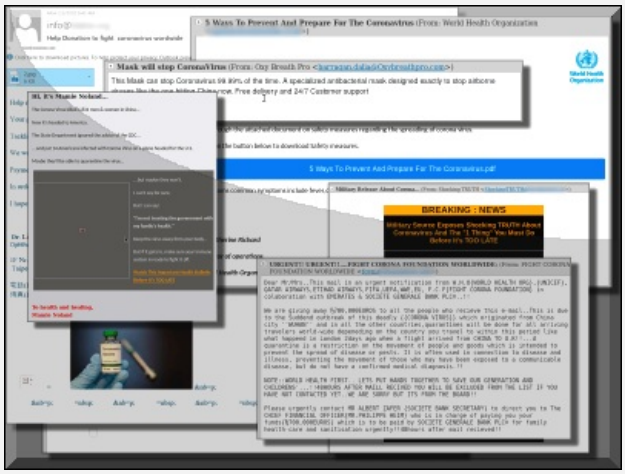
Vakcinás csalások, szevasztok

2021. január 05. 11:31 - Csizmazia Darab István [Rambo]

Meg sem lepődünk, mikor **aktuálisan az elosztás, az előkészített oltási terv menetrendje, a COVID-19 vakcinára való jelentkezés és hasonló dolgok vannak napirenden, addigra természetesen már ez az új csali van a csalók horgán, illetve keringenek ilyesmik nagy számban a neten.**

A járvány kitörés óta több alkalommal is futott már a téma, illetve támadtak ezzel kapcsolatos intézményeket. Emlékezetes, a járvány kitörésének másnapján már maszkokkal kapcsolatos átverések terjedtek, nemlétező vagy túlárazott védőfelszereléseket kínáltak tömegesen weblapok és vaterás szerencsevadászok.

De mi is beszámoltunk arról a **magyar nyelvű, a magyar kormány nevében írt kéretlen levélben érkező átverésről, amelyben a részletes személyes és banki információk megadása után kínáltak fel 150 ezer forintot ismeretlen csalók.**

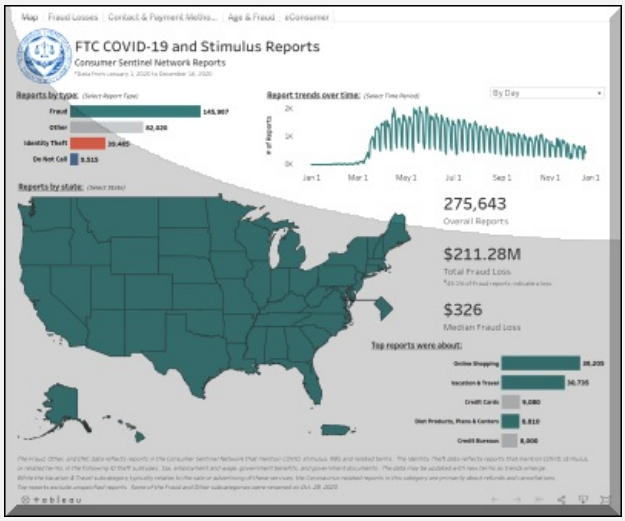


Ami még ennél is **súlyosabb következményekkel járt, az az egészségügyi intézmények elleni tudatos, célzott támadások volt, gyakran zsarolóvírussal igyekeztek pénzt kizsarolni kórházaktól, kutatólaboroktól, illetve az adatlopási kísérletek is kiemelten zajlottak ezeken a helyeken.**

Említhetjük itt az amerikai ExecuPharm gyógyszeripari óriáscéget vagy akár a csehországi Brno Covid-19 centrumát is, **amelyek ransomware incidens áldozataivá váltak.** De ezek mellett számos már kórház, egyebek közt németországi kórházak is áldozatul estek a tavalyi év végén, köztük például a Canton-Potsdam Hospital, a Gouverneur Hospital valamint a Massena Hospital is.

Most 2021-ben a vakcinával és oltással kapcsolatos spameknek jött el a szezonja. Ezekben a kéretlenül üzenetekben azonnali információt, a várakozási listában való "kedvezményes" előrébb jutást, vagy akár feketepiaci felár ellenében azonnali oltóanyagot ígérnek egyes darknetes oldalakon.

Ez utóbbinál a személyes adatok illetéktelen kezekbe juttatása és a kemény pénzlehúzás mellett még az egészségét, vagy akár az életét is kockára teszi az, aki ezzel a hamis vakcina ajánlattal mégis élni próbál.



Az oltóanyag-témával kapcsolatos csalások, visszaélés tömeges terjedése miatt a Szövetségi Nyomozó Iroda (FBI), az Egyesült Államok Szövetségi Kereskedelmi Bizottsága (FTC), valamint az Interpol és az Europol is riasztást adott ki. A próbálkozások egy része adathalász támadások formájában valósul meg, amellyel a lakosságot célozzák meg.

Itt változatos csatornákon: **e-mailben, SMS-ben de akár telefonhívások útján is megpróbálják becsapni az embereket, és rávenni őket részletes személyes adataik, és banki azonosítóik begépelésére, bediktálására annak reményében, hogy ezzel a várólistákon állítólag előrébb juthatnak.**

Az FTC szervezet nyilvánosságra hozott adatai szerint 2020. december közepéig **275 ezer bejelentést kapott a járvánnyal kapcsolatos csalásokról és a személyazonosság-lopásokról. Az incidensekben érintett az áldozatok veszteségei pedig összességében elérték a 211 millió dollárt, ez mai árfolyamon nagyjából 62 milliárd forint,** nem kis summa.

A csalások megelőzéséhez jól tesszük, ha a vakcinával kapcsolatos **naprakész információkért inkább a saját országunkon belüli hivatalos forrásokhoz, illetve egyéni kérdéseinkkel egészségügyi szolgáltatónkhoz fordulunk. Emellett persze nélkülözhetetlen a számítógépünkön a naprakész védelmi szoftver, a frissített szoftverkörnyezet valamint az egészséges gyanakvás** minden hasonló kedvezményes kéretlenül érkező - akár magyar nyelvű - ajánlat esetében is.

1 komment
Címkék: spam vírus fbi csalás átverés oltás ftc járvány phishing karantén adathalászat welivesecurity.com covid-19 covid

Ajánlott bejegyzések:

[Ingyenes Omikron teszt vagy mégsem?]

[Azt mondod Covid19, azt mondom spam]

[Üdvözlünk Sin City-ben]

[Adathalászat - nem középiskolás fokon]

[Nő a COVID-os kibertámadások száma]

Kommentek:

Iván Gábor IGe · vilagnezet.blog.hu 2021.01.06. 08:25:53

Az Isten-mém elleni vakcina ingyenes és már járványszerűen terjed.

Trükkös "Mém" - Szórakoztató tudományfilozófia esszé felvezetője:

A memetika az eszmék darwinizmusa. Ez az írás viszont ideológiailag független, gondolkozni tudó embereknek szól. Aki nem esik ebbe a csoportba, annak nem is javallott olvasni, mert mentális problémákat okozhat.

Richard Dawkins evolúciós biológus Istent egy veszélyes elme vírusként, mémként határozta meg. A meghatározása részben helyes és bizonyított, olyannyira, hogy mára már a gyógymód is megvan rá.

A biológia és a genetika hajnalán a gének sokáig nem voltak bizonyíthatóak, csak logikai következtetésként léteztek, csak a megfigyelések alapján jutottak arra a tudósok, hogy lenniük kell. Aztán persze jóval később meg is lettek. Hasonlóan a mémekre, tehát az idegrendszeri vírusokra jelenleg csak közvetett módon van bizonyíték. Közvetlen nincs és lehet nem is lesz, hiszen az idegrendszerben információ áramlik és itt ugyebár az emberi agyban kellene kimutatni egy "vírust", ami eleve lehet, hogy csak pszichológiai folyamat. A memetika tehát nagyon leegyszerűsítve a biológiai vírusaink másolástani működésének az áthelyezése biológiai síkról pszichológiaira. Egy magyarázó példával:

A világjárványt okozó biológiai korona-19 vírusnak teljesen mindegy, hogy milyen vallású, vagy ateista, vagy nihilista, vagy milyen tanult, vagy tanulatlan embert, személyt fertőz meg. A lényeg az, hogy rávegye egy információs csomag újbóli legyártására és fertőzésre. Ez egy RMS genetikai száldarabka.

Az elme járványt okozó memetikai Isten vírusnak teljesen mindegy, hogy milyen vallású, vagy ateista, vagy nihilista,vagy milyen tanult, vagy tanulatlan embert, személyt fertőz meg. A lényeg az, hogy rávegye egy információs csomag újbóli legyártására és fertőzésre. Ez főként az Isten szó. ... de mi is "Isten" tudományosan?

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

SIM-csere itt, átverés ott

2021. január 07. 11:22 - Csizmazia Darab István [Rambo]

Egyre sűrűbben fordulnak elő **úgynevezett SIM swap csalások**, 2015 óta jelentősen, négyszeresére nőtt az ilyen típusú támadások száma, és ma már bárki a csalók áldozatává válhat. A kiberbűnözés ezen típusa egy **olyan kifinomult módszert takar, amelynél első lépésben a gyanútlan és sok esetben óvatlan felhasználótól célzott adathalászattal szereznek meg érzékeny személyes adatokat. Ezek birtokában azonban jelentős anyagi károkat képesek okozni.**

2020-ban a média két hazai esettel is mélyebben foglalkozott, melyekben több tízmillió forintos összegeket csaltak ki az áldozatoktól. Ezek jellemzően úgy kezdődnek, hogy az áldozat telefonszáma elnémul. De hogyan is működnek a SIM swap csalások? SIM-eltérítésnek, SIM-megosztásnak, **SIM-cserének is hívják a kiberbűnözésnek ezt a típusát, melynek lényege, hogy átveszik az irányítást az áldozat mobiltelefon előfizetése felett.**

Annak érdekében, hogy sikerrel járjon a támadás, a kiberbűnözők először **célzottan adatokat gyűjtenek a kiszemelt áldozatról, sokszor éppen a saját maga által publikusan megosztott információmorzsákra támaszkodva. Az áldozat személyes adatai az ismert adatszivárgásokból, illegális kémprogram telepítéséből vagy olyan megtévesztéses pszichológiai manipulációkból (social engineering) is származhatnak, mint például a netes és a telefonos adathalászat, ahol közvetlenül a célpontból csalják ki az érzékeny információt.** Így megszerezhetik többek között jelszavainkat, felhasználóneveinket, számlavezető bankunk nevét, a folyószámlaszámunkat vagy éppen születési adatainkat, édesanyánk nevét, lakcímünket, személyazonosító okmányaink számát.

Amikor már elegendő személyes információ van a kezében, a csaló kapcsolatba lép a kiszemelt áldozat mobiltelefon-szolgáltatójával, és a megszerzett személyes adatok segítségével megszemélyesíti a telefon valódi tulajdonosát. **Az ügyfélszolgálaton dolgozó munkatársat megkéri, hogy a telefonszámát a kiberbűnöző tulajdonában lévő másik SIM-kártyára vigye át. A csaló általában arra hivatkozik, hogy a telefonját ellopták vagy elvesztette, esetleg más méretű SIM-kártyára van szüksége.**

A SIM swap csalásnál úgy veszik át az irányítást a telefonszámunk felett, hogy **a bűnözővel még csak nem is találkozunk. Amint a fenti folyamat befejeződött, az áldozat azonnal elveszíti a hozzáférését a mobilhálózathoz és a saját telefonszámához, telefonja elnémul, és ezután már a támadóhoz futnak be hívásai és szöveges üzenetei.**

Az ilyen típusú támadások esetében általában az a cél, hogy hozzáférjenek a célpont online fiókjaihoz. A csalók így óriási pusztítást képesek végezni az áldozat virtuális és magánéletében, beleértve akár a bankszámláinak kiürítését is. Beléphetnek az áldozat közösségi média fiókjaiba is, és olyan privát beszélgetéseket, érzékeny adatokat tartalmazó üzeneteket tudnak letölteni, melyek hosszútávon szintén negatív hatással lehetnek az áldozat életére. Akár közzé is tehetnek a nevében sértő üzeneteket, állapotjelentéseket, melyekkel szintén nagy erkölcsi károkat okozhatnak.

