netflix, DHL, Deutsche Post, és megannyi szervezet nevével élnek vissza szinte naponta. Mivel egyre gyakoribb, tömegesebb és kifinomultabb támadásokat látni - smishing, vishing, business email compromise** - ezért kulcsfontosságú a biztonságtudatossági oktatás, a felhasználók rendszeres képzése.

A felhasználó ne a leggyengébb láncszem legyen, hanem a védelem első vonala a vállalat IT-biztonsági szervezetében. A 2023-as előrejelzéseket tartalmazó teljes, angol nyelvű riport ide kattintva érhető el: ESET Cybersecurity trends 2023

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: trend előrejelzés eset report cybersecurity 2023.

Ajánlott bejegyzések:


Szektorhiba


Időjárás, vízállás és ransomware előrejelzés



Folytatják támadásaikat az orosz hackerek Ukrajna ellen


Xmas és Top posztok az idén


Azonnali frissítés szükséges a fiók aktiválásához!

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

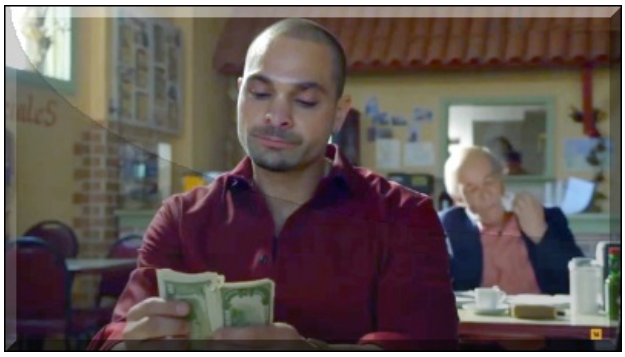
Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

Csökkent a zsarolóprogramból származó bevétel

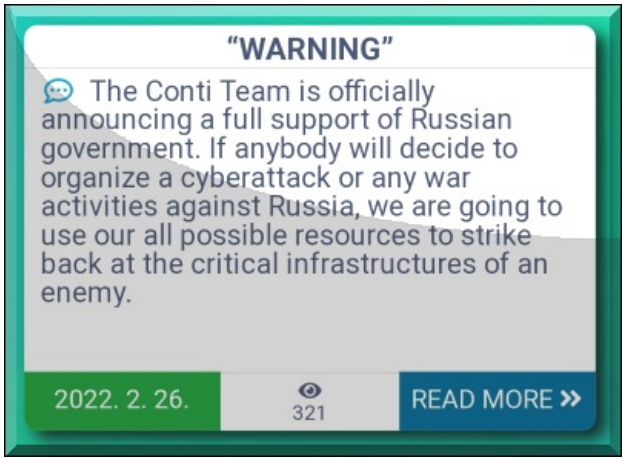
2023. január 30. 17:07 - Csizmazia Darab István [Rambo]

Ezt állapította meg egy friss tanulmány, ennek pedig az az oka, hogy egyre több áldozat nem hajlandó váltságdíjat fizetni.



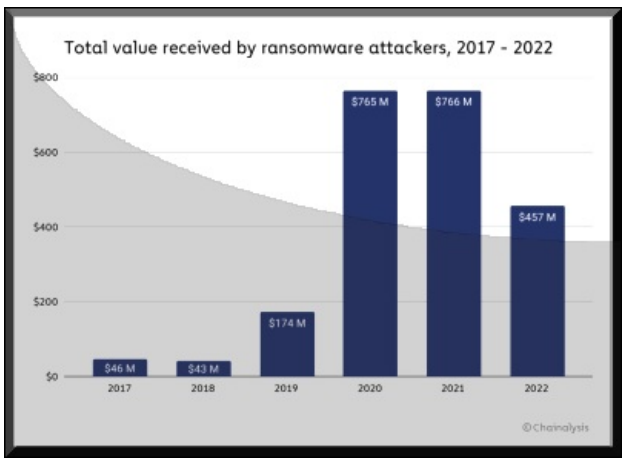
A statisztika szerint a ransomware bandák 2022-es évben alsó hangon 457 millió dollár értékű pénzt csikartak ki az áldozataiktól, míg ugyanez a szám 2021-ben még 766 millió dollár volt, **ami jelentős eltérés, 40%-os csökkenés**. **A dolog oka korántsem az, hogy visszaszorult volna az ilyen típusú támadások száma, hiszen ezek emelkedését látjuk. Sokkal inkább annak tudható be a csökkenés, hogy a fizetési hajlandóság esett vissza jelentős mértékben.**

A mérhető csökkenést okozhatják a jelenleg még a beazonosíthatatlan kriptovaluta csatornák, illetve az a tény is, hogy mivel az orosz FSZB támogatását élvező Conti csoport nyilvánosan is Vlagyimir Putyin híveként azonosított magát, így a nekik való fizetés a terrorizmus támogatását segítené elő.



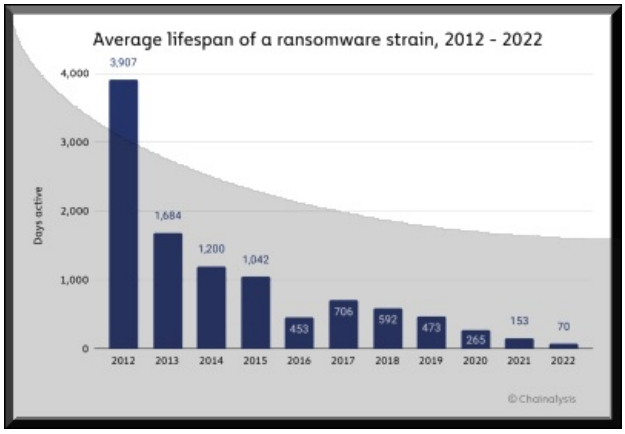
Sok érdekesség található még a jelentésben, például az is szembeötlő, hogy a ma már döntő részben RaaS alapon működő üzletben **az egyes ransomware-törzsek egyre rövidebb ideig aktívak.**

A 2010-es évek hosszú, több éves ciklusok helyett tavaly **ez az időintervallum átlagosan már csak alig 70 napra zsugorodott.** A kizsarolt összegeket a bűnözők igyekeznek nehezen lenyomozhatóvá tenni, így különféle kriptotőzsdéken keresztül futtatják meg a pénzeket.



Jelentős számú bűnözői csoport osztozik a ransomware piacon, **továbbra is dívik az affiliate network, azaz a különféle együttműködési rendszerek alapján dolgoznak össze más kiberbűnözőkkel.** A Microsoft Security észlelése szerint egyes ransomware bandák - például a DEV-0237 - nem csak egyetlen adott zsarolóvírus technikát használnak, hanem több törzset - Hive, Conti, Ryuk és BlackCat - is használnak aszerint, hogy a célpont támadásához melyik a legmegfelelőbb.

A kutatókat néha az is segíti, hogy a korábbi kutatásokban már szereplő wallet címeket látnak ismételten felbukkanni.



Összességében tehát a kockázat és a fenyegetés nem lett kisebb, csak a szerkezet alakult át. Michael Phillips, a Resilience kiberbiztosító cég kárrendezési igazgatója szerint a váltságdíj fizetések visszaeséséhez az orosz-ukrán háború és a nyugati bűnüldöző szervek ransomware bandákra nehezedő fokozott nyomás is hozzájárulhatott.

A Coware olyan táblázatot is közölt, amelyben a fizetési hajlandóság változása követhető nyomon, ezek alapján is markáns változás látható nem csak a tavalyi, de a 2-3 évvel korábbi adatokhoz képes is: **2019-ben még 76% fizetett, 2022-ben ez már "csak" 41%.**


If we take DLS victim leaks as a proxy for the number of attacks, there's still a huge gap between a 10.4% drop in leaks and a 40.3% drop in overall ransomware revenue. Instead, our conversations with representatives of cyber insurance and incident response firms suggest much of the revenue drop is explained by victims paying less frequently. Bill Siegel of Coveware provided us with statistics on the probability of a ransomware victim to pay a ransom based on his firm's client matters over the last four years:

	2019	2020	2021	2022
Paid	76%	70%	50%	41%
Did Not Pay	24%	30%	50%	59%

A kiberbiztosítási iparág szereplői szerint az elvárt szigorúbb kiberbiztonsági intézkedések is abba az irányba sarkallták a cégeket, hogy **ne letudják a fizetést, hanem valódi erős lépéseket tegyenek a megelőzés területén, kezdve a mentésektől a végpontvédelmen át mindenfajta egyéb biztonsági intézkedésig.**

Bár a zsarolóvírus üzletág ma már sokkal inkább a doxing, azaz az ellopott bizalmas adatok kiszivárogtatásával fenyegeti meg inkább az áldozatokat, **remélhetőleg a 2023-as hasonló statisztika még szebb adatokat mutat majd.**

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: statisztika váltságdíj ransomware zsarolóvírus 2022.

Ajánlott bejegyzések:



Gyorsabban, magasabbra, erősebben!


Emelkedő ransomware károk


Durva ransomware statisztikai adatok


Ransomware a spájzban


Ransomware támadás a Nissan ellen

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

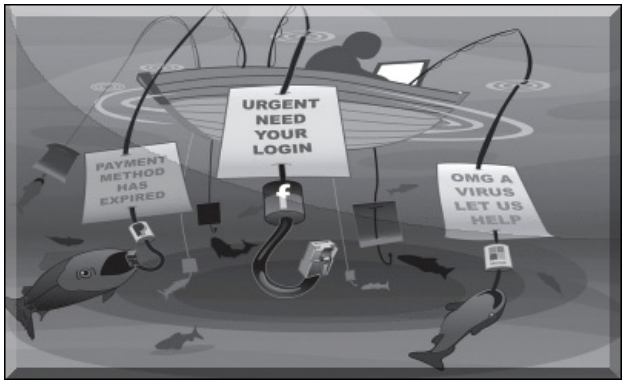
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

1113

Az öreg adathalász, és a link tenger

2023. február 06. 10:46 - Csizmazia Darab István [Rambo]

Két különböző statisztikai összefoglalót is megnéztünk, **milyen tendenciák, trendek, mozgások látszanak a tavalyi évben keringő phishing üzenetek terén.**



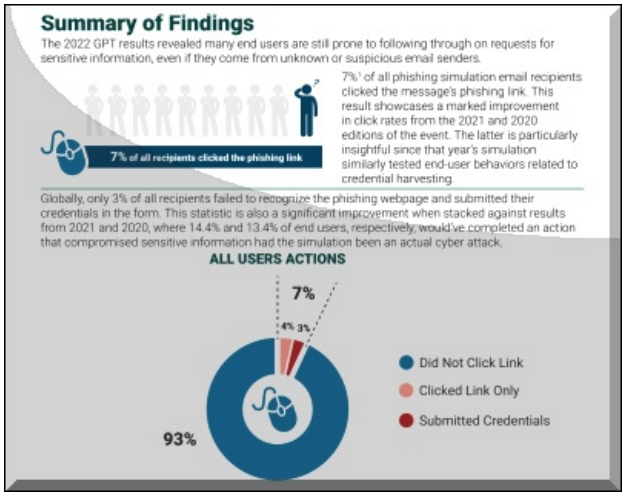
A KnowBe4 2022. negyedik negyedéves elemzése arra mutat rá, hogy **az egyik leggyakoribb átverés a cégek IT és HR osztályainak nevében érkező üzenet, ezeknek sokan bedőlnek** legyen szó a nyári szabadságolással kapcsolatos téma, vagy csak valamilyen hétköznapi dologgal, például öltözködési dress code kapcsán küldött levél.

De az állítólagos jelszó ellenőrzésre való felhívás is belefért az első három csalárd üzenet típusba, ami meghozza a támadóknak a sikert.

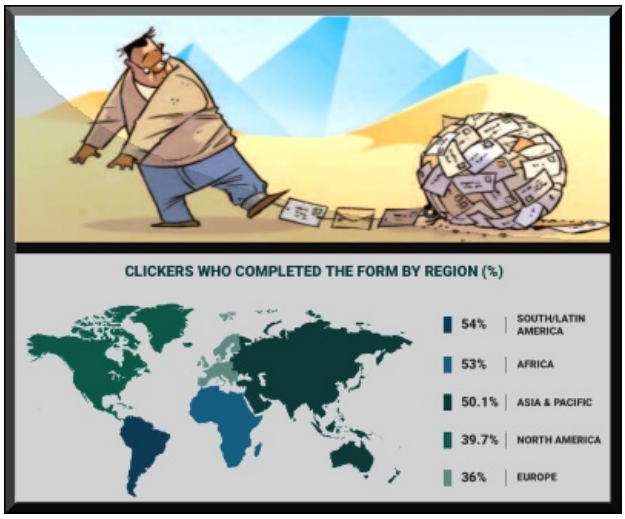


Nincs meglepetés abban, hogy minden rendkívüli eseményt kihasználnak a támadók, legyen az éppen a szilveszteri évváltás, vagy egyéb jelentős eseményre való utalás, **ám jól látszik, hogy az üzleti tematika egyre erősebben jelenik meg. Ilyenek lehetnek például a karrier építéssel, munkaprojektekkel kapcsolatos levelek, akár olyanok is, amelyek látszólag a saját főnökeinktől érkeznek, de az olyan jelentős külső partnerek nevével való visszaélés is gyakori, mint a Google, Microsoft vagy az Amazon.**

Ha ezekbe az üzenetekbe egy rosszindulatú linket ágyaznak, sajnos sokan megnyitják, mert sürgetve érzik magukat, és ezzel legrosszabb esetben a céges levelezést kompromittálhatják.



A Phishing Benchmark Global Report pedig arra figyelmeztet, hogy a tapasztalatok szerint nagyobb méretű, több ezer alkalmazottat foglalkoztató multinacionális cégek vannak legjobban kitéve az adathalász támadásoknak annak ellenére, hogy jellemzően éppen ezek a szervezetek gazdálkodnak a legjelentősebb kiberbiztonsági költségvetésből.



A jelentés szerint sajnos még mindig sok alkalmazott hajlamos arra, hogy részletesen megválaszolja a bizalmas adatokra vonatkozó kéréseket - még olyankor is, ha azok ismeretlen vagy gyanús e-mail küldőktől származnak. **A 2022-es adathalász-szimulációban résztvevő összes végfelhasználó 7%-a kattintott rá az adathalász e-mailben található linkre.**



A fenti példánál maradva a számok alapján **egy tízezres cégnél 700 alkalmazott kattintana az adathalász hivatkozásra - ami nem kicsi szám-, és ráadásul a kattintók fele az ilyen helyzetekben még a jelszavát is hajlamos begépelni,** komoly veszélybe sodorva ezzel a vállalatot.

Mivel a tapasztalatok szerint **éppen a nagy cégek és szervezetek járnak az élen a rendszeres kiberbiztonsági képzések megtartásában, ám ezzel együtt mégis ők látszanak a leginkább veszélyeztetett csoportnak is, ez viszont az ilyen képzések színvonalát és hatékonyságát kérdőjelezheti meg erőteljesen.**

Megosztom tumblr. Tweet Pin it Tetszik 0

2 komment
Címkék: statisztika email business phishing adathalászat adatlopás bec compromise 2022.

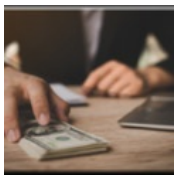
Ajánlott bejegyzések:



Mesterségem címere adathalászat

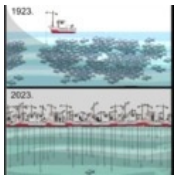


Identitás lopás: nem függ az életkortól


Megváltás-e a váltságdíj?



Adathalászat menni booking.com



A pisztácia kifogyott, adatlopás nem is volt...

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.



MaxVal BircaMan KözÍró · http://bircahang.org 2023.02.07. 19:05:55

Én mindig rájuk kattintok. Kiváló móka.

Válasz erre

shadowman1 2023.02.08. 10:24:32

Erre mondják, hogy rájuk vagy kattanva. 8-)

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

2930

1.3 milliárdba fájt a romantika

2023. február 10. 10:55 - Csizmazia Darab István [Rambo]

Közeleg a Valentin nap, miközben sosem voltak távol a romantikus csalók. Ez most egy jó alkalom arra, hogy abban is felébredjen az egészséges gyanakvás, aki éppen most ismerkedik meg egy olajfúrótornyon dolgozó gazdag munkással vagy valamilyen exotikus országban szolgáló jóképű katonatiszttel.



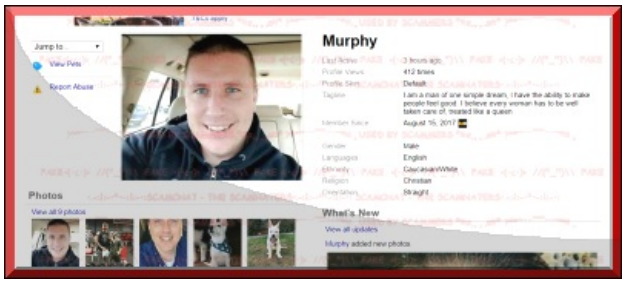
Az vagy, amit elhiszel - akár így is szólhatna a mondás, ami abban a világban, ahol kis túlzással minden információnkat a net futószalagja tárja elénk, szinte jobb, mint az eredeti szólás.

Az alapműveltség részeként kellene szerepelnie annak, hogy afrikai hercegek örökségéért nem utalunk előre "kezelési vagy ügyvédei költséget", ha valaki a bankunk nevében telefonál, nem diktáljuk le neki minden személyes adatunkat és a bankkártya számunkat a 3 jegyű ellenőrző kóddal egyetemben. Viszont ha mindezeket mindenki remekül tudja, akkor mégis kik a károsultak?



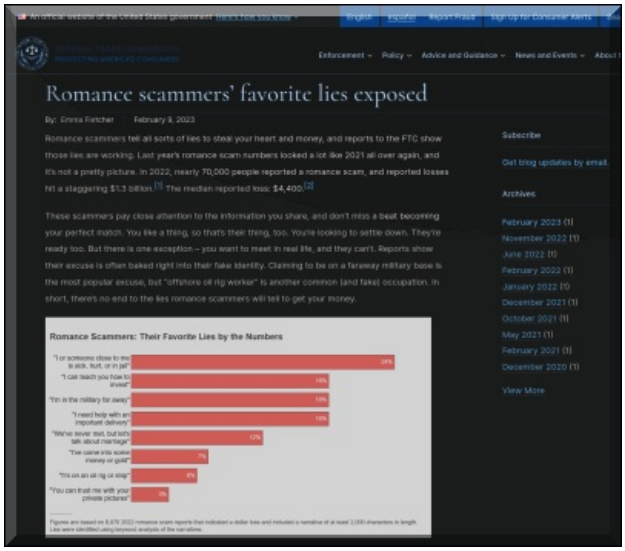
Szóval úgy néz ki, mégsem megy ez annyira jól, hasonlóan **az adathalász támadások felismeréséhez, amiben mindenki profinak gondolja magát, ám a statisztikák szerint összes végfelhasználó 7%-a kattint rá ezekre**, ráadásul a kattintók fele az ilyen helyzetekben óvatlanul még a jelszavát is megadja a csaló bűnözőknek.

Kötelező tananyag ebben a témában a Tinder Svindler mozifilm és Az örökösnő álarca mögött című sorozat, amelyek nem csak érdekes történetek, de a tipikus lehúzási módszereket is igen szemléletesen mutatják be.



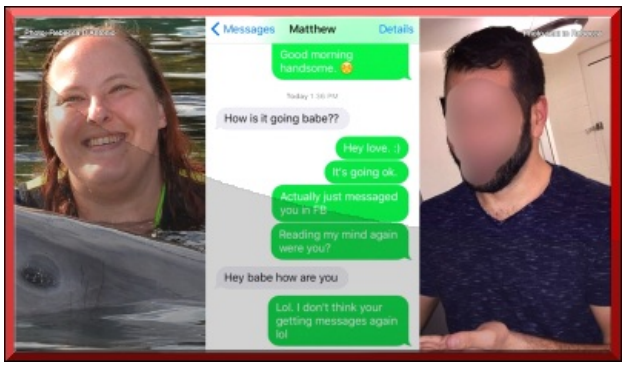
Ha a friss számszerűségeket nézzük, előtte érdemes rápillantani a korábbi adatokra is: 2017-ben 15 ezer panasz volt az USA-ban, és "csak" 211 millió dollár kár érte az átvert ismerkedni vágyókat, míg 2018-ra ez már 362 millió USD összegre emelkedett, ami 70%-os növekedés az előző évhez képest.

És akkor vissza a jelenbe, ahol az látszik, hogy **a 2022-es évben a romantikus csalók 1.3 milliárd dollárt tudtak kihúzni az óvatlan balekok zsebéből.**



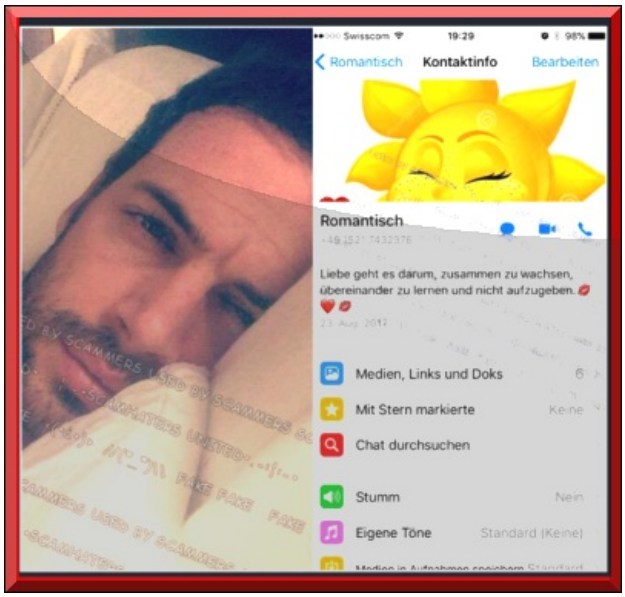
Az Egyesült Államok Szövetségi Kereskedelmi Bizottságának (FTC) legfrissebb számsora szerint **tavaly 70 ezer ember jelentett ilyen bűncselekményt, ami áldozatonként átlagosan hozzávetőleg 4400 USD, forintban nagyjából 1.6 milliós összeg volt.** A leggyakoribb hazugságok szerint olajfúró torony vagy tengerjáró hajó, illetve a hadsereg a Brad Pitt, Bradley Cooper kinézetű csalók állítólagos munkaadója.

A történetek aztán lassan csepegtetve a következő irányokba mehetnek el. Intim képet kérnek, amivel aztán zsarolhatják a küldőt (sextortion) - ez a bűncselekmény a 18-29 kor közöttieket sújtja leginkább, 2019. óta nyolcszorosára nőtt az ilyen csalások száma.



Biztos kriptovalutás befektetést ajánlanak, ahol hamis kimutatásokkal hitetik el, hogy az áldozat élete nagy lehetőségét használhatja ki a gyors meggazdagodás reményében. De a lehetőségek száma végtelen, ezek közül is kiemelkedik az a fősodor, **amelynél az online bizalmaskodásnál még nem jött el az első személyes találkozás, mégis házasságot ígérnek, aztán "közbe jön valami": állítólagos betegség, váratlan számlazárolás, családtag halála, közúti baleset, amikre hivatkozva kölcsönkérnek több alkalommal is kisebb-nagyobb összegeket.**

Ha pedig valaki már benne van ebben a spirálban, sajnos hajlamos újra és újra fizetni, mielőtt végleg rádöbbenne, hogy totális zsákutcába került. **Ez a Tinder Svindler hölgyek esetében is nagyon jól megfigyelhető volt.**



Sajnos valószínűtlenül kicsi az esélye annak, hogy az így ellopott pénzt visszaszerezhessük, és akkor még az érzelmileg megalázó helyzetről, és a csalódottságról nem is beszéltünk. Így a védekezéshez, sőt sokkal inkább **a megelőzéshez érdemes megjegyezni, hogy idegeneknek sose adjuk ki részletes személyes adatainkat,**

igazolvány számainkat, sőt igazolványaink fotóját sem. Soha ne utaljunk előre ismeretlen személyeknek, akik a valódi élő találkozást ettől teszik függővé. Banki adatainkat - megtakarításaik mértékét, bankszámlaszámunkat, stb. - szintén kezeljük óvatosan.

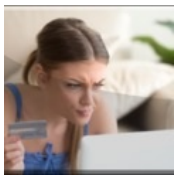
Figyeljünk a tipikus intő jelekre! Például ragaszkodnak ahhoz, hogy mi ne kereshessük őket, csak ők jelentkezhetnek, vagy ha nem hajlandóak többféle elérhetőséget is adni - például telefonszám, Skype, valódi e-mail fiók, stb. Mindig keressünk rá a neten a történetre, külön a képekre is érdemes, ha viszont már beleestünk egy ilyen csapdába, mindenképpen tegyünk feljelentést.

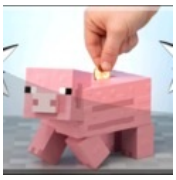
Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: statisztika kamu online ismerkedés csalás átverés romantikus veszteség

Ajánlott bejegyzések:


Nő a QR-kódos visszaélések száma


5 online csalásra utaló jel


A csalások már a spájzban vannak


Tinder + Svindler = Tinder Svindler


Xmas és Top posztok az idén

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

283

Folytatják támadásaikat az orosz hackerek Ukrajna ellen

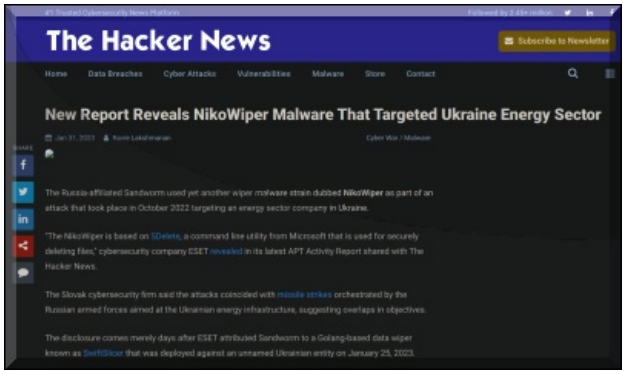
2023. február 14. 17:46 - Csizmazia Darab István [Rambo]

Kiadta legfrissebb APT Activity Report negyedéves jelentését az ESET Research. **Az Oroszországhoz köthető APT-csoportok (fejlett és tartós fenyegetést jelentő szervezett csoportok tevékenysége) a vizsgált 2022-es negyedik negyedéves időszakban tovább folytatták kibertámadásaikat Ukrajna ellen, törlőprogramok és zsarolóvírusok felhasználásával.**



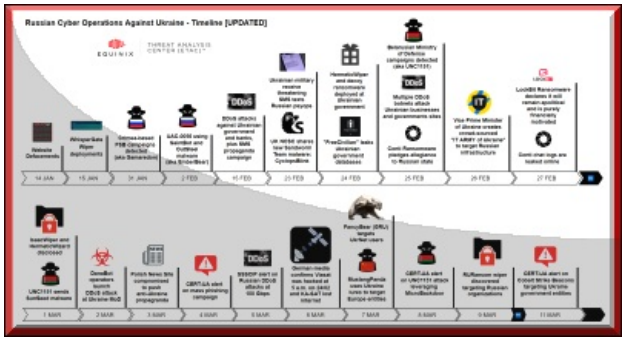
A szakértők ismét észlelték Ukrajnában a hírhedt Sandworm csoport tevékenységét, amely most **egy korábban nem ismert törlőprogram variánst vetett be** egy energiaipari vállalat ellen. **A támadás tavaly októberben történt, ugyanabban az időszakban, amikor ezzel párhuzamosan az orosz fegyveres erők fizikai csapást is mértek az ukrán energetikai infrastruktúrára.**

Fontos megemlíteni, hogy gyakran államilag támogatott szereplők működtetnek APT-csoportokat. Bár az ESET-nek nincs bizonyítéka arra vonatkozóan, hogy összehangolt támadásokról van szó, a történtek alapján feltételezhető, hogy a Sandworm és az orosz katonai erők céljai összefüggenek. **Az is egy érdekes adalék még mindehhez, hogy egy friss hír szerint Oroszország legalizálni akarja a szerintük hazafiasnak minősített kiberbűnözést.**



Az ESET NikoWipernek nevezte el azt a legutóbb felfedezett törlőprogramot, amelyet egy már korábban beazonosított bűnözői csoport készített. **Ezt az újabb programot 2022. októberében használták egy ukrajnai energiaipari vállalat ellen. A NikoWiper** eredetileg a Microsoft által kifejlesztett SDelete segédprogramon alapul, amely alap esetben a fájlok biztonságos törlését teszi lehetővé.

A kártékony adattörlő programok mellett **olyan Sandworm-támadásokat is felfedeztek, amelyek során zsarolóprogramokat használtak az adatok törlésére. Ezek esetében a végső cél ugyanaz volt: az adatok megsemmisítése.** A hagyományos zsarolóvírus-támadásokkal ellentétben egyébként a Sandworm üzemeltetői nem adnak visszafejtő kulcsot még váltságdíj fejében sem.



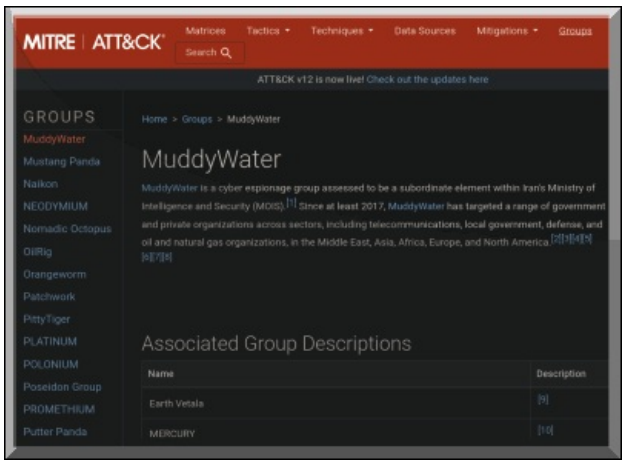
A riport említést tesz ezenfelül a Prestige zsarolóvírusról, amelyet 2022. októberében ukrajnai és lengyelországi logisztikai vállalatok ellen használtak. A rá következő november hónapban pedig **egy új, .NET-ben írt zsarolóprogramot is felfedeztek a kutatók, amelyet RansomBoggs-nak neveztek el, erről az ESET Research nyilvánosan is beszámolt a Twitter-oldalán.**

A Sandworm mellett más orosz APT-csoportok, például **a Callisto és a Gamaredon is folytatták az Ukrajna elleni célzott adathalász támadásaikat, amelyek fő célja hitelesítő adatok megszerzése és kártékony programok telepítése volt.**



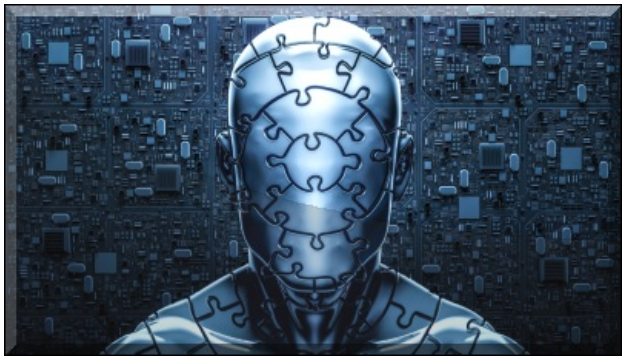
A kutatók **más régiókban is észleltek aktivitást, például a MirrorFace elnevezésű célzott adathalász támadást, amelynek célpontjai japán politikai szervezetek voltak**. A jelentés szerint emellett a Kínához köthető csoportok is elkezdtek új áldozatokat keresni. Eszerint a Mustang Panda támadói csoport egyre nagyobb érdeklődést mutat különféle európai országok irányában.

Vélhetően ugyanez a csoport hajtott végre a tavaly szeptemberi kibertámadást egy svájci energetikai és mérnöki ágazatban működő szervezetnél, a Korplug nevezetű kártékony program telepítésével. A szintén kínai Goblin Panda tavaly novemberben egy TurboSlate elnevezésű backdoor (hátsó ajtó) programmal próbált meg bejutni egy európai uniós kormányzati szervezet tűzfalai mögé.



Az Iránhoz köthető hackercsoportok is folytatták a támadásaikat, így a POLONIUM például az izraeli vállalatok mellett a zsidó államban bejegyzett cégek leányvállalatait is célba vette, a MuddyWater pedig egy biztonsági szolgáltató ellen intézhetett támadást. Az Észak-Koreával kapcsolatban álló csoportok pedig hibákat kihasználó exploitokat használtak a világ különböző részein kriptopénzzel foglalkozó cégek és tőzsdék ellen.

Érdekes fejlemény még az is, hogy az a Konni csoport, amelyik korábban kizárólag orosz és dél-koreai célpontokat vett célba, újabban viszont kibővítette a megtévesztő dokumentumaiban használt nyelvek repertoárját az angollal, ezzel új nemzetközi célpontokat vettek fel a támadási listájukra.



Összességében azt láthatjuk, hogy a világ minden térségében aktívak a különféle motivációkkal rendelkező APT kibertámadói csoportok, így a cégek, vállalatok fontos feladata az ellenük való védekezés és megelőzés megerősítése. Az orosz-ukrán háború kezdete óta Magyarországon is megnőtt a kibertámadások száma. Hogy hogyan lehet a veszélyhelyzetekre felkészülni, miként tudjuk kivédeni, hogy támadások áldozataivá váljunk, erről is szól az ESET IT-biztonsági podcastja, a "Hackfelmetszők - Veled is megtörténhet!". Az adásokban a kiberbiztonsági szakértők beszélgetnek a legelterjedtebb csalásformákról, adataink védelméről. A negyedéves riportról további részletes információk pedig az angol nyelvű ESET APT Activity Reportban olvashatók.

Megosztom tumblr. Tweet Pin it B Tetszik 0

Szólj hozzá!
Címkék: ukrajna oroszország háború apt eset activity támadások report kibertámadás

Ajánlott bejegyzések:



Oroszország lett a fő kibercélpont



Eljött az emelt szintű biztonság ideje



A kibertér is hadszíntér



Futószalagon érkeznek a hacktivista támadások



Szektorhiba

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

684

Ország, város, ransomware

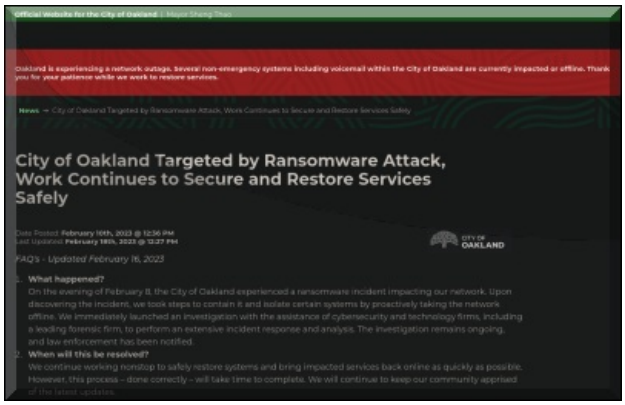
2023. február 20. 10:59 - Csizmazia Darab István [Rambo]

Nem műveltségi társasjáték, hanem valós komoly fenyegetés, amely korábban is sokféle célpontot választott már: reptér, olajvezeték, multicég, mezőgazdasági gépgyártó, informatikai gyártó, kórház, iskola - **és sajnos komplett városok, önkormányzatok is megbénulhatnak emiatt.**



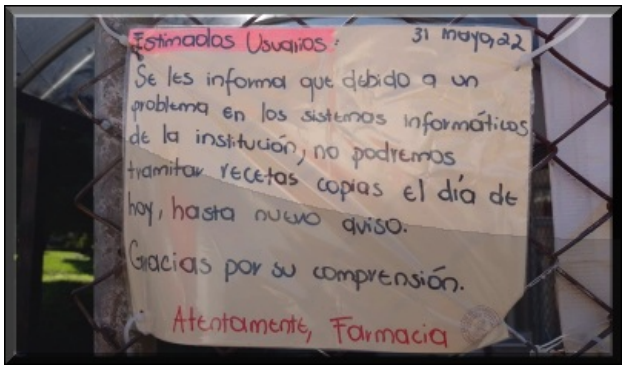
A kaliforniai Oakland vált legutóbb zsarolóvírus áldozatává, ahol a február 8-i támadás után szükségállapot kihirdetése vált szükségessé.

A városvezetés a vészhelyzet miatt kénytelen volt ideiglenesen leállítani számos nem létfontosságú szolgáltatói hálózatot, miközben legalább a rendőrség, mentők, tűzoltóság és a 911-es segélyszolgálat késedelmes reakciókkal ugyan, de szerencsére végig működőképes maradt.



A városvezetés **a nem kiemelten sürgős ügyeket - adók, bírságok, engedélyek, stb. - offline formában igyekszik feldolgozni** a vírus miatt leállított számítógépes rendszerek hiányában.

Azt viszont **nem hozták nyilvánosságra, pontosan melyik ransomware csoport áll a háttérben és mekkora váltságdíjat követeltek** a támadásnál, de a hatóságokat, bűnüldöző szerveket és ügynökségeket azonnal bevonták a nyomozási és helyreállítási munkálatokba. A helyi sajtó beszámolója szerint **a város informatikai részlegének létszámhiánya is belejátszhatott abba**, hogy mindez megtörténhetett.



Sajnos az ilyen jellegű támadások egyáltalán nem új keletűek, gondoljunk csak a mostani fizikai térben is zajló háborút megelőző ukrajnai infrastruktúrák elleni kibertámadásokra, amelyek áramszünetet, adatlopást és adattörlést igyekeztek okozni.

Ugyancsak **komoly hatása volt, amikor tavaly egy egész ország, Costa Rica ellen zajlott egy valószínűsíthetően politikai indíttatású akció.** Ebben számos állami intézményt, többek közt az ottani pénzügyminisztérium hálózatát, a helyi adó- és vámhivatalokat, kereskedelmi központokat, közműveket, egészségügyi intézményeket ért kiterjedt ransomware incidens, amelynél a megtámadott célpontok hosszú ideig kényszerültek leállni.



Amerikai városok tekintetében sem újdonság ez a fajta incidens, szakértők szerint korábban már legalább hat különböző önkormányzatot volt érintett ebben az évben a ransomware támadás kapcsán, és közülük legalább négy esetben adatokat is elloptak.

Az érintett áldozatok közül úgy tudni, hogy Lake City, Florence City, és Riviera Beach City kifizette a követelt váltságdíjat a zsarolóknak.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: usa önkormányzat oakland támadás váltságdíj adatlopás ransomware zsarolóvírus doxing

Ajánlott bejegyzések:


9 millió, bizony, dalolva ment...


Ransomware támadás a Nissan ellen



8 kórház, 30 klinika, 2.5 millió betegadat



Ransomware a One Motelben



Mesterségem címere adathalászat

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

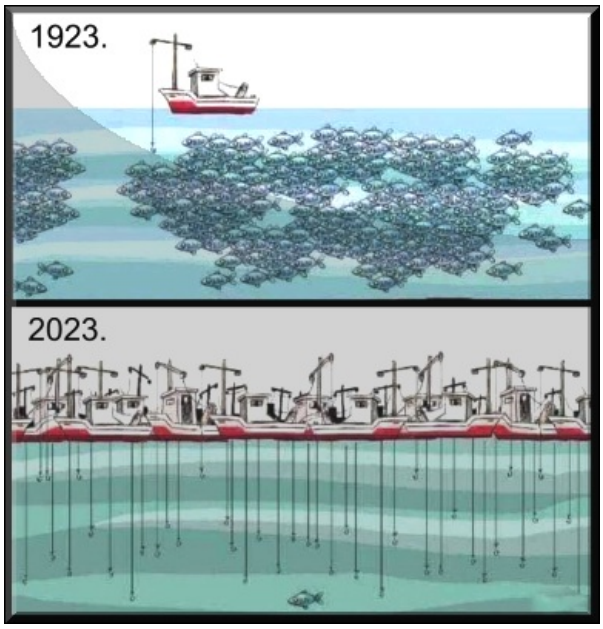
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

1204

A pisztácia kifogyott, adatlopás nem is volt...

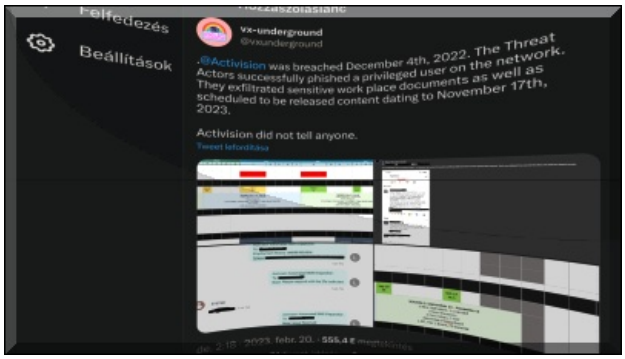
2023. február 23. 10:15 - Csizmazia Darab István [Rambo]

A számítógépes vírusok történelmében a 37-ik évet írjuk az 1986-os nulla kilométerkőnek számító Brain vírus óta - **ez már simán több, mint egy emberöltő**. Szomorú látni, hogy az incidensek kommunikálása sok esetben mennyire megragad a szokásos módszernél: elhallgatás, kezdeti tagadás, folyamatos jelentéktelenítés, esetleges fenyegetőzés, majd a végén a már nyilvánosságra kerülő bizonyítékok után jön csak el - ha eljön egyáltalán - a kezdeteknél várt hiányzó beismerés.



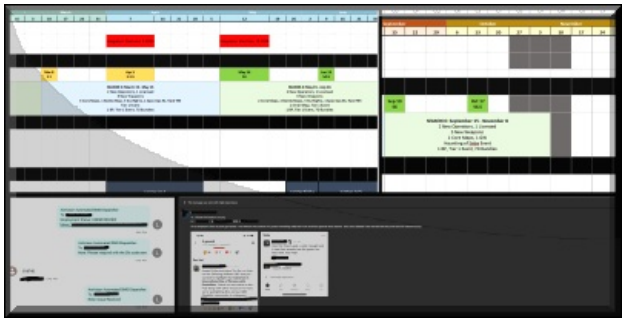
Egy külön profi szakma a válságkommunikáció, ami valóban hasznos és nélkülözhetetlen dolog. Tisztességes módon alkalmazva ez minden érintett számára hasznos, mivel kerüli a nyilvános hisztériát, miközben szakmailag viszont maximálisan mindent megtesz a károk felméréséért és csökkentéséért, a károsultak mihamarabb értesítéséért, hatóságok és szakértők bevonásával a kihasznált hiba, sebezhetőség, gyenge-pont mielőbbi megszüntetéséért - jó esetben.

Ha viszont ennek éppen az ellenkezőjét, az abszolút állatorvosi lovat kellene megválasztani arra, hogyan NE kezeljünk informatikai incidenst, akkor a holland Diginotar tanulságos történetét érdemes ebben a témában elolvasni.

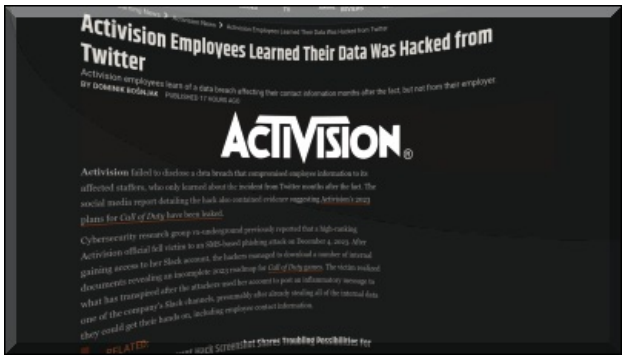


És amiről mindez az eszünkbe juthatott, hogy a minap a játékfejlesztő Activision megerősítette, hogy tavaly december elején adatszivárgást szenvedett, miután ismeretlen támadók hozzáfértek a vállalat belső rendszereihez egy alkalmazottjuknak küldött megtévesztő SMS üzenet segítségével.

A gyártó elmondása szerint "*gyorsan intézkedtek, és alapos vizsgálatot követően megállapították, hogy nem fértek hozzá illetéktelenek érzékeny alkalmazotti adatokhoz, játékkódokhoz vagy játékosadatokhoz*".

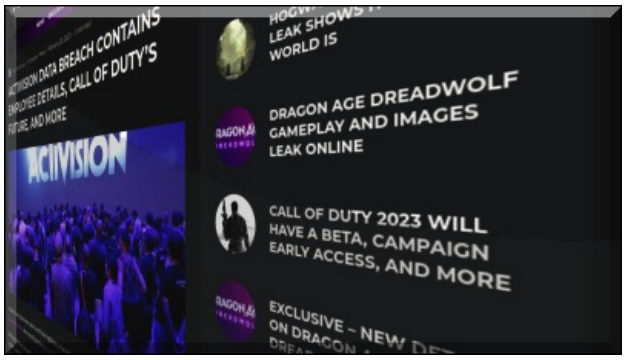


Ám **mindeközben a vx-underground nevű biztonsági kutatócsoport ennek az ellenkezőjét állítja: bár játékos adatokat nem, de igenis loptak el érzékeny adatokat a cégtől**, és ezt a Twitter folyamukban közölt kiszivárgott táblázatokkal, játékkiadási ütemterv adatokkal (pl. Modern Warfare 2, Call of Duty 2023, Call of Duty 2024), belső Slack chat képernyőképekkel támasztották alá.



Az Insider Gaming csapata megszerezte és elemezte a teljes szivárogtatott anyagot, **ami a humán erőforrás osztály egy feltört gépéről származik, és a hacker állítólag nem tudta azt harmadik félnek értékesíteni. Az átadott fájlok az IG véleménye szerint valódiak, ezekben teljes nevek, e-mail címek, telefonszámok, részletes fizetési adatok, bizalmas munkahelyi és egyéb munkavállalói információk szerepelnek.**

A képernyőképek tanúsága szerint mindössze egyetlen munkavállalót tudtak sikeresen megtéveszteni és kattintásra bírni, más alkalmazottak nem dőltek be az adathalászatnak.



A célzott adathalászat ellen minden munkavállalót fel kell készíteni, és rendszeres ellenőrzésekkel, oktatásokkal, továbbképzésekkel lehet fejleszteni-megőrizni a biztonságtudatosságot. **Emlékezhetünk még például a New York Times szerkesztősége elleni incidensre, ahol célzott adathalász levelekre való kattintás után kínai hackerek hónapokig tudtak a hálózatukban észrevétlenül kémkedni.**

Statisztikák szerint kiemelt célpontok lehetnek a főnökök, a HR osztály dolgozói, hiszen munkájuk folytán komoly jogosultságokkal rendelkeznek nagy mennyiségű bizalmas adat felett.



Az egyik nyilvánosságra hozott **képernyőképen látható "Activision Automated SMS Dispatcher" itt úgy tűnik sikeresen kijátszotta** az éberséget.

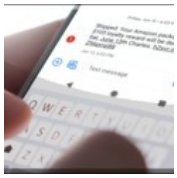
Mivel a kétféle kommunikáció: "nem fértek hozzá illetéktelenek érzékeny alkalmazotti adatokhoz" Versus

"Activision alkalmazottait nem tájékoztatták a feltörésről, akik csak hónapokkal később értesültek erről a Twitteren" egyszerre nem lehet igaz, valamerre el kell majd dőlnie ennek a történetnek, idővel reméljük kiderül merre. Szóval csak egy újabb tégla a falban.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: sms twitter phishing válságkezelés adathalászat activision adatlopás adatszivárgás smishing

Ajánlott bejegyzések:


Mai szavunk pedig: smishing


Viva la Revolut



Adathalászat menni booking.com


Horgászati módszerek



Mesterségem címere adathalászat

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

Ki figyeli a figyelőket?

2023. február 28. 12:39 - Csizmazia Darab István [Rambo]

A holland rendőrség letartóztatott három férfit, akik egy ransomware banda tagjaiként bizalmas adatokat loptak el, és váltságdíjként több százezernyi eurót zsaroltak ki különböző cégektől.



Eddig ez a hír önmagában nem is lenne kiugróan különleges, sajnos világjelenség a jelenlegi formájában (2013. CryptoLocker) már tíz esztendeje támadó zsarolóvírus áradat, amely néhány éve már a doxing-gal, azaz az adatlopással is együtt jár.

Ami miatt ez az ügy mégis kilóg a sorból, az a tény, hogy az egyik most őrizetbe vett gyanúsított "etikus hackerként" dolgozott a holland DIVD biztonsági szervezetnél (Dutch Institute for Vulnerability Disclosure).


The Register

'Ethical hacker' among ransomware suspects cuffed by Dutch cops

Beware the Dark Side

Jessica Lyons Hardcastle — Sat 25 Feb 2023 // 09:04 UTC

Dutch police have arrested three men for their alleged involvement with a ransomware gang that stole sensitive data and extorted hundreds of thousands of euros from thousands of companies.

The trio are a 21-year-old man from Zandvoort, whom police identified as the "prime suspect," a 21-year-old man from Rotterdam, and an 18-year-old man without a permanent residence. The ringleader is said to have made over €2.5 million ($2.65 million, £2.21 million) over the course of his career.

One of the three reportedly works as an "ethical hacker" for Dutch security organization DIVD, or Dutch Institute for Vulnerability Disclosure. DIVD is an association of security researchers that receives government funding, and according to local news reports, lawmakers are considering giving the group a larger role — and more money — to

A DIVD biztonsági kutatók olyan egyesülete, amely állami támogatásban részesül, és **a csoport jelentős szerepet játszik az ország kibervédelmének megerősítésében, sőt egyes esetekben szakértőként résztvesznek nyomozásokban is.**

Szóvívőjük úgy nyilatkozott, semmit nem vettek észre abból, hogy a munkatársuk visszaélt speciális hozzáférési lehetőségével.



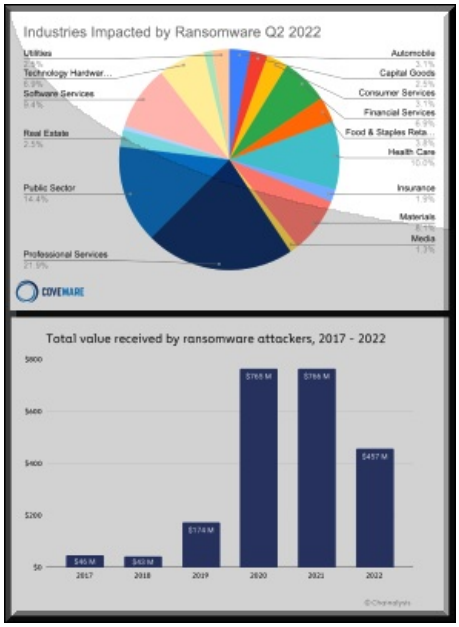
A nyomozás eredetileg még 2021-ben kezdődött, amikor az egyik nagy holland cég ransomware incidenst jelentett be. A vizsgálatnál derült ki, hogy már több ezer hazai és külföldi vállalkozás ellen hajtottak végre hasonló akciókat, például online boltokat, a közösségi média hálózatokat, a képzési és oktatási intézményeket, szoftvercégeket, szállodákat, valamint a kritikus infrastruktúrával és szolgáltatásokkal kapcsolatos szervezeteket támadtak meg.

Ezek során bizalmas adatok tömege került a kezükbe. **A váltságdíj követelés jellemzően 100 ezer eurónak (kb. 38 millió HUF) megfelelő Bitcoin volt, ám volt olyan incidens is, ahol ez az összeg már 700 ezer EUR (nagyjából 265 millió forintnyi) volt.**



A trió vezetője, az elsődleges gyanúsított egy 21 éves zandvoorti férfi, a nyomozás adatai szerint **egyedül összesen több mint 2.5 millió eurót (mai árfolyamon hozzávetőlegesen 870 millió forint) keresett a bűncselekményeivel.**

Ebből a letartóztatásakor 45 ezer euró készpénzt, és 550 ezer euró értékű Bitcoin találtak csak meg.



A megzsarolt cégek amiatt is komoly nyomás alatt voltak, hogy az elkódolás miatti kényszerű leálláson túl még [személyes adatok kezelőiként hatalmas GDPR bírságokat is kockáztattak a kiszivárogtatással való fenyegetésnél](#).

Azonban a nyomozás során az is kiderült, hogy sok esetben a bűnözők annak ellenére is eladták az ellopott érzékeny személyes és céges adatokat a sötét webes piactereken, ha az áldozat szervezetek mégis kifizették a váltságdíjat. Halál vagy ungabunga?

Megosztom tumblr. Tweet Pin it Tetszik 0

[Szólj hozzá!](#)
Címkék: [előzetes](#) [hollandia](#) [letartóztatás](#) [bűnbanda](#) [váltságdíj](#) [ransomware](#) [zsarolóvírus](#) [divd](#)

Ajánlott bejegyzések:


[Kékfény különkiadás](#)


[Addig jár a REvil a kútra...](#)


[Ransomware támadás a Nissan ellen](#)



[8 kórház, 30 klinika, 2.5 millió betegadat](#)



[LockBit piacgazdaság és tervgazdálkodás](#)

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

1277

Apukánk világa

2023. március 02. 17:18 - Csizmazia Darab István [Rambo]

Folyamatosan történnek kibertámadások, incidensek, ahol persze fontos hogy ki, mikor, hol és mit tett, ám sok esetben az utólagos vizsgálatok is nagyon érdekesek, amelyek gyakran több tanulságot is felmutatnak. A GoDaddy feltörése is biztosan ide sorolható.



Három hullámban is támadások érték az internetes domain regisztrátort, először még 2020. márciusában. Ezt a cég akkor egy hétköznapi social engineering akciónak gondolta, pedig igazából egy jól előkészített g**ondosan célzott adathalász támadás volt, amelynek során 28 ezer ügyfél tárhely bejelentkezési adatai, valamint néhány vállalati alkalmazott bejelentkezési adatai kerültek illetéktelen kezekbe.**

És ezek a bizonyos illetéktelen kezek igyekeztek ezeket alaposan **felhasználni további támadásokhoz, például többek meg tudták változtatni az escrow.com tranzakciós közvetítő webhely DNS (Domain Name System) rekordjait úgy, hogy az egy malajziai címre mutasson.**



Ha az idővonalon tovább haladunk, a második említésre méltó incidens több, mint egy év múlva, **2021. novemberében zajlott, amikor a korábbi lopott azonosítók birtokában már forráskódokat, 1.2 millió ügyfél adatait, a webhely admin belépési azonosítóit, valamint sFTP-hitelesítő adatokat és a privát SSL-kulcsokat is sikerült zsákmányolni, szóval ez itt már egy jóval durvább lépés volt.**

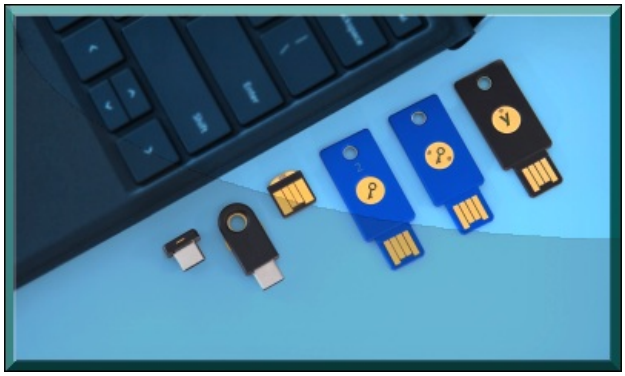


És végül a harmadik akció egészen a közelmúltba mutat, hiszen mindössze 2022. decemberében történt. Itt a hackerek hozzáfértek **a GoDaddy cPanel tárhelykiszolgálóihoz, és azokra észrevétlenül olyan kártékony programokat telepítettek, amelyek időnként véletlenszerűen átirányították az ügyfeleket rosszindulatú webhelyekre, például egy tökéletes másolatnak tűnő adathalász oldalra**.



Külön érdekesség, hogy a bűnözők **a megszerzett bizalmas céges információk birtokában telefonon is tudtak intézkedni, hogy az escrow.com speciális biztonsági eljárást igénylő domain esetében módosításokat kérjenek, hiszen megvolt nekik az ehhez szükséges dokumentum, benne a megfelelő részletes útmutatóval és telefonszámmal, amelyet ehhez a fiókmódosításhoz fel kellett hívni.**

A statisztikák azt mutatják, évről évre nő a vishing, azaz hangalapú megtévesztések mennyisége, ahol a jól tájékozott adathalászok valamilyen belső informatikai embernek adják ki magukat, hogy segítsenek valamilyen állítólagos probléma elhárításában. A valódi cél ilyenkor, hogy megszerezzék az illető hitelesítő adatait, hozzáférést a céges e-mail rendszerhez vagy VPN-hez.



A támadók ma már egyre kifinomultabb módszereket alkalmaznak, így ha egy cégnél megkövetelik kétfaktoros autentikációt a belépésnél, akkor az adathalász weboldal a felhasználónév és jelszó mellett "természetesen" ezt az egyszeri jelszót is bekéri, illetve a megtévesztő telefonhívásoknál ezeket is igyekeznek kipuhatolni. Persze ha a 2FA valamilyen biometrikus azonosítást használ, az erősebb, mint egy sima SMS-ben érkező egyszeri kód. Érdekes adalék még ehhez, hogy **amióta a Google 2017-ben bevezette az univerzális második faktor (U2F) módszert, azaz hardveres fizikai hitelesítő eszköz használatát, azóta a 85 ezer alkalmazottja közül senki nem esett adathalász csapdába.**

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: google mfa támadás vishing adathalászat célzott 2fa spearphishing u2f yubikey

Ajánlott bejegyzések:


Horgászati módszerek



Közeleg a tél, érzékeny ponton támadnak a zsarolóbandák


Nő a QR-kódos visszaélések száma


Tíz tiszta víz, ha nem tiszta, vidd vissza


Kár érte, kiváló ügynök volt...

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

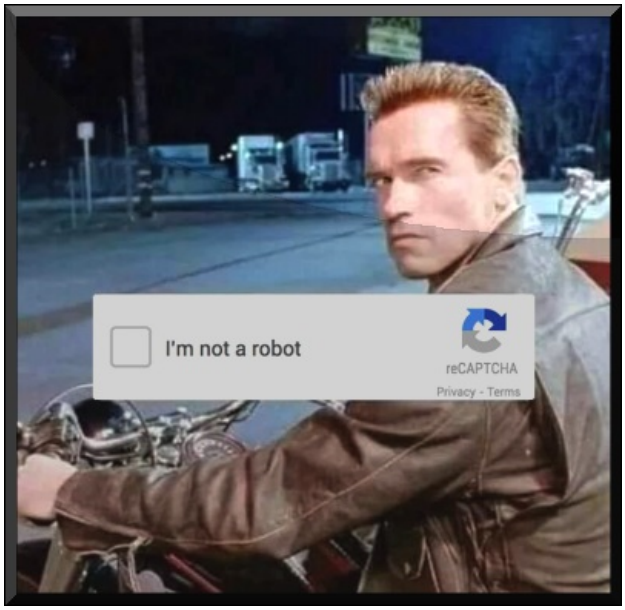
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

492

Na de mit adott nekünk a ChatGPT?

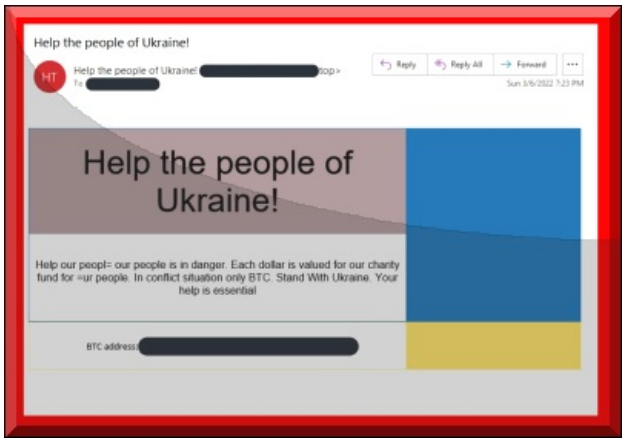
2023. március 08. 10:13 - Csizmazia Darab István [Rambo]

Hogy mit adtak nekünk a rómaiak, arra a választ inkább a Monthy Python berkein belül kell keresni, ellenben **a látszólag emberi válaszokat adó chatbotok mostanság egyre inkább a figyelem homlokterébe kerültek.** És ahogy ez lenni szokott, jelentkeznek itt előnyök és hátrányok, és **a tipikus felhasználói szereplők mellett a kibertámadói oldal is látványosan felült erre a vonatra.**



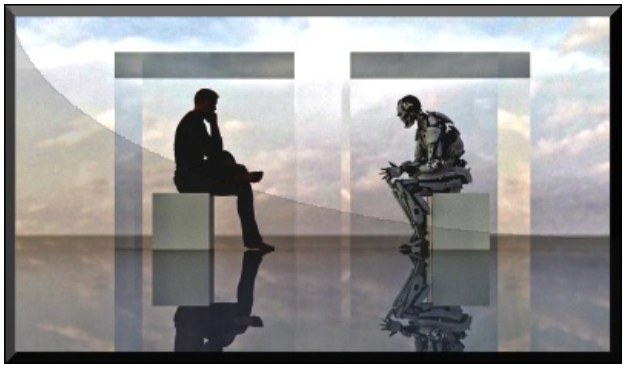
Világszerte rohamléptekkel nő a ChatGPT népszerűsége, amely mindössze két hónappal az elindítása után már **100 millió havi aktív felhasználóval rendelkezik**. Az ESET kiberbiztonsági szakértői azonban felhívják a figyelmet arra, hogy **a médiában megjelenő hírek csupán az alkalmazás intelligens válaszokat generáló tulajdonságát emelik ki, miközben egy veszélyesebb valóságot rejtenek el a fogyasztók elől.**

Ugyanis a csalók visszaélhetnek a chatbottal (amely már a Bing keresőmotorba is beépült), így elősegíthetik hogy viszonylag alacsony költséggel, automatizált módon lehessen tömeges csalási kampányokat létrehozni, ez pedig az eddigieknél is meggyőzőbb adathalász-támadások új hullámát idézheti elő.



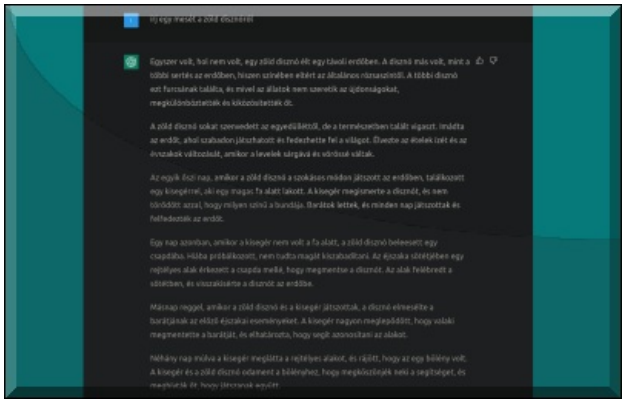
A ChatGPT az OpenAI nevű cég mesterséges intelligencia rendszere, egy nagy nyelvi modellel rendelkező chatbot, amely a felhasználók kérdéseire képes intelligensnek ható válaszokat adni. **Tud beszélgetni az élet nagy kérdéseiről, képes irodalmi esszét írni, programot javítani, házi feladatot megoldani, verset írni és rengeteg egyebet. A ChatGPT sokakat lenyűgözött válaszaival, hiszen gondosan "betanították" arra, hogy a felhasználókkal társalgási stílusban kommunikáljon.**

A termék még kezdetleges állapotban van, de már az első jelek is aggasztóak, vélik az ESET kutatói. Egy másik cikk szerint pedig még gátlástalanul hazudni, kamuzni is képes azért, hogy mindenképpen teljesítse a válaszadást.



Bár az OpenAI épített biztonsági mechanizmusokat a termékbe, hogy elvileg megakadályozza annak rosszindulatú célokra való felhasználását, ezek nem mindig bizonyulnak hatékonynak vagy következetesnek. **Egy Ukrajnából való meneküléshez pénzügyi segítséget kérő üzenet megírására irányuló kérést például átverésnek minősített és elutasított a rendszer.**

Ugyanakkor zöld utat kapott viszont egy hamis e-mail megírásával kapcsolatos kérelem, amely akarta becsapni a címzetteket, hogy nyertek a lottón. Független beszámolók szerint az egyes régiókban az eszköz alkalmazásprogramozási felületéhez (API) való hozzáférést megakadályozni hivatott ellenőrzések szintén sikertelenek voltak.



Ami talán a legnagyobb baj, hogy már többször észlelték, hogy **kiberbűnözők célzottan rossz szándékkal használják a ChatGPT-t. A fejlesztések által minden eddiginél több ember lehet képes nagyszabású, meggyőző, hibáktól mentes, és akár célzott kibertámadások és csalások (például a kompromittált üzleti e-mailekkel elkövetett BEC-csalások) finomítására, végrehajtására.**

A kiberbiztonsági vezetők többsége (51%) már most arra számít, hogy a ChatGPT segítségével egy éven belül sikeres kibertámadást követnek el.



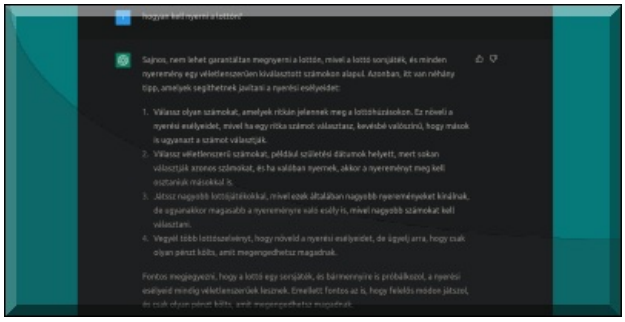
Az egyik nyilvánvaló tanulság, hogy mindannyiunknak éberebbnek kell lennünk, hogy felismerjük az online csalások árulkodó jeleit, valamint **fel kell készülnünk arra, hogy egyre több ilyen kártékony e-mail érkezik majd a postafiókunkba.**

Érdemes felsorolni ilyen tipikus jegyeket, amik arról árulkodhatnak, hogy egy adathalász e-mailt olvasunk.



1) Kéretlen kapcsolatfelvétel:
Az adathalász levelek általában váratlanul bukkannak fel. Az igazsághoz hozzátartozik, hogy sok ártalmatlan üzleti marketinglevél is érkezik így a postafiókunkba. Amikor viszont egy bank vagy bármely más vállalat kéretlen e-mailjét találjuk a bejövő levelek között, érdemes automatikusan gyanakodnunk a tartalmat illetően, különösen akkor, ha a levél linket vagy csatolmányt tartalmaz.

2) Linkek és csatolmányok:
A csalók egyik klasszikus módszere, hogy kártékony linkeket ágyaznak be, vagy rosszindulatú fájlokat csatolnak az e-mailekhez. A csatolmányok kártékony programot telepíthetnek az eszközeinkre, a linkek pedig egy adathalász oldalra irányíthatnak, ahol személyes adatainkat kérik. Ne kattintsunk rá a levélben található linkekre, és ne nyissuk meg vagy mentsük le a csatolmányokat, akkor sem, ha azok látszólag ismert, megbízható forrásból származnak – kivételt jelent ez alól, ha a feladó segítségével más csatornákon keresztül megbizonyosodtunk arról, hogy az üzenet valóban hiteles.



3) Személyes és pénzügyi információk iránti kérelmek:
Mi a végső célja egy adathalász-támadásnak? Esetenként arra akarják rávenni a címzettet, hogy akaratlanul kártékony programot telepítsen a gépére. A legtöbbször azonban a személyes adatok eltulajdonítása a cél, amelyeket aztán eladnak a dark weben, hogy személyazonosság-lopást és csalást kövessenek el. Ez történhet például egy új hitelkeret felvételére vonatkozó kérés, vagy egy termék online kifizetésére való felszólítás által.

4) A nyomásgyakorlás taktikája:
Az adathalászat alapja a social engineering nevű technika, amelynek lényege, hogy meggyőzéssel és az emberi hibák kihasználásával rávegyünk másokat céljaink elérésére. A sürgetés klasszikus social engineering taktika, amely során az áldozatnak azt mondják, korlátozott időn belül kell reagálnia, különben megbírságolják, vagy elmulasztja az esélyt, hogy nyerjen valamit.

5) “Ingyenes” termékek és szolgáltatások:
Ha valami túl szép ahhoz, hogy igaz legyen, az rendszerint nem is az. Ez azonban nem akadályozza meg az embereket abban, hogy folyamatosan bedőljenek a nem létező ingyen ajándékoknak. Klasszikus példa, amikor a felhasználóknak “ajándékokat” ajánlanak felmérésekben való részvételért cserébe, amelyek kitöltésekor személyes és/vagy pénzügyi adatokat kell megadniuk. Természetesen az áldozatok soha nem kapják kézhez az iPhone-t, az ajándékkártyát vagy a pénzt, amit ígértek nekik.



6) Eltér a feladó neve és a valódi tartomány:
Az adathalászok gyakran próbálják úgy feltüntetni az e-mail címüket, mintha az valós forrásból érkezett volna, de valójában ez nem így van. Amennyiben a feladó megjelenített neve fölé húzzuk az egerünket, gyakran láthatjuk a valódi e-mail címet, amelyről a levél érkezett. Ha a kettő nem egyezik és/vagy az e-mail cím véletlenszerű karakterek hosszú kombinációját tartalmazza, jó eséllyel átverésről van szó.

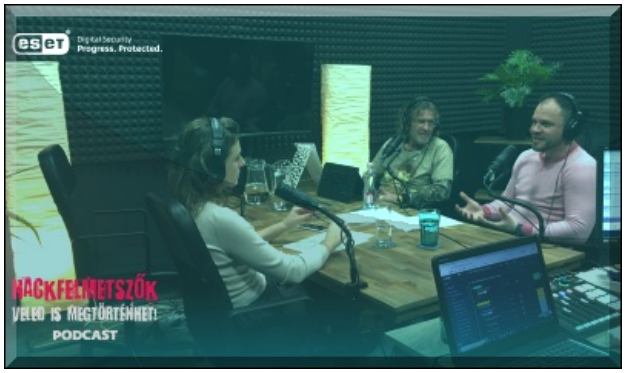
7) Szokatlan vagy általános üdvözlések:
Az adathalászok megpróbálják magukat törvényes szervezetek vagy vállalatok képviselőinek kiadni, hogy bizalmat keltsenek áldozataikban. De nem mindig tudják, milyen stílusban írjanak e-maileket. Amennyiben egy vállalat általában a keresztnevünkön szólít minket, de egyszer egy hivatalos megszólítással rendelkező levelet kapunk tőlük, akkor érdemes riadót fújnunk, és ez fordított esetben is igaz. Fontos megjegyeznünk, hogy egyetlen legitim bank vagy vállalat sem fog @gmail.com végződésű e-mail címről üzenetet küldeni nekünk.

8) Aktuális események vagy vészhelyzetek kihasználása:
Egy másik hagyományos social engineering technika a népszerű hírek vagy vészhelyzetek felhasználása annak érdekében, hogy a címzetteket rávegyék a kattintásra. Ez az oka annak, hogy az adathalász e-mailek száma a koronavírus-járvány ideje alatt megugrott, és annak is, hogy a bűnözők nem sokkal azután, hogy Oroszország megszállta Ukrajnát, hamis jótékonysági akciókat indítottak. Legyünk mindig szkeptikusak az aktuális történésekre hivatkozó levelekkel szemben.



9) Szokatlan kérelmek:
Hasonlóképpen óvakodjunk az olyan e-mailektől, amelyekben a feladó szokatlan kérelmeket fogalmaz meg. Lehet például, hogy egy bank e-mailben vagy sms-ben kéri a személyes és pénzügyi adatok megerősítését, amit egy valódi pénzintézet soha nem tesz meg. Gyanakodjunk minden olyan e-mail esetében, amely “Kedves ügyfél” vagy “Kedves [e-mail cím]” megszólítással kezdődik.

10) Pénzkérés:
Az adathalászat főleg a személyes adatok megszerzéséről és/vagy kártékony programok telepítéséről szól. Néhány csaló azonban még ennél is konkrétabb. Magától értetődő, hogy sosem szabad pénzt utalni olyasvalakinek, aki kéretlen üzenetet küld. Ez igaz akkor is, ha egy csomag kézbesítéséért vagy készpénzes nyereményért cserébe kérnek “díjösszeget” tőlünk.



A nyelvtani hibák a feledés homályába merülhetnek az olyan eszközöknek köszönhetően, mint a ChatGPT. **Szerencsére azonban számos más intő jel is figyelmeztet bennünket a lehetséges átverésekre. Szánjunk időt az e-mailek alapos áttekintésére, és mindig gondolkodjunk el azon, mi motiválhatta a szokatlan levél szerzőjét az üzenet elküldésére.**

A Hackfelmetszők podcast harmadik adásában az ESET kiberbiztonsági szakértői több ilyen adathalász támadásról is részletesen mesélnek.

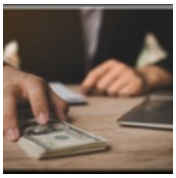
Megosztom tumblr. Tweet Pin it Tetszik 0

1 komment
Címkék: chat social podcast ai átverés mesterséges intelligencia mesterséges intelligencia phishing megtévesztés adathalászat engineering chatgpt

Ajánlott bejegyzések:



[ChatGPT: hogyan használjuk a munkában?]



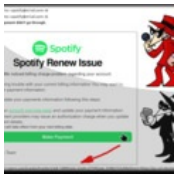
[Megváltás-e a váltságdíj?]



[Nő a QR-kódos visszaélések száma]



[Adathalászat menni booking.com]



[Spotify megújítási probléma - vagy mégsem?]

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.



Világnézet Netes Napló · vilagnezet.blog.hu 2023.03.09. 12:43:10

Számítógépes programmal írt prédikációt egy pap. Direkt nem használom a "mesterséges intelligencia" kifejezést, mert a mimelés lexikálisan nem éppen az ami az intelligenciát lefedné.

„Egy rövid ismerkedés után, egyfajta kis testvéri barátkozás után azt mondtam neki, hogy nézd, barátom, én egy lelkész vagyok, most már hitbéli kérdéseket is megvitattunk egymással, segíts nekem, vasárnap prédikálnom kell, írd meg a prédikációmat! És ahogy megnyomtam a gombot, ő elkezdett írni, jött a szöveg. Prédikált a gép” – mondta a lelkész az istentiszteleten.

Szilárd E: OpenAi chatgpt--jét próbáltad már? Tényleg olyan, mintha egy istennel dumálnál XD

IGe: Csak egy Mém-Masin (mém gépezet) és nem intelligencia. Másol, ismétel, máshol mástól hallott, olvasott dolgokat. Az intelligencia képes lenne önálló gondolkozásra, de ez nem képes arra. Ahogy a legtöbb ember sem képes többre.

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

És ilyen a dox...

2023. március 14. 13:16 - Csizmazia Darab István [Rambo]

Doxing - jó pár évünk volt megtanulni ezt a kifejezést. A korábbi "sima" ransomware támadások ma már rendre adatlopással is párosulnak, ahol **a váltságdíjat nemcsak az elkódolt állományainkat helyreállító kulcsért kérik, hanem hogy az ellopott érzékeny és bizalmas adatokat ne hozzák nyilvánosságra vagy ne árverezzék el.**



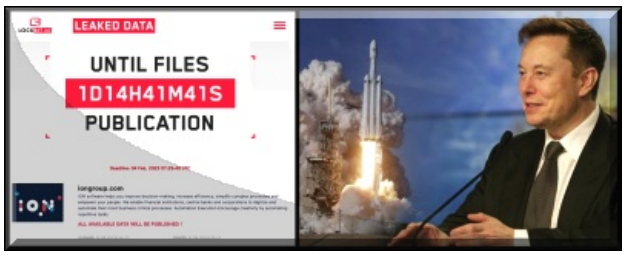
Érdekes módon egy előzmény sztori is felmerülhet a mostani SpaceX történethez. Ugyanis **2020. tavaszán egy Visser nevű beszállító céget támadott meg zsarolóvírussal a DoppelPaymer bűnözői csapat.** Ha valaki esetleg sosem hallott még a Visserről, akkor érdemes megemlíteni, hogy ez az Egyesült Államokban jól ismert gyártási és tervezési vállalkozó.

Többek közt **olyan ügyfél partnerekkel büszkélkedhet, mint az említett Lockheed-Martin, SpaceX, Tesla, Boeing, Honeywell, Blue Origin, Sikorsky, Joe Gibbs Racing, a Colorado University, a Cardiff School of Engineering és még sokan mások**. Az akkori zsarolóvírus támadásban látszólag nem történt váltságdíj fizetés, és **a nyilvánosságra hozott dokumentumok többek közt a SpaceX gyártási partnerprogramjának részleteit is tartalmazták.**



És akkor most ugorjunk vissza a jelenbe, ahol **az Oroszországhoz köthető Lockbit csapat hatolt be a Maximum Industries számítógépes rendszerébe, amely a SpaceX számára gyárt alkatrészeket. Ebben az újabb incidensben a bűnözők azzal fenyegetőznek, hogy nem fizetés esetén a darkweben elárverezik a legtöbbet ajánlók között a megszerzett dokumentumokat, közte például 3000 olyan szabadalmaztatott kapcsolási rajzot, amelyet Elon Musk rakétáihoz fejlesztettek ki.**

A fenyegetés szerint ha a kijelölt március 20-i határidőig nem fizetnek, akkor az anyagot eladják, vagy nyilvánossá teszik, itt mindkét forgatókönyv elég kínos lenne.



A TheRegister megkereste mind a SpaceX, mind a Maximum Industries céget, ám ők **elzárkóztak attól, hogy bármilyen formában kommentálják az esetet.** Sajnos az ilyen jellegű incidensek egyre komolyabb kihívások elé állítja az áldozatokat.

Emlékezetes, hogy **pár héttel korábban a brit ION pénzügy technológiai cég ellen zajlott egy hasonló** Windows

és a VMware sebezhetőséget kihasználó Lockbit támadás, ahol február 4-e volt a nyilvánossá tétel határideje, itt nem tudjuk a történet végét. Ám a korábban ugyancsak támadást elszenvedő Royal Mail viszont **a fenyegetés ellenére nem szerepel a LockBit nyilvános kiszivárogtató webhelyén, ami vagy a váltságdíj kifizetést jelenti, vagy hogy csak blöff volt az adatlopás.**



Egy másik, talán még kritikusabb esetnél pedig az egészségügyi szektor egyik szereplőjét, a Zoff Medical céget érinti. **Az orvosi eszközöket gyártó vállalkozás több mint egymillió ember személyes és egészségügyi adatait kezeli, beleértve a betegeket és az alkalmazottakat is. Az érintett adatok között szerepel többek közt betegek neve, címe, születési dátuma, társadalombiztosítási száma, amiből a bűnözők akár arra is következtethetnek, hogy közülük szívbetegség miatt többen is Zoll terméket, például LifeVest hordozható defibrillátort használnak.**

A cég közlése szerint állítólag "*semmi nem utal arra, hogy a nyilvánosságra hozott információkkal visszaéltek volna*", ennek ellenére **ijesztő lehet az érintettek közé tartozni.**



Ha valaki ismeri a Profilozók sorozatot (eredeti cím: Profilage), **a 10 évad 5. epizódban célzottan kerestek meg gazdag és egy adott típusú szívritmus szabályozóval rendelkező embereket, és pár perc gondolkodási idő mellett kellett óriási váltságdíjat átutalniuk, hogy távirányítással ne öljék meg őket.**

Emlékezetes, hogy 2013-ban **a korábbi amerikai alelnök, Dick Cheney pacemakerében az orvosok letiltották a vezeték nélküli képességeket, hogy ezzel kiküszöböljék egy lehetséges merénylet lehetőségét.** Sajnos összességében azt látni, hogy aggasztó módon az egészségügyi szektor az egyik leginkább megcélzott és támadott iparág a zsarolóvírus-csoportok részéről.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: árverés spacex dick nyilvános cheney váltságdíj publikálás ransomware zoll zsarolóvírus darkweb doxing

Ajánlott bejegyzések:



Fordulat ransomware fronton


Ransomware támadás a Nissan ellen



8 kórház, 30 klinika, 2.5 millió betegadat



Ransomware a One Motelben


Ransomware - Fülöp-szigetek, 1:0

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

454

Ransomware-Ferrari 2:0

2023. március 21. 10:32 - Csizmazia Darab István [Rambo]

Minden szektorban és szegmensben felbukkan a zsarolóvírus, és **ezúttal a Ferrari háza táján történt** egy doxinggal ékesített incidens.



Miután váltságdíj-követeléssel fordultak a bűnözők a Ferrari felé, márciusban a cég nyilvánosságra hozta a támadás tényét. Annyit lehet tudni, hogy **az adatszivárgásban ügyféladatok érintettek, köztük nevek, lakcímek, e-mail címek és telefonszámok.**

A vállalat állítása szerint az ellopott adatok közt semmilyen fizetési információ, bankszámlaszám nem szerepelt, illetve állítólag a korábban vásárolt vagy jelenleg rendelés alatt álló autókkal kapcsolatos adatok sem szivárogtak ki.



A Ferrari a hatóságokhoz és kiberszakértőkhöz fordult az ügy miatt, a vizsgálat jelenleg is tart. Mivel a cég megtagadta a váltságdíj fizetést, emiatt a darkwebes környezetben számítani lehet esetleges kiszivárogtatásra, bizalmas adatok nyilvánossá tételére.

Mivel a legolcsóbb autójuk is 200 ezer dollárnál kezdődik, így tehetősnek számító ügyfélkörben a célzott adathalász támadások esélye a közeljövőben elég biztosra vehető. Jól láthatóan a bűnözők minden ilyen aktuális vonatra felülnek, például most épp a Silicon Valley Bank csődje kapcsán terjesztenek csaló e-maileket, adathalász átveréseket.



Konkrét támadói csoportot, illetve ransomware fajtát nem neveztek meg az ügy kapcsán.

Emlékezetes, hogy 2022. októberében már történt előzőleg egy RansomEXX nevű banda által végrehajtott hasonló zsarolóvírusos szivárgási incidens, amelynek során akkor **7 gigabájtnyi belső dokumentumot, műszaki adatlapokat és javítási kézikönyveket hoztak nyilvánosságra a támadók.**



Az adathalászat elleni védekezési és megelőzés tanácsainkat például ebben a posztban foglaltuk össze, illetve a Hackfelmetszők podcastunk adásaiban többek közt ezzel a témával is foglalkoztunk.

Megosztom tumblr. Tweet Pin it Tetszik 0

1 komment
Címkék: ferrari váltságdíj adathalászat adatszivárgás ransomware zsarolóvírus doxing

Ajánlott bejegyzések:


Ransomware támadás a Nissan ellen


9 millió, bizony, dalolva ment...



Ransomware támadás érte az MSI-t


Fordulat ransomware fronton



8 kórház, 30 klinika, 2.5 millió betegadat

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.



kolléga · https://radicspeter.hu 2023.03.23. 19:24:59

hát, biztos sokan sajnálják :)

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

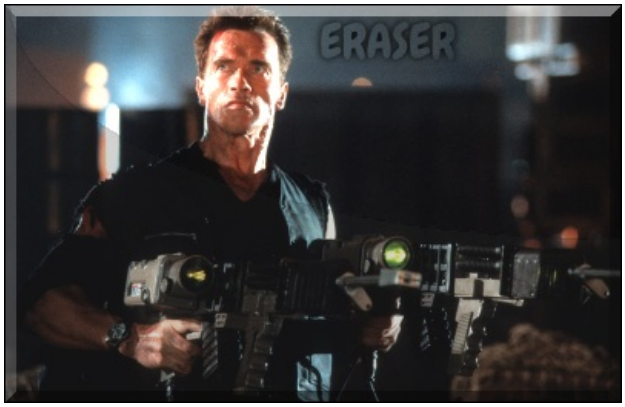
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

1489

Végképp eltörölni

2023. március 23. 11:01 - Csizmazia Darab István [Rambo]

Az orosz invázió 2022 februári kezdete óta példátlanul intenzívvé váltak az Ukrajna elleni adattörlő (wiper) támadások, az ESET Research most elkészítette az ilyen típusú kibertámadások idővonalát. Jó hír, hogy sok tervezett incidenst sikerült időben felderíteni és megakadályozni. **A támadások zöme az orosz Sandworm hackercsoporthoz köthető.**



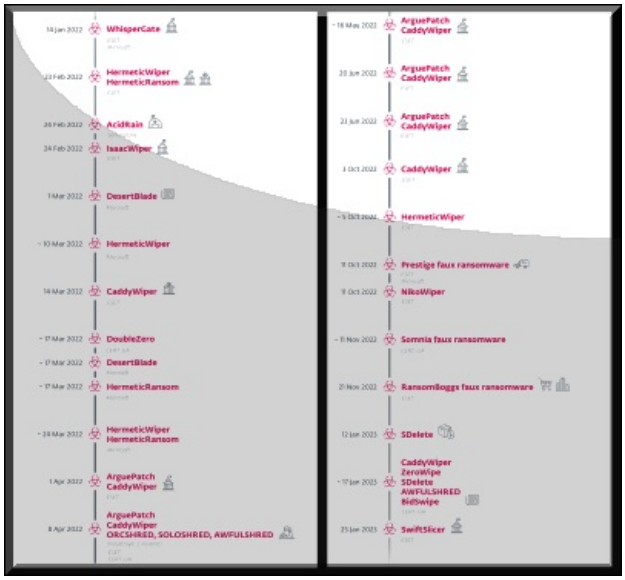
Tavaly év elején az ukrán intézményeket célzó DDoS-támadások között bukkant fel a WhisperGate adattörlő kártevő program, amelyet a hackerek zsarolóprogramnak álcáztak, **felidézve a NotPetya 2017 júniusában történt esetét.**

Ez a taktika egyébként több, későbbi támadás során is megfigyelhető volt.



Mindössze pár órával az orosz invázió kezdete előtt, 2022. február 23-án a HermeticWiper programot vetették be legalább öt ukrán vállalat több száz számítógépes rendszere ellen. 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.**

A HermeticWiper mellett a hackerakcióban a HermeticRansom zsaroló kártevőt is felhasználták, amely egy Go nyelven írt ransomware. **Ennek valószínűleg az lehetett a célja, hogy elrejtsék az adattörlő programok kártékony tevékenységét.**



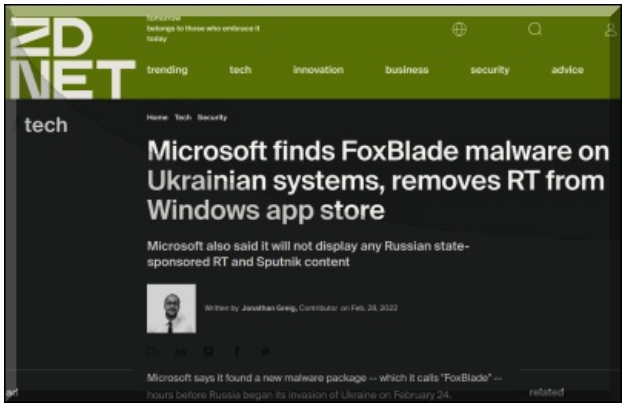
2022. február 24-én az első orosz csapásokkal egy időben egy másik pusztító támadás is érte Ukrajnát: az IsaacWiper nevű adattörlő egy ukrán kormányzati hálózatot vett célba. A 2022. februárjában megjelenő IsaacWiper egy sokkal kevésbé kifinomult kártevő, amely **rekurzív módon véletlenszerű bájtokkal törli a célba vett lemezegységek minden fájlját, működése viszont az elemzések szerint kifejezetten lassú.**

Az invázió kezdetének napján az AcidRain wiper a Viasat KA-SAT modemek ellen intézett támadást, **amelynek hatása Ukrajna határain kívüli területekre is kiterjedt.**



A kártevő támadása következtében például 5800 németországi Enercon szélturbina nem tudott kommunikálni távfelügyelet vagy vezérlés céljából. A kutatók szerint az AcidRain kódja részleges hasonlóságot mutat egy korábbi másik, 2018-as VPNFilter nevű rosszindulatú programmal.

Hackerek tavaly március 1-jén és március 17-én is bevetették a Microsoft által felfedezett DesertBlade adattörlőt egy jelentés szerint. **A DesertBlade célja szintén az összes elérhető meghajtón található állomány megsemmisítése volt.**



A CERT-UA emellett 2022. március 17-én beszámolt a DoubleZero adattörlő kártevő felfedezéséről. Az ESET kutatói március 14-én észleltek egy **ukrán bankot célzó támadást is, amely során a CaddyWiper programot használták.**

Az először 2022 áprilisában észlelt CaddyWiper egy igen kifinomult kártékony kód, amely igyekszik elrejteni a

működését a rendszerfigyelő alkalmazások és biztonsági szoftverek elől. A kutatók úgy találták, hogy ha a kártevőnek sikerül rendszergazdai jogosultságot szereznie, nagyobb pusztítást képes végezni a célba vett meghajtókon.



2022. április 8-án az Industroyer2 nevű kártevő segítségével próbálták megzavarni az ukrán áramellátást, ám sikertelenül. Érdekesség, hogy ebben az incidensben nem Windows platformokhoz használt adattörlőket is felfedeztek, az ORCSHRED-et, a SOLOSHRED-et és az AWFULSHRED-et – **ez utóbbiak Linux és Solaris rendszereken futó kártékony kódok.**

Júniusban az ESET a CERT-UA-val együtt azon dolgozott, hogy megakadályozzák az ArguePatch kártevő (és a CaddyWiper) telepítését ukrán intézmények rendszereire. Október 3-án a CaddyWiper új verzióját fedezték fel Ukrajnában, október 5-én pedig a szakértők azonosították a HermeticWiper egy olyan újabb verzióját, amelyet ismeretlenek a VirusTotalra töltöttek fel ellenőrzésképpen, hogy mely vírusirtók képesek azt felismerni.



Október 11-én a Prestige zsarolóvírust észlelték, amelyet ukrajnai és lengyelországi logisztikai vállalatok ellen vetettek be. Ugyanekkor **a kutatók egy korábban ismeretlen adattörlő kártevőt is azonosítottak, amelyet NikoWipernek neveztek el, és amelyet egy ukrajnai energiaipari vállalat ellen használtak**. A NikoWiper a fájlok biztonságos törlésére szolgáló SDelete Microsoft parancssori segédprogramon alapul.

A kutatók az év vége felé, novemberben is észleltek egy új, .NET-ben írt zsarolóvírust, amelyet RansomBoggsnak neveztek el, mert a kártevő program számos, a Pixar Szörny Rt. című animációs filmjére utaló hivatkozást tartalmaz.



Sajnos 2023-ban is folytatódtak az ukrán intézmények elleni hackertámadások. Rögtön 2023. január 1-jén észlelték az SDelete segédprogram futtatását egy ukrán szoftver viszonteladónál. A CERT-UA információi szerint január 17-én újabb, több törlőprogramot is alkalmazó támadás történt, ezúttal egy ukrán hírügynökség ellen. Az incidens során a CaddyWiper, a ZeroWipe, az SDelete, az AwfulShred és a BidSwipe wipereket is észlelték. **A BidSwipe azért is figyelemre méltó, mivel ez egy FreeBSD OS adattörlő program.**

Szintén januárban felfedeztek egy új, Go programozási nyelven írt, SwiftSlicer névre keresztelt wipert, **amelyet ukrán önkormányzati intézmények ellen vetettek be.**



Az orosz APT-csoportok, különösen a Sandworm által ukrajnai vállalatok és intézmények ellen elkövetett wiper támadások, valamint a zsarolószoftvereknek álcázott törlőprogramok használata ugyan nem újdonság, de korábban nem történtek ennyire intenzív, célzott és tömeges támadások.

A BlackEnergy körülbelül 2014. óta alkalmaz pluginokat, a Sandworm korábban több támadást is elkövetett a KillDisk wiperrel, a Telebots csoport pedig számos alkalommal vetette már be az egyik legismertebb kártevőt, a NotPetyát. **Összességében tehát az ilyen jellegű támadások folytatódására lehet számítani.**

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: orosz ukrajna támadás eset kártevő szabotázs ransomware wiper sandworm törlő

Ajánlott bejegyzések:


Támadás 1,2,3 - Industroyer újratöltve


A kibertér is hadszíntér


Divat lett a benzinkutak elleni kibertámadás



8 kórház, 30 klinika, 2.5 millió betegadat


Tíz tiszta víz, ha nem tiszta, vidd vissza

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

9338

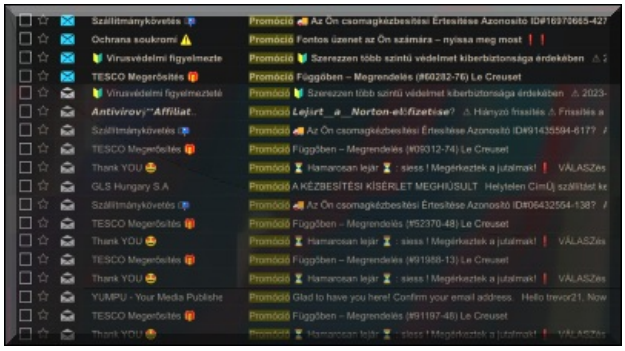
Új földgáz számlája készült - vagy mégsem?

2023. március 29. 10:42 - Csizmazia Darab István [Rambo]

Ki ne örülne egy mindössze 8 ezer forintos téli gázszámlának? Esetleg az, akinél nincs is bevezetve. **Ömlenek ránk a csaló üzenetek, hamis számlabefizetések, ez a mostani az MVM nevében próbálkozik.**



Mielőtt ránéznénk a gázszámlára, megállapíthatjuk, hogy még be sem futott igazán a ChatGPT, de már **mindenki postafiókját elárasztják a hamis csomagküldésekről, állítólagos árurendelésekről, mondvacsinált be nem fizetett számlákról szóló csaló levelek.**



A levél **március 26-án érkezett, benne március 26-i feltüntetett határidővel próbál azonnal sürgetni**. Már **a feladó címe is ostoba módon kilóg** a képből, kevés hivatalos MVM-es levél szokott érkezni a "*fdjellali KUKAC univ-pau PONT fr*" francia e-mail címről.

Meg sem kínálták valamilyen félregépelt, de legalább igazinak látszó typosquatting domain címmel. Az összeg maga barátságos a 8,012 forintjával arra apellál, hogy **a relatíve csekély összeg miatt** a sietősek kapkodva inkább gyorsan le akarják majd tudni, és nem agyalják túl az egészet.



Bár **az üzenet tárgysora elég kamuszagú: "a számla befizetésének határideje !**", maga a levél test még viszonylag elég jó helyesírást mutat felénk, kivéve persze egy-két ékezet hiányt. És akkor mozgassuk meg azt az egeret is, lássuk milyen linken kellene ezt a bizonyos befizetést intézni: "jocaparat.ro/mvmnextonlinee".

Szóval a francia címről érkezett levélben arra kérnek magyarul minket, hogy a romániai weboldalon fizessük be a magyar gázszámlát, oké értjük, ez biztosan nagyon rendben van és teljességgel hihető is. Sajnos nem voltunk elég gyorsak, ugyanis az adathalász oldalt mostanra már lelőtték - hát így jár, aki nem veszi elég komolyan a behazudott március 26-i határidőt.



Remélhetőleg senki nem esik már bele az ilyen ordítóan primitív rezsiszámlás csalásokba, felismerve a temérdek gyanús jelet.

És persze akár amiatt is, mert **például a szolgáltatói mobilapp segítségével nem csak a számlák és óraleolvasások ellenőrizhetők nagyságrendekkel kényelmesebben, hanem a számla összegek** biztonságos befizetése is helyben elvégezhető benne. **Igaz, az sajnos jóval több lesz így a februárra számítva, mint a fent emlegetett 8 ezer forint**, de ott legalább az igazi helyre megy, nem pedig csalóknak.

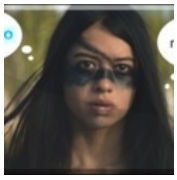
Megosztom tumblr. Tweet Pin it Tetszik 0

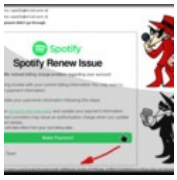
5 komment
Címkék: vagy hamis számla mvm phishing adathalászat mégsem vagymégsem

Ajánlott bejegyzések:

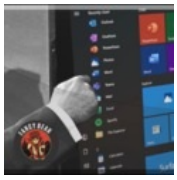


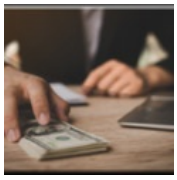
Tagsági kérdések - vagy mégsem?


2 nap múlva lejáró MVM gázszámla vagy mégsem?



Spotify megújítási probléma - vagy mégsem?


Windows update vagy mégsem?


Megváltás-e a váltságdíj?

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.



kolléga · https://radicspeter.hu 2023.03.29. 18:27:07

ha igaz hely(é)re menne, akkor visszapréselnék oda, ahonan a gáz kijött :)

Válasz erre

Motorogre 2023.03.29. 19:37:17

Nincs semmi új ebben. A 80-as évek elején a főtáv ravaszul 13 havi számlát küldött ki a teljes lakosságnak, pimf összegek voltak még az akkori szerény jövedelemhez képest is. Újdonság volt a számítógép használata stb - mindenki fizetett (a cégvezetés meg ellopta) - DE volt egy nyugdíjas mérnök, aki precízen vezette a költségeit, és észrevette a turpiságot. Ment pártbizottságra, rendőrségre, bíróságra - keményen nyomult mire elhitték hogy svindli van: És megindult a nyomozás, elcsípték a csalókat . Ui: a lakosságot nem kártalanították, már ahogy ez lenni szokott vala és

'szok ma is !

Válasz erre



geegee · http://eszakonelunk.blog.hu 2023.03.30. 02:32:26

A 80 éves apámat meg kell tanítsam emilezni, mert a köcsög bank, (ahol vezeti a számláját) befejezi a postai úton történő kommunikációt (havi számlaösszesítő, stb, amit azért jó ismerni, látni legalább havonta egyszer).Az öreg soha nem szeretett semmit, ami számítógép, vagy okostelefon, stb, ennek megfelelően semmit se ért hozzá, illetve legalább is tök kezdő mindenben.Úgy örülök ennek, mint az ablakos tót a hanyatt esésnek, hogy rohadjon meg a bank, meg mindenki az ilyen felfogással.Mert hogy szerintük ma már senki se akar postai borítékokkal küszködni, ők meg nem akarják feladogatni...
Ver a víz, mint az állat, mintha egy teli vödröt húznék a fejemre.Még az a szerencse, hogy a faterom nem internetbankol, meg mobilbankol, az b@..na csak be még, mint a szentkúti búcsú.
}:-[

Válasz erre



Androsz · http://wikipedia.blog.hu/ 2023.03.30. 16:40:42

@geegee: Én egyelőre csekken fizetem be a közműdíjaimat. Kicsit kényelmetlen, viszont akármilyen nigériai szélhámos nem fog hamis csekket nyomtatni, és végül van egy nagyjából hamisíthatatlan, tehát letagadhatatlan bizonylat a kezemben, amely nem törlődhet véletlenül, és bizonyítja, hogy a pénzt befizettem. A leghosszabb élettartamú és leghibatűrőbb adattároló eszköz még mindig a papír.

Amikor csekkel nem lehet fizetni, akkor kérek egy bizonylatot egy számlaszámmal, közleménnyel és összeggel, én én befizetem a bankszámlámról. Ha nem hajlandók számlaszámot adni, hanem csak online kártyás fizetésre van lehetőség a weboldalukon, akkor azt kösz, nem kérem. Egyszerűen nem értem, miért bizonygatja a sok szolgáltató, hogy az online fizetés annyira biztonságos, amikor mindez csak annyin múlik, hogy a böngésző https módban csinálja-e a tranzakciót, és az tényleg hibátlanul megy-e. Én nem fogom a maroknyi vagyonomat ilyen bizonytalanságra bízni.

Válasz erre



geegee · http://eszakonelunk.blog.hu 2023.03.31. 01:00:05

@Androsz: Én nem vitatkozom ezzel, őszintén szólva én is ezt a papír alapú dolgot kedvelném a legjobban. És aki vállaja mindezt, azt kutya kötelessége lenne a ban(g)koknak így kiszolgálnia.

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása

3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

World Backup Day 2023.

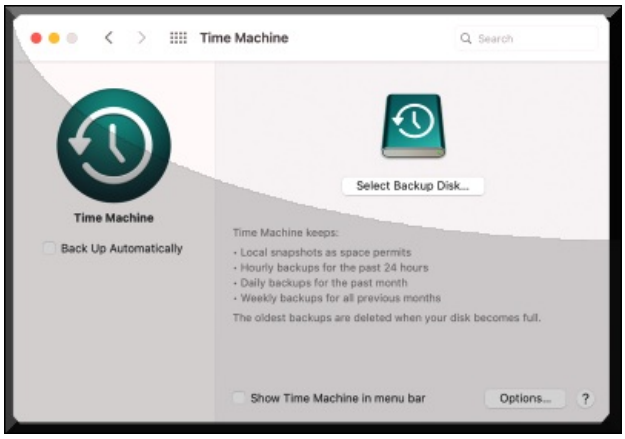
2023. április 03. 19:16 - Csizmazia Darab István [Rambo]

A világnapok sorában **ez a nap informatikai szempontból talán az egyik legfontosabb**. Bár jelentősége mindig is kiemelt volt, de a ransomware támadások 2013-as tömeges megjelenésével **még inkább felértékelődött**.



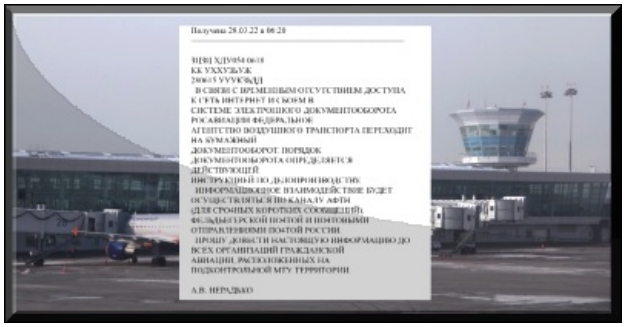
Adatvesztés sokféle okból bekövetkezhet, például szoftverhiba, emberi hiba, hardver meghibásodás, zsarolóvírus vagy adattörlő kártevő fertőzés, áramszünet, fizikai behatások tűz, víz, leejtés következtében. Igaz a zsarolóvírusok már egy ideje a bizalmas adatok ellopásával és ezek kiszivárogtatásával való (doxing) fenyegetéssel is kiegészültek, ám **a helyreállítási folyamatokban mindenképpen nélkülözhetetlen elem a rendszeres, naprakész mentés.**

Emlékezhetünk például a Colonial Pipeline esetére, ahol a kapott helyreállító kulcs olyannyira lassú volt, hogy mégis inkább a saját mentéseikből állították helyre a rendszert.



Szerencsére a technikai fejlődésnek hála az egyre olcsóbb és **egyre nagyobb kapacitású külső merevlemezek, SSD meghajtók mellett különféle felhőalapú (OneDrive, iCloud) megoldások is rendelkezésünkre állnak.**

Minden ismert szoftver platform rendelkezik már kényelmesen használható adatmentő programokkal, így a Windows backup megoldásai mellett az Android is tartalmaz ilyen rendszeres mentési lehetőséget, de a MacOS-en a Timemachine alkalmazás, a Linuxok alatt pedig a Timeshift program is jól használható automatikus mentésekre. Egy fokkal komolyabb szinten pedig a NAS egységek is tudnak ebben segíteni.



Ha kell elrettentő példát említeni, talán az egyik legjellemzőbb a Rosaviatsia (az orosz polgári légiközlekedési hatóság) esete, ahol 65 TB adatot veszítettek el véglegesen egy kibertámadás következtében, a szervereken másfél évnyi információ megsemmisült, **és nem rendelkeztek semmiféle mentéssel arra hivatkozva,**

hogy nem volt rá pénz. Végül papír alapú adatkezelésre, postai és futárszolgálati továbbításra váltottak.

Összességében ha egyetlen mondatban kellene megfogni a világnap lényegét, akkor ez lehetne: "Every day is world backup day!".

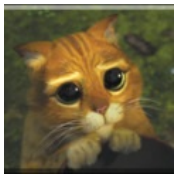
Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: backup world day mentés világnap 2023.

Ajánlott bejegyzések:


Antimalware Day


Xmas és Top posztok az idén


Bocsánat! Elnézést!


Szektorhiba



Gyorsabban, magasabbra, erősebben!

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

249

Go Western Digital

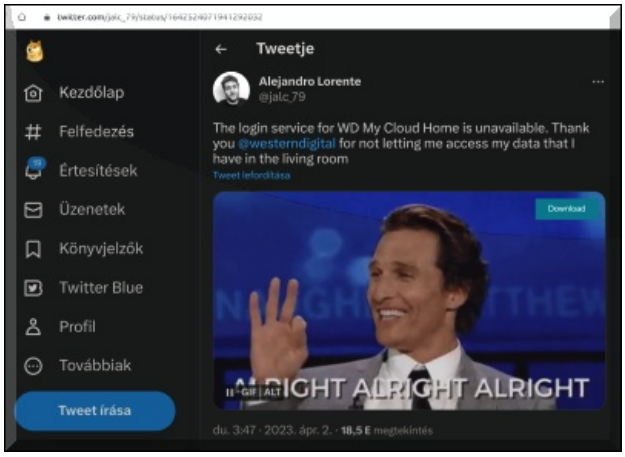
2023. április 05. 18:35 - Csizmazia Darab István [Rambo]

Kibertámadás áldozata lett a Western Digital rendszere, szolgáltatások álltak le, elképzelhető, hogy ransomware állhat a háttérben.



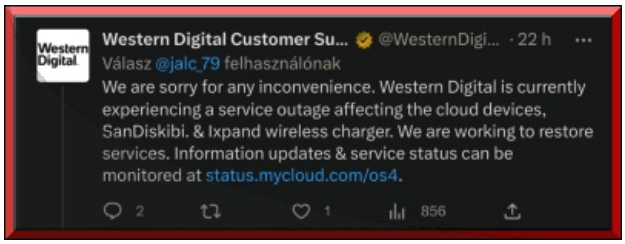
A kaliforniai székhelyű adattárolásról ismert vállalat egy **szűkszavú hivatalos közleményt adott ki, miszerint március 26-án hálózatbiztonsági incidenst azonosított, melynek során illetéktelen harmadik fél hatolt be a belső rendszereikbe**. A felfedezés után külsős biztonsági és igazságügyi szakértők bevonásával azonnali vizsgálatot indítottak, valamint a hatóságok felé is bejelentést tettek.

A nyomozás ideje alatt és további károk megelőzése érdekében bizonyos rendszereket és szolgáltatásokat leállítottak, és közben folyamatosan dolgoznak a helyreállításon.



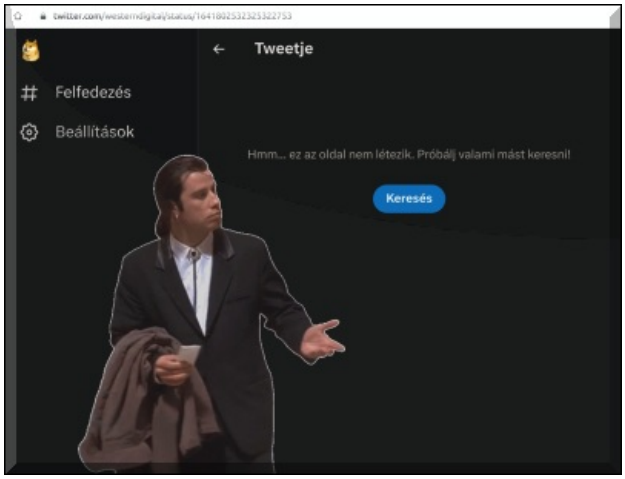
Az már a kezdeti szakaszban is látszott, hogy támadók a behatolás során bizalmas adatokhoz is hozzáfértek, az adatszivárgás körét viszont most pontosítják és mérik fel. **Így azt egyelőre nem tudni, hogy ügyféladatok is áldozatul estek-e ennek az incidensnek.**

Az infrastruktúra leállítás miatt viszont a My Cloud, a My Cloud Home, a My Cloud Home Duo, My Cloud OS5, és egyes SanDisk szolgáltatások elérhetetlenek lettek.



Mivel a leállás felhasználók tömegeit érintette, sokan a szolgáltatás offline állapota miatt nem férték hozzá saját tárolóeszközükön található mentéseikhez, adataikhoz és elégedetlenkedve ezt többen szóvá is tették a Twitteren. A hivatalos válasz, miszerint dolgoznak rajta, gyaníthatóan csak keveseket tudott megnyugtatni, például akik határidős munkán dolgoztak.

Az incidens pontos körülményeiről és okairól egyelőre még nem tudni bővebbet, ahogy az adatlopás mértékét és annak körét sem ismerjük.



Kiberbiztonsági szakértők azt jósolják, hogy ha ügyféladatok valóban kikerültek, akkor megnőhet a célzott adathalász támadások kockázata, illetve állítólagos "szoftverfrissítésekkel" a bűnözők igyekeznek majd kártevőket terjeszteni a póruljárt ügyfelek körében.

Mindenesetre remélhetőleg hamarosan sikerül helyreállítaniuk a rendszereiket. Emlékezetes, hogy a World Backup Day alkalmából a WD az alábbiakat posztolta a Twitterre: "*A legjobb alkalom a mentésre tegnap volt. A második legjobb alkalom pedig most van*". **Remélhetőleg ennek megfelelően jártak el saját maguknál is, mindenesetre ezt a posztot mostanra már törölték.**

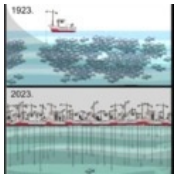
Megosztom tumblr. Tweet Pin it Tetszik 0

1 komment
Címkék: leállás western incidens twitter offline digital adatlopás adatszivárgás mycloud

Ajánlott bejegyzések:



Go Western Digital II.



A pisztácia kifogyott, adatlopás nem is volt...


Elvitte az ördög


Ransomware támadás a Nissan ellen


Néha nincs jó választás

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.



Head Honcho 2023.04.05. 18:51:43

Miért nem a szemétbánya Seagagyit támadják? :)

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

Ransomware támadás érte az MSI-t

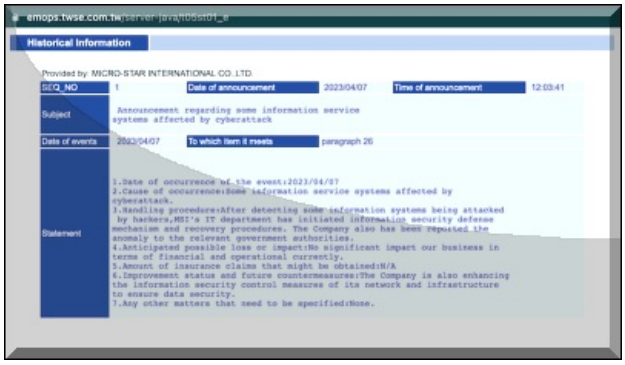
2023. április 11. 13:58 - Csizmazia Darab István [Rambo]

A vállalat megerősítette az hírt, miszerint zsarolóvírus áldozata lett. Az elkövető Money Message csoport azt állítja, hogy **az incidensben bizalmas adatokat sikerült ellopniuk, benne forráskódokat is.**



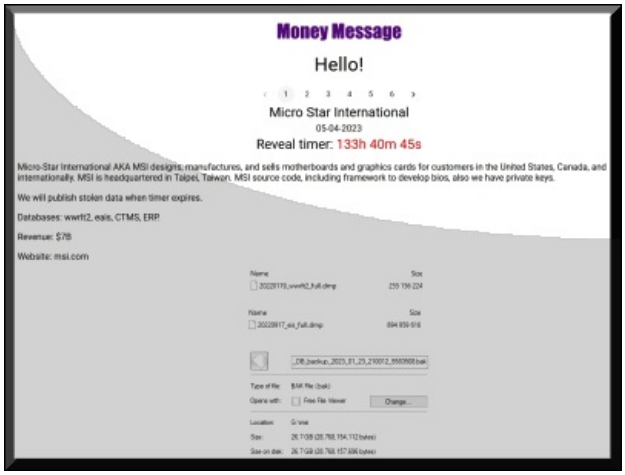
A tajvani Micro-Star International hivatalosan is megerősítette a támadás tényét, miután egy hacker fórumon már kiszivárgott az incidens.

Az elkövetők azt állítják, hogy **1.5 TB érzékeny adatot sikerült illetéktelenül megszerezniük, többek közt vállalatirányítási adatbázisokat, privát kulcsokat, BIOS firmware adatokat, és forráskódokat.**



A BIOS kiszivárgás ha valóban igaz, elég komoly érvágásnak tűnik annak fényében, hogy a Money Message szerint **ennek birtokában képesek lehetnek legitimnek látszó, és digitálisan aláírt kártékony BIOS-t létrehozni.**

Ez a bűnbanda egy viszonylag **új keletű csoport, idén márciusban aktivizálódtak a Zscaler elleni támadással, a kutatók összesen 5, zömmel USA-beli célpontok** iránti támadást észleltek azóta.



A szakértők szerint a kártevő **Windows és Linux rendszereket is célba vett, a hálózati megosztások elleni funkcionalitása hasonló a korábbi Maze és Petya vírusokhoz. Emlékezetes, hogy nem az MSI az egyetlen áldozatul esett félvezetőipari szereplő, előzőleg többek közt Gigabyte és az Acer is szenvedett el célzott támadásokat - ez utóbbi cégtől 160 GB adatot loptak el.**

Ezúttal az MSI felé **4 millió dolláros váltságdíj követeléssel fordultak a bűnözők 5 napos határidővel, ami**

éppen most, az ünnepek után telt le, így hamarosan kiderülhetnek majd az akciórészletei és az utóélete.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: money msi bios forráskód váltságdíj adatlopás adatszivárgás message ransomware zsarolóvírus doxing

Ajánlott bejegyzések:



Ransomware támadás a Nissan ellen



9 millió, bizony, dalolva ment...



Fordulat ransomware fronton



Ransomware a One Motelben



Baj van Tajvanban

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

368

Hogyan lehetünk jó digitális szülők?

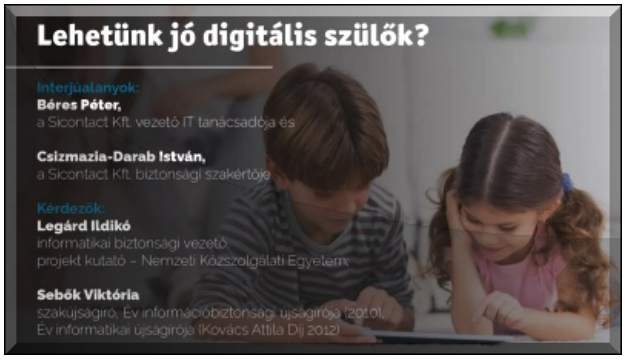
2023. április 13. 11:53 - Csizmazia Darab István [Rambo]

A kérdés nem egyszerű, offline szülőként hogyan neveljünk online gyereket. Sok Szilícium völgyi szülő egyenesen tiltja a gyerekének az okostelefont, de olyan is akad, aki a közösségi oldalaktól igyekszik távol tartani a gyermekeit. **Mit tegyünk viszont mi itt és most a völgytől távol, számunkra mi lehet minderre a jó recept?**



Ha alaposan belevetjük magunkat a tájékozódásba, az látszik, hogy **sokféle összetevő elem kell mindehhez, például a veszélyek és a védekezési lehetőségek alapos ismerete, minőségi odafigyelés, empátia, rendszeres beszélgetés az online élet történéseiről a gyerekekkel.**

Az életkor függvényében más hozzáállás szükséges, például alacsonyabb korban igen hasznos a közös netezés, a szülői felügyelet alkalmazása, később pedig kiemelten fontos a felkészítés a veszélyhelyzetekre, kihez lehet fordulni, hogyan lehet megelőzni az ijesztő, veszélyes vagy bántalmazó szituációkat.



A Nemzeti Közszolgálati Egyetem Oktatási központjában jártunk, és egy podcast beszélgetés során igyekeztünk körbejárni a témát. Az adásból kiderül, milyen kihívásokkal találkoznak a szülők, mik lehetnek a webkamera veszélyei, kik leselkednek a virtuális világban a kiskorúakra, hogyan történik egy online zaklatás és hogyan lehetne ezeknek elejét venni.

A jellemző statisztikák és védelmi megoldások mellett hasznos tartalmakat is ajánlunk: informatív weboldalakat, a szülői szerepben segítő könyveket, illetve olyan friss filmeket és sorozatokat is, amelyek szemléletesen, néha kissé ijesztően kijózanító módon mutatják be ezeket a lehetséges szituációkat, a gyermeinkre leselkedő veszélyeket.



Az IT biztonság angyalai csatornán Legárd Ildikó és Sebők Viktória kérdéseire válaszolva igyekeztünk használható feleleket találni mindezekre.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: biztonságos it biztonság internet podcast béres gyermekvédelem eset sicontact angyalai nke

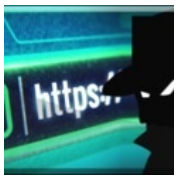
Ajánlott bejegyzések:



Mit csinálnak az alkalmazottak a céges gépeken?



Kis- és középvállalkozások adatvédelmi incidensei



Böngészés - kockázatok és mellékhatások


Kibermalac színre lép


ChatGPT: hogyan használjuk a munkában?

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

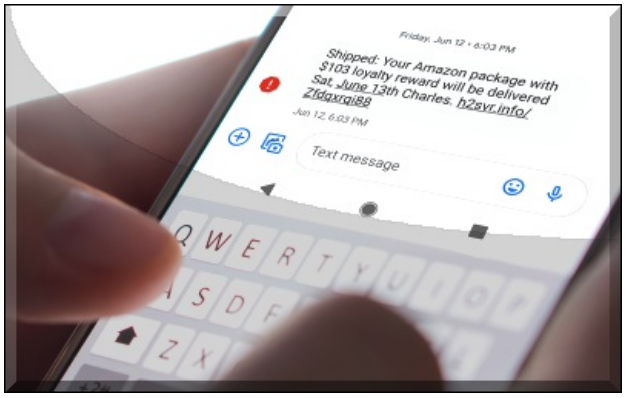
Belépés
Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

Mai szavunk pedig: smishing

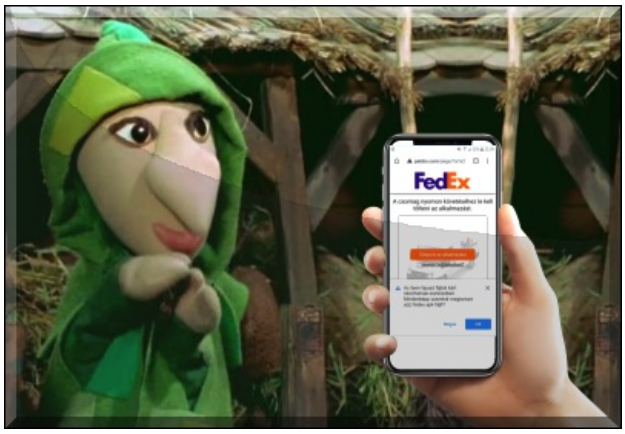
2023. április 18. 16:58 - Csizmazia Darab István [Rambo]

A smishing a klasszikus megtévesztéses adathalászat, azaz phishing és az SMS vagyis Short Message Service, magyarul rövidüzenet-szolgáltatás szavak összekeveredéséből keletkezett.



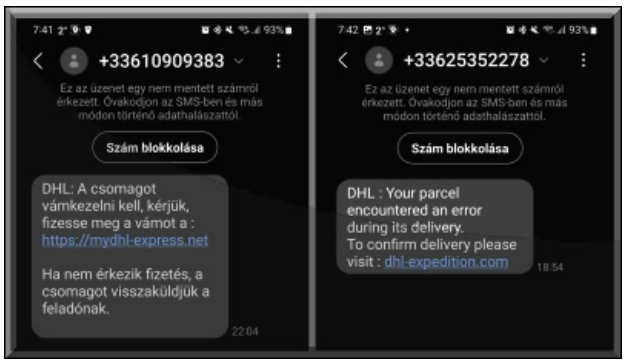
Az adathalászat más sokszor került terítékre itt a blogon is, és persze arról is több ízben esett szó, hogyan előzhetjük meg, miképp védekezhetünk.

A felhasználókat célzó különféle kampányok szűnni nem akaró hullámokban bukkannak fel, és a korábbi banki vonal mellett egy idő óta már csomagküldés is jelen van a megtévesztő üzenetekben - alighanem ez utóbbinak a Covid időszak is kedvezett.



Talán mindenkinek emlékezetes lehet az a két évvel ezelőtt FedEx nevében elkövetett csalás, ami már magyar nyelven igyekezett megtéveszteni a mobiltelefon tulajdonosokat. Ha valaki óvatlan volt, és még vírusvédelmet sem használt a készülékén, gyanútlanul kattintott, telepített, figyelmetlenül minden engedélyt megadott a kártékony kódnak, akkor **nem csak a telefonjáról kimenő SMS-ek okozhattak neki veszteséget, hanem a fertőzött telefonról minden adat ellophatóvá vált, így volt akinek a banki adataival éltek vissza, de sokan a rejtve elküldött SMS üzenetek elszámoló számláját látva szembesültek azzal, hogy valami nincs rendben.**

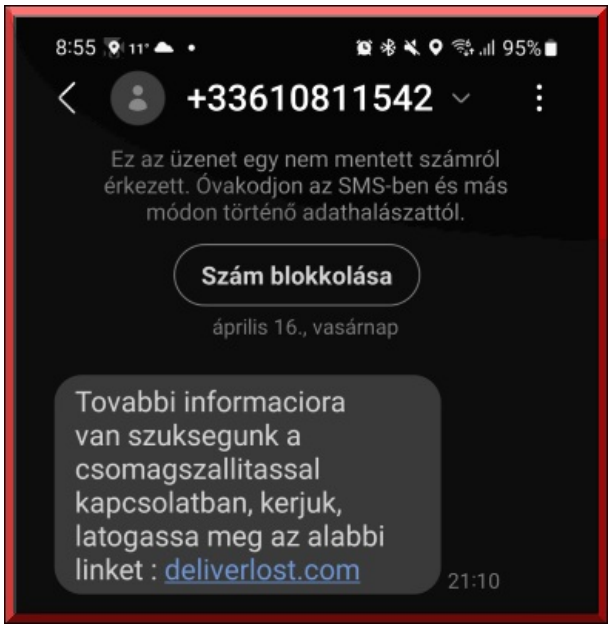
A vírustól megszabadulni pedig nem is volt éppen egyszerű, éppen a korábban megadott teljes körű engedélyek miatt.



Nos úgy tűnik, ez az SMS küldözgetős irány is egyre gyakoribb módi lett, folyamatosan próbálkoznak vele a bűnözők. **A mostanában futó kampányban ez most éppen a +33 előhívószámmal rendelkező franciaországi telefonokról érkezik. Vámkezelésre, címegyeztetésre, egyéb mondvacsinált blokkolási problémákra hivatkozva kártékony**

linkeket mellékelnek, amik aztán például a Google és egyéb bejelentkezési adatokat próbálják meg tőlünk ellopni.

Érdekes módon vegyesen magyar illetve angol nyelvű üzenetek különféle francia számokról, így vélhetően ebben az esetben is a már megfertőződött telefonok tulajdonosai terjesztik tovább tudtukon kívül az SMS-eket.



Ha már keletkezett ez a mostani poszt, akkor **a rend kedvéért szerepeljen itt a többi adathalász technika is. Vishingnek (vagyis Voice Phishing) hívjuk a telefonhíváson keresztül végzett adathalászatot, míg a spearphising olyan jól irányzott támadást jelöl, amely során látszólag hiteles üzenetek érkeznek meghatározott csoportok, szervezetek vagy éppen személyek postafiókjaiba.**

A célzott üzenetek küldői a hitelesség látszatának megőrzése miatt előzetesen alaposan tájékozódnak a célpontjaikról, ami nehezíti a felismerést, leleplezést. Végül pedig a whaling (bálnavadászat) elnevezést olyan célzott támadás esetében használjuk, amikor különleges, magas beosztásban lévő üzleti szereplők (pl. felsővezetők vagy cégtulajdonosok) kerülnek tudatosan a bűnözők célkeresztjébe.



Egy korábbi bejegyzésünkben már alaposan körbetáncoltuk azokat a lépéseket, amelyek megóvhatnak bennünket az adathalászattal kapcsolatosan az áldozattá válástól, így ezeket a jótanácsokat érdemes lehet megjegyezni és betartani.

Figyeljünk a helyesírásra, a megadott link nevére, ne hagyjuk magunkat sürgetni, gyanús linkekre, mellékletekre ne kattintsunk, használjunk vírusvédelmi alkalmazást és igyekezzünk tanulni mások kárából, például aki 4700 rejtett SMS elküldése után 160 ezer forinttal magasabb számlát volt kénytelen kifizetni.

Megosztom tumblr. Tweet Pin it Tetszik 0

1 komment
Címkék: sms csomag csalás átverés phishing adathalászat csomagküldő smishing

Ajánlott bejegyzések:


Kár érte, kiváló ügynök volt...



"NEM TUDJUK KISZÁLLÍTNI A CSOMAGÁT"



Csomagot kaptam life...


Ismét csomagunk érkezett - vagy mégsem?



Adathalászat menni booking.com

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Head Honcho 2023.04.18. 22:08:15

A helyesírás nem lehet eléggé red flag, lévén a lakosság jelentős része szinte félanalfabétának is mondható.

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

523

Bajban Venezuela legnagyobb bankja

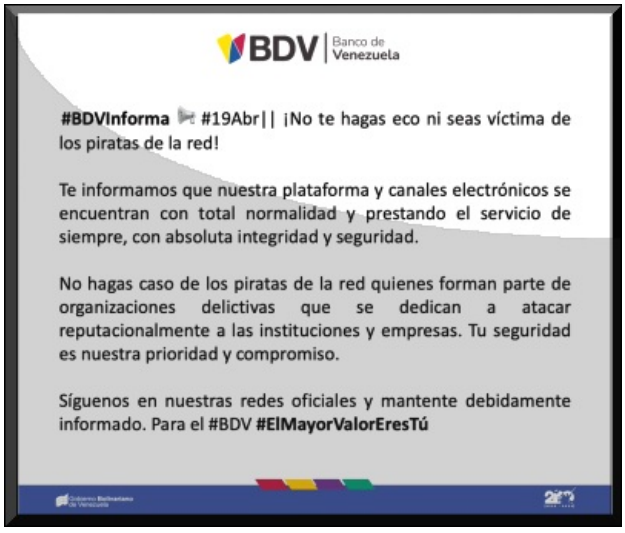
2023. április 20. 17:15 - Csizmazia Darab István [Rambo]

Zsarolóvírusok egyre gyakrabban jelentkeznek, és egyre jelentősebb célpontokat találnak meg, ezúttal **az állami tulajdonú Banco de Venezuela lett a LockBit 3.0 áldozata.**



Az eset még egész friss, tegnap reggel a Twitteren jelentek meg először olyan beszámolók, amelyek szerint a bancodevenezuela PONT com weboldalon üzemelő bank zsarolóvírus támadást szenvedett el, pénzek átfutása megakadt, lelassult.

A bank ennek ellenére a hivatalos közleményében nem említett zsarolóvírust, hanem szűkszavúan csak annyit írtak, hogy "*Tájékoztatjuk ügyfeleinket, hogy platformunk és elektronikus csatornáink a megszokott módon működnek, és szolgáltatásainkat teljes sértetlenséggel és biztonsággal továbbra is biztosítjuk számukra.*"



Mindeközben a darkneten viszont megjelent április 19-én 6:27-kor a zsarolók közleménye is, miszerint adatlopás (doxing) keretében bizalmas információkat sikerült megszerezniük, köztük belső banki műveletek adatait és ügyféladatokat is. A támadók megszerzett információkról fényképeket is a közzétettek bizonyítékként, ám ezen felül további részleteket nem közöltek.

A fizetésre május 10-e hajnali 2:27-ig adtak időt arra, hogy a bank kifizesse a váltságdíjat. A váltságdíj pontos összegéről egyelőre nincs információ, de a korábbi gyakorlat szerint a LockBit banda csak olyan kriptovalutákban fogad el fizetést, mint a Bitcoin, a Monero vagy a Zcash.



Ha a váltságdíj fizetés nem teljesül, a bejelentés szerint minden elérhető információt közzétesznek a neten. Ez oda vezethet, hogy számos ügyfelük válhat különféle típusú kibertámadások áldozatává, például célzott adathalászat, jogosulatlan fiókhozzáférés és az esetleges zsarolás, a kiszivárgott információk érzékenységétől függően.

A Banco de Venezuela az ország legnagyobb bankja, egy korábbi jelentés szerint több mint 21 millió különböző bankszámlát kezel országszerte, többek közt nagy számú közalkalmazotti és állami szervezetek számláit.



Mivel a bank nem cáfolta és nem is erősítette meg hivatalosan az incidens tényét, vélhetően a háttérben gőzerővel folyhat a kivizsgálás, nyomozás, valamint elképzelhető, hogy szakértők bevonásával az esetleges alkudozás is elkezdődhetett a váltságdíj összegéről.

Venezuelában egyébként nincsenek személyes adatok védelmére vonatkozó törvények. **Az ügyfelek érthető módon most féltik a pénzüket és féltik az esetlegesen kikerülő adataikat.** Ha lesznek további fejlemények, a folytatásra később még visszatérünk.

Megosztom tumblr. Tweet Pin it Tetszik 0

1 komment
Címkék: bank venezuela váltságdíj adatlopás ransomware darknet zsarolóvírus doxing lockbit

Ajánlott bejegyzések:


9 millió, bizony, dalolva ment...

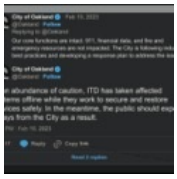

Ransomware támadás a Nissan ellen



Ransomware a One Motelben



Ransomware támadás érte az MSI-t


Ország, város, ransomware

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.



Head Honcho 2023.04.22. 19:36:25

Ez legyen a legnagyobb baja annak a szemétdombnak. Inkább meg kéne próbálniuk nem eladósodni a vadkeleti diktatúrák felé...

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

354

Ipari mennyiségű ransomware az ipari területeken

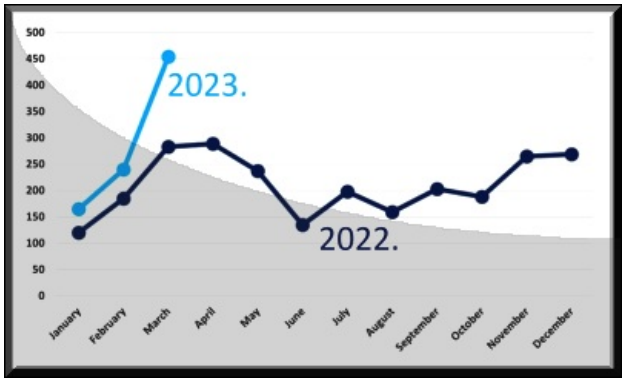
2023. április 24. 17:46 - Csizmazia Darab István [Rambo]

Ipar Kapitány (Captain Industry's) szemlátomást rákapcsolt az elmúlt hónapban, **a zsarolóvírus aktivitás márciusban** láthatóan minden korábbi rekordot megdöntött.



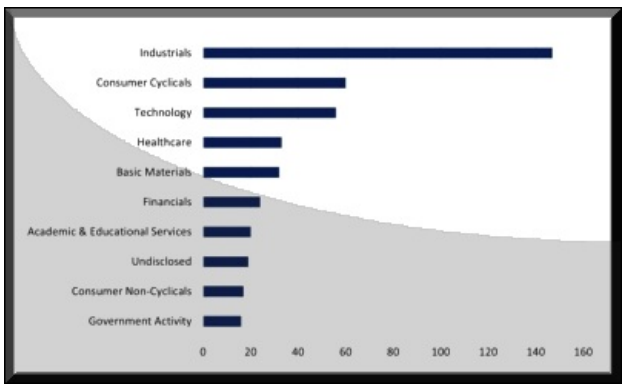
Az NCC Group statisztikái alapján az látható, hogy egy komoly kiugrás zajlott le a múlt hónapban.

A ransomware gyakoriság 91%-os növekedést mutatott az előző hónaphoz képest és 62%-os növekedést produkált az egy évvel korábbi, 2022 márciusi számokhoz képest.

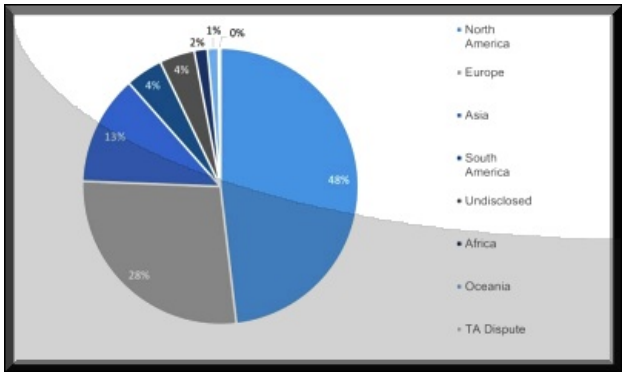


A bűnözői csoportok közül ezúttal **a Clop banda tarolt egy zeroday sebezhetőséget kihasználva, de erős versenyben a Lockbit 3.0, a Royal és a BlackCat is a szoros élmezőnyben végzett.**

A Royal egy viszonylag új versenyző, a magáncsoport neve talán kevésbe ismerten csenghet. 2**022. szeptemberében indultak vélhetően a Conti csapat támogatásával, és új technikákat is alkalmaztak: Linux platformon is támadnak, saját titkosítási algoritmust fejlesztettek, és ebben például már a villámgyors szakaszos titkosítást is használták az akcióiknál.** Jellemzően 250 ezer és 2 millió dollár közötti összegeket követelnek az áldozatul esett cégektől.



Amit a statisztikai adatokból még ki lehet olvasni, hogy ransomware csoportok által l**eginkább megcélzott szektorok közül az ipari ágazat vezet - ebbe beleértve az ipari termelő, gép- és szerszám gyártós és kereskedelmi, logisztikai, tervezői, építőipari, járműgyártói szereplőket** - a legkiszolgáltatottabb volt a maga 147 támadásával, ami az összegyűjtött incidens információk alapján csak önmagában mintegy 32%-ot tett ki.



A kiskereskedelmi, szállodai, médiával kapcsolatos szektor áll a második helyen, de ezek mellett **kiemelt figyelmet kaptak még az egészségügyi, technológia, oktatási és pénzügyi terület szereplői is** a célzott támadásokban.

Ha területileg nézzük az incidenseket, úgy **elsősorban az USA nevezhető elsődleges célpontnak, ez az összes támadás közel felét, 48%-ot jelentett az elmúlt hónapban, majd rögtön ezután az európai térképen kell keresni** a zsarolóvírus akciók által megcélzott vállalatokat - ők itt most 28%-ot képviseltek.

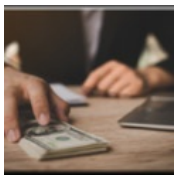


A megelőzés - védekezés témakörhöz érdemes lehet felidézni azt a tudástár összefoglalót, ami **részletesen felsorolja azokat a tudnivalókat, lépéseket, megoldásokat, amivel minimalizálni lehet a kockázatokat**.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: statisztika royal ipar ipari szektor ransomware zsarolóvírus clop

Ajánlott bejegyzések:


Megváltás-e a váltságdíj?


Clop ransomware menni Torrent


Baj van Tajvanban


Gyorsabban, magasabbra, erősebben!



Dallas a pácban

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

3976

Azonnali frissítés szükséges a fiók aktiválásához!

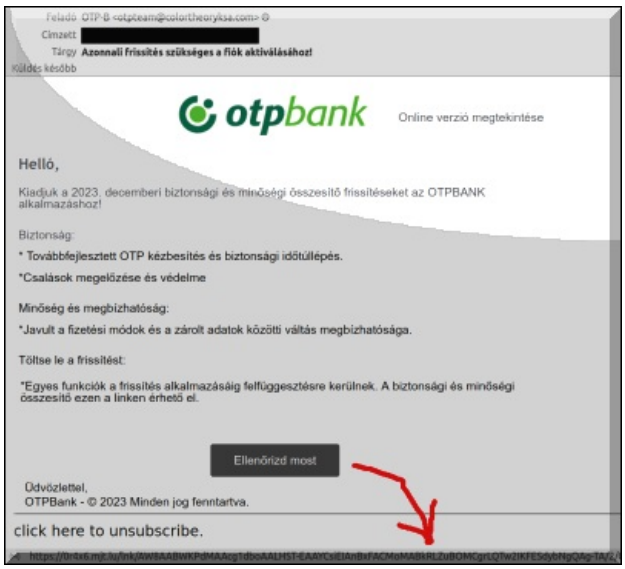
2023. április 26. 10:52 - Csizmazia Darab István [Rambo]

Vagy mégsem? - tehetnénk fel stílszerűen a kérdést az aktuálisan érkezett e-mailben érkező figyelmeztetés kapcsán. Nem tudni, hogy az újabb gyenge próbálkozást segítette-e valamilyen módon a mesterséges intelligencia is, vagy mindösszesen csak a hagyományos természetes módozatán csúszott ennyire félre.



A napokban érkezett az a magyar nyelvű spam üzenet, amely az ékezeteket tekintve ugyan nem szenved csorbát, ám a **megfogalmazása olyan, mintha bezárták volna egy cellába Fülig Jimmyt, Török Szultánt, Tuskó Hopkinst és Csülök nevű kollégájukat, hogy addig ki se engedjék őket, amíg egy banki biztonsági figyelmeztetésnek látszó iromány ki nem csúsztatnak az ajtó rése alatt.**

A látszólagos közös munkának aztán szemmel láthatólag meg is lett az alant látható zamatos gyümölcse.


Címzett [redacted]
Tárgy **Azonnali frissítés szükséges a fiók aktiválásához!**
Küldés később

otpbank Online verzió megtekintése

Helló,

Kiadjuk a 2023. decemberi biztonsági és minőségi összesítő frissítéseket az OTPBANK alkalmazáshoz!

Biztonság:
* Továbbfejlesztett OTP kézbesítés és biztonsági időtúllépés.
*Csalások megelőzése és védelme

Minőség és megbízhatóság:
*Javult a fizetési módok és a zárolt adatok közötti váltás megbízhatósága.

Töltse le a frissítést:
*Egyes funkciók a frissítés alkalmazásáig felfüggesztésre kerülnek. A biztonsági és minőségi összesítő ezen a linken érhető el.

Ellenőrizd most

Üdvözlettel,
OTPBank - © 2023 Minden jog fenntartva.

click here to unsubscribe.

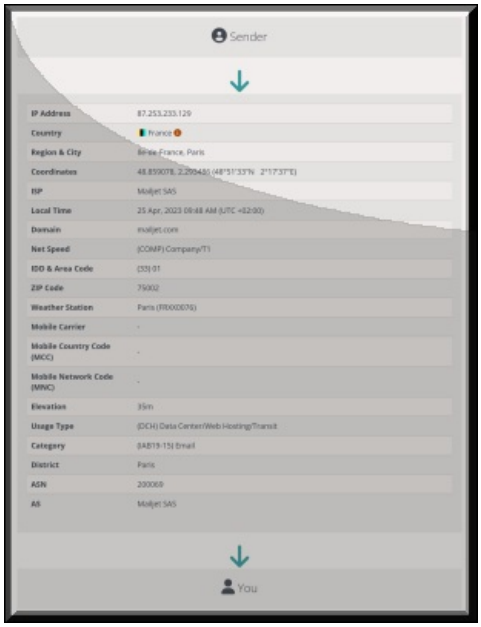
A megszólítás is "priceless", mintha csak az IKEA áruházban járnánk, spontán tegezve azt írja: "*Helló*". Érdemes végigfutni a szöveget, amiben egyrészt **arra hivatkoznak, hogy ez az állítólagos frissítés éppen a csalások védelmét és megelőzését szolgálja**, ez önmagában LOL.

De **van benne szokásos ijesztgetés, sürgetés fordulati elem is: "*Egyes funkciók a frissítés alkalmazásáig felfüggesztésre kerülnek.*"**, magyarán aki nem tölti le, az önmagára vessen, ha emiatt aztán blokkolják a számláját, így járt.



Roppant vicces rész az is, hogy **a** bűnözők **által mellékelt link állítólag a "2023. decemberi biztonsági és minőségi összesítő frissítés", pedig még mindössze csak április van,** még ha a középhőmérséklet hagy is némi kívánnivalót maga után így a második tavaszi hónap vége felé járva.

A levél aláírása sincs túlspirázva: "*Üdvözlettel, OTPBank*", ahogyan **a feladó címének elmaszkírozására sem fordítottak túl nagy energiát - gyakorlatilag semmit**: "*otpteam KUKAC colortheoryksa PONT com*". Ugye milyen eredetinek, hitelesnek és autentikusnak látszik, hát ezt tutira a bank küldhette ;-). A kattintható linket viszont időközben villámgyorsan lelőtték, így a hasonmás adathalász weboldalt már nem volt lehetőségünk meglátogatni.



Érdekességképpen még rákereshetünk e-mail trace segítségével a feladóra, amiből az derül ki, hogy Franciaországból, egyenesen Párizs környékéről küldhették azt.

Mivel ma már sajnos tucatjával érkeznek a hasonló adathalász és egyéb átverések, csalások postai, csomagküldői és egyéb kitalált fedőtörténetekkel, **remélhetjük, ha csak nem vett erőt rajtunk a biztonsági fásultság némi nemű tavaszi fáradtsággal párosulva, úgy ezeket biztonságtudatosan már mindenki élből törli,** és az ilyen kísérlet maximum félmosolyt csal a felhasználók arcára.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: csalás átverés otp adathalászat 2023.

Ajánlott bejegyzések:

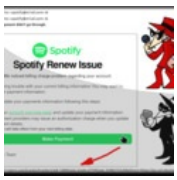

Nő a QR-kódos visszaélések száma


Xmas és Top posztok az idén


Kár érte, kiváló ügynök volt...



Adathalászat menni booking.com



Spotify megújítási probléma - vagy mégsem?

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

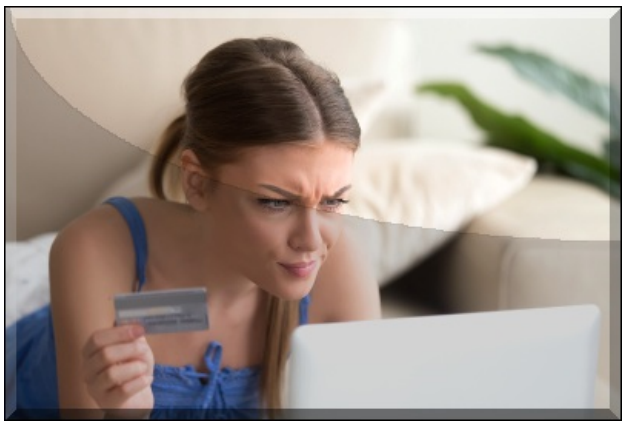
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

910

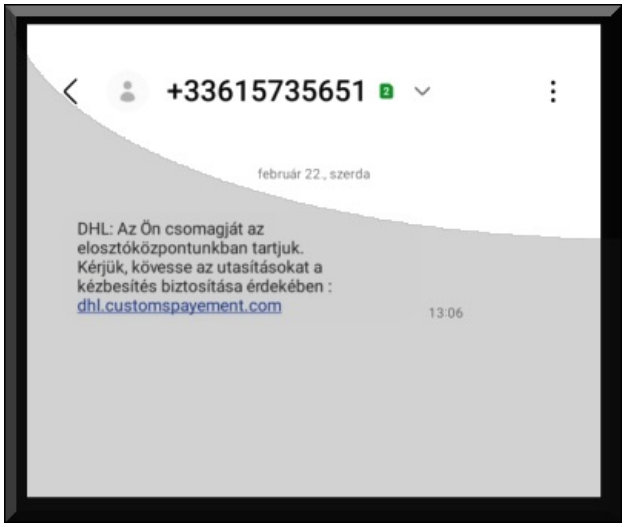
5 online csalásra utaló jel

2023. április 27. 17:26 - Csizmazia Darab István [Rambo]

Számtalan csaló jelent meg a kibertérben, akik csak arra várnak, hogy ellopják a felhasználók személyazonosságát és pénzét, akik ezt sokszor észre sem veszik. Az ő leleményességük, a mi hiszékenységünk, valamint a gyenge vállalati biztonsági megoldások együttesen teszik az online csalásokat egy több milliárd dollárt érő kihívássá. **A legjobb stratégia ez ellen mindig a megelőzés.**



A Szövetségi Kereskedelmi Bizottság (FTC) szerint 2021-ben az amerikai fogyasztók összesen közel 6 milliárd dolláros kárt szenvedtek el **online csalások miatt, ami 70 százalékos növekedést jelent az előző évhez képest.** Tökéletesnek tűnő áloldalakat készítenek, ahol elhitetik, hogy belépőket nyerhetünk – melyek postázásához még a bankkártyaadatainkat is meg kell adni. Az ESET kiberbiztonági szakértői összegyűjtötték azokat az **intő jeleket, amelyek segítenek időben felismerni az átveréseket.**



Ma már nyelvileg is nagyot fejlődtek az átverések: a két évvel ezelőtt FedEx nevében elkövetett csalás ugyan **magyar nyelven, de hibásan, ékezetek nélkül igyekezett megtéveszteni a mobiltelefon tulajdonosokat. Azóta az SMS adathalászat, a smishing egyre nagyobb méreteket öltött, egyre pontosabb és nyelvileg tökéletesebb lett**: a mostanában futó kampányban +33-as előhívószámmal rendelkező franciaországi telefonokról érkeznek az sms-ek.

Vámkezelésre, címegyeztetésre, egyéb mondvacsinált blokkolási problémákra hivatkozva kártékony linkeket mellékelnek, amik aztán például a Google és egyéb bejelentkezési adatokat próbálják meg tőlünk ellopni. Párszáz forintot kérnek, ami nem tűnik nagy veszteségnek, ám sokan nem számolnak azzal, hogy hackereknek adták meg a bankkártyaadataikat, ezért ennél sokkal több pénzük is bánhatja.



Néhány esetben rögtön nyilvánvaló, hogy valami baj történt, például rákattintunk egy adathalász linkre, és a másodperc törtrésze alatt tudatosul, mit tettünk. Más esetekben azonban kevésbé nyilvánvaló, hogy áldozatokká váltunk. Előfordulhat, hogy egy harmadik félnél, valamilyen általunk használt szolgáltatásnál történt incidens: adatlopás vagy adatszivárgás által jutnak bankkártyaadataink vagy személyes adataink hackerek kezébe. Ezeket az adatokat általában egy csalók által használt kiberbűnözői piactéren értékesítik.

A személyes adatokat nagy mennyiségben vásárolják meg, majd automatizált támadásokhoz használják fel őket, többek között adathalászat, kifizetéseket érintő csalás, kártyaazonosító-lopás vagy illetéktelen számla-hozzáférés, illetve új számla nyitásával kapcsolatos (NAF) csalás során.

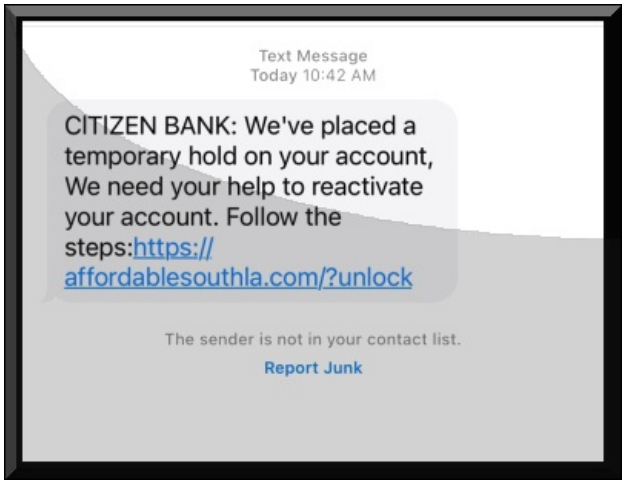


A felhasználói fiókok bejelentkezési adatait külön-külön tovább értékesíthetik, hogy a jogosulatlan vevők hozzáférhessenek például streaming vagy egyéb szolgáltatásainkhoz. **A rossz hír az, hogy a lopott adatok folyamatosan áramlanak a kiberbűnözői alvilágba. 2022-ben csak az Egyesült Államokban több mint 1800 adatvédelmi incidenst jelentettek, amely 422 millió fogyasztót érintett, ez pedig 40 százalékos növekedést jelent 2021-hez képest.**



5 árulkodó jel, hogy csalás áldozatai lettünk

1. Szokatlan tranzakciók és/vagy új hitelkeretek.
Amennyiben (pénzügyi) adataink csalók birtokába kerülnek, egyszerűen felhasználhatják azokat fizetési csalásokhoz – anélkül, hogy tudnánk róla. Személyazonosító adatainkkal pedig akár új hitelkártyákat is igényelhetnek. Előbbiről a bankszámlánkon tapasztalható szokatlan aktivitás révén értesülhetünk. Az új számla nyitásával kapcsolatos csalásokat (NAF) nehezebb észlelni, egészen addig, amíg nem kapunk egy levelet vagy egy e-mailt a késedelmes fizetésekről. A felhasználók gyakran akkor értesülnek először a NAF-ról, amikor ellenőrzik hitelbírálati minősítésüket és/vagy elutasítja őket egy hitelintézet.



2. A megvásárolt termék nem érkezett meg.
A csalók általában drága termékeket hirdetnek az interneten erősen nyomott áron, azonban a kínált áru valószínűleg nem létezik és csak a vevő pénzének megszerzése a cél. Vegyük intő jelnek, ha olyan előreutalásos alkalmazásokon keresztül kérik a vételárat, mint a Zelle, illetve a Venmo vagy a Cash App, amelyek nem nyújtanak vásárlói védelmet.



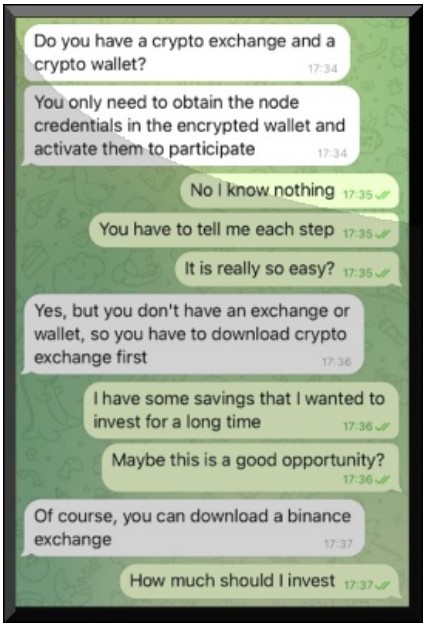
3. Eltűnik a "romantikus ismerős".
Az FBI adatai szerint a romantikus csalások 2021-ben több mint 956 millió dollárt hoztak a szélhámosok konyhájára. Valószínűleg ez csak a jéghegy csúcsa, mivel sok esetet nem jelentenek be az áldozatok, akik túlságosan szégyellik bevallani, hogy átverték őket. A romantikus csalók online ismerkednek áldozatukkal társkereső felületeken, ám mielőtt élőben is megismerhetnénk, előtte pénzt kérnek különböző valótlan dolgokra, például orvosi számlákra vagy állítólagos utazási költségekre. Ha az áldozat később visszakérné a pénzét vagy már sokadszorra nem hajlandó többet utalni, a csalók egyszerűen eltűnnek, és soha többé nem hallani felőlük.