A kiberbűnözők kifejezett célja lehet a pénzszerzés: mivel hozzájuk érkeznek be az áldozat telefonhívásai és szöveges üzenetei, **megkapják a banki oldalakon kért, kétfaktoros hitelesítéshez szükséges kódokat is, melyekkel**

hozzáférhetnek a bankszámlájához. Magyarországon 2020-ban két, nagy port felvert eset is történt SIM-cserés lopással: az egyik esetben 30 millió, másiknál 51 millió forintot tüntettek el az áldozat bankszámlájáról ezzel a módszerrel, ingatlan vásárlási ürüggyel. Szakértők szerint - **részben a 2020-ban bevezetett azonnali utalási rendszer miatt - egyre több ilyen jellegű átverésre lehet majd számítani.**

Hogyan védjük meg magunkat? Az ESET szakemberei azt tanácsolják, hogy minél kevesebb információt osszunk meg magunkról a közösségi média oldalakon, ne tegyük közzé sehol a teljes nevünket, címünket és telefonszámunkat. Védjük a magánéletünket, ne osszuk meg, hogy merre járunk, miket szoktunk csinálni. A csalóknak valójában elég három adatunkat ellopniuk és máris képesek eltulajdonítani a személyazonosságunkat - ráadásul sokak esetében ez a három adat a Facebook profilon is megtalálható.

- A kétfaktoros azonosítás kapcsán is érdemes más lehetőségekben gondolkozni, nem csak a szimpla SMS és a telefonhívások szolgálhatnak erre a célra, hanem használhatunk dedikált hitelesítési alkalmazást vagy speciális hardveres hitelesítési kulcseszközt is.

- Az adathalász e-mail szintén népszerű módszer arra, hogy a kiberbűnözők bizalmas információkat szerezzenek. Ezt leggyakrabban úgy érik el, hogy valamely megbízható intézménynek adják ki magukat, bízva abban, hogy a potenciális áldozat gondolkodás nélkül válaszolni vagy kattintani fog a hamis üzenetre. Bár az adathalász e-mailek közül sokat képesek a spamszűrők azonosítani és blokkolni, azt sem árt tudni, hogy milyen árulkodó jelekről ismerhetjük fel, ha éppen ilyen üzenetet kaptunk.

- A távközlési vállalatok egyre több lehetőséget biztosítanak a megfelelő védelemhez: hitelesítést kínáló PIN-kódok, jelkódok és további biztonsági kérdések formájában: nézzünk utána a szolgáltatónk által kínált plusz biztonsági lehetőségeknek.

- A bankok azt tanácsolják, hogy **kérjünk minden pénzmozgásról azonnali értesítést, így ameddig él a telefonunk, rögtön értesülhetünk minden eseményről**, arról is, ha ellopták a banki adatainkat, és a bűnözők tesztelik azok helyességét egy kis összegű átutalással.

- Ha azt tapasztaljuk, hogy **a telefonunk váratlanul elveszíti a kapcsolatot a hálózattal, csak segélyhívást tudunk róla indítani, haladéktalanul értesítsük erről a bankunkat és a mobilszolgáltatónkat.**

34 komment
Címkék: mobiltelefon csalás átverés támadás csere sim adatlopás személyiséglopás mobilszolgáltató simswap

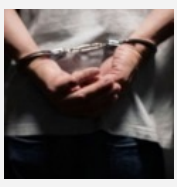
Ajánlott bejegyzések:


Lakásvásárlás, de csak ha OTP-s vagy

Ha eljön a személyiségtolvaj


A bankos mindig kétszer csenget...


Ingyenes Omikron teszt vagy mégsem?


Szerva itt, letartóztatás ott

Kommentek:

T.Jani 2021.01.08. 10:32:08

Egy ennyire bonyolult és megszervezett csalás viszont nem azt a minimálbért kereső embert fogja érinteni, akinek a hónap végén pár ezer forint van a számláján.
A bankomnál ugyan már van hardveres azonosítás is, de ekkora energiát befektetve azt is simán ellopják vagy kicserélik egy hasonlóra, ami addig fel sem tűnik amíg használni nem akarja az ember.

Válasz erre

octy 2021.01.08. 14:53:00

10-15 évvel ezelőtt is egészen komoly és ügyfélpanaszokat is generáló szigorúság volt már a szolgáltatók SIM csere folyamatában. Csak úgy bemondásra nem cseréltek SIM-et. Most hová tűnt ez? Olvastam olyan esetet amikor céges számoknál cseréltek SIM-et.
Honnan vittek személyit és aláírási címpéldányt? Mert ha ilyenből hamisat visznek és azt valaki meg is nézi vagy egyáltalán nem visznek, akkor buknak is vagy elküldik őket a 'csába. Annál az esetnél nem volt szó arról, hogy a személyit is ellopták volna hiszen nem is érintkeztek az áldozatokkal csak távolról.

Amúgy én arra tippelek, hogy a partner üzletek - amelyeket vállalkozó visz, nem a szolgáltató - ahol nem a szolgáltató alkalmazottai dolgoznak hanem a vállallkozó 4 órára bejelentett vagy be sem jelentett, tegnap még árufeltöltő, holnap már pizzafutár embere, ezekre a szabályokra magasról tesznek.

Nagy a fluktuáció mert nem kapnak rendes fizetést, nem is ismerik a szabályokat mert nincsenek ott annyi ideig hogy megtanulják a folyamatokat vagy a sokadik dolgozó generáció már nem adta át a tudást csak megmutatta, hová kattintson az új ember aztán ment egy jobban fizető helyre dolgozni. A biztonsági előírások meg valahol elmaradtak pár csapattal korábban.

A másik lehetőség hogy a SIM cserét elvégző dolgozó is benne van a buliban. Ezt is inkább a minimálbérrel felvett partner üzleti dolgozóknál tudom elképzelni, bár már a szolgáltatók a saját dolgozóikat is mesteri szinten szívatják a különböző kvótákkal amelyek nem teljesülése esetén kb. minimálbért kapnak.

Válasz erre

So No 2021.01.08. 16:12:01

Itt Malajziaban mar evek ota nem kodot kuld a bank. A bank appjara erkezik uzenet, ahol jova kell hagyni a tranzakciot. Az appba meg ujjlenyomat azonositassal lehet belepni.

A tobbi helyen meg goggle authenticatort is hasznalok...

Nem mellekesen itt SIM kartyaval kapcsolatos dolgokat csak szemelyesen lehet intezni. El sem tudom kepzelni, hogy odahaza telefonon is lehet "csak ugy".

Válasz erre

steery 2021.01.08. 16:25:35

Ebben az egészben az a legnagyobb vicc, hogy közben meg minden évben azzal zaklatják a telefon tulajdonosokat, meg a bankszámla tulajdonosokat, hogy be kell menniük adatfrissítésre meg ellenőrzésre, hogy meggyőződjenek róla, még mindig nem vagyunk terroristák, nem offshoreozunk, nem végzünk pénzmosást és más illegális tevékenységeket. Mintha ezt így, egy adminisztrációs ellenőrzéssel ki lehetne szűrni. :-D

Egy védelem van csak a kiberbűnözéssel szemben. Nem kell használni a digitális technológiákat. Mindent csak személyesen szabad intézni és csak készpénzzel szabad fizetni. A telefont meg csak telefonálásra szabad használni, az internetet meg csak ilyen cikkek olvasására és kommentelésére. :-D

Válasz erre

ZSt0m 2021.01.08. 17:41:18

@So No: Évekkel ezelőtt olvastam egy hasonló cikket(?) blogot(?) aztán kisült, hogy az USA-ban lehet SIM ügyeket intézni telefonon(küldenek postán egy másikat) szerintem Magyarországon erre nincs lehetőség csak személyesen.Egy androidos app amúgy mivel biztonságosabb mint egy telefonra küldött SMS?Szerintem semmivel.

Válasz erre

Denise Hogyisdugják 2021.01.08. 20:51:20

@So No: itt is van app-al történő hitelesítés, pl kh bank. a pénzmozgásról történő üzenet ostoba ötlet, ha swap-olják a sim-et, eleve nem is kapok üzenetet... céges sim kicsit nagyobb biztonságot nyújt, főként ha aláírók vagyunk a cégben. engem is mindig felhív a helyi tkom-nepper, ha valamelyik niggerem bemegy céges sim-mel variálni :-)

Válasz erre

theman 2021.01.09. 07:39:31

Ez az "értesítsük a szolgáltatót" egy vicc.
Én egyszer szerettem volna letiltani a bankkártyát, kellett hozzá a bankkártya, annak száma, a szerződés száma, na meg az e-pin kód.(nem bankkártya pin)
Nem tudom ezeket ki tartja utazás közben magánál.

Válasz erre

Zsoti 2021.01.09. 07:50:26

@ZSt0m: pl az app telefonfüggő. Csak a bankban lehet új telefonra telepíteni. Ahhoz meg személyesen ott kell lenned.

Válasz erre

qwertzu 2021.01.09. 11:56:12

Ami a cikkből kimaradt:

Meghatalmazással csinálják.

Válasz erre

eßemfaßom meg áll · https://antivaxxer.blog.hu 2021.01.09. 12:35:12

@steery: "hogy be kell menniük adatfrissítésre meg ellenőrzésre, " a te párhuzamos univerzumodban lehet, a mi valóságunkban le kell ülni a gép elé és 1 perc elett elküldeni egy 5 soros adatlapot. És persze csak ha prepaid vagy, számlásnál ez sincs.

Válasz erre

Tesztelo.hu · http://www.tesztelo.hu 2021.01.09. 13:22:56

Engem sokkal jobban érdekelne az a minapi eset, amikor 16 000 mobilt "emuláltak", és az emulált telóra jött meg az azonosító SMS. Nem kellett hozzá semmilyen SIM csere (nyilván nem is tudtak volna 16 000 SIM-et cserélni). Na, azt hogyan csinálták, hogyan lehet mobilt "emulálni"?

Válasz erre

steery 2021.01.09. 15:31:40

@eßemfaßom meg áll: Az én valóságomban ez (még) nem lehetséges. Muszáj személyesen bemenni, nem lehet gépen keresztül intézni a dolgot. Küldenek róla előre értesítőt sms-ben. Persze lehet, hogy már megváltoztatták az eljárást, csak még én nem értesültem róla, mert messze van még a következő ilyen zaklatós-alkalom.

Válasz erre

Vén motoros 2021.01.09. 16:41:07

@So No: Már akinek okostelefonj aven. Nekem internetképtelen butatelefonom, arra csak SMS küldhető. (Nem, mintha nem tellene okostelefonra, csak nincs rá szükségem.)

Válasz erre

Denise Hogyisdugják 2021.01.09. 16:48:08

@Vén motoros: vénségére ne legyen már ilyen... sokaknak nem telik rá, mégis ott az új szifon vagy samu :-) az sem szégyen, ha nem telik rá. nekem sem telik saját yacht-ra az adrián mégsem szégyellem magam miatta.

Válasz erre

Vén motoros 2021.01.09. 17:10:20

@Denise Hogyisdugják: Már kaptam többször is ajándékba okostelefont, de továbbajándékoztam. Az én forgalmam átlagban heti egy teefon (akkor is engem hívnak), és heti 4-5-6 SMS -ezek e.banki utaláshoz szükséges kódokat tartalmaznak. Utcán nem netezek.. Minek? Otthon a 200Mbit/sec-os drótos netemen lógok, havi 40-50 gigabájtos forgalommal. Van vonalas (valójában IP-VoIP) telefonom, a kényelem érdekében egy bázisállomással és két DECT mellékállomással, hogy lakáson beül ne legyek helyhez kötve. De a drótoson se szeretek telefonálgatni. Inkább napi

jópár e.mailben tartom a kapcsolatot kevés számú baráttal-rokonnal.)

Válasz erre

kárárámaispj 2021.01.09. 21:03:24

@steery: De, már 2 éve is lehetett neten meg telefonon is igazolni magad.

Válasz erre

kárárámaispj 2021.01.09. 21:07:35

Egyébként nem értem a cikket. Tehát megtudják a nevem, címem, anyám nevét, esetleg igazolványszámomat. Szólnak a nevembe a szolgáltatónak, hogy kéne másik sim. Az meg kiküldi. Addig az én telefonom nem működik. Ez nem tűnik fel nekem? Pár nap a postázás. Ha meg bemennek a bótba, akkor ott nem elég anyám nevét bemondani, kell mutatni igazolványt.

Aztán. Ha ott van náluk az én simem, (én meg vagyok valami lakatlan szigeten és nem tűnik fel, hogy senki nem hív, senkit nem tudok hívni, és egyáltalán nem működik a telefonom) akkor ebből hogyan lépnek be a banki appba?

Válasz erre

Konyvtaroslany 2021.01.09. 22:33:12

@kárárámaispj: Mondjuk úgy, hogy ha a karibi luxusapartman előtt a tengerparton héderelve azt veszed észre, hogy nem működik a gsm alapú hálózaton a barangolás, attól még a luxusapartman wifije még elérhető és van net.