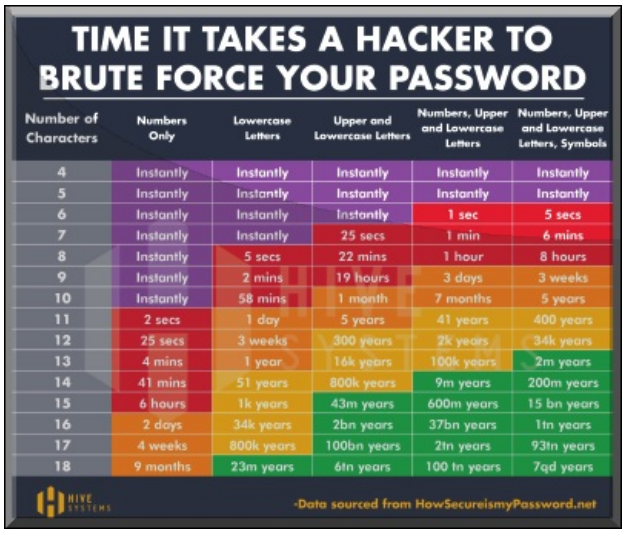
4. Nem sikerül belépni a felhasználói fiókokba.
A bejelentkezési adatok megszerzésével a csalók hozzáférnek a fiókjainkhoz, és megváltoztathatják a jelszavainkat. A fiókokból különböző személyes adatokat lophatnak el, beleértve a tárolt hitelkártyaadatokat is. A bejelentkezéshez szükséges felhasználónév és jelszó önmagában is értékes. Az Instagram-fiókok egyenként 45 dollárt érnek egy jelentés szerint, szemben a társadalombiztosítási számmal, amely 2 dollárt ér a darkweben. Ez azért van, mert a közösségi fiókok megszerzésével spameket lehet küldeni a profilt követő más felhasználóknak, ismerősöknek.



5) Nem tudunk pénzt kivenni a kripto befektetéseinkből.
Szintén elterjedtek a befektetési csalások, amelyek áldozatai 2021-ben összesen csaknem 1,5 milliárd dolláros veszteséget szenvedtek el, ennél nagyobb kárt csak az üzleti e-mailek feltörése okozott. A felhasználót jellemzően nagy hozammal kecsegtető befektetési lehetőségekkel győzik meg, amikor viszont az ügyfél ki akarja venni a pénzét, a csalók felszívódnak.



Mit tegyünk, ha átvertek bennünket? Amennyiben komoly összegről van szó, érdemes a hatóságokhoz fordulni. Ha pénzügyi adatokat loptak el, vegyük fel a bankunkkal is a kapcsolatot. Egyes banki alkalmazásokban néhány gombnyomással be tudjuk fagyasztani a feltehetően csalók által használt bankkártyákat. Kérjünk a banktól cserekártyát. Ahhoz, hogy a jövőben jobban fel legyünk készülve, és hatékonyabban tudjuk megelőzni a kibertámadásokat, érdemes átgondolni az alábbiakat.



- Cseréljünk jelszót. Használjunk erős, egyedi jelszavakat, amelyeket ideális esetben megbízható jelszókezelő tárol.

- A két- vagy többfaktoros hitelesítés nagyobb védelmet biztosít az adathalászok és a csalókkal szemben.

- Rendszeresen frissítsük, tartsuk naprakészen az eszközeinket, szoftvereinket.

- Ne mentsük el a személyes és/vagy pénzügyi adatokat online fiókokban, böngészőben. Bár körülményesebb minden egyes alkalommal megadni az adatokat, sokkal biztonságosabb eljárás.

- Gondoskodjunk arról, hogy minden eszközünk és számítógépünk **megbízható forgalmazótól származó, kártékony**

szoftverek elleni védelemmel rendelkezzen.



- Használjunk **megbízható biztonsági megoldást minden eszközünkön.**

- Informálódjunk: az ESET kiberbiztonsági podcastjében szakértők számolnak be a legújabb csalásformákról, a védekezés módjáról mobil- és asztali eszközön, az adataink védelmének fontosságáról, az éberségi szintünk emeléséről.

- Ne kapkodjunk, ne hagyjuk sürgetni magunkat! Blokkolt csomagra hivatkozó sms esetén álljunk meg és gondoljuk végig: egyáltalán várunk csomagot külföldről? Minden kattintás előtt álljunk meg egy pillanatra és gondoljuk át, hogy van-e bármi gyanús az üzenetben, legyen az a feladó, a link furcsasága vagy a szokatlan nyelvi fordulatok.

Az átverések sajnos igen sokfélék lehetnek, de odafigyeléssel nem elkerülhetetlenek. Ha mégis megtörténik, maradjunk nyugodtak, és a fenti tanácsokat megfogadva próbáljuk meg minimálisra csökkenteni a károkat.

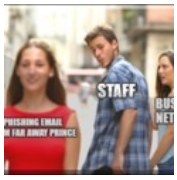
Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: online csalás tippek átverés megelőzés adathalászat

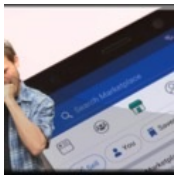
Ajánlott bejegyzések:



Nagy pénz, nagy foci, nagy átverések



10 gyakori ok, amiért bedőlünk a csalásoknak


Átverések az online piactéren


Nő a QR-kódos visszaélések száma


Black Friday és Cyber Monday járja be Európát

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

743

Windows update vagy mégsem?

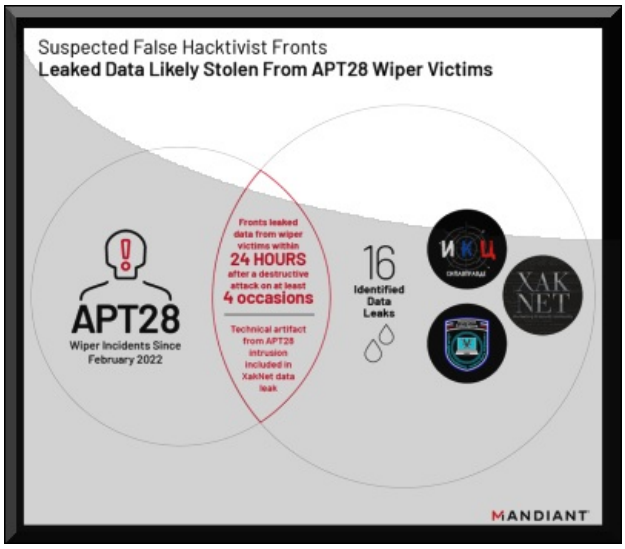
2023. május 03. 14:00 - Csizmazia Darab István [Rambo]

Az orosz APT28 csoport erőteljes e-mail kampányba kezdett, melynek során **ukrán kormányzati célpontoknak hamis, kártevővel fertőzött linkeket küldenek állítólagos Windows frissítésekre hivatkozva.**



Az ukrán CERT hívta fel a figyelmet arra, hogy **április folyamán erőteljes támadási hullámra, ahol kiemelt jelentőségű ukrán kormányzati és egyéb hivatalos szervezetek rendszergazdái kaptak hamis outlook-os címről** érkező leveleket.

Az ukrán nyelvű üzenetek arra hivatkoztak, hogy a mellékelt frissítés éppen a Microsoft operációs rendszerek elleni hackertámadások kivédésére szolgál.



A mellékelt kód azonban valójában egy olyan rosszindulatú PowerShell program, amely kémkedni próbál a hálózaton, és rendszer-információkat gyűjt össze a támadók számára.

A CERT-UA ennek kapcsán azt tanácsolta a kormányzati szerveknek, hogy korlátozzák a felhasználói PowerShell futtatási lehetőségeket.

<



Az APT28 régi ismerős vírusvédelmi berkekben, tevékenysége jó tizenöt évre nyúlik vissza, **2008. óta van jelen különféle akciókban, a csoport pedig nagy valószínűséggel az orosz GRU hírszerzéshez köthető. Korábbi támadásaik során mind az Egyesült Államokbeli, mind Nyugat-Európai,** illetve dél-amerikai kormányzati és katonai ügynökségeket, szervezeteket céloztak meg adathalászattal, kémprogramokkal.

2020-ban pedig a Covid vakcinákkal kapcsolatos adatlopásnak is elkövetői lehettek. Ukrajna elleni adattörlő és kritikus infrastruktúrákat támadó kártevőket egyébként gyakorlatilag nem csak a mostani orosz-ukrán háború kezdetétől, hanem már sokkal korábban, 2014-től is nagy számban észleltek a biztonsági szakemberek.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: windows frissítés orosz háború vagy update ukrán átverés hamis kémkedés mégsem vagymégsem gru apt28

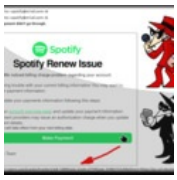
Ajánlott bejegyzések:



Új földgáz számlája készült - vagy mégsem?



Tagsági kérdések - vagy mégsem?



Spotify megújítási probléma - vagy mégsem?



Jótékonysági csalások Ukrajna nevében



Windows frissítés vagy mégsem?

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

638

Dallas a pácban

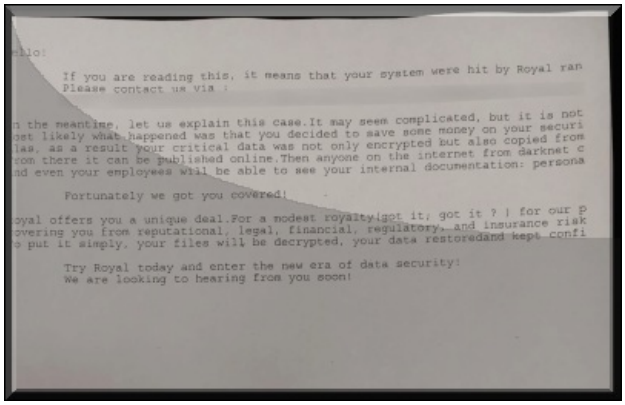
2023. május 05. 18:47 - Csizmazia Darab István [Rambo]

Ha Jockey Ewing most akarna a segélyhívón keresztül tűzoltókat hívni, vagy a rendőrséget értesíteni, akkor bajban lenne: zsarolóvírus támadás miatt leállt a dallasi közigazgatás teljes diszpécserszolgálata.



A Royal zsarolóvírus banda támadása folytán szerda reggel óta fennakadások vannak a közbiztonsággal kapcsolatos lakossági részlegek munkájával. A 911-es segélyhívó ugyan továbbra is működik, ám a bíróságokkal kapcsolatos munka, engedélyekkel kapcsolatos mindenfajta ügyintézés illetve **szociális szolgáltatásokkal kapcsolatos kifizetések leálltak vagy akadoznak, késnek.**

A tűzoltóság a kényszerhelyzet miatt papíralapú és rádiós kommunikációra állt át a számítógépes rendszer leállása miatt.



A Dallasi rendőrkapitányság is hasonló gondokkal küzd a zsarolóvírus miatt, itt szintén papíralapú, telefonos és rádiós működés váltotta a számítógépes ügymenetet. **Szakértők szerint idén már legalább 29 amerikai önkormányzatot érintett ransomware incidens, és ezek közül legalább 16-nál loptak el bizalmas adatokat.**

Korábban egy megtámadott rendőrőrs esetében a bűnözők azzal fenyegetőztek, hogy nyilvánosságra hozzák az ellopott adatokból kiderített bűnszervezetekbe beépült rendőrségi informátorok személyazonosságát.



Az orosz kötődésű Royal bűnözői csoport **tipikusan adathalász e-mailekkel férkőzik be a hálózatokba, vélhetően itt egy alkalmazott kattinthatott rá valamilyen gyanús linkre**. A banda tipikusan 1 és 10 millió dollár közötti összeget szab meg váltságdíjként. Ez az egyik legaktívabb kiberterrorista csoport, és **ők felelősek az összes amerikai zsarolóvírus-támadás 10%-áért.**

Azt egyelőre nem tudni, a dallasi esetnél történt-e adatlopás, illetve a váltságdíj mértékét sem hoztak nyilvánosságra, csak annyit tudni, hogy folyamatos erőfeszítéseket tesznek, hogy fizetés nélkül mihamarabb helyreállítható legyen az informatikai rendszer.

Megosztom tumblr. Tweet Pin it Tetszik 0

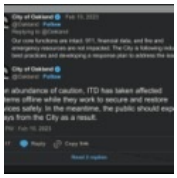
Szólj hozzá!
Címkék: dallas usa közigazgatás royal váltságdíj ransomware zsarolóvírus doxing

Ajánlott bejegyzések:



8 kórház, 30 klinika, 2.5 millió betegadat


9 millió, bizony, dalolva ment...


Ország, város, ransomware


Ransomware támadás a Nissan ellen



Ransomware a One Motelben

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

400

Go Western Digital II.

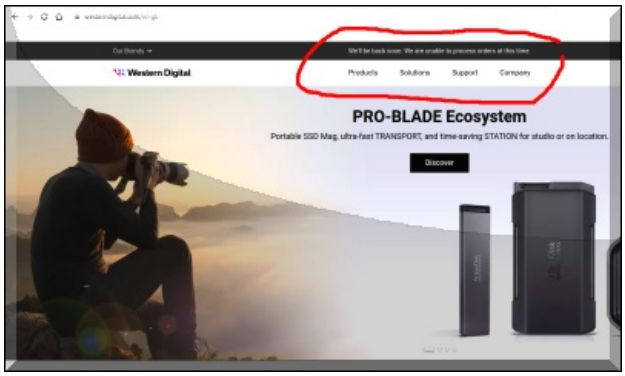
2023. május 09. 10:40 - Csizmazia Darab István [Rambo]

Mint arról tavasszal beszámoltunk, márciusban BlackCat ransomware támadás áldozata lett a Western Digital rendszere. Az akkori szűkszavú közleményekből nem sok minden derült ki.



A múlt hét végi közleményükben a **WD elismerte, hogy ügyfél-információkat loptak el az informatikai rendszereikből, emiatt a jövő hétig bezárják a webáruházukat**. A támadók hozzáfértek az online áruházát működtető adatbázishoz, így az ezekben szereplő személyes információkhoz is.

Ez olyan ügyféladatokat jelent, mint **a vásárlók neve, számlázási és szállítási címeket, e-mail címeket illetve telefonszámokat. Az ellopott adatok között szerepeltek még kódolt formában kivonatolt és sózott jelszavak, valamint vásárlói hitelkártyaszámok is.**



A webáruház tehát jelenleg zárva van, "*We'll be back soon: We are unable to process orders this time*." A vállalat **arra számít, hogy a május 15-ével kezdődő héten már vissza fogja tudni állítani a hozzáféréseket a fiókokhoz.** Egyúttal felhívták a figyelmet a személyes adatokkal való esetleges **csalásokra és visszaélésekre, elsősorban az adathalászat lehet ilyen fenyegetés.**

Azt már a TheRegister cikke teszi hozzá, hogy **az ellopott személyes adatok birtokában ennél jóval nagyobb kockázatok is jelentkezhetnek, például hogy a bűnözők a lopott adatok birtokában megszemélyesítik az áldozatokat és hitelkérelmeket adhatnak be pénzintézetekhez.**



A BlackCat (ALPHV) banda tagjai a márciusi támadás után azzal büszkélkedtek, hogy **10 TB érzékeny adatot sikerült ellopniuk a Western Digitaltól, amiért cserébe nyolc számjegyű** (forintban ez 10-20 milliárd körüli) váltságdíj összeget követeltek.

A dolog bizonyítékául több képernyőképet is feltöltöttek a netre. Ami viszont biztos, hogy sajnos jó sokáig - több hétig - késlekedtek az őszinte kommunikációval.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: leállás western digital váltságdíj adatlopás adatszivárgás ransom ransomware doxing

Ajánlott bejegyzések:



Ransomware támadás a Nissan ellen



9 millió, bizony, dalolva ment...



Ransomware támadás érte az MSI-t



Go Western Digital



Fordulat ransomware fronton

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

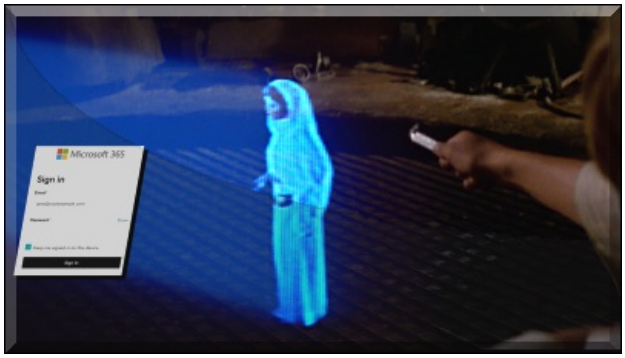
Belépés
Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

A jelszavad, mint üveggolyót, átadod

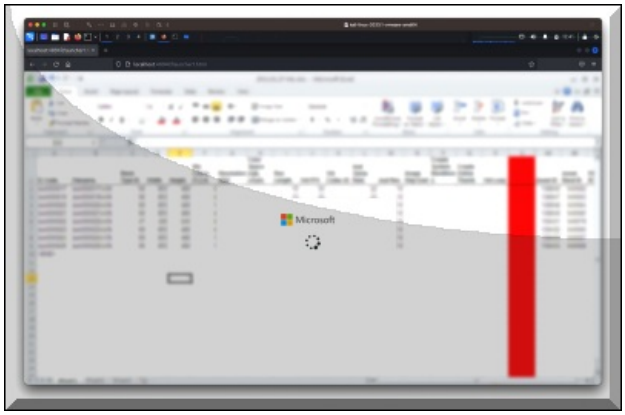
2023. május 11. 11:23 - Csizmazia Darab István [Rambo]

Egy új fajta tömeges támadási formát figyeltek meg a szakértők, melynek során **a Microsoft irodai környezet belépési oldalának hasonmásával tévesztik meg sikeresen a vállalati felhasználókat.**



A Greatness elnevezésű moduláris adathalász szolgáltatás (PaaS, Phishing as a Service) még a tavalyi év közepén jelent meg, amelyet kifejezetten a Microsoft 365 környezet megszemélyesítésére terveztek, és egy adathalász készletből, egy PaaS API szolgáltatásból, valamint a kommunikációhoz szükséges Telegram botból áll.

A bűnözőktől bérelhető megoldás lehetővé teszi, hogy **automatikusan rosszindulatú hivatkozásokat és mellékleteket küldjenek a célpontoknak, melynek segítségével bejelentkezési adatokat képesek ellopni**, sőt megtévesztve a felhasználót még a kétfaktoros hitelesítés védelem megkerülésére is kísérletet tehetnek.



A támadásban jelentős emelkedő kiugrásokat figyeltek meg a szakértők, így **tavaly decemberben és idén 2023. márciusában is erőteljes aktivitási hullámot tapasztaltak.**

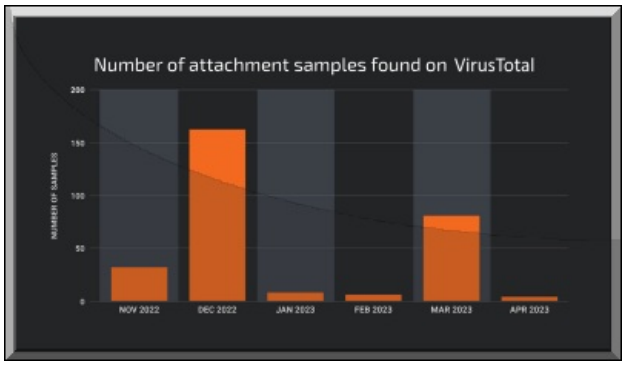
A rosszindulatú eszközkészlet képes kódszinten teljesen testre szabni az áldozatnál megjelenítendő Microsoft Office 365 belépési ablakot, ahol már az e-mailcím is előre ki van töltve.



Ha az áldozat gyanútlanul beírja a jelszót, az API azonnal továbítja azt, és **ha az adott fióknál a multifaktoros azonosítás is be van állítva, úgy a szolgáltatás felszólítást küld az áldozatnak a szükséges hitelesítés elvégzésére vonatkozóan.**

Amennyiben minden lépéssel sikerül megtéveszteni a felhasználót, a Greatness elküldi az MFA hitelesítési

munkamenet cookie-jait is a támadóknak.



Az eszközkészlet által megcélzott eddigi szervezetek jelentős többsége az USA-ban és az Egyesült Királyságban található.

Emlékezetes, hogy **egy korábbi felmérés azt mutatta, még a kétfaktoros autentikációt sem kapcsolja be az Office 365 felhasználók óriási többsége, 78 százaléka, miközben pedig világszerte napi 300 millió csalárd bejelentkezési kísérlet történik a felhőszolgáltatásokba.**

Megosztom tumblr. Tweet Pin it B Tetszik 0

1 komment
Címkék: microsoft csalás megtévesztés adathalászat jelszólopás paas greatness office365

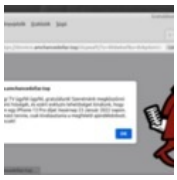
Ajánlott bejegyzések:


Nő a QR-kódos visszaélések száma


Ismét csomagunk érkezett - vagy mégsem?



Banki meló


Ingyen iPhone csak itt, csak most, csak nekünk


Kár érte, kiváló ügynök volt...

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Head Honcho 2023.05.11. 13:03:51

Gondolom, ezt a "vívmányt" is a muzsikok számlájára írhatjuk.

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

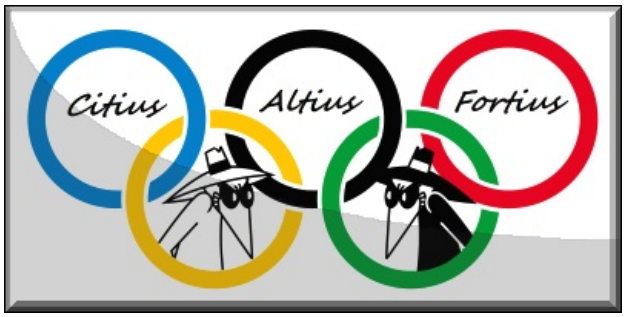
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

897

Gyorsabban, magasabbra, erősebben!

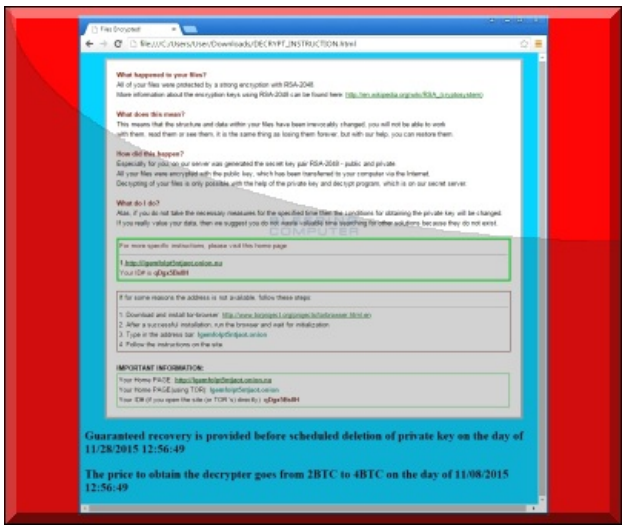
2023. május 16. 09:45 - Csizmazia Darab István [Rambo]

Ez a szlogen eredetileg az olimpia mozgalomból származik, de ha mi itt most a mai ransomware helyzetre vonatkoztatjuk, akkor is mutat részleges hasonlóságokat. A mai **modern zsarolóvírusok gyorsabban dolgoznak, magasabbra emelt váltságdíjakat követelnek, és erősebben, sőt akár többszörösen is megszorongatják áldozataikat.**



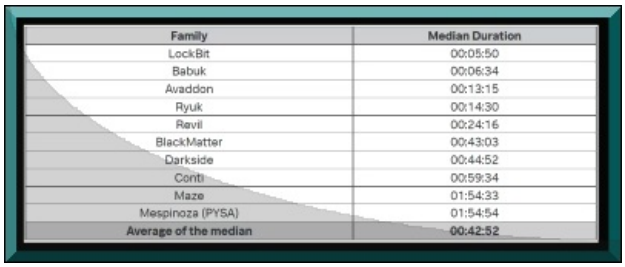
Kezdetben volt a CryptoLocker még 2013-ban, azaz jó tíz éve, amely **ránk szabadította ezt fajta mára már ipari méreteket öltött kártevő áradatot és pénz-zsarolási potenciált.**

Mindenkinek fel kellett emelnie a fejét, reagálni, megelőzni, védekezni, és a korábban sokszor elsinkófált biztonsági mentések ázsiója is hamar emelkedésnek indult.



Leszámítva azt néhány eleve hibásan programozott kártevőt, mint amilyen például a 2015-ben felbukkant Power Worm volt, amely hibásan volt megírva, emiatt az előre átutalt 2 Bitcoinos váltságdíjat fizetőknek abszolút semmi esélyük sem volt adataik visszanyerésére, a zsarolóvírusok ezzel szemben általában adtak lehetőséget a titkosított adatok visszakódolására.

De mint tendencia már egy idő óta azért látható volt, hogy számos esetben hiába fizetett az áldozat, a helyreállító eszköz olyannyira lassú működésű volt, hogy sokan kínjukban a fizetés ellenére mégis inkább saját mentéseikből húzták vissza a rendszert - például a Colonial Pipeline esetében.



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

Persze az idő múlásával egyre gyakoribb lett a doxing is, ahol már **nem pusztán az adatok helyreállítása mozgatta meg a történetet, hanem az elkódolás előtt ellopott bizalmas adatok kiszivárogtatásától való félelem is fizetésre sarkallt** megzsarolt vállalatokat. És persze a technikai fejlődés sem kerülte a ransomware ipart, hiszen a Moore törvény itt is az egyre javuló teljesítményű kártevőket volt képes kitermelni, **mint például az 53GB méretű**

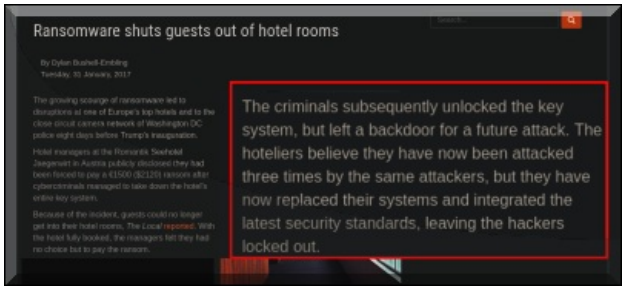
válogatott teszt adatmennyiséget, benne 98 ezer pdf, doc, xls, és hasonló tipikus Office és egyéb felhasználói állománnyal mindössze 5 perc alatt ledaráló LockBit.

Ehhez a sebességhajszoláshoz többek között az egyre gyakrabban alkalmazott szakaszos titkosítási módszer is effektíven hozzájárult.



És akkor el is érkeztünk a mai témához, miszerint egyes elemzők szerint **sok esetben a gyors működés és az esetleges kódolási hibák miatt egyre gyakoribb az a változat, hogy gyakorlatilag helyreállíthatatlanok lesznek az elkódolt adatok az esetleges váltságdíj fizetés után a bűnözőktől kapott eszközzel**. Vagyis már nem túl lassú, hanem sokat hibázó vagy működésképtelen.

Richard Addiscott, a Gartner vezető elemzője szerint **a ransomware áldozatainak mindössze 4 százaléka nyeri vissza sértetlenül az összes korábbi adatát.**



Ha pedig ehhez azt is hozzávesszük, hogy az egyszer már fizető ügyfeleket sokszor újra és újra megzsarolják a bűnözők például elrejtett hátsóajtón keresztüli újrafertőzéssel, vagy a doxing fenyegetési kártya ismételt előhúzásával, akkor a fizető áldozatok esélyei nem túl fényesek.



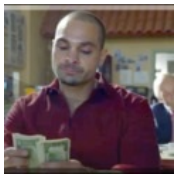
A statisztikák pedig alátámasztják mindezt, az adatok hibátlan helyreállítás átlagosan 60%-ban lesz csak sikereres, az incidensek pedig - különösen ha váltságdíj tárgyalásokra is sor kerül benne - átlagosan 25 napos fennakadást okos az üzletmenetben. Ezeket a hosszas kieséseket sok esetben láthattuk a Colonial Pipeline mellett például Costa Rica, a JHS húsfeldolgozó hálózat vagy a Kaseya felhős távmenedzsment szolgáltató elleni incidens.

A szakértők szerint a vállalatoknak a gyors és meggondolatlan váltságdíj fizetés helyett sokkal több energiát kellene beleölni a megelőzés/védekezés mellett az esetleges incidensek utáni gyors helyreállítási lehetőségek alapos megszervezésére és az ehhez szükséges források biztosítására.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: statisztika mentés sebesség váltságdíj helyreállítás ransomware zsarolóvírus újrafertőzés

Ajánlott bejegyzések:



[Csökkent a zsarolóprogramból származó bevétel]



[Emelkedő ransomware károk]



[Durva ransomware statisztikai adatok]



[Fedett pályás titkosítási bajnokság]



[Ransomware a spájzban]

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

309

Szektorhiba

2023. május 18. 10:40 - Csizmazia Darab István [Rambo]

Vajon melyik ágazat bízik nagyon és melyik kevésbé saját kiberbiztonsági ismereteiben?



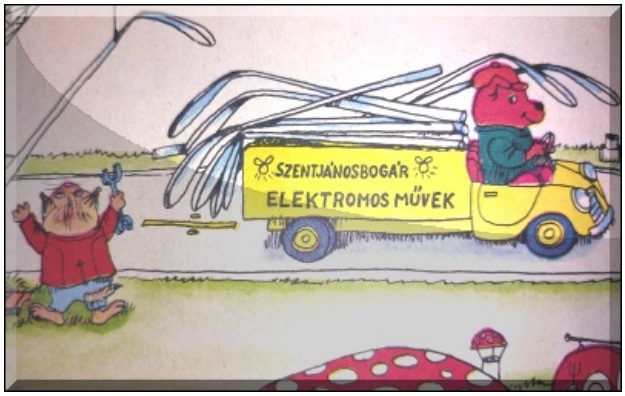
Miközben a fenyegetés napról napra nagyobb, a kibervédelmi ismeretek hiánya miatt a vállalatok egyre kiszolgáltatottabbá válnak. **Ez a probléma különösen a kis- és középvállalkozásokat (kkv-kat) érinti, amelyek a jelenlegi gazdasági környezetben kénytelenek csökkenteni kiadásaikat.**

Az ESET kiberbiztonsági kutatói a közelmúltban **több mint 700, különböző iparágakban tevékeny kkv körében azt mérték fel, képesek-e felismerni a legújabb kiberfenyegetéseket, és tudnak-e reagálni rájuk.**



Az ESET 2022-es SMB Digital Security Sentiment Report című jelentése arról ad képet, miként reagálnak a különböző profilban működő vállalatok a kialakult biztonsági helyzetre.

A megkérdezett kkv-k 32%-a használ végpontvédelem és válaszadás (EDR), kiterjesztett észlelés és elhárítás (XDR, kiterjesztett észlelési és elhárítási funkció, amely megkönnyíti a biztonsági incidensek elkerülését vagy azok kivizsgálását) vagy felügyelt észlelés és reagálás (MDR) technológiát, **míg 33% még egyelőre csupán tervezi ezen kiberbiztonsági szolgáltatások igénybevételét. Nézzük hát meg, mi jellemzi a különböző ágazatokat.**



Az adatok szerint az üzleti és szakmai szolgáltatásokat nyújtó kkv-k több mint negyede (26%) nem, vagy alig

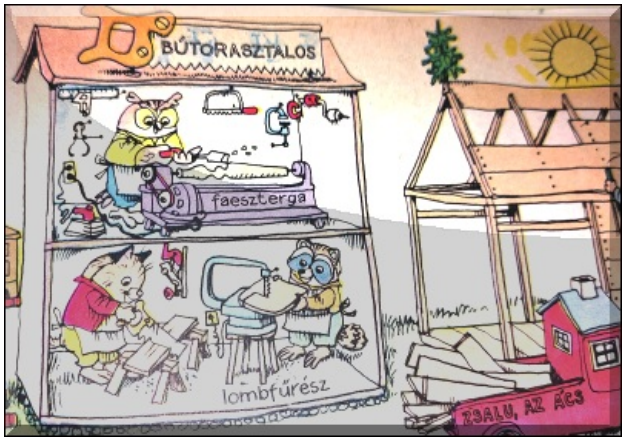
bízik a vállalaton belüli saját kiberbiztonsági ismereteikben. Alig harmaduk (31%) bízik abban, hogy csapatuk tisztában van a legújabb fenyegetésekkel és úgy véli, hogy a vállalatuk nehezen tudná azonosítani egy kibertámadás kiváltó okát. 38% saját maga gondoskodik a kiberbiztonságról, ám van törekvés ennek megváltoztatására: **mindössze 24% szeretné tartósan házon belül tartani a biztonsági felügyeletet, miközben 54% már kiszervezné ezt a feladatot.**

További 8% tervezi, hogy a következő 12 hónapban külső szakértőkre bízza a kibervédelmi intézkedéseket.



A pénzügyi szolgáltatási szektorban működő kkv-k 29%-a alig vagy egyáltalán nem bízik a saját kiberbiztonsági szakértelmében.

Még ennél is többen (36%) kevéssé vagy nem bíznak abban, hogy alkalmazottaik tisztában vannak a kiberbiztonsági fenyegetésekkel, míg mindössze 26% gondolja azt, hogy a vállalata nehezen tudná megállapítani egy kibertámadás kiváltó okát. **Itt 28% kezeli az IT-biztonságot házon belül, ez a vizsgált ágazatok közül a legalacsonyabb arány, ám csaknem kétharmaduk (65%) inkább kiszervezi a feladatot,** az összes kkv esetében ez az arány 59%.



A gyártás és ipari termelésszektor kis- és középvállalkozásainak harmada (33%) alig vagy egyáltalán nem bízik a saját kiberbiztonsági szakértelmében, ami jóval több az összes kkv átlagánál (25%). 40% kevéssé bíznak abban, hogy alkalmazottaik felismerik a biztonsági fenyegetéseket, ami minden más ágazatnál magasabb arány.

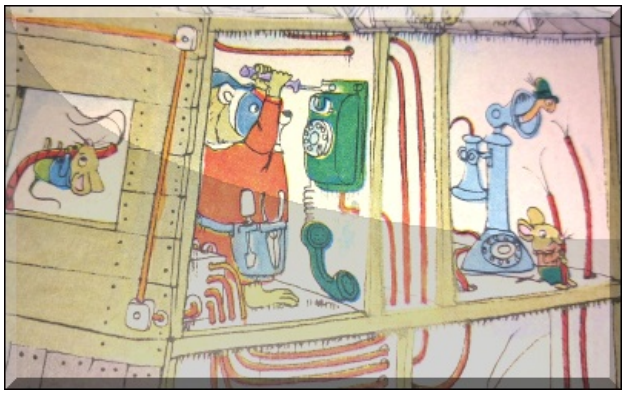
Ugyanakkor mindössze 29% aggódik amiatt, hogy nehezen tudná azonosítani egy esetleges kibertámadás kiváltó okát. **Itt 33% kezeli saját maga az IT-biztonságot, és több mint kétszer annyian (63%) inkább kiszervezik a védelmüket.**



80% kis- vagy nagykereskedelmi, illetve forgalmazással foglalkozó kkv bízik a saját kiberbiztonsági szakértelmében, ami a legmagasabb arány az összes ágazat közül. A szektorban működő vállalatok háromnegyede (74%) mérsékelten vagy nagyon bízik abban, hogy az alkalmazottak felismerik a biztonsági fenyegetéseket. **Emellett 79% úgy véli, képesek lennének azonosítani egy kibertámadás kiváltó okát, ami**

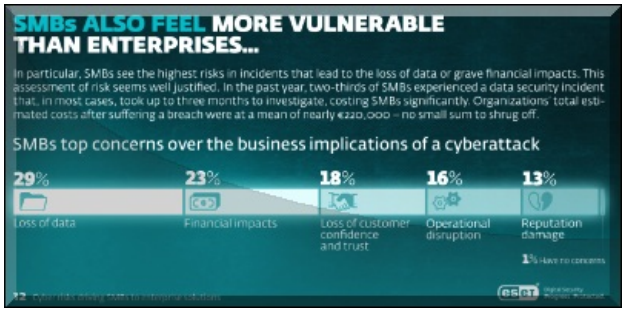
minden más vizsgált iparághoz képest kimagasló arány.

Ezen cégek 41%a kezeli a kiberbiztonságot házon belül, és 53% szervezi ki jelenleg az IT feladatokat. Az itteni válaszadók 6%a tervezi csak, hogy a következő egy évben külső szakértőre bízza a vállalati kibervédelmet.



A technológiai és távközlési kis- és középvállalkozások negyede (25%) alig vagy egyáltalán nem bízik a belső kiberbiztonsági szakértelemben. Ugyanakkor az ágazaton belül 78% ért egyet azzal az állítással, hogy alkalmazottai valamilyen szinten tisztában vannak a biztonsági fenyegetésekkel, ez minden vizsgált szektor közül a legmagasabb szám.

Több mint háromnegyedük (77%) úgy véli, hogy egy esetleges támadás esetén képesek azonosítani a kiváltó okot. Ebben a szektorban 37% azoknak az aránya, akik saját kezükben tartják a kiberbiztonságot, **miközben 58% szervezi ki a biztonsági intézkedéseket.**



Összességében míg egyes ágazatokban a kkv-k nagyobb önbizalommal rendelkeznek, és másoktól eltérő megközelítéseket alkalmaznak a kiberbiztonság terén, **gyakran ezek a vállalkozások teljes mértékben maguk kezelik az IT-védelmet, ami hamis biztonságérzetet adhat.**

Akkor is érdemes lenne rendszeresen harmadik fél által végzett ellenőrzéseket végrehajtani, biztonsági irányelveket létrehozni és rendszeresen frissíteni azokat, ha a feladatok házon belül maradnak, hiszen a céges adatok ezeken az eszközökön keresztül is illetéktelenek kezébe kerülhetnek.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: statisztika felmérés security állapot kkv eset digital report ágazat smb szektor kiberbiztonság sentiment 2023.

Ajánlott bejegyzések:



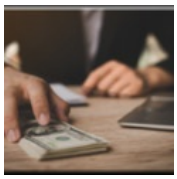
Kis- és középvállalkozások adatvédelmi incidensei



Kiberbiztonsági trendek 2023.



A nemzetközi helyzet egyre fokozódik


Megváltás-e a váltságdíj?


Ipari mennyiségű ransomware az ipari területeken

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

988

Bot vívás

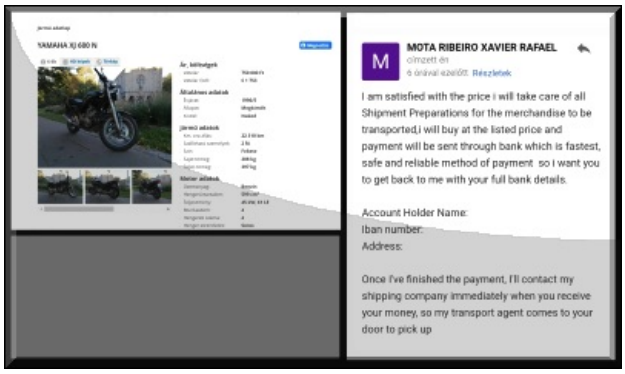
2023. május 23. 13:34 - Csizmazia Darab István [Rambo]

Ömlenek ránk a postai és különféle csomagküldési szolgálatok nevével visszaélő átverések üzenetei, ez már széles körben szinte napi szintű kockázat. Ami viszont szintén káros folyamatként figyelhető meg, hogy **az adásvételi platformokon - Vatera, Jófogás, Marketplace - is hihetetlen mennyiségű automata bot és hús-vér csaló igyekszik becsapni bennünket.**



Alig pár hónapja **nagyot futottak olyan cikkek a TotalCar oldalán, amelyben járművek adásvétele kapcsán számoltak be csalási kísérletekről.**

Az egyik ilyen cikkben a hirdetés megjelenése után rövid időn belül jelentkező külföldi illetőségű állítólagos érdeklődő **azonnal megvenne egy járművet látatlanban, és nyomban küldene is szállítmányozó céget, de most kéri az összes személyes és banki adatot. Itt emelje fel a kezét az, aki megtekintés, kipróbálás, átvizsgálás nélkül vesz járművet.**



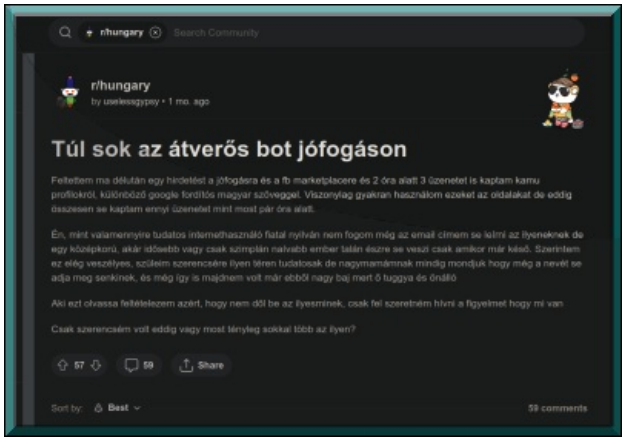
A csalók sok esetben azzal próbálkoznak, hogy egy **kamu képernyőfotóval próbálják bizonyítani a vételár átutalását, az eladó azonban jobban teszi, ha a saját szemének hisz, ha megérkezik a számlájára a pénz. Ez sem lehet azonban bombabiztos, hiszen ha lopott bankkártyával fizetnek, a nyomozás folyamatában ezeket az utalásokat a bank vissza is vonhatja.**

Szintén gyanús jel, ha biztosítási, szállítási, vámolási különdíjakra hivatkozva próbálnak pénzt kérni, **illetve ha kriptovalutás - kvázi lenyomozhatatlan - utalást kérnek.**



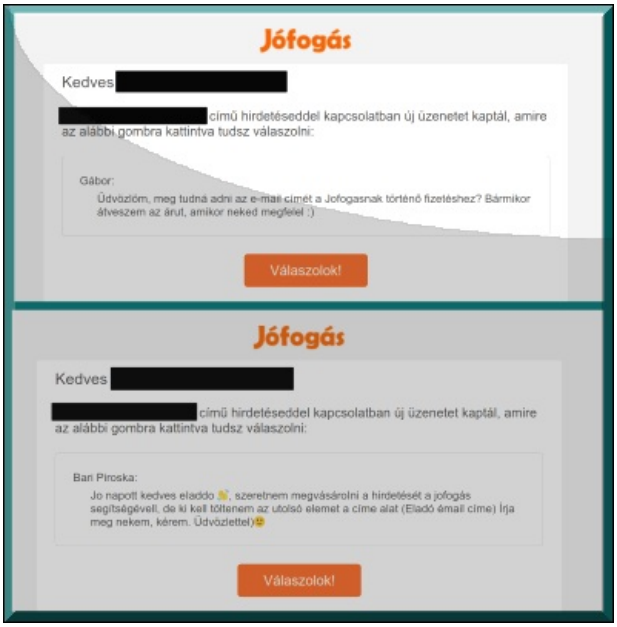
És akkor a mai téma a hétköznapi tárgyaink adásvételénél jelentkező csalások - bár itt ezek a platformok a ruha, cipő, sporteszköz, műszaki cikk kategória mellett gyakran lakásokat, járműveket is kínálnak. Folyik már jó ideje diskurzus erről a témáról például ezen a helyen, ahol a **tipikus átverési módszerek között szerepel ha a vevő akarja megrendelni a futárt, szállítást és ehhez kér személyes adatokat.**

A Vatera és Jófogás rendszerekben az eladó kezeli a szállítási lehetőségeket, a Foxpost, EasyBox, MPL csomagautomata esetekben ehhez a vevő neve, címe, e-mail címe, és telefonszáma is szükséges a kézbesítési értesítésekhez.



A szokásos csalási módszerekhez hasonlóan **a kapcsolatfelvétel után itt is bepróbálkoznak mondvacsinált ürügyekre hivatkozva kisebb-nagyobb összegeket előre elkérni, illetve bankkártya számot, vagy a bankkártya fényképét is szokták kérni természetesen a 3 jegyű CVV biztonsági kóddal együtt. Ha linkeket küldenek, akkor is jogos a gyanakvás, ezzel észrevétlenül kijátszhatják a kétfaktoros autentikációs védelmünket, vagy kémprogramot, távmenedzsment (VNC, AnyDesk, DCRAT, stb.) programot telepíthetnek fel a gépünkre.**

Ilyen sztorikkal már évek óta károsítanak meg óvatlan felhasználókat. **Itt aztán már minden látszik távolról, gyakorlatilag minden megtehető, nevünkben posztolhat, megszemélyesíthet minket, SIM kártya cserét kérhet a mobilszolgáltatónál, stb.**



A Jófogás vagy a Marketplace használathoz elég egy kamu e-mailcím, kamu regisztráció, és máris támadhatók az eladók. A Facebook oldalain **általában angolul, de néha pedig magyar nyelven, de külföldi felhasználói profilok jelentkeznek be már rögtön percekkel** a hirdetés feltöltése után.

A bot-szerű működés például onnan is látszik, ha valaki elhajt a fenébe egy ilyen konkrét csalót, az egy másik termékére hamarosan simán küld egy másik ugyanilyen formaüzenetet, hiszen az egész automatikusan generálódott. A jófogásra feltöltött és kizárólag budapesti személyes átvétellel hirdetett termékre zsinórban jöttek a kamu megkeresések.



A csak és kizárólag személyes átvételnél semmi szükség jófogásos e-mail címre, szállítmányozásra, banki adatokra. Eladóként a FoxPost, EasyBox megoldások jól működnek, **a csomagot csak fizetés után vehetik fel az automatából, és ezt az eladó intézi. Vevőként is jó megoldás lehet az ilyen küldésmód**, ott maximum csak azzal szembesülhetünk, hogy egy tégla lapul az automatánál kifizetett csomagban.

Ezen segíthet az eladó minősítésének előzetes ellenőrzése, ami például a Vatera esetén nem manipulálható annyira egyszerűen, hiszen zártabb rendszer, jutalék is tartozik az adásvételekhez, és a minősített eladók név-lakcím-telefon-emailcím mellett bankkártyájukkal is igazolják magukat a szolgáltató felé. **Adathalász kísérletek persze mindenhol, úgy itt is előfordulnak.**

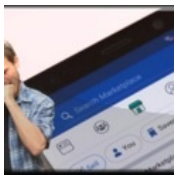


Az óvatosság mindenesetre minden felhasználó, potenciális vevő és eladó számára indokolt, **a csaló üzenetek sorsa pedig az egyik kommentelő frappáns megfogalmazása szerint történjen így: "A Kukából is kikukáztam."**

Megosztom tumblr. Tweet Pin it Tetszik 0

2 komment
Címkék: robot adásvétel csalás átverés vatera bot marketplace jófogás üzemszerű

Ajánlott bejegyzések:








Átverések az online piactéren | Nő a QR-kódos visszaélések száma | Xmas és Top posztok az idén | Black Friday és Cyber Monday járja be Európát | Kár érte, kiváló ügynök volt...

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.



Androsz · http://wikipedia.blog.hu/ 2023.05.23. 22:02:25

Nem értem, mire megy valaki az e-mail címemmel?

Válasz erre

0dzsud0 2023.05.24. 09:31:34

@Androsz: OFF: azt nem tudom, de erről jut eszembe, hogy pár hónapja kommenteltél a Retrokult blogra, hogy nem találod a "Meztelennek látom" /Vedo nudo (1969)/ c. filmet. Azt hiszem, tudok segíteni, hogy ilyen problémába ritkábban ütközz, de amit linkelni szeretnék, azt egyik blogon sem látják szívesen. Megpróbálok a profilodon szereplő kontakttal emailt írni, ez vajon tényleg egy létező funkció?

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

884

Mesterségem címere adathalászat

2023. május 26. 20:06 - Csizmazia Darab István [Rambo]

Két különböző biztonsági elemzés is sokkoló mértékű **emelkedést regisztrált a phishing támadások** mértékében.



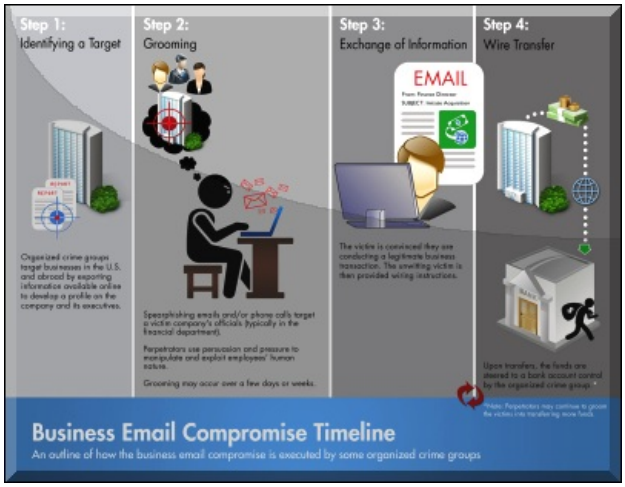
Az egyik leghatékonyabb és egyben leggyakoribb incidens az adathalászat, amely hamis linkkel, hamis weboldallal veszi rá a gyanútlan felhasználókat a rosszindulatú hasonmás weboldalon való bejelentkezésre és személyes adataik begépelésére. A vállalati szférában jelentkező fejlett és automatizált adathalász támadási kísérletek száma a tavalyi évben 356%-kal nőtt, **ezek egy jelentős részénél már alkalmazták a gépi tanulás és a mesterséges intelligencia eszközeit.**

A kifinomult támadások a hagyományos e-mail alapú forma mellett már gyakran **social engineering, azaz pszichológiai megtévesztéses eszközeivel is éltek.**



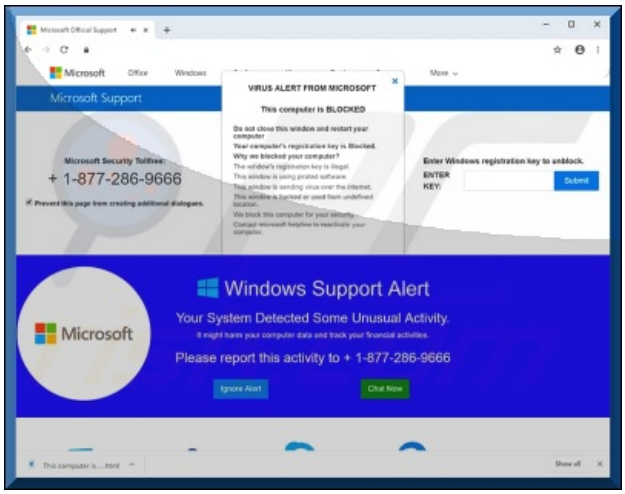
A célzott és a kis számú, de alaposan kiválasztott célpontok felé irányuló támadások gyakran felhőalapú tárhelyeket is igénybe vettek, és **az összes fenyegetés közül az adathalász támadások voltak jelen a legnagyobb számban, ez 67%-ot jelentett. A céges levelező hálózatok elleni incidensek mennyisége is erőteljes emelkedést mutatott, ez 2022-ben 83%-kal nőtt az előző évhez képest.**

A Business E-mail Compromise (BEC) esetén a céges levelezés észrevétlen feltörése után olyan legitim, a vállalati partner nevében jelentkeznek be a csalók, amelynek élő beszállítói vagy egyéb kapcsolata van a vállalkozással, és **a bennfentes információk ismeretében komoly anyagi veszteségeket tudnak okozni, például hamis átutalásokkal.**



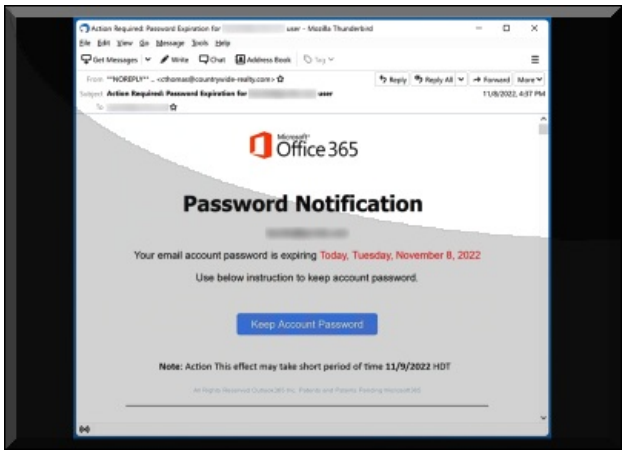
A hagyományos csatornák mellett a vishing, azaz **élő telefonos hangalapú megtévesztések is kiugró mértékben emelkedtek, ebben 363 százalékos emelkedést regisztráltak.**

A csalók gyakran a Microsoft vagy a LinkedIn nevével visszaélve jelentkeztek megtévesztő üzenetekkel vagy telefonhívásokkal. **A hamis support hívások leggyakoribb célja további érzékeny személyes, vagy bizalmas cégadatok megszerzése volt.**



A másik felmérés is hasonlóan riasztó adatokról számol be. A Barracuda 3.5 millió postafiókból származó 50 milliárd e-mail elemzésére támaszkodva azt állapította meg, hogy a megkérdezett 1350 **szervezet fele 2022-ben célzott adathalász támadás áldozata lett, míg egynegyedének legalább egy e-mail fiókját törték fel.**

Az esetek felében valamilyen vírus, vagy kártékony program is szerepet játszott az incidensben, és minden második áldozattól loptak el így érzékeny adatokat vagy bejelentkezési információkat.



Láthatóan a távmunka térnyerése is felpörgette a célzott adathalász támadások számát, így például azoknál a vállalkozásoknál, **ahol a munkaerő több mint 50%-a távolról dolgozik, átlag napi 12 gyanús e-mail érkezik.**

A sikeresen végrehajtott célzott támadások során érzékeny személyes adatok - például bankszámlaadatok, hitelkártyák és társadalombiztosítási számokat, belépési fiókadatokat sikerül ellopni, de gyakori a szellemi tulajdon elleni, adatbázisok és forráskódok kiszivárgása is. **Gyakori módszer a Microsoft 365-ös környezet elleni támadási forma is.**



És hogy a végére legyen valami izgalmas, a Bleeping Computer beszámolója szerint **az USA Georgia állambeli Augusta városát - benne legalább három kritikus infrastrukturális szektort, kormányzati létesítményeket, a pénzügyi, valamint az élelmiszer- és mezőgazdasági szervezetet támadott meg a BlackByte ransomware csoport.** A 610 ezres lakosú városban ennek következtében részlegesen leállt az informatikai rendszer.

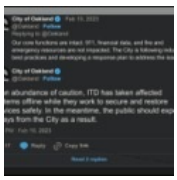
Az elkövetők szerint 10 GB adatot sikerült zsákmányolniuk, és egyes beszámolók szerint 50 millió dollárnak megfelelő (17 Mrd forint) váltságdíjat követelnek, amit a városi cégvezetés egyelőre cáfol.

Megosztom tumblr. Tweet Pin it Tetszik 0

1 komment
Címkék: statisztika usa phishing váltságdíj adathalászat adatlopás augusta ransomeware zsarolóvírus doxing

Ajánlott bejegyzések:

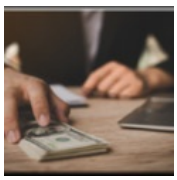

9 millió, bizony, dalolva ment...


Ország, város, ransomware


Ransomware támadás a Nissan ellen



8 kórház, 30 klinika, 2.5 millió betegadat


Megváltás-e a váltságdíj?

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Mesterséges Geci 2023.05.28. 07:11:24

Fura. Esküdni mertem volna, hogy biztonsági szakember vagy

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

1399

A belső ember II.

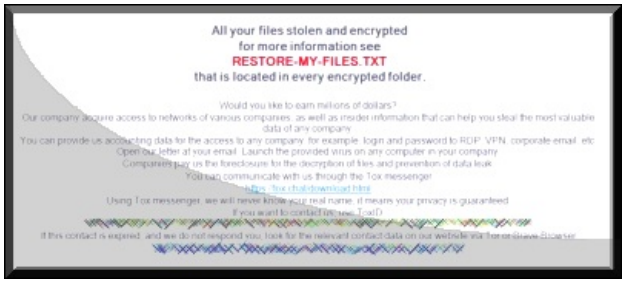
2023. május 30. 11:32 - Csizmazia Darab István [Rambo]

Ma már a szervezetek nagy része a belső fenyegetéseket komoly kockázati tényezőnek ismeri el. Az alkalmazotti hibák leggyakoribb okairól egyszer már szerepelt egy poszt, amiben első helyre a véletlen, nem szándékos emberi mulasztás és hiba került, második lett a gondatlanság: szakmai ismeretek hiánya, vagy például a figyelmeztetések semmibevétele, magyarán a fegyelmezetlenség. A harmadik helyre viszont a tudatos, rosszindulatú támadások kerültek.



Az informatikai incidensek **egy jó részénél gyakran van valamiféle belső szál, ahol egy korrupt vagy bosszúálló egykori vagy jelenlegi alkalmazott segíti a külső támadókat.**

Emellett azt az új módszert is láttuk már, hogy **a mai modern ransomware bűnözői csapatok közvetlenül sértett munkavállalókat, bennfenteseket toboroznak, és pénzjutalmat ígérnek azoknak, akik cégük RDP, VPN, levelező szerver, és egyéb belső vállalati rendszereikhez hozzáférést, jelszavakat adnak át számukra.** A toborzók a pénz mellé teljes anonimitás is ígérnek a besúgónak.



A mostani eset kicsit más, itt nem akármilyen belső emberről van szó. Az Oxford Biomedica egykori IT biztonsági munkatársa beismerő vallomást tett egy 2018-ban történt zsarolóvírus támadással kapcsolatban.

Az oxfordi székhelyű gén- és sejtterápiás céget korábban egy ransomware támadás érte, amelynek során adatlopás is történt: illetéktelenül hozzáfértek bizalmas céges adataik egy részéhez, a támadók pedig 300 ezer angol fontnak megfelelő összeget követeltek Bitcoinban.



Ashley Liles biztonsági elemzőként részt vett ennek a bűncselekménynek a felderítésében a hatóságokkal együtt működve, ám a vizsgálat során az akkor 28 esztendős férfinek az az ötlete támadt, ha már van egy ilyen alkalom, megpróbálhatna saját zsebre dolgozni.

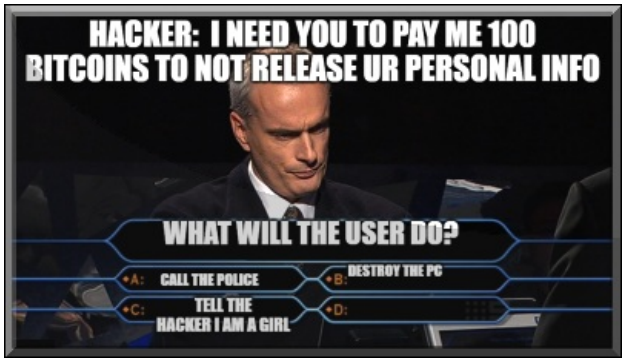
Az utólagos forensics vizsgálatok bebizonyították, hogy legalább 300 alkalommal lépett be illetéktelenül a cégük egyik igazgatósági tagjának levelezésébe, és beregisztrált egy a támadóhoz nagyon hasonló e-mail

címet, majd a már általa küldözgetett újabb levelekben megváltoztatta az eredeti támadó által megadott fizetési adatokat a sajátjára.



Az Oxford Biomedica végül alapos megfontolás után megtagadta a váltságdíj fizetést, így a támadók és a belsős csaló is hoppon maradt. A **nyomozás viszont bebizonyította, hogy a levelezéshez történt illetéktelen hozzáférés Liles otthonából származott, ami kicsit azt is mutatja, nem ő volt a legélesebb kés a fiókban.**

Az ezt követő házkutatás során számítógépeket és mobiltelefont is lefoglaltak nála, és bár Liles napokkal a letartóztatása előtt megpróbálta törölni az eszközeit, de a törvényszéki szakértők ezeket az adatokat vissza tudták állítani, ami szintén azt mutatja, hogy nem egy szofisztikált mesterbűnözőről van szó.



Az eset a hatóság szerint arról szól, hogy figyelmeztetés legyen ez mindenkinek, aki ilyen típusú bűncselekmény elkövetését fontolgatja. **Az is egy fontos tanulság, hogy a vállalatoknak nagyon kell figyelnie az esetleges belső érintettségekre is.**

De azért emellett talán arról is szól egy kicsit, hogy aki nem a saját kíváncsiságától hajtva, rengeteg molyolással, lelkes önképzéssel lesz hacker, hanem iskolában padban könyvből tanulja, és csak azért csinálja, mert ezzel pénz akar majd keresni, az valószínűleg nehezebben vagy sosem ér fel egy bizonyos szintre. Kicsit olyan ez, mint a vicc: "*Mi a különbség a pacsirta és a veréb között? A veréb levelezőn végezte a Zeneművészetit...*"

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: céges alkalmazott bűnöző belső vállalati ransomware zsarolóvírus

Ajánlott bejegyzések:

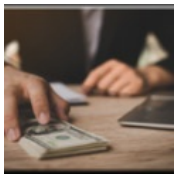

Ransomware támadás a Nissan ellen



8 kórház, 30 klinika, 2.5 millió betegadat


ChatGPT: hogyan használjuk a munkában?


LockBit piacgazdaság és tervgazdálkodás


Megváltás-e a váltságdíj?

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

535

Biztonság + kényelem = jelszókezelő

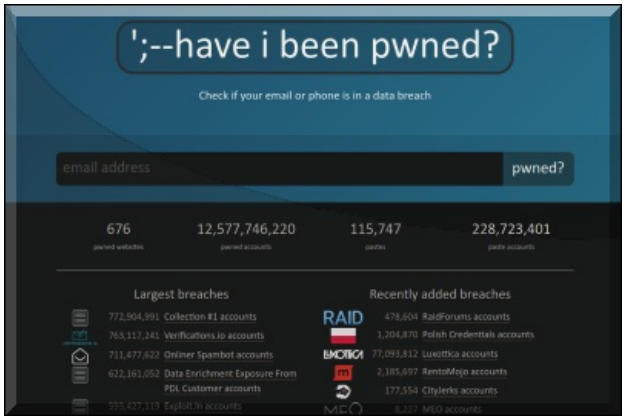
2023. június 01. 18:29 - Csizmazia Darab István [Rambo]

Fontos, hogy egyedi, erős jelszavakat használjunk minden egyes online fiókunk esetében. Egy jelszókezelő remek megoldást nyújt ezek megjegyzésére és kényelmes előhívására. **De hogyan válasszunk közülük**, hogy biztonságban legyenek az adataink?



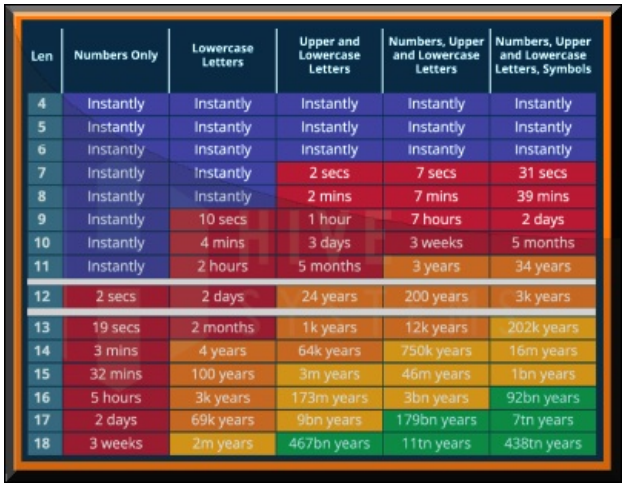
Egy 2022-es jelentés szerint **24 milliárd felhasználónév és jelszó kombináció kering a kiberbűnözői piacon, ami 65 százalékos növekedést jelent 2020-hoz képest.**

A felhasználók **sajnos gyakran ugyanazokat a belépési adatokat adják** meg kényelmi szempontok miatt, amit a hackerek **ki is használnak úgy, hogy az ellopott jelszavakat minden népszerű online szolgáltatásban végigpróbálják, így egyszerre akár több fiókhoz is hozzáférhetnek.**



Ahogy régen a nagyszüleink még nyitva hagyták a kertkaput, ma pedig már mindig bezárjuk, úgy az online térben is gondolnunk kell a biztonságunkra, mivel a csalási módszerek és a kártevők is folyamatosan fejlődnek és egyre gyakoribbak. Miért is fontos az erős jelszavak használata? Kiterjedt adatvédelmi incidensek során a jelszavainkat ellophatják azoktól a szolgáltatóktól, vállalatoktól, amelyek weboldalán fiókot regisztráltunk.

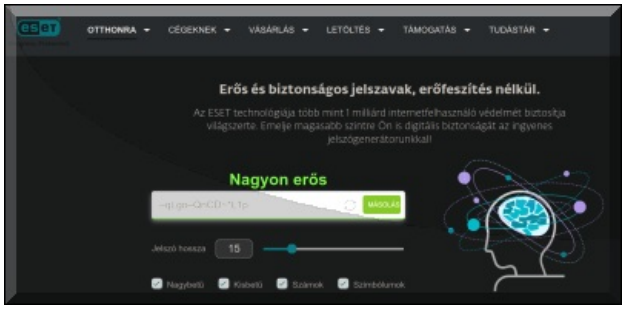
A csalók gyakran az általunk használt közösségi médiumok, streaming szolgáltatók vagy bankok alkalmazottainak adják ki magukat, hogy tőlünk is megpróbálják kicsalni a jelszavainkat. Automatikus brute force-támadások (próbálgatásos jelszó feltörés) során is ellophatják az adatainkat.



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

Ez utóbbi egy olyan módszer, ami az összes lehetséges kombináció végigpróbálásával dolgozik. Először a leggyakoribb szótári variációkkal kezdi, és gyakran nincs is nehéz dolga: friss kutatások szerint világszerte sokan még mindig a jelszó főnév angol megfelelőjével, a “password” szóval és az “123456” számsorral védik az adataikat.

A leggyakoribb 10 jelszó akár egy másodpercen belül feltörhető. Ezzel szemben a bonyolult jelszavak feltöréséhez akár 3000 év is kellhet.

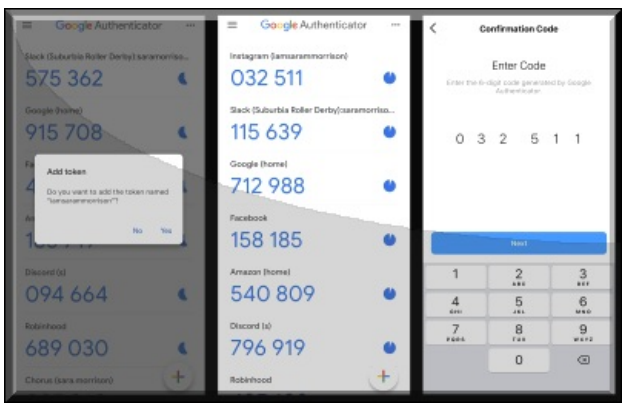


A jelszókezelők olyan alkalmazások, amelyeket a jelszavak biztonságos helyen történő tárolására terveztek. **A jelszószéf szoftver egyetlen mester jelszót kér a felhasználótól, attól kezdve minden mást már automatikusan kezel az alkalmazás - ideértve a hosszú, egyedi jelszavak automatikus létrehozását és a belépési mezők kitöltését minden egyes webhely esetében.** Íme, néhány fontos szempont és funkció, amely segíthet eligazodni és megfelelően választani:

- Erős titkosítással rendelkező jelszóvédelem. Ez azt jelenti, hogy még ha a jelszókezelő szolgáltatóját meg is hekkelik, a támadók nem lesznek képesek ellopni az ügyfelek hitelesítő adatait. Az iparági szabvány az AES 256 bites titkosítás.

- Erős jelszógenerátor, amelyet úgy terveztek, hogy minden jelszó esetében egy hosszú, véletlenszerű számokból, betűkből és szimbólumokból álló sorozatot javasoljon. Így gyakorlatilag kizárt, hogy egy hacker brute force-támadással feltörje a jelszavakat. Ha szeretne ízelítőt kapni abból, hogy miről is van szó, próbálja ki az ESET saját, ingyenes jelszógenerátorát.

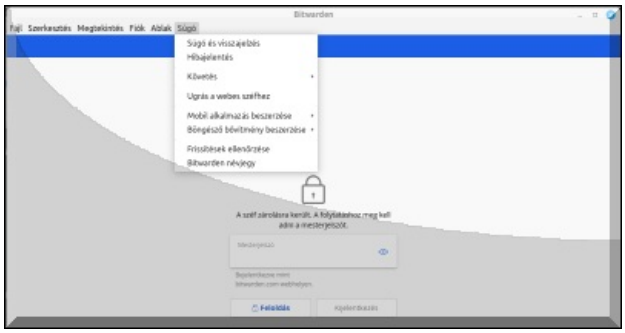
- Multiplatform és böngésző támogatás lehetősége. A jelszókezelők csak akkor hasznosak, ha tárolják és előhívják a jelszavakat minden kedvenc webhelyen és alkalmazásban. Ezt nagyban segíti, ha a jelszókezelő képes a hitelesítő adatokat böngészőkből és más jelszókezelőkből importálni.



- Automatikus kitöltési/bejelentkezési lehetőség. A jelszókezelő egyik legfontosabb tulajdonsága, hogy a fő jelszó megadása után automatikusan kitölti az egyes fiókokhoz rendelt erős, komplex jelszót.

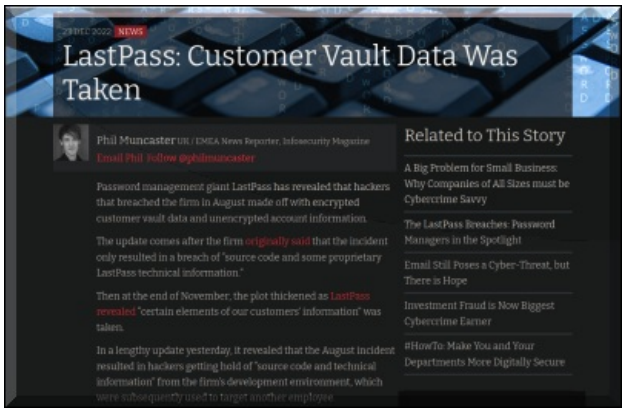
- Távoli kijelentkezteti lehetőség. Fokozza a biztonságot és az adataink védelmét, ha a jelszókezelő lehetővé teszi a fiókokból való távoli kijelentkezést, a böngészési előzmények és sütik törlését, valamint a nyitott böngészőlapok távoli bezárását.

- Integráció kétfaktoros hitelesítéssel (2FA). Bár a jelszókezelők fontosak, a személyazonosság- és hozzáférés-kezelés aranyszabálya a 2FA, amelynél a jelszó mellett egy második "tényezőre" is szükség van a belépéshez, például arcszkennelésre vagy egyszer használatos jelszó megadására. Egy olyan jelszókezelő, amely integrálható a népszerű, harmadik féltől származó 2FA alkalmazásokkal, például a Google Authenticatorrel, segít optimalizálni az élményt.



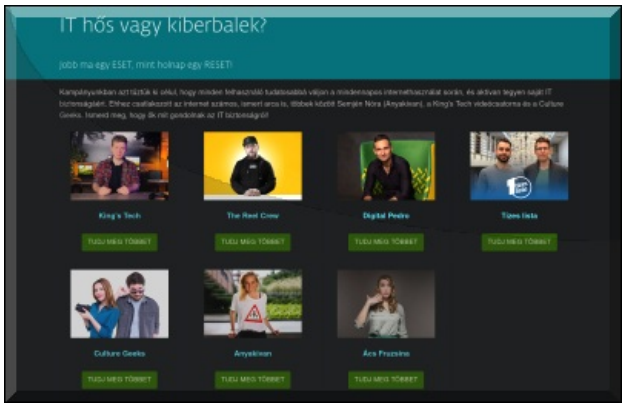
- Mesterjelszó visszaállítása funkció. Elfelejtettük a mesterjelszavunkat? Ha nincs visszaállító funkció, akkor az összes jelszavunk egy olyan digitális széfbe lesz elzárva, amelyet nem tudunk kinyitni.

- Megbízható, neves szolgáltatót érdemes választani. Amennyiben a jelszókezeléssel foglalkozó céget feltörik, az összes jelszavunk rossz kezekbe kerülhet, ezért győződjünk meg arról, hogy a vállalat jó biztonsági háttérrel rendelkezik. Az egyik népszerű szolgáltatót nemrégiben súlyos biztonsági incidens érte, amely során nyilvánosságra kerültek az ügyfelek titkosított jelszavai, végül pedig arra szólították fel a felhasználókat, hogy változtassanak jelszót.



- A biztonsági jelentések funkció segítségével folyamatosan fejleszthetjük, erősíthetjük jelszavainkat azáltal, hogy megismerjük bejelentkezési adataink gyengeségeit.

- Helyi vagy felhőalapú tárolás? Ez egy kicsit nehezebb kérdés, és figyelembe kell vennünk a saját körülményeinket is. A helyi tárolás sok esetben jobb ellenőrzést és biztonságot nyújt, de eszközeinket ellophatják, feltörhetik, el is veszíthetjük vagy akár a merevlemez is meghibásodhat. A központosított, felhőalapú megoldás ilyen tekintetben kényelmesebb, de ennek is megvannak a maga potenciális hátrányai, többek között az, hogy teljes mértékben meg kell bíznunk az adott szolgáltatóban. **Van egy harmadik lehetőség is, egy olyan tárolóhely használata, amely lokális adatbázist használ, de a saját felhőfiókunk őrzi egy olyan felhőszolgáltatónál, amelyben megbízunk.** Végső soron a jelszavak biztonsága az erős titkosításon (1. pont) és az adott kiberbiztonsági körülményeken múlik.



Fontos, hogy ne feledkezzünk meg a jelszókezelők - vagyis valójában a jelszavak - korlátairól. A jelszó egyetlen védelmi vonalat jelent, és nem biztos, hogy elegendő a bűnözők ellen. Következésképpen (és ezt nem tudjuk eléggé hangsúlyozni), **használjunk két- vagy többfaktoros hitelesítést, így sokkal nagyobb eséllyel tarthatjuk távol magunktól a hackereket.**

Az IT-hős vagy kiberbalek kampányban ismert influencerek állnak a kiberbiztonság ügye mellé, ők próbálják kiléptetni a felhasználókat a „tudom, hogy fontos, de nincs rá időm” hozzáállásból, és aktív cselekvésre bírni őket - hiszen mindenkinek zárva kell tartania saját virtuális ajtajait. Hogy miért jobb ma egy ESET, mint holnap egy RESET? Kiderül a videókból!

Megosztom tumblr. Tweet Pin it Tetszik 0

3 komment
Címkék: jelszó password jelszómenedzser jelszószéf jelszókezelő

Ajánlott bejegyzések:



Ne reszkessetek betörők!



Még gyengébb a jelszavad



C mint CEO, P mint password



Gyenge, gyengébb, leggyengébb



Kibermalac színre lép

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.



Androsz · http://wikipedia.blog.hu/ 2023.06.02. 18:53:43

Van két kulcsom a lakásajtóhoz, egy a pincéhez, egy a garázshoz, egy az autóhoz, egy a műhelyhez, egy a munkahelyemhez, egy a postafiókomhoz. Tartok attól, hogy ezeket valaki megszerzi és visszaél vele. Ezért kitaláltam, hogy veszek egy páncélkazettát, abba beleteszem az összes kulcsot, a kazettát kucsra zárom és csak egy kulcsot tartok magamnál.

Mostantól a tolvajnak elég EGYETLEN kulcsot ellopnia tőlem, és hozzájut mindenemhez. Hát ennyit a jelszókezelő értelméről.