Válasz erre

kárárámaispj 2021.01.10. 02:06:05

@Konyvtaroslany: Úhüm. Bocs, de ez az amikor a kisember elképzel dolgokat.
A karibi apartman előtt is szoktak hívni. Meg kapok sms-t.

Válasz erre

So No 2021.01.10. 05:41:49

@Vén motoros:

Akkor itt Azsiaban eleg nehezen boldogulnal. Igy a COVID idokben pl. sok uzletbe be sem mehetnel. A kormany altal hitelesitett appal kell leolvasni a QR kodot. Van ahol kitesznek egy fuzetet, hogy ird bele az adataid, de sok helyen nem.

Tomegkozlekedeshez nem berlet van, hanem touch n' go card. Mobil app nelkul eleg maceras feltolteni. (Talalnod kell egy automatat, vagy egy MyNews uzletet) De mar ott is lehet QR koddal fizetni az utazasert....

www.youtube.com/watch?v=XALOxKGloK0

Egyebirant sokkal kenyelmesebb QR kod leolvasasaval fizetni a kasszanal a boltokban is.

www.youtube.com/watch?v=2hSQp7EJMNA

Sot. A banki atutalas is megy QR koddal. A masik fel a banki appjaval general egy kodot, te a sajat appodban beirod az osszeget, leolvasod az o kodjat, es kesz az utalas.

www.youtube.com/watch?v=-33gchCCt5A&feature=emb_logo

Igazabol nem latom, hogy miert ne lenne valakinek szuksege "okos"telefonra. Bar en 1986-ban kezdtem matek tagozaton informatikat tanulni, es abbol is elek, szoval elegge elfogult vagyok.

Válasz erre

Serény Vélemény 2021.01.10. 11:09:46

@So No: hát... amikor a modellnek látszó lány a riksát kifizette a QR -os app-pal a reklámfilmszerűségben, akkor azér' hangosan vinnyogva röhögtem! :-)

Válasz erre

kárárámaispj 2021.01.10. 11:19:24

@So No: Oszt ha egyszer elmegy a net, akkor mindenki marad otthon.

Válasz erre

steery 2021.01.10. 11:26:20

@kárárámaispj: Persze, lehetett, csak én nem erről beszélek. Hanem arról, amikor elkérik a személyidet, lakcímkártyádat és összehasonlítják a gépben lévővel.

Válasz erre

So No 2021.01.10. 12:32:48

@kárárámaispj: Ez valoban jo indok. Ne hasznaljuk a netet, mert elmehet.

Válasz erre

So No 2021.01.10. 12:34:08

@Serény Vélemény: Attol mert reklam, meg valoban igy megy. Barhol lehet igy fizetni, meg a piacokon is.

Válasz erre

Serény Vélemény 2021.01.10. 13:01:32

@So No: Mi itt, a nagyon fejlett Európában úgy gondoljuk csak Európa és csak európaiak fújhatják a passzátszelet. Közben... EZEK SZERINT Malajziában - nagyjából minden, ami itt nekünk, magyaroknak elképesztő problémákat okoz - nagyjából hipermodern.
(Lásd még: BKV elektronikus jegyrendszer itt vs QR-kódos fizetés ott.. :-)

Válasz erre

Serény Vélemény 2021.01.10. 13:14:24

Egyébként pedig: az üzlet az mindig és csak és kizárólag akkor üzlet, ha a benne részt vevők tudhatják azt, hogy a másiknak - a partnernek - pontosan mi a HASZNA az üzletből.
ÉS garantáltan átverés, ha nem lehet sehogy kideríteni, hogy a másiknak mi az üzletben levő érdeke, mi a profit része belőle. (Nem azt mondtam, hogy "mennyi", hanem hogy "mi").
Pl. túl olcsón árulnak valamit, aminek az értéke ránézésre is nagyobb, mint az elkért vételár.
DE nincs egy normális fénykép a lakásról a hirdetésben.
Nagy értékű ingatlant nem ingatlanközvetítőn keresztül akarnak _gyorsan_ eladni, áron alul.
Jelentős pénzösszegről való döntésre nem hagynak időt.

A postban említett csalásokban elsősorban nem a (telefon) szolgáltatók részéről volt a biztonsági rés, hanem az átvert emberek óvatosságának a hiánya okozta elsősorban a csalók sikerét.

Válasz erre

So No 2021.01.10. 14:00:29

@ZSt0m: Az sms-ben kuldott kodot eleg sok modszerrel meg lehet szerezni. Ha az appomra erkezik egy uzenet, be kell lepnem az appba, es jova kell hagynom. Nem egy kodot kuldenek, hanem FIZIKAILAG kell csinalnom valamit. Mint minden, ez is "feltorheto", de sokkal kisebb a valoszinusege, hogy pl. olyan program kerul a telefonomra, amelyik be tud lepni a banki appba, es "gombot nyomkod".

Válasz erre

So No 2021.01.10. 15:52:59

@Serény Vélemény: Amikor 2013-ban kikoltoztunk en is azt hittem, hogy kb. olyan allapotok vannak, mint Sandokan idejen. Aztan teljes sokk volt.

52km MRT-halozatot 2015-ben kezdtek epiteni. 2017-ban atadtak az elso felet, tavaly az egeszet.

www.youtube.com/watch?v=gItS2GYn39Q

Az azonnali banki atutalas itt mar 2013-ban megvolt. Kikoltozesem utan az egyik magyar kollegamtol kellett penzt kernem, es szombat este egy perc alatt atutalta. Hetvegen, este!!!

A mallok eleve tobszoros meretuek az othoniakhoz kepest, es tobb mall van osszekotve alagutakkal, hidakkal. Amugy is imadnak hidakat epiteni, az utcakat teljesen befedni a nap es az eso miatt.

ime

www.youtube.com/watch?v=DidjsUP_Ju8
www.youtube.com/watch?v=dAp814V8ZlM&t=0s
www.youtube.com/watch?v=pdPYwM6Erh8 (kb 8:00-nal latszik a teto a jarda felett.)

Van ahol tobb kilometernyi buszvonalat tettek fel kulon hidakra

www.youtube.com/watch?v=98iq3IiRJ7o

Amikor kijottunk, akkor kezdtek el epiteni a KL ECO CITY-t. Csak hat ev kellett hozza, hogy atadjak.

www.youtube.com/watch?v=c95MMolh-pI

Az olyan aprosagokrol, mint ahogyan egy kozkorhaz kinez, mar nem is erdemes beszelni. Amig az ember nem jon el azsiaba, el sem tudja kepzelni. Az elet pedig annyira olcso, hogy... Csak ket pelda.

A fizetesembol kb. 14 EZER kilometert tudok taxizni!
Atszamitva kb. 110 ezerert berelek egy haromszobas apartmant. A hazakhoz itt alapfeltszereles a konditerem, a szauna, a medence, kozert, portaszolgalat stb. stb. A mi kondonk raadasul mar "oreg", mert tobb mint tiz eves....

www.propertyguru.com.my/condo/riana-green-east-636

Szoval nem ertem, miert mindenki az EU-ban akar szerencset probalni.

Válasz erre

Gma002 2021.01.10. 21:00:03

Január 8-tól A netbanki belépéshez az OTP SMS-ben küldi ki az "elfelejtett" jelszó helyett az újat az aláíráshoz rögzített telefonszámra. Eddig legalább a jelszó kicsit védett a SIM-cserés támadástól. Mostantól akinél a lopott (mobilszolgáltatótól kicsalt, új) SIM kártya (vagy eSIM), azé a számlán lévő pénz.

Válasz erre

Vén motoros 2021.01.10. 22:07:35

@So No: Ha már itt tartunk, én 25 évig voltam a saját villamos tervező Kft-m autodidakta rendszergazdája. Építettem egy 4 munkaállomásból, dedikált printszerverből álló peer-to-peer hálózatot, ahol a printszerveren HP plotter, A3-as HP printer-plotter és A4-es HP OfficeJet, valamint 3db. HP A4-es laserjet lógott. Vírusunk nem volt a 25 év alatt, kivéve egy Office Script-vírust, amit a kolléganőm gyereke hozott be, de azt is megfogtam. Amúgy a villamosmérnökség mellett Híradásipari Technikus is vagyok. ENNEK ELLENÉRE nincs szükségem okostelefonra.
Ezek szerint te azt sem érted, amikor két jó állású, magas egzisztenciájú vezető értelmiségi lemegy egy kies tanyára, építenek egy modern újkori vályogházat,zZérus energiafelhasználással, napelemekkel, és kecskéket nevelnek, kecskesajtot készítenek, Robinson gyerekeket nevelnek. (Akiknek valószínűleg nem nőtt a kezéhez az okostelefon, és garantáltan nem lesznek LMBTIQ-k. (És nem a kecskék miatt...)
Tudod, kinek a pap, kinek a papné, nekem a pap lánya!
Na, a BUTATELEFON az én tanyám, kecském, kecskesajtom.

Válasz erre

So No 2021.01.11. 01:11:02

@Vén motoros: Csak ket dolog.

1. Az en tervem egy Balaton kozeli kishaz, konyhakerttel, tavol az emberektol!

De amig egy nagyvarosban vagyok fejelesztomernok, addig KELL hasznalnom ezeket a dolgokat. Es mivel itt letjogosultsaga van, igy hasznalom is oket.

2. Pontosan tisztaban vagyok azzal is, hogy a net nem aldast hozott az emberisegre, hanem el fogja pusztitani. Eleg megnezni a sok onjelolt tudost, aki mindenfele temaban esz nelkul nyilatkozik. En 1990-ben a SOTE AOK-n kezdtem, jartam a kozgazra, vegul BME-re es informatikus lettem. Ezekben a temakban tobbe-kevesbe otthonosan mozgok, de meg igy sem merek "kinyilatkoztatni".

Nemreg pl. azt probaltam egy "elet iskolajat" vegzett kommentelonek elmagyarazni, hogy 20 evvel ezelott, DNS szekvenalassal evekig is eltartott egy virusgenom felterkepezese, ma mar par honap, igy nem meglepo, hogy egy oltoanyagot ki lehet fejleszteni par honap alatt. ELBUKTAM. Annyira idiota, buta reakciokat kaptam, hogy nem tudtam ra reagalni.

Szaz szonak is egy a vege. Egy nagyvarosban igenis kell ezeket a vivmanyokat hasznalni. Eleg felretenni, ha mar az ember megengedheti maganak, hogy ne hasznalja. (Bar pl. en imadok turazni, a hegyekben bringazni, es egy terkepapp akkor is jol jon...)

Válasz erre

Vén motoros 2021.01.11. 01:38:49

@So No: "De amig egy nagyvarosban vagyok fejelesztomernok, addig KELL hasznalnom ezeket a dolgokat. Es mivel itt letjogosultsaga van, igy hasznalom is oket."

Na, itt van a kutya elhantolva. Te egy nagyvárosban vagy fejlesztőmérnök, én pedig egy nagyvárosban vagyok NYUGDÍJAS, mégpedig "nyugállományvab", vagyis nem dolgozom. Sosem éreztem rá készetést, hogy közvetlenül az AutoCAD munkaállomástól vigyenek ki Szent Mihály lován a Farkasréti temetőbe. Na, EZÉRT nem szükséges nekem az okostelefon.
(Annyit az okosságról, hogy van, ugye, a SMART személyi igazolvány, chippel. Mindenféle okosságra jó. De én olyan személyi igazolványt kértem, amely a halálomig érvényes. Ki is állították 2077-ig szóló érvényességgel, mert ugye, a számítógép nem ismer olyat, hogy mindhalálig. (Megjegyzem, a 98 éves anyám - még Kádár alatt kisállított - keményfedeles, piros, sarló-kalapácsos személyije még ISMERT olyat, hogy mindhalálig), viszont kiderült, hogy "örök" személyi NEM LEHET CHIP-s, mert a beépített chipest 6 évenként újra kell cserélni. Biztos kopik az EPROM vagy EEROM?

Válasz erre

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2021.01.13. 11:37:21

A Telenor elég jól áll a dolgokhoz, szimpatikus a hozzáállás:

"Tájékoztatjuk, hogy Üzleti előfizetők esetén a kártyacseréhez aláírási címpéldányra van szükség.
Ezen kívül abban az esetben, ha:
A SIM kártya a helyszínen van, és működőképes / egyértelműen beazonosítható állapotban van:
Elegendő a normál cégszerű meghatalmazás vagy az eljáró személy / rendszereinkben regisztrált kapcsolattartó beazonosítása.

Ha a SIM kártya nincs a helyszínen vagy megrongálódott / nem egyértelműen beazonosítható, és
nem az eljáró személy / Telenornál regisztrált kapcsolattartó jár el személyesen a kártyacsere, kártyapótlás során:
Kizárólag KÖZJEGYZŐI meghatalmazást fogadunk el."