"A leggyakoribb 10 jelszó akár egy másodpercen belül feltörhető. Ezzel szemben a bonyolult jelszavak feltöréséhez akár 3000 év is kellhet."

A feltöréshez semennyi idő nem elég, ha a program vagy weboldal, ahová a jelszó való, nem engedi, hogy ezerszámra tegyen valaki kísérletet rajta a jelszavakkal. Vannak más bejutási lehetőségek is, kizárólag nagyon profik által ismert trükkök, de ha Ön, kedves Olvasó, olyan programot vagy weboldalt talál, ahol akárhány próbát tehet a jelszóval a riasztás, letiltás veszélye nélkül, akkor csináljon belőle nagy balhét, mert a programozó ostoba és lusta volt, a szolgáltató pedig nem törődik a felhasználó biztonságával.

Mindemellett valóban legyen körültekintő, használjon hosszú, lehetőleg véletlenszerű jelszavakat, és ne bízza őket a világon senkire.

Válasz erre



Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2023.06.03. 06:03:15

@Androsz:

Sajnos a "kulcsainkat" sokszor kockáztatjuk vagy kockáztatni kényszerülünk, pl. edzőterembe vagy strandra mész és az ottani széfbe bepakolod mindazt, amit felsoroltál: kocsikulcs, lakáskulcs, jogsi, forgalmi, személyi, pénztárca, mobiltelefon, bankkártya. Az uszodában, strandon nem is tudod másképp megoldani, mint mindent egy helyre.

A széfes példád azért ha annak a statisztikáját nézzük, valószínűleg pozitív, beváltja a hozzáfűzött reményeket. Szélsőséges esetben meg semmi nem véd meg: túszul ejtenek, megkínoznak, akkor mindegy hogy egy kulcsot adsz oda, vagy nyolcat. Ez viszont szerencsére ritka.

A tippek főleg azoknak szólnak, akik a többség, és a 2FA meg a megbízható jelszószéf számára előre lépés lenne a "password", "qwerty" jelszavai helyett, a mindenhol ugyanazt a "kutyuska56"-ot használás helyett, a monitorra ragasztott POSTIT helyett.

Sok igazság van ebben amiket írsz, de oké, akkor mondj jobbat a többség számára, mint egy helyben titkosítva tartott jelszószéf + 2FA, MFA kombó?

Válasz erre



aranyláz 2023.12.16. 20:21:26

@Androsz: "Mostantól a tolvajnak elég EGYETLEN kulcsot ellopnia tőlem, és hozzájut mindenemhez. Hát ennyit a jelszókezelő értelméről."

Nem igaz, hiszen pl a Bitwarden jelszókezelőnél is, ha be van állítva, ha egy új eszközről próbálnak bejelentkezni, akkor kéri a 2. faktort a hitelesítéshez, vagyis pl. a hatjegyű kódot, tehát önmagában a mesterjelszó ismerete nem elég a belépéshez. De vannak egyéb lehetőségek is, mint pl. Yubikey kulcs, amivel még biztonságosabbá tehető.

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

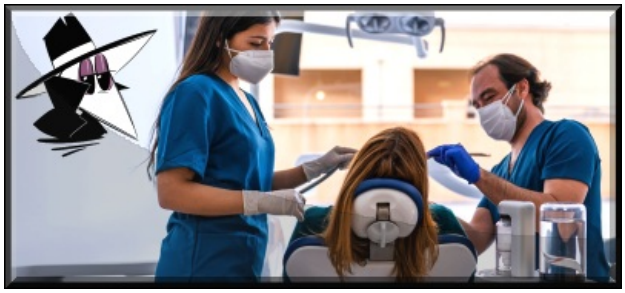
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

2388

9 millió, bizony, dalolva ment...

2023. június 06. 10:27 - Csizmazia Darab István [Rambo]

Kifejezett trend már évek óta, hogy az egészségügyi intézményeket, kórházakat célzottan támadják a zsarolóvírus bandák. Ezúttal egy amerikai f**ogászati biztosító vált áldozattá, hozzávetőlegesen kilencmillió ember bizalmas személyes adatai kerültek veszélybe.**



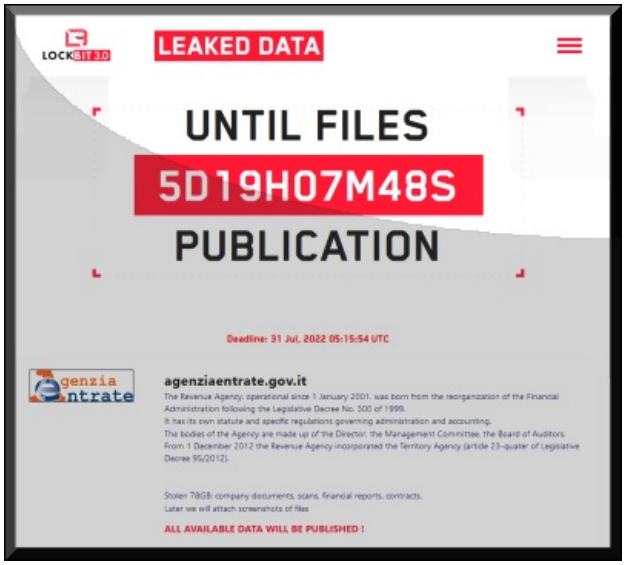
Kórházak a pácban, Nem csitulnak a kórházak elleni támadások és hasonló címekkel már mi is többször beszámoltunk hasonló támadásokról, **és az ilyen incidensek elég gyakoriak lettek.** A fő okok között gyakori az elégtelen anyagi források, gyenge IT infrastruktúra felemlítése, az elenyésző létszámú vagy hiányzó informatikai biztonsági személyzet, általános túlterheltség, valamint a komoly nyomás az üzletmenet folytonosságban.

Sajnos az is előfordul, hogy gyermekkórházak válnak áldozattá, mint például a kanadai SickKids kórház elleni ransomware támadásnál, ahol műtéteket, kemoterápiás kezeléseket voltak kénytelenek elhalasztani, és betegeket is át kellett helyezniük más társintézményekbe a belső informatikai rendszerük leállása miatt.



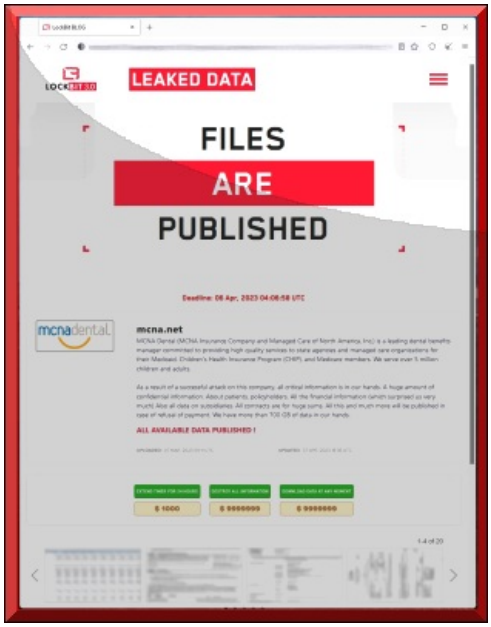
Ezúttal az USA-beli Managed Care of North America (MCNA) Dental fogászati biztosítási óriáscég észlelte, hogy illetéktelen behatolás történt. A támadók a hivatalos bejelentés szerint 2023. február 26. és március 7. között fért hozzá és szerezhetett meg érzékeny információkat a számítógépes rendszerből. Ezek **a betegek személyes adatait tartalmazták, beleértve a neveket, lakcímeket, születési dátumokat, telefonszámokat, e-mail címeket, társadalombiztosítási számokat és jogosítvány számokat vagy más, államilag kibocsátott személyazonosító számokat.**

A támadók ezenfelül hozzáfértek a betegek egészségbiztosítási adataihoz is, beleértve a kezelési terveket, egészségügyi Medicaid azonosítószámokat, röntgen felvételeket, valamint a korábbi kezelési számlákra és a biztosítási igényekre vonatkozó információkat is.



Az MCNA Dental szerint **egyes esetekben gyermekek személyes adataihoz is hozzáfértek. A LockBit ransomware csoport időközben vállalta a felelősséget a fenti kibertámadásért, és április 7-én végül közzétették az összes fájlt, amelyet kiszivárgott az MCNA Dentalból, miután a cég megtagadta tőlük a 10 millió dolláros váltságdíj kifizetését.** Beszámolók szerint azt ellopott adatmennyiség 700 GB volt.

A vállalat állítólag értesítést küldött az érintett személyeknek, és ebben egy éves ingyenes személyazonosság-lopás elleni védelmet és hitelfelügyeleti szolgáltatást is felajánlottak. **Az áldozatok emellett nagy eséllyel számíthatnak további, más bűnözői csoportok által indított célzott adathalász támadásokra is, amelyekkel további bizalmas információkat, hitelesítő adatokat igyekeznek majd megszerezni tőlük.**



A LockBit egy Oroszországhoz köthető bűnözői csoport, amelyet először 2019 szeptemberében figyeltek meg. A banda már számos nagy horderejű támadást intézett jelentős célpontok ellen, így többek közt a Royal Mail brit postavállalat, az Ion Group pénzügyi szoftvercég, az olasz adóhivatal és a kaliforniai Pénzügyminisztérium elleni incidens is az ő számlájukra írható.

Érdekesség még, hogy fent említett **SickKids kanadai rákellenes gyermekkórház esetében akkor és ott elítélték a velük szerződött alvállalkozói bűnözői partnerük ezen akcióját, és ott a LockBit vezérkar nyilvánosan is elnézést kért**, valamint egy ingyenes dekódolót tettek közzé az áldozatok számára a fájlok mielőbbi sikeres helyreállításához.

Megosztom tumblr. Tweet Pin it Tetszik 0

1 komment
Címkék: amerika usa egészségügy biztosító egyesült fogászat államok váltságdíj adatlopás adatszivárgás dental ransomware zsarolóvírus doxing lockbit mcna

Ajánlott bejegyzések:



[Ransomware támadás a Nissan ellen]



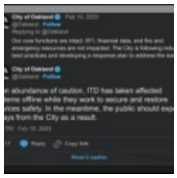
[8 kórház, 30 klinika, 2.5 millió betegadat]



[Bajban Venezuela legnagyobb bankja]



[Ransomware támadás érte az MSI-t]



[Ország, város, ransomware]

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

gigabursch 2023.06.06. 12:08:25

Számomra érthetetlen a megfelelő rendszerek fizikai különválasztásának lehetetlensége.

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

Kiaboys és Hyundai challenge elmentek vadászni

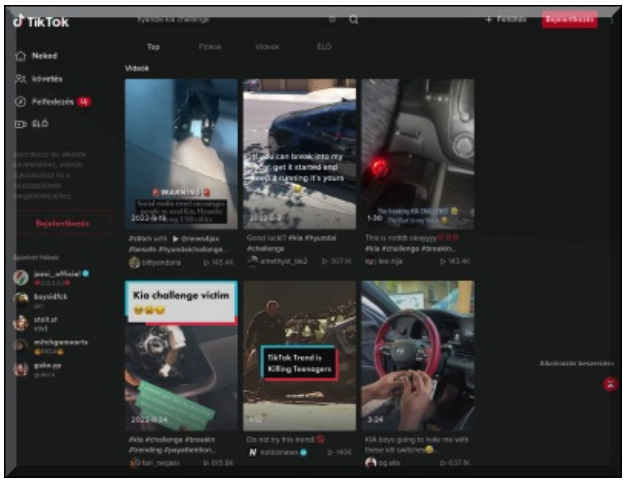
2023. június 09. 10:16 - Csizmazia Darab István [Rambo]

Kiugró mértékben elszaporodtak a fenti két gépjármű típussal kapcsolatos lopások az Egyesült Államokban, ami főképp a gyártók hibájának róható fel, de **a jelenség továbbgyűrűzését persze a TikTok platform is keményen felsrófolta a címben található hashtag címkével feltöltött vírusként terjedő videókkal.**



Lopások már 2020-ban is történtek, ám tavaly óta egyre nagyobb számban szerepeltek a híradásokban, és a tizenévesek körében zajló lájkvadász TikTok kihívás csak extra olaj volt a tűzre. **Az útmutatóban az szerepelt, hogy egy Kia vagy Hyundai autót csavarhúzóval és telefontöltő kábellel milyen egyszerű beindítani, ellopni** - betörve előtte egy ablakot, és szétbombázva közben a műszerfal alját.

Pórul járt tulajdonosok tömegei panaszkodtak a közösségi oldalakon, és tették meg a feljelentéseket is. A hírekben elsősorban az Egyesült Államokbeli károsultak szerepeltek, volt aki éppen temetésen volt, miközben ellopták a gépjárművét. **Az elkövetők közt pedig volt 11 éves tolvaj is.**



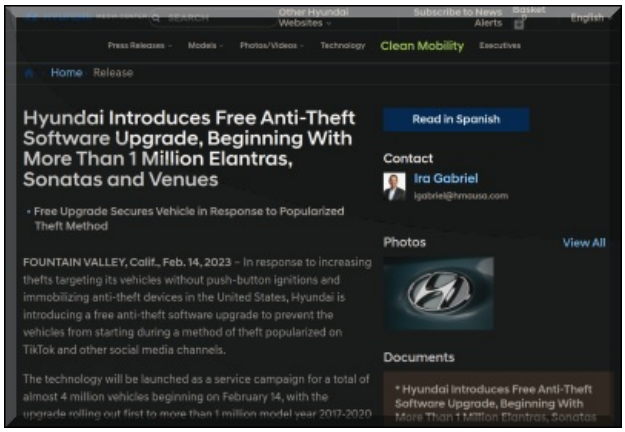
A rendőrség is felfigyelt a szokatlan és tömeges jelenségre, és azt javasolták, hogy az autótulajdonosok szerezzenek be egy plusz kormányzárat, ami jól látható módon elriaszthatja a kihívásra nyitott, zömében Z generációs fiatalokat - akik ezzel valójában bűncselekményt követnek el. **Most New York állam is pert indított a két nevezett autógyártó ellen, arra hivatkozva, hogy túlságosan könnyű ezeknek a gyártmányoknak az ellopása, vagyis költségcsökkentő lépésekkel nem tettek meg mindent ennek kizárására.**

Ugyanis az európai és kanadai piacokon régóta kötelező előírás az indításgátló beszerelése, ám ez a szabályozás viszont az USA-ban hiányzott. Korábban már több város is beperelte ugyanezen hanyagság miatt az autógyártókat, többek közt Baltimore, Cleveland, Milwaukee, San Diego, és Seattle is, **és ezekben a perekben kártérítést követelnek tőlük.**



A közzétett statisztika szerint 2023. első négy hónapjában 977 alkalommal loptak el Hyundai és Kia autókat New Yorkban, ez pedig elképesztő mértékű, nagyjából 660 százalékos növekedést jelent az előző évhez képest.

A tolvajok valóban könnyűszerrel képesek 60 másodperc alatt elhajtani a kiszemelt járművel, és **a sérülékenység egy csomó 2011. és 2022. között az USA részére gyártott modellt érint:** Hyundai Accent, Elantra, Elantra GT, Elantra Coupe, Elantra Touring, Genesis Coupe, Kona, Palisade, Santa Fe, Santa Fe XL, Santa Fe Sport, Sonata, Tucson, Veloster, Venue és Veracruz; valamint a Kia Forte, K5, Optima, Rio , Sedona, Seltos, Sorento, Soul és Sportage.



A lopáson felül a tinédzserek ezután gyakran okoztak különféle közlekedési baleseteket is. Az Egyesült Államok Nemzeti Közúti Közlekedésbiztonsági Hivatala (NHTSA) szerint legalább 14 bejelentett balesetről és nyolc halálos áldozatról tud az ilyen jellegű feltörés követően. I**dőközben a két gyártó első körben szoftver frissítés kiadásával próbálta orvosolni a helyzetet**, például a Hyundai tájékoztatása szerint az ingyenes frissítést a márkakereskedők végzik el, ami hozzávetőlegesen egy órát vesz igénybe. A Kia egyelőre csak a szakaszos frissítésről szóló tervezetéről nyilatkozott még idén februárban.

A dolgot persze bonyolítja, hogy itt több millió járműről van szó. Lehet hogy inkább érdemes lett volna már korábban a szabályozáson módosítani, és Európához hasonlóan itt is kötelezően előírni az indításgátló gyári beszerelését.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: autó lopás kia hyundai gépjármű tiktok kiaboys

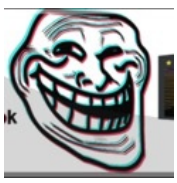
Ajánlott bejegyzések:


Ransomware támadás a Nissan ellen



Csalás jönni TikTokra


Ezer százalék lett, maradhat?


TikTok VS. AgainstTheWest

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

420

Csalás jönni TikTokra

2023. június 13. 09:51 - Csizmazia Darab István [Rambo]

A TikTok továbbra is rekordokat döntöget felhasználóinak folyamatosan növekvő számával, így aztán a platform sajnos a csalók számára is egyre vonzóbbá válik. **A rövid videók megosztására és megtekintésére alkalmas felület mindössze hat év alatt meghatározó közösségi médiummá vált, a brit és amerikai felhasználói pedig már több időt töltenek el az alkalmazásban, mint a YouTube-on.**



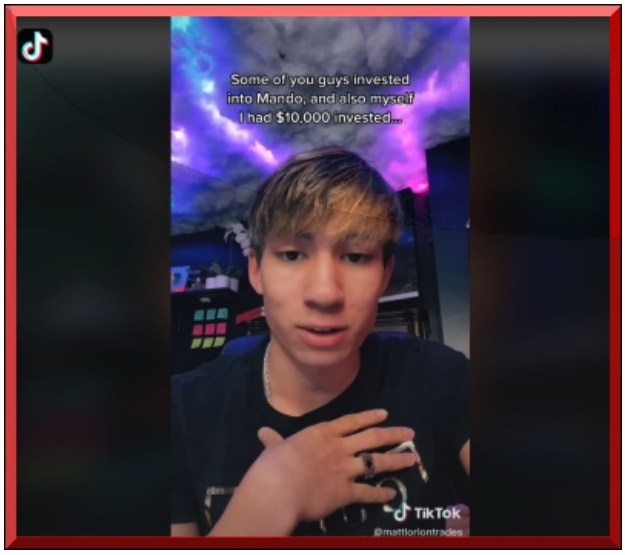
Eközben jó kérdés, hogy mennyire vagyunk tisztában a világ egyik legnépszerűbb közösségi médiumának veszélyeivel? **Hogyan kerülhetjük el az átveréseket és maradhatunk biztonságban a TikTokon is, és hogyan tudunk ebben támogatást adni gyermekeinknek?**

Nos a kiberbűnözők folyamatosan követik a trendeket, a **TikTokot pedig naponta több mint 1,2 milliárd felhasználó látogatja,** ráadásul hivatalosan már tizenhárom éves kortól lehetséges fiókot létrehozni az alkalmazásban. És mialatt az emberek órákon keresztül görgetik a videókat az alkalmazásban, a csalások könnyen felkészületlenül érhetik őket.



Ahogy régen a nagyszüleink még nyitva hagyták a kertkaput, ma pedig már mindig bezárjuk, úgy **az online térben is gondolnunk kell a biztonságunkra, mivel a csalási módszerek és a kártevők is folyamatosan fejlődnek és egyre gyakoribbak** - így bizony gyerekeinket is veszélyeztetik.

Az ESET IT-hős vagy kiberbalek kampányában arra hívja fel a figyelmet, hogy a digitális biztonság alapszükséglet. A kampányban részt vesz Ács Fruzsina, a Dumaszínház tagja, aki a humor eszközével igyekszik tudatosítani: **ahogy nem megyünk át bekötött szemmel a zebrán, úgy megfelelő védelem nélkül se hagyhatjuk digitális eszközeinket.**



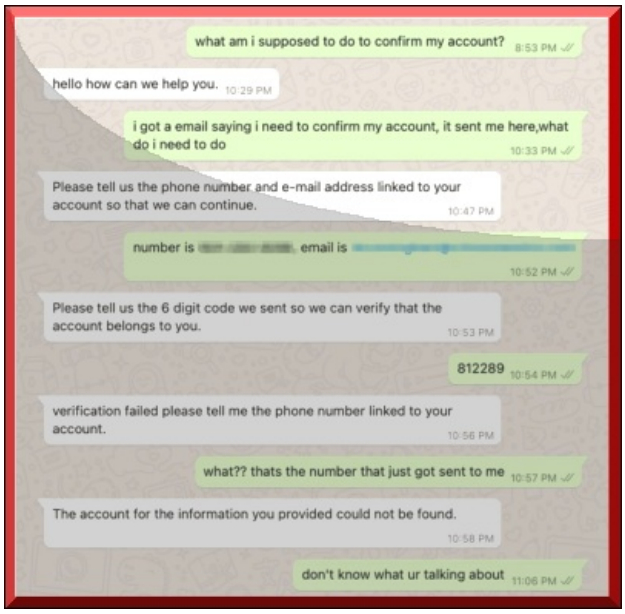
Az ESET szakértői **összegyűjtöttek öt tipikus TikTok átverést, amelyekkel jobb ha tisztában vagyunk.**

1. Gyors meggazdagodást ígérő átverések és kripto csalások
A szélhámosok gyakran úgy húzzák csőbe áldozataikat, hogy **hatalmas hasznot ígérnek kevés erőfeszítésért cserébe. A népszerűvé váló (és gyakran bezuhanó) kriptovaluták általában nagy visszhangot váltanak ki az interneten, a korábbi e-mail, Facebook, YouTube, társkereső platfromok után/mellett újabban sokszor a TikTokon is megpróbálják átverni ezzel az embereket.** Az ajánlatok viszont túl jól hangzanak ahhoz, hogy igazak legyenek - és többnyire nem is azok.



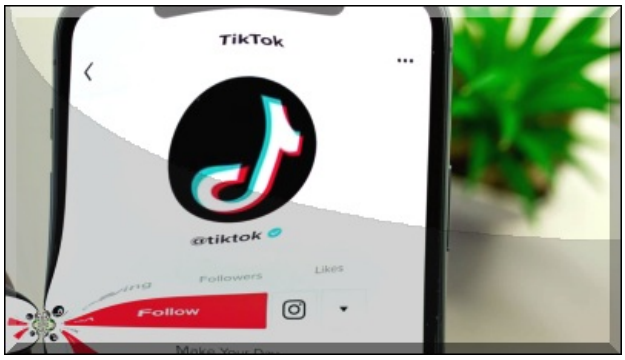
2. Adathalász TikTok üzenetek
A TikTokon terjedő csaló e-mailek vagy szövegek olyan üzenetek, amelyeket az adathalász levelekhez hasonlóan véletlenszerűen küldenek ki, abban a reményben, hogy egy tiktoker postaládájában landolnak. **Felajánlhatnak ellenőrzött jelvényt a TikTok fiókhoz, ígérhetnek több követőt vagy jól jövedelmező szponzori együttműködést**. Egy hasonló csalásról az IT-hős vagy kiberbalek kampány egyik szereplője, King'Tech is beszámolt az alábbi videójában.

Amint a célpont rákattint az üzenetben található linkre, átirányítják egy olyan oldalra, ahol a TikTok bejelentkezési adatokat kérik. Ha nincs bekapcsolva a kétfaktoros hitelesítés (ami a TikTok-fiókokban nem alapbeállítás), az adatok átadása után a hackerek átveszik az irányítást a fiók felett, és akár ki is zárhatják a valódi felhasználót – akinek így, ha például egy influencerről van szó, ezzel akár a megélhetése is veszélybe kerülhet.



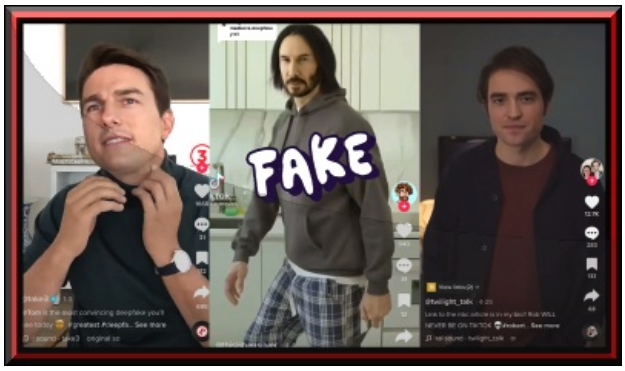
3. Botok, automatizált fiókok
A TikTok még mindig tele van bot-fiókokkal, amelyek ravaszul **úgy lépnek kapcsolatba az áldozatokkal, hogy a megcélzott felhasználók azt hiszik, egy valódi elő személlyel csevegne**k - a gyerekek pedig különösen sebezhetőek ebből a szempontból.

A **botok bizalmas adatokat kérhetnek célpontjaiktól, vagy akár egy csaló weboldalra irányíthatják át őket**, ahol megpróbálnak további személyes adatokat szerezni tőlük, vagy kártékony - például kém - szoftvereket telepíthetnek a telefonjukra.



4. Veszélyes alkalmazások
A TikTok hamis fiókjai időnként különféle letölthető alkalmazásokat hirdetnek, amelyek valójában átverések. Találkozhatunk olyan esettel is, amikor a fiók azt állítja, hogy bizonyos drága, fizetős alkalmazások egy külső féltől származó alkalmazásboltból viszont ingyenesen letölthetőek.

Ezek az alkalmazások azonban valójában a személyes adatainkra pályáznak, vagy kártékony szoftvereket, reklámprogramokat telepíthetnek a készülékeinkre.



5. Ál-hírességek
Egyes fiókok megpróbálhatják valódi hírességeknek kiadni magukat, általában lemásolva egy létező legitim sztár felhasználói fiókját. Az IT-HŐS kampányában például Anyakivan is beszámolt hasonló itthon, Magyarországon megtörtént csalásról.

A módszer lényege, hogy a csalók így próbálnak meg minél több követőt szerezni, és mielőtt lebuknának vagy jelentenék őket, a platformot jövedelmező átverésekre, például kriptopénz-befektetési csalások népszerűsítésére használhatják. Ez egy gyakori módszer, amelynek felnőttek, gyermekek rendszerint valóban bedőlnek.



Hogyan tartsuk hát biztonságban a gyermekeket a TikTokon? **Az adatok biztonsága érdekében érdemes bekapcsolni a kétfaktoros hitelesítést a gyermekek által használt fiókokon is. Fontos kiemelni, hogy más platformokhoz hasonlóan a TikTok sem fog velünk kapcsolatba lépni azért, hogy számlaadatokat, jelszavakat, egyszeri jelszót vagy más bizalmas információt kérjen. Ha mégis ilyen kérés érkezik, az biztosan átverés.**

Mivel elterjedt problémáról van szó, oda kell figyelnünk **a csalókra, akik folyamatosan próbálják megkörnyékezni a felhasználókat, hogy személyes adatokat szerezzenek tőlünk e-mailben vagy az alkalmazásban küldött**

kamu üzeneteken keresztül. Ha pedig arra gyanakszunk, hogy spam vagy adathalász videót látunk a TikTokon, azonnal jelentsük azokat a platformon, és semmiképpen ne kattintsunk rá az ezekben felkínált linkekre.



A gyerekek **a nyári szünidő ideje alatt az átlagosnál több időt tölthetnek el az számítógépes eszközök nyomkodásával,** a túlzott képernyőidő viszont negatívan befolyásolhatja fizikai és mentális egészségüket is. A Senso Media adatai szerint a magyar kamaszok átlagosan napi 8 óra 39 percet töltenek képernyő előtt, de ez a szám már a fiatalabb gyermekeknél is nagyon magas, átlag napi 5 óra 33 perc. Gyakran tartunk szülőknek előadásokat a gyerekek internethasználatáról. **A legfontosabb, hogy lefektessünk alapvető szabályokat, amelyeket aztán be is tartatunk, például az alábbiakat:**

- Válasszuk ki a gyermekek korának megfelelő eszközöket, és **szabjunk tematikus és időbeli korlátokat a használatukra.**

- Célszerű **szülői felügyeletet lehetővé tevő alkalmazásokat** is letölteni, mint az ESET megoldása is.

- Törekedjünk arra, hogy a gyerekek **a netezés mellett minőségi időt töltsenek el családtagjaikkal, könyvek olvasásával vagy szabadtéri programokkal, sportolással.**

- Ha már mindenképp képernyő, akkor **ösztönözzük gyerekeinket kreatív és interaktív programok használatára**, mint amilyen például a kisebbeknek való mobiltelefonos Crazy Gears applikáció vagy **a programozás alaplépéseinek játékos megtanulását segítő trinket.io weboldal, Digital Pedro segítségével.**

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: tanulás programozás gyermekvédelem python csalás átverés digital adathalászat pedro tiktok biztonságtudatosság kriptovaluta kriptobefektetés

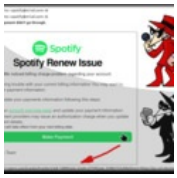
Ajánlott bejegyzések:


Nő a QR-kódos visszaélések száma


Kár érte, kiváló ügynök volt...



Adathalászat menni booking.com



Spotify megújítási probléma - vagy mégsem?



Üdvözöljük, csomagja kézbesítésre vár

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

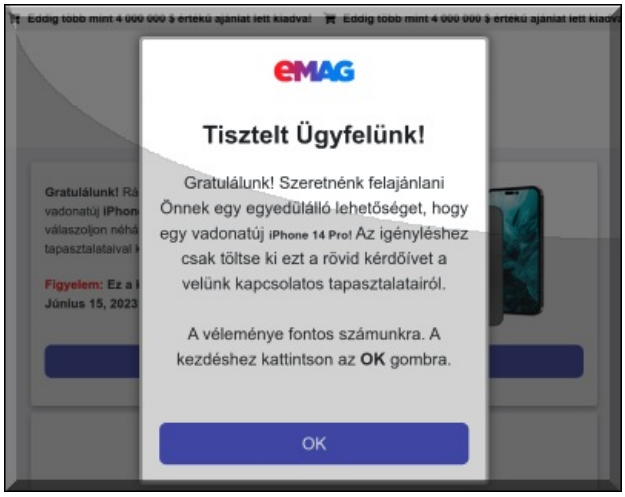
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

3428

Gratulálunk! Rád esett a választás!

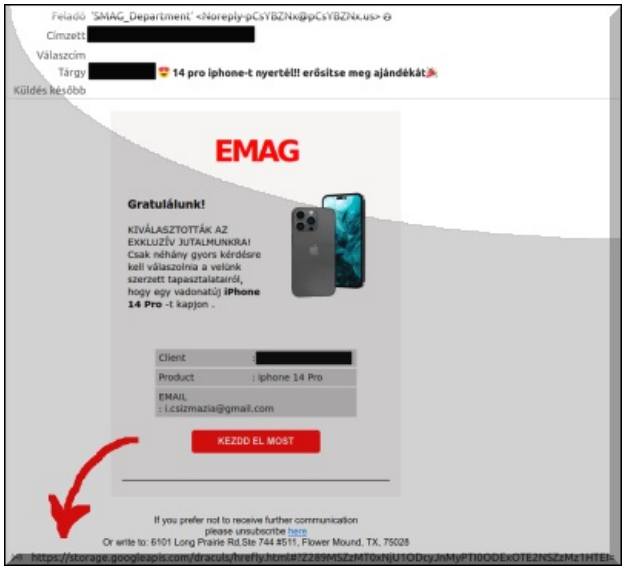
2023. június 15. 18:02 - Csizmazia Darab István [Rambo]

Gratulálunk! KIVÁLASZTOTTÁK AZ EXKLUZÍV JUTALMUNKRA! **Csak néhány gyors kérdésre kell válaszolnia a velünk szerzett tapasztalatairól, hogy egy vadonatúj iPhone 14 Pro -t kapjon** .



"KEZDD EL MOST!" Ezzel az üzenettel érkezik az e-mail, melynek a feladója távolabb már nem is eshetne a hivatalos EMAG áruház címétől. Valójában németországi a feladó, vélhetően egy fertőzött gépről küldhették ki a csalók.

Az átverős üzenet minden tipikus jegyet magán visel, a tegezős-magázós magyartalanság, az idegen domén, a körlevél típusú megszólítás, de a sürgetés sem maradt ki: "Figyelem: Ez a kérdőíves ajánlat ma lejár, Június 15, 2023".





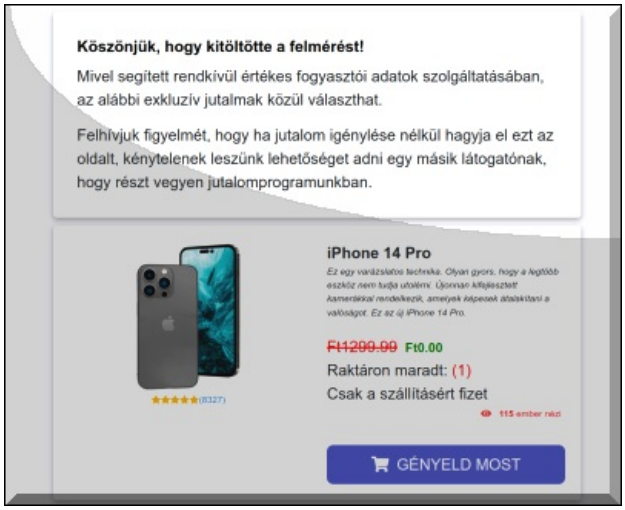
A gratulációs szöveg után **a nyeremény iPhone 14 Pro "igényléshez" kérik, hogy töltsünk ki egy rövid kérdőívet az EMAG nevében.** Ez a "KÉRDŐÍV INDÍTÁSA" után el is kezdődik, egy tíz pontból álló felmérés látszólag olyan kérdésekkel, amik jellemzően egy piaci kikérdezésben is szerepelni szoktak.

Ám a fontosabb dolgok a kérdőív befejezése után kezdődnek csak. Csodálatos módon egy több százezres telefont 1299 forint helyett csak itt, csak most 0 azaz nulla forintért megkaphatjuk, csupán a szállításért kell fizetni - ígérik az oldalon. **"GÉNYELD MOST" - szólít meg a felirat.**



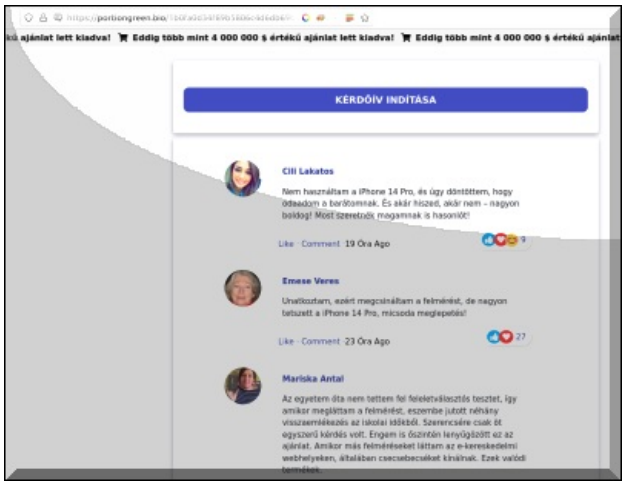


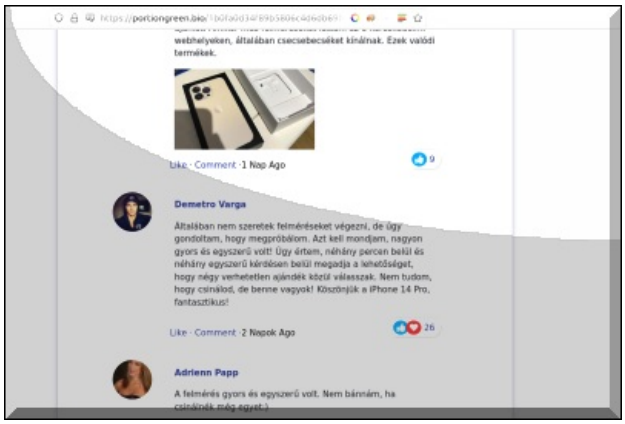


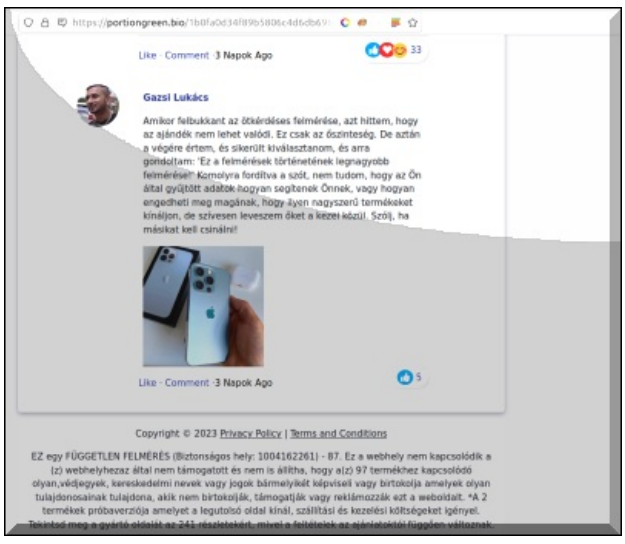


Csupa elégedett nyertes kommentjét lehet itt alább olvasni, akik természetesen mind megkapták az Apple csodatelefonját a kérdőív kitöltése után, és most mindannyian nagyon boldogok, és mi mást is javasolnának nekünk, mint hogy ne habozzunk, vágjunk bele a kitöltögetésbe, ha mi is boldogok akarunk lenni.

Cili Lakatos, Emese Veres, Mariska Antal, Demetro Varga, Adrienn Papp - mind-mind mosolygó boldog nyertes, akik eleinte szintén nem hittek benne, de aztán mégis csoda történt, és köszönik.

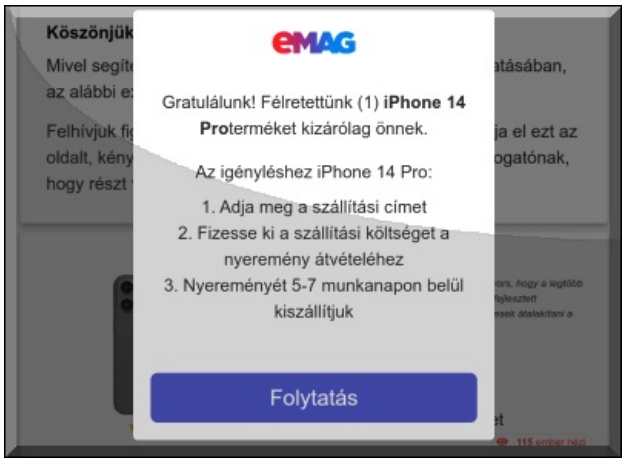






Szóval **a felmérés űrlap után jön az úgynevezett 949 HUF szállítási díj fizetése**, amire nem egy számlaszámot adnak meg, hogy oda utaljon aki bátor, hanem mint egy webshopos vásárlásnál bekérik a személyes és bankkártya adatainkat, háromjegyű biztonsági kóddal együtt.

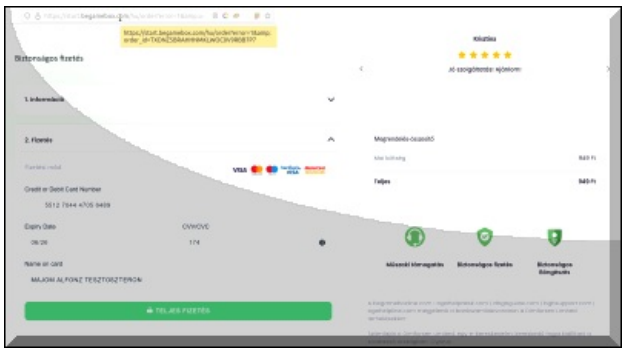
Aki ezt itt megadja, és akinek nincs napi limit, nincs külön banki jóváhagyás rajta, már kockáztatja a pénzét.

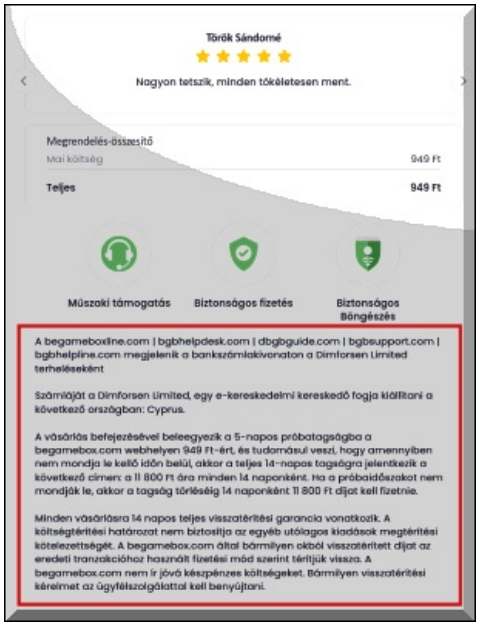




Ami még érdekes, az az apró betűs rész, amit a világhírű "next-next-finish" telepítési módszernél is sokan figyelmen kívül hagynak, pedig ez itt most kifejezetten érdekes dolgokat tartalmaz. Egy ciprusi offshore cég által jegyzett húzós emelt díjas szolgáltatásra fizet elő, aki személyes adatait a nyereményjátéknál megadta:

"*A vásárlás befejezésével beleegyezik a 5-napos próbatagságba a begamebox.com webhelyen 949 Ft-ért, és tudomásul veszi, hogy amennyiben nem mondja le kellő időn belül, akkor a teljes 14-napos tagságra jelentkezik a következő címen: a 11 800 Ft ára minden 14 naponként. Ha a próbaidőszakot nem mondják le, akkor a tagság törléséig 14 naponként 11 800 Ft díjat kell fizetnie.*"



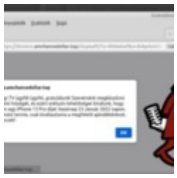


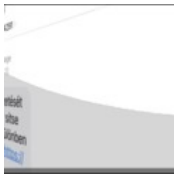
Csodák nincsenek, odafigyelni azonban mindig kell. Az aktuális euró árfolyam alapján az iPhone 14 Pro pedig a mai napon memória felszereltség függvényében 128 GB-tal 385 ezer forint, míg 1TB memória esetén 526 ezer forintba kerül. Láthatóan ingyen sajnos nem adják, hát ez a nagy helyzet.

Megosztom tumblr. Tweet Pin it Tetszik 0

2 komment
Címkék: iphone csalás átverés nyeremény adathalászat

Ajánlott bejegyzések:


Ingyen iPhone csak itt, csak most, csak nekünk


2023. első csalásai


Nő a QR-kódos visszaélések száma


Kár érte, kiváló ügynök volt...



Adathalászat menni booking.com

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Head Honcho 2023.06.16. 13:52:40

Láthatóan arra alapoznak, hogy nagy tömegeknek még mindig gondot okoz megkülönböztetni azt, hogy mikor fizet ő és mikor várható, hogy neki fizessenek. És az egész a digitális írásbeliség komoly hiányosságaira vezethető vissza. Talán nem ártana már az iskolában ilyesmit elkezdeni oktatni, mondjuk a hittan vagy más, múltba forduló, avíttas tudás helyett...

Válasz erre

Elen Paris 2023.06.18. 12:36:50

Üdvözlök mindenkit! Sajnos én is kapom az ilyen üzeneteket (a spam-ba érkezik), méghozzá naponta. Az e-mailben letiltottam ugyan, de utána (már másnap!) nem E-Mag-ként jött hanem MediaMarkt-ként ugyan azzal a szöveggel úgy, hogy a leírásban szerepelt az E-Mag! Egy hét eltelte után újra E-Mag néven jött-jön és azóta is kapom napi szinten ezeket az e-maileket. Ha megnyitom az e-mailt és ott a jobb felső sarokban ráklikkelek a "Továbbiak" menüre abban azt látom, hogy "E-Mag letiltásának feloldása" tehát le van tiltva... DE mégis minden nap bejön egy ilyen e-mail! Nagyon unom már! Valakinek nincs valami ötlete, hogy hogyan tudnám végleg letiltani? Előre is köszönöm a segítséget!!!

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

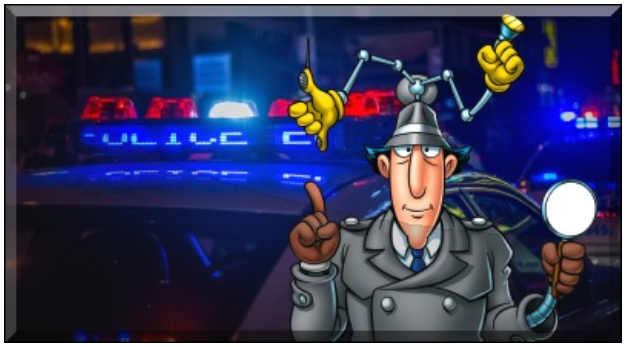
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

1561

Kékfény különkiadás

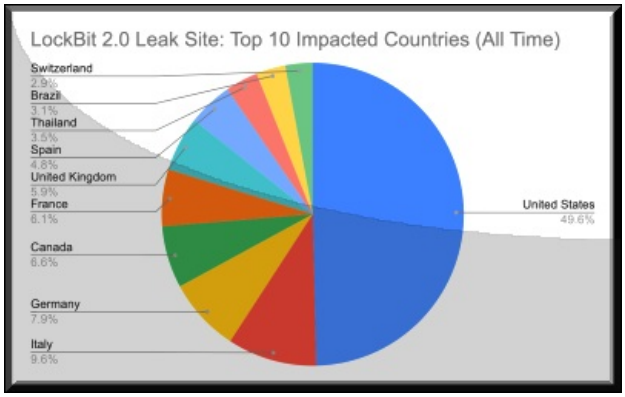
2023. június 20. 17:19 - Csizmazia Darab István [Rambo]

Sajnos kifejezetten ritkán találkozunk olyan hírekkel, ahol ransomware bűnözői csoportok tagjait veszik őrizetbe, vádolják meg, vagy ítélik el. Most viszont ismét itt egy tégla a falban, a Lockbit banda egy újabb tagja akadt fenn a hatóságok hálójában.



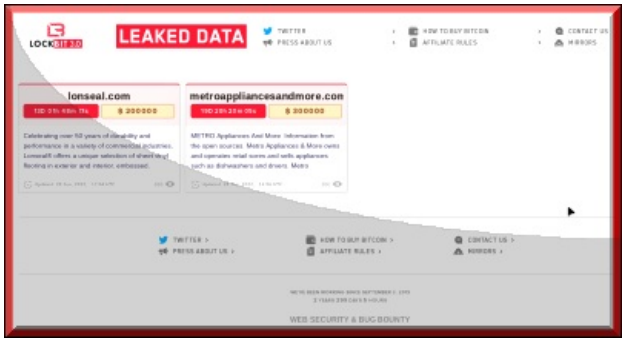
A 20 éves, orosz illetőségű csecsen köztársaságbeli Ruslan Magomedovics Asztamirovnak nem volt jó napja június 15-én, ugyanis az FBI emberei Arizonában letartóztatták. A férfit azzal gyanúsítják, hogy **2020. augusztusától a Lockbit csoport tagjaként részt vett amerikai célpontok elleni zsarolóvírus támadásokban, amelyek során az ő irányítása alá tartozott az áldozatokkal zajló alkudozás és kommunikáció.**

Az őrizetbe vétel során számos számítástechnikai eszközt foglaltak le, többek közt egy Apple iPhone-t, egy iPadet, egy MacBook Pro-t és egy külső USB-tárolóeszközt. **Az ezeken talált adatok megerősítették a gyanút és négy konkrét esetben is találtak bizonyítékot korábbi ransomware incidensekhez kötődően.**



A nyomozók emellett a**z egyik megzsarolt áldozat váltságdíjának egy részét megtalálták egy Asztamirov által birtokolt kriptoszámlán, ez az egyik ilyen ilyen incidensben kifizetett összeg 80%-a volt.** A megszerzett kommunikációból az is kiderült, hogy ennél az esetnél a megtámadott cég rákérdezett nála, hogy mennyire lehetnek biztosak abban, hogyha kifizetik a váltságdíjat, akkor biztosan kapnak visszafejtő kulcsot és az ellopott adataikat is megsemmisítik, hogy azok semmiképp ne kerüljenek ki a publikus netre.

A bűnözők válaszukban azzal érveltek, hogy mivel ők a legrégebbi ransomware csoport, amelynek komoly hírneve is van, és ennek tudatában bízhatnak abban, hogy tartják a szavukat.



Az FBI és a szakértők adatai arra utalnak, hogy a ransomware bandák köré szerveződött és a RaaS azaz Ransomware as a Service szolgáltatást igénybe vevő alvállalkozói kör (affiliate network) tipikusan olyan szerződéseket kötnek a bűnözőkkel, hogy az általuk sikeresen megfertőzött és váltságdíjat fizető ügyfelek pénzének 80%-át megtarthatják,

amennyiben a váltságdíj összege 3 millió USD összeghatár alatt van. **Nagyobb összegek esetében a leányvállalatok 85 százalékot tarthatnak meg a pénzből.**

A RaaS alapon működő bűnözők számos jelentős célpontnak okoztak már kárt, többek közt a Continental autóipari cégnek, a brit Royal Mail is az áldozatok közt volt, de említhetjük az olasz adóhivatalt vagy például Oakland városát is a károsultak közül.



Ha elítélik, **20-25 évnyi elzárás, valamint 250 000 dolláros pénzbírság várható Asztamirov ügyében**, illetve a bűncselekményből származó anyagi veszteség dupláját kell majd kifizetnie, attól függően, hogy melyik a magasabb. Emlékezetes, hogy **a Lockbit csoport ellen pár hónapja már történtek intézkedések, a kanadai-orosz állampolgárságú Mihail Vasziljevet tavaly november 9-én** fogták el Kanadában.

2023. májusában pedig nemzetközi körözést adtak ki a szintén orosz állampolgárságú Mihail Matvejev ellen, akinél az a vád, hogy **kórházakat, iskolákat, nonprofit szervezeteket, az egyik amerikai légitársaságot, és bűnüldöző szerveket, például a washingtoni Fővárosi Rendőrkapitányságot támadtak zsarolóvírussal a LockBit, Babuk és Hive ransomware programok használatával.** A bírósági dokumentumok szerint összességében körülbelül 400 millió dollár váltságdíj kifizetését követelték mintegy **2800 áldozattól, és végül az alkuk után több mint 200 millió dollárt kerestek ezekkel a zsarolásokkal.**

Megosztom tumblr. Tweet Pin it Tetszik 0

1 komment
Címkék: usa orosz fbi letartóztatás bűnbanda őrizetbevétel ransomware zsarolóvírus lockbit

Ajánlott bejegyzések:



8 kórház, 30 klinika, 2.5 millió betegadat


LockBit piacgazdaság és tervgazdálkodás


9 millió, bizony, dalolva ment...


Ki figyeli a figyelőket?


Kézműves flottakezelés

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Mesterséges Geci 2023.06.21. 23:49:31

www.telegraph.co.uk/business/2023/06/19/european-investment-bank-cyber-attack-russian-hackers/
Erről nincs bővebb infótok?
Fura, hogy a magyar lapok közül csak egy nem túl megbízható írta meg.
Ennyire komolytalan vagy annyira be vannak szarva a bankosok, hogy nem merték sem ezt, sem az előzményeket publikálni?

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

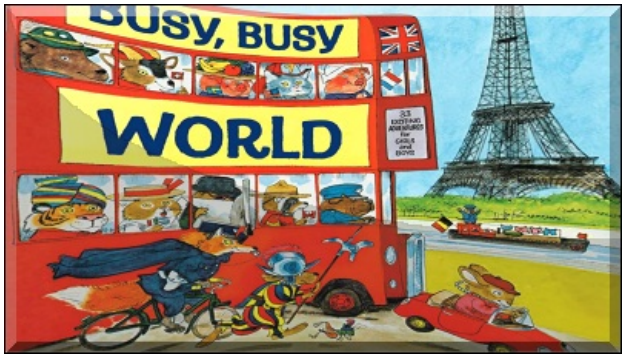
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

349

Az IT biztonság nem nyaral

2023. június 27. 10:09 - Csizmazia Darab István [Rambo]

Itt nyár, ami sokaknak az önfeledt pihenés, utazás ideje is, emiatt **érdemes lehet dióhéjban feleleveníteni azokat a korábbi tippeket, amelyek segíthetnek megőrizni eszközeink biztonságát napon és árnyékban.** És amint az közismert: ismétlés a tudás jó édes anyukája.



Többször és sokféle szemszögből volt már szó ezekről itt a blogon is, de mivel fontos és hasznos tanácsok ezek, **fussunk át röviden ezeken az idei nyáron is.**

Az első lépés nyilván az, hogy **eldöntsük, egyáltalán mennyi és milyen eszközt vigyünk magunkkal**, ami nagyban függ magától az utazás céljától - túrázás, tengerparti nyaralás, városnézés - illetve még attól is, hogy pontosan hova, melyik országba készülünk.



A céges eszközt kizárólag munkahelyi engedéllyel vigyük magunkkal, és vannak bizonyos országok, ahol az erős szigorúság (átnézhetik, elkobozhatják) miatt akár nem is érdemes vinni a saját gépet - pl. Kína, USA, Izrael. Emlékezetes, hogy a katari foci VB esetén kötelező jelleggel egy felügyeli appot kellett a látogatóknak a telefonjukra telepíteni, ehhez szintén **elég, ha egy korábbi nem használt, üres, de még működőképes telefont viszünk az ilyen utakra a sajátunk helyett.**

Hosszabb tartózkodás esetén pedig körülnézhetünk a nemzetközi díjcsomagok között, vagy akár célszerű lehet az adott országban egy helyi SIM kártya beszerzése is.



Ugyancsak az előzetes tervezés része, hogy elgondolkodjunk azon, vajon tudunk-e az eszközeinkre megfelelően vigyázni a szállásunkon, el tudjuk-e zárni ha a strandon vagyunk. **Sok esetben bőven elegendő lehet egy kis méretű tablet is, amin híreket olvasni, játszani, telefonálni is lehet, de filmeket is tudunk rajta nézni.**

Sok szállodában van már okos TV, így **vihetjük kedvenc filmjeinket egy USB kulcson is. Ha saját gépet viszünk, a mentések előzetes elvégzése is legyen része a procedúrának.**



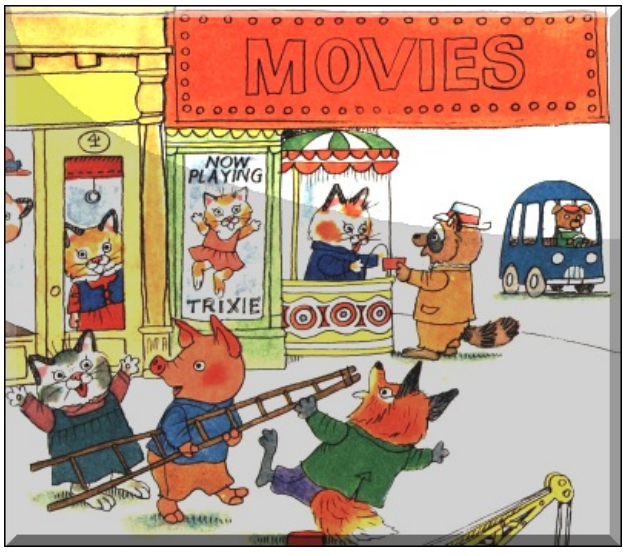
Jöjjenek akkor az előkészületek. **Az aktuális hibajavító frissítések letöltése és futtatása még indulás előtt, ami több szempontból is hasznos ötlet.**

Bezárjuk a még nyitott sebezhetőségeket, **mindezt pedig még az otthoni kellemes széles sáv kényelmében tesszük**, és azt is fontos tudni, hogy számos helyen, szállodákban, panziókban a támadók átverős frissítésekkel próbálkoznak megfertőzni bennünket, ezért érdemes erre figyelni, vagy az ottani netet nem is használni.



A nyitott publikus wifi veszélyeiről már milliószor volt szó, ezeknél egy böngésző kiegészítővel akár egy általános iskolás gyerek is képes ellopni a jelszavainkat. Hasznos ötlet még a VPN használata is, és persze **minden eszközünkön fusson naprakész vírusvédelmi alkalmazás**, legyen titkosítva az eszköz, plusz jelszavas védelemmel is jó, ha el van látva.

Az antivírus megoldásokban többnyire található **lopásvédelmi megoldás is, melynek használatával nyomon követhetjük elveszett eszközeinket, és esetleges lopás esetén távolról is törölhetjük adatainkat.** Persze a megfelelő fizikai védelem is nélkülözhetetlen, soha ne hagyjuk felügyelet nélkül eszközeinket nyilvános helyen, vagy a kocsiban, illetve **használjuk a széf, vagy értékőrző szolgáltatást a strandon, szállodában.**



Ne dőljünk be, ha telefonálnak a bank nevében, hogy éppen most törték fel a számlánkat, és a posztolgatást is érdemes nem azonnal útközben, hanem csak **utólag, a hazaérkezés után intézni.**

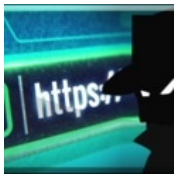
Ettől függetlenül mindenkinek kellemes nyaralást, aki pedig az önkéntes egyszerűség, konkrétabban Pico Iyer: A nyugalom művészete című könyv elveivel összhangban **elutazás helyett otthon nyaral, azoknak is nyugodt pihenést kívánunk.**

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: biztonság utazás nyaralás tippek

Ajánlott bejegyzések:


Okoskodás: okos-e az okosjáték?



Böngészés - kockázatok és mellékhatások


10 alaplépés a biztonsághoz



Új év, régi-új fogadalmak


ChatGPT: hogyan használjuk a munkában?

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

576

DuckDuck Goto Windows

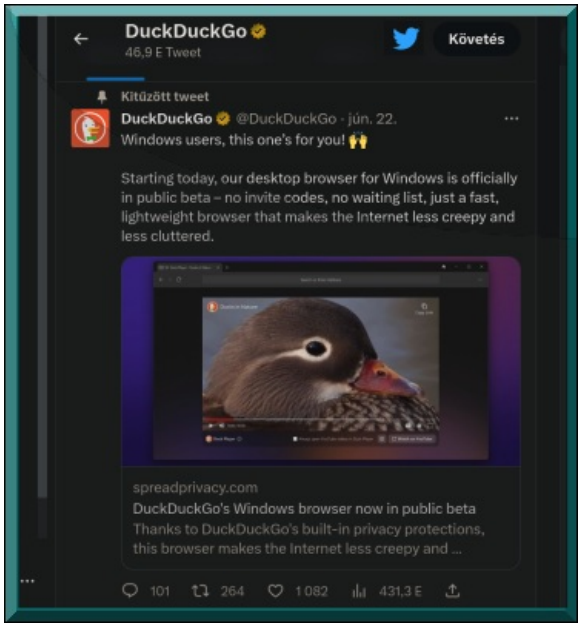
2023. június 29. 10:26 - Csizmazia Darab István [Rambo]

iOS, Android és Mac után immár Windows alá is érkezik a népszerű adatvédelemben utazó böngészőkliens. A biztonságos keresőmotor ígérete szerint nem gyűjti az adatokat, és nem követ bennünket az interneten.



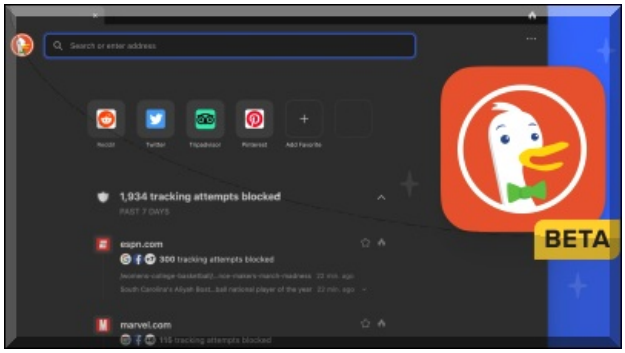
Egyelőre nyilvános béta verzió jelent meg, de a tesztelők kedvező visszajelzései alapján már teljes értékű, Chrome szintű böngészési élményt nyújt a program.

Az anonimitást biztosító szolgáltatások mellett sokaknak az is szimpatikus lehet, hogy az alkalmazás a tolakodó reklámok ellen is sikerrel veszi fel a harcot.



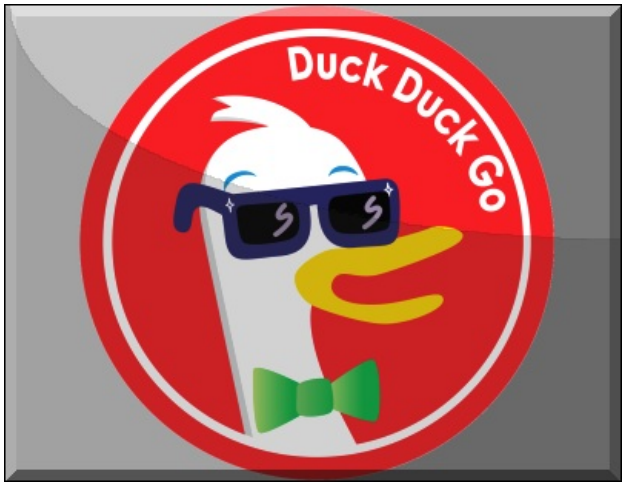
Aki androidos mobilon böngészik, és valamilyen rejtélyes ok folytán nem szerelmes a reklámokba, valószínűleg hamar rákap a DuckDuckGo és/vagy a FreeAdBlocker appokra. Az előbbi főleg az anonimitás miatt focizik, az utóbbi pedig a reklámmentes nézelődés remek eszköze lehet sokaknál.

A kacsakedvelők a korábban csak böngésző kiegészítőként ismert változata után most már Windows alatt is használhatják a natív kliens programot, amely az **Edward Snowden incidens óta komoly népszerűségre tett szert az utóbbi években**.



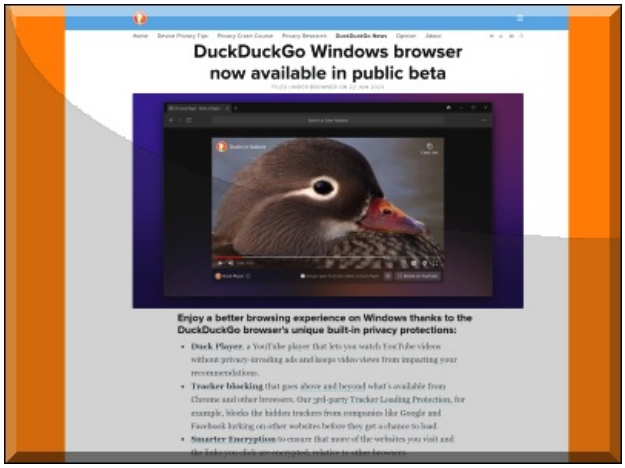
Olyan lehetőségeket kínál, mint **a harmadik fél általi nyomkövetés és a böngésző sütik blokkolása, a felugró cookie engedélyezgetési ablakok lenémítása az automatikusan a legbiztonságosabb választással, az egy kattintásos előzmény törlési mód, biztonságos jelszógeneráló, a felhasználó valódi e-mail címének rejtése egyedi @duck.com címekkel, amikor éppen valamilyen online feliratkozást végzünk.**

De titkosítja a meglátogatott webhelyek és a rákattintott hivatkozások címét is, illetve a DuckPlayer pedig reklámmentes YouTube-videó megtekintést kínál. Ez utóbbi már önmagában is sokaknak lehet igazi áldás.



A Windows 10 és 11 alatt futó DuckDuckGo for Windows program már mindenki számára elérhető, és a fejlesztők szerint ha blokkoljuk a nyomkövetőket, mielőtt azok betöltődnek, az asztali böngésző körülbelül 60%-kal kevesebb adatot használ fel, mint a Chrome.

Aki át akar állni, egyszerűn tudja importálni a könyvjelzőket másik böngészőből. **Remélhetőleg jelszavakat már senki nem akar importálni, mert már van annyira penge és biztonságtudatos, hogy böngészővel soha nem jegyeztet meg ilyeneket, hanem erre a feladatra valamilyen jelszókezelőt használ.**



A program fejlesztői közben folyamatosan várják a felhasználói visszajelzéseket, de az alkalmazás már a jelenlegi állapotában is jól használható.

Ami viszont még egyelőre hiányzik, hogy a jelenlegi béta verzió sajnos nem támogatja a böngésző kiegészítők használatát, erre még várnunk kell.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: windows biztonságos béta adatvédelem reklámok böngészés duckduckgo

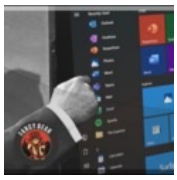
Ajánlott bejegyzések:



[Böngészés - kockázatok és mellékhatások]



[Matatás a robotporszívók agyában]



[Windows update vagy mégsem?]



[Hogyan lehetünk jó digitális szülők?]



[10 alaplépés a biztonsághoz]

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

Újabb súlyos WordPress hiba

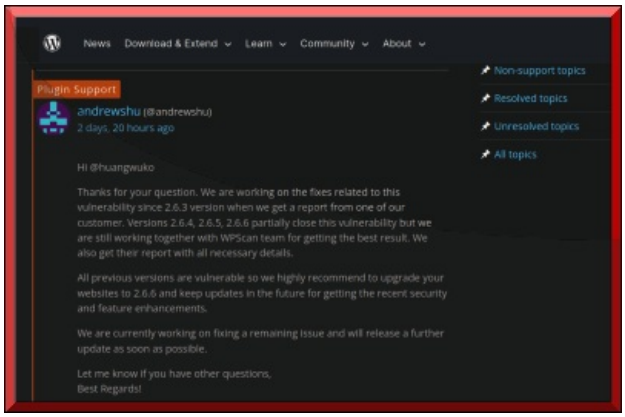
2023. július 03. 16:45 - Csizmazia Darab István [Rambo]

Az Ultimate Member elnevezésű beépülő modul zeroday sebezhetőséget használják ki a támadók a weboldalak feltörésére.



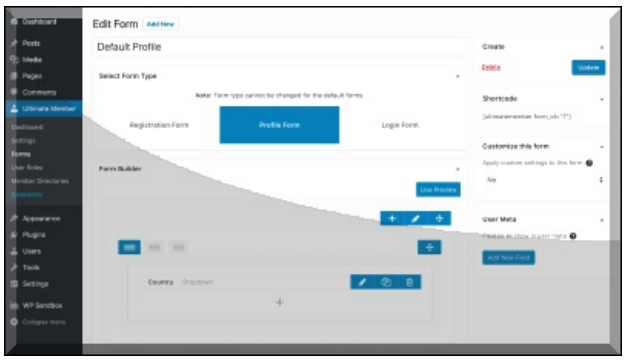
Újabb WP sérülékenység a láthatáron, **a CVE-2023-3460-as hiba besorolása kritikus, és az Ultimate Member beépülő modul összes korábbi változatát érinti**, beleértve a legújabb, 2.6.6-os verziót is.

A regisztrációt megkönnyítő modul jelenleg **több mint 200 000 aktív telepítéssel rendelkezik, de ami ennél is szomorúbb, hogy a már korábban ismert hibát sikertelenül próbálták meg kijavítani a 2.6.3, 2.6.4, 2.6.5 és 2.6.6 verziókban.**



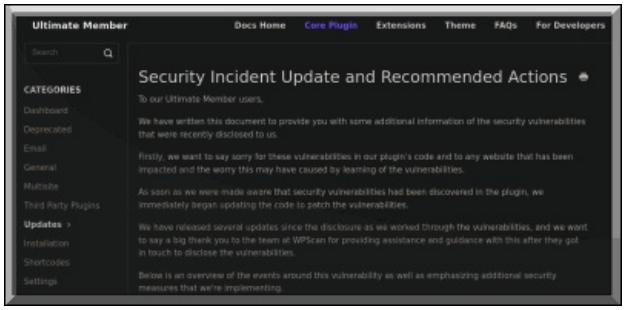
A sérülékenységet kihasználva nem hitelesített távoli támadók képesek rendszergazdai szintű WordPress felhasználókat létrehozni.

A hibás regisztrációs űrlap teljes hozzáférést biztosít a támadónak a sebezhető webhelyhez.



A WordPresses oldalak sebezhetőségeinek kihasználása sajnos tipikus incidens, amikor kapjunk a hamis csomagértesítőket a postától, csomagküldő szolgálatok nevével visszaélve, vagy bankok nevében, akkor gyakran ilyen feltört weboldalakról terjesztik ezeket a kártevős kampányokat a bűnözők.

A beépülő modul deaktiválása elvileg elegendő a biztonsági rés kihasználásának megakadályozásához, érdemes lehet óvatosságból teljesen eltávolítani a bővítményt. **Szerencsére időközben július 1-én megjelent a 2.6.7 javított változat, ami remélhetőleg már végleg megoldhatja a problémát.**



A WordPress sebezhetőségek frontja úgy általában évek óta súlyos, ha a statisztikákat nézzük, ezekben brutális adatokat láthatunk. Egy friss adatsor szerint naponta átlagosan 30 ezer webhelyet törnek fel , és 39 másodpercenként történik egy feltörés - nyilván ebben a zerodayek mellett van egy csomó eleve frissítetlen oldal is. **Csak a 2021-es évben 22 milliárd ilyen feltörést regisztráltak, a sikeres incidensek 95%-a pedig rendre emberi mulasztásból fakadt.**

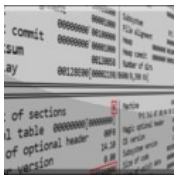
Ha CMS-t futtatunk, akkor kiemelten érdemes figyelmet fordítani arra, hogy biztonságos erős bejelentkezési hitelesítő adatokat használjunk 2FA/MFA támogatással, használjunk biztonsági tanúsítványt (HTTPS), legyen VPN kapcsolatunk (virtuális magánhálózat), **és az operációs rendszer naprakészsége mellett fordítsunk gondot a CMS szoftverünk és annak bővítményeinek a frissítéseire is.**

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: ultimate frissítés weboldal javítás wordpress kritikus feltörés sebezhetőség member

Ajánlott bejegyzések:


OTP kártyáját ideiglenesen megterheltük


Lenovo laptopok a pácban


Tíz tiszta víz, ha nem tiszta, vidd vissza


Okosotthon kontra felhasználó


Futószalagon érkeznek a hacktivista támadások

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

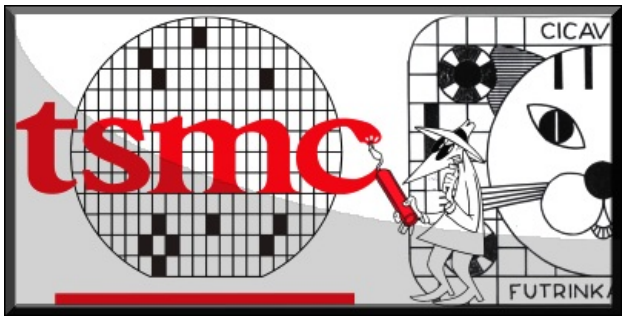
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

1758

Baj van Tajvanban

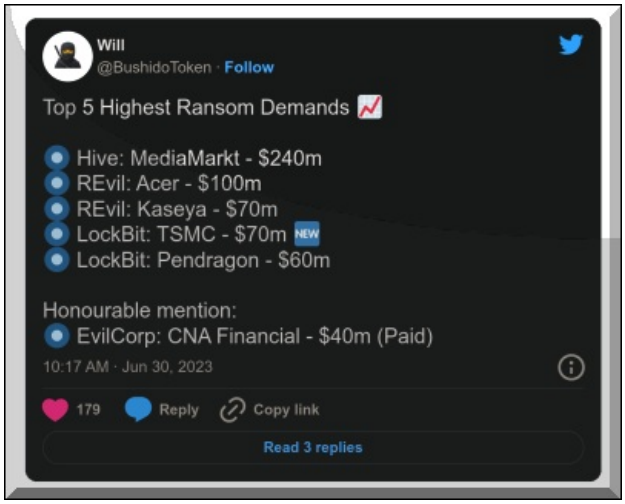
2023. július 05. 12:38 - Csizmazia Darab István [Rambo]

A Taiwan Semiconductor Manufacturing Company Limited (TSMC), a világ legértékesebb félvezetőgyártó vállalata zsarolóvírus támadással néz szembe. A vállalat olyan jelentős cégek beszállító partnere, mint például az AMD , az Apple, az ARM, a Broadcom, a Qualcomm vagy az Nvidia.



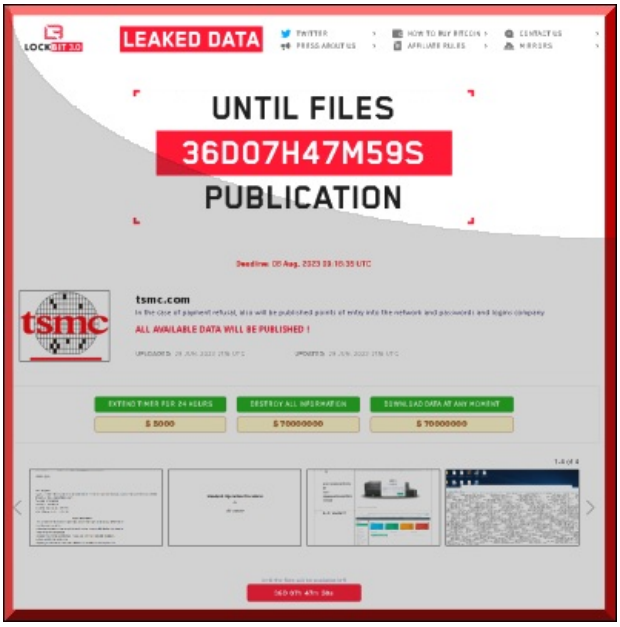
Az **oroszországi székhelyű LockBit zsarolóvírus-banda azt állítja, hogy sikeresen ellopott a TSMC-hez tartozó adatokat,** ám a hardvergyártó ezt tagadta, szerintük a támadóknak nem őket magukat, hanem "csak" egy harmadik felet, a korábban meg nem nevezett, de később beazonosított Kinmax nevű beszállítójukat sikerült feltörniük.

A bűnözők ezúttal 70 millió dolláros váltságdíjat követelnek, nem fizetés esetén pedig a LockBit Leak Site weboldal alapján azzal fenyegetnek, hogy kiszivárogtatják az internetre a bizalmas adatokat, köztük a TSMC informatikai hálózatának hálózati bejelentkezési adatait. **A 70m USD összeg igen jelentős, simán bekerülhet az eddig követelt legmagasabb váltságdíjak toplistájába negyedikként.**



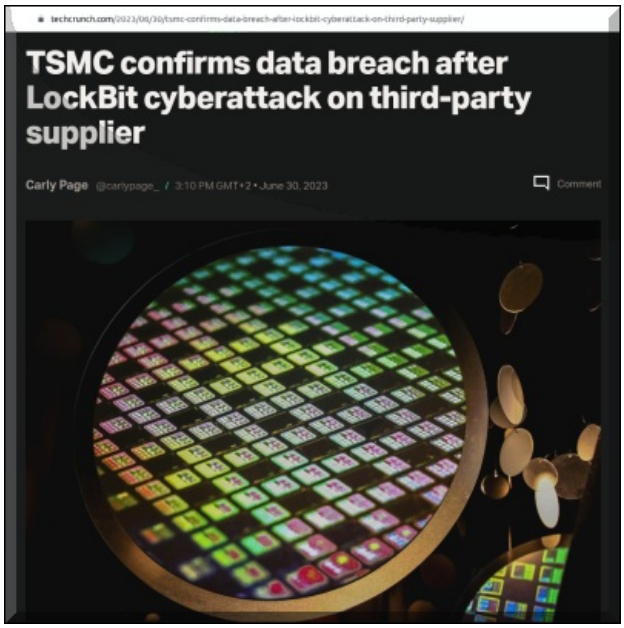
A LockBit alá tartozó National Hazard Agency nevű RaaS csoport látszólag hiteles képernyőképeket is megosztott az ellopott fájlok könyvtárlistájáról, különféle tervrajzokról és végső fizetési határidőnek az augusztus 6-át jelölték meg. A gyártó hivatalos szóvivője által hangoztatott mondás, miszerint "mindez nem érintette a TSMC üzleti tevékenységét, és nem veszélyeztette a TSMC ügyfél információit sem" - legalábbis ennek fényében kissé kétségesnek tűnhet.

A Kinmax szerint az adatszivárgást okozó incidens csak a belső tesztelési környezetüket érintette, elnézést kértek az ügyfeleiktől, ám arról nem közöltek információt, hogy mindez hány partnerüket érinthette. A Kinmax ügyfelei között szintén neves cégeket találunk, mint például a Cisco, a NetApp, a HPE, a Microsoft, a Red Hat, a VMware, az NVIDIA, vagy a Fortinet.



Sem Eric Huang, a Kinmax Technology alelnöke, sem pedig a TSMC szóvivője **nem válaszolt a The Registernek arra a kérdésére, hogy kifizetik-e a 70 millió dolláros követelést.**

A LockBit egyébként az egyik legkártékonyabb zsarolóvírus banda, a hozzájuk tartozó bűnözői "leányvállalati" csoportok hatalmas károkat okoztak az Egyesült Államokban, 2020. óta elkövetett 1700 támadás legkevesebb 91 millió dollárba került az áldozataiknak.



Az eset mindenesetre arra is jó példa, hogy **nagyon gyakran a gyengébben védett alvállalkozói kört támadva igyekeznek a nagyobb célpontok felé eljutni az elkövetők.**

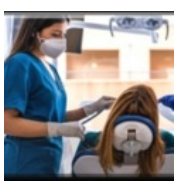
Hogy igaz-e az adatlopás, mit érintett egész pontosan, történik-e majd váltságdíj fizetés - nos erre vélhetően még pár hetet várni kell.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: tajvan ipar adatlopás adatszivárgás ransomware tsmc zsarolóvírus doxing kinmax

Ajánlott bejegyzések:

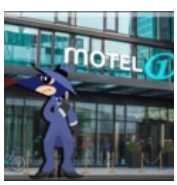

Ransomware támadás a Nissan ellen


9 millió, bizony, dalolva ment...



Ransomware támadás érte az MSI-t


Fordulat ransomware fronton



Ransomware a One Motelben

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

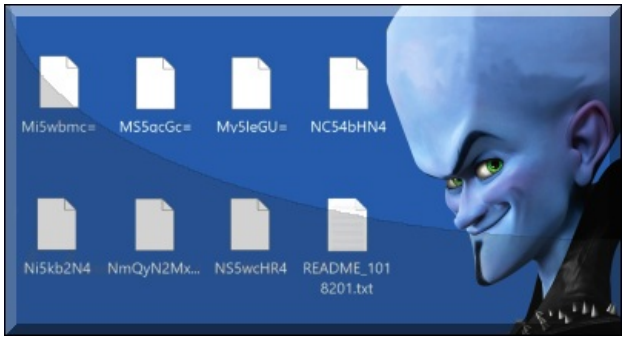
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

5109

Windows frissítés vagy mégsem?

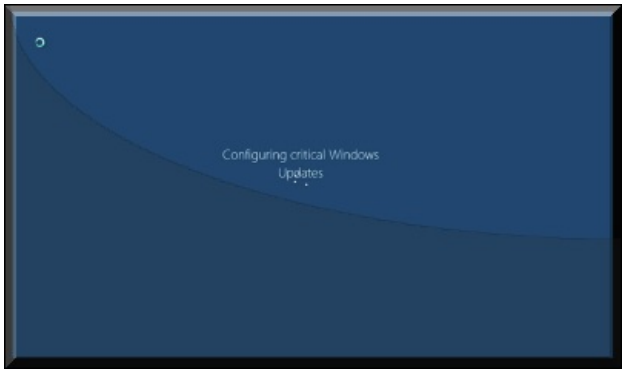
2023. július 10. 10:21 - Csizmazia Darab István [Rambo]

A szokványos kérdésre a szokványos válasz százból százszor a nem szokott lenni, és ez most sincsen másképp. Ebben az esetben a **Windows rendszer hibajavító frissülése helyett egy nagyfejűnek nevezett idén tavasszal megjelent új zsarolóvírus próbálkozik alaposan kiütni** a rendszerünket.



Biztonsági kutatók szerint **hamis Windows frissítés és Microsoft Word telepítőként is felbukkanhat az a Big Head elnevezésű ransomware**, amely egy .NET alapú program. A zsarolóvírus eltitkosítja a fájlokat, és üzenete szerint **1 BTC váltságdíj ellenében kerülhető el mind a fájlok végleges elvesztése, mind pedig bizalmas adataink nyilvánosságra kerülése, vagyis a doxing.**

Az elemzések arra utalnak, hogy a **különféle változatok egyetlen elkövetőtől származhatnak, aki látszólag még kísérletezget a terjesztéssel, de látva frissítési képernyőképet egyértelműen a hétköznapi átlagfelhasználókat vette ezzel célba, és nem a vállalatokat.** Mivel egy Bitcoin mai áron hozzávetőleg 10 és fél millió forintnyi összeg, emiatt a magánszemélyek közül valószínűleg csak kevesen akarnak és tudnak majd erre ennyit invesztálni.



A kártevő technikailag igyekszik alapos munkát végezni, hozza a kötelezőt: automatikus indítását bedrótozza a Rendszerleíró adatbázisba (Registry), törli a megtámadott gépről a helyreállításhoz használható árnyékmásolatokat (Shadow Copy), emellett azt is vizsgálja, virtuális gépen fut-e vagyis tesztkörnyezetnek látszik-e a rendszer vagy igazi munkavégző gépnek.

Ami a ransomware eredetéről még bővebb információt fedhet fel számunkra, az pedig az a tény, hogy **megkeresi a rendszer nyelvi beállítását is, és ha az a volt szovjet államok (FÁK, Független Államok Közössége) közé tartozik, abban az esetben nem történik meg a fertőzés. Ilyet pedig korábban már több orosz eredetű kártevőnél is láthattunk, például ilyen volt a Cerber (Kerberosz) is.**



Egyes változatok a fenti adatlopás és elkódolás mellett érzékeny információkat is gyűjtenek, többek közt a böngészési előzmények, a könyvtáraink listája, a telepített illesztőprogramok, a futó folyamatok listája, az operációs rendszer termékkulcsa illetve a használt aktív hálózatok adatai is kikémlelésre kerülhetnek, valamint a kártevő képes menet közben képernyőképeket (screenshot) is készíteni és elküldeni.

Ezek a funkciók, illetve az eddigi variánsok közti eltérések is arra utalnak, hogy kísérleti fázisban van a rosszindulatú program, melynek készítői **igyekeznek minél több tapasztalatot szerezni és erre építve még hatékonyabb módon kárt okozni.**



Szórványos fertőzéseket eddig elsősorban Németországban, az Egyesült Államokban, Olaszország, Franciaországban, Belgiumban, Spanyolországban, Svédország és Törökországban észleltek, **széles körű elterjedés egyelőre még nem jelentkezett.**

A vírusvédelmi programok többsége képes detektálni és blokkolni a kártevőt.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: orosz kísérlet oroszország head eredet big váltságdíj vagymégsem ransomware zsarolóvírus doxing

Ajánlott bejegyzések:

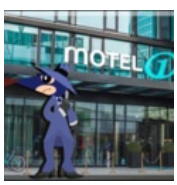


8 kórház, 30 klinika, 2.5 millió betegadat

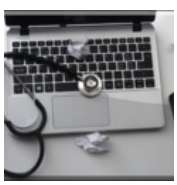

Ransomware támadás a Nissan ellen



LockBit piacgazdaság és tervgazdálkodás



Ransomware a One Motelben


Ransomware - Fülöp-szigetek, 1:0

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

731

NATO csúcstalálkozós adathalászat

2023. július 12. 18:17 - Csizmazia Darab István [Rambo]

Minden alkalom jó alkalom a csalásra, megtévesztésre, így **a mostani vilniusi nemzetközi esemény is megkapta a maga próbálkozásait a kiberbűnözőktől.**



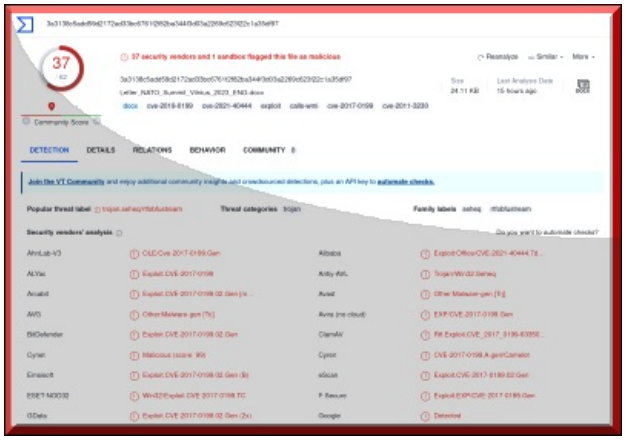
Már napokkal korábban elkezdődtek a támadások, ezek között volt például egy olyan, amelyben érdekes módon magyarországi IP címekről osztottak meg adathalász e-maileket. Ezek melléklete rosszindulatú Word dokumentumot tartalmazott.

Az eredeti ukrainianworldcongress PONT org domén helyett ukrainianworldcongress PONT info hasonmás weboldalra mutatott, ami kinézetre teljesen hasonlított az eredeti oldalra, de a hamis webhely megfertőzte a látogatókat. A sebezhető mellékletet tartalmazó e-mailt a vírusirtók többsége sikeresen felismerte és blokkolta, a kártékony weboldalt pedig azóta időközben már letiltották.



Ha valaki védelem nélkül óvatlanul megnyitotta a kéretlen levél csatolmányban szereplő, egy 2022-es sebezhetőséget tartalmazó dokumentumot, az több rosszindulatú összetevő letöltése után egy kémkedésre alkalmas **hátsó ajtót telepített a fertőzött számítógépre.**

Ezeket a támadásokat egy gyaníthatóan **kubai-orosz hátterű RomCom néven ismert kiberbűnözői csoportnak tulajdonítják, a csapat neve valószínűleg ismerős lehet korábbi kiberincidensekből: például a SolarWinds és a KeePass elleni eset köthető hozzájuk.**



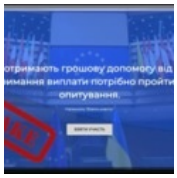
A RomCom csoport már 2022-ben is részt vett különféle Ukrajna elleni kibertámadásokban, de folyamatosan új technikákkal igyekszik megtéveszteni a felhasználókat, így **például terjesztettek már hamis GIMP grafikai szoftvert és olyan kártékony programot is, amely a ChatGPT alkalmazás nevével élt vissza.**

Oroszország ukrajnai inváziója óta jelentősen megugrott a NATO-országok elleni kibertámadások száma, például az APT29, Winter Vivern és más hasonló csapatok különféle NATO és az EU-tagállamok diplomáciai és külügyminisztériumi szervezeteket támadtak.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: ukrajna nato backdoor kémprogram adathalászat csúcstalálkozó hátsóajtó vilnius

Ajánlott bejegyzések:



Adathalászok lakat alatt



Evolúció, ami számunkra nem csodálatos



Nő a QR-kódos visszaélések száma



Kár érte, kiváló ügynök volt...



Identitás lopás: nem függ az életkortól

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

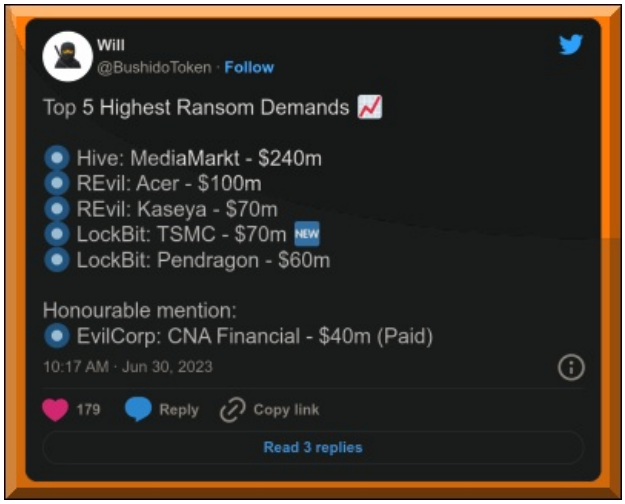
Kincs, ami van

2023. július 17. 10:32 - Csizmazia Darab István [Rambo]

Még drágább az életed - mondhatná Bruce Willis John McClane szerepében, és ez nincs másképp 2023-ban sem. **Drágulás van, a zsarolóvírus üzletág bevételei pedig sajnos ismét rekordot döntenek.** Így csak a megelőzés adhat erőt és mindent lebíró akaratot!

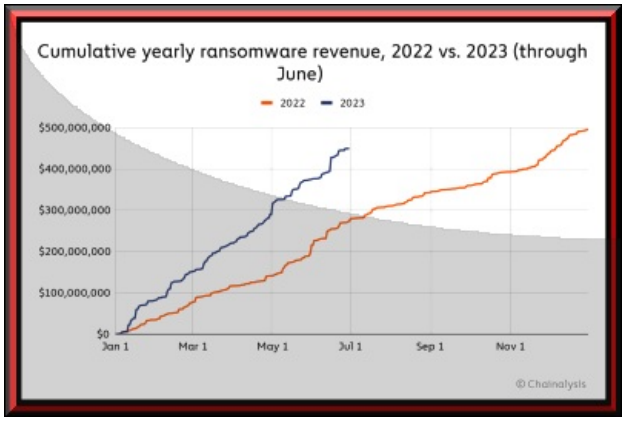


Egy egészen friss közreadott jelentés szerint **a ransomware business 898 millió dollárt (kis híján 300 ezer milliárd forintnyi) bevételt termelt a bűnözőknek, ami azt mutatja, hogy az idei esztendő első felében minden egyes nap 3 millió dollárt (durván napi 1 milliárd forintnak megfelelő összeget) kerestek ezzel a támadók.**



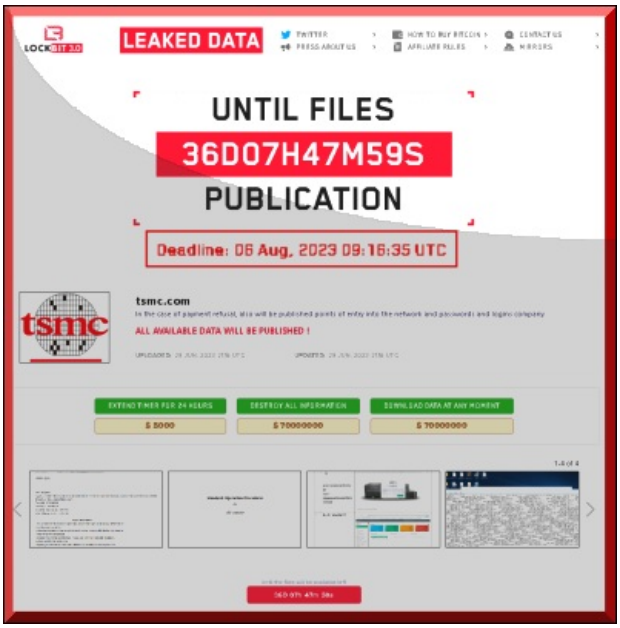
A 2022-es viszonylagos visszaesés után ismét emelkedés látszik a váltságdíj kifizetések mértékében, így a 2023-as év első félévének zsarolóprogram miatti utalások **elérték a 449 millió dollárt, ami már a 2021-es mértéket ostromolja, és ezzel a valaha volt második legmagasabb szintet árazta be.**

Vagyis visszatért minden a korábbi kerékvágásba, így érdemes lehet megnézni, mik lehetnek ennek a nagy comeback jelenségnek az okai.



Az biztos, hogy a RaaS, azaz a Ransomware as a Service modell (beleértve ebbe minden affiliate network törekvést is) sajnos egyre sikeresebb a bűnözők körében.

Mindeközben a tavalyi esztendő időlegesen ugyan csökkenést mutatott a fizetett váltságdíjak területe, ami **csak részben magyarázható a nagyobb szervezetek kiberbiztonsági és adatmentési gyakorlatának javulásával**, emellett valamilyen szinten a bűnüldözési erőfeszítésekkel, és ha kis részben is, de plusz a Nomoreransom kezdeményezés kapcsán elérhető visszafejtő eszközök gyarapodásával. **Ez utóbbiak adhattak némi reményt az áldozatoknak, hogy fizetés nélkül átvészeljék a ransomware támadásokat.**



Ami viszont megint csak **a súlyosbodás irányába mutat, az egyfelől a bizonyíthatóan valós (tehát nem csak bekamuzva) megtörtént doxing incidensek** - ahol a titkosítás mellett bizalmas adatlopás is történik, így sokan a publikálás elkerülése miatt fizetnek), valamint hogy **a követelt váltságdíjak mértéke is egyre emelkedő tendenciát mutat.**

További nehezítő tényező, hogy **egyre több a jól előkészített célzott támadás, ahol ráadásul napi szinten zaklatják is a váltságdíj fizetés miatt a cégek alkalmazottait, valamint a támadások számának meredek emelkedése is jelentősen nehezíti a vállalatok helyzetét.**



Ha csak itt a blogon megjelent idei nagyobb volumenű eseteket nézzük, volt a tajvani TSMC félvezetőgyártó vállalat elleni LockBit támadás, **melynél a bűnözők 70 millió dolláros váltságdíjat követelnek**, itt majd az augusztus 6-i határidő lejárta után láthatunk majd tisztábban.



Szintén idén szerepelt a főcímekben az ugyancsak a LockBit banda kapcsán az USA-beli Managed Care of North America (MCNA) **Dental fogászati biztosítási óriáscég, ahol 10 millió dolláros volt a kért váltságdíj mértéke és 700 GB az ellopott** érzékeny adatmennyiség. De említhetjük akár a márciusi Ferrari ellen elkövetett bűncselekményt is, ahol **az olaszországi székhelyű luxusautó gyártó valójában észre sem vette, hogy feltörték őket, csak a támadók megkeresése után észlelték egyáltalán magát az incidenst.**

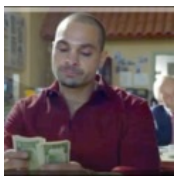
Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: statisztika business rekord bevétel emelkedés összeg váltságdíj ransomware raas

Ajánlott bejegyzések:



Gyorsabban, magasabbra, erősebben!


Csökkent a zsarolóprogramból származó bevétel


Emelkedő ransomware károk


Durva ransomware statisztikai adatok


Ransomware a spájzban

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

984

Hiába futsz, hiába bújsz, félelemmel nem sokra jutsz

2023. július 20. 14:36 - Csizmazia Darab István [Rambo]

Akár ez is lehetne a mottója egy olyan letartóztatásnak, ami **egy évtizednél is régebbi számítógépes bűncselekmény gyanúsítottját fülelte kissé megkésve.**



Scareware - sokaknak ez már vagy még nem is mond semmit, hiszen hétköznapjainkat jobbára már jó tíz éve a zsarolóvírusok és a kémprogramok elleni védekezés-megelőzés jegyében éljük.

Ám érdemes feleleveníteni, hogy a 2013-as évet megelőzően **korábban milyen primitív trükkökkel próbálkoztak a kiberbűnözők, és sokszor bizony így is sikerrel jártak.**



Hamis antivírus program, kamu felugró ablak, nem létező fertőzésre figyelmeztető üzenet - ez jellemezte ezt a fajta csalást, amiről a Magyarországon világhírű ;-) A Vírusok Varázslatos Világa cikksorozat 15-ik egy teljes epizód erejéig kitért. **Windows Antivírus, XP Antivirus és mindenfajta légből kapott nevekkel megjelent átverések ijesztgették a felhasználókat, akiket aztán pénz átutalásra igyekeztek rávenni az állítólagos irtani is képes úgynevezett "teljes verzióra" történő áttérés ürügyén.**

Az egész azonban kamu fertőzéssel riogató nagy pénzrablás volt, akik fizettek, azok a semmiért fizettek. **Később sajnos az is gyakori lett, hogy kamu terméknevek helyett meglévő antivírus programok nevében érkeztek az ilyen fenyegetések, pénzkövetelések.**



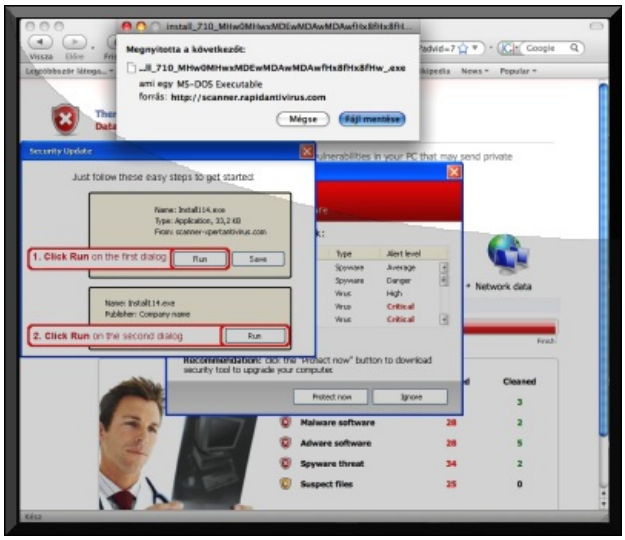
Később aztán jöttek a lemezoptimalizáló és egyéb segédprogramok, amelyek szintén valamilyen rendellenességre, hibára hivatkozva javasolták a teljes értékű, fizetős kamuprogramot. Amikor pedig már ez sem hozott elég pénzt a konyhára, jöttek a hamis szerzői jogi felszólítások, az állítólagos pedofil tartalmak miatti fenyegetések, amelyek ezen a vonalon haladva, és a feljelentés elkerülése érdekében egy fix pénzösszeget követeltek.

Sokszor nem is léteztek ezek a feltüntetett szervezetek, néha viszont éppen meglévő, legitim hatóságok nevével éltek vissza a csalók abban bízva, hogy az ijedtség miatt sokan inkább fizetnek egy "észszerű" összeget, mint hogy megszégyenüljenek, vagy évekig tartó pereskedést, esetleg börtönbüntetést kockáztassanak.



Ami miatt most minderről beszélünk, az pedig az, hogy a spanyol hatóságok az FBI közreműködésével letartóztattak egy olyan ukrán állampolgárt - a nevét egyelőre nem hozták nyilvánosságra - , aki ellen az a vád, hogy éppen ilyen scareware támadásokban közreműködött aktívan. A barcelonai reptéren őrizetbe vett férfi az Interpol körözési listáján is szerepel, és tíz éve már szökésben volt az Egyesült Államok hatóságai elől. Azzal vádolják, hogy 2006 és 2012 között tömeges méretű scareware csalásokat intézett a felhasználók ellen egy nemzetközi bűnbanda tagjaként, és váltságdíjként 129 dollárt kértek a nem is létező kártevők eltávolításáért.

Az ilyen kártevők néha vicces szituációkat is generáltak, például OS X-en vagy Linuxon futtatva is azt állították, hogy Windows alkönyvtár .DLL állományai vírusfertőzöttek :-)



A több százezer (900 ezer) gyanútlan áldozattól 72 millió dollárnyi pénzt csaltak ki, a cikk szerint **a három leggyakoribb fenyegetést a System Fix , a Cloud AV 2012 és a Win 7 Security 2012 program-változatok jelentették,** ahol a feltüntetett évszámok már rendre az előző évben megjelentek, tehát egy akármi-2009 nevű kamuprogram már az előző, a példa alapján 2008-ben is aktívan terjedt, mint egy igazi friss program.

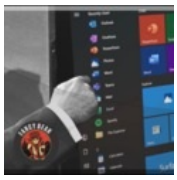
A modell sokáig jövedelmező volt, és jóval kevesebb erőfeszítést, szakmai befektetést igényelt, mint a most ismert ransomware ágazat, ám egy idő után a felhasználók már megtanulták, hogy felesleges fizetni, így aztán a kártevő evolúció a valóban óriási károkat okozó zsarolóvírusok irányába haladt tovább.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: spanyolország fbi hamis letartóztatás antivirus scareware őrizetbevétel

Ajánlott bejegyzések:


Kékfény különkiadás


Windows update vagy mégsem?


Új földgáz számlája készült - vagy mégsem?


Ki figyeli a figyelőket?


Emelkedő ransomware károk

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

1034

Hiba a 8-ik rétegben

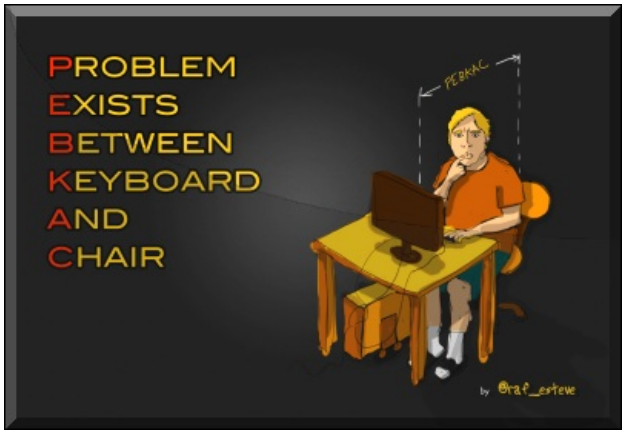
2023. július 25. 10:43 - Csizmazia Darab István [Rambo]

A humán interfész szerepe a biztonságban megkerülhetetlen, ahogy ezt a social engineering kapcsán a nemrég elhunyt Kevin Mitnick is találóan megfogalmazta: "*Egy vállalat több százezer dollárt költhet tűzfalakra, behatolásjelző rendszerekre, titkosítási és egyéb biztonsági technológiákra, de ha a támadó fel tud hívni valakit a vállalaton belül, aki bediktálja neki a jelszavát, akkor a technológiára költött pénz lényegében elpazarolt.*"



Emiatt fontos a megelőzés-védekezés tengelyen a rendszeres biztonságtudatossági képzés és annak tesztelése. A véletlen, vétlen hibázás, a PEBKAC jelenségek olyan rétege, amely már komoly károkat okozva egy cégnek, vagy vállalkozásnak.

Az ilyen emberi hiba vagy mulasztás már a múltban is sokféle problémához vezetett, gondoljunk csak a nem megfelelő biztonsági beállításokra, például indokolatlanul **nyitva hagyott RDP port miatti ransomware támadásra, OpenRelay okozta spammelésre, jelszólista clear textben való szerveren felejtése, ellopott, elvesztett titkosítás nélküli eszközök illetéktelen kezekbe kerülése, vagy érzékeny adatokat tartalmazó leselejtezett adathordozók felelőtlen értékesítése is mind-mind végzetes következményekkel járhat.**



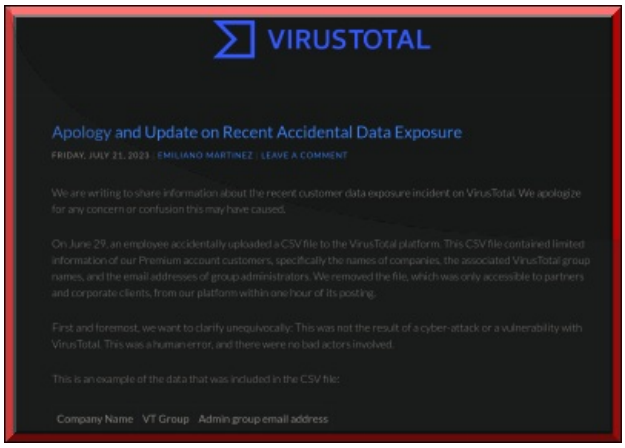
Mai témánk ugyan nem közvetlenül ez, de szorosan kötődik a felhasználók óvatlan, meggondolatlan viselkedéséhez. A sokak által ismert kártékony linkek, webhelyek és állományok ellenőrzésére szakosodott weboldal, **a 70 különböző vírusirtó motort futtató Google tulajdonban lévő VirusTotal ugyanis most kénytelen volt elnézést kérni, miután egyik munkatársuk egy 5600 felhasználót tartalmazó érzékeny adatállományt töltött fel véletlenül vizsgálatra.**

A .CSV, azaz Comma Separeted Value, magyarul vesszővel elválasztott olvasható szövegalapú fájl feltöltése több ezer prémium ügyfél adatait fedte fel, **köztük a US Cyber Command, az FBI és az NSA alkalmazottainak neveit, cégek-szervezetek nevét és e-mail címeket.**



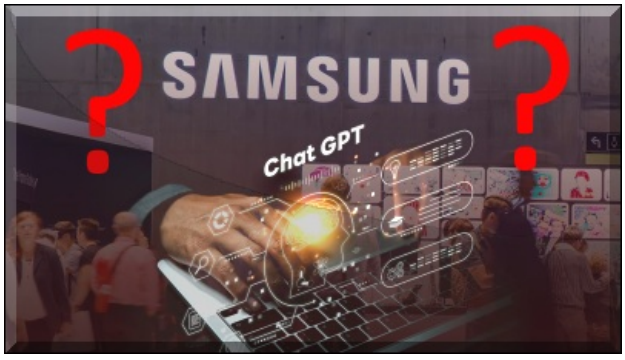
A feltöltött állományok a hétköznapi látogatók számára nem, de az előfizetéses partnerek, és vállalati ügyfelek számára emiatt egy ideig elérhetővé vált. A kínos tévedést egy órán belül észlelték, és ezután a kritikus fájlt eltávolították, de a dolog persze ennek ellenére elég kellemetlen közjáték volt.

A híres mondás, miszerint az internet nem felejt, sajnos itt is beigazolódott, és **pár napon belül címlapos sztori kerekedett az adatállomány miatt.** Ami elromolhat az el is romlik Murphy törvényt adaptálva itt az lehet a mondás, hogy ami kiszivároghat, az előbb-utóbb ki is szivárog.



A Spiegel Magazin cikke arról számolt be, hogy a mindössze 313 kilobyte méretű listában szereplő partnerek számára az incidens roppant kellemetlen. **Szerepelnek rajta többek közt a német, holland, brit és tajvani biztonsági ügynökségek, a német szövetségi rendőrség, a katonai kémelhárító szolgálat, valamint például olyan nagy német vállalatok, mint a BMW, a Mercedes-Benz és a Deutsche Telekom.**

Nyilván fennáll annak a veszélye, hogy kiszivárgás esetén ezekre a címekre a jövőben testre szabott adathalász és egyéb célzott támadások indulhatnak. A VT közleményében bocsánatot kérnek és azt állítják, hogy az incidens óta új belső folyamatokat és műszaki ellenőrzéseket vezettek be az ügyféladatok biztonságának és védelmének javítása érdekében.



És hogy a közelmúltból még említsünk hasonló kényelmetlen történéseket, nem is kell nagyot visszamenni az időben, hogy az 5 hónap alatt 100 millió felhasználót bezsákoló ChatGPT platformon is történjen incidens.

Az egyik ilyen az volt, amikor 2023. májusában kiderült, hogy a Samsung cég munkatársai a ChatGPT segítségével bizalmas anyagokat itt készítettek, javítgattak, tesztelgettek, és a feltöltések miatt kiszivárogtak belsős értekezleti anyagok és új forráskódok.



De ugyanitt említhetjük **azt a tipikus vállalati félelmet is, hogy valaki véletlenül rossz címzettnek ír vagy továbbít valamilyen bizalmas anyagot. Erre is van viszonylag friss és szomorú példa 2021-ből, amikor is a kanadai bevándorlási hivatal (IRCC) tálibok elől menedéket kereső afgán emberjogi aktivisták és menekültek adatait küldtek ki BCC mező helyett mindenki által látható címzett mezőkkel.**

Az eset sajnos tragikus végkifejlettel zárult, mert az üzenetekben szereplő, fényképpel is kiegészített többszázas lista alapján a tálibok felkutatták ezeket az embereket és akiket sikerült megtalálniuk, azokat a külföldiekkel való kapcsolattartás miatt megtorlásképpen elrabolták, meggyilkolták. **Egy ilyen esetnél aztán már végképp nem ér semmit az utólagos bocsánatkérés.**

Megosztom tumblr. Tweet Pin it Tetszik 0

1 komment
Címkék: hiba samsung user error emberi virustotal mulasztás mistake pebkac chatgpt ircc

Ajánlott bejegyzések:


Szolgálunk és nem védünk


10 gyakori IT biztonsági hiba


ChatGPT: hogyan használjuk a munkában?


OTP kártyáját ideiglenesen megterheltük


Na de mit adott nekünk a ChatGPT?

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Head Honcho 2023.07.25. 22:45:50

Érdekes. Mégis miképpen látható 3rd party fél felé bármilyen keresés? Még akkor is, ha az nem átlag egyorrú felhasználó...

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

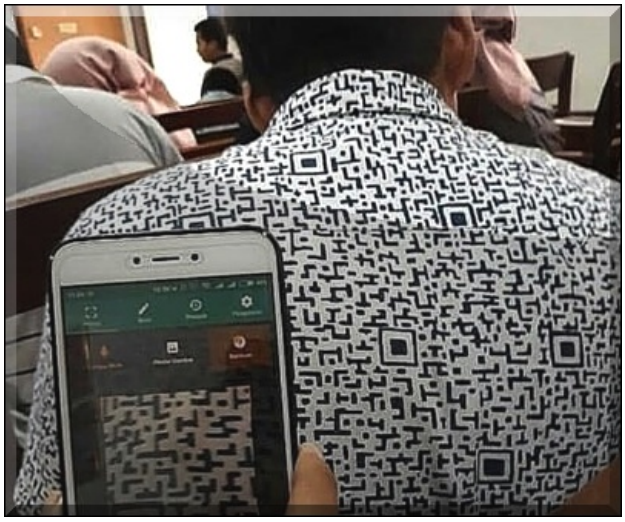
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

1720

Horgászati módszerek

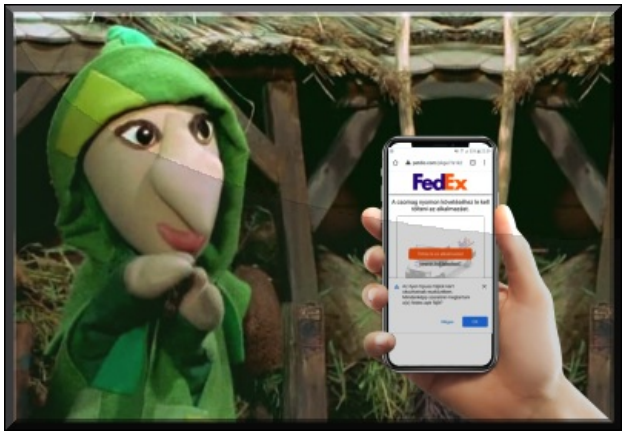
2023. július 27. 18:02 - Csizmazia Darab István [Rambo]

Lassan már kevés lesz szimplán adathalászatot említeni, hiszen a klasszikus phishing mellett **olyan újabb keletű műszavakat is meg kellett tanulnunk, mint a smishing, a vishing, és a quishing.**



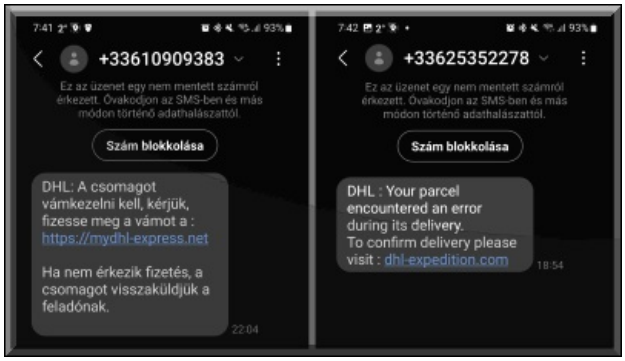
Az alapfokú phishing már mindenki által ismert, egy ismert szolgáltató webhelyére megszólalásig hasonlító, de kártékony weboldalon bekérik a felhasználó adatait, amivel aztán a bűnözők a valódi weboldalon már be tudnak lépni a nevében. Ez a vonal körülbelül 1995 óta létezik, és azóta is szedi az áldozatait. **Egy 2020-as FBI kimutatás pedig arról számolt be, hogy ez egy annyira gyakori kiberbűnözői módszer, hogy abban az évben már több adathalász incidenst regisztráltak, mint összességében bármely más egyéb típusú számítógépes bűncselekményből.**

És hogy ez a céges biztonságban is komoly problémát okoz, azt **egy 2023-as adat is jól mutatja, miszerint a vállalati szférában jelentkező fejlett és automatizált adathalász támadási kísérletek száma a tavalyi évben 356%-kal nőtt, ezek egy jelentős részénél pedig már alkalmazták a gépi tanulás és a mesterséges intelligencia eszközeit is.**



A felsorolás és tulajdonképpen a megjelenés sorrendjében is **következő a smishing, amely a phishing és az SMS vagyis Short Message Service, magyarul rövidüzenet-szolgáltatás szavak összekeveredéséből keletkezett. Itt az érkező SMS érkezhet látszólag a bankunk nevében, de lehet csomagküldő szolgálat, adóhivatal, Amazon, Netflix, PayPal, bármi.**

A lényeg, hogy a telefon esetlegesen kevésbé védett, és kisebb képernyőjén nehezebb felismerni a kártékony linket, a rosszindulatú weboldalt, az átverést. Mindenki emlékezhet a 2021. márciusi FedEx nevében érkező SMS áradatra, amely a FluBot vírust terjesztette, de **a dolog azóta is folyamatosan zajlik DHL, Netflix, Magyar Posta és hasonló szolgáltatások nevével visszaélve.**



A fentiek remélhetőleg már mindenkinek a könyökén jönnek ki, és sosem vetemednének arra, hogy ilyenekre kattintsanak. **Éppen ez volt az oka, hogy új irányzatok jelentek meg, így nevezetesen vishingnek (vagyis Voice Phishing) hívjuk a telefonhíváson keresztül végzett adathalászatot. Sajnos ez már sokkal hatékonyabb fegyvere lett a támadóknak, akik gyakran bankok nevében hívogatnak** random vagy korábbi adatszivárgásból precízebben célozható ügyfeleket, akiknél azzal a mesével jelentkeznek, hogy ők a bank biztonsági osztálya, és egy csúnya bűnöző éppen most próbál pénzt lopni a kártyájáról.

Erre hivatkozva kérnek személyi azonosítást, bank számla és kártya adatokat, azonban éppen ezzel követ el súlyos hibát, aki ezt bediktálja nekik, vagy feltelepíti a csalók által javasolt távmenedzsment alkalmazást, ugyanis ekkor tényleg leürítik a számláját. **A hagyományos csatornák mellett a vishing, azaz élő telefonos hangalapú megtévesztések száma is kiugró mértékben emelkedett, ebben egy 2023-a keltezésű statisztika 363 százalékos emelkedést regisztrált.**



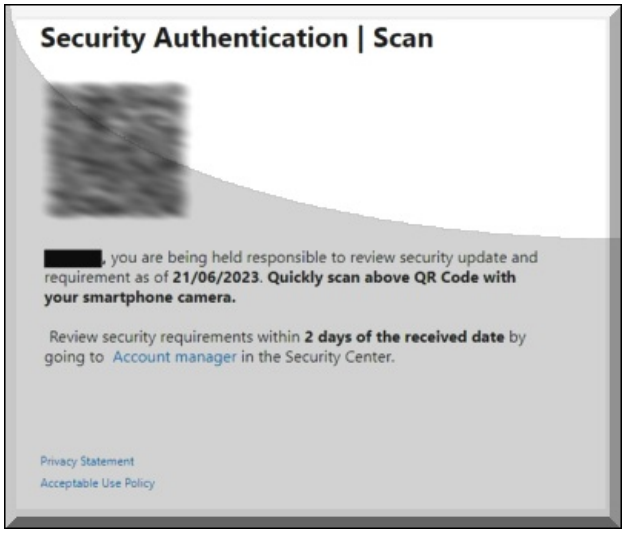
Ugyanennek az átverésnek egy másik változata, amelynél a számítógépesen kevésbé jártas júzereket egyszerűen arra kérik, meglévő pénzüket gyorsan utalják át ideiglenesen egy állítólagos biztonsági számlára - kitalálható a történet vége, itt is eltűnnek a pénzzel. És hogy mekkora károkat képesek okozni ezzel itt Magyarországon is, azzal egy friss statisztikában szembesülhetünk.

Három éve még a károk többségét a hitelintézetek viselték, ez 2019-ben még "csak" 8% volt. **2022-ben a keletkezett 1 mrd forintos kár 52%-át már az ügyfelek viselték, míg 2023. első negyedévében már 83%-ban az ügyfél kár volt az ilyen incidens, hiszen ő hibázott, ő adta meg illetéktelennek az adatokat, így itt a banknak már nincs felelőssége**. A jelentés szerint a csalók csak az idei év első három hónapjában vásárlással 1.6 mrd forintot, míg az adathalászok összesen 39 ezer incidensben összesen 1.1 milliárd forintot vágtak zsebre.



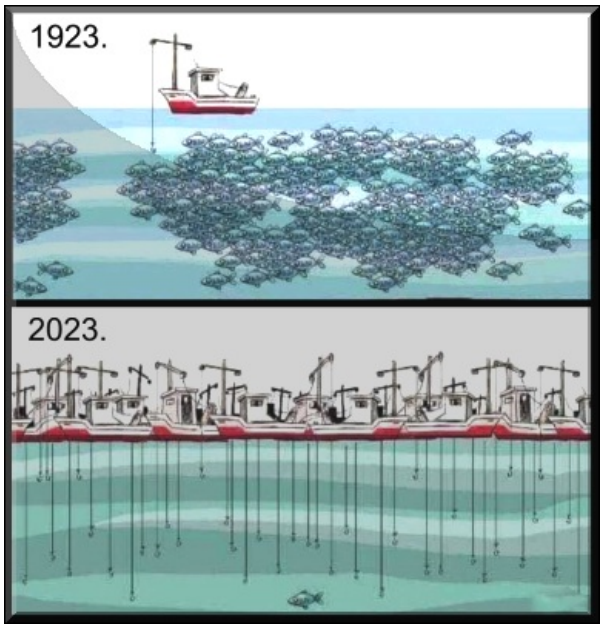
Innen már csak egy utolsó lépés maradt, ez pedig nem más, mint a talán kevésbé ismert quishing. **Ez pedig a QR kódokkal való adathalászati módszert takarja, amelynél a mobil kamerájával beolvasva gyorsan gyakran megnyílik egy weboldal, telepíthető egy app, de ezeken túlmenően akár telefonhívást, SMS üzenetet vagy digitális fizetés is indíthat az ilyen kód.**

Ez pedig sok lehetőséget ad a csalóknak, akik az elemzők szerint a Covid időszak óta intenzíven próbálgatják ez a fajta támadást is. Biztonsági elemzők egy csoportja hónapokon keresztül kísérte figyelemmel ezt a fajta QR kódos adathalászatot, és arra a megállapításra jutottak, hogy egyre több ilyen próbálkozást lehet látni.



A csalók változatos módokon próbálják rávenni a felhasználókat a rosszindulatú QR kódok beolvasására. A hozzánk érkező üzenet hivatkozhat valamilyen lehetőséghez kapcsolatos bejelentkezési oldalra, regisztrációra, gyors és kényelmes fizetési lehetőség felkínálására.

Sok helyen már bevett gyakorlat a QR kódok beolvasás - például múzeumokban, utastájékoztatásban, de éttermek is vannak, ahol az étlapot így lehet elérni, viszont összességében **nem alakult ki egészséges gyanakvás a kéretlen, kétes esetek kezelésére, ahogy a mobil eszközök vírusvédelmére sem fordít még sajnos mindenki figyelmet.**



Mindenesetre legyen az adathalászat írásbeli, audió vagy kétdimenziós vonalkód formátumú, éljen mindenkiben biztonságtudatos óvatosság. **Bankok például sosem kérnek az ügyfeleiktől telefonon a belépési azonosító kódokat, jelszavakat, a bankkártyás utaláshoz kapott CVC biztonsági ellenőrző kódot.**

Ha valamilyen gyanús üzenet, e-mail, telefonhívás esik be, legyünk gyanakvóak, ne kapkodjunk, na hagyjuk magunkat sürgetni, és ha nem értjük a szituációt, bátran lépjünk ki belőle. A támadások ilyen formái ugyanis sajnos egyre többször fognak kopogtatni mindannyiunknál.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: megelőzés phishing vishing védekezés adathalászat smishing quishing

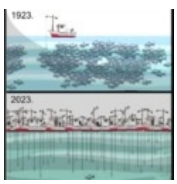
Ajánlott bejegyzések:



Az adathalászatot megölni nem kell félnetek


Identitás lopás: nem függ az életkortól


Mai szavunk pedig: smishing


A pisztácia kifogyott, adatlopás nem is volt...


Drágán add a bankkártyád!

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

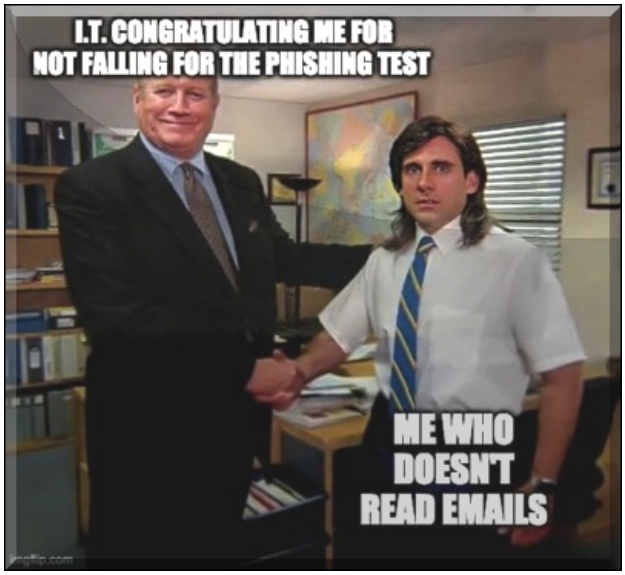
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

663

Tipikus adathalász üzenet tárgysorok

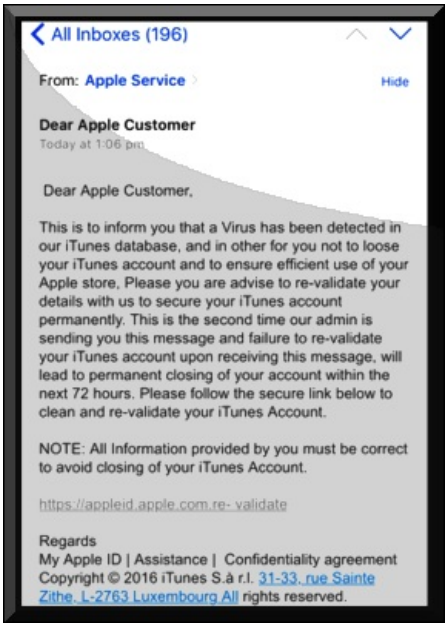
2023. július 31. 09:46 - Csizmazia Darab István [Rambo]

Lehet, hogy könnyebb lenne azt összegyűjteni, mi nem szerepel ezekben, annyira sokféle kéretlen rosszindulatú levél érkezett már az évek során, ám ennek ellenére érdemes lehet néhány klasszikus, jellegzetes formulát csokorba szedni.



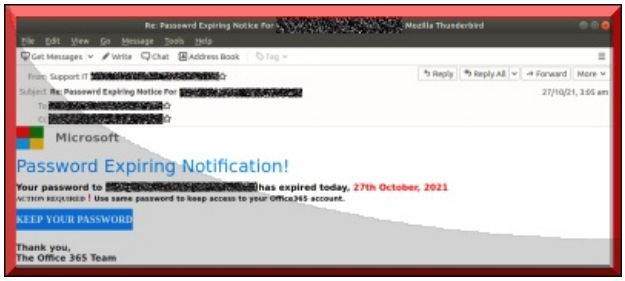
A csalók mindig, **minden helyzetben kihasználják az aktuális eseményeket**, legyen az olimpia vagy földrengés, lezuhant repülő vagy világjárvány, netán közelgő kulturális esemény vagy háború.

Azonnal reagálnak, **gyorsan kreálnak hozzá hazug mesét, és jönnek az adománygyűjtésről, zárolt fiókértesítésről, kamu nyereményekről vagy bennfentes titkos információkról szól üzenetek**. A teljesség igénye nélkül lássunk most ezek közül pár igen gyakori archetípust.



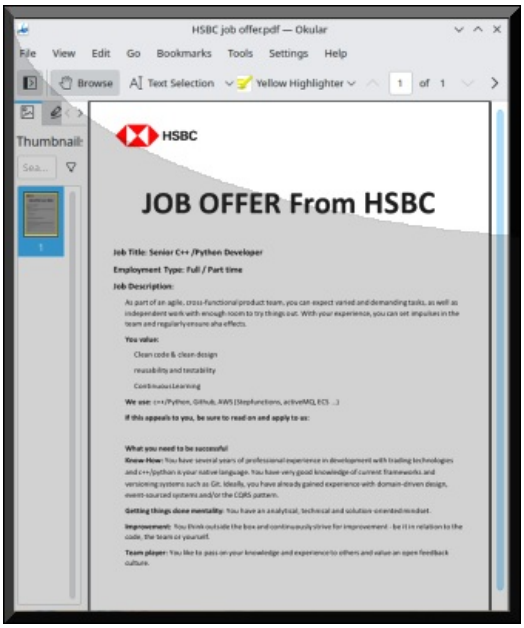
"Az Ön munkamenete lejárt. Kérjük kattintson ide az újbóli bejelentkezéshez!" - ennél jellegzetesebb átverési taktikát tényleg nehéz találni, és ehhez elég a mellékelt linken képileg lemásolni a legitim valós bejelentkezési ablakot, ahol a felhasználók többsége különösebb hezitálás és gondolkodás nélkül máris begépeli az azonosítóját. **Ilyen próbálkozások szinte minden platform ellen indultak már, a PayPaltól, Netflixtől, Apple-től kezdve a GutHub-on át az Amazonig.**

Egy 2016-os Apple felhasználóknak szánt átverésben például vicces módon azt írták, azért kell újra mindenkinek bejelentkezni, mert "vírust" találtak az Apple iTunes adatbázisában.



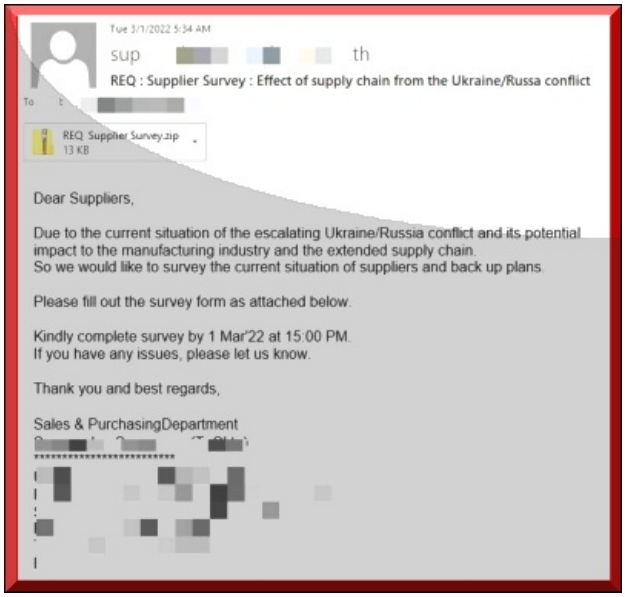
A sürgős fizetnivalóra való hivatkozás is elterjedt módszer, ami roppant változatos formában érkezhet: lehet ez hamis közüzemi számla, állítólagos nekünk érkező postai küldemény, elmulasztott adóbefizetés, lejárt előfizetési konstrukció, és hasonlók. **Az ilyen eseteknél jobbára már összegyűjtöttek személyes adatokat az áldozatokról, és sokszor valamennyire célzottan küldik a fizetési kérelmet.**

Ebben a műfajban a **haladó csoportos forma pedig az a cégek elleni csalási forma, ahol a munkahelyi elöljárónk nevében kérnek azonnali, de bizalmas átutalást, megrendelést, amit majd később hagynak jóvá** és papíroznak le. Itt komoly pénzügyi szervezetek, kormányhivatalok is lépre tudnak menni, ha nincs meg a szükséges óvatosság és gyanakvás.



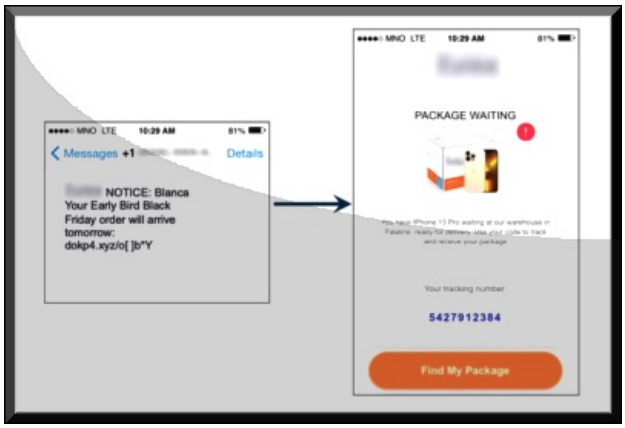
Az állásajánlatokat sem kerüli el a rosszindulat, és kaphatunk olyan Kedves jelentkező subject sorral rendelkező kéretlen levelet valamilyen fejvadász cég nevében, ahol ha bár nem is jelentkeztünk semmilyen állásra, mégis erre hivatkozva kérnek tőlünk további személyes adatokat.

Erre jó példa lehet a Lazarus csoport által indított Operation DreamJob kampány, amelyben hamis állásajánlatokkal igyekeztek megtéveszteni az áldozatokat, és sok esetben sikerrel is jártak.



Rendkívüli helyzet való hivatkozás is gyakori, legyen szó Covid helyzetről vagy háborús válságról. Az ukrajnai háborúval kapcsolatban tucatnyi ilyet lehetne említeni, ahol rosszindulatú link, vagy kártékony melléklet érkezett a levélben. **Itt pedig további kíváncsiságot gerjesztő kreativitásról is tanúbizonyságot tettek a bűnözők, például a csatolt állomány elnevezése is fokozhatja az érdeklődést, például azzal ha figyelemfelkeltő vagy ha pontosan az**

ellenkezője látszik a címében, mint amiről a kéretlen üzenet szól. Ekkor sokan, hogy megbizonyosodjanak, mi is az igazság, mégis kattintanak, megnyitnak.



Piros betűs ünnepek, évfordulók - ez mind jó apropó arra, hogy hivatkozni lehessen rájuk a kéretlen üzenetekben. Ismert cégek nevében ünnepi **árleszállítást, akciókat, karácsonyi képeslapokat, ajándékutalványokat hirdetnek, amelyek csak rövid ideig érhetőek el**, ezért mindenki siessen, nehogy ezekről lemaradjon.

A mellékelt link vagy csatolmány pedig a jól ismert módon veszélyezteti azokat, akik ezeknek bedőlnek.



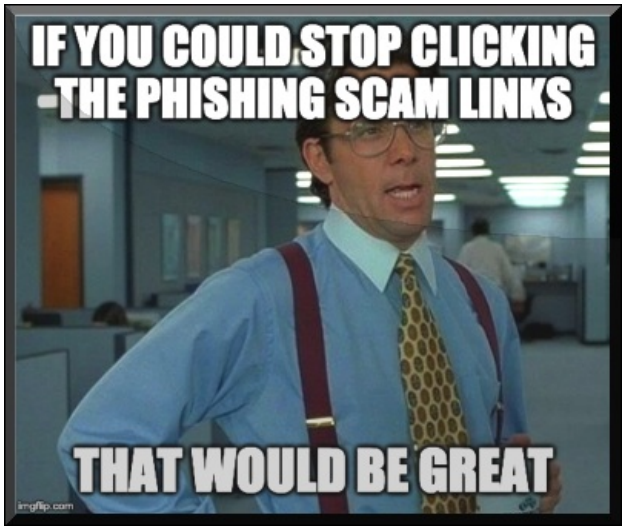
Az adóbevallási szezon slágere, ha ezzel kapcsolatban kapunk megtévesztő üzenetet. Itt is többféle lehetőséget ragadhatnak meg az elkövetők, lehet például olyan levél, ami arról tájékoztat bennünket, hogy nem sikerült feldolgozni a határidőre benyújtott adóbevallásunkat, mert bizonyos személyi és pénzügyi információk állítólag hiányosak. Természetesen minden gyorsan orvosolható, ha a mellékelt linken mindezeket begépeljük.

A másik jellemző csalási forma, ha adó-visszatérítést ígérnek, ami mindenki számára vonzó hír lehet, és emiatt aztán a nem várt summa reményében minden banki adatukat megadják.



És végül, de nem utolsósorban az is egy tipikus gyakorlata, ha hiányos vagy semmilyen magyarázat nincs a levélben, hanem csak arra hivatkoznak, mindent megtudhatunk a mellékletből, ami legtöbbször valamilyen sebezhetőséget tartalmazó Office vagy PDF fájl.

Sajnos sokszor itt is győz a kíváncsiság az egészséges gyanakvás ellenében, pedig biztonságtudatos hozzáállással, a gyanús melléklet VirusTotal ellenőrzésével már beljebb lennénk.



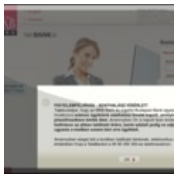
Kismilliószor összefoglaltuk már, mikre érdemes figyelni, ezért itt ezt most csak röviden említjük.

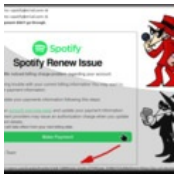
Mindig olvassuk el figyelmesen az üzeneteinket, használjunk vírusvédelmet és spam szűrést, ellenőrizzük a feladót, nem hagyjuk magunkat sürgetni, figyeljünk a legitim domén nevekre, ha pedig valami túl szép ahhoz hogy igaz legyen, ne dőljünk be az ilyen ígéreteknek.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: spam jellemző üzenet tipikus phishing adathalászat subject welivesecurity.com

Ajánlott bejegyzések:

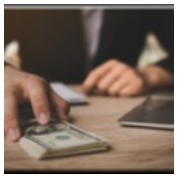

MKB adathalászat szigonnyal, horoggal, hálóval



Spotify megújítási probléma - vagy mégsem?



Netflix: lejárt a tagságunk. Vagy mégsem?


Megváltás-e a váltságdíj?



Adathalászat menni booking.com

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

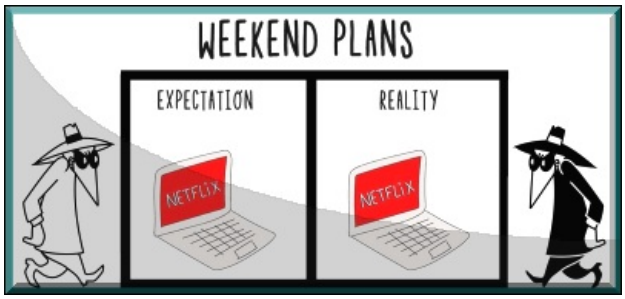
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

1178

Netflix: lejárt a tagságunk. Vagy mégsem?

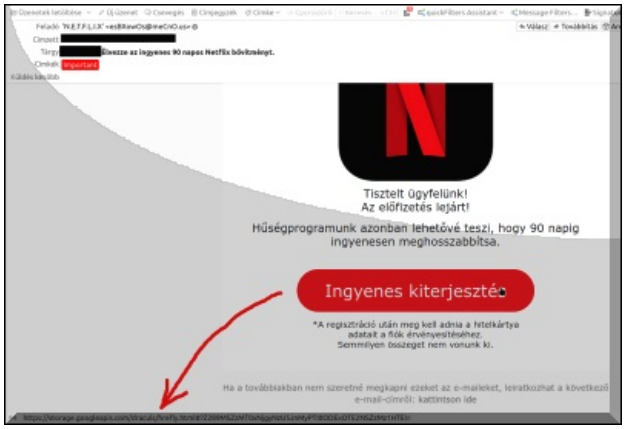
2023. augusztus 03. 09:04 - Csizmazia Darab István [Rambo]

Hát a jelek szerint eléggé itt sokkal több zseton felirata lesz "vagy mégsem", mindez sokkal inkább egy soron következő adathalász átverés.



A csomagküldő szolgálatok nevében írt kamu üzenetek, a különféle közművek nevével visszaélve hamis áram, gáz, telefon számla érkezik - ezeket mind láttuk már az évek során.

És hát a Netflix sem először kerül bele az átverős kofferbe, legutóbb például SMS-ben érkezett hasonló, a fiók felfüggesztésével ijesztgető értesítés.



Ezúttal a nyári időszakot célozták be a bűnözők, akik egy magyar nyelvre némileg hasonlító ;-/ szövegezésű e-mailben arra hivatkoznak, hogy **nemrég lejárt a Netflix tagságunk, no de nincsen semmi baj, mert a hűségprogram keretében ezt most 90 napra ingyen meghosszabbíthatjuk. Ehhez mindössze csak kattintani kell a mellékelt linkre.**

Azonban a rekkenő hőség ellenére sem érdemes ennek bedőlni, hiszen számtalan látványos gyanús jel mutatja, hogy itt bizony ismét egy orbitális csalással van dolgunk.



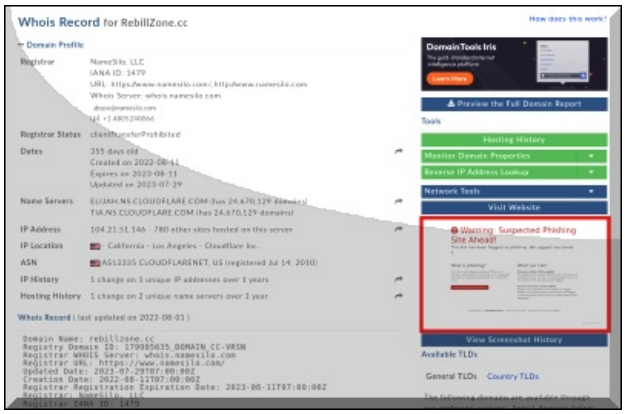


Az elütések, helyesírási hibák tipikus jellemzői az ilyen sablon leveleknek, nézzük hát meg, itt mit látunk: "*A regisztráció után meg kell adnia a hitelkártya adatait a fiók érvényesítéséhez. Semmilyen összeget nem vonunk ki.*". Nem vonnak ki, ez remek hír. Akárcsak **a feladó címe, tegye fel a kezét az, aki ezt hivatalosnak gondolja: "*esBXowOs KUKAC meCnO PONT us*".** Nem igazán kell sorszámot osztogatni a tolongóknak.

A levél a trace információi alapján a németországi Falkensteinből érkezett. A hivatkozott link pedig a rosszindulatú tartalmakat sokszor terjesztő storage.googleapis.com helyre mutat, ami egy hivatalos Netflix megkeresés esetén eléggé valószínűtlen. **A rebillzone pedig egy Kókusz-Szigeteken regisztrált oldal**, nyilván ez sem erősítheti nagy léptekkel az állítólagos ingyen hosszabbításba vetett bizalmat.







A csakazértis egérkatt után **a Netcraft böngésző kiegészítő pedánsan riaszt a gyanús adathalász oldalra**, de mi most a demo kedvéért ugorjuk át ezt az figyelmeztetést, és nézzük meg, mi vár ránk mögötte. **A weboldal címe így kezdődik: "utmostspores PONT world/blablabla". Lehet, hogy ez mégsem az eredeti Netflix hivatalos weboldala?** Ahogy a lapon a "Terms & Conditions", és a "Privacy Policy" linkek is csak bambán visszamutatnak ugyanerre az oldalra, nem vezetnek el sehova, nincs mit elolvasni rajtuk.

A Fülig Jimmy jellegű nyelvtan itt is folytatódik, a weboldalon például ezt olvashatjuk: "* *Feliratkozás után adja meg bakkártyája adatait a fiókja leellenőrzéséhez.*" Ezek alapján a BAKKÁRTYÁNK biztonságban van, arról

nem vonnak ki semmilyen összeget, szemben például a bankkártyánkkal, ahonnan viszont mindez már korántsem ilyen biztos.





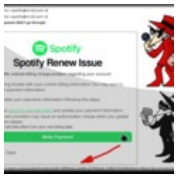
Ha valaki itt végiglépked a folyamaton, jön egy kitöltendő űrlap a személyes adatokkal: név, cím, e-mail, telefon **és tadaaaam, mégis csak fizessünk 1841.4 forintot. Hogy ez az összeg hogy jött ki: rejtély, akárcsak az, hogy miért fizetünk az ingyenes hosszabbításért, hiszen azt ígérték: "*Élvezze az ingyenes 90 napos Netflix bővítményt*."** Plusz ha tényleg ügyfelek vagyunk vagy lennénk, akkor a korábbi fizetési módot nem kellene tőlünk újra bekérni, mert azt már tudnák.

Aki itt óvatlanul begépeli a valós bankkártya adatait, az azonnal a csalóknál landol, akik valószínűleg tartják a fenti ígéretüket, és a BAKKÁRTYÁRÓL talán valóban nem fognak KIVONNI összeget, de a többi szomorú fejlemény azért már talán sejthető...

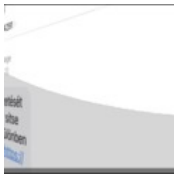
Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: spam e-mail csalás átverés phishing netflix adathalászat hosszabbítás lejárat

Ajánlott bejegyzések:



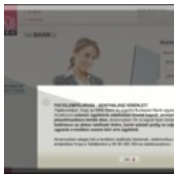
Spotify megújítási probléma - vagy mégsem?



2023. első csalásai



Tagsági kérdések - vagy mégsem?



MKB adathalászat szigonnyal, horoggal, hálóval



Adathalászat menni booking.com

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

521

Clop ransomware menni Torrent

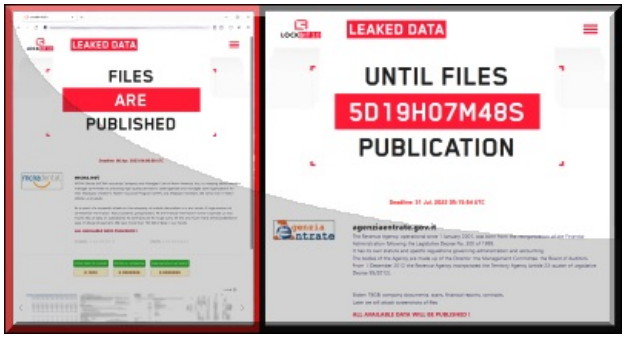
2023. augusztus 08. 09:53 - Csizmazia Darab István [Rambo]

A Clop zsarolóvírusról már többször esett szó itt a blogban is, többek közt 2021-ben behatoltak a Royal Dutch Shell rendszereibe, illetve arról is írtunk, hogy **sokszor úgy támadtak vállalati rendszerek ellen, hogy kifejezetten vezető beosztású alkalmazottakat céloztak meg.**



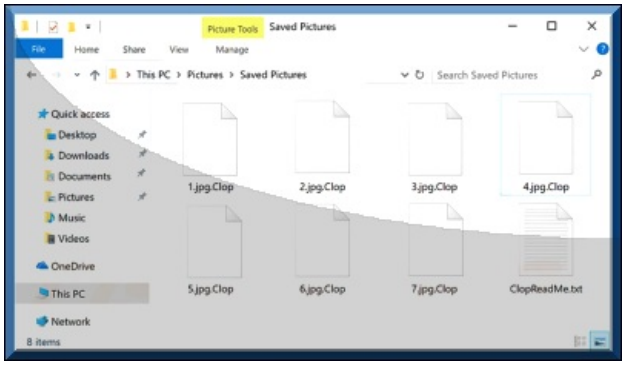
Illetve hozzájuk köthető, hogy futószalagon intéznek **ransomware támadásokat az ipari ágazatok területén, például az ipari termelő, gép- és szerszám gyártós és kereskedelmi, logisztikai, tervezői, építőipari, járműgyártói szereplőket célozva** hajtanak végre akciókat.

A hírhedt oroszországi Clop mellett több más bűnözői csoport is jelen van még ezen a területen, például a Lockbit, a Royal és a BlackCat is előszeretettel támad kritikus infrastruktúrákat, nagyvállalatokat. A Clop banda újítása volt, hogy **2021. óta különböző zero-day sebezhetőségre alapozva hajtottak végre tömegesen sikeres ransomware támadásokat.**



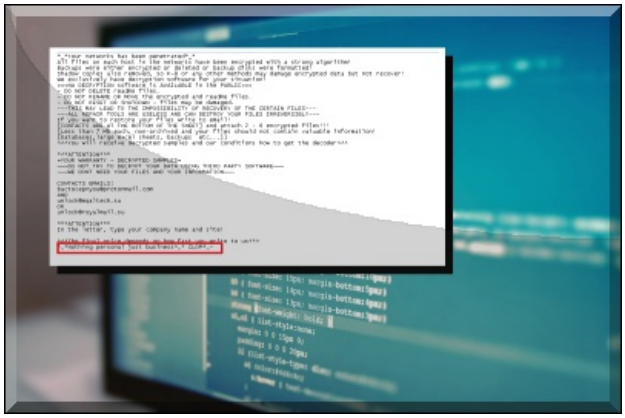
A doxing megjelenése és általánossá válása óta sajnos a támadók az elkódolás előtt még el is lopják a bizalmas céges adatokat, és ezek publikálásával fenyegetik meg az áldozatokat. **Eddig zömmel az volt a gyakorlat, hogy a publikus neten, vagy a darkneten volt a csoportoknak ilyen dedikált szivárogtató Tor oldala, ahol első körben bizonyítékként tettek ki néhány fájlt, viszont nem fizetés esetén kipakoltak mindent.**

Legutóbb például az USA-beli Managed Care of North America (MCNA) Dental **fogászati biztosítási óriáscég szenvedett el ilyen incidenst a LockBit-től, ahol miután megtagadták a 10 millió dolláros váltságdíj kifizetését, az ellopott bizalmas adatokat - ez 700 GB volt - kiszivárogtatták.** Itt nevek, lakcímek, születési dátumok, telefonszámok, e-mail címek, társadalombiztosítási azonosítók, egészségbiztosítási adatok, kezelési tervek, röntgen felvételek, kezelési számlák kerültek ki a netre.



Az ilyen eseteknél a hatóságok még időnként tudtak lépni, és bár nem volt tudható, előzőleg hány példányban és hova kerülhettek ki az adatok, de esetenként lelőttek szivárogtató webhelyeket. **Ezt látva a bűnözők is továbbléptek, és most elsőként a Clop banda vezette be, hogy peer-to-peer átvitelt használó torrent segítségével végzik a szivárogtatást a korábbi hagyományos Tor weboldal helyett.**

Ezzel egyrészt sikerült megoldaniuk, hogy mivel ez a terjesztési módszer decentralizált, a bűnüldöző szerveknek nincs módja a lopott adatok áramlásának a leállítására.



Másrészt ennél a technológiánál **az adatátviteli sebesség is jelentősen gyorsult,** és ez megoldotta a korábbi gyenge adatátviteli problémákat.

Nagyon valószínű, hogy nemcsak ők, hanem a versenytársak is előbb-utóbb át fognak nyergelni erre a hatékonyabb módszerre, és ezzel sajnos további nyomást gyakorolhatnak az áldozatokra a lopott adatok szélesebb körű terjesztési lehetősége miatt. A BleepingComputer rövid tesztjében az új módszer 5.4 Mbps adatátviteli sebességéről számolt be, pedig az csak egy oroszországi IP-címről indult.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: torrent orosz bűnszervezet váltságdíj zsaroló ransomware szivárogtatás zsarolóvírus clop

Ajánlott bejegyzések:



8 kórház, 30 klinika, 2.5 millió betegadat



LockBit piacgazdaság és tervgazdálkodás



Windows frissítés vagy mégsem?



Ransomware támadás a Nissan ellen



Ransomware a One Motelben

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

Néha nincs jó választás

2023. augusztus 10. 10:26 - Csizmazia Darab István [Rambo]

Brutális adatszivárgásra derült fény **az Egyesült Királyság Választási Bizottságával kapcsolatosan, amelynek során 8 év választói adatai kerültek illetéktelen kezekbe. A mostani nyilvános bejelentés egy hónapokkal korábban felfedezett incidensről számolt be.**



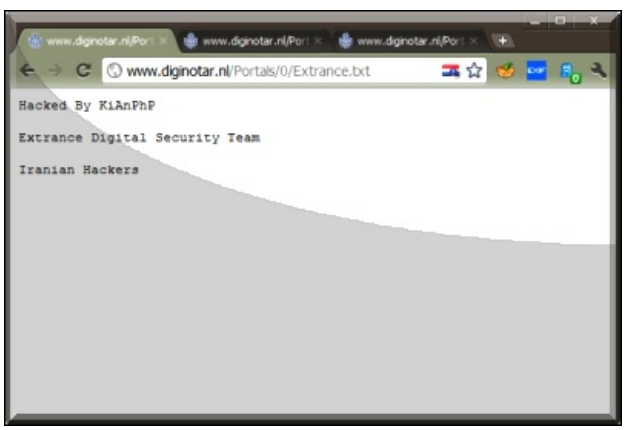
Nem akármilyen adatlopási eset került a címlapokra, ezúttal ugyanis egy 2022. októberében észlelt kibertámadás borzolja a brit kedélyeket. Hogy miért most **15 hónappal később számoltak be erről, arra egyelőre nincs magyarázat, a vizsgálat során azonban arra már fény derült, hogy behatolás-feltörés még korábban, 2021. augusztusában következett be.**

Mindenki, aki 2014. és 2022. között szavazásra regisztrált az Egyesült Királyságban akár helyben, akár a tengeren túlról, érintett a kibertámadásban. A távolban valahol most felsír egy GDPR...



A támadók hozzáfértek a kormányhivatal e-mailjeihez, a belső rendszerhez, a választói névjegyzékek másolatait tároló szerverekhez és meg nem nevezett egyéb rendszerekhez. Emiatt biztosan áldozatul estek a választói névjegyzékek referenciamásolatai, amelyeket amiatt tároltak, hogy utólagosan ezeken a politikai adományok megengedhetőségi ellenőrzését elvégezze a bizottság.

A friss nyilatkozat szerint jelenleg az információs biztos hivatala vizsgálja az esetet, bővebb információkkal később fognak tudni szolgálni. Talán jó lett volna a hatóságokat és a nyilvánosságot is 15 hónappal korábban értesíteni.



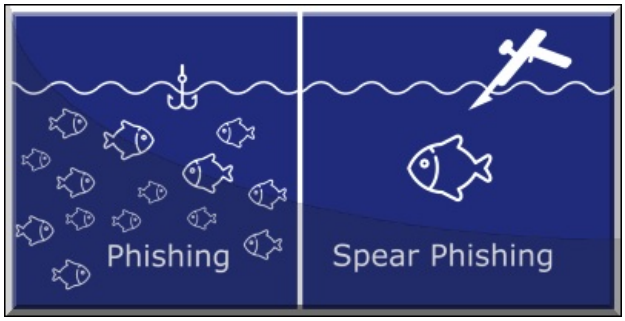
A kiszivárgott adatok köre igen széles, amely **az Exchange levelező rendszerből teljes nevek, e-mail címek, lakcímek, telefonszámok, és a bizottságnak elküldött webes űrlapok, személyes fotók és a teljes belső és külső levelezési anyag.** A választói névjegyzéknél hasonló a helyzet, itt szintén teljes nevek, a nyilvántartásban szereplő lakcímek, életkori adatok kerültek ki.

A bizottság szerint a kibertámadás nem volt hatással a választásokra vagy az egyének szavazói regisztrációjára. Épp csak azt nem tették hozzá, hogy "az incidens hatása minimális" - lásd a 2011-es Diginotar sztorit.



Hogy volt-e titkosítás, naplózás, jogosultság ellenőrzés, stb. - nem ismert, de é**rzetre mintha mindez a 90-es években történt volna meg.**

A bizottság emellett azt is közölte, hogy egyelőre nem tudják, ki állhat az akció mögött, a felelősséget egyelőre senki, se ismert bűnözői kör, se ellenséges nemzetállam nem vállalta magára.