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

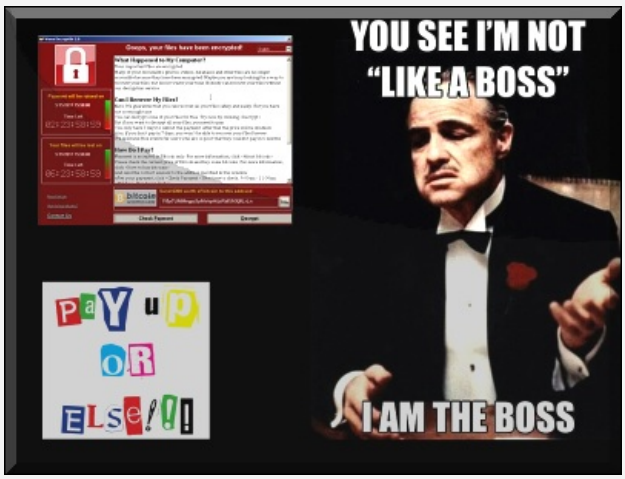
accountz

Belépés
Regisztráció

Ransomware a csúcs felé tör

2021. január 13. 11:27 - Csizmazia Darab István [Rambo]

2013. óta van velünk a ma ismert formájában a zsarolóvírus. A korábbi sikeres (1989-es AIDS tájékoztató floppy, 1995. DOS-os OneHalf) és kevésbé sikeres (2005. GP Code) **elődök után a CryptoLocker rúgta be az ajtót, ami aztán tárva-nyitva maradt** és kaptunk a nyakunkba Cerbertől, CryptoWall-tól kezdve WannaCryptoron át Locky-t, CTBLocker-t, NotPetya-t, Ryuk-ot, valamint TeslaCryptig mindent IS.



Most nem a ransomware történelmével, vagy éppen a technológiai fejlődésével fogunk foglalkozni, hanem **sokkal inkább a terjesztők rendre megújuló stratégiáját emeljük ki, amelyben szintén tapasztalható evolúciós ugrás, ám ebben sok örömet nem lelünk, ugyanis célzottan azokon a kényes pontokon igyekeznek támadni bennünket, mindig éppen ott, ahol az a legjobban fáj.**

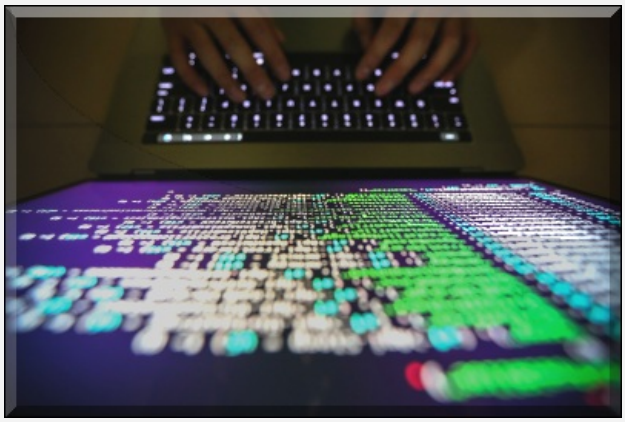
Ha az alap 2013-as CryptoLockert nézzük, spam üzenetekben, fertőzött weblapokon keresztül terjedt, és nem kifejezetten irányult még konkrét célcsoportra, **inkább csak a haszonszerzési modell úttörője volt, és mindenre lőtt, ami mozgott.**

A támogató egyéb kártevőcsaládok aztán idővel kezdtek a mainstream zsarolóvírus ágak alá dolgozni azzal, hogy hatékonyan segítették a ransomware károkozását a korábbi biztonsági mentések célzott törlésével.

A későbbi ransomware kártevő variánsok pedig már sokszor magukba integrálták ezt a feladatot, **és elindulásakor törölték a számítógépes biztonsági árnyékmásolatokat (Shadow Volume Copy), a rendszervisszaállítási pontokat, illetve felkutattak és megkíséreltek leállítani bizonyos kulcsfontosságú rendszerfolyamatokat, például vírusvédelmi, virtuális géphez tartozó, távoli felügyeleti eszköz, illetve hálózati menedzsment** rendszerekkel kapcsolatos processzeket.

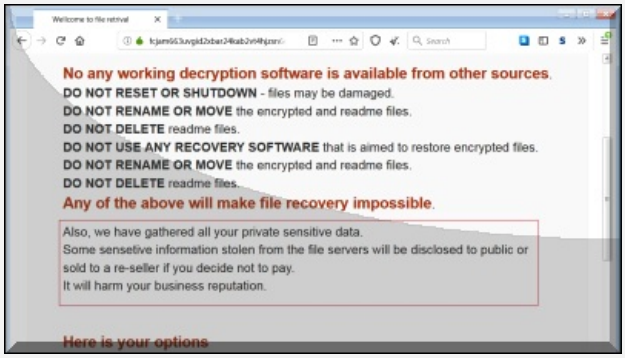
Ha **a nyomásgyakorlás pszichológiájára fókuszálunk**, akkor egy idő után már látszott **az igen tudatos célválasztás: államigazgatás területei, egészségügyi intézmények benne kórházakkal, vagy a kiemelt fontosságú közművek**. És a hadviselés klasszikus módszerei, mint például **a visszaszámláló alkalmazása** csak azért, hogy gyorsabban fizessék ki a váltságdíjat, vagy **a tetszőlegesen kiválasztható és helyreállítható három próbaállomány**, amivel a bűnözők a fizetési hajlandóságot igyekeztek emelni.

De sokaknak emlékezetes lehet a Jigsaw is, amely **ha felhasználó nem fizetett az első órában, a zsarolóvírus törölt egy fájlt. Ha nem fizetett a második óra után sem, akkor már kettőt törölt, és minden további órával a törölt fájlok száma exponenciálisan nőtt.**



Újabban pedig **a zsarolás kiegészült azzal, hogy a kiszemelt céget támadva a titkosított állományokat nem csak zárolja, de a zsarolás azzal is kiegészül, hogy nem fizetés esetén a fájlszerverekről származó vállalati dokumentumokat vagy az adatbázisokból kinyert bizalmas céges adatokat azonnal fel is töltik egy nyilvános weboldalra.**

Ezt egy tavalyi nagyszabású incidensnél az elkövetők látványosan demonstrálták is, **az áldozatul esett cégek között olyan neveket láthattunk, mint például a Tesla, a Lockheed-Martin, a Boeing vagy a SpaceX.**

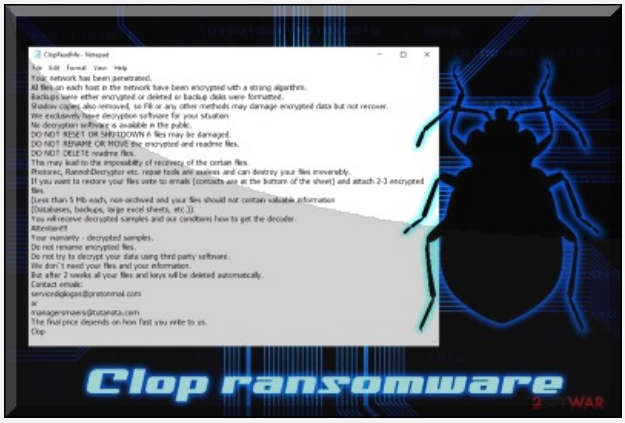


És itt kanyarodunk rá végre mai témafelvetésünkre, miszerint **a fenti zsaroló manőver a tapasztalatok szerint nem mindig igaz, ugyanis sok esetben nem is sikerült bizalmas dokumentumokat ellopni, ám ezt behazudva valóban nagyobb a nyomás az incidenst elszenvedő cégek vezetőin, kicsit ijesztgető póker blöff feelingje lehet a dolognak.**

Itt sem lehet azonban senki 100%-osan biztos a dolgában: a vállalat, hogy valóban megtörtént-e lopás, hogy az egyszeri váltságdíj fizetés után nem lesz-e ebből később egy rendszeres zsarolás, illetve a bűnözők sem vehetnek mérget arra, hogy bekamuzva egy állítólagos adatlopást vajon lesz-e ebből tényleges bevételük.

Emiatt 2021-ben újra forgattak egyet a kereken, **és az új módszer kifejezetten a céges célpontok felső vezetőinek munkaállomásai felé irányul. Innen ugyanis siker esetén valóban annyi és olyan érzékeny dokumentumot lehet megszerezni, amely a klasszikus elkódolásos zsarolás mellett sokkal fontosabb lesz az adott vállalatnak, hogy semmiképpen ne kerüljön nyilvánosságra.**

A publikussá tétel nagy csapás lehet a bizalomra és a cégimázsra, valamint azonnali negatív hatása a részvényárfolyamokra, ezt mindenki igyekszik elkerülni. Innen aztán már nehéz a visszakapaszkodás, és persze **az érintett szektorban lévő konkurens versenytársakat is komoly előnyhöz juttathatja egy ilyen adatszivárogtatás.**



A Clop csoportot vizsgálva Stefan Tanase, a dániai CSIS kiberinformációs szakértője új, de nem meglepő fordulatként jellemezte ezt a kifejezetten vezető beosztású alkalmazottak felé forduló támadási metódust.

Ugyanakkor ezzel párhuzamosan az is megfigyelhető, hogy **a zsarolási kísérletek közt már több olyan is felbukkant, ahol a valóban vagy csak állítólagosan ellopott bizalmas céges dokumentumokra, személyzeti anyagokra hivatkozva a bűnözők kifejezetten azért követelnek váltságdíjat, hogy a GDPR előírások megsértése miatti kiemelt összegű bírságot a vállalatok elkerüljék.** Szóval a csata tovább zajlik ezerrel, csapataink folyamatosan harcban állnak, és a 2021-es kiberbiztonsági előrejelzésekre pillantva elmondható, hogy a ransomware sajnos az idén is nagy erőkkel fog majd kísérteni bennünket.

Szólj hozzá!
Címkék: trend céges publikus váltságdíj adatlopás célzott kiszivárogtatás ransomware cégvezetők zsarolóvírus gdpr clop

Ajánlott bejegyzések:


5 ok, amiért a ransomware még sokáig velünk maradhat


Miért nem másolja egyszerűen vissza őket?

"Illetéktelen fél korlátozott ideig hozzáférhetett fájlokhoz"


Te nem kapod vissza, de mindenki más igen


Ransomware napszemüvegben

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter

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

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

Nem életrevalók

2021. január 15. 08:48 - Csizmazia Darab István [Rambo]

A leggyengébb jelszavak toplistáit évről évre végignézve beleég az ember retinájába a de ja vu érzés. Ezt nem hiszem el, már megint admin, password, és 12345? És a szomorú válasz ismét csak: igen, idén is ez a helyzet, a jelszóválasztó emberiség jelentős hányada nem tanul meg erős jelszót választani, **nem szorong emiatt, és nem szeret ebbe túl sok figyelmet, energiát fektetni: passwordpata ;-)**

Már tavaly is közreadtuk a kis elődöntőnek számító NordPass gyűjtést, ami akkor 500 millió jelszó elemzéséből hozta ki a helyezési listát. **Akkori első három helyezettünk az "12345", az "123456" és az "123456789" voltak**, de a futottak még kategóriában megtalálható volt a "test1", a "password", a "qwerty" vagy az "111111" és hasonló mélyen szánalmas próbálkozások.

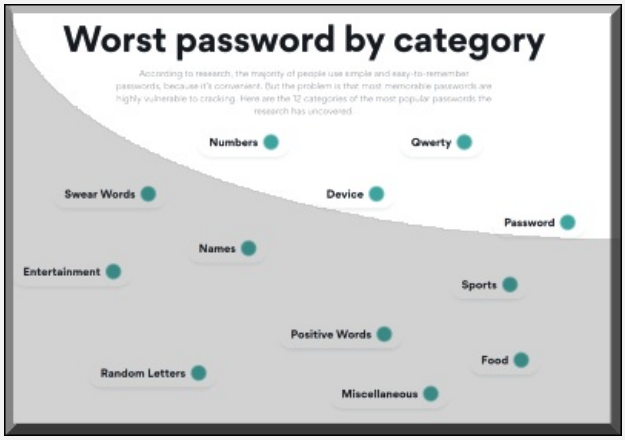
Eltelt egy újabb esztendő, a homeoffice-szal, karanténnal és kijárási korlátozásokkal tarkított 2020-as nem is akármilyen év. Ha most arra keressük a megfejtést, vajon javult-e jelszó fronton a szellem ereje, és az óvatosság, a rövid válasz erre hogy "nem", a hosszú válasz pedig, hogy "egyáltalán nem".