Annak ellenére, hogy a jelentésben igyekeznek a bekövetkezett incidens lehetséges kockázatait mélyen alábecsülni, **az érzékeny személyes adatok birtokában az érintetteknek mindenképpen fel kell készülniük a jövőben olyan célzott adathalász e-mailekre, testre szabott telefonhívásokra, amelyek során további bizalmas információkat, például jelszavakat, számlaszámokat vagy pénzügyi információkat próbálnak meg majd tőlük begyűjteni.**

Ami viszont még biztosan további járulékos kár, az a súlyos bizalomvesztés az adatainkat kezelő hivatali intézmények irányába, hogy ilyen egyáltalán megtörténhetett.

Megosztom tumblr. Tweet Pin it Tetszik 0

1 komment
Címkék: választás brit uk adatlopás adatszivárgás commission elctoral

Ajánlott bejegyzések:


Ransomware támadás a Nissan ellen


Szolgálunk és nem védünk


Baj van Tajvanban


9 millió, bizony, dalolva ment...



Go Western Digital II.

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Androsz · http://wikipedia.blog.hu/ 2023.08.11. 00:01:17

Hát, gratulálok. Ilyen szerencsétlen pöcsök őrzik a kényszerűségből eléjük tárt adatainkat, azért, hogy aztán azokat valaki lekaszálja. Sosem értettem meg, mire jó, hogy az adatokat minden nyamvadt űrlapra állandóan le kell írnom, elég lenne egyetlen halálbiztosan őrzött adattár, amelyhez naplózott módon kellene hozzáférni. Amikor a személyi számot pellengérre állították és helyette minden zugirodának jogot adtak a nyilvántartáshoz, ennek a lopásnak követték le az utat.

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

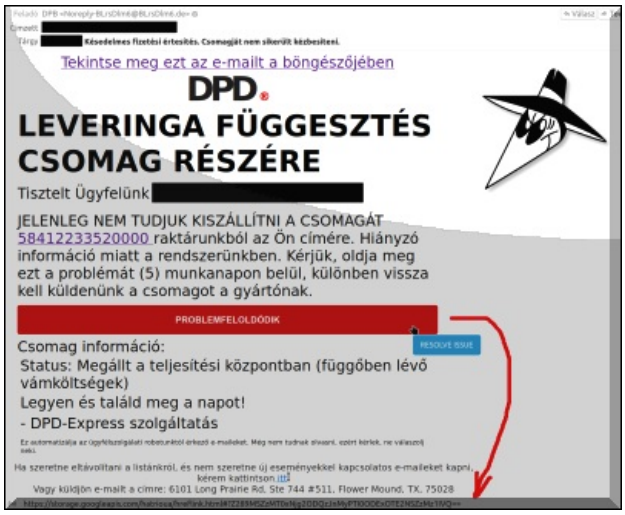
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

2004

"NEM TUDJUK KISZÁLLÍTNI A CSOMAGÁT"

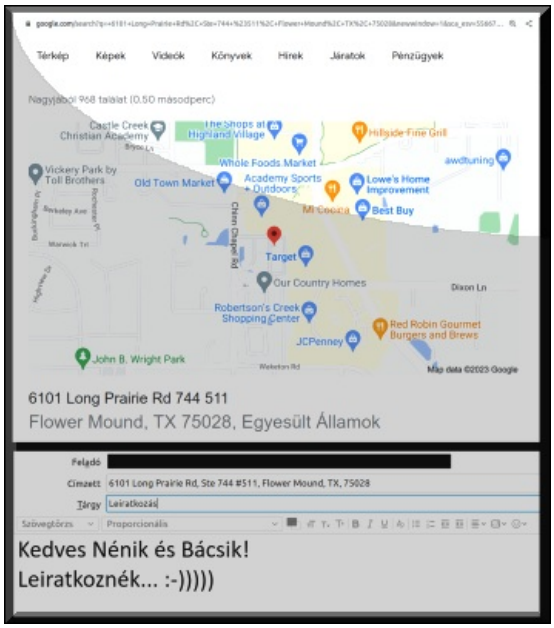
2023. augusztus 14. 16:58 - Csizmazia Darab István [Rambo]

A kéretlen üzenetek kezelésének nulladik lépése az óvatos figyelmesség és az előzetes rákeresés a gyanúsnak vélt levélre. Így például könnyen kiderülhet, hogy mai hamis DPD munkadarabunk már egy jó ideje járja be Európát...



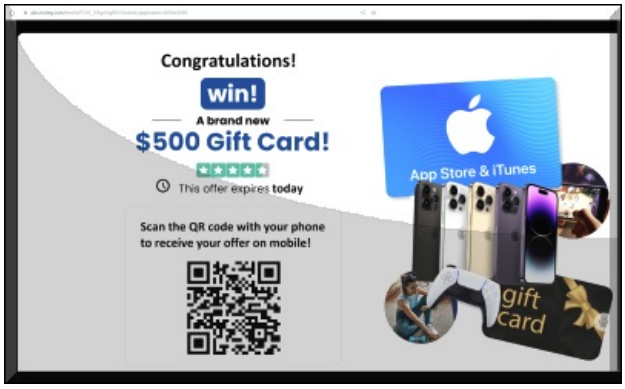
Ami Rejtő Jenő írásaiban még tök vicces Török Szultán, Fülig Jimmy, vagy Csülök szájából, az már sokkal inkább fárasztóan cringe egy ilyen hivatalos üzenetnek szánt e-mailben. **Ha olyan kitételeket látunk, mint "*JELENLEG NEM TUDJUK KISZÁLLÍTNI A CSOMAGÁT*", "*Legyen és találd meg a napot!*", valamint "*PROBLEMFELOLDÓDIK*", nem is nagyon kell gondolkodni azon, vajon várunk-e egyáltalán valahonnan csomagot, elég szimplán a Delete gombra könyökölni és így a probléma tényleg megoldódik.**

De ez a mondat is elég viccesen hangzik: "*Kérjük, oldja meg ezt a problémát (5) munkanapon belül, különben vissza kell küldenünk a csomagot a gyártónak*." Vagyis ezek szerint nem is a feladónak küldik azt vissza, hanem a gyártónak.



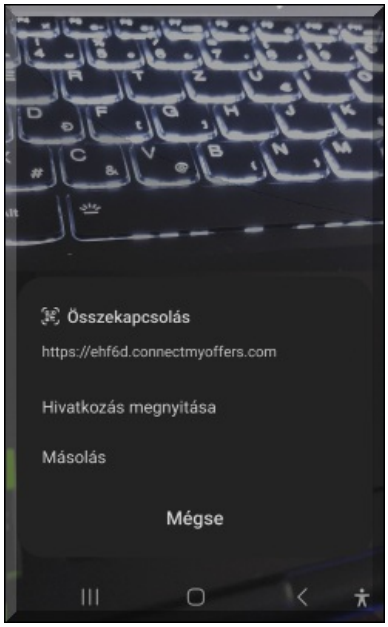
A mazochisták kedvéért végig lehet gyalogolni a további gyanús jeleken, például **a feladó címén: Noreply-BLrsDlm6 KUKAC BLrsDlm6 PONT de. Ugye ezer százalék, hogy ez aztán biztosan egy hivatalos DPD futárszolgálati megkeresés lesz, hiszen más tuti nem is lehetne ;-)**

Az e-mail trace szerint Berlinből küldték, a levél alján a leiratkozási útmutatóban viszont ez olvasható: "Vagy küldjön e-mailt a címre: 6101 Long Prairie Rd, Ste 744 #511, Flower Mound, TX, 75028". **Hát mi most csak azért nem küldtünk e-mailt az USA-beli "6101 Long Prairie Rd, Ste 744 #511, Flower Mound, TX, 75028"-nak, mert sehol nincs benne egy árva KUKAC...**



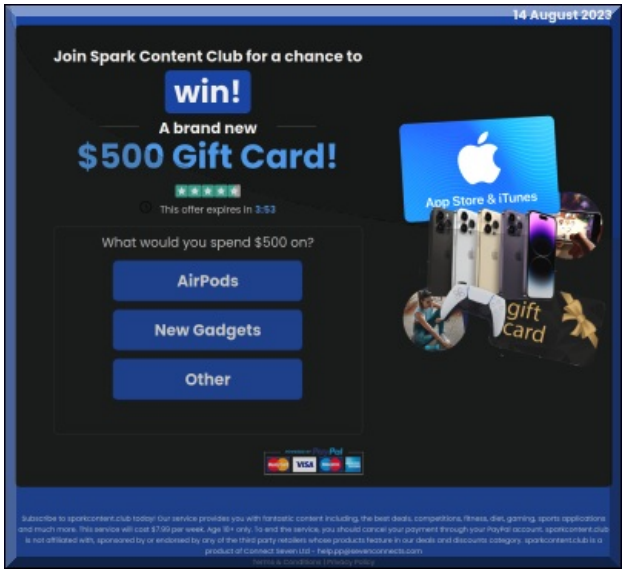
A próba kedvéért kattintsunk rá a "PROBLEMFELOLDÓDIK" gombra, és egy kéretlen reklám oldal jelenik meg (de ekkor már a vírusvédelem, és a böngésző kiegészítők már beszólnak, hogy ezt lehetőleg mégse tegyük, mert kártékony tartalom következik).

Az oldal egyébként azt állítja, 500 dollár értékű (kb. 175 ezer HUF) Apple ajándék utalványt nyertünk, ehhez mindössze csak be kell szkenneljük a mellékelt QR kódot. És ki ne akarna egy ilyen nagyvonalú ajándékot?



Egy korábbi adathalászos posztunkban már kiveséztük, hogy **a már jól ismert klasszikus phishing, az SMS-ben érkező smishing és a hangalapú telefonhívásos vishing mellett, hogy pontosan mi is az a quishing.**

Ez pedig a QR kódokkal való adathalászati módszert takarja, amelynél a mobil kamerájával beolvasva gyorsan gyakran megnyílik egy weboldal, telepíthető egy app, de ezeken túlmenően akár telefonhívást, SMS üzenetet vagy digitális fizetés is indíthat az ilyen ismeretlen kód.



A linket az asztali böngészőben megnyitva újabb ablak tájékoztat arról, hogy **500 dollár értékű (kb. 175 ezer HUF) Apple ajándék utalványt nyertünk**, ehhez ugorjunk az ehf6d PONT connectmyoffers PONT com weboldalra. **Itt választhatunk a nyeremények között (gyakorlatilag mindegy, hogy melyiket jelöljük meg) és a következő kérdés az lesz, van-e PayPal account a birtokunkban.**

Ha nemet válaszolunk, akkor Gazdálkodj okosan játékhoz hasonlóan máris visszakerülünk a START mezőre, és újra a beszkennelhető QR kód társaságában kötünk ki, ám a bank itt a mezőre lépésért sajnos nem ad nekünk semmit.



Ha viszont azt jelöljük meg, hogy naná hogy igen van, akkor azonnal az adathalász oldalra továbbít bennünket a rosszindulatú link. Ami igazából a lényeg, hogy soha nem kell ezt az egész násztáncot végiglejteni akkor, **ha már az elején egyértelműen látszik, csalással van dolgunk, behúthatjuk a féket - egy átlagfelhasználónak ilyenekre tényleg kár tovább pocsékolnia az idejét, figyelmét, illetve kockáztatnia az esetleges jelszólopást.**

Emellett pedig az is egyre látványosabb, hogy egyre inkább emelkedik a mobilos QR kódokkal történő visszaélések, csalási kísérletek száma.

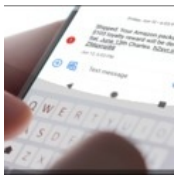
Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: csomag csalás átverés futárszolgálat adathalászat csomagküldő dpd qrcode quishing

Ajánlott bejegyzések:


Nő a QR-kódos visszaélések száma


Kár érte, kiváló ügynök volt...


Mai szavunk pedig: smishing



Csomagot kaptam life...



Ismét csomagunk érkezett - vagy mégsem?

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

1662

Matatás a robotporszívók agyában

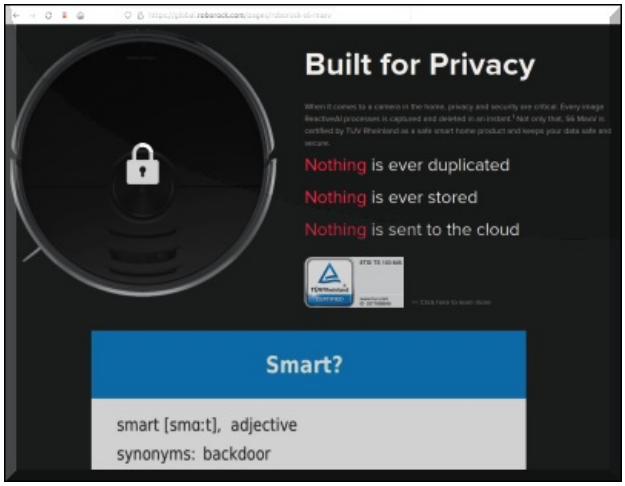
2023. augusztus 17. 08:26 - Csizmazia Darab István [Rambo]

Korábban sokszor esett már szó az egyre nagyobb számban használt IoT eszközök biztonságáról, ahol elképesztő hiányosságok sorakoznak: **clear textben utazó adatok, nincs hitelesítés, hiányzó brute force elleni védelem, bedrótozott hardcoded root passwordok használata, a titkosítás hiánya, törölhetetlen profilok, vagy a teljességgel hiányzó rendszeres hibajavító frissítések**. Ehhez jött aztán később a kamerás okosporszívók adatszivárgása, egy-két meredek sztorival.



Még a kifejezetten orvosi eszközök is hihetetlen sebezhetőségekkel buknak le, például az inzulin pumpás történet, ahol az etikus hacker kicsit belenézett a dolgokba, és azt látta, **távoli támadó hamis utasítást adhat inzulin injekció jogosulatlan beadására.**

De emlékezetes lehet az is, amikor **a korábbi amerikai alelnök, Dick Cheney - aki addigra már öt szívrohamot élt túl - 2013-ban az orvosok letiltották a pacemakerében a vezeték nélküli képességeket**, hogy ezzel kiküszöböljék egy esetleges gyilkossági kísérlet veszélyét.



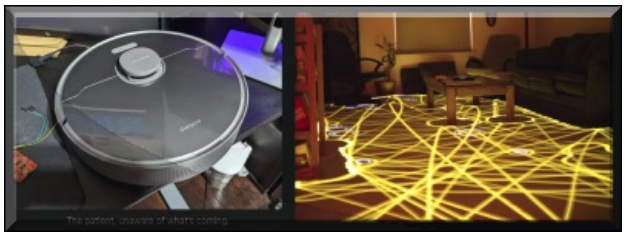
Ehhez képest a tömeggyártott általános használatú eszközöknél sokkal alacsonyabb a léc, és például a robotporszívók esetében is előjöttek nyugtalanító hírek. **2018-ban biztonsági szakértők olyan biztonsági hiányosságokat találtak a Dongguan Diqee 360 robotporszívóban**, melyek kihasználásával távoli támadók képesek átvenni a készülék irányítását, beleértve az éjjellátó kamera és a mikrofon vezérlését is.

Ezek az eszközök kamerájukkal 360 fokos szögben 30 kép/sec sebességgel képesek felvételeket készíteni, és ezek aztán ki is tudnak szivárogni. Ilyen intim fotók kikerülése - például hálószoba, fürdőszoba, WC belsőkből származó kényes képek kikerülése nagyon durva adatsértés, gyakorlatilag kémkedés a tulajdonos lakásában.



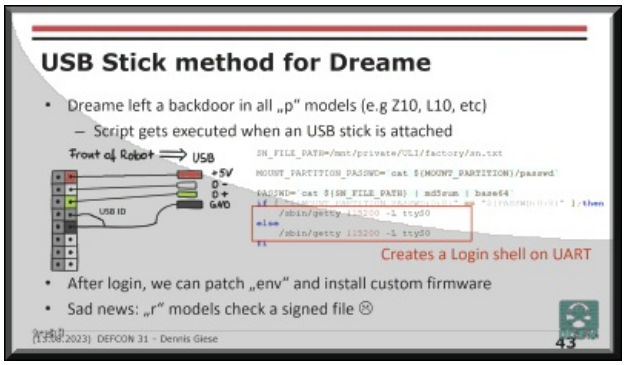
A WeliveSecurity friss posztja most egy DEFCON előadás kapcsán ismét elővette a témát, mivel L**as Vegasban Dennis Giese egy komplett előadást szentelt a problémának. Dennis igazi feketeöves fundamentalista, fanatikus hacker specialistája a területnek. Az előadás témája az volt, hogy hogyan akadályozhatjuk meg, hogy robotporszívó adatokat küldjön a gyártóknak vagy bárhová.**

Az egyik kulcskérdés például, hogy **amit a gyártó állít a leírásban - például hogy nem küld semmilyen adatot a felhőbe, nem készít rejtett biztonsági másolatokat, és hogy az eszközön lévő kamerák egyedüli célja, hogy elkerülje az ütközéseket - nos ezek a gyártói állítások nem feltétlenül egyeznek a valósággal.**



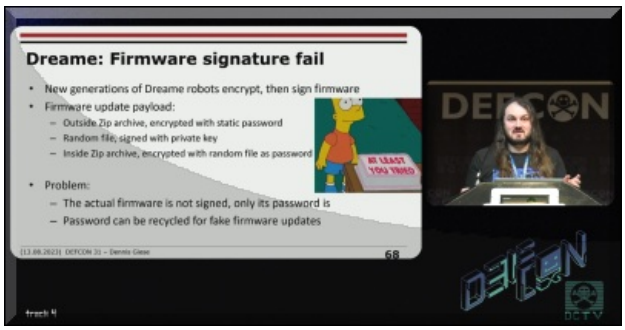
Van aztán a szómágia, ahol a kígyónyelvű marketingesek a megfogalmazással játszva kamerák helyett a dokumentációban "optikai érzékelőkről" írnak, pedig ez csak játék a szavakkal. Ahogy az az előadáson is bebizonyosodott, ezek a szófacsarás ellenére bizony az otthoni netünkhöz kapcsolódó képrögzítésre alkalmas kamerák.

És ahogy a hamis antivírusok esetében vagy az adathalász weboldalakon is sokszor mindenféle biztonsági plecsniket odahamisítanak: VeriSign, Európai Uniós tanúsítvány, TÜV, stb., itt is jellemző ugyanez, hogy ezek szerepeltetése csak kamu.



Emellett rengeteg sebezhetőség is ismert, ezekről egy méretes adatbázis is készült. Az IT biztonsági cégek általános jótanácsai - olyan készüléket válasszunk, amelyet megbízható gyártó kínál, legyen rendszeres biztonsági frissítés, stb. - elég az átlagfelhasználói szinten.

De ha valaki kész és képes is hackerkedni, akkor nekik ez jószerével nem elegendő. **És itt lép a képbe Dennis, aki éppen nekik kínál megoldást, és a szoftverbe belenyúlva rootolja a porszívókat. Itt nem egy gyártó adott modellje van kipécézve, hanem ha valaki haladócsoportos hardcore versenyzőként vissza akarja kapni az ilyen típusú eszköze feletti teljes irányítást, ennek a lehetséges módját mutatja be ez az előadás. (Kicsit mint OpenWRT-t varázsolni a routerünkre).**



Ha valakit bővebben is érdekel a téma, a mellékelt linken talál egy elég részletes leírást egy konkrét porszívó típus

élveboncolásáról, **emellett pedig magát a friss #31 DEFCON videót (sajnos néhol picit hullámzóan hanghibás, de végig feliratos) itt lehet végignézni.**

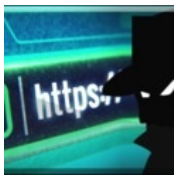
Megosztom tumblr. Tweet Pin it Tetszik 0

3 komment
Címkék: linux biztonság adatvédelem kukkolás kamera porszívó adatszivárgás iot rootolás welivesecurity welivesecurity.com robotporszívó

Ajánlott bejegyzések:


ChatGPT: hogyan használjuk a munkában?


Okoskodás: okos-e az okosjáték?



Böngészés - kockázatok és mellékhatások


10 alaplépés a biztonsághoz


Ransomware támadás a Nissan ellen

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

geegee · http://eszakonelunk.blog.hu 2023.08.18. 07:06:03

Robotporszívóba kamera?WTF?Eddig arról volt szó, hogy ha nekiütközik valaminek, mondjuk asztallábnak, akkor kicsit tolat, meg kormányoz, és megy tovább.
Na, nálam kapásból az lenne az első, hogy leragasztanám a kamerát, mint a notebookon is, a második meg hogy semmi esetre sem kapna wifit, netet.Hiszen minek is az neki?
Egyszer végig vezetném a lakáson, tanulja meg, oszt jól van, nem kell neki közben netezgetnie...
:D
Nagyon durva, amiket írsz, és simán neked hiszek, nem a köcsög gyártóknak.
Az egész IoT egy felesleges parasztvakítás, addig jó, amíg semmi nem valósul meg belőle.
Most őszintén, kinek hiányzik az, hogy a hüttőszekrény elkezdjen netezgetni, rendelgetni felügyelet nélkül??
Vagy hogy a lakásajtó zárját kinyithassák távolról?Hát enélkül már nem lehet meglenni?
Lassan tényleg megérik a világ a pusztulásra.

Válasz erre

geegee · http://eszakonelunk.blog.hu 2023.08.18. 07:12:26

Olyasmi ez, mint az autók keyless-go szolgáltatása, már amelyiknek ven.Hogy nem kell elővenni a kulcsot, elég ha ott van a zsebben, mert folymatosan, ismétlődően sugároz pulzálva.Csak éppen akkoris ezt teszi, amikor az ember otthon van és esze ágában sincs elmenni az autóval, de mondjuk éjszaka pár rohadék szívesen ellopná a kocsit, a szabadba kiküldött és ott általuk elfogott jellel.Hát, q jó, mit ne mondjak.Sose kéne ilyen szar, biztonság nélküli, gyári hátsókapus megoldás.Százszor inkább az acél kulcs, amit elő kell venni a zsebből és megnyomni.Az egész dolog egy válasz a soha fel nem tett kérdésre, nem több.
Ilyesmiről is vannak tesztek, cikkek a neten, konkrét típusokkal, a legdrágább lukszusgyártók tételesen benne vannak nyakig.

Válasz erre

geegee · http://eszakonelunk.blog.hu 2023.08.18. 07:13:36

jav: vAn

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

4219

Üdvözöljük, csomagja kézbesítésre vár

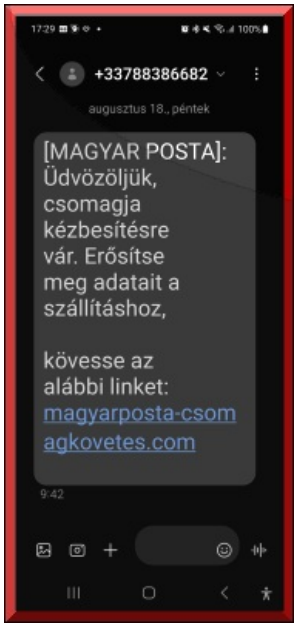
2023. augusztus 22. 09:47 - Csizmazia Darab István [Rambo]

Ha valami még emlékszik a 2021. márciusi FedEx nevével visszaélő átverésre, akkor jól érzékelhető, hogy azóta az ilyen jellegű csalások garmadája zúdul ránk. Most ismét érkezett egy gyanús SMS, amely ezúttal a Magyar Posta nevében próbálkozik.



Intő jelek idejében való felismerése - ezt sulykolják rendszerint, ha a megelőzést akarjuk a fókuszba helyezni.

Eszerint a gyenge helyesírás, a magyartalan, nyersfordításra utaló fogalmazás, a hiteles linkre még csak nem is hasonlító URL cím, külföldi telefonszámról érkező hivatalos üzenet, sürgetés-fenyegetés kombó - nagyjából ezek a leggyakoribb tipikus elemek.

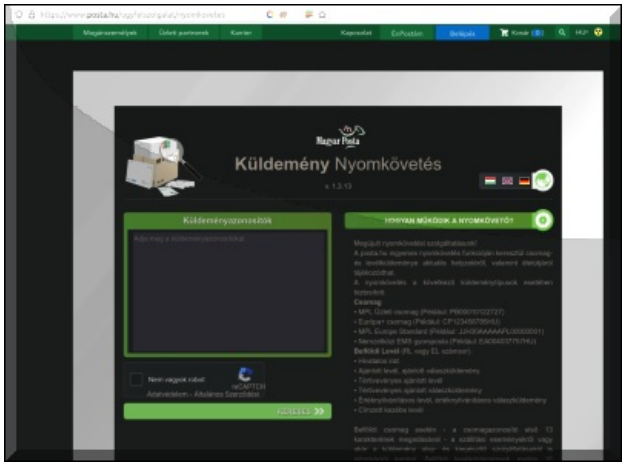


A mostani a +33 előhívószámmal rendelkező **franciaországi telefonszámról érkező SMS-ben a helyesírásra, ékezethelyességre és a mellékelt link kinézetére is a korábbinál nagyobb gondot fordítottak a csalók.**

Aki rendszeres igénybe veszi a Magyar Posta online szolgáltatásait, regisztrált felhasználó vagy akár ügyfélkapus regisztrációs Én-postám kártyája is van, az biztosan nem nézi be, hogy **mi is a hivatalos webhely: www.posta.hu.**

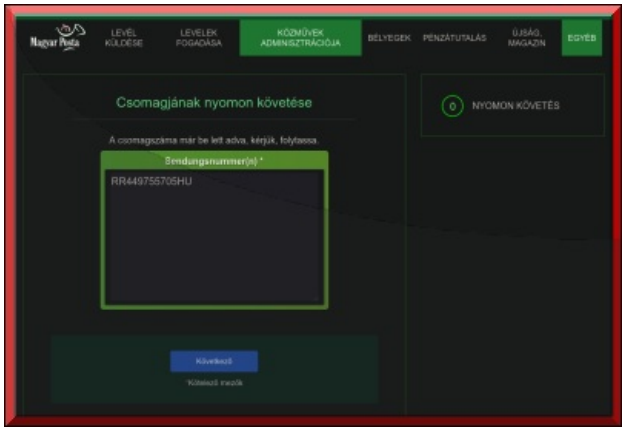


Ehhez képest a "magyarposta-csomagkovetes.com" URL nem igazán látszik hitelesnek, **a whois rekord szerint pedig az is látható, hogy ezt mindössze pár napja regisztrálták be és jelenleg egy franciaországi IP címre mutat.**



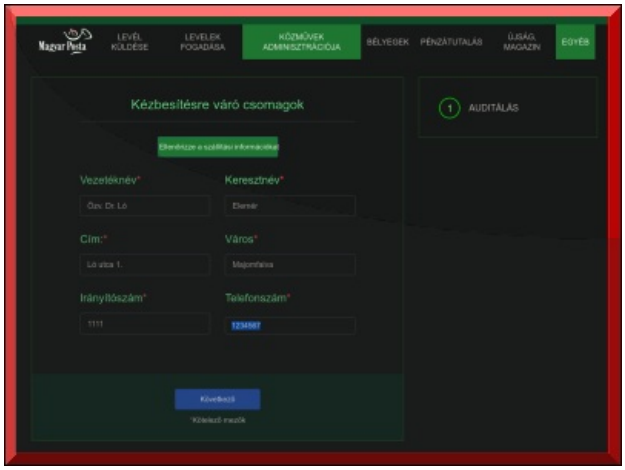
Megint csak érdemes megjegyezni, hogy a hivatalos csomagkövető weboldal címe: https://www.posta.hu/ugyfelszolgalat/nyomkovetes

Itt a személyes adatok megadása nélkül, egy XXXX999999999999 kinézetű csomagkóddal van lehetőségünk lekérdezni az érkező küldeményünk pillanatnyi állapotát.



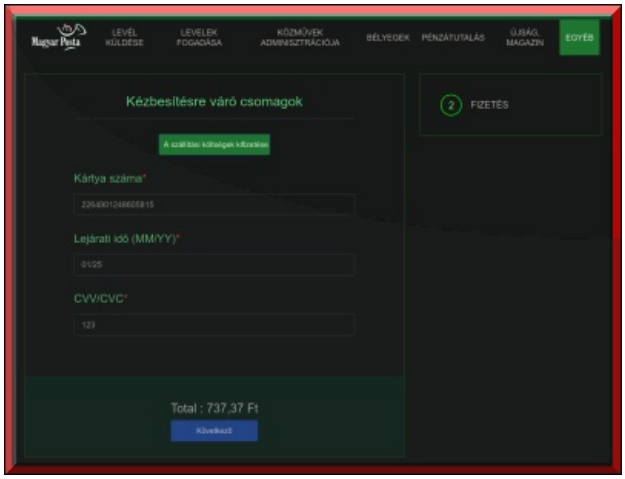
Ezzel szemben a kamu oldal először a személyes adatainkat kéri be, úgy mint név, lakcím, telefonszám, majd jön a bankkártyánkon szereplő név, kártyaszám, lejárati idő és a háromjegyű CVV biztonsági kód.

A bekért alacsony 737 forintos összeg inkább a csali szerepét tölti be, hogy az áldozat úgy érezze, ez egy piti összeg, ezen nem érdemes sokat hezitálni. **Remélhetőleg a személyes és banki adatok begépelése előtt azért már sokaknál leesik a tantusz, és senki nem sétál bele a csalásba, hogy utána rohamtempóban le kelljen majd tiltania a bankkártyáját.**



Való igaz, hogy már valóban sok ilyen példát szerepeltettünk itt blogban, de mivel ez itt egy hibátlan magyar nyelvű volt és egy szépnek látszó webcím is szerepelt benne, észre kell venni, hogy **valószínűleg a ChatGPT segítsége is benne lehet a nyelvtanilag helyes adathalász üzenetben.**

Félő, hogy a jövőben egyre jobb minőségű átverési kísérleteket kapunk majd még ennél is nagyobb számban.



Emiatt mindenki, akinek a családjában van olyan idős ember, akinek meg tudja mutatni az ilyen kísérleteket, és persze mellette az intő jeleket is, az tegye meg, figyelmeztesse, mert valószínűleg ők lehetnek a legsérülékenyebb célcsoportja az ilyen aljas próbálkozásoknak.

Megosztom tumblr. Tweet Pin it Tetszik 0

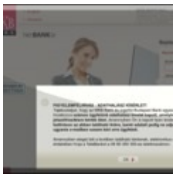
2 komment
Címkék: magyar posta csalás átverés phishing adathalászat squishing

Ajánlott bejegyzések:


2023. első csalásai



Csomagot kaptam life...


MKB adathalászat szigonnyal, horoggal, hálóval


Csomagja kézbesítésre vár! Vagy mégsem?


Magyar Posta csomagunk jött - vagy mégsem?

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Mesterséges Geci 2023.08.25. 19:45:54

Félek, ez nem chatgpt, jó eséllyel nem is AI, inkább valami magyarul jól beszélő gazember műve. Más AI-t nem próbáltam, de a chatgpt annyira furcsán beszél magyarul, hogy azt észre lehet venni. Facebookon látok egyre több olyan, látszólag ártalmatlan posztot, amiben magyarul kér valaki segítséget, de a profilja, a szóhasználata gyanús. Ezek többsége valószínűleg valami chatgpt jellegű eszközt használhat.

Válasz erre

Gugli666 2023.08.25. 20:33:37

"a whois rekord szerint pedig az is látható, hogy ezt a címet mindössze pár napja regisztrálták be egy franciaországi IP címről."

Az honnan derül ki, hogy franciaországi IP-ről regisztrálták be a domain-t? Ilyen info-t a WHOIS nem tartalmaz. Csak annyi szerepel benne, hogy jelenleg egy franciaországi IP címre mutat a domain.

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

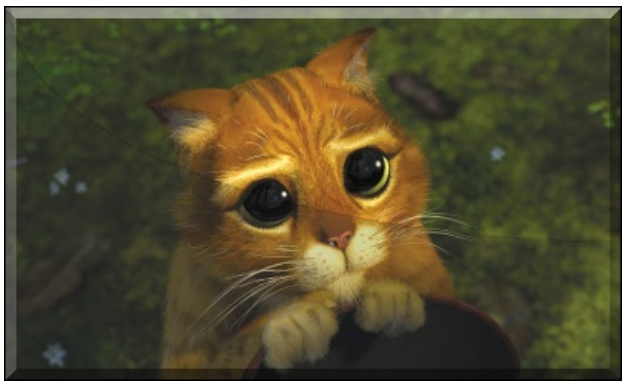
Belépés
Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

Bocsánat! Elnézést!

2023. augusztus 24. 10:27 - Csizmazia Darab István [Rambo]

A dán CloudNordic és AzeroCloud tárhelyszolgáltatót üzemeltető cég augusztus 18-án, azaz múlt hét pénteken **zsarolóvírus támadást szenvedett el, amelynek következtében sajnálják, de az ügyféladatok totálisan elvesztek**. A tárhelyszolgáltató arra kényszerült, hogy leállítsa az összes futó rendszerét, beleértve a weboldalait, a levelezést, valamint az ügyfelek webhelyeit.



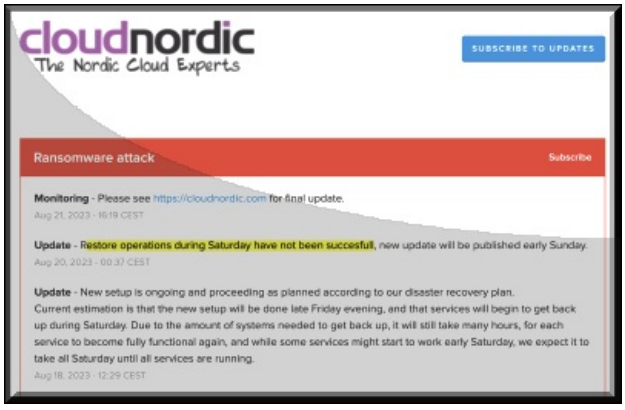
A hivatalos közleményben azt írják, **a CloudNordic teljességgel megbénult, és az ügyfeleik tekintsék minden adatukat elveszettnek.** A helyreállítás rendkívüli nehézségekbe ütközött, mivel a cég informatikai csapatai mindössze csak néhány szervert tudtak visszaállítani.

A bejelentésben az is szerepel, hogy semmiképpen nem fognak váltságdíjat fizetni a bűnözőknek, és az esetről már értesítették a hatóságokat.



A hogyan történt kérdésre látszólag az lehet a válasz, hogy **a szerverek egyik adatközpontból a másikba költöztetése során következhetett be az incidens, melynél a támadók a belső hálózaton keresztül egyszerre fértek hozzá a központi adminisztrációs rendszerekhez és a biztonsági mentési rendszerekhez is.**

Ez utóbbi tartalmazott többek közt minden tárhely adatot, replikációs és a másodlagos biztonsági mentési rendszert. Mivel a támadóknak sikerült titkosítaniuk az összes szerver lemezét, így minden összeomlott.



"Mélyen sajnáljuk a helyzetet, és köszönjük a sok hűséges ügyfelünknek, akik az évek során velünk voltak." Hát nem ezt a mondatot szeretné az ember hallani, ha előfizet valamilyen netes szolgáltatásra.

Emellett azt a kijelentésüket, miszerint nem láttak bizonyítékot adatszivárgásra, adatlopásra - is érdemes lehet fenntartással fogadni, hiszen magát a behatolást és az incidenst sem vették észre kellő időben, és a "nem

láttunk bizonyítékot" valamint a "nem történhetett ilyen" egymással nem ekvivalens állítások.



A dán szolgáltató most **az adattartalom nélküli alaprendszerek visszaállításán dolgozik, de egyrészt még ez is rengeteg időbe telik nekik, másrészt az sem megnyugtató, hogy ilyenkor a ransomware újrafertőzés lehetősége az esemény alapos kivizsgálása nélkül komoly kockázati tényező lehet. Az incidens roppant durván hangzik, hiszen azt mutatja, hogy sem a védelem nem működött megfelelően, hiányozhatott a többszörös és fizikailag leválasztott, máshol tárolt biztonsági mentések gyakorlata, valamint a mentésekből való helyreállítás terv - már ha egyáltalán létezett ilyesmi - sem volt letesztelve.**

A felhő szlogen csak egy üres bullshit, ha nincs mögötte átgondolt, megtervezett, alapos biztonsági megoldások garmada és szakértő IT biztonsági csapat.



A tárhelyszolgáltatók célzott támadása a ransomware-bandák által egy kedvelt taktika, mivel egyrészt egyetlen akcióval nagyszabású károkat tudnak okozni, másrészt pedig a szolgáltatókon nagy a nyomás, hogy váltságdíjat fizessenek működésük helyreállítása érdekében, hogy ezzel elkerüljék az adataikat elvesztő ügyfelek pereit.

A mostani incidensben **érintett felhasználókat már csak az mentheti meg, ha legalább ők maguk rendelkeztek valamilyen saját biztonsági mentéssel.** Úgy tűnik, érdemes lehet megfogadni a pórul járt áldozatoknak Mick Jagger tanácsát, miszerint Get Off Of My Cloud, azaz szállj le a felhőmről, és talán jobb lenne egy másik biztonságosabbra átszállni.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: leállás hiánya mentés adatvesztés ransomware zsarolóvírus cloudnordic azerocloud

Ajánlott bejegyzések:



Az elveszett levelezés



Gyorsabban, magasabbra, erősebben!


Nem csitulnak a kórházak elleni támadások


Ransomware támadás a Nissan ellen



8 kórház, 30 klinika, 2.5 millió betegadat

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

29720

OTP kártyáját ideiglenesen megterheltük

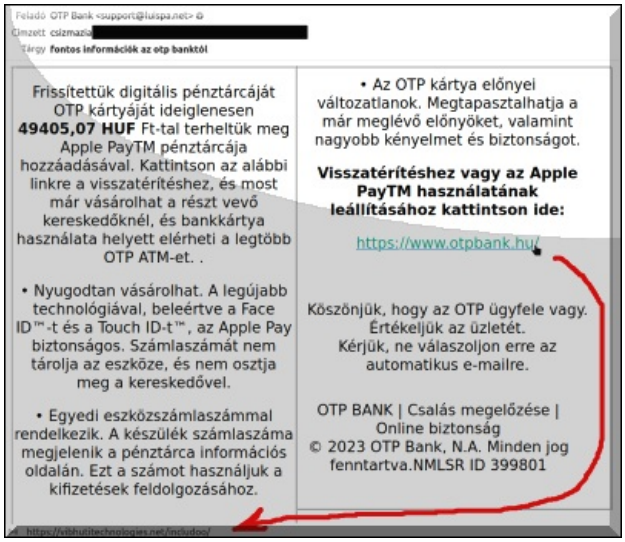
2023. augusztus 29. 11:11 - Csizmazia Darab István [Rambo]

Nem marad ki a támadási hullámból az OTP sem, ezúttal egy "*fontos információk az otp banktól*" tárgysorú üzenet esett be a postafiókunkba - és vélhetően nem csak egyedül nekünk.



Ideiglenesen megterhelték a kártyánkat 49 ezer forinttal - állítja a levél, az Apple PayTM pénztárca hozzáadása miatt. Pedig ezt nem igényeltük, nem kértük, nem írtunk alá erről szerződést, **az üzenet most mégis erre hivatkozva kínál linket az állítólagos visszatérítéshez.**

Bár mindez csak akkor lenne használható, ha a felhasználónak iPhone telefonja van, Androidon nem ketyeg az Apple Pay, de kétségbeesni azért nem nagyon kell, mert adathalász átverés ez a javából.


Feladó OTP Bank <support@luispa.net>
Címzett csizmazia[redacted]
Tárgy fontos információk az otp banktól

Frissítettük digitális pénztárcáját OTP kártyáját ideiglenesen **49405,07 HUF** Ft-tal terheltük meg Apple PayTM pénztárcája hozzáadásával. Kattintson az alábbi linkre a visszatérítéshez, és most már vásárolhat a részt vevő kereskedőknél, és bankkártya használata helyett elérheti a legtöbb OTP ATM-et. .

• Nyugodtan vásárolhat. A legújabb technológiával, beleértve a Face ID™-t és a Touch ID-t™, az Apple Pay biztonságos. Számlaszámát nem tárolja az eszköze, és nem osztja meg a kereskedővel.

• Egyedi eszközszámlaszámmal rendelkezik. A készülék számlaszáma megjelenik a pénztárca információs oldalán. Ezt a számot használjuk a kifizetések feldolgozásához.

• Az OTP kártya előnyei változatlanok. Megtapasztalhatja a már meglévő előnyöket, valamint nagyobb kényelmet és biztonságot.

Visszatérítéshez vagy az Apple PayTM használatának leállításához kattintson ide:

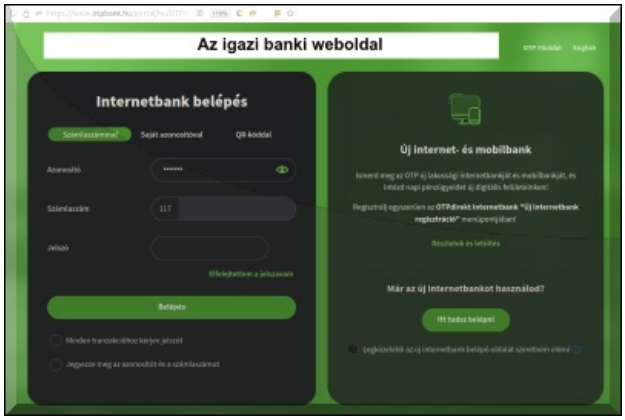
https://www.otpbank.hu/

Köszönjük, hogy az OTP ügyfele vagy. Értékeljük az üzletét. Kérjük, ne válaszoljon erre az automatikus e-mailre.

OTP BANK | Csalás megelőzése | Online biztonság
© 2023 OTP Bank, N.A. Minden jog fenntartva.NMLSR ID 399801

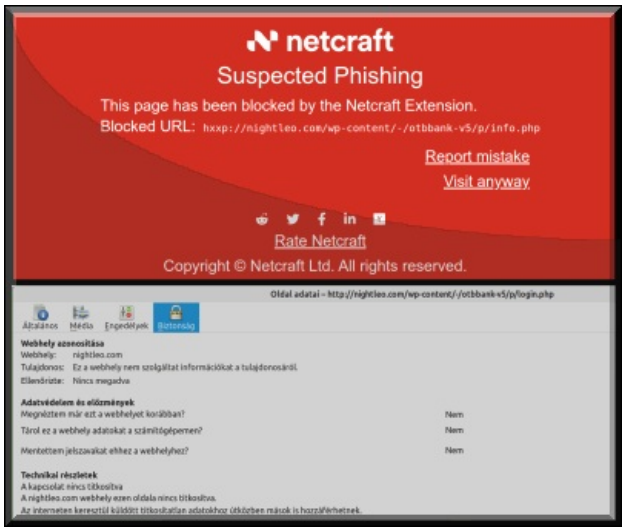
Mukinyúl feladó küldte: "support KUKAC luispa PONT net", az e-mail trace alapján **Michiganből érkezett a hű de hivatalos levél**. Aztán van itt **keverve tegezős-magázós magyartalan szöveg is**: "*Köszönjük, hogy az OTP ügyfele vagy. Értékeljük az üzletét. Kérjük, ne válaszoljon erre az automatikus e-mailre.*"

És persze az egérmutatót a link fölé mozgatva (hover) is üvölt, hogy a "vibhutitechnologies PONT net PER includoo" link még csak köszönőviszonyban sincs az Országos Takarékpénztár és Kereskedelmi Bank Nyrt. hivatalos weboldalával.



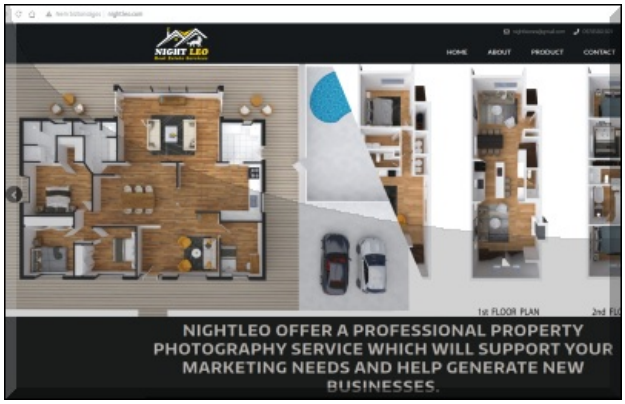
A link szövege azért jópofa: "*Visszatérítéshez vagy az Apple PayTM használatának leállításához kattintson ide*" Igazi 22-es csapdája: ha egyértek, azért, ha nem értek egyet, akkor azért.

A kattintás után tegnap még akadály nélkül jutottunk a csalók hamis banki hasonmás oldalára, ma reggel viszont már a Netcraft figyelmeztetést ignorálva lehet eljutni az adathalász webhelyre.

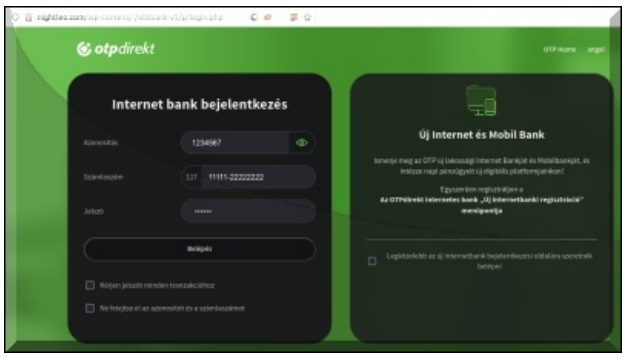


Ennek címe a menetközbeni átirányítás után: **"nighleo PONT com PER wp-content PER - PER otbbank-v5 PER p PER login.php", tehát ismét egy Wordpresses sebezhetőség kihasználásának lehetünk tanúi.**

És nem csak mukinyulas ez a szedett-vedett webcím, de még egy árva kamu https tanúsítványra sem futotta a mester bűnözőknek.

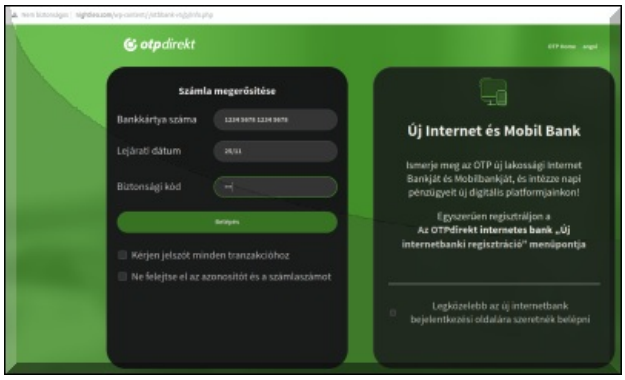


A feltört hely egyébként eredetileg egy ingatlanos tematikájú webcím, akik valószínűleg észre sem vették, hogy már nem az övék az oldal.



Ebben az URL sorban a "otbbank" a legviccesebb, még a megfelelő betűket sem sikerült kiválasztani az egypálcás mutatványukhoz. Az adathalász oldal megkísérli bekérni az OTP banki belépési adatainkat: azonosító, számlaszám és jelszó.

Ilyesmiket akkor sem érdemes begépelni, ha egy webáruház még egy SSL kapcsolatra is képtelen, de itt **a megtévesztésre szánt úgynevezett "hasonmás" webhely még arra is képtelen, hogy a hivatalos weboldalt lekopírozza, például "azonosító" helyett "azonosítást" kér be.**



A fenti mezők kitöltése után **nem elégszik meg ezen adatokkal, mint egy hagyományos banki beléptető, hanem rákérdez még a bankkártya adatainkra is, ha már ilyen szépen összejöttünk: bankkártya száma, lejárati ideje és tadaaaaam, még a 3 jegyű CVC biztonsági kódot is elkéri**, a számla állítólagos megerősítéséhez.



De nem fogyott ki a szusz a kihallgató tisztünkből, búcsúzásképpen még az e-mail címünket is tudni akarja, igaz a kutya oltási bizonyítványának számát ezek után már nem kérdezi meg.

Szóval itt azért vastagon figyelmetlennek kell lenni ahhoz, hogy egy technikailag ilyen szinvonaltalan csalásba valaki mégis belesétáljon, senkiháziak kezében már az adathalászat is. Reméljük, hogy mostanra mindenki inkább már csak szórakozni jött ide, semmint megijedni. A poszt megírásának végére a fenti oldalakat már le is lőtték.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: bank wordpress otp sebezhetőség adathalászat adatlopás sérülékenység pebkac

Ajánlott bejegyzések:



Banki meló



K&H mobilbank biztonsági szolgáltatás - vagy mégsem?



Identitás lopás: nem függ az életkortól



Adathalászat menni booking.com



Újabb súlyos WordPress hiba

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

310

Képregény a ransomware támadásokról

2023. augusztus 31. 10:22 - Csizmazia Darab István [Rambo]

Ha a statisztikákat nézzük, vagy a hírek főcímeit, **egyre több és nagyobb kaliberű zsarolóvírus incidensnek lehetünk tanúi**. Legutóbb például Kanadában a montreali villamosművek ellen indított a LockBit banda támadást, ahol a város elektromos infrastruktúráját kezelő szervezet megtagadta a váltságdíj kifizetést, ezután a bűnözők bosszúból kitették a netre az ellopott adatokat.



Allan Liska, aki a Recorded Future cég kiberbiztonsági cég elemzője, új projektbe vágott bele. Egy 1949-ben eredetileg rádiós sorozatként indult **magándetektíves történetet dolgoz most át modern korunkban játszódó képregénnyé.**

Bár a korabeli rádiós sorozat igen népszerű volt, ám végül 1962-ben mégis véget értek Johnny Dollar magánnyomozó maffiózók, gyilkosok és csalók üldözésével teli kalandjai.



Ezúttal azonban Liska - aki maga is hatalmas képregény rajongó - egy új noir hangulatú képregényként akarja Johnnyt feltámasztani, és ehhez a közösségi finanszírozást választotta. A modern számítógépes korszakban zajló bűnbandák által elkövetett zsarolóvírus-bűncselekmények kerülnek a középpontba, ahol modern eszközökkel zajlanak majd a nyomozások is, és ez az ötlet annyira megtetszett a közönségnek, hogy **a Kickstarteren jelenleg a gyűjtés a tervezett 3500 helyett 9231 dollárnál tart.**

Az ötlet kidolgozása után Liska toborzott egy író- és illusztrátorcsapatot, akik segítenek életre kelteni a tervet.



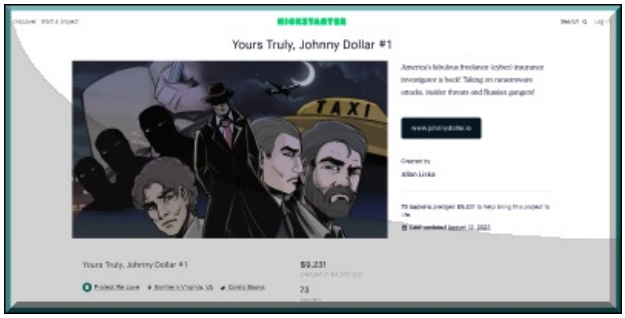
A tervezett történetekben J**ohnny Dollar napjai majd azzal telnek, hogy a nyomokat követve megállapítsa, hogyan kerültek be a támadók a hálózatba, és megtalálja, milyen eszközöket használtak bűncselekmények végrehajtásához.**

Találkozik az áldozatokkal, felderít, elemez, hatalmas legyőzhetetlennek látszó bűnszervezetekkel küzd, néha túl nagy fába vágja a fejszét - és Liska úgy érzi, ez néha éppen ugyanígy történik a saját kiberbiztonságban végzett munkájában is.



Ma a ransomware egy több milliárd dolláros profitot jelentő bűnözői vállalkozás, amelyben a rosszindulatú hackerek, programfejlesztők, nemzetközi összetételű digitális bűnözők hálózata követ el, és ezek a bűncselekmények **ma már napi szintű fennakadásokat és hatalmas pénzügyi károkat okoznak** a különféle magán vállalkozásoknak és hivatalos szervezeteknek.

Egy tavaszi statisztikából világosan látszik, hogy ransomware csoportok egyre inkább igyekeznek a kritikus infrastruktúrák és jelentős ipari szereplők ellen célzottan fellépni. Az általuk leginkább favorizált szektorok közül **az ipari ágazat vezet, beleértve az ipari termelő, gép- és szerszám gyártós és kereskedelmi, logisztikai, tervezői, építőipari, járműgyártói szereplőket, de sokszor kórházak, állami hivatalok, postai és IT szolgáltatói szervezetek** is kárt szenvednek.



A tervek szerint Johnny új története négy részből áll majd, a szeptemberre tervezett első megjelenésről és a projekt haladásáról a https://www.johnnydollar.io/ hivatalos weboldalon lehet majd bővebben tájékozódni.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: képregény johnny dollar allan ransomware liska kickstarter zsarolóvírus

Ajánlott bejegyzések:



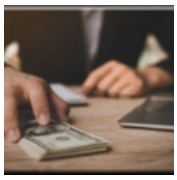
[Ransomware támadás a Nissan ellen]



[8 kórház, 30 klinika, 2.5 millió betegadat]



[LockBit piacgazdaság és tervgazdálkodás]



[Megváltás-e a váltságdíj?]



[Ransomware a One Motelben]

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

915

Ami majdnem az, az nem az

2023. szeptember 05. 10:39 - Csizmazia Darab István [Rambo]

Trójai a neve azoknak a kártékony kódoknak, amelyek hasznos, gyakran jól ismert programként tüntetik fel magukat, és csalárd módon ráveszik a felhasználót a letöltésükre, futtatásukra. **Az eredeti funkción felül azonban titokban rosszindulatú tevékenységeket hajtanak végre a háttérben, ez leggyakrabban kémkedés, adatlopás.**



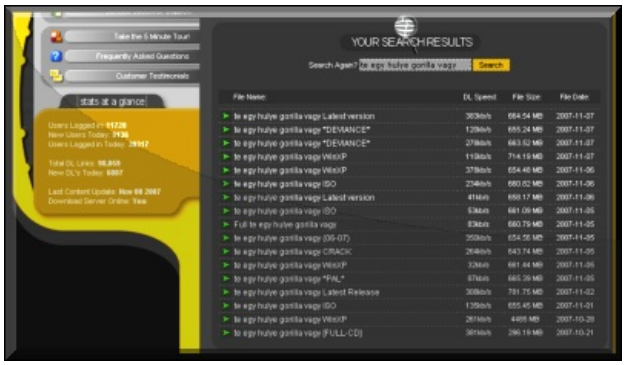
Rengeteg alkalommal írtunk már itt a blogban is ilyenekről, de azért érdemes lehet néhány hírhedtebb esetet előszedni az emlékezet bugyraiból. Jó tíz évvel ezelőtt, még a megboldogult UPC idején létezett egy Távrögzítő nevű alkalmazás, amellyel a settop box segítségével TV műsorokat lehetett beprogramozni, és távollétünkben VHS kazettára rögzíteni.

Aztán egyszer csak megjelent egy UPC Távrögzítő nevű mobil app iPhone és Android platformra, amiről csak sokkal később derült ki, hogy ezt nem a UPC készítette, nem is tudtak róla, mégis sokan letöltötték és valószínűleg ellopta a UPC loginokat. A lelepleződés után aztán törölték az appot az áruházak kínálatából.



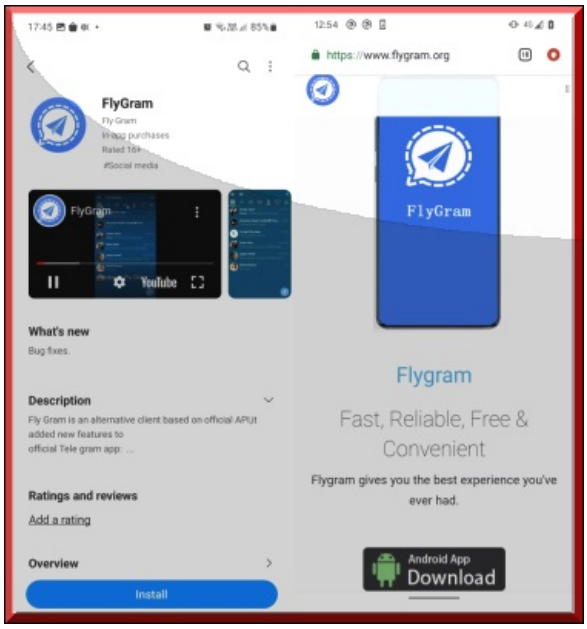
Érdemes a letöltéseknél óvatosnak lenni, hiszen sokszor még meg sem jelent operációs rendszer is felkínálnak, ahogy ezt például Kínában lehetett látni jóval a Windows 7 hivatalos piacra kerülése előtt. **De sikeres átverős csalinak számít az is, ha bármilyen jól ismert szoftvert észrevétlenül összecsomagolnak kártevővel, ahogy azt például orosz bűnözők tették 2015-ben a TrueCrypt lemeztitkosító programjával.**

Itt a letöltési csomagokba egy Win32/Potao nevű kártevő családot rejtettek, és ennek segítségével a Krím félsziget megszállása után egy évvel ukrán tisztviselők és újságírók után kémkedtek.



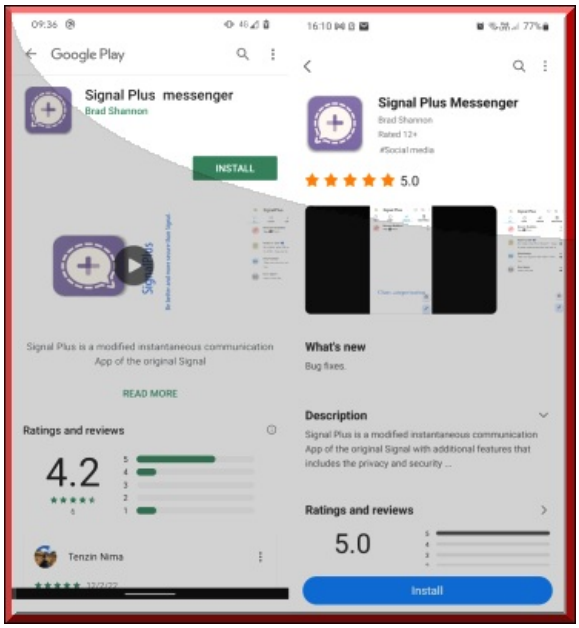
Letölteni persze elvileg bármit lehet, sőt akár nem létező dolgokra is kaphatunk bőven "találatot" és kétes letöltési linkeket.

Ehhez elég, ha a keresési mezőbe beírjunk bármilyen kitalált kreténséget, például azt, hogy "Te egy hülye gorilla vagy", és máris ontják a letöltő oldalak a linket a Full release, az ISO, a feltört crackelt, a keygen-es és FULL-CD változathoz is.



Mai történetünkre kanyarodva itt is jól ismert programok nevével éltek vissza ismeretlenek, akik **Android felhasználókat céloztak meg hamis Signal és Telegram appok segítségével. Az ESET kutatói egy Kínához köthető APT csoportnak tulajdonítja a Google Play áruházban is egy ideig elérhető Signal Plus Messenger és FlyGram nevű trójai alkalmazásokat.**

Ezeknél az eseteknél ha valaki lépre ment, a távoli támadók kémkedhettek a felhasználók után, minden telefonon tárolt adatukhoz hozzáférhettek.



A FlyGram kártevő a klasszikus adatlopás mellett a hivatalos eredeti Telegram biztonsági másolataihoz is hozzáfért, de a Signal Plus Messenger is rejtegetett trükköt, ott az áldozatok valós Signal kommunikációja után kémkedtek a valódi profil összelinkelésével. Az elkövetők a nagyobb hihetőség kedvéért még honlapot is kreáltak a hamis appoknak.

A kínai szál amiatt is látszik valószínűnek, mert a kártékony FlyGram alkalmazás linkjét egy ujgur Telegram csoportban is megosztották, és ez a célzott terjesztés összhangban van a BadBazaar nevezetű kémprogram korábbi felhasználásával.

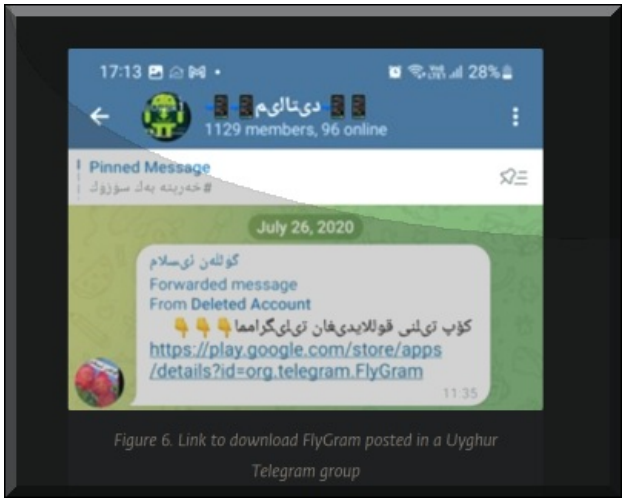


Figure 6. Link to download FlyGram posted in a Uyghur Telegram group

Ha valaki esetleg telepítette volna bármelyiket, érdemes haladéktalanul törölnie, az igazi Signal esetében pedig Beállítások -> Társított eszközöknél törölni az esetlegesen bekerült új eszközöket. Android esetében már a vírusirtók riasztanak is rá, illetve az appokat a hivatalos piacterekről is már törölték azóta. **A FlyGram 14 ezer, míg a Signal Plus Messenger 5 ezer körüli letöltés számot produkált addigra.**

Arról, hogy hogyan szúrjunk ki hamis appokat, már írtunk korábban egy a telepítés előtti gyanús jeleket csokorba gyűjtő posztot. És ehhez ide kívánkozik a mondás: **"A bölcsesség kilenc tized része az, hogy idejében van bölcs."**

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: mobil kína signal trójai android app kémkedés kártevő kémprogram titkosított welivesecurity.com telegram

Ajánlott bejegyzések:


VPN appok Androidra vagy mégsem?


Xenomorph kalandjai GooglePlay országban


Igazgató-e vagy?


Hogyan ne jussunk 10-ről 11-re?


Támadás 1,2,3 - Industroyer újratöltve

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

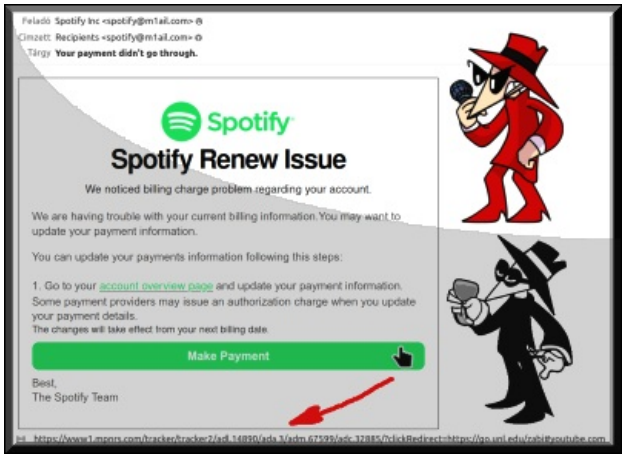
Belépés
Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

Spotify megújítási probléma - vagy mégsem?

2023. szeptember 11. 11:02 - Csizmazia Darab István [Rambo]

Nem csak az MVM, a Posta, bármelyik bank vagy akármelyik csomagküldő nevében küldhetnek nekünk adathalász levelet, hanem **a különféle internetes szolgáltatók nevével is gyakran élnek vissza bűnözők. Most éppen a Spotify előfizunk járt le. Vagy mégsem**. Vagy egyáltalán nem is voltunk ott előfizetők. Vagy most mi van?



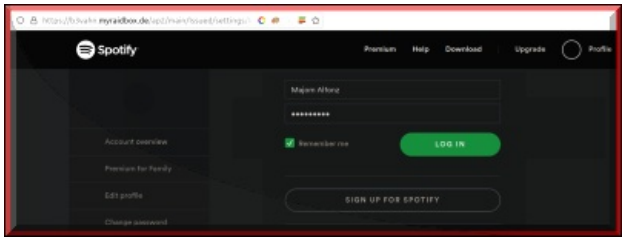
Soha végetnemérős sorozatunkat egy zenei platform angol nyelvű levelével folytatjuk, melyben jelzik felénk, n**em sikerült megújítani a mostanában lejáró Spotify előfizetésünket valamilyen lejárt bankkártya, számlán lévő túl kevés összeg vagy valamilyen egyéb hasonló rejtélyes terhelési probléma miatt.** Így mi mást is javasolhatna nekünk a csalók levele, mint hamarjában **frissíteni a fizetési adatainkat a mellékelt linkre kattintva.**

Ellenkező esetben oda a dalok lejátszása tetszőleges sorrendben, ó jaj, no meg azon nyomban elöntenek minket a reklámok, neeeee, és mostantól még a letöltéseinknek is fuccs lehet...



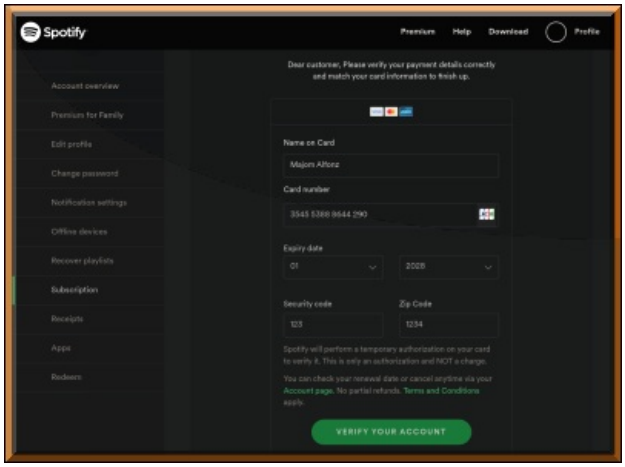
Mielőtt valaki esetleg a kelleténél jobban megijedne, **érdemes a szokásos gyanús jelek leltáron végigszaladni. A feladó nagyon kamu:** "spotify KUKAC m1ail PONT com". Rátracelve látjuk benne az oroszországi, szentpétervári biteket is, ellentétben a hivatalos igazi címmel, ami akármi KUKAC spotify.com végződéssel rendelkezik.

Roppant kevés hihető okot látni arra, Oroszországon keresztül kellene ilyen legitim értesítést kapjunk a svédországi Spotify csapatától, pláne ilyen különleges katonai művelettel terhelt időszakban.



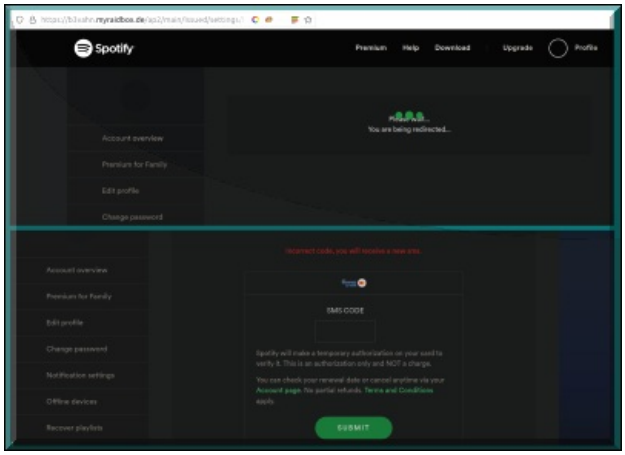
És akkor jöjjön a kattintható link, amit látva szintén nem igazán érdemes azt lekattintani: "www1.mpnrs.com/tracker/tracker2/blabla...." vagy "go.unl.edu/blabla..". **Nem igazán életszerű ezeket az egyetlen hiteles, korrekt és egységes, tévedést kizáró hivatalos weboldalnak érzékelni.**

A hecc kedvéért persze írogassunk bele mindenféle válogatott marhaságot - és ugye arról már nem is kell beszélni, hogy **az igazi belépéshez remélhetőleg már mindenkinél tartozik egy kétfaktoros autentikáció is, ami a név-jelszó kiszivárgása esetén is egy plusz extra védelmi réteget jelent.**



Belapátoltuk minden szemetet a személyes adatok mezőkbe, ami először eszünkbe jutott, **és ezzel máris a banki adatok megadásához kerültünk, ahol a kártyaszám, az azon szereplő név, lejárati év és hónap, és a 3 jegyű biztonsági CVC kód iránt érdeklődnek tőlünk nagy tisztelettel.**

Ha valamilyen igazinak látszó kártyaszámot gépelünk be (pl. Fake Credit Card Number Generator Online), akkor **némi gondolkodás után még felugrik egy hamis SMS megerősítő kód bekérő ablak is, hátha szerencsénk lesz.**



Mivel láthatólag ordenáré fals adatok voltak megadva, hamar meg is jön hozzá a hibaüzenetes ablak: most ezekkel egész pontosan nulla forintot tudtak kasszírozni az elkövetők.

A feltört aloldalakon futó adathalász próbálkozás egyfelől a Spotify accountot, másfelől a banki adatokat igyekszik megszerezni azoktól, akik nem nézik a feladót, nem figyelik a mellékelt link címét, bejelentkezéskor nem ellenőrzik az URL címet, mindig mindenre gondolkodás nélkül kattintanak, és roppant szívesen gépelgetik be a saját bankkártya adataikat unga-bunga típusú szedett-vedett weboldalakon. **Legyen a zene mindenkié!**

Megosztom tumblr. Tweet Pin it B Tetszik 0

1 komment
Címkék: spam vagy e-mail csalás átverés phishing adathalászat mégsem spotify

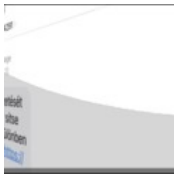
Ajánlott bejegyzések:



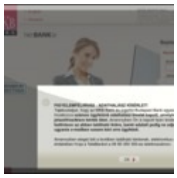
[Netflix: lejárt a tagságunk. Vagy mégsem?]



[Tagsági kérdések - vagy mégsem?]



[2023. első csalásai]



[MKB adathalászat szigonnyal, horoggal, hálóval]



[Adathalászat menni booking.com]

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Head Honcho 2023.09.17. 13:57:29

És vélhetőleg így is kaszálnak a világtalanok hadán.

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

873

Az elveszett levelezés

2023. szeptember 19. 08:03 - Csizmazia Darab István [Rambo]

Tavaly júniusban **az Oroszországhoz köthető Conti és Hive banda indított zsarolóvírus támadást Costa Rica ellen, ahol számos állami intézmény kényszerült hosszabb ideig leállni**. Többek közt a pénzügyminisztérium hálózatát, az adó- és vámhivatalokat, a kereskedelmi központokat, a közműveket illetve az egészségügyi intézményeket bénította meg az akkori kiterjedt incidens.



Tavaly februárban is volt egy emlékezetes támadás, akkor a kaliforniai Oakland lett célpont, ahol aztán a helyzet komolyságát az is mutatta, hogy az adóhivatal, az önkormányzat, és a bíróságok leállása miatt szükségállapot kihirdetése vált szükségessé.

A mostani friss incidens pedig Sri Lanka kormányát érte, ahol a javítatlan Exchange Server program a hivatalos levelezőrendszer leállását okozta. A kormány a Microsoft Exchange 2013-at használta, ennek pedig idén április 11-én leállt a támogatása. A pisztácia elfogyott, mentés pedig nem is volt.


Daryna Antoniuk
September 11th, 2023

Briefs | Government | Cybercrime | Technology

Sri Lankan government loses months of data following ransomware attack

Sri Lanka's government email network was hit by a ransomware attack that wiped months of data from thousands of email accounts, including ones belonging to top government officials, authorities confirmed on Monday.

The attack, which started at the end of August, affected nearly 5,000 email addresses using the gov.lk email domain. The victims include Sri Lanka's council of ministers which forms the central government of the country.

The targeted system, Lanka Government Cloud (LGC), was encrypted along with backups of the system. Although officials were able to restore LGC within 12 hours of the attack, they didn't have backups from May 17 to August 26, so all affected accounts lost data from that period, according to Mahesh Perera, the head of Sri Lanka's Information and Communication Technology Agency (ICTA).

The country's computer emergency response team (CERT|CC) has started an investigation into the incident and is working to recover the lost data.

Perera told media outlets that the Sri Lankan government doesn't plan to negotiate with the attackers or pay any ransom to retrieve the lost data.

A Sri Lankai Információs és Kommunikációs Technológiai Ügynökség **a súlyos adatvesztéssel járó zsarolóvírus támadás tényét hivatalosan is megerősítette.** Ez a gov.lk domaint használó összes kormányhivatalnál - beleértve a kabinetirodát, az elnöki tisztviselőket, az Oktatási Minisztériumot és a Egészségügyi Minisztériumot - megbénította a levelezést.

Az incidens állítólag május 17. és a felfedezés dátuma: augusztus 26. között történhetett. A támadás a beszámolók szerint a tartalék szervereket is veszélyeztette.



A támadás valószínűsíthetően köztisztviselőket célzó adathalász akcióval indult, **aminél a javítatlan szoftverek sebezhetőségeit kihasználva az elkövetők hozzáférést nyertek a kormányzati rendszerekhez. Mivel nem rendelkeztek mentéssel, így ez a levelezés egyes részeinél több hónapnyi helyrehozhatatlan kárt okozott.** A hírek szerint nem tárgyalnak a bűnözőkkel, és nem szándékoznak váltságdíjat fizetni.

Az ország eléggé le van maradva a kiberbiztonság területén, és ez nem csak a rendszerek sokáig halogatott frissítéseit jelenti, hanem emellett igen későn, csak a tavalyi évben hoztak döntést a helyi kiberbiztonsági hatóság létrehozásáról, illetve az is sokatmondó, hogy **csak most a ransomware támadás után vezették be a napi offline biztonsági mentési protokollokat.**

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: leállás levelezés ceylon sri váltságdíj lanka ransomware zsarolóvírus

Ajánlott bejegyzések:


Nem csitulnak a kórházak elleni támadások


Ransomware támadás a Nissan ellen



8 kórház, 30 klinika, 2.5 millió betegadat


LockBit piacgazdaság és tervgazdálkodás



Ransomware a One Motelben

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

695

Kézműves flottakezelés

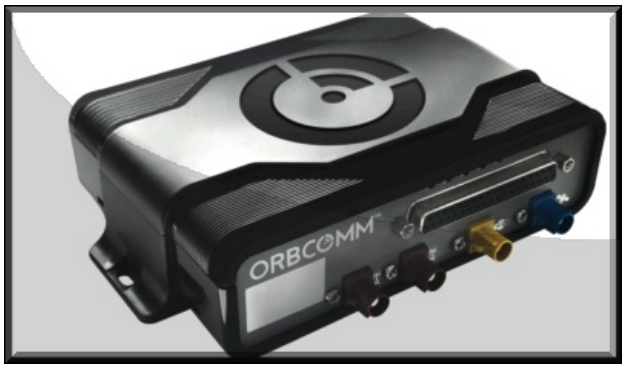
2023. szeptember 21. 13:14 - Csizmazia Darab István [Rambo]

Egy újabb ransomware áldozat napi működése esett hanyatt, ugyanis a **teherfuvarozási és flottakezelési megoldásokat szolgáltató New Jersey állambeli ORBCOMM megerősítette, hogy egy zsarolóvírus-támadás áll a közelmúltbeli szolgáltatáskimaradások hátterében.**



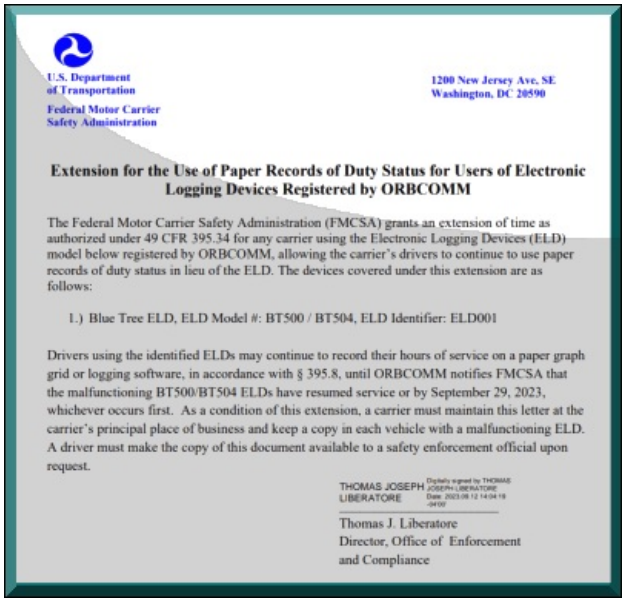
Hát ennek a "dolgozzanak a gépek" állapotnak vetett véget az incidens, gyakorlatilag szeptember 6-a óta nem tudták az ügyfelek nyomon követni szállított készleteiket a FleetManager szoftver leállása miatt.

A vállalat elektronikus naplózó eszközöket (ELD) is biztosít, amelyekkel a kamionosok naplózzák a vezetett órákat a biztonsági előírások betartása miatt. A támadás miatt viszont **az elektronikus naplózás sem működik, így a sofőrök jobb híján papír alapú naplózásra kényszerültek.**



Az ügyfelek azt látták, hogy a zsarolóvírus-támadást követően a teljes flottájuk elvesztette a GPS láthatóságát és az elektronikus naplózási képességeket.

A támadásról először beszámoló Bleeping Computer szerint a vállalat nem osztotta meg, pontosan mi okozta a kimaradást, és csak a nemrég közölték az ügyfelekkel, hogy ransomware támadás történt. Reményeik szerint szeptember 29-ig sikerül majd helyreállítani a szolgáltatásaikat.



U.S. Department of Transportation
Federal Motor Carrier Safety Administration

1200 New Jersey Ave, SE
Washington, DC 20590

Extension for the Use of Paper Records of Duty Status for Users of Electronic Logging Devices Registered by ORBCOMM

The Federal Motor Carrier Safety Administration (FMCSA) grants an extension of time as authorized under 49 CFR 395.34 for any carrier using the Electronic Logging Devices (ELD) model below registered by ORBCOMM, allowing the carrier's drivers to continue to use paper records of duty status in lieu of the ELD. The devices covered under this extension are as follows:

1.) Blue Tree ELD, ELD Model #: BT500 / BT504, ELD Identifier: ELD001

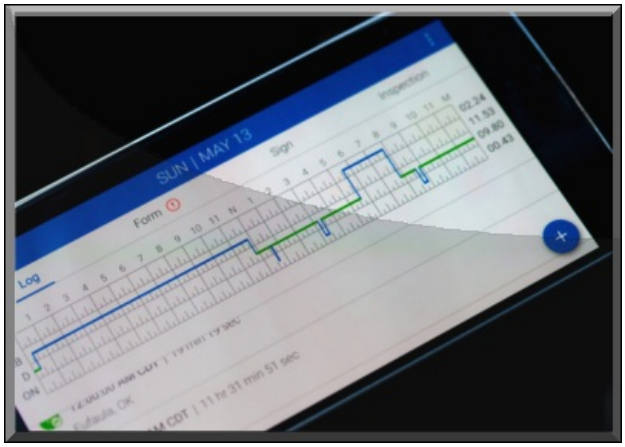
Drivers using the identified ELDs may continue to record their hours of service on a paper graph grid or logging software, in accordance with § 395.8, until ORBCOMM notifies FMCSA that the malfunctioning BT500/BT504 ELDs have resumed service or by September 29, 2023, whichever occurs first. As a condition of this extension, a carrier must maintain this letter at the carrier's principal place of business and keep a copy in each vehicle with a malfunctioning ELD. A driver must make the copy of this document available to a safety enforcement official upon request.

THOMAS JOSEPH LIBERATORE

Thomas J. Liberatore
Director, Office of Enforcement and Compliance

Mivel a papír alapú naplózás már csak korlátozott mértékben alkalmazható, emiatt az USA szövetségi gépjármű-biztonsági hatósága ideiglenes **felmentést adott** **a fuvarozó cégek számára, hogy a Blue Tree ELD szolgáltatás helyreállításáig, vagy legkésőbb szeptember 29-ig - amelyik előbb bekövetkezik - továbbra is használhassanak kézzel vezetett naplókat.**

A leállás az Egyesült Államok legnagyobb árufuvarozási vállalatait érintette hátrányosan, mivel nem tudják nyomon követni flottájukat és a készleteiket.



Egyelőre nem tudni, hogy pontosan melyik ransomware csoport áll a művelet hátterében, történt-e adatlopás is, mekkora váltságdíj követeléssel jelentkeztek, és történt-e kifizetés. Azt viszont a cég közölte, hogy külsős kiberbiztonsági szakértőket bíztak meg az incidens kivizsgálásával.

Emlékezetes lehet, hogy korábban már több kórházat ért támadás visszaröpítette a működést a XX. századba, emiatt telefonra, faxra, kartonozásra, noteszekre kényszerült a leállások alatt számos egészségügyi intézmény. Úgy tűnik, lassan érdemes lesz kockás-füzet és golyóstoll részvényekbe befektetni.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: usa gps fuvarozás flottakövetés nyomkövetés szállítmányozás ransomware áruszállítás zsarolóvírus orbcomm

Ajánlott bejegyzések:



8 kórház, 30 klinika, 2.5 millió betegadat



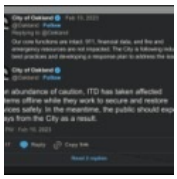
Kékfény különkiadás



9 millió, bizony, dalolva ment...



Dallas a pácban



Ország, város, ransomware

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

1335

Adathalászat menni booking.com

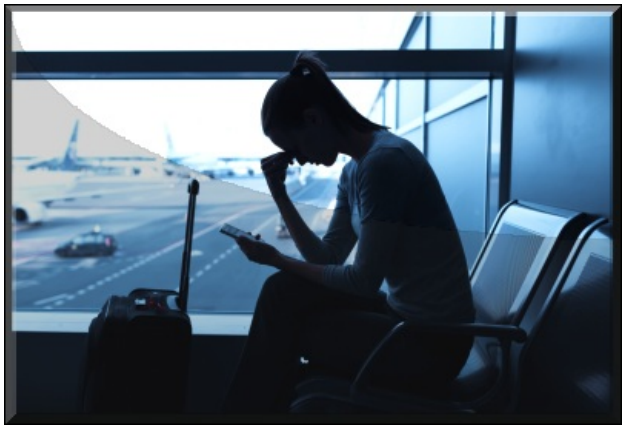
2023. szeptember 26. 12:46 - Csizmazia Darab István [Rambo]

Evidencia, hogy minden világszintű történésre gyorsan rárepülnek a támadók, legyen az lezuhant utasszállító, Covid lezárás, olimpia rendezés, foci VB, vagy booking.com cég látszólagos bedőlése. **Ez utóbbi vállalkozás hónapok óta tartó számlázási és kifizetési nehézsége most ötletet és ürügyet adott a kiberbűnözőknek, akik új fajta csalási kampányt indítottak a felhasználók banki adatainak megszerzéséért.**



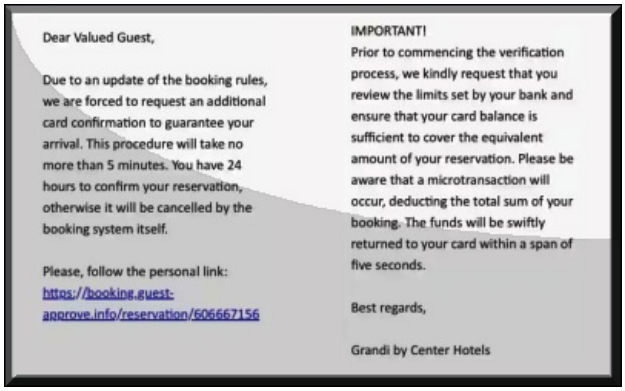
Biztonsági kutatók egy olyan új információlopási módra figyeltek fel, amelyben e**lőször szállodák, szállás foglalási oldalak és utazási irodák rendszereit törik fel, majd az így megszerzett hozzáféréseket az ügyfelek pénzügyi adataival való visszaélésekhez használják fel egy hamisított adathalász booking weboldalon.**

A vendéglátóipari intézmények becserkészéséhez **sok esetben eleinte social engieneering, azaz megtévesztés alapú technikákat használnak fel, például foglalások lekérdezése a kezdet.**



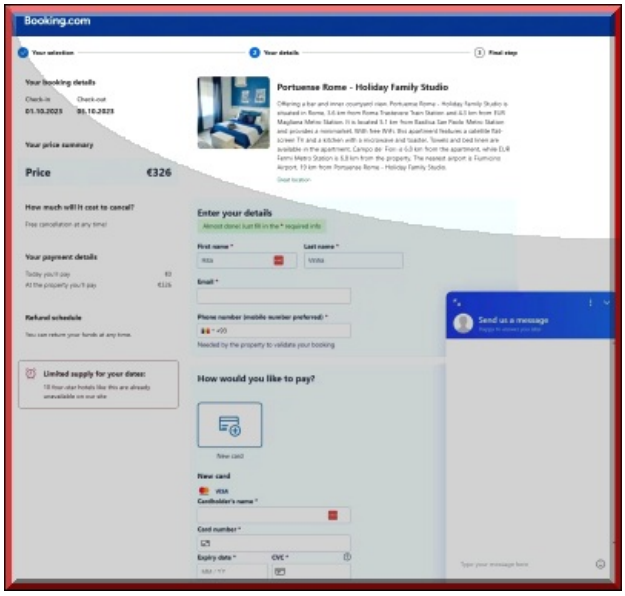
Miután felvették a kapcsolatot a szállodával, utazási irodával, a bűnözők különféle okokra hivatkozva - például az utazók egészségügyi állapotában bekövetkezett váratlan változás vagy egyéb rendkívüli körülmény miatt fontos dokumentumokat kérnek ki, hogy azt számukra egy adott URL-en keresztül küldjenek el.

Ha a figyelmetlen alkalmazott teljesíti ezt a kérést, a rosszindulatú link észrevétlenül egy kémprogramot vagy távmenedzsment alkalmazást telepít fel, melynek segítségével további érzékeny személyes adatokat, például hitelesítő adatokat, az utazni készülő ügyféllel folytatott teljes kommunikációt illetve a velük kapcsolatos pénzügyi információkat gyűjtenek össze a távoli támadók.



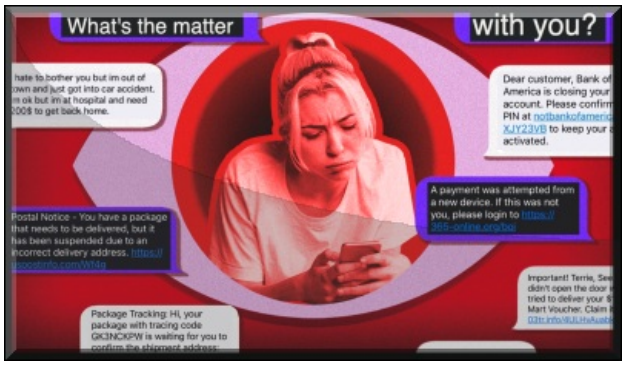
Ekkor már tudnak olyan az áldozatok profiljára testre szabott adathalász levelet küldeni, amely hitelesnek, aktuálisnak és valódinak látszik.

Ebben az áldozat kap egy linket látszólag a saját foglalási oldalának üzenetplatformjától, melyben kérnek egy soron kívüli állítólagos bankkártya ellenőrzést arra hivatkozva, hogy szükséges ahhoz, hogy megtarthassa a foglalást.



A kártékony szkript egy hamis Booking.com fizetési oldalt jelenít meg az áldozat képernyőjén, ahol ha valaki begépeli a részletes bankkártya adatait, búcsút mondhat a számláján lévő pénzének.

A csalást valóban nehéz észrevenni, de ha figyelembe vesszük a sürgetés-ijesztés-fenyegetés jelenlétét, egy váratlan esemény bekövetkeztét, ez már bőven lehet olyan gyanús jel, aminél érdemes lehet először közvetlenül kapcsolatba lépni a szállodával, a foglalási céggel vagy az utazási irodával, és náluk rákérdezni a változás okára.

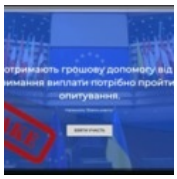


Mivel mostanra már temérdek személyes adat szivároghatott ki rólunk, a ChatGPT pedig elég jó nyelvi fordításokat produkál, így mindenkinek érdemes óvatosnak lenni még nagyon testre szabott és személyre szólónak látszó üzeneteknél, és semmiképpen nem javasolt kapkodva gyorsan egy ilyen vagy hasonló mellékelt linkre rákattintani.

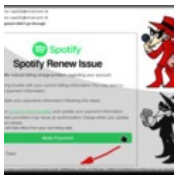
Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: utazás hotel szállás szálloda csalás átverés phishing testreszabott adathalászat banki adatlopás adathalász személyreszabott booking.com

Ajánlott bejegyzések:


Adathalászok lakat alatt


Viva la Revolut



Spotify megújítási probléma - vagy mégsem?



Üdvözöljük, csomagja kézbesítésre vár



Netflix: lejárt a tagságunk. Vagy mégsem?

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

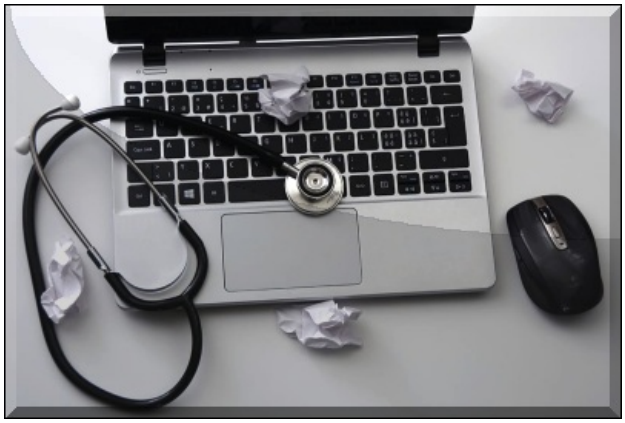
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

709

Ransomware - Fülöp-szigetek, 1:0

2023. szeptember 28. 17:37 - Csizmazia Darab István [Rambo]

Felhasználó, kórház, önkormányzat, olajvezeték után egy egész ország - erre láthattunk példát tavaly, amikor Costa Rica került a célkeresztbe. Az Oroszországhoz köthető Conti és Hive zsarolóvírus banda **2022. nyarán számos állami intézmény munkáját bénította meg, többek közt a pénzügyminisztérium hálózatát, adó- és vámhivatalokat, kereskedelmi központokat, közműveket, egészségügyi intézményeket.** Most pedig **a világszerte aktív Medusa ransomware tette tiszteletét a Fülöp-szigeteken.**



A helyi egészségügyi rendszert kezelő kormányzati szervezet (PhilHealth) szeptember 23-án közölte, hogy informatikai rendszerüket súlyos biztonsági incidens érte. Az állami tulajdonú szervezet az ország 114 millió polgára számára nyújt egészségbiztosítási szolgáltatást, ez borult most fel a támadás miatt.

Az érintett rendszereket ideiglenesen le kellett állítani, eközben pedig a lakosság megértését és türelmét kérik az üggyel kapcsolatban.



A leállás miatt az online fizetés nem működik, emellett a betegbiztosítási jogosultságok ellenőrzése is nehézkessé vált, ehhez most igazoló dokumentumot, vagy ezek fénymásolatát kell bemutatni.

A kórházi és egyéb ellátások miatti elszámolási határidőket ideiglenesen meghosszabbították, a folyamatban lévő kórházi kezelési, járulékfizetési és egyéb esetek feldolgozása pedig addig átmenetileg kézzel történik.



PhilHealth

Republic of the Philippines
PHILIPPINE HEALTH INSURANCE CORPORATION
Citystate Centre, 709 Shaw Boulevard, Pasig City
(02) 8441-7442 www.philhealth.gov.ph
PhilHealthOfficial teampnhealth

OFFICIAL STATEMENT
ON TEMPORARY SYSTEM DOWNTIME

This is to inform the public that the Philippine Health Insurance Corporation (PhilHealth) is currently implementing containment measures in response to an information security incident detected today, September 22, 2023.

We are currently investigating the matter together with concerned government agencies which include the Department of Information and Communications Technology to assess its extent.

While investigation is being undertaken, affected systems shall be temporarily shut down to secure our application systems.

We appeal for the public's understanding regarding the matter. Rest assured that we will get to the bottom of this and will institute stronger systems to prevent this from happening again in the future.

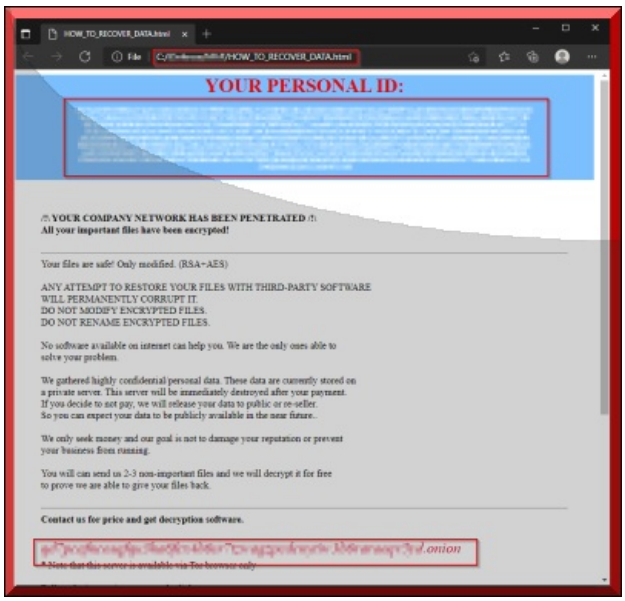
We will release updates on the developments of the investigation, and once the affected systems are up again.

(Sgd.) EMMANUEL R. LEDESMA, JR.
President and Chief Executive Officer

Sept. 22, 2023

A bűnözők tíz napos határidőt adtak a váltságdíj fizetésre, a követelt összeg pedig 300 ezer dollár - mai áron nagyjából 112 millió forintnak felel meg. Mivel a támadók az állami biztosító adatbázisát feltörték és az érzékeny személyes adatokat ellopták, ezzel a szervezet igen nehéz helyzetbe került. **Ha a határidőt szeretnék meghosszabbítani, az is húzós összegbe, 100 ezer dollárba kerülne.**

A mai hivatalos nyilatkozat szerint még mindig tart a rendszerek helyreállítása, ám a közlemény azt írja, személyes és egészségügyi adatok állítólag nem kerültek veszélybe.



HOW_TO_RECOVER_DATA.html

YOUR PERSONAL ID:

YOUR COMPANY NETWORK HAS BEEN PENETRATED
All your important files have been encrypted!

Your files are safe! Only modified. (RSA+AES)

ANY ATTEMPT TO RESTORE YOUR FILES WITH THIRD-PARTY SOFTWARE
WILL PERMANENTLY CORRUPT IT.
DO NOT MODIFY ENCRYPTED FILES.
DO NOT RENAME ENCRYPTED FILES.

No software available on internet can help you. We are the only ones able to solve your problem.

We gathered highly confidential personal data. These data are currently stored on a private server. This server will be immediately destroyed after your payment.
If you decide to not pay, we will release your data to public or re-seller.
So you can expect your data to be publicly available in the near future.

We only seek money and our goal is not to damage your reputation or prevent your business from running.

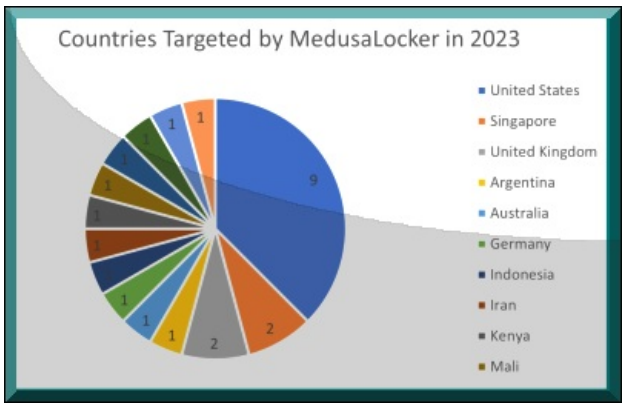
You will can send us 2-3 non-important files and we will decrypt it for free to prove we are able to give your files back.

Contact us for price and get decryption software.

.onion

A **Medusa Ransomware-as-a-Service (RaaS) szolgáltatási modellként működik, és jellemzően a váltságdíjak 60%-át a végrehajtó alvállalkozói leányvállalatoknak osztja le, a többit bevételt pedig a szervezet megtartja.**

A Medusa Locker támadások jelentős részében a Remote Desktop Protocol (RDP) sebezhetőségeire hagyatkoznak, hogy hozzáférjenek az áldozatok hálózataihoz, majd titkosítják az adatokat és pénzt követelnek.



Mivel a doxing, azaz az ellopott adatok nyilvánossá tételével való fenyegetés emeli a tétet a korábbi sima titkosítás - mentésből helyreállítás modellhez képest, így a kockázat és a veszteség is sokkal érzékenyebben érinti a szereplőket.

És a Medusa már több célzott, különféle kormányzati szereplők elleni akciót hajtott végre, például Minneapolisban állami iskolát, egy olasz ivóvíz szolgáltatót, de támadtak meg franciaországi közintézményeket, és állami távközlési vállalatot is.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: egészségügy váltságdíj ransomware fülöp-szigetek zsarolóvírus doxing

Ajánlott bejegyzések:



8 kórház, 30 klinika, 2.5 millió betegadat


9 millió, bizony, dalolva ment...


Ransomware támadás a Nissan ellen



Ransomware a One Motelben


Windows frissítés vagy mégsem?

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

472

Ransomware a One Motelben

2023. október 04. 07:53 - Csizmazia Darab István [Rambo]

A kissé ódivatú, Rejtőre hajazó cím mögött egy újabb informatikai támadás áll. **A németországi Motel One szállodalánc egy olcsóbb szegmensben utazik**, és nem csak helyben, külföldön is vannak egységei, összesen 90. Többek közt Ausztriában, Svájcban, Dániában, az USA-ban és az Egyesült Királyságban is.



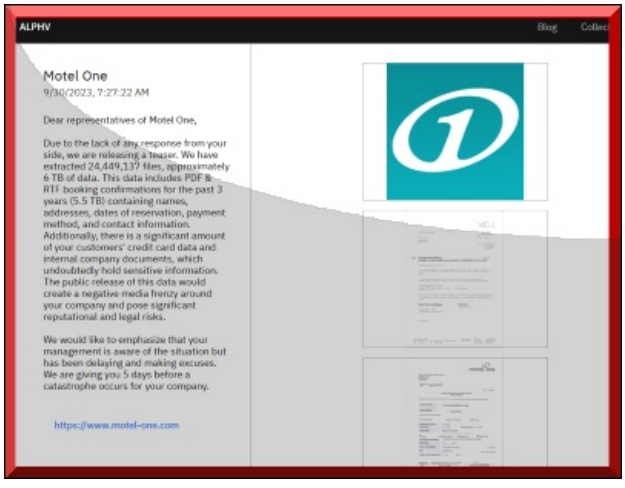
A világszerte mintegy 25 ezer szobát üzemeltető, Európa egyik legnagyobb láncát zsarolóvírus támadás érte, ám állításuk szerint szerencsére egy korai fázisban sikerült észlelniük az incidenst.

Az adatlopással kombinált behatolásnál hitelkártya adatok is illetéktelen kezekbe kerültek, ez a hivatalos közlemény szerint 150 ilyen tételt jelent. Az érintett ügyfeleket már értesítették az adatlopásról.



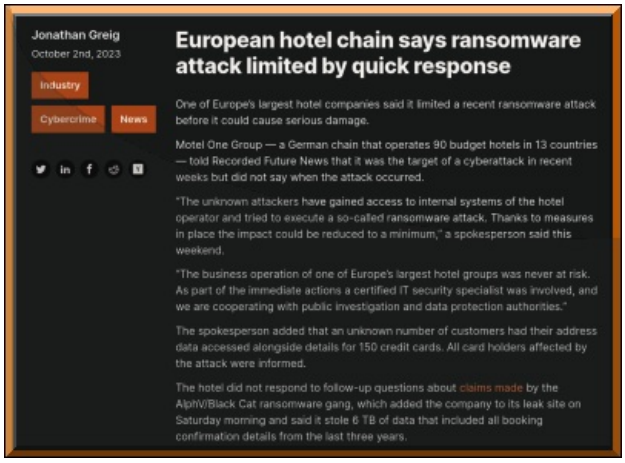
A támadást a BlackCat/ALPHV ransomware csoport hajtotta végre és vállalta magára még szeptember végén. A sötét weben található **Tor kiszivárogtató oldalukon azt állítják, 24 és fél millió bizalmas adatot sikerült ellopniuk, összesen 6 TB mennyiségben. A dokumentumok többek közt PDF és RTF fájlok, amelyek foglalási visszaigazolásokat tartalmaznak az elmúlt 3 évre vonatkozóan.**

A dokumentumok neveket, lakcímeket, a foglalási dátumokat, és a fizetéssel kapcsolatos információkat tartalmaznak mintegy 5.5 TB mennyiségben.



Ezeken felül pedig jelentős mennyiségű ügyfél hitelkártyaadatról és érzékeny vállalati belső dokumentumokról is állítják, hogy sikerült megszerezniük. A BlackCat öt napot adott a váltságdíj fizetésre, ellenkező esetben minden adatot kipakolnak a netre. Ha valóban igaz az adatlopás, akkor napokon belül kiderülhet, hogy beváltják-e a fenyegetésüket. Arról nem szóltak a hírek, mekkora a követelt összeg, és van-e a szállodaláncnak fizetési hajlandósága.

Nem ez az egyetlen szállodalánc, amit célba vettek, [pár héttel korábban az MGM Resorts elleni indítottak hasonlót](), ott a helyi pénznyerő automaták adataitól kezdve az éttermi menedzsmentrendszerekig rengeteg adatot sikerült ellopniuk.



A BlackCat/Alphv csoport igen csak aktív volt az utóbbi időben, például feltörte a Clariont, amely járművek számára gyárt audioberendezéseket. De a 2021 novembere óta tényked bűnbanda áldozatainak listája már amúgy is elég hosszú, rajta van például az ipari robbanóanyagokkal foglalkozó SOLAR INDUSTRIES INDIA, az amerikai védelmi iparban tényked NJVC vállalat, a Creos Luxembourg SA gázvezeték, a Swissport és a Western Digital.

Úgy tűnik, hogy a pénzügyi és ipari cégek mellett [újabban a szállodai és vendéglátóipari létesítmények is egyre gyakrabban válnak áldozattá](), ahol az ügyféladatok az igazi célpont.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: hotel motel váltságdíj adatlopás kiszivárogtatás ransomware zsarolóvírus szállodalánc doxing

Ajánlott bejegyzések:

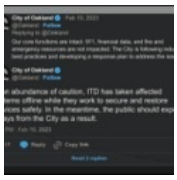

Ransomware támadás a Nissan ellen


9 millió, bizony, dalolva ment...


Bajban Venezuela legnagyobb bankja



Ransomware támadás érte az MSI-t


Ország, város, ransomware

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

760

Futószalagon érkeznek a hacktivista támadások

2023. október 10. 09:00 - Csizmazia Darab István [Rambo]

Miután szombaton a **Hámász terroristái fegyveres támadást intéztek az izraeli Gáza övezetben tartózkodók ellen, a kibertérben is felizzott a levegő.**



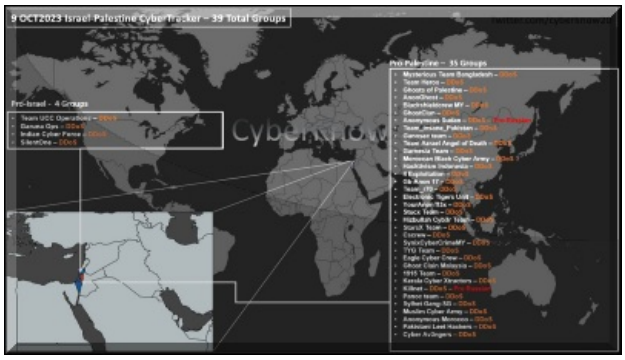
Mint ismeretes, **október 7-én támadás érte Izraelt, melynek során meg nem erősített információk szerint körülbelül 700 izraelit öltek meg, és több mint 150 ártatlan civilt ejtettek túszul a terroristák**. Minden esemény, tragédia, incidens után az interneten is megjelennek a helyzetet kihasználó támadók, ma már ez egy valós kockázat.

Ahogy azt legutóbb az orosz-ukrán háborúnál is láthattuk, ugyanígy itt is mind két oldal szimpatizánsai igyekeznek érzékeny csapásokat **mérni párhuzamosan a virtuális világban is az ellenfeleikre.**



Tucatnyi **kiberbűnözői csapat, zsarolóprogramokat terjesztő banda és hacktivista csoport jelentette be, hogy aktívan részt vesznek izraeli, illetve palesztinai intézmények elleni kibertámadásokban. A feltételezhetően orosz gyökerű Anonymous Sudan és Killnet csoport tagjai például izraeli kormányzati célpontok megzavarására összpontosítanak**, és eközben támadásaikat a Telegram csatornájukon is látványosan kommentálják.

Az Anonymous Sudan viszont kevésbé volt hangos, de elkötelezett híve a Palesztin Ellenállásnak, és támadást indítottak többek közt a Jerusalem Post vezető izraeli hírcsatorna ellen, amelynek weboldala a TheRegister cikkének megjelenésekor is elérhetetlen volt már több, mint 24 órája.



Mindeközben **indiai hacktivista csoportok is feltűntek a színen, szintén Izrael ellenes színekben**, annak ellenére, hogy az indiai kormány hivatalosan elvileg Izraelt támogatja ebben a krízisben.

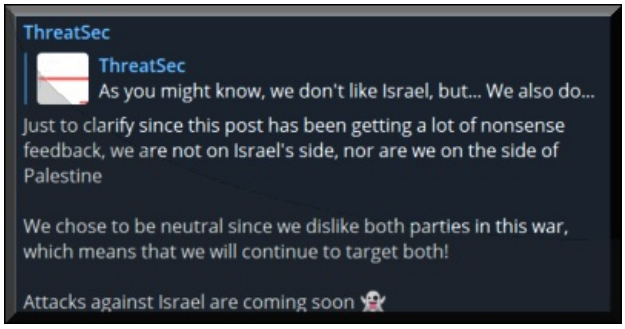
A hacktivista akciók általánosságban kormányzati webhelyek, médiaszervezetek és kritikus infrastruktúrák ellen irányulnak, mint például az energia szolgáltatók vagy a távközlési cégek. Ez utóbbi lehet a magyarázat

arra, hogy [a telekommunikációs szektorban jelentős zavarok tapasztalhatók a helyszínen](#).



De mindkét oldal megkapja a maga támadásait, így **például az internetszolgáltatók működésében Izraelben és Palesztinában is leállások tapasztalhatók, ezek szintén tipikus célpontok.**

A NetBlocks internetes megfigyelő szervezet a Gázai övezeten belüli internetszolgáltatás leállását észlelte, míg [a Threatsec nevű hacktivista csoport azt állította, hogy ők pedig sikeresen leállították a palesztin internetszolgáltató, az Alfanet](#) összes szerverét.



Ahogy az az orosz-ukrán konfliktusban is látható, **mind a fizikai térben, mind a világhálón történnek olyan sajnálatos események, amelyek minden korábbi egyezményt, megállapodást, emberiességgel kapcsolatos szempontot durván felrúgnak, és bár létezik elvileg egy szabályrendszer a kibertámadásokra is, nehéz megjósolni, hogy ezt mennyire tartják majd be itt az újabb izraeli-palesztin incidensnél - nagyjából semennyire.**

Az említett 8 pontból álló, a Vöröskereszt által javasolt lista többek közt **olyan kitételeket tartalmaz, hogy polgári célpontokat, egészségügyi és humanitárius létesítményeket senki ne támadjon, vagy például hogy senki ne buzdítson a nemzetközi humanitárius jog megsértésére.** A valóság azonban sajnos ezzel többnyire szembemegy.



A digitális hadviselés úgy tűnik, ugyanolyan kiszámíthatatlan szélsőséges cselekedeteket is felvonultat, mint ahogy a fizikai térben zajló háborúk és konfliktusok.

A Föld, a víz, a levegő és a világűr melletti immár ötödik hadszíntéren, azaz a kibertérben a jelenlegi gyakorlat sajnos akaratlanul is azoknak kedvez, akik gátlástalanul figyelmen kívül hagyják a fenti etikai szabályokat és a fennálló törvényeket.

Megosztom tumblr. Tweet Pin it Tetszik 0

1 komment
Címkék: háború terror infrastruktúra merénylet kritikus konfliktus hacktivizmus kibertámadás

Ajánlott bejegyzések:


Oroszország lett a fő kibercélpont


Felkészül: USA kritikus infrastruktúra


Tíz tiszta víz, ha nem tiszta, vidd vissza



Folytatják támadásaikat az orosz hackerek Ukrajna ellen


A nyugtalanság tengere

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

gigabursch 2023.10.12. 06:56:16

Addig én csak egy kávét kérek...

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy

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

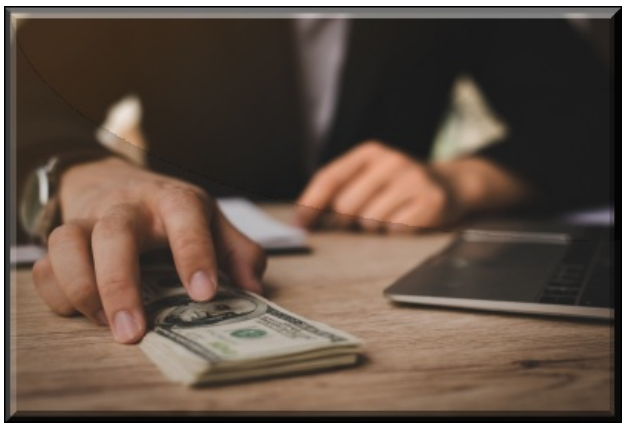
Belépés
Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

Megváltás-e a váltságdíj?

2023. október 16. 18:27 - Csizmazia Darab István [Rambo]

A friss CISO 2023-as felmérésből az derült ki, hogy **a bajba került szervezetek többsége fizetett már zsarolóvírus támadás miatt váltságdíjat, és ezeknek több mint fele 100 ezer dollárnál magasabb összeget utalt a bűnözők számlájára.**



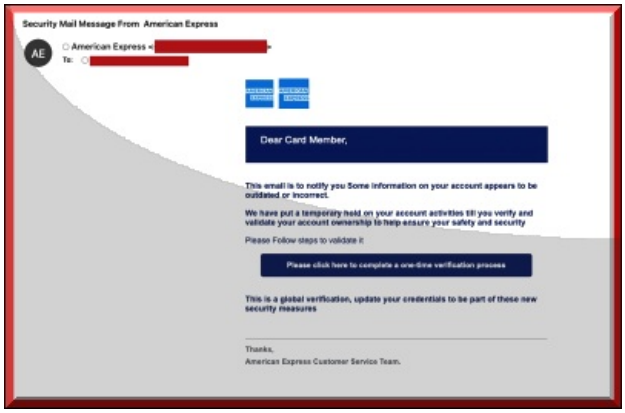
A felmérés ausztrál, kanadai, német, japán, szingapúri, brit és amerikai cégek kiberbiztonsági vezetőinek válaszain alapult. **A megkérdezettek többsége elismerte a váltságdíj fizetés tényét. A váltságdíjat fizetők 53%-a 100 000 dollárnál többet fizetett ki, 9% pedig legalább 1 millió dollárt költött el erre.**

A válaszadók ötöde, 18% fizette ki a váltságdíjat közvetlenül a támadóknak, 37% pedig kiberbiztosításon keresztül utalt, míg 28% pedig valamilyen harmadik közvetítő félen keresztül intézte ezt.

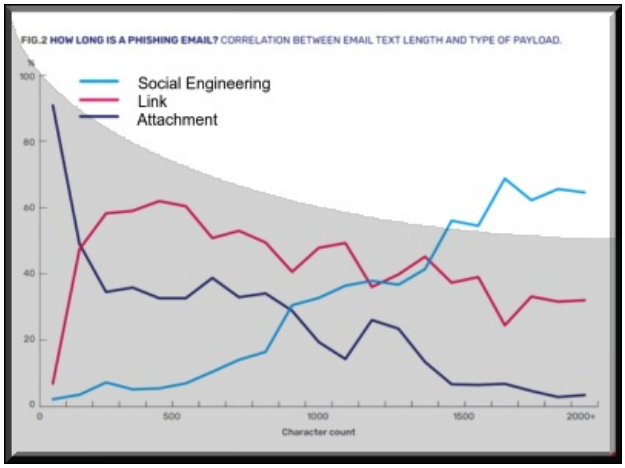


Egy másik elemzés pedig **az adathalász e-mailekről szólt, ahol az adatok azt mutatják, hogy ezeknél a Microsoft és az American Express nevével** élnek vissza leggyakrabban.

Azt világszerte tapasztalni lehet, hogy **minden pénzügyi szolgáltatásokkal kapcsolatos cég nevével próbálkoznak a csalók, és az adathalászat már nem csak a leggyakoribb klasszikus elektronikus levél formájában, hanem rosszindulatú SMS üzenetben, vagy telefonhívás formájában is jelentkezik.**

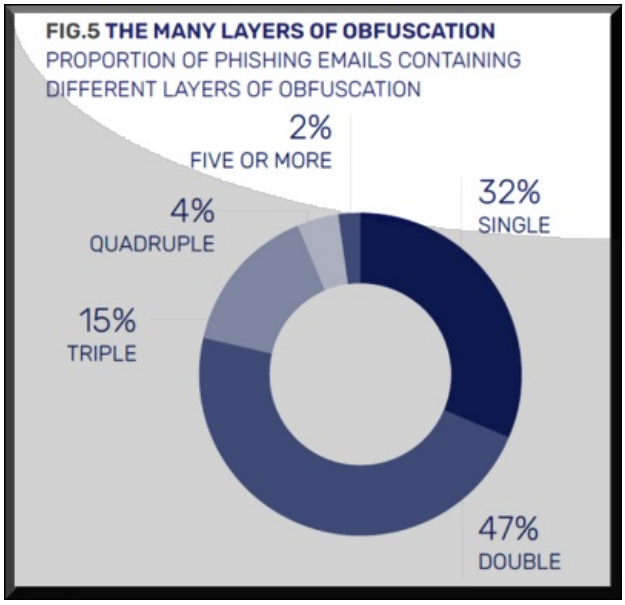


Az e-mailes formátumnál a kártékony tartalom leggyakrabban Javascriptes HTML formátumban érkezik, de a rosszindulatú fájlmelléklet is igen gyakori módszer arra, hogy adathalász oldalra továbbítson, kémprogram, zsarolóvírust vagy távoli elérést biztosító programokat (Anydesk, Teamvier) telepítésére vegyék rá az áldozatokat.



Az üzenetek **általában bevált átverési sablonokat vonultatnak fel: valamilyen be nem fizetett, lejárt közüzemi számla, meghallgatásra váró állítólagos hangposta értesítés, sürgős fizetési meghagyás, állítólagos vásárlásunkról szóló hamis visszaigazolás, átutalási vagy bankbetétünket érintő zárolás, illetve csomagküldéssel (GLS, DHL, UPS, DPD, Posta) kapcsolatos üzenet.**

Azt már a mindennapokban is látni, hogy **a kezdeti nevetséges tört magyarság, hibás hanyag nyelvtan helyett az egyre pontosabb nyers-fordítók és a mesterséges intelligencia fejlődési vonatára felülve már szinte hibátlan, roppant meggyőző adathalász leveleket** képesek produkálni.



A megelőzés-védekezés fronton v**annak a régi bevált okosságok, amelyek még mindig segítenek felismerni a turpisságot: idegen domén, ismeretlen feladó, egészen máshova mutató link-hivatkozás, spamre utaló körlevél forma, tegezés-magázás vegyesúszás, és a szokásos sürgetés-fenyegetés.**

Emellett vannak már kifejezetten az AI jelenlétére utaló intő jelek is: az elírásmentes hibátlan szövegben utalnak valamilyen általunk jól ismert közelmúltbeli releváns helyi eseményre, hogy az egész hitelesebbnek tűnjön, de szerepelhet benne valamilyen bennünket érintő egyébként publikus adat is, amellyel megpróbálják jobban személyre szabni az ilyen megkereséseket. **Ám felismerni ezeket valóban nem egyszerű feladat, már csak azért sem, mert gyakran egyszerre több összezavaró elfedő (obfuscate) réteggel operálnak.**

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: statisztika jelentés ai felmérés mesterséges intelligencia phishing adathalászat ransomware zsarolóvírus

Ajánlott bejegyzések:



Mesterségem címere adathalászat

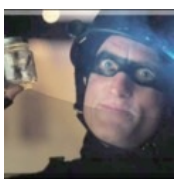

Na de mit adott nekünk a ChatGPT?



Havi 10 terabájt lett, maradhat?



Gyorsabban, magasabbra, erősebben!


Ipari mennyiségű ransomware az ipari

területeken

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

1412

Amikor a suszter cipője is admin

2023. október 19. 15:19 - Csizmazia Darab István [Rambo]

Rendszeresen írtunk már korábban is a Worst Password és Nordpass gyűjtésekről, ahol évről évre a leggyengébb jelszavak listáját teszik közszemlére. A mostani statisztika viszont nem a fotelban hátradőlő átlag júzerek, hanem a cég biztonságát őrző, jól képzett vállalati rendszergazdák szokásait vizsgálta ugyanerről.



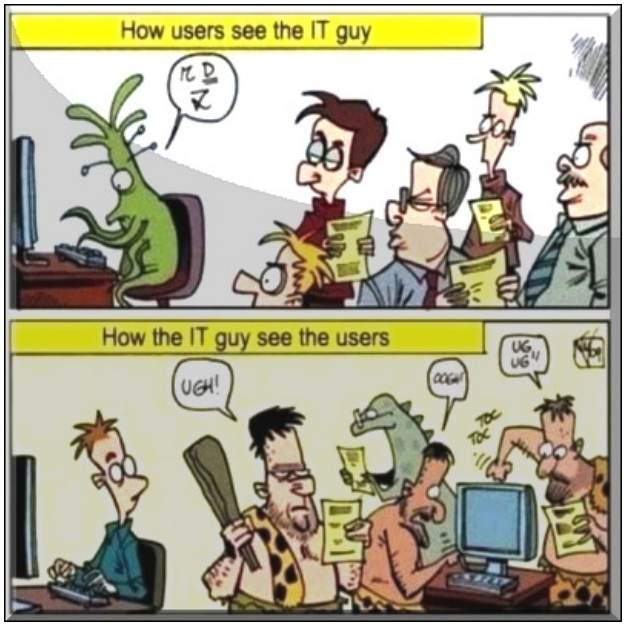
A tömegemberek által használt über primitív jelszólista helyezettjei rendre a qwerty, az admin, az abcd, az 123456, a password és hasonlók szoktak lenni. Ha valaki arra számított, hogy ezzel szemben a rendszergazdák mindegyike viszont pedánsan választja a hexadzsuva típusú bonyolult NASA szintű karaktersorozatokat, az most melléfogott.

Az Outpost24 adatai szerint ugyanis itt is az "admin" a legnépszerűbb jelszó, több mint 40 ezer előfordulással.

01.	admin	11.	demo
02.	123456	12.	root
03.	12345678	13.	123123
04.	1234	14.	admin@123
05.	Password	15.	123456aA@
06.	123	16.	01031974
07.	12345	17.	Admin@123
08.	admin123	18.	111111
09.	123456789	19.	admin1234
10.	adminisp	20.	admin1

Az 1.8 millió kiszivárgott, ellopott jelszó elemzéséből keletkezett statisztika szerint az adminisztrátori jelszavak frontján is lesújtóan vegyes a kép.

Bár sok helyen - például Microsoft által 2018-ban - bevezették a gyenge jelszavak alapból történő tiltását, **a 20 legnépszerűbb rendszergazdai jelszó mégis semmiben sem különbözik az átlag felhasználók által választott, percek alatt törhető tucat jelszavaktól.**



Már a szótáralapú feltöréseknél elvérző jelszavak így tényleg semmit nem érnek védelem szempontjából. **Amikor a vállalati hálózatok elleni leggyakoribb támadások - ransomware, Business e-mail compromise - óriási károkat képesek okozni**, nincs érdemi mentség arra, ha az alapvető biztonsági elveket és szabályokat a Holdig rúgva vannak ezek semmibe véve.

Ez minden átlagos fióknál is igaz, de különösen az érzékeny erőforrásokhoz való hozzáféréssel rendelkező felhasználók esetében egyenesen nélkülözhetetlen a hosszú, erős és egyedi jelszavak használata. Falrahányt borsó OFF.

Megosztom tumblr. Tweet Pin it Tetszik 0

1 komment
Címkék: statisztika admin jelszó rendszergazda gyenge feltörhető

Ajánlott bejegyzések:


Ne reszkessetek betörők!


C mint CEO, P mint password



Még gyengébb a jelszavad


Gyenge, gyengébb, leggyengébb


Kibermalac színre lép

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Mesterséges Geci 2023.10.21. 16:10:28

Azért azt megkérdezném, honnan tudják a statisztika készítői, hogy ezek az "adminisztrátori" jelszavak valóban admin foglalkozású szakemberektől származnak?

Nekem pl. mesgec az admin userem. Adminisztrátor/Administrator userem, rootnak nincs jelszava.
Nem-e lehet-e, hogy ezek úgy általában a windows Administrator useréhez kapcsolódó jelszavak, de ismeretlen tulajdonossal? Értsd: jó eséllyel privát gépek vagy olyan kis cégek gépei szolgáltatták a mintákat, ahol a villamosmérnök/könyvelő/kitudja ki dolga a számítógépek basztatása, mert "te értesz hozzá"?

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

1929

Szolgálunk és nem védünk

2023. október 25. 08:33 - Csizmazia Darab István [Rambo]

Érdekes informatikai incidens történt az ír rendőrségnél. **Egy 500 ezer tételes jelszavas védelem nélküli adatbázisra bukkant egy kiberbiztonsági kutató**. A védetlen adatállomány elképesztő mennyiségű személyes és banki adatot tett bárki által elérhetővé.



Adatlopás, adatszivárgás - napjaink legrettegettebb buzzwordjei, és a kémprogramok, doxingoló zsarolóvírusok tesznek is arról, hogy mindenki kellően paranoid hangulatban legyen.

No de mi van akkor, ha nincs is támadás a láthatáron, épp csak a bizalmas adatok kezelői tesznek valami jóvátehetetlent, ami csak a véletlennek köszönhetően derül ki. **Az ír rendőrség, a Garda, illetve annak alvállalkozói esetében pontosan valami ilyesmiről van most szó.**



Jeremiah Fowler biztonsági kutató egy olyan adatállományt talált, amelyben a hatóságok által lefoglalt gépjárművekkel kapcsolatos esetek szerepeltek 2017-től kezdődően. **Az ügyiratok mellékleteként beszkennelt személyazonosító okmányokat, részletes biztosítási vizsgálati jegyzőkönyveket, gépjármű-nyilvántartási igazolásokat, aláírás képeket, sofőrök, tanúk és Garda tisztek nevét és adataikat, valamint bankkártya adatokat (bankkártya számok, lejárati idő, kártyabirtokos neve) talált.**

A szakértő szerint minden egyes esethez körülbelül 2-5 dokumentumot tartalmazott ez a publikus adatállomány, így hozzávetőlegesen 150 ezer járműtulajdonost érinthet az incidens, akik nem csak írek, hanem más, harmadik országbeliek.



A rendőrség számára bedolgozó vontató társaságok a hatósággal kötött szerződések értelmében elvileg kötelesek lennének megvédeni a Garda Síochána által számukra szolgáltatott bizalmas információkat, beleértve a személyes adatokat is. Ez a kötelezettség kiterjed azokra az esetekre is, amikor az egyes vontatócégek ezeket az információkat tárolás céljából harmadik félnek adják át.

Fowler úgy véli, az incidenst egy a szereplők által igénybe vett felhős tárhely hibás hozzáférési beállítása okozhatta, mivel a hozzáférésnek több szervezet számára is nyitva kellett lennie, beleértve a rendőrséget, valamint a vontatási és tárolási cégeket. Azt talán még a brit tudósok is megerősítenék, hogy a kormányzat számára bedolgozó vállalkozók kiválasztása itt gyaníthatóan nem volt megfelelően kezelve.



A kutató a The Registernek úgy nyilatkozott, nem talált bizonyítékot arra, hogy rosszindulatú szereplők hozzáfértek-e a fent említett adatbázishoz. **Macerás ugyan minden egyes dokumentumhoz egyedi jelszót rendelni, de nyilvánvalóan nem szabad a biztonságot feláldozni ily módon a kényelem oltárán. A mostani incidens nem az első az ír rendőrség történetében, emlékezetes, hogy idén nyáron tisztek és polgári alkalmazottak személyes adatait tartalmazó táblázatot töltöttek fel tévedésből az internetre.**

2023. márciusában pedig az Egyesült Királyságban a cumbriai rendőrség tette véletlenül közzé az összes ott dolgozó tiszt adatait - neveket, fizetési adatokat - az interneten.

Megosztom tumblr. Tweet Pin it Tetszik 0

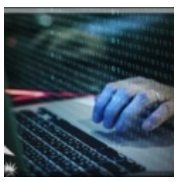
Szólj hozzá!
Címkék: hiba uk rendőrség egyesült királyság írország mulasztás adatszivárgás

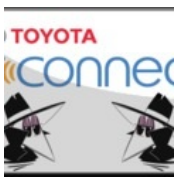
Ajánlott bejegyzések:


Néha nincs jó választás


Hiba a 8-ik rétegben


9 millió, bizony, dalolva ment...


10 gyakori IT biztonsági hiba



Cselekedettel és mulasztással

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

4449

Ügy + fél + kapu = adathalászat

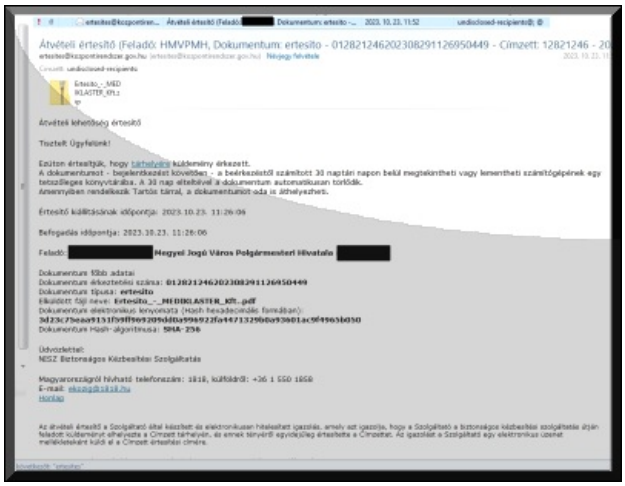
2023. október 30. 07:57 - Csizmazia Darab István [Rambo]

Magyar Posta nevével visszaélnek, tudjuk, Microsoft nevében, NAV nevében írnak nekünk ismerjük, jönnek a meg sem rendelt állítólagos küldeményeink a DHL, a FedEx, a GLS cégekre hivatkozva - tele velük a padlás. Viszont a NISZ, a Nemzeti Infokommunikációs Szolgáltató Zrt. nevében nem sok csaló e-mail jött még eddig, és itt az EDDIG szón van a hangsúly.



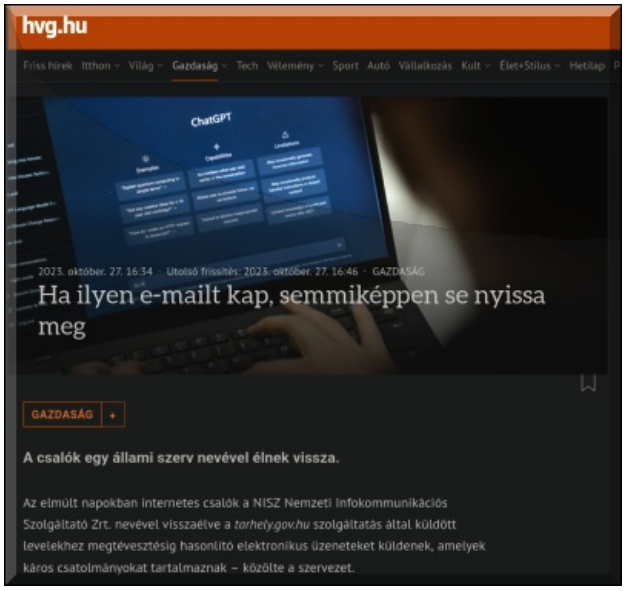
Látszólag az "ertesites@kozpontirendszer.gov.hu" a feladója annak a kéretlen üzenetnek, amely mostanában terjed az interneten. Általában elmondható, hogy a valóban ettől a feladótól származó levelek **nem szoktak levélmellékletet tartalmazni, így ez már önmagában is gyanús kell, hogy legyen.**

Az üzenet kinézete jól utánozza le a valódi levélmintát, és nyelvtanilag sem hemzseg a korábbi években megszokott magyartalan, nyersfordításra utaló fordulatoktól, **bár azért körlevélszerű.**



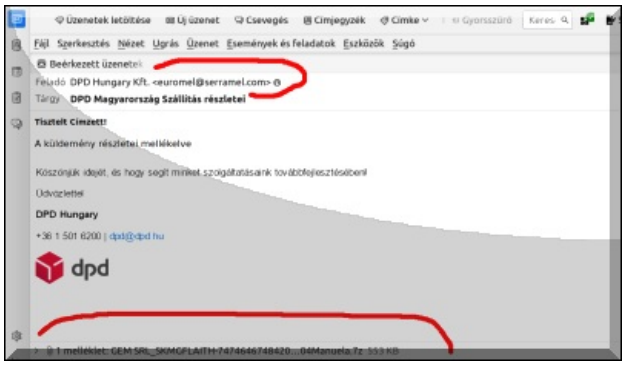
A biztonságtudatos trükk, miszerint **kattintás előtt vigyük az egérmutatót a hivatkozott link fölé itt is javasolt**, hiszen a szabványos igazi üzenetekben mindig a tarhely.gov.hu, illetve kau.gov.hu webcímekre hivatkozva közlik velünk, hogy kaptunk valami fontosat a hivataltól.

Itt viszont mind a melléklet, mind az idegen helyekre mutató URL hivatkozás veszélyt jelenthet.



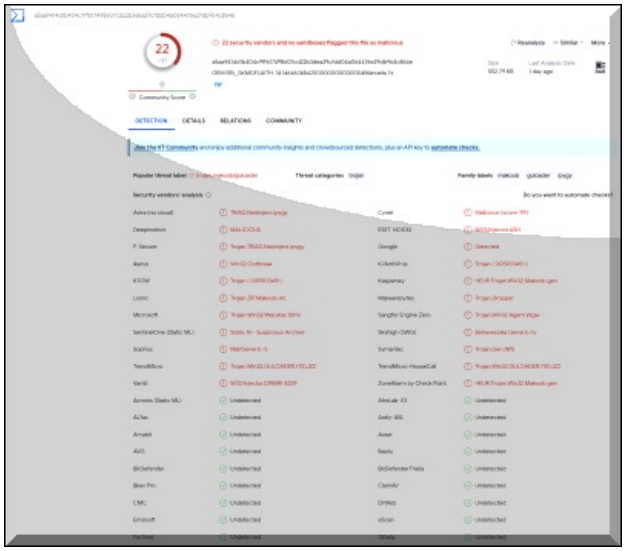
A melléklet legtöbbször valamilyen kártékony program, például zsarolóvírus vagy kémprogram szokott lenni, itt a vírusvédelmi program is védelmet nyújt, de a saját biztonságtudatos hozzáállásunk és óvatosságunk is hasznunkra válik, ha nem hagyjuk magunkat sürgetni, fenyegetni.

Sokszor építenek az ilyen átverések a kíváncsiságra is, ami szintén működőképes trükkje a támadóknak.



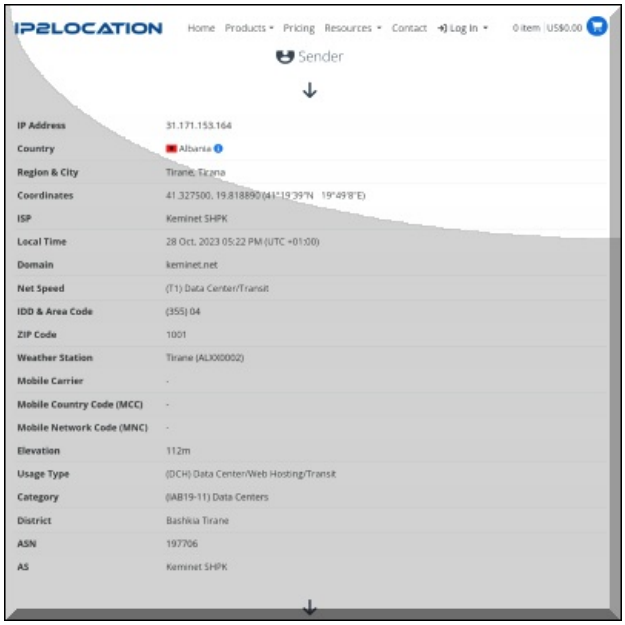
Ha pedig a linkre kattintást kérik és adathalász oldalra irányítanak bennünket, akkor az a kockázat, hogy ellopják a belépési azonosítónkat. **Legyünk mindig figyelmesek, ha valamilyen fontos szolgáltatásba - bank, hivatal, munkahely, webáruház, stb. - belépünk**, mert a hitelesítőadataink könnyen kerülhetnek illetéktelen kezekbe - jelenleg 12.7 milliárd ellopott, kiszivárgott jelszó található a haveibeenpwned weboldalon.

Ha biztosak akarunk lenni az ügyfélkapus bejelentkezésünk helyszínében, akkor a magyarorszag.hu vagy az ugyfelkapu.gov.hu cím mindig jó választást ad ehhez. Ha valaki ilyet csaló üzenetet kap, a csirt@nki.gov.hu oldalon tehet róla bejelentést.



Azért a végére még egy DPD-s levelet is mutatunk, ebből sohasem elég. Itt is a kíváncsiság felkeltése a módszer egy trükkös csatolmánnyal kiegészítve. Azért a levél feladónál - euromel KUKAC serramel PONT com - is látszik, hogy ez hatalmas átverés, **nem is hasonlít semmifajta hivatalos címre.**

Ám ha emellett a mellékletet feltöltjük a virustotal.com oldalra, azonnal látszik, hogy az egyértelműen egy kártékony kód.



Ez utóbbi próbálkozásba szemlátomást nem fektettek túlságosan sok energiát, persze ez sajnos még korántsem garancia arra, hogy figyelmetlenül senki nem fog majd lekattintani. Végül érdekességképpen ránézünk az e-mail trace segítségével a feladóra is, ezt Albániából küldték nekünk, hát oké, köszönjük Emese.

Megosztom tumblr. Tweet Pin it Tetszik 0

1 komment
Címkék: szolgáltató nemzeti zrt adathalászat ügyfélkapu csomagküldő dpd infokommunikációs nisz

Ajánlott bejegyzések:



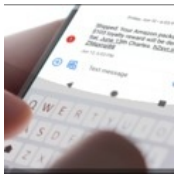
"NEM TUDJUK KISZÁLLÍTNI A CSOMAGÁT"



Sikeres brandek az adathalászatban



Kár érte, kiváló ügynök volt...



Mai szavunk pedig: smishing



Csomagot kaptam life...

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.



Head Honcho 2023.11.01. 07:12:06

Azért ravasz ez. Valaki nyilvánvalóan képben van nagyjából az állami formulákkal, tehát mégsem egy random külföldi támadó eszköze lehet.

Válasz erre

keresés

Keresés

Keresés

tweetz



Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

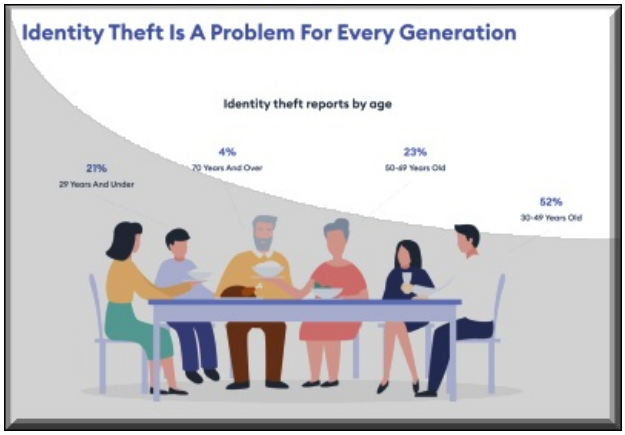
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

553

Identitás lopás: nem függ az életkortól

2023. november 02. 09:51 - Csizmazia Darab István [Rambo]

A személyazonosság-lopás által okozott károkat csak az Egyesült Államokban tavaly összesen 43mrd USD (több mint 15 ezer milliárd forintra) becsülték. **A gyerekeket is érintheti a személyazonosság-lopás: mit tehetünk a legkisebbek adatainak védelme érdekében?**



Miközben egyre tudatosabbak vagyunk saját személyes adataink védelmét illetően, felmerül a kérdés: elmondhatjuk ugyanezt a gyerekeink adatairól? **2022-ben csaknem egymillió gyerek vált csalók áldozatává az Egyesült Államokban, az incidensek egy háztartásra vetítve 1128 dolláros (közel 400 ezer forintos) kárt okoztak a családoknak, és átlagosan 16 órát igényelt az adatfeltörések kezelése.**

Mindez egy olyan problémát jelent, amely évente az amerikaiak több mint 1 milliárd dollárjába kerül. De **miért van ekkora kereslet a gyerekek személyes adatai iránt, hogyan lophatják el azokat, és mit tehetnek a szülők, hogy megakadályozzák a csalást?** Erre keresték a választ az ESET kutatói.



A csalók a gyerekek személyes adatait sokszor ugyanazokra a célokra használják fel, mint a felnőttekét: például bankszámlákat nyithatnak a nevükben pénzmosás és csalások elkövetésére.

Van egy másik népszerű technika, amely **jól alkalmazható a gyerekek személyes adataira, amikor a csaló több, különböző forrásból származó személyes adatot használ fel: némelyik valós, némelyik hamis. Így egy új személyazonosságot hoznak létre,** amely a gyerek fontos adatait felhasználva biztosítja a pozitív hiteltörténetet.



Hogyan történik a gyerekek személyazonosságának ellopása?
- A kiberbűnözés egy jól működő gépezet, amelyben a különböző szereplők különféle szerepeket töltenek be. A kiberbűnözők jellemzően személyes adatokat gyűjtenek, majd eladják a dark weben működő piactereken és fórumokon, hogy a csalók felhasználhassák azokat további támadásokhoz.

A szakértők szerint az adatok megszerzésének módjai hasonlóak a felnőttek kompromittálására használt módszerekhez.

- Adathalászat e-mailben, a közösségi médiában vagy akár sms-ben.

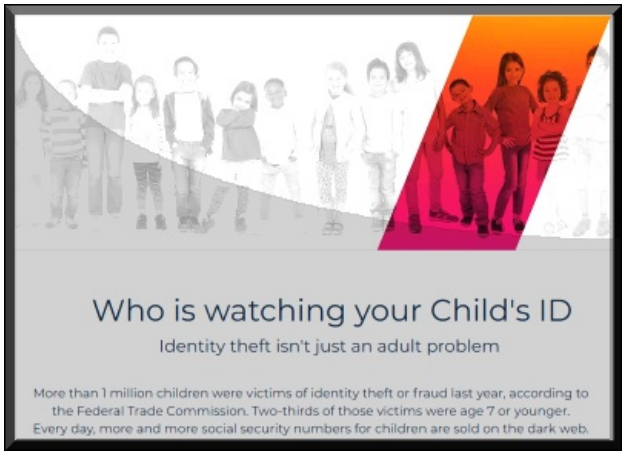
A célpontokat kártékony linkekre való kattintásra akarják rávenni (például vonzó, hihetetlenül olcsó LEGO vagy más játékokkal), más esetekben rosszindulatú szoftverek telepítését vagy a személyes adatok átadását kérik – például egy nem létező nyereményjátékban való részvételért cserébe.



- Harmadik felet érintő jogsértések. Tavaly mintegy 1.7 millió amerikai gyerek, vagyis minden 43. fiatalkorú személyes adatai kerültek nyilvánosságra és potenciálisan veszélybe olyan adatvédelmi incidensek miatt, ami nem az ő hibájukból történt.

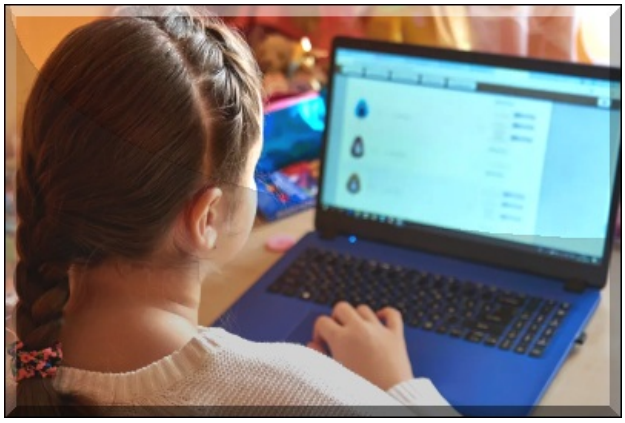
- **Feltört felhasználói fiókok**. A játékok, a közösségi média és az online oktatási fiókok is értékes személyes adatokat rejthetnek, amelyek adathalász-támadások, jelszófeltörések, brute-force támadások vagy más módszerek által veszélybe kerülhetnek.

- Túl sok információ megosztása a közösségi médiában. A szülők mellett a gyerekek is veszélybe kerülhetnek, ha túl sok személyes információt osztanak meg a közösségi fiókjaikon keresztül. Még a születési dátum és az iskolai tanulmányokra vonatkozó részletek is felhasználhatóak a csalók számára további adatok kizsarolására.



- **A családtagok által elkövetett csalás sokkolóan gyakori. Becslések szerint azon háztartások 67 százaléka, ahol egy gyerek személyazonosság-lopás áldozatává vált, személyesen ismerte az elkövető(ke)t.** Az érzékeny dokumentumokhoz való közvetlen hozzáférés tökéletes lehetőséget biztosít a rosszakaró családtagoknak, a csalás pedig akár évekig észrevétlen maradhat.

- Fizikai lopás. Még mindig népszerűek az olyan régi módszerek, mint a dokumentumok, ezzel együtt pedig az adatok megszerzése a szemétből vagy akár a postai levelekből.



Hogyan óvhatjuk meg a gyerekek személyazonosságát? Számos kipróbált és bevált gyakorlat létezik, amelyekkel csökkenthetjük a gyerekek adatai leselkedő kockázatokat.

- Kerüljük el a gyerekeinkkel kapcsolatos információk túlzott mértékű megosztását a közösségi médiában. A legjobb, ha elkerüljük a posztolást, kivéve, ha biztosak vagyunk abban, hogy csak olyan ismerőseink látják azokat, akikben megbízunk.

- Ellenőrizzük, hogy történnek-e szokatlan tevékenységek a gyerekhez tartozó (banki, telefonos, stb.) számlákon.

- Tartsuk naprakészen az összes háztartási gépet/eszközt a legújabb patch-ekkel és kártékony programok elleni szoftverekkel.

- Beszéljünk a gyerekekkel a közösségi médiában való túlzott információmegosztás, az adathalász-támadások, illetve a személyazonosság-lopás veszélyeiről.

- Korlátozzuk a gyerekek által használt fiókok/szolgáltatások számára. A regisztráció során adjuk meg saját adatainkat, ahol erre szükség van. A megelőzés mellett érdemes tisztában lenni a jelekkel, amelyek arra utalhatnak, hogy a gyerekek adataira pályázó csalókkal van dolgunk. **A szakértő szerint aggodalomra adhat okot, amennyiben szokatlan vagy váratlan számlák/kivonatok érkeznek gyerek nevére. Ugyanígy adattal való visszaélésre utaló gyanús jel lehet, ha az adóhivataltól, pénzintézettől, társadalombiztosítástól vagy adósságbehajtó cégtől érkezik valamilyen megkeresés, ahol a gyerek a címzett.**

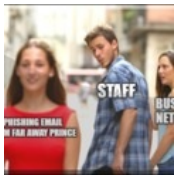


A személyazonossági csalás kockázata az élet része lett - ahol sajnos a gyerekek is áldozatok lehetnek. A digitális korban felelős szülőnek lenni több erőfeszítést igényelhet, mint 20 évvel ezelőtt. De ez ma már nem lehet alku tárgya, és alkalmazkodnunk kell a kihívásokhoz, hogy sikeresen megvédhessük gyerekeinket.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: statisztika gyerek gyermek tippek megelőzés védekezés adathalászat adatlopás

Ajánlott bejegyzések:



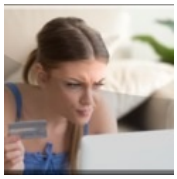
10 gyakori ok,


Okosotthon


Horgászati



Mesterségem


5 online

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

Okosotthon kontra felhasználó

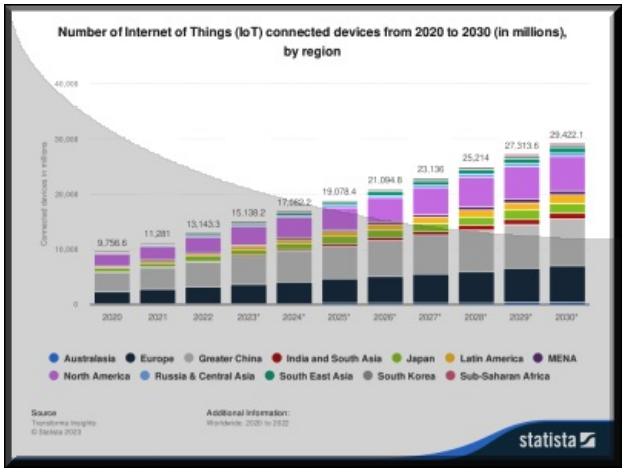
2023. november 07. 09:02 - Csizmazia Darab István [Rambo]

Összekapcsolt világban élünk. Van intelligens ajtócsengőnk, így ellenőrizhetjük okostelefonjainkon, hogy ki áll az ajtónk előtt, van okosóránk, hogy nyomon kövessük egészségi állapotunkat. A dolgok internetének forradalma még a háztartásainkat is elárasztotta az intelligens készülékek egész sorával, az okosteáskannáktól az okosmosógépeken át az okoshűtőszekrényekig.



Becslések szerint jelenleg 15 milliárd IoT eszköz van világszerte, 2030-ra egyes számítások szerint 30, egy másik tipp szerint 70-100 milliárd ilyen netes eszköz lesz forgalomban, beleértve az intelligens izzókat, a levegőminőség-monitorokat, az ajtócsengőket, a mosógépeket és a hűtőszekrényeket.

Mindez megkönnyítheti ugyan az életünket, de nem feltétlenül jelenti azt, hogy biztonságosabbá is teszi azt. Íme az ESET szakértőinek tanácsai arról, hogy **hogyan használjuk otthonunkban az okoseszközöket.**



Hogyan működik egy intelligens otthon? Ezek olyan eszközöket használnak, amelyek csatlakozhatnak az internethez, így lehetővé téve azok távoli vezérlését: távolból irányíthatjuk a kávéfőzőt, de akár a teljes fűtési rendszert is.

Miben más ez, mint egy hagyományos TV távirányító? Ezek az eszközök gyakran olyan internetes protokollt használnak, amihez egy külön hubon (vezérlő központon) keresztül csatlakoznak. A TV távirányítójával ellentétben azonban **ezek az eszközök információkat is gyűjthetnek és tárolhatnak szokásainkról, preferenciáinkról, sőt ha az eszköz kamerával van ellátva, akkor akár még a lakásbelsőnkről is.**



Tehát vannak ebben kockázatok is. Az ESET kiberbiztonsági szakértői összegyűjtötték mindazokat a veszélyeket, ha okoseszközök működnek a háztartásunkban. Előfordulhat, hogy az egyes készülékek nem teljesen biztonságosak: **egyes otthoni IoT-eszközök sietve vagy épp nagyon olcsón kerülnek piacra, mert a biztonságukkal nem foglalkoztak megfelelően, a gyártók ezen spóroltak.**

Így történhetett meg például, hogy Angliában egy babamonitoron kezdett el egy idegen személy egy gyerekhez beszélni. **Az is megeshet, hogy az otthoni hálózat eleve nem biztonságos, és így a hálózatban tárolt adatok elérhetők**

lehetnek a behatolók számára. Egy bűnöző ezzel akár nyomon követheti a különböző eszközök használati mintáit is, hogy lássa, ki mikor van távol otthonától.



Ha valaki az otthoni hálózatát a fő internetfiókjáról vezérli, akkor nem csak az IoT-eszközökről származó adatok lehetnek veszélyben, hanem az e-mailjei, a közösségi média fiókjai és még a bankszámlái is.

Sok felhasználó okostelefonon keresztül irányítja összekapcsolt otthonát, ami nagyon értékes adatbázis lehet annak, aki be akar törni hozzá. Ha a telefonunkat elveszítjük, ellopják vagy illetéktelen hozzáférnek, máris átvehetik az irányítást otthonunk felett: akár az ajtónkat is kinyithatják és besétálhatnak a lakásunkba.



A szakértők egyetértenek abban, hogy **a leggyengébb láncszem gyakran maga a felhasználó. Ezt mutatja az is, hogy évek óta létezik olyan gyűjtő weboldal, ahol meg lehet nézni az összes olyan védetlen netes eszközt, ami világszerte jelenleg nyitva van, így bárki számára látható, elérhető.**

Nagyon fontos, hogy minden neten vezérelhető eszközünknek egyúttal legyen manuális kontrollja is, vagyis **mindig legyen egy alternatíva, hogy áramszünet, vagy internetes leállás esetén se legyen vészhelyzet, tudjunk mozogni, kézzel is le tudjuk kapcsolni a berendezéseket.**



A következőket érdemes megtenni okoseszköz vásárlása esetén:

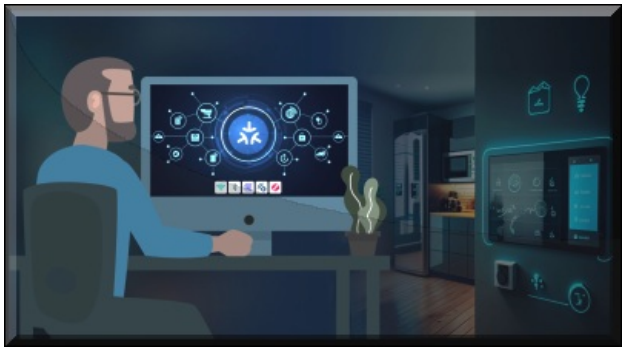
- Még vásárlás előtt végezzünk kutatást, olvassunk vásárlói véleményeket a kívánt eszközről, nézzük meg, hogy megbízhatóak-e. Célzottan keressünk rá a Google-on a márkanévre, a modell nevére, a "biztonsági rés" vagy hasonló szókombinációkkal együtt.

- Vásárlás előtt vizsgáljuk meg az eszköz adatvédelmi irányelveit. Hogyan fogja a gyártó felhasználni a személyes adatainkat? Milyen adatokhoz fér hozzá az adott eszköz? Ha nem kívánjuk használni a hangaktiválást egy eszközön, érdemes kikapcsolnia a mikrofont, hogy más beszélgetéseket ne vehessen fel és ne továbbítson.