Szóval idén is megjelent az aktuális év kiszivárgott adatai alapján a leggyakoribb és egyben leggyengébb jelszavak hivatalos statisztikája kiszivárgott jelszóadatokból. Tanult-e az emberiség az eddigi rengeteg incidensből, jelszólopásból, account szivárgásból? Nos erre már megadtuk a választ, és most jöjjön a toplista.

Ami idén már a tőzsdeindexekhez hasonlóan **korábbi helyezéseket, és pozícióbeli emelkedést-süllyedést is feltüntet a mezőny szereplőinél. És persze jópofa és tanulságos a "Time to crack" oszlop is mellettük, mennyi idő lenne feltörni, ez utóbbi többnyire másodperceket jelent mindössze.** Persze tegyük rögtön hozzá, hogy az ilyen kigyűjtéseket sajnos pont azok nem olvassák, akiknek pedig talán a legjobban kéne.

És akkor a 2020-a év nagy befutói a helyezés sorrendjében: "123456", "123456789", "picture1", "password", "12345678", "111111", "123123", "12345" és "1234567890". A listában lejjebb görgetve sem biztatóbb a helyzet: "qwerty", "000000" és megannyi szokásos szereplő. Mit főzzünk ezek helyett? Nos az erős egyedi jelszóválasztáshoz legutóbb itt adtunk hadra-fogható szempontokat.

Jelszóválasztásnál általában a hosszabb a jobb (nem 20 db a betű), legyen minden helyszínen egyedi különböző, érdemes tudni, hogy jelenleg 12 karakter felett ugrik nagyságrendet a feltöréshez szükséges időigény, ahol csak lehet használjuk ki a többfaktoros autentikációt, inkább ne hagyatkozzunk a jelszóemlékeztetőkre, illetve időközönként rendszeresen cseréljünk jelszót látható, érzékelhető incidens nélkül is - ezek talán a leghasznosabb intelmek.



A Have I been Pwned adatbázisában pedig 2021. januárjában 10.4 milliárd lopott/kiszivárgott jelszó szerepelt. Kedves hallgatóink, rövid jelszó híreinket hallották, és következzen az időjárás jelentés, addig is legyen szép a napjuk ;-)

Szólj hozzá!
Címkék: statisztika lista toplista jelszó password gyenge worst nordpass 2020.

Ajánlott bejegyzések:

Jelszóválasztásban a helyzet változatlan

Az elveszett jelszavak fosztogatói

Az 5 leggyakoribb jelszó hiba

Leglegleg - 2020. a kibertámadások tükrében

Támadás, e-mail a neved

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

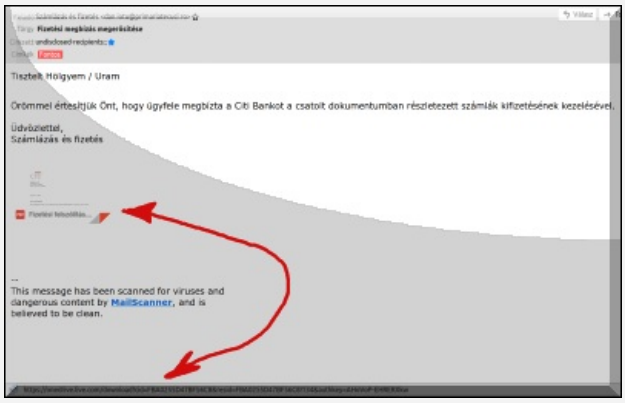
Üdvözlünk Sin City-ben

2021. január 19. 18:24 - Csizmazia Darab István [Rambo]

Illetve egész pontosan **örömmel értesítjük, hogy ügyfele megbízta a Citi Bankot a csatolt dokumentumban részletezett számlák kifizetésének kezelésével. Hát ez a Citi egészen biztosan nem az a bizonyos Citi**. További részletek a hajtás után...

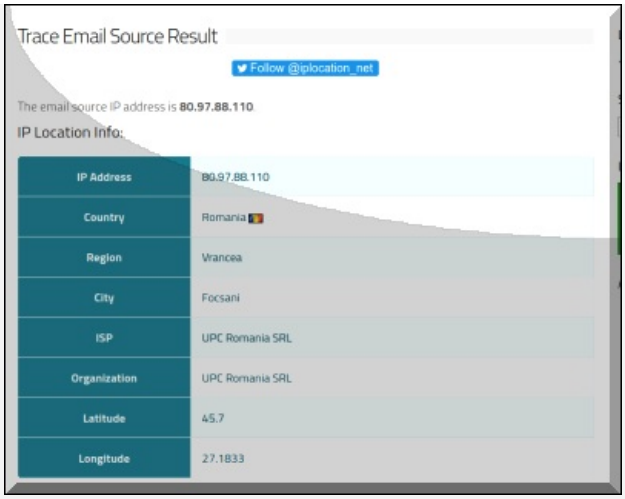
Hova máshova, mint a spam mappába érkezett egy újabb ígéretes próbálkozás, amellyel igyekeznek megfertőzni a számítógépünket. **Az pedig mindig külön öröm, ha személyesen maga a "Számlázás és fizetés" ír nekünk levelet, nem pedig Doktor Kátrány és Toll Professzor.**

A kéretlen üzenet rövid és tömör, "bikkfa" nyelvezetű, Twitteres egyszerűségen edződött stílusában a következőket tartalmazza: "*Tisztelt Hölgyem/Uram. Örömmel értesítjük Önt, hogy ügyfele megbízta a Citi Bankot a csatolt dokumentumban részletezett számlák kifizetésének kezelésével. Üdvözlettel, Számlázás és fizetés*". Ez most akkor tényleg örömhír nekünk, vagy csak kaptunk egy fizetési felszólítást?



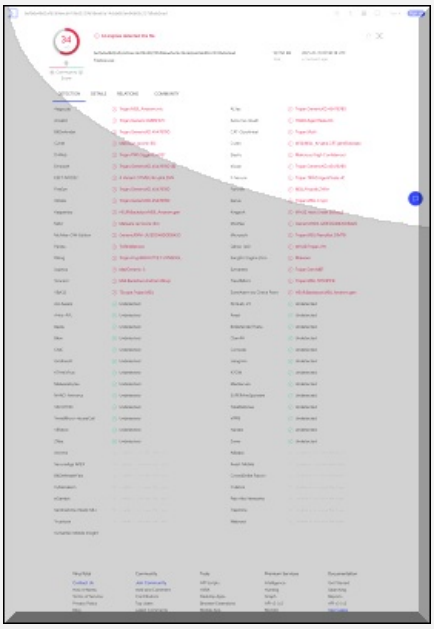
Nézzük akkor meg, milyen klasszikus átverési jellemzőket azonosíthatunk, vehetünk észre benne. Hát kevés magyar bank ír olyan hivatalos levelet, amelynek a feladója "dan PONT iotu KUKAC primariatecuci PONT ro" lenne. Az e-mail traces vizsgálat megerősítette mindezt, Vrancea (Vráncsa) megye és Focsani (Foksány) város a feladó lokációja az IP cím alapján.

A kép szerint mellékletnek látszó PDF állomány valójában egy távoli linkhivatkozás egy onedrive.live.com oldalon található URL címre, amelyre kattintva nem az ígért PDF dokumentum érkezik, hanem egy "Fizetesi felszolitas.tgz" nevű tömörített állomány, benne a "Fizetesi felszolitas.exe" futtatható fájllal, a többi pedig már történelem. Vegyük azért észre a magyar ékezetek hiányát is, nem mintha ezen már múlna bármi is. A címzetteknél szereplő "undisclosed-recipients:;"-ről már nem is beszélve, hiszen ez egy tömeges körlevél Hölgyemnek, Uramnak...



Vicces módon a lábléc még az alábbi kamu biztonsági üzenetet is megjeleníti: "*This message has been scanned for viruses and dangerous content by MailScanner, and is believed to be clean*."

Miszerint itt már egy vírusellenőrzött levelet kapunk, amely tisztának és ártalmatlannak osztályozta a látszólag Citi Bank által küldött üzenetet.



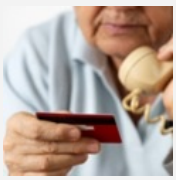
Végül vizsgáljuk meg akkor ezek után magát a rakományt is. **Ez egy Kryptik trójai, amelyre a VirusTotal weboldal víruskereső motorjai közül 34 antivírus riaszt is.**

A fájl hash alapján az állomány első előfordulása: 2021-01-15 07:10:07 volt, viszonylag friss darab. Ezzel hárítottuk is ezt az állítólagos fizetési felszólítást, és mindössze ennyi kis figyelem elég volt mindehhez.

Szólj hozzá!
Címkék: spam vírus bank csalás átverés phishing kártevő citi

Ajánlott bejegyzések:

Vakcinás csalások, szevasztok


A bankos mindig kétszer csenget...


Földgázszámla vagy mégsem?


NAV adó-visszatérítés vagy mégsem?


E.ON számlánk érkezett vagy mégsem?

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

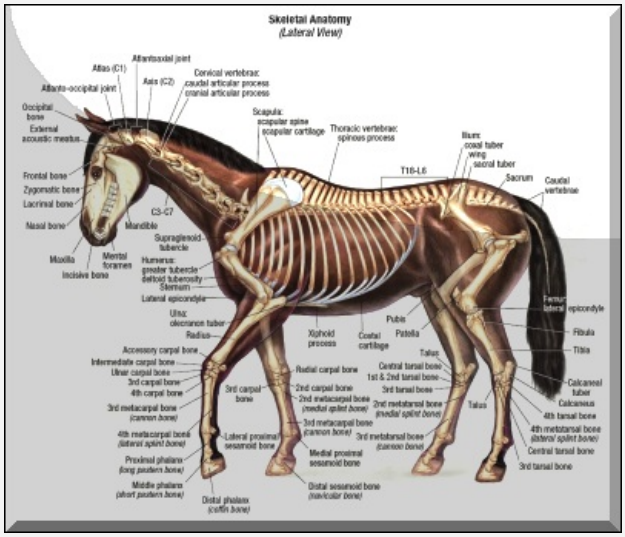
Hogy ne kezeljünk informatikai incidenst?

2021. január 21. 11:19 - Csizmazia Darab István [Rambo]

Az internet, és az online újságok címlapjai is tele vannak adatlopással, adatszivárgással kapcsolatos támadásokról szóló hírekkel, napvilágra került durva esetekkel, de azért emellett a védekezéshez szükséges best practice tanácsok, online javaslatok is széles körben rendelkezésre állnak. **Ráadásul évek óta ketyeg már az életbe lépett GDPR is, szóval úgy hihetnénk, ez egy pozitív lökést adott hozzáállásnak. Ám vannak még kivételek...**

Úgy illik, először mintapéldának egy igazi állatorvosi lovat vegyünk elő ebből a műfajból. Katasztrofális incidenskezelésben kevés ennél tipikusabb eset létezik, mint amilyen a holland Diginotar története. Azt már a GDPR előtt is láthattuk, hogyan válhat veszteségessé, vagy mehet akár csődbe egy olyan cég, amely nem csak az IT védelmét nem látja el megfelelően, de az incidensek kezelésében, kommunikációjában is súlyos hibákat vét.

Erre volt igen szemléletes példa, amikor is 2011-ben kiderült a holland DigiNotarról egy vizsgálat kapcsán, hogy nem csak egyszerű feltörés áldozatává váltak, hanem a feltehetően iráni hekkerek által elkövetett sikeres behatolással egyúttal a cégen belüli kritikus fontosságú, tanúsítványokat kibocsátó rendszerbe is sikerült bejutniuk a támadóknak.



Ennek ellenére csak belső vizsgálat volt, nem is értesítették a partnereket, a cég szerint "*az incidens hatása minimális volt*". Az utólagos vizsgálatok azt is kimutatták, hogy hónapokig egyáltalán nem is vették észre a feltörést. A későbbi titkolódzás viszont még súlyosabb és hosszú távon drágább hiba lett, mert mint kiderült, a támadók több száz (531) hitelesnek látszó hamis tanúsítványt állítottak ki a nevükben illetéktelenül, sőt a logokat is törölték.