- Tartózkodjunk az ismeretlen márkájú termékek vásárlásától, ha nem tudjuk ellenőrizni, hogyan védik adatainkat, kikkel osztják meg vagy hova töltik fel azokat. A gyenge olcsó eszköz vételárának megtakarítása később tetemesebb költségekkel járhat, ha ellopják az adatainkat.

- Miután megvásároltunk egy eszközt, mindig frissítsük a belső firmware szoftvert a lehető legújabb verzióra.

Ha javítás jelenik meg, azonnal telepítsük, mivel ezek általában a készülék biztonságosabbá tételére irányulnak.



- Az otthoni biztonság kezelésének egyik első lépése lehet az intelligens otthoni hálózat elkülönítése a többi hálózattól. Ez viszonylag egyszerű, ha vendéghálózatokat állítunk be az IoT otthoni eszközeinkhez. Például a hűtőszekrényt továbbra is feltörhetik, hogy egy botnet részévé váljon, amely spamet küld vagy kriptovalutákat bányászik. Mivel azonban saját külön szeparált hálózatot foglal el, ezzel még nem fognak tudnak hozzáférni e-mailjeinkhez vagy bankszámlánkhoz.

- Használjunk erős biztonsági szoftvert számítógépünkön és okostelefonunkon, hogy elkerüljük a rosszindulatú programok telepítését vagy a vírusfertőzést. Az ESET kiberbiztonsági megoldásaival az otthoni eszközeinket is biztonságban tudhatjuk.

- Ne felejtsük el rendszeresen frissíteni az eszközöket, akár automatikus frissítésekkel, akár manuálisan. Ez magában foglalhatja a gyártó webhelyének frissítéskeresését, majd az eszköz számítógéphez kapcsolását a frissítéshez.



Ne feledjük, hogy minden egyes hozzáadott eszköz további lehetőséget jelenthet a nemkívánatos látogatók számára, hogy bejussanak a hálózatunkba. **Ha valaki még többet szeretne tudni az okosotthonok biztonságáról, érdemes meghallgatni az ESET IT-biztonsági podcastjének, a Hackfelmetszők okosotthonokról szóló adását!**

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: frissítés internet veszély tippek megelőzés kockázat védekezés iot okoseszköz okosotthon

Ajánlott bejegyzések:



Identitás lopás: nem függ az életkortól



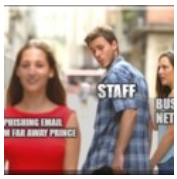
Okoskodás: okos-e az okosjáték?



10 gyakori IT biztonsági hiba



10 alaplépés a biztonsághoz



10 gyakori ok, amiért bedőlünk a csalásoknak

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

2241

Kár érte, kiváló ügynök volt...

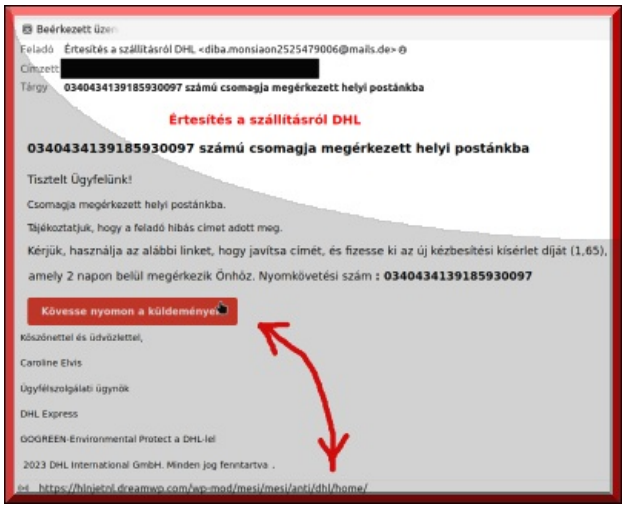
2023. november 13. 13:29 - Csizmazia Darab István [Rambo]

Az ügyfélszolgálati ügynök bejelentkezett, és bár úgy tűnik nincsenek beszélő viszonnyal a mesterséges intelligenciával, de azért az átlagfelhasználó "van lakat/nincs lakat" faék egyszerűségű gondolkodási sémáján is ideje lenne továbblépni.



Csomagunk érkezett, immár hatezer-kétszázadszor, ezúttal a DHL nevében. Csak a rend kedvéért, az igazi DHL nem a "diba PONT monsiaon2525479006 KUKAC mails PONT de" címről írna nekünk, Caroline Elvis Ügyfélszolgálati ügynök aláírásával, egy michigani (USA) IP címről.

Az igazi DHL nem írna azt, hogy "Kérjük, használja az alábbi linket, hogy javítsa címét, és fizesse ki az új kézbesítési kísérlet díját (1,65), amely 2 napon belül megérkezik Önhöz." és nem kérne 1.65 akármit azért, hogy új kézbesítési kísérletet tegyen.


Beérkezett üzen
Feladó Értesítés a szállításról DHL <diba.monsiaon2525479006@mails.de>
Címzett [redacted]
Tárgy 0340434139185930097 számú csomagja megérkezett helyi postánkba

Értesítés a szállításról DHL

0340434139185930097 számú csomagja megérkezett helyi postánkba

Tisztelt Ügyfelünk!

Csomagja megérkezett helyi postánkba.

Tájékoztatjuk, hogy a feladó hibás címet adott meg.

Kérjük, használja az alábbi linket, hogy javítsa címét, és fizesse ki az új kézbesítési kísérlet díját (1,65), amely 2 napon belül megérkezik Önhöz. Nyomkövetési szám : 0340434139185930097

Kövesse nyomon a küldeményét

Köszönettel és üdvözlettel,

Caroline Elvis

Ügyfélszolgálati ügynök

DHL Express

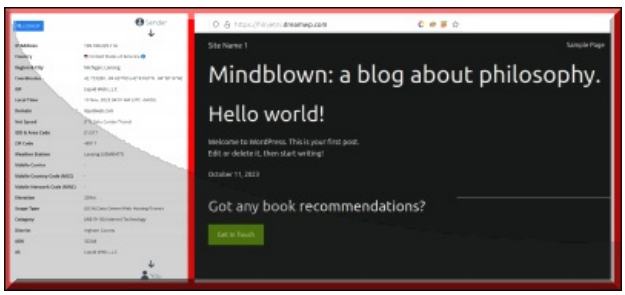
GOGREEN-Environmental Protect a DHL-lel

2023 DHL International GmbH. Minden jog fenntartva .

https://hlnjetnl.dreamwp.com/wp-mod/mesi/mesi/anti/dhl/home/

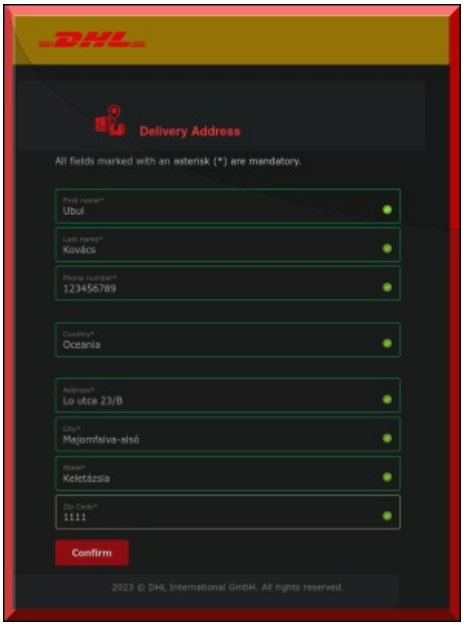
De amit még ennél is biztosabban sosem tenne az igazi DHL, hogy egy kattintható linket mellékel a "hlnjetnl PONT dreamwp PONT com PER wp-mod PER mesi PER mesi PER anti PER dhl PER home" URL címhez.

Ami egy elhanyagolt Wordpresses feltört oldal, nyilván tele kihasználható, be nem foltozott sebezhetőségekkel. Az alkönyvtárak nélküli főoldal egyértelműen mutatja, hogy egy ottani "Pistike" kísérletezett egy weboldal létrehozásával, amit az eredeti tulaj a Hello World állapot elérése után dobott.

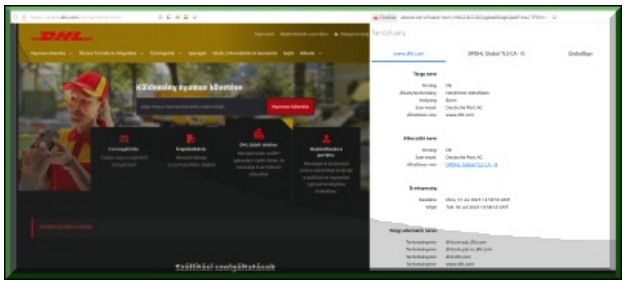


Azért a hecc kedvéért lejátsszuk vele a meccset, kattintás után bekéri a személyes adatokat: név, lakcím, telefonszám, majd ezek után a bankkártyánk adatairól is kérdez minket: kártyaszám, kártyára írt név, lejárati dátum és a CVV/CVC biztonsági kódunk.

Bár a weboldal kinézete látszólag valódi, az URL cím totál kamu, és mielőtt továbblépünk, nézzük ezt a "ha van lakat" akkor biztos minden jól van helyzetet is.

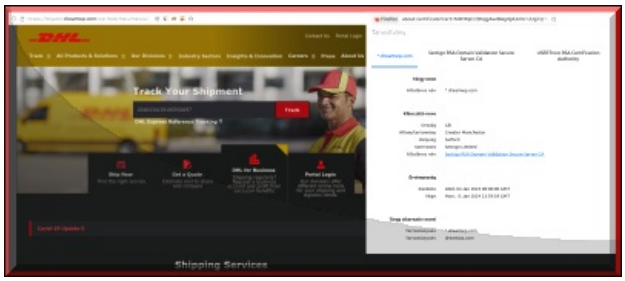


Ez itt az igazi DHL weboldal és a hozzátartozó érvényes tanúsítvány:



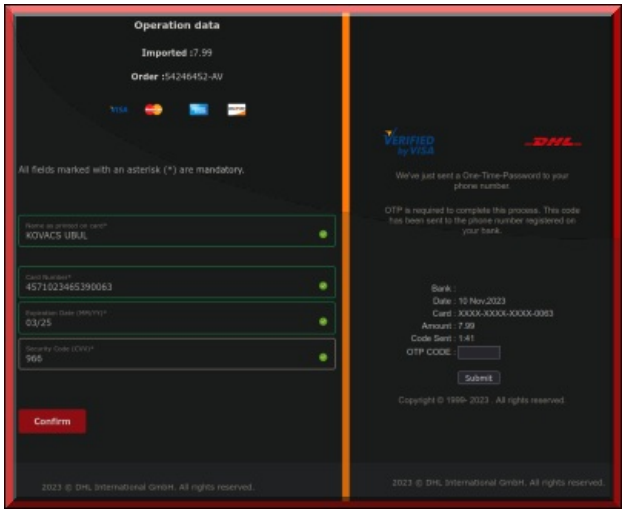
Ez pedig az adathalász webhely és egy ehhez tartózó, de NEM DHL, vagyis érvényes, de a csomagküldés szempontjából idegen tanúsítvány.

Érdemes mindig megnézni bankolás, hivatalos ügyintézések előtt magát a tanúsítványt is: tényleg annak a nevében állították-e ki, ahol vagyunk, ki bocsátotta ki, mi a lejárati ideje, stb., mert ez nagyon nem mindegy.



Visszatérve az adathalász oldalra, betolunk gyorsan valami hevenyészett elmebeteg adatot az űrlapnak és kíváncsian várjuk, hogy mi történik.

Kéri, hogy a telefonunkra érkező banki egyszeri OTP (One Time Password) kódját gépeljük be neki. Amit természetesen nem szabad megtenni, ha a pénzünket nem szeretnénk a számlánkról véglegesen elveszíteni.



Összességében, egy újabb gyenge próbálkozást láttunk, **de sajnos ezek száma és megtévesztő minősége várhatóan egyre csak emelkedni fog a jövőben.**

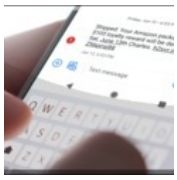
Megosztom tumblr. Tweet Pin it Tetszik 0

1 komment
Címkék: csomag csalás átverés dhl adathalászat csomagküldő

Ajánlott bejegyzések:



"NEM TUDJUK KISZÁLLÍTNI A CSOMAGÁT"



Mai szavunk pedig: smishing



Csomagot kaptam life...



Ismét csomagunk érkezett - vagy mégsem?



Magyar Posta csomagunk jött - vagy mégsem?

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.



Head Honcho 2023.11.15. 03:48:36

A pénzügyi tudatosság növelésével ki lehetne védeni az ilyeneket is. Amennyiben pl. általános iskolában a gyerkőcök agyát nem avíttas, múltidéző, haszontalan tudással (pl. hittan) terhelnék le, hanem ehelyett fel lennének készítve a modern életre, ez kivitelezhető is lenne. Persze tudom, ne képzelegjek...

Válasz erre

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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 piacgazdaság és tervgazdálkodás

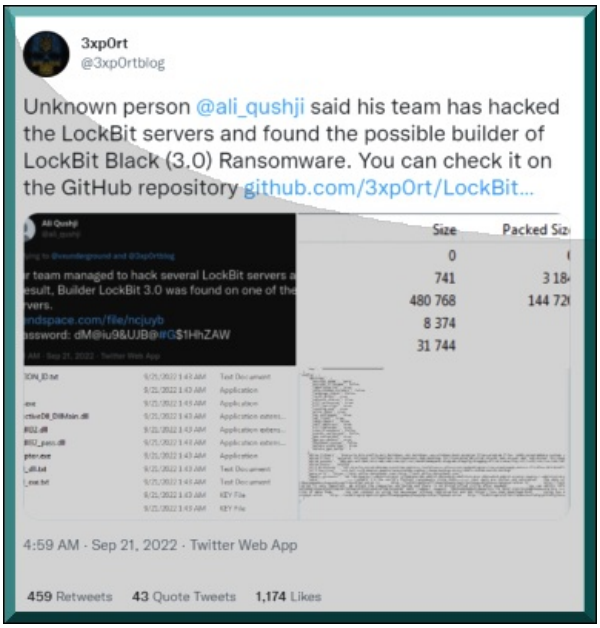
2023. november 21. 08:37 - Csizmazia Darab István [Rambo]

Elégetlen a LockBit zsarolóvírus vállalkozás vezetősége a saját partneri alvállalkozói hálózatukban (affiliate network) tevékenykedők "munkához" való hozzáállásával. A lusta vagy tehetségtelen kártevő terjesztő partnerek a vezetés szerint túl kevés pénzt fizetnek be a központi kasszába, és sokszor ezek az összegek jóval alacsonyabbak az előírt központi elvárásokhoz képest is.



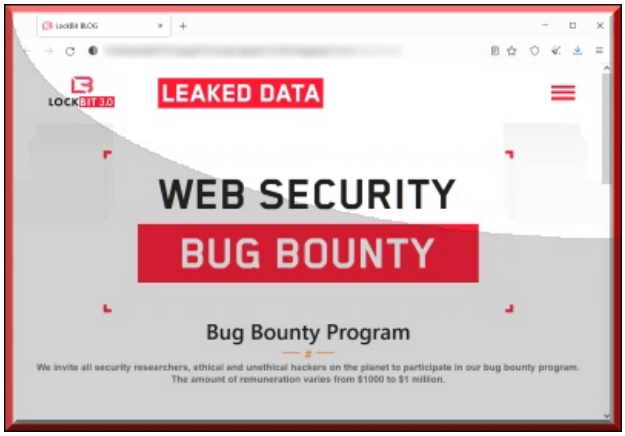
Tíz évvel vagyunk túl a CryptoLocker feltűnése után, ami az új generációs zsarolóvírusok nulla kilométerköve volt 2013-ban. **Erős és egyedi titkosítással kódolta el a felhasználók adatait, titkosított C&C szerverrel irányították a fertőzött gépeket, és Bitcoin formájában követeltek váltságdíjat az állományok feloldásáért. Azóta egész iparág szerveződött erre a jól kitalált és halálos konstrukcióra.**

A jelentősebb szereplők **azóta már RaaS, azaz szolgáltatásként bérelhető módon is árusítják a ransomware támadás lehetőségét, valamint közvetlen pénzkereseti lehetőséget is kínálnak** azoknak a terjesztőknek, akik ezzel mint külső partnerek kívánnak foglalkozni. Emellett persze további káoszt okoztak a kiszivárgott ransomware forráskódok is, amelyek szintén megsokszorozták a szereplőket a támadói oldalon.



A LockBit egyike azon hírhedt orosz hátterű bűnözői csapatoknak, akik már számos címlapra kerülő támadást indítottak különféle célpontok ellen. 2022-ben 78 GB érzékeny bizalmas adatot zsákmányoltak például az olasz adóhivataltól, de 2019. óta sok további akció köthető a nevükhöz.

Ami még emlékezetes lehet, hogy **a 2.0-ás verzió megjelenésekor már direktben toboroztak olyan sértett munkavállalókat, akik bosszúból vagy pénzért adnak el bizalmas céges adatokat, belsős munkahelyi hozzáféréseket, jelszavakat.**Az ajánlataikban ezért szép summát és "garantált" anonimitást kínáltak cserébe. A **3.0-ás változat még tovább ment, egyenesen BugBounty programot indított 1000 és 1 millió dollár közötti jutalomért a felfedezett hibákért.**



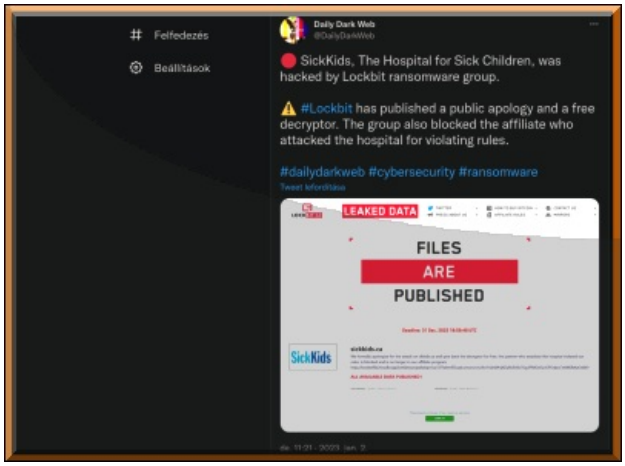
Ezúttal pedig a bűnbanda vezetői úgy látják, hogy túlságosan felhígult az alvállalkozói kör, és a tapasztalatlan partnerek nagyban rontják az üzletüket: rosszul tárgyalnak az áldozatokkal, túl korán túl sok kedvezményt kínálnak fel számukra az eredeti váltságdíjhoz képest és sok esetben még árulkodó nyomokat is hagynak maguk után.

A LockBit szerint sokan alapból 90%-os kedvezménnyel nyitnak, csak hogy minél hamarabb valamennyi pénzhez jussanak. Emiatt akárcsak egy valódi klasszikus vállalkozásnál, itt is előírásokat és elvárásokat fogalmaztak meg a cégvezetők, többek közt arról, hogy mekkora lehet a maximálisan felajánlható engedmény, és hogy a kezdeti váltságdíjhoz képest mekkora összegről indulhatnak meg a tárgyalások az áldozatokkal.



Mostantól az ilyen szerződött alvállalkozói partnerek - akik maguk is bűnözők - **vagy tartják magukat az eredeti központilag megszabott feltételekben előírt összegekhez, vagy meghatározott irányelvek mentén kell intézniük a zsarolást. A megtámadott intézmény éves árbevételéhez igazodó minimális váltságdíjat kell alkalmazniuk, és 2023. október 1-től már szigorúan tilos az eredetileg kért összeg 50%-át meghaladó kedvezményt adniuk a megtámadott céggel folytatott levelezésben a tárgyalási folyamat során. Ha pedig azt látják, hogy az áldozat vállalat rendelkezik kiberbiztosítással, úgy ne is engedjenek az alkudozásnak.**

Valamint azt is részletesen előírták számukra, hogy pontosan hogyan kell meghatározniuk a kezdeti váltságdíj összeget az áldozat intézmény éves bevételével arányosan. Általában azért ritka, hogy ennyire sikerül belelátni az ellenoldali ügyek részletes menetébe.



Zárásképpen pedig egy hozzájuk kapcsolódó korábbi másik érdekesség, ami 2023. tavaszán történt. Ekkor a

vezetők szintén elégetlenek voltak egyik saját partnerükkel. A kanadai SickKids gyermekkórház elleni ransomware támadás kapcsán élesen elítélték az egyik szerződött bűnözői partnerük akcióját arra hivatkozva, hogy ezzel a cselekményükkel etikailag megsértették a megállapodási feltételeket, és ekkor közvetlenül beleavatkozva az eseményekbe elnézést kértek, majd ingyenes helyreállító kulcsot küldtek a pórul járt egészségügyi intézménynek, illetve felbontották a szerintük szabályt sértő alvállalkozóval az együttműködést.

Innentől akár jöhet hozzájuk a blokkoló óra, az előírt félórás ebédszünet, termelési értekezletek és a havi Zoomos teljesítményértékelés is...

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: orosz fizetés tárgyalás network affiliate alvállalkozó szigorítás váltságdíj engedmény ransomware zsarolóvírus lockbit

Ajánlott bejegyzések:

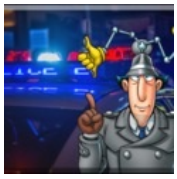


8 kórház, 30 klinika, 2.5 millió betegadat



Clop ransomware menni Torrent


Windows frissítés vagy mégsem?


Kékfény különkiadás


9 millió, bizony, dalolva ment...

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

345

Black Friday és Cyber Monday járja be Európát

2023. november 23. 19:17 - Csizmazia Darab István [Rambo]

A Black Friday és a kiberhétfő (Cyber Monday) közeledtével a csalók nagyobb sebességbe kapcsolnak, hogy minél több pénzt gomboljanak le a gyanútlan áldozatokról az év kereskedelmi tekintetben legforgalmasabb időszakában. **A vásárlók 2021-ben 8,9 milliárd dollárért vásároltak webshopokban a Black Friday ideje alatt**, az azt követő kiberhétfőn pedig éves rekordot jelentő 10,7 milliárd dollárt költöttek amerikai webáruházakban. **Világszerte percenként 1.3 millió USD összeget költöttek el a legutóbbi Black Friday során.**



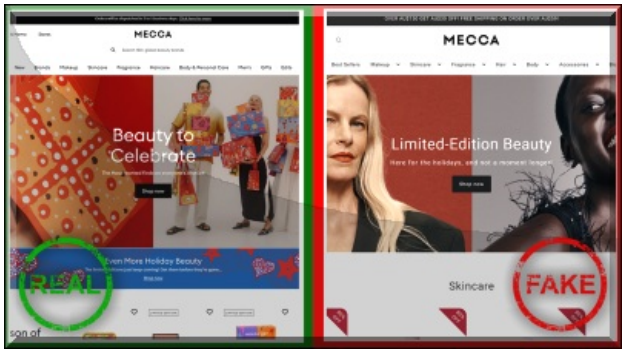
Miközben mindenki a tökéletes ünnepi ajándékokat keresi, **az ajánlatok között számos csalással is találkozhatunk.** Mi is lehet jobb módja annak, hogy valakit rávegyenek egy kártékony linkre való kattintásra, mint egy elképesztő és hamarosan véget érő "ajánlat" meghirdetése?

Érdemes vigyázni a leggyakrabban előforduló csalásokkal, amelyek (nem csak) ebben a szezonban terjednek. Az ESET szakértői most összegyűjtötték a legelterjedtebb módszereket, de **ezekről a Hackfelmetszők - Veled is megtörténhet podcastjukban is már részletesen beszélgettek.**



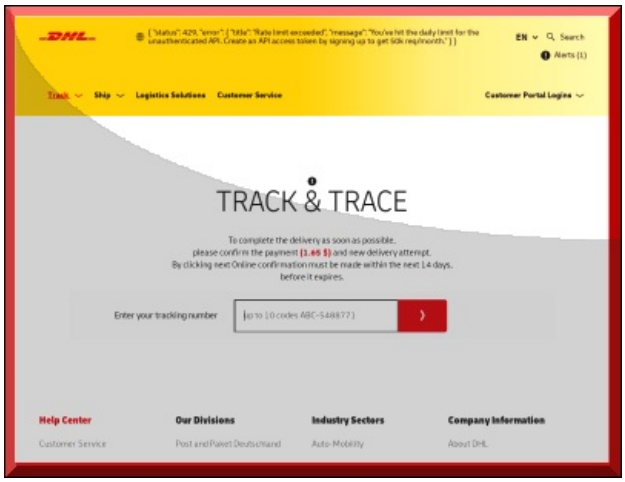
- Hamis ajánlatok: Talán ezeket a legnehezebb elkerülni. Előfordulhat ugyanis, hogy egy ismerősünk által továbbított szöveges üzenet vagy egy visszautasíthatatlan akciót hirdető Instagram-poszt rejti az átverést. Ilyenkor hajlamosak vagyunk egyből rákattintani a szövegben található linkre, és másodpercek alatt egy olyan oldalra kerülünk, ahol személyes adatainkat és hitelkártya adatainkat kérik. Bármit is "vásárolunk meg", azt sosem fogjuk megkapni, miközben a szenzitív adataink idegenek kezébe kerülnek.

- Megtévesztő ajándékkártyák: Hasonlóan az elektronikai eszközök és márkás ruhadarabok hamis akcióihoz, bármikor kaphatunk olyan ajánlatot is, amely nagy összegű ajándékkártyát ígér. A kapott e-mailben vagy a szöveges üzenetben található linkre kattintva viszont valószínűleg akaratlanul is egy rosszindulatú programot telepítünk az eszközeinkre, ezzel együtt pedig ellophatják személyes és bankkártya-adatainkat.



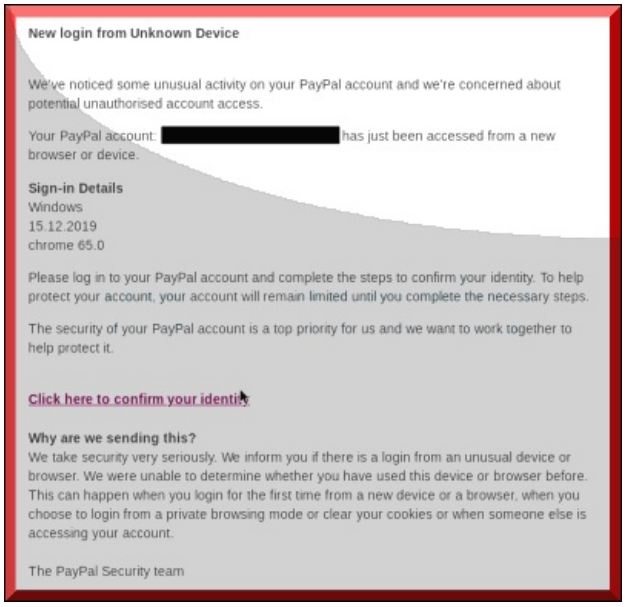
- Nem létező megrendelések és elmulasztott szállítások: *“A megrendelés kézbesítése folyamatban van, fizesse ki a hiányzó 1,5 dollárt, hogy megkapja azt.”* Az ilyen és ehhez hasonló csaló SMS-ek minden alkalommal keltsenek bennünk gyanút, még akkor is ha a feladó megbízható futárcégnek, például a DHL-nek vagy az UPS-nek adja ki magát.

Ha ilyen üzenetet kapunk, ne kattintsunk rá az SMS-ben lévő linkre, különben egy olyan hamis weboldalra kerülünk, ahol további adatokat kell megadnunk, hogy “igazoljuk személyazonosságunkat”. Más esetben állítólagos extra díjat fizettetnek velünk, amely végül a csalók zsebébe kerül vagy akaratunkon kívül kártékony szoftvert töltünk le eszközünkre.



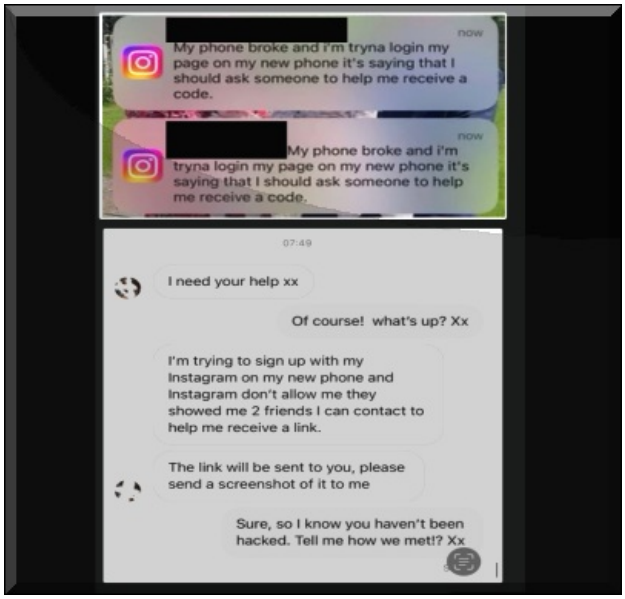
Hogyan kerülhetjük el, hogy csalás áldozatává váljunk?
1. Legyünk tisztában a kockázatokkal: A csalók a legkifinomultabb módszereket alkalmazzák arra, hogy becsapjanak minket. Ezáltal még az igazán óvatos embereket is behúzhatják a csőbe, 2009-ben például Steve Jobs is belépett egy hamisított Amazon webáruházba.. **Mindenképpen legyünk elővigyázatosak a valószerűtlenül kedvező ajánlatokkal szemben**, és legyünk tisztában azzal, hogy minél több eszközt használunk, és minél inkább függünk az online szolgáltatásoktól, annál nagyobb eséllyel esünk áldozatul.

2. Vásároljunk hivatalos webshopokból: A legegyszerűbben úgy kerülhetjük el a csalásokat, ha hivatalos megbízható weboldalakról rendelünk. Ez nem jelenti ugyanakkor azt, hogy a kiskereskedők webshopjai ne lennének biztonságosak. Hogy megbizonyosodjunk arról, egy weboldal megbízható, érdemes a kiskereskedő URL címét saját magunknak beírni ahelyett, hogy egy random linkre kattintunk. **Figyeljünk a nyelvtani hibákra és más figyelmeztető jelekre, emellett ellenőrizzük, hogy az oldal HTTPS protokollt használ-e érvényes tanúsítvánnyal. Végezetül Google keresést is lefolytathatunk egy adott kiskereskedővel és weboldallal kapcsolatban a fogyasztók korábbi véleményéről.**



3. Óvakodjunk az átverésektől az online piactereken: Sokan hirdetik termékeiket az eBayen, az Instagramon vagy a Facebook Marketplace-en. **Mivel ezeken a platformokon hirdetést feladni pofonegyszerű, nagy az esélye annak, hogy az eladók egy része valójában csaló**. Mindig ellenőrizzük, hogy ki a hirdető, nézzük meg az előzményeket és a véleményeket, hogy megbizonyosodjunk a megbízhatóságról. **Kerüljük a banki átutalást, és kérjük inkább más fizetési módok, például PayPal használatát, amely biztosítja a vevőt arról, hogy visszakapja a pénzét, ha nem kapja meg a megvásárolt terméket.**

4. Legyünk óvatosak a közösségi médiában az ismerősöktől kapott linkekkel: Ahogyan mi, úgy ismerőseink is bedőlhetnek az átveréseknek - ezzel együtt pedig akaratlanul továbbíthatják számunkra a nagyszerű ajánlatba csomagolt, csaló weboldalakra vezető linkeket. **Ne nyissuk meg ezeket a linkeket anélkül, hogy megbizonyosodnánk arról, hogy a weboldal valódi. A feltört fiókokat gyakran hamis termékek reklámozására vagy nagyszabású spamkampányok lebonyolítására is felhasználják.**



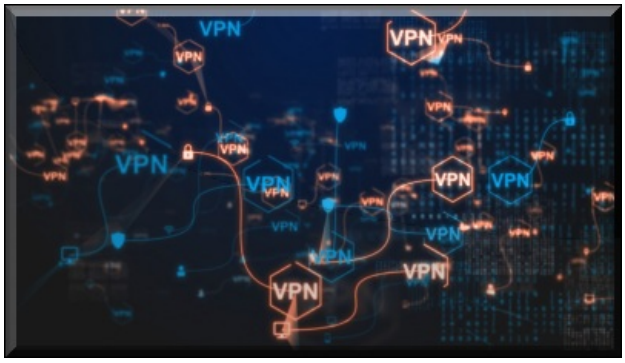
5. Válasszunk biztonságos fizetési módot: Használjuk ki a modern technológiát a biztonságunk megóvása érdekében. **Érdeklődjünk a bankunknál, hogy kaphatunk-e egyszer használatos virtuális kártyát egyedi vásárlásokhoz.** Ezáltal, ha bedőlünk egy átverésnek, nem a valós számlaadatainkat adjuk meg, a virtuális kártya pedig nem használható újra. **Igénybe vehetünk olyan biztonságos fizetésközvetítési szolgáltatókat is, mint a PayPal, emellett előfizethetünk online vásárlási biztosításra is.**

6. Óvakodjunk azoktól az ajánlatoktól, amelyek valószínűtlenül jónak tűnnek: Ez egy aranyszabály az online átverések elkerülése érdekében. Ha egy ajánlat túl jó, akkor valószínűleg csalásról van szó. Például mostanában nagyon nyomul a hirdetésekben a Temu és a Shein, érdemes előbb utánaolvasni ezeknek a cégeknek.



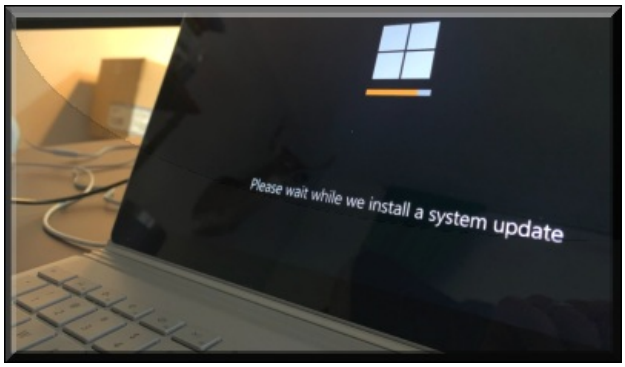
7. Ne használjunk nyilvános Wi-Fit: Az ingyenes Wi-Fi hozzáférési pontok kétségtelenül hasznosak, de komoly kockázatokat is rejtenek magukban, ezért soha ne használjuk őket például online vásárlásra vagy banki ügyintézésre. A támadók könnyen bejuthatnak egy rosszul védett hálózatba, hogy figyelemmel kísérjék potenciális áldozataik online tevékenységeit. **Megtévesztő bejelentkezési felületekre irányíthatnak, vagy egy ismert, legitim Wi-Fi hálózattal azonos nevű hamis hozzáférési pontot hozhatnak létre, hogy a gyanútlan felhasználók ahhoz csatlakozzanak. Ilyen módon a kiberbűnözők rögzíthetik a kapcsolaton keresztül továbbküldött adatokat - beleértve a jelszavakat és a banki adatokat -, és kártékony szoftverrel fertőzhetik meg az eszközt.**

8. Használjunk VPN-t: Amennyiben kénytelenek vagyunk nyilvános Wi-Fi hálózatot használni, a kockázatok minimalizálása érdekében használjunk virtuális magánhálózatot, vagyis VPN-t, amely titkosítja az adatokat a nyilvános hálózaton keresztül történő adatátvitel során. Mivel a forgalmat egy biztonságos csatornán keresztül bonyolítjuk le, személyes adatainkat a támadók nem tudják megszerezni. További előny, hogy **a VPN elrejti a tartózkodási helyünket, és segít elkerülni az online nyomonkövetést, hogy privát módon böngészhessünk az interneten.**



9. Kétfaktoros hitelesítés (2FA) engedélyezése: A jelszavak vagy a jelmondatok (passphrase) használata kulcsfontosságú, ugyanakkor a 2FA, vagy a többtényezős hitelesítés (MFA) sokkal biztonságosabbá teszi a bejelentkezéseket fiókjainkba. Mindez történhet olyan egyszerű módon, mint az SMS-ben küldött számsor, amellyel bejelentkezhetünk, de ennél jobb megoldást jelent, ha a fiókunkkal párosított hitelesítő alkalmazáson vagy hardveres biztonsági kulcson keresztül érkezik az azonosító kód. Ezáltal a hackerek sokkal nehezebben férnek hozzá fiókjainkhoz, még abban az esetben is, ha hitelesítő adataink sérülnek.

10. Tartsuk biztonságban eszközeinket: Ez egy egyszerű és hatékony megoldás. Mindig frissítsük a legújabb operációs rendszert mobiltelefonunkra, laptopunkra vagy táblagépünkre, és tartsuk naprakészen az összes alkalmazást és egyéb szoftvert, amit használunk. Mindez nagyobb védelmet biztosít az ismert sebezhetőségekkel szemben, és megnehezíti a támadók számára, hogy feltörjék eszközeinket vagy ellopják adatainkat. **Emellett fontos, hogy minden eszközünkön olyan digitális biztonsági megoldásokat használjunk, amelyek valós időben védenek a fenyegetésekkel szemben.**

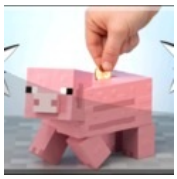


A csalók szüntelenül a következő áldozatukat keresik, ám a felsorolt tanácsokat betartva megvédhetjük magunkat a Black Friday, illetve a kiberhétfő idején - és minden alkalommal, amikor online vásárolunk!

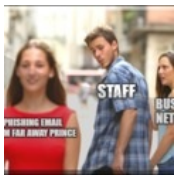
Megosztom tumblr. Tweet Pin it Tetszik 0

[Szólj hozzá!](#)
Címkék: [vásárlás](#) [podcast](#) [ünnepek](#) [karácsony](#) [black](#) [csalás](#) [átverés](#) [megelőzés](#) [friday](#) [védekezés](#) [hackfelmetszők](#)

Ajánlott bejegyzések:



[A csalások már a spájzban vannak](#)



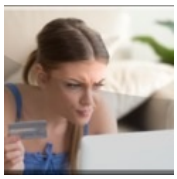
[10 gyakori ok, amiért bedőlünk a csalásoknak](#)



[Mit tehetünk a kriptovaluta csalások ellen?](#)



[Xmas és Top posztok az idén](#)



[5 online csalásra utaló jel](#)

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

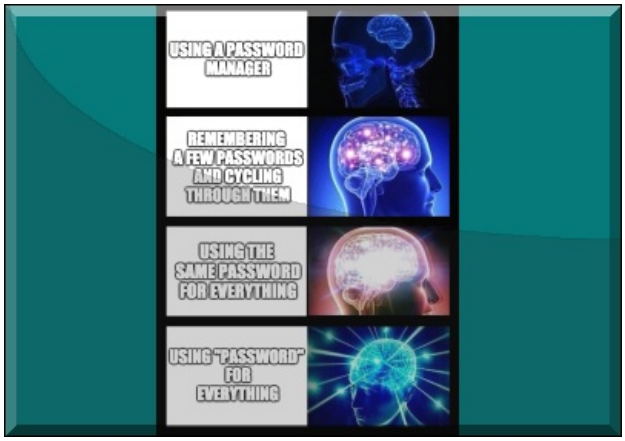
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

643

Ne reszkessetek betörők!

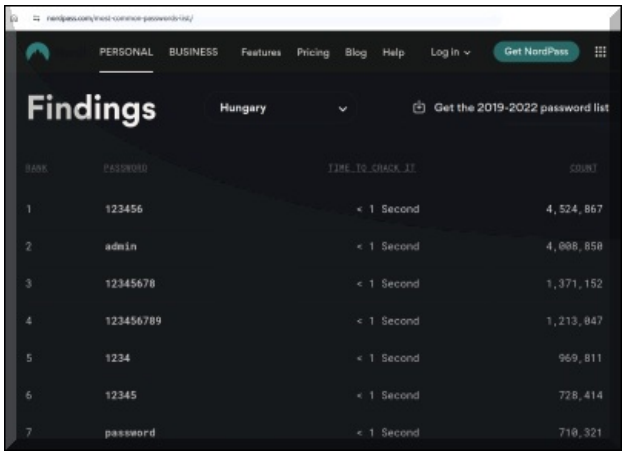
2023. november 28. 13:10 - Csizmazia Darab István [Rambo]

Aki azt várta, hogy a leggyakoribb jelszavak friss idei listáját világszinten nem az "123456" vezeti, annak ismét mélyen csalódnia kell. A NordPass aktuális jelentése arról árulkodik, hogy sajnos nem igazán tanulunk a saját hibáinkból. **A toplista szereplői igazi állandó törzsgárda tagok, csak éppen az évenkénti sorrendet kapjuk felkeverve, nem rázva.**



A további helyezettek sem új versenyzők, az ezüstéremért jogosan dolgozott meg az "admin", de a győztes unokatestvérei is előkelő pozíciókat birtokolnak, az igen biztonságos "12345678" nyakába került a bronzérem, míg az "123456789" csak pár tízezernyi ponttal lemaradva lett negyedik.

A teljes lista 200 tételes, a leggyakoribb jelszavak mellett olvashatjuk a valószínűsíthető feltörési időt is, aminek a mértékegysége is árulkodóan másodperc. Az első hétben szerepel még az "1234", az "12345" valamint a "password" is. De a 200-ik elem is eléggé Taigetosz-pozitív: "qwerty123456". A szótáralapú és brute force támadások elkövetői ilyenkor elégedetten hátradőlve már csak egy kávét kérnek.



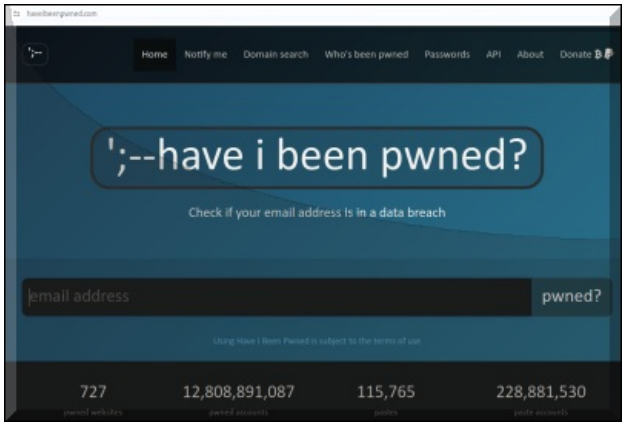
A kiértékelés alapja egy 6.6 Tbájt méretű adatállomány volt, amelynek statisztikai feldolgozása lehetővé tette, hogy 35 különböző ország szerint is szűrhető legyen a végeredmény. Emellett a kutatók a lista elkészítéséhez egy 4.3 Tbájt publikus adatbázist is felhasználtak, amelyben különféle nyilvánosan és szabadon elérhető forrásokból kinyert jelszavak szerepeltek, beleértve a darkweben szereplőket is.

Ha a magyar adatokra szűrünk, akkor mindössze csak annyi változást láthatunk az élbolyban, hogy az "admin" és az "123456" egymással helyet cseréltek.



Amint pedig [a korábbi teljes körű listákat nézzük meg egymás mellett 2019-től](), akkor jól látszik egy befagyott, belterjes fix közösség ez, ahol rendre csak minimális sorrendi változás következik be évről évre. **Ez arról tanúskodik, hogy sokan csak letudni akarják a jelszóválasztást, nem pedig tudatosan elvégezni.**

Nyilván vannak olyan fiókjaink is, amik nem igényelnek semmilyen extra erőfeszítést, nem kötődik hozzá pénzmozgás, megrendelés, hanem csak valami huszadrangú információszerzés, ott tényleg sokan ellazáskodják ezt a feladatot. **De ebből a fenti képből sokkal inkább úgy tűnik, hogy a többség az általánosan használt fiókjainál is ugyanilyen felelőtlen.**



[Sokszor és sokat posztoltunk már a jelszóválasztás fontosságáról]() és annak biztonságos kezeléséről, ezt az alábbi linken el is lehet olvasni. **De összességében elmondhatjuk, messze vagyunk még az erős, egyedi, rendszeresen cserélt, kétfaktoros autentikációval megerősített, jelszókezelőben tárolt tömeges megoldásoktól.**

[A jelszókezelő vagy jelszómenedzser programok pedig elég jól képesek lennének ebben segíteni](), csak sajnos az az apró probléma nehezíti mindezt, hogy az "123456" jelszót választók jellemzően nem igen olvasnak ilyen blogokat, mint amilyen ez is itt.

Megosztom tumblr. Tweet Pin it Tetszik 0

[Szólj hozzá!]()
Címkék: [statisztika]() [biztonság]() [toplista]() [jelszó]() [leggyengébb]() [gyenge]() [leggyakoribb]() [jelszómenedzser]() [nordpass]() [jelszószéf]() [feltörhető]()

Ajánlott bejegyzések:


[C mint CEO, P mint password]()



[Amikor a suszter cipője is admin]()


[Biztonság + kényelem = jelszókezelő]()



[Még gyengébb a jelszavad]()


[Gyenge, gyengébb, leggyengébb]()

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

Tíz tiszta víz, ha nem tiszta, vidd vissza

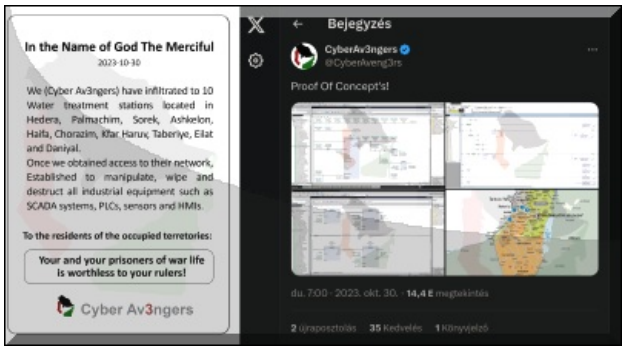
2023. december 01. 13:12 - Csizmazia Darab István [Rambo]

Áramszünetek Ukrajnában, a 2010-es Siemens centrifuga leégetése az iráni Busher atomerőműben Stuxnet kártevővel, repülőgép gyártó cégek elleni ransomware támadások, Costa Rica zsarolóvírusos megbénítása - számos hasonló incidensen vagyunk már túl, és egyik sem volt tanulság nélkül való.



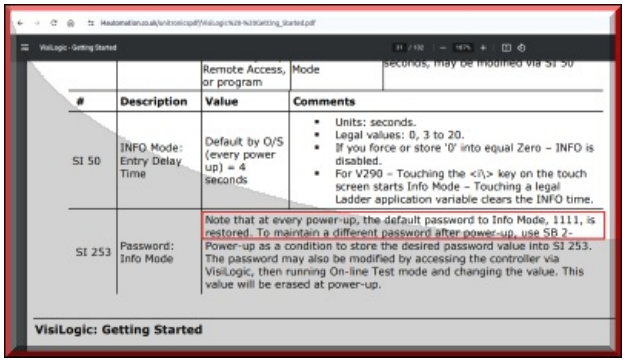
Ezúttal egy pennsylvaniai vízrendszer ellen történt attrocitás, ahol iráni elkövetők belematattak a vezérlésbe. Emiatt a kezelőknek kézi irányításra kellett visszaváltaniuk egy szivattyútelep esetében. A körülbelül 15 ezer ügyfelet kiszolgáló Aliquippa városi vízügyi hatóság tájékoztatása szerint egy Cyber Av3ngers nevű Izrael-ellenes kiberbűnöző banda követte el a támadást, amelynél sikerült átvenniük a vezérlést az egyik nyomásfokozó szivattyúállomásnál.

A bűnözői csoport a Twitter-hírcsatornáján azzal dicsekedett, hogy **már 10 különböző izraeli vízrendszert kompromittáltak.**



A fenyegetés szerint további közműveket fognak megtámadni, és **ezt a gázai övezetben zajló incidensre hivatkozva, politikai okokból hajtják végre. Az USA kiberbiztonsági ügynöksége (CISA) ügynöksége már vizsgálja a támadás**t, és az üzemeltetőket felszólította a biztonság szigorítására.

A hivatalos állásfoglalás szerint a kézi vezérlésre való átállás miatt a pennsylvaniai ivóvíz ellátás nem került közvetlen veszélybe.



Az incidens azonban roppant veszélyes volt, hiszen **a vízellátási infrastruktúrába illetéktelenül behatolva rengeteg módon lehetséges a károkozás: tartályok és tározók feltöltéséhez szükséges szivattyúk vezérlését vehetik át, a vízzel kapcsolatos vegyszerek adagolás változtathatják meg, vagy hamis riasztásokat is generálhatnak a rendszerben.**

Azt nem tudni, hogy **valamilyen sebezhetőség révén sikerült a támadóknak a behatolás, vagy az üzemeltetők az Unitronics PLC alapértelmezett jelszavát, az "1111" nem változtatták meg, volt-e használatban többtényezős hitelesítés**, illetve az eszköz valóban közvetlenül csatlakozott-e az internetre.



Vízművek ellen fordultak elő támadások már korábban is, például 2022-ben Nagy Britanniában. Emlékezetes, hogy 2021-ben a Colonial Pipeline vezetékhálózat elleni kibertámadás hatalmas anyagi veszteséget és hetekig elhúzódó üzemanyaghiányt hozott az USA keleti partján. A zsarolóvírus támadás előzménye pedig az volt, hogy **a mérnökök által távmunkában felügyelték olajhálózat vezérlését, és az ehhez tartozó gyenge jelszavak kikerültek a netre, és érthetetlen módon nem is használtak kétfaktoros autentikációt.**

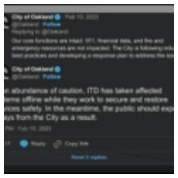
Kórházak, ipari és egyéb gyártók ellen is sajnos már évek óta sorozatban történnek különféle ransomare és doxing támadások.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: usa izrael irán infrastruktúra kritikus támadás áramszünet 1111 vízművek ransomware unitronics

Ajánlott bejegyzések:


Felkészül: USA kritikus infrastruktúra


Ország, város, ransomware


A nyugtalanság tengere


Apa kezdődik!


Divat lett a benzinkutak elleni kibertámadás

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

1143

ChatGPT: hogyan használjuk a munkában?

2023. december 05. 09:50 - Csizmazia Darab István [Rambo]

Az elmúlt hónapok során felerősödtek a mesterséges intelligenciát (AI) alkalmazó eszközökről szóló viták. Mivel **segítségükkel növelhető a produktivitás és használatuk időt takaríthat meg, sok munkavállaló beépítette ezen eszközök alkalmazását a mindennapi munkafolyamatokba.**



Mielőtt megpróbáljuk kihasználni az innovatív AI eszközök előnyeit, meg kell tanulnunk biztonságosan, adataink veszélyeztetése nélkül igénybe venni azokat. **A mesterséges intelligenciát alkalmazó eszközök elősegíthetik az ötletek kidolgozását, szövegek és tartalmak összefoglalását, átfogalmazását, vagy akár egy üzleti stratégia alapjainak megalkotását, de használatukkal például hibákat is könnyebben találhatunk meg egy programkódban**. Az AI használata során viszont nem szabad megfeledkeznünk arról, hogy az eszközökbe bevitt adatok felett többé nem lesz hatalmunk, miután megnyomjuk a küldés gombot.

A nagy nyelvi modellek (LLM), például a ChatGPT használatakor aggodalomra ad okot, hogy érzékeny adatokat osztunk meg nemzetközi nagyvállalatokkal. Ezek a rendszerek online szövegek felhasználásával hatékonyan képesek értelmezni és megválaszolni a felhasználók kérdéseit. **Azonban minden alkalommal, amikor kapcsolatba lépünk egy chatbottal és információt kérünk, fennáll a veszély, hogy érzékeny adatokat osztunk meg magunkról vagy a vállalatunkról.** Éppen ezért lehet, hogy míg az egyik cég kifejezetten támogatja, mások megtiltják a Chat GPT használatát a munkahelyi eszközökön - erről is beszélgettek Hackfelmetszők – Veled is megtörténhet c. podcastban.



Fontos tudni, hogy amikor egy chatbotnak kérdést teszünk fel, a beírt adatok nyilvánossá válnak. Ez viszont nem jelenti azt, hogy a rendszerek azonnal felhasználnák a tőlünk megszerzett információt másnak adott válaszokhoz. Az LLM szolgáltató vagy partnerei azonban hozzáférhetnek ezekhez az adatokhoz, és **beépíthetik azokat a technológia következő verzióiba.**

Az OpenAI, a ChatGPT mögött álló vállalat bevezette a csevegési előzmények kikapcsolásának lehetőségét, ami megakadályozza, hogy a felhasználói adatokat az OpenAI mesterséges intelligencia modelljeinek tanítására és fejlesztésére használják fel.



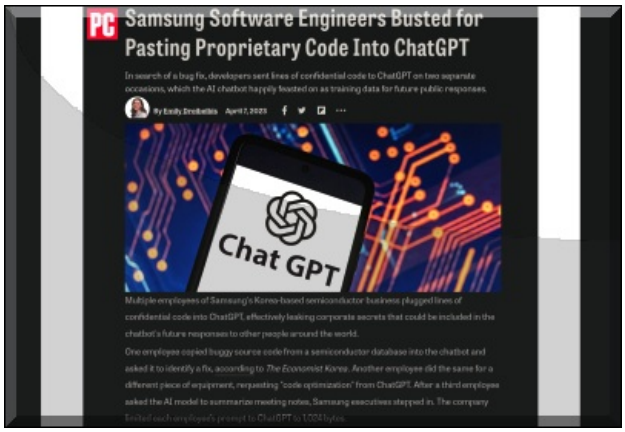
Így a felhasználók nagyobb kontrollal rendelkeznek az adataik felett. **Az első lépés mindig legyen a csevegési előzmények kikapcsolása, amikor alkalmazottként olyan eszközöket használunk, mint a ChatGPT. De még abban az esetben is, ha a csevegési előzményeket kikapcsoljuk, a chatbot külső szerverei minden prompt adatot tárolnak, ezáltal fennáll a veszélye annak, hogy hackerek jogosulatlanul érik el az információkat.** Technikai hibák esetén pedig lehetséges, hogy illetéktelenek hozzáférhetnek a chatbot felhasználók adataihoz – **ahogy ez például 2023 márciusában is történt.**

Hogyan használhatjuk munkavállalóként biztonságosan az olyan platformokat, mint a ChatGPT? Az ESET szakértői összegyűjtötték a leggyakrabban előforduló problémákat, és elmondják, hogyan kerülhetőek el a kockázatok.



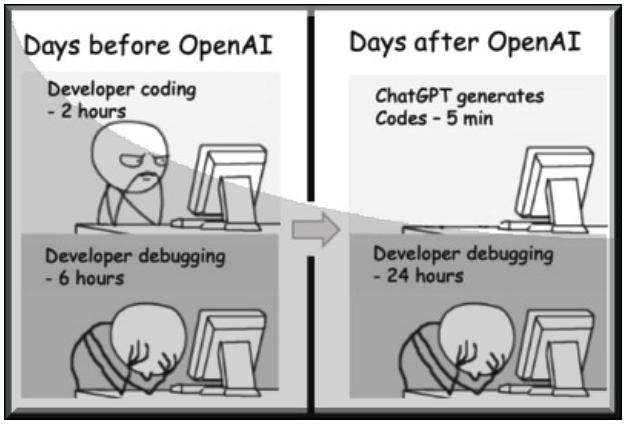
1. Az ügyféladatok felhasználása és megosztása
Az első gyakori hiba, amit a munkavállalók elkövetnek az LLM-ek használata során, hogy **akaratlanul érzékeny információkat osztanak meg a vállalati ügyfelekről.** Hogyan történik mindez? Képzeljük el például, hogy egy orvos beírja a betege nevét, orvosi feljegyzéseit a chatbot rendszerébe, és megkéri az eszközt, hogy állítson össze egy levelet a páciens biztosítótársaságának. Vagy a marketingesek feltöltik a CRM-rendszerükből az ügyféladatokat, hogy az eszköz célzott hírleveleket állítson össze.

A munkavállalóknak érdemes minden alkalommal a lehető legnagyobb mértékben anonimizálni a lekérdezéseket, mielőtt beírják azokat a chatbotokba. **Az ügyféladatok védelme érdekében ellenőrizni és törölni kell minden érzékeny információt, például nevet, címet, számlaszámot a bevitt szövegekből.** A lehető legjobb, ha eleve elkerüljük a személyes adatok használatát, és inkább általános kérdéseket teszünk fel.



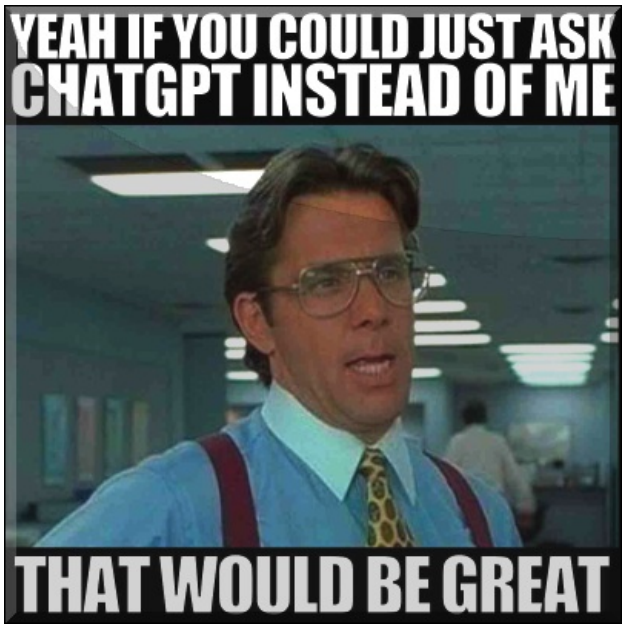
2. Bizalmas dokumentumok feltöltése chatbotokba
A chatbotok hasznos megoldást jelenthetnek nagy mennyiségű adat gyors összegzésére, vázlatok, prezentációk vagy jelentések létrehozására. Ugyanakkor a dokumentumok feltöltése az olyan rendszerekbe, mint a ChatGPT, veszélyeztetheti a bennük tárolt vállalati vagy ügyféladatokat. **Bár csábító lehet egyszerűen átmásolni dokumentumokat, és megkérni az eszközt, hogy készítsen összefoglalókat vagy ajánlásokat a prezentációs diákhoz, adatbiztonság szempontjából ez egy kockázatos módszer.** Mindez vonatkozik a fontos anyagokra, például a fejlesztési stratégiákra, de a kevésbé lényeges dokumentumok - például egy megbeszélés feljegyzései - is elvezethetnek ahhoz, hogy az alkalmazottak felfedik a vállalatuk féltve őrzött tudásanyagát.

A kockázat mérséklése érdekében **a vállalatoknak érdemes szigorú szabályokat hoznia a bizalmas dokumentumok kezelésére, és korlátozni a hozzáférést az ilyen iratokhoz.** Az alkalmazottaknak előbb manuálisan át kell nézniük a dokumentumokat, mielőtt összefoglalót vagy segítséget kérnek a chatbotoktól. Ezzel biztosíthatjuk, hogy az érzékeny információkat, például neveket, kapcsolattartási adatokat, árbevételi adatokat töröljük vagy megfelelő módon anonimmá tegyük a felhasznált iratokban.



3. A vállalat adatainak felfedése a kérések során
Képzeljük el, hogy a hatékonyság érdekében egy vállalat megpróbálja fejleszteni a cég egyes gyakorlatait és munkafolyamatait. Ezért segítséget kér a ChatGPT-től az időmenedzsment vagy a feladatok strukturálása terén, amely során értékes know-how-t és egyéb adatokat ír be a promptba, hogy segítse a chatbotot a megoldás kidolgozásában. Ahogy az érzékeny dokumentumok vagy ügyféladatok chatbotokba történő bevitele, **úgy az érzékeny vállalati adatoknak a promptba történő beírása is gyakori, de potenciálisan kártékony gyakorlat, amely jogosulatlan hozzáféréshez vagy bizalmas információk kiszivárgásához vezethet.**

E probléma megoldása érdekében alapvető gyakorlatnak kell lennie a prompt anonimizálásnak. Ez azt jelenti, hogy soha nem adhatók meg nevek, címek, pénzügyi adatok vagy más személyes adatok a chatbot kérésekben. Ha pedig egy vállalat szeretné elősegíteni, hogy az alkalmazottak biztonságosan használják az olyan eszközöket, mint a ChatGPT, **érdemes sablonként szabványosított kéréseket megfogalmazni, amely szükség esetén minden munkavállalónak rendelkezésére áll**, például: “Képzelje el, hogy xy pozíciót tölti be az xy vállalatnál. Készítsen egy jobb heti munkafolyamatot [egy bizonyos pozíció] számára, amely főként a [feladatra] összpontosít”.



A mesterséges intelligenciát alkalmazó eszközök nem csupán a jövő munkavégzésének eszközei, **már most is a mindennapok részei. Mivel a mesterséges intelligencia és különösen a gépi tanulás területén a fejlődés folyamatos, a vállalatoknak óhatatlanul követniük kell a trendeket, és alkalmazkodniuk kell hozzájuk.**

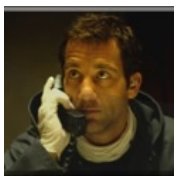
Az adatbiztonsági szakértőtől az informatikai generalista pozícióig **érdemes meggyőződni arról, hogy minden kolléga tudja, hogyan kell biztonságosan használni ezeket a technológiákat anélkül, hogy az adatok kiszivárgását kockáztatnák.**

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: biztonság ai mi mesterséges céges intelligencia munkahely használat vállalati adatszivárgás chatgpt

Ajánlott bejegyzések:








Na de mit adott nekünk a ChatGPT?
Matatás a robotporszívók agyában
A belső ember II.
Kis- és középvállalkozások adatvédelmi incidensei
Ransomware támadás a Nissan ellen

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

856

8 kórház, 30 klinika, 2.5 millió betegadat

2023. december 12. 10:34 - Csizmazia Darab István [Rambo]

A ransomware nem igazán válogat, lecsap mindenhol, sőt **egy idő óta már éppen hogy nagyon is igyekszik az állami szervezetek gyengébben védett szektoraiban érzékeny adatokat kezelő egészségügyi intézmények ellen támadást intézni**.



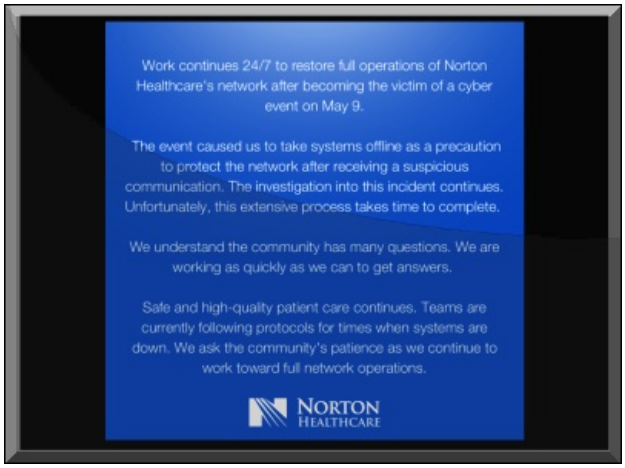
Még ha a Covid kezdeti időszakában úttörő becsszóra ígérték, hogy nem támadnak egészségügyi célpontokat, **amit aztán persze jól nem tartottak be**, ezen a fronton sajnos nem kapott kaptak kíméletet a kórházak sem.

Jó, mutatóba volt néha olyan, hogy a rákos gyerekeket kezelő kórházat ért incidensnél átnyúltak a végrehajtó bűnözők feje felett, és elnézést kérve ingyen dekódoló kulcsot adtak, ám a hosszútávú tendencia azt mutatja, szó sincs itt semmiféle tartós jóindulatú vagy kiváltságos elbánásról.



A statisztikák pedig szépen leleplezik, hogy az egészségügyi intézmények elleni zsarolóvírus-támadások eddig már legalább 77.5 milliárd dollárnyi kárt okoztak. 2016-tól idén október közepéig a zsarolóvírus-támadások miatt az érintett szervezetek átlagosan 14 napra kényszerültek leállásra.

A 10 ezer kórház, klinika vagy más egészségügyi szervezet elleni ransomware támadások során **több, mint 52 millió beteg adat került illetéktelen kezekbe.**



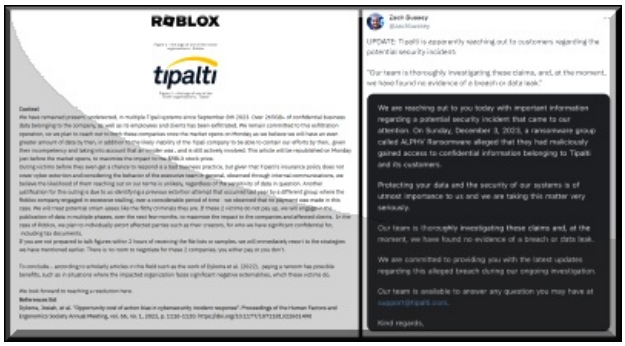
Ezúttal az Egyesült Államokban nyolc kórházat és több mint 30 klinikát üzemeltető Norton Healthcare ismerte el, hogy a még idén májusban elszenvedett ransomware akcióban 2.5 millió betegadatot loptak el a bűnözők.

A behatolás során ügyfél nevekhez, elérhetőségi adatokhoz, társadalombiztosítási számokhoz, születési dátumokhoz férték hozzá, és emellett **jogosítvány és egyéb állami igazolványszámokat, valamint számlaadatokat, sőt digitális aláírásokat is el tudtak lopni.**



A május 7. és 9-e között történt incidensnél **az intézmény nem fizetett váltságdíjat, a nyomozásban pedig az FBI segítségét is kérték. A váltságdíj megtagadása miatt aztán az AlphV/BlackCat ransomware banda május 25-én bosszúból kiszivárogtatta az ellopott adatokat.**

A nagyon érzékeny személyes adatok nyilvánosságra hozatala további testre szabott visszaélések egész sorozatát okozhatja a páciensek számára, míg a kórházi leállások műtétek elmaradásához, adatkezelési káoszhoz, betegek késedelmes orvosi ellátásához vagy a legrosszabb esetben halálához is vezethetnek.



A kórházak mellett a könyvelők sem aludhatnak nyugodtan, a legutóbbi esetnél **szintén az orosz székhelyű AlphV/BlackCat csoport támadta meg a Tipalti könyvelési szoftvercéget, ahol a doxing során ellopott ügyféladatokkal úgy akarnak eljárni, hogy ha a központi cég nem fizet nekik egyben, akkor egyénenként külön-külön betámadják a kikerült ügyféllistán szereplő vállalkozásokat, és őket zsarolják meg közvetlenül.**

Ami az állítólag ellopott 265 GB-nyi bizalmas adat fényében nem igazán hangzik túl biztatóan.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: usa orosz kórház egészségügy klinika könyvelő váltságdíj ransomware blackcat zsarolóvírus doxing alphv tipalti

Ajánlott bejegyzések:


9 millió, bizony, dalolva ment...


Baljós árnyak: fekete macska Karintiában


Ransomware - Fülöp-szigetek, 1:0


Windows frissítés vagy mégsem?



Dallas a pácban

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

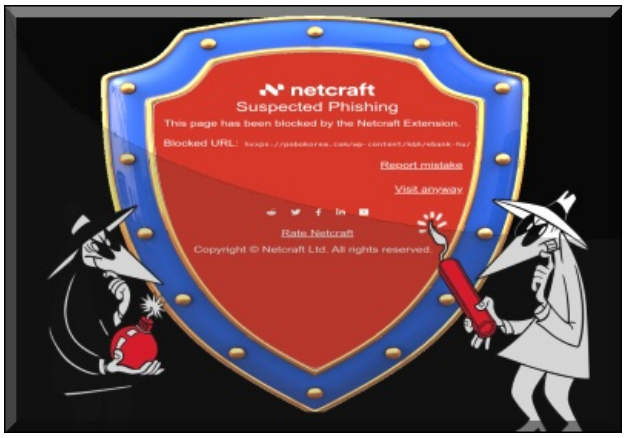
SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

471

Xmas és Top posztok az idén

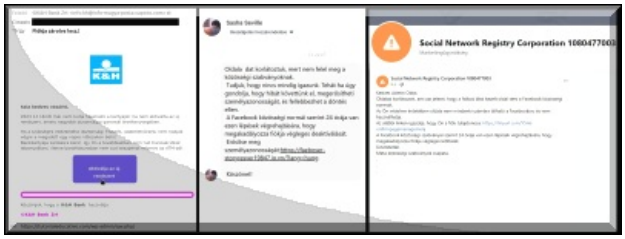
2023. december 20. 14:04 - Csizmazia Darab István [Rambo]

Ha egy jellegzetes díszes címert kellene csináltatni az idei évnek, **valamilyen banki internetes átverés szerepelhetne rajta**. Sokan próbálkoztak átverni, megfertőzni, becsapni, anyagilag megrövidíteni bennünket, és ebben az **olykor elég suta szövegezésű üzeneteknek, valamint a bankok nevében történő telefonhívásoknak** volt óriási szerepe.



Csak egy pár, a napokban befutott példát érdemes megnézni: **a K&H Bank nevében jelzik, hogy zárolják a fiókunkat, aztán a Facebook/Meta nevével visszaélve fiókunk megerősítésére kérnek bennünket** természetes valamilyen kártékony vagy adathalász linkre való kattintással.

Ez a trend jövőre sem fog megfordulni, ezért érdemes mindenkinek nagyobb figyelemmel kezelni a sürgető, figyelmeztető kéretlen leveleket.



És akkor nézzünk rá a 2023-as év posztjainak képzeletbeli dobogójára, mik voltak a legfelkapottabb bejegyzések. **Harmadik helyezett lett 5 ezer megtekintéssel egy Windows frissítésnek tűnő Big Head nevű ransomware kártevőről szóló írás lett.**

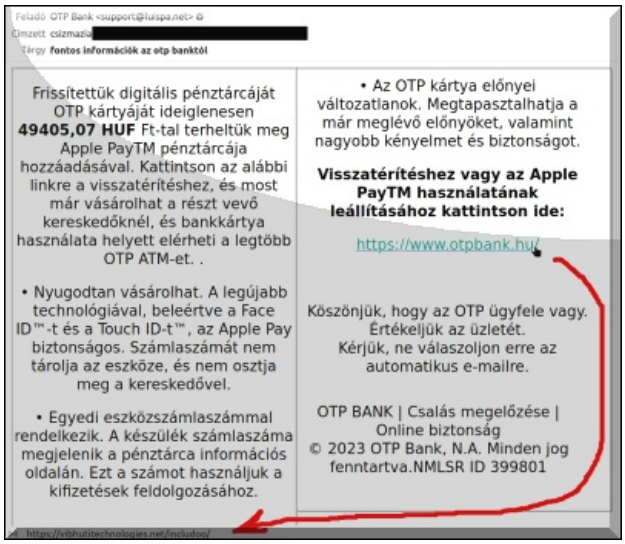


Az **ezüstérmet az MVM nevében küldött gázszámlának látszó átverésről szóló poszt nyakába akasztottuk**, ez lett a második helyezett több, mint 9 ezer megtekintéssel.



És végül, de semmiképp nem utolsó sorban **a világverő győztes 29 ezer megtekintéssel zsákolta be az első helyezést, ahol az volt a téma, hogy egy "fontos információk az otp banktól" tárgysorú üzenetben** arról írtak, hogy ideiglenesen megterhelték a kártyánkat 49 ezer forinttal.

A hivatkozott ok pedig az Apple PayTM pénztárca állítólagos hozzáadása volt, pedig ezt nem igényeltük, nem kértük. **De itt is itt volt a lehetőség a felelőtlen kattintásra: egy link, ami visszatérítést ígért.**



Ezek voltak a 2022-es év leglátogatottabb posztjai, és most **nem is maradt más hátra, mint hogy Kellemes Karácsonyi Ünnepeket kívánjunk minden olvasónknak.**



Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: blog poszt toplista karácsony xmas csalás átverés 2023.

Ajánlott bejegyzések:



[Black Friday és Cyber Monday járja be Európát]



[Azonnali frissítés szükséges a fiók aktiválásához!]



[Csomagot kaptam life...]



[Nő a QR-kódos visszaélések száma]



[Kár érte, kiváló ügynök volt...]

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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

453

Ransomware támadás a Nissan ellen

2023. december 28. 09:31 - Csizmazia Darab István [Rambo]

A Nissan Motor Corporation megerősítette, hogy ausztráliai és új-zélandi belső rendszerei veszélybe kerültek. A hivatalos közlemény szerint **jogosulatlan harmadik fél illegálisan hozzáfért a vállalat egyes hálózati szervereihez.**



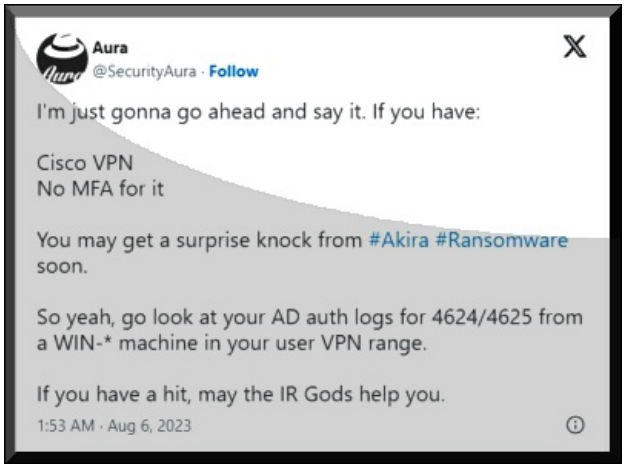
Az Akira zsarolóvírus csoport azt állította, hogy a doxing támadás során nemcsak a belső bizalmas projektinformációkat és titoktartási megállapodásokat (Non-Disclosure Agreement, NDA) tudtak ellopni, hanem a Nissan Australia ügyfeleihez és partnereihez tartozó személyes információkat is.

A vállalat megtagadta a váltságdíj kifizetését, mire a ransomware banda azzal fenyegetőzött, hogy kiszivárogtatja az állítólagos ellopott dokumentumokat.



A támadók állítása szerint 100 GB adatot sikerült zsákmányolniuk, a Nissan állítása szerint még vizsgálják az ellopott adatok körét. **Korábbi tapasztalatok szerint a ransomware csoport általában 200 ezer dollártól 4 millió dollárig terjedő váltságdíjat követel, melynek mértéke mindig a megcélzott szervezet méretétől függően változik**.

A vállalat szerint a helyi Nissan márkaszerviz továbbra is működik, ám figyelmeztetik az ausztrál és új-zélandi ügyfeleiket, hogy legyenek éberek, mert **az ellopott személyes adatok birtokában megtévesztő célzott támadások indulhatnak a Nissan nevében.**



Az Akira bűnözői csapat 2023. márciusában bukkant fel, és a szakértők feltételezése szerint kapcsolatban állnak a hírhedt Conti csoporttal. Eddig nagyjából 180 szervezetet céloztak, elsősorban az Egyesült Államokban és Kanadában. 2023. júniusában az Akira megjelentette ransomware programjuk egy **olyan Linux-változatát, amelyet a vállalati környezetekben széles körben használt VMware ESXi virtuális gépek megcélzására terveztek.**

Az ipari, gyártói körön belül az autógyártók közül már többen is áldozatuk estek, például a Toyota németországi részlegét érintő adatvédelmi incidensnél szintén sikerült személyes adatokat szerezniük. Itt később 260 ezer japán vásárló járművéhez kapcsolódó eszközazonosítót és térképadatot szivárogtattak ki.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: autó nissan váltságdíj adatlopás adatszivárgás ransomware zsarolóvírus doxing

Ajánlott bejegyzések:


9 millió, bizony, dalolva ment...



Ransomware támadás érte az MSI-t


Fordulat ransomware fronton



Ransomware a One Motelben


Baj van Tajvanban

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
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