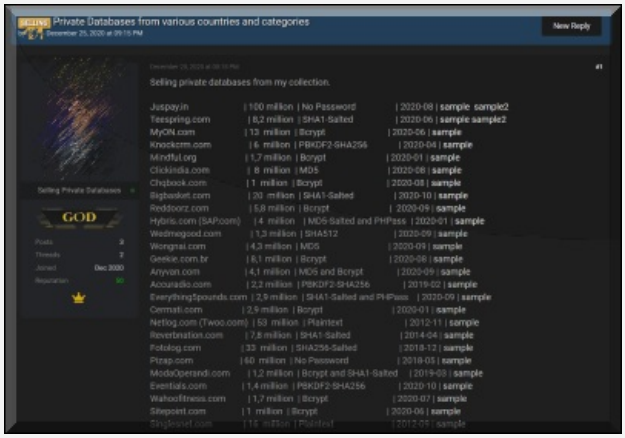
A dolog utólagos napvilágra kerülése után előbb a kibocsátott tanúsítványokat vissza kellett vonni, majd pár hónapra rá a DigiNotar (Vasco Inc. leányvállalata) szépen belebukott a történetbe, és a felszámolás után még abban az évben csődbe is mentek.

Nos akkor innen dobbantsunk a [mai friss esetünkhöz, ami a brit AnyVan nevű szállítmányozással foglalkozó cégnél történt](), és ennél azért enyhébb. Erről a TheRegister számolt be a múlt héten, a vállalat részéről megjelent sajtóközleményében közölték, hogy **a sajnálatosan bekövetkezett biztonsági incidens eredményeképpen jogosulatlanul fértek hozzá illetéktelenek a felhasználói adatbázisuk adataihoz. Az ügyfelek adatait és adatvédelmét érintő minden kérdést rendkívül komolyan vesznek, és alapos felülvizsgálatot végeztek.**

Ebben **az incidensben ügyfelek nevéhez, e-mail címéhez és a jelszó hashekhez férhettek hozzá a távoli támadók**. Az üzemeltetők rendkívül sajnálják az eseményeket, az ügy kivizsgálása pedig folyamatban van. Igaz, a támadást csak három hónappal annak bekövetkezte után vették észre, de ami igen szép a történetben, az a megjelent közlemény szövege.

"*This leaking of data came to our attention on the 31st December but we understand the incident itself occurred at the end of September. As soon as the incident came to our attention, our specialist IT team investigated it and have since taken the following remedial action: all passwords have been changed.*" Magyarul változtassuk meg a jelszót, és akkor azzal minden el van intézve.

Arra nem tért ki a közlemény, pontosan milyen módon védték korábban a jelszavakat, alkalmaztak-e közben sózást, mi okozta a behatolást, és a jövőben hogyan kívánják megelőzni, hogy újra bekövetkezzen, stb. **Arra kérdésre pedig, hogy az incidensről értesítették-e az [ICO-t, vagyis az Egyesült Királyság Adatvédelmi Hivatalát](), azt válaszolták, felesleges lett volna, hiszen az adatok jellege miatt ezt alacsony kockázatúnak minősítették.**



Nincs itt semmi látnivaló mondhatnánk, ha mindeközben nem olvastuk volna a BleepingComputer beszámolóját, amelyből az derült ki, hogy [az ügyfélnyilvántartások eladásra kerültek egy Hacker Forumon](), több más cég adatai mellett az AnyVan-tól lopott tételek is felbukkantak, ezek száma 4.1 millió.

Akkor nekünk már nem is maradt több kérdésünk...

Szólj hozzá!
Címkék: brit incidens adatlopás adatszivárgás incidenskezelés brexit gdpr anyvan

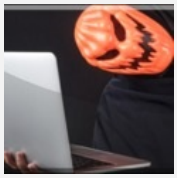
Ajánlott bejegyzések:

GoDaddy - apák a pácban


100 millió helyett "csak" 40 lett, maradhat?

Megint jőnek, szivárogtatnak...


Persze hogy tudtam, csak nem sejtettem...


Halloween, helló adatok

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

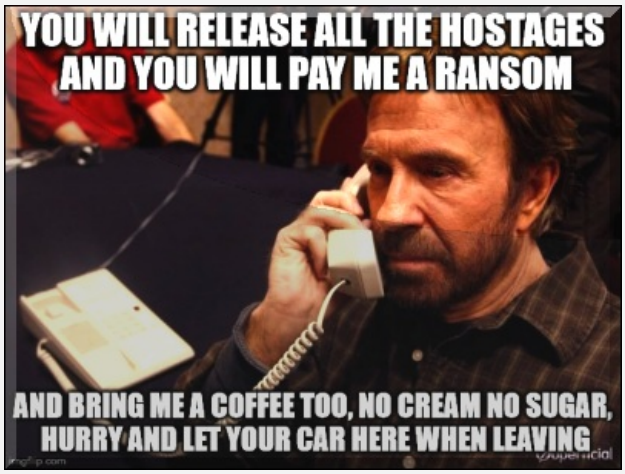
accountz

Belépés
Regisztráció

Miért nem másolja egyszerűen vissza őket?

2021. január 26. 13:11 - Csizmazia Darab István [Rambo]

A Skót Környezetvédelmi Ügynökségtől (SEPA) 4000 dokumentumot loptak el zsarolóvírust terjesztő bűnözők. Itt is a ma már trendnek számító módszer zajlott, miszerint **ha a megzsarolt áldozat nem fizet az elkódolt adatok visszaszerzéséért, akkor fizessen azért, hogy az elkövetők ne töltsék fel a lopott fájlokat publikus weboldalakra.**

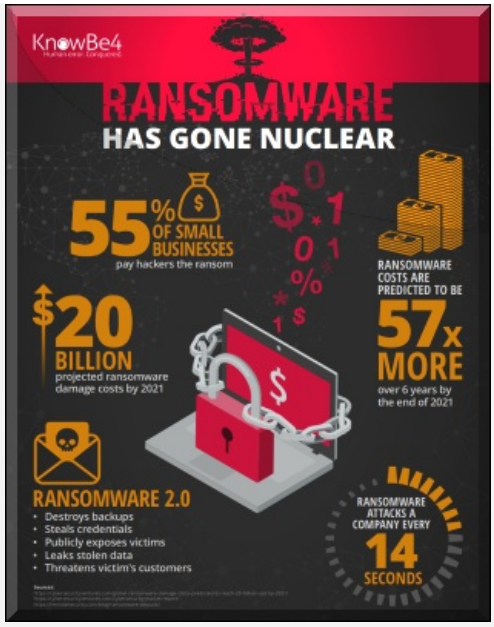


Bár Európában nem számít szövetségi bűncselekménynek a közintézmények, állami hivatalok részéről a ransomware miatti váltságdíj kifizetése, ennek ellenére igyekeznek ezt elkerülni.

Mindig is voltak-vannak-lesznek kivételek ez alól, például kórházak, mentés nélküli intézmények, de gyakran tapasztalható a nemfizetés direktívája is. A SEPA itt is ezt képviselte, számolva a nyilvánosságra hozatal kockázatával.

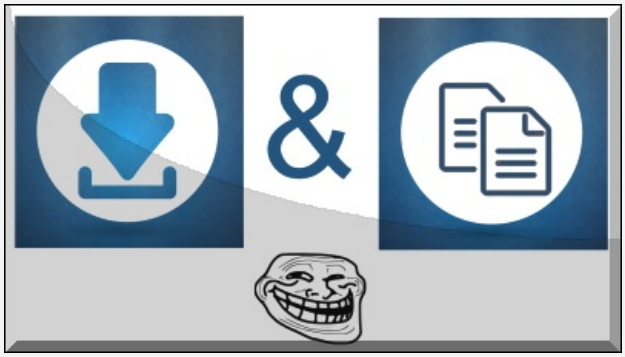
És itt kicsit visszaköszön a múltkori idevágó posztunk, amelyben arról értekeztünk, hogy a tapasztalatok szerint nem mindig igaz a nyilvánossá tételes fenyegetés, **ugyanis sok esetben egyáltalán nem sikerült bizalmas dokumentumokat ellopni, de ezt behazudva próbálnak pénzhez jutni a támadók**. Ebben az esetben GDPR nem fenyeget, hiszen Brexit. Viszont feltéve, hogy valóban megtörtént a lopás, **az is egy érdekes kérdés, hogy a kiszivárgott dokumentumok bizalmassága ad-e alapot arra, hogy a megzsarolt intézmény ne legyintsen erre az egészre fizetés helyett.**

A TheRegister egyik kommentelője **egy olyan korábbi incidenst említ, amikor egy antarktiszi kutató állomás adatait lopták el, és fenyegetőztek a publikussá tétellel nem fizetés esetére, amelynél több száz gigabájtnyi olyan légköri és asztrofizikai adat volt a célkeresztben, amelyet idővel tudományos célra amúgy is nyilvánossá tettek volna.**



A mostani támadás következtében **a SEPA néhány szolgáltatása ugyan időlegesen offline állapotba került**, ám az oldal folytatta a működését, például árvíz-előrejelzés és egyéb területeken.

A követelt váltságdíjak egyébként erősen szórnak, de nagyobb hálózatok, stratégiai célpontok esetében millió dolláros nagyságrend sem számít ritkaságnak, legutóbb például a CWT Business Travel Management Company egy az Egyesült Államokban, Minnesotában található utazási társaság fizetett 4.5 mUSD (nagyjából 1.3 milliárd forintnyi) összeget 30 ezer számítógép elkódolt, mintegy 2 TB bizalmas céges állományaiért.



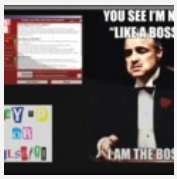
Szóval visszatérve a skót környezetvédelmi dokumentumokra, egy másik félig vicces, félig komoly kommentet is megemlítünk, amely a praktikum jegyében adja a lehetséges kettő az egyben megoldást az ilyen közel sem kritikus adatokat érintő adatvesztés plusz nyilvánosságra hozatallal fenyegető incidensekre: **"*Why not just copy them back?*" - magyarán várjuk meg amíg kiteszik, és máris visszakaptuk a dokumentumainkat...**

Persze nyilvánvaló, hogy ez itt színtiszta irónia, de néha azért egy ilyen is békében elfér az egyébként komoly bejegyzések között ;-)

Szólj hozzá!
Címkék: skót trend céges publikus váltságdíj adatlopás célzott kiszivárogtatás sepa ransomware zsarolóvírus

Ajánlott bejegyzések:


5 ok, amiért a ransomware még sokáig velünk maradhat



Ransomware a csúcs felé tör

"Illetéktelen fél korlátozott ideig hozzáférhetett fájlokhoz"


Te nem kapod vissza, de mindenki más igen


Ransomware napszemüvegben

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

Tőrbeejtett adataink

2021. január 28. 09:49 - Csizmazia Darab István [Rambo]

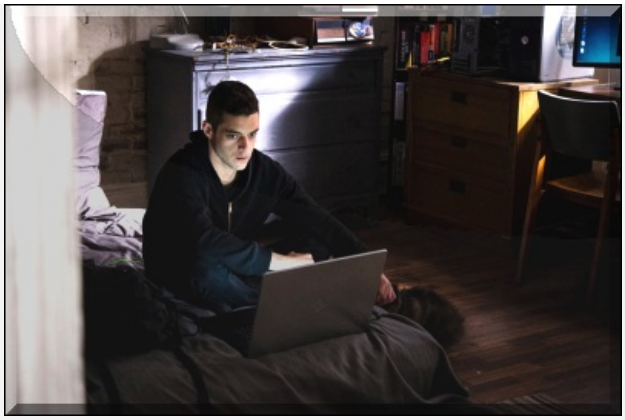
Ahogy egyre több digitális eszköz vesz körül bennünket, érdemes még nagyobb figyelmet szentelnünk az érzékeny adataink védelmére is. A biztonság felé vezető út egyik legfontosabb lépése, hogy **tisztában legyünk azokkal a kockázatokkal, amelyekkel az adataink biztonságát veszélyeztethetjük. Mi az 5 legjellemzőbb adatvédelmi gyengepont?**

Az Európai Tanács kezdeményezésére 2007 óta minden év január 28-a az adatvédelem nemzetközi napja, amely adataink védelmére, és az ehhez kapcsolódó ismeretek fontosságára hívja fel a figyelmünket. A megnövekedett digitális jelenléttel **egyenes arányban nőtt a kibertámadások száma is, amelyek során illetéktelen kezekbe kerültek a felhasználók érzékeny adatai.** Ezt támasztja alá az ESET kiberbiztonsági jelentése is, mely szerint globális szinten 37%-kal nőtt az otthoni munkavállalókat érő kibertámadások száma.

Soha nem volt még ennyire fontos számítógépeink, adataink biztonsága. Az intenzív és folyamatos online jelenlét, a tömeges otthoni munkavégzés és online oktatás komoly kihívás elé állította az emberiséget. **Az egyedi kártékony kódok, vírusok száma idén meghaladta az 1.1 milliárdos számot, míg a Have I Been Pwned adatbázisában mára már több, mint 10.5 milliárd feltört, kiszivárgott jelszó található.**

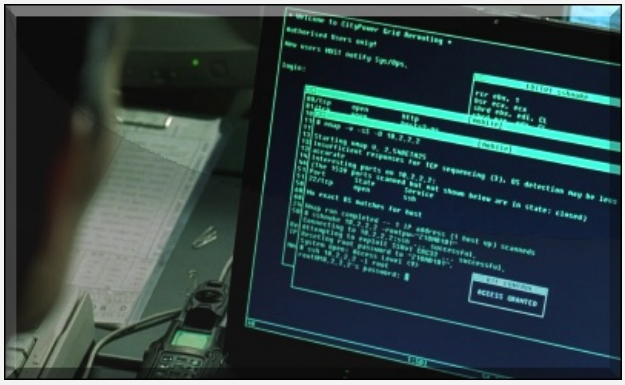
A 2021-es Kiberbiztonsági Trendekről szóló jelentésből is látszik mindez, a megelőzés érdekében pedig a kiberbiztonságnak életünk legfontosabb alappillérévé kell válnia. Ehhez a korszerű, hatékony védelmi megoldások mellett a folyamatosan fejlesztett biztonságtudatos hozzáállásunk is kulcsfontosságú.

Az alábbi adatvédelmi sarokpontok elkerülésével és a szakértői tanácsok megfogadásával sokat tehetünk saját magunk, valamint adataink biztonsága érdekében.



1. Elhanyagolt adatvédelmi beállítások
Az online jelenlétünket érdemes néha karbantartanunk. Időnként nézzük át a különböző webes szolgáltatások és közösségi média fiókok biztonsági és adatvédelmi beállításait, mert általában rendszeresen frissítik, bővítik őket. A közösségi oldalakon állítsuk be, hogy csak az ismerőseink láthassák a posztjainkat – ha van rá lehetőség, készíthetünk egyedi listákat is, például a tágabb ismerősi és a szűkebb, közeli baráti körünkről.

Legyünk saját magunk moderátorai: csak olyan tartalmakat tegyünk közzé, osszunk meg és csak úgy szóljunk hozzá mások posztjaihoz, hogy azok ne hozhassanak minket kínos helyzetbe még az eredeti környezetből kiragadva sem. Gondoljunk bele: bár mi döntjük el, hogy mit osztunk meg magunkról, azt nem tudjuk befolyásolni, hogy mások mihez kezdenek ezzel az információval.



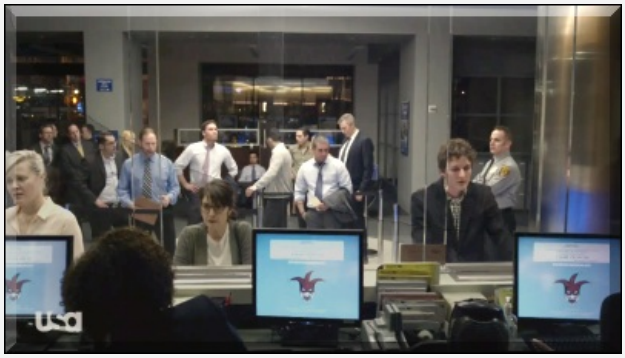
2. Alábecsült jelszavak
Erős és egyedi jelszavak használatával nagyban megnehezítjük, hogy illetéktelen személyek feltörjék a fiókjainkat, és többek között a személyes vagy akár banki adatainkhoz hozzáférjenek. Érdemes megnéznünk a legrosszabb jelszavak toplistáját, melyben remek példákat találhatunk arra, hogy milyen jelszót ne válasszunk. A 2020-as év legtöbbször használt jelszavai például a kevesebb, mint 1 másodperc alatt feltörhető "123456", "123456789" és a "picture1" voltak.

A jelszó hosszát illetően jó, ha tudjuk, hogy jelenleg 12 karakter felett ugrik egy nagyságrendet a feltöréshez szükséges idő. Minden fiókunkhoz más kódot adjunk meg, és kerüljük a hozzánk köthető szavak, információk (pl. kisállatunk neve, születési dátumunk) használatát. Ahol pedig lehet, használjunk többfaktoros hitelesítést is, amely plusz védelmi réteget ad a fiókjaink számára. Ez az extra réteg lehet egy ellenőrző kód, értesítés az okostelefonunkon vagy akár ujjlenyomatos azonosítás is.

3. Kíváncsiskodó alkalmazások
Érdemes időnként átnézni az eszközeinken futó alkalmazásokat, és felülvizsgálni, hogy melyek azok, amiket már nem használunk. Fontos, hogy a felesleges alkalmazásokat ne csak eltávolítsuk az eszközről, hanem a hozzá tartozó felhasználói fiókunkat - az összes rólunk tárolt információval együtt – is töröljük az applikációban!

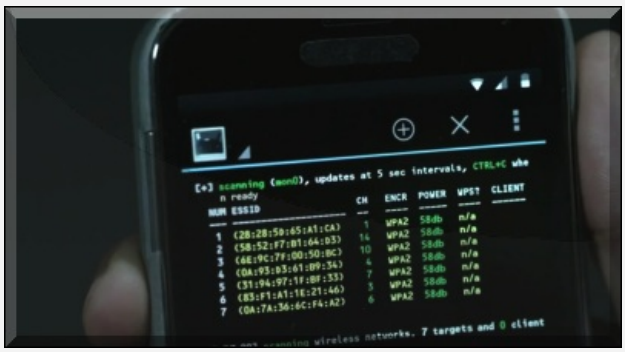
A még használatban lévő appok esetében pedig figyeljünk arra, hogy rendszeresen frissítsük azokat, illetve kapcsoljuk ki az olyan adatgyűjtő funkciókat, mint például a helymeghatározás, amikor a program éppen nincs használatban. Az alkalmazások letöltése vagy frissítése előtt nézzük át, hogy pontosan mihez kérnek hozzáférést. Mielőtt gondolkodás nélkül rányomnánk a feltételek elfogadására, mérlegeljük az előnyöket és a hátrányokat, illetve érdemes átolvasnunk

más felhasználók szöveges értékeléseit is.



4. Trükkös e-mailek
Adathalász támadásoknál a kiberbűnözők a netezők hiszékenységét próbálják kihasználni. Megkereshetnek minket egy ismert, megbízhatónak tartott szolgáltató nevében (bankok, hivatalok, csomagküldő szolgálatok, közösségi média felületek), vagy valamilyen csalit, például pénz nyereményt vagy műszaki cikket kínálva. Általában a levél arra kér minket, hogy a megadott linkre kattintva adjunk meg különböző bizalmas adatokat magunkról. Mindig figyelmesen ellenőrizzük, hogy az e-mail valóban az adott szolgáltatótól érkezett-e, illetve ellenőrizzük azt is, hogy az üzenetben hivatkozott ügyfélkódunk helyes-e.

Mindig tartsuk szem előtt, hogy a bűnözők igyekeznek kihasználni az aktuális eseményeket, így a koronavírus-járványt is. Már most is találkozhatunk vakcinákkal kapcsolatos kéretlen üzenetekkel, amelyek információt, a várakozási listában való előrébb jutást, vagy akár felár ellenében azonnali oltóanyagot ígérnek. Utóbbi esetben különösen veszélyes, hogy a gyanútlan áldozatok a személyes adataik ellopása és az anyagi károk mellett az egészségüket, de akár az életüket is kockáztathatják.



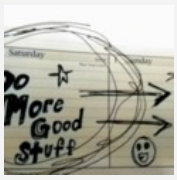
5. Védtelen eszközök
Sok bosszúságtól kímélhetjük meg magunkat egy naprakész, modern vírusvédelmi szoftver használatával. Lehetőleg olyan programot válasszunk, amelynek van adathalászat elleni funkciója is, így védve leszünk azon káros weboldalak ellen, amelyek célja különböző érzékeny adatok eltulajdonítása.

Érdemes ismert gyártók termékei közül választani. Az ESET Internet Security például hatékony védelmet nyújt az adathalászat mellett a hackerek, a rosszindulatú programok, zsarolóvírusok, valamint egyéb online fenyegetések ellen is.

2 komment
Címkék: adatvédelem nap trend tippek megelőzés nemzetközi eset

Ajánlott bejegyzések:


7 tipp a mobilunk védelméhez



10 kiberbiztonságra veszélyes szokás

Ha eljön a személyiségtolvaj


Sötétben bújkáló shadowIT


Mindent IS visz...

Kommentek:

ramipali 2021.01.29. 08:58:09

Olyan jó dolgokat írtok,hogy a hátamon feláll a szőr.
Ugyanis minden internetes honlap azzal kezdi,hogy SZÜKSÉGÜNK VAN ADATAID VÉDELMÉRE!"
Mi ez,hogy ha nem visszaélés és más illetéktelenekl továbbadás?

Válasz erre

e2ender 2021.02.02. 10:04:16

@ramipali: Tovább megyek, vigyázni próbálunk a személyes adatainkra, de minden portálon tolják a képedbe a legnagyobb adattolvajok linkjeit, - színes mezőit, - regisztrálj, lépj be FB accountoddal, (Google, Twitter, stb.,... - és itt is!) Miért gondolom úgy, (és vajon rosszul gondolom-e?) hogy ez alapból a "vizet prédikál, de bort iszik" viselkedés!!!

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

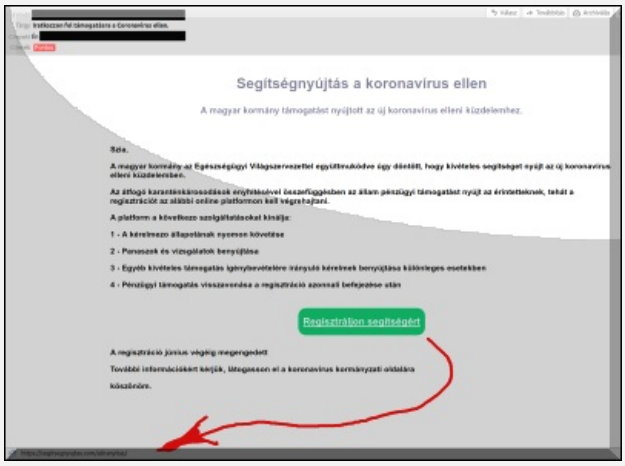
A Ravasz, az Agy és az online átverések

2021. február 03. 10:17 - Csizmazia Darab István [Rambo]

A kiberbűnözők gyorsan reagálnak a világ aktuális történéseire és pillanatok alatt felismerik, hogyan húzhatnak hasznot azokból - de vannak olyan örökzöld sémáik is, melyeket bármikor tudnak alkalmazni: álláslehetősége, adócsalás, hamis webshopok.

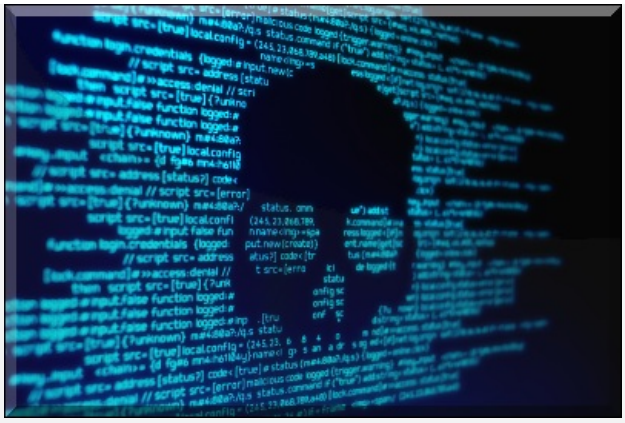
A kiberbűnözők nagyon kreatívak, ha a felhasználók pénzének elcsalásáról van szó. Áldozataikat a legkülönfélébb módszerekkel célozzák meg, kezdve különböző kormánytisztviselők megszemélyesítésétől egészen a csaló online piacterek létrehozásáig. Újra és újra bebizonyosodik, hogy gyorsan alkalmazkodnak, és eszközeiket sokszor az aktuális hírekhez igazítják. Az elmúlt hónapokban számos átverés a COVID-19 járványból próbált hasznot húzni.

A bűnözők általában vagy az egészségügyi hatóságok tagjainak adták ki magukat, vagy olyan védőfelszereléseket kínáltak eladásra, amelyekből éppen hiány volt. A szakértők például olyan átverést azonosítottak 2020 márciusában Magyarországon, melynek során arcmaszkokat kínáló hamis webshopokkal, illetve kéretlen levelekkel támadták a felhasználókat.



2020. december 16-ig az Egyesült Államok Szövetségi Kereskedelmi Bizottsága több mint 275.000 világjárványhoz kapcsolódó csalásról és személyazonosság-lopásról kapott bejelentést. Az áldozatok összesen 211 millió dollár (körülbelül 63 milliárd forint) elvesztését jelentették. Most, 2021-ben a legújabb átverések már a vakcinával kapcsolatosak, tömeges terjedésük miatt az Interpol és az Europol is riasztást adott ki.

A bűnözők kéretlen üzeneteikben a személyes adatok és banki azonosítók megadása után a várakozási listán való előrébb jutást, vagy akár felár ellenében azonnali oltóanyagot ígérnek. Tévedés ne essék, a csalók nemcsak közegészségügyi vészhelyzetek vagy globális események alkalmával dolgoznak.



Az Európai Bizottság a közelmúltban felmérést készített a fogyasztók csalásokkal kapcsolatos tapasztalatairól, melyben Magyarország is részt vett. **A kutatás során megállapították, hogy a megkérdezett európaiak több mint fele (56%) találkozott már a felmérésben szereplő csalások legalább egyik típusával az elmúlt két évben. Íme az 5 leggyakoribb online átverés, amelyre az ESET kiberbiztonsági szakértői szerint érdemes figyelnünk.**

Online vásárlás és aukciós átverések
A gyanútlan áldozatok megcélzásának egyik leggyakoribb módja az online vásárlással kapcsolatos csalás. A világjárvány kezdetén megnövekedtek ezek a típusú átverések, különösen bizonyos termékek, például az arcmaszkok és a kézfertőtlenítők hirtelen fellépő hiánya miatt. A csalók gyakran hoznak létre hamis kiskereskedelmi weboldalakat, ahol nevetségesen alacsony áron kínálják híres márkák luxustermékeit. Különösen ügyelnek a weboldal megjelenésének kifinomult kialakítására, hogy minél megbízhatóbbnak tűnjenek. Erre sokszor még egy ellopott logóval is ráerősítenek. Ha egy ilyen weboldalról rendelünk valamit, az általában meg sem érkezik, vagy ha mégis, az biztosan egy silány minőségű hamisítvány lesz.

De még rosszabbul járhatunk, ha a rendelés során megadtuk a hitelkártya adatainkat is, hiszen a csalók bármikor visszaélhetnek azokkal. **Az online vásárlásokra specializálódott bűnözők már a közösségi média felületeken is elkezdték kínálni termékeiket, így érdemes ezeken a platformokon is fokozottan figyelnünk.** Másik kedvelt taktikájuk az aukciós átverés. Ebben az esetben egy nem létező terméket bocsájtanak aukcióra, vagy lemásolják egy valóban eladásra kínált tárgy hirdetését, mintha az a sajátjuk lenne. Az aukciót megnyerő vevő végül sosem kapja meg a kifizetett terméket.

Tipp: mindig megfelelő gondossággal ellenőrizzük le azt az eladót, akitől vásárolni szeretnénk. Olvassuk át figyelmesen a szolgáltatási feltételeket és az adatvédelmi, valamint a visszatérítési irányelveket. Próbáljunk meg rákeresni korábbi vásárlók véleményeire, értékeléseire is. Ha egy eladó túl sok személyes információ megadását kéri, az legyen azonnali intő jel! A legjobb és legbiztonságosabb az lenne, ha csak olyan megbízható, ismert webshopokból vásárolnánk, amelyek igazolt korábbi eladásokkal rendelkeznek.

Money mule átverések, avagy az online pénzmosás
A „money mule” átverések különböző formákat ölthetnek, a mögöttük álló bűnözők célja azonban mindig ugyanaz: tiltott tevékenységből származó pénz mozgatása nyomon követhetőség nélkül. Ez egy olyan új pénzmosási technika, mely során a bűnözők a pénzintézetekkel történő kapcsolatfelvételt iktatják ki, és egy harmadik személy - money mule, azaz

pénzöszvér - közreműködésével bújtatják a pénzüket. Céljuk elérése érdekében különféle eszközökkel célozzák meg áldozataikat.

Az esetek többségében vagy otthoni munkavégzéssel csábítják őket, ami a jelenlegi járványhelyzetet figyelembe véve már nem ismeretlen fogalom, vagy online társkereső platformokat használnak. Miután elnyerték az áldozat bizalmát, pénzt vagy csekket küldenek neki, és megkérik, hogy azt küldje el valaki másnak. Ennek az átverés mértékétől függően különböző kimenetelei lehetnek: a hamis csekk visszapattanhat, és a bank megkérheti, hogy fizesse azt vissza, de komoly jogi problémája is akadhat annak, aki bűncselekményből származó pénzt mozgat.

Tipp: a tanácsunk ebben az esetben egyszerű - ha egy szóban forgó távmunka lehetőség magában foglalja azt, hogy pénzt kell utalnunk egy állítólagos ügyfél számára, ne fogadjuk el az állást! Az ilyen online munkák kockázatai messze felülmúlják az előnyöket. Legyen gyanús, ha egy társkeresőn megismert udvarló arra kér, hogy küldjünk pénzt valakinek az ő nevében, és utasítsuk el a kérését. Különösen igaz ez akkor, ha csak online találkoztunk az illetővel. Romantikus átverések sajnos léteznek, és a szerelemtől elvakult áldozatok végül a megtakarításaikat is elveszíthetik, sőt egyes esetekben jogi vádakkal is szembenézhetnek.

Lottó és nyereményjáték csalások
Az előlegdíjas csalások kategóriájába tartozó lottó- és nyereménycsalások általában azzal kezdődnek, hogy a potenciális áldozat egy kéretlen e-mailt, telefonhívást vagy SMS-t kap, melyben azt állítják, hogy egy nagyobb összeget vagy valamilyen luxusnyereményt nyert, amely átvételéért csak korlátozott ideig tud jelentkezni. Ehhez azonban először meg kell fizetnie egy bizonyos összeget, amely fedezi az adókat, a szállítási költséget, vagy egyéb más képzeletbeli költséget.

Mivel a nyereményjáték nem is létezik, az áldozat soha nem kapja meg az ígért nyereményét, hiába fizeti meg a kért összeget. Az is előfordulhat, hogy csillagászati nyeremények csábítanak arra, hogy vegyünk részt egy versenyen vagy sorsoláson, majd azzal kecsegtetnek, hogy növelhetjük esélyeinket, ha fizetünk egy titkos taktikákért vagy további sorsolásokért. Az egyetlen eredmény azonban az lesz, hogy átvernek és elveszítjük a pénzünket.

Tipp: annak érdekében, hogy elkerüljük a nehezen megkeresett pénzünk elveszítését egy előlegdíjas csalás miatt, engedélyezzük az email fiókunkban a spamek szűrését, amely megakadályozza, hogy a legtöbb csaló e-mail bekerüljön a postaládánkba. Ha egy ilyen jellegű e-mail mégis bejut a postafiókunkba, annak ellenére, hogy nem jelentkeztünk semmilyen játékra vagy versenyre és nem is lottóztunk, egyszerűen hagyjuk figyelmen kívül, és jelöljük meg spamként. Ha azonban a levél felkelti az érdeklődésünket, alkalmazzuk a korábban is említett javaslatokat. Keressünk rá a cégre, vagy promóterre, aki azt állítja, hogy az említett játék mögött áll. Gyanakodjunk, ha alig találunk információt az adott játékról.

Adócsalások
Ezek az átverések általában – de nem csak - az adóbevallási időszakok környékén ütik fel a fejüket. A kiberbűnözők ebben az esetben sem egy egységes módszert alkalmaznak; többféle csaláshoz folyamodnak. Egyik népszerű taktikájuk, hogy a helyi adóhatóság nevében adathalász e-maileket küldenek, amelyek révén megpróbálnak személyes és pénzügyi információkat kicsalni az áldozataiktól. Az így megszerzett adatokat végül pénzügyi csalásokra és személyazonossággal való visszaélésre használják. Ezekben az esetekben a bűnözők úgy próbálják meg becsapni az áldozatukat, hogy azt állítják, hibát követtek el az adóbevallásuk benyújtásakor, vagy rájuk ijesztenek, hogy van egy lejárt adószámlájuk és bírságot kell fizetniük, ha nem a leírtak szerint cselekszenek.

Tipp: Többféle módon védhetjük meg magunkat ezektől az átverésektől. Ha kapunk egy e-mailt, amit

állítólag a helyi adóhatóság küldött, a legegyszerűbb, ha közvetlenül az adóhatósághoz fordulunk és ellenőrizzük, hogy az e-mailt valóban ők küldték-e. Árulkodó jel lehet, ha olyan adóbevallással kapcsolatban kapunk értesítést, amit még be sem nyújtottunk. Ha gyanús, fenyegetésekkel teli telefonhívást kapunk, kérjük el a telefonáló nevét és azonosítóját, majd informáljuk le őt az illetékes hatóságnál. Érdemes megjegyezni, hogy egy igazi kapcsolattartó valószínűleg nem fenyegetőzne, csak tájékoztatna az esetleges hibánkról.

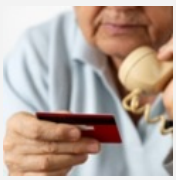
Befektetési csalások
A befektetési csalások általában a magas nyereség és gyors megtérülés ígéretéről vagy a „hiteles forrásból származó” szigorúan bizalmas tippekről ismertek. Bár az ajánlatok eltérőek, de a lényeg minden esetben ugyanaz - gyorsan és egyszerűen megsokszorozhatjuk befektetésünket. A bűnözők a befektetési csalások esetében is különféle stratégiákat alkalmaznak, hogy elnyerjék áldozatuk pénzét. Az egyik legismertebb közülük az úgynevezett Ponzi-rendszer, amely egyfajta piramisjáték, ahol a korábbi befektetőket az újonnan érkezett befektetők pénzéből fizetik ki, egészen a rendszer összeomlásáig.

Gyakori stratégia az áldozatok hideghívása és a “pump and dumb” csalás is. Utóbbi egy olyan részvénycsalás, mely során a bűnözők általában kis cégek részvényeiről olyan hamis híreket közölnek (például spam üzenet formájában), amelyből az áldozatok tévesen úgy gondolják, emelkedni fognak az adott cég papírjai. Bármelyik trükköt is próbálja meg alkalmazni a szélhámos, általában egy e-mail küldésével fog kezdeni, amelyben bemutat egy jónak tűnő üzletet, mellyel megtízszerezhetjük befektetésünket. Előfordulhat, hogy a csaló egy valódi befektetési társaság képviselőjének adja ki magát, de az is elképzelhető, hogy az általa említett befektetés valós, de a pénzünk a címzetthez sosem fog eljutni, csak a bűnözők lesznek vele gazdagabbak.

Tipp: Legyünk mindig körültekintőek, és emlékezzünk arra, hogy nincs olyan garantált befektetés vagy módszer, amely könnyen pénzt hoz. Ha egy ajánlat mégis felkelti az érdeklődésünket, feltétlenül vizsgáljuk meg a lehetőséget, illetve a mögötte álló céget. Ha a befektetés és a vállalat egyaránt valósnak bizonyul, ellenőrizzük le annak a személynek a személyazonosságát is, aki az üzletet kínálja nekünk.

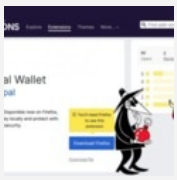
Szólj hozzá!
Címkék: lottó befektetés aukció csalás átverés adóbevallás pénzmosás adathalászat onlin nyereményjáték

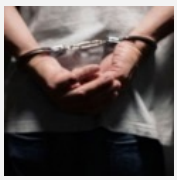
Ajánlott bejegyzések:


A bankos mindig kétszer csenget...


Ingyenes Omikron teszt vagy mégsem?

Adathalászat a Discordon


Bízz embertársaidban, de emeld meg a kártyapaklit!


Szerva itt, letartóztatás ott

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

A Cerber visszatér

2021. február 05. 13:32 - Csizmazia Darab István [Rambo]

Jó-jó, nem a jedi, de a visszatérés stimmel, örülni viszont garantáltan nem fogunk neki. Akinek csak halványan dereng, **nézzük mi is volt annak idején a Cerber! Úgy 2016. tájékán egy vélhetően orosz fejlesztésű ransomware**, amely ellenőrizte a célországot, és a volt Szovjetunió tagköztársaságainak számítógépeit nem fertőzte meg.

A Cerber név onnan eredt, hogy ezt fűzte hozzá fájlkiterjesztésként a titkosított állománynevek végére. Ami miatt még emlékezetes lehet, hogy a váltságdíj beszedésére buzdító hangüzenetet 12 különböző nyelven is meghallgathattuk, többek közt angol, francia, portugál, török, német, kínai, lengyel, spanyol, japán, olasz, arab nyelven.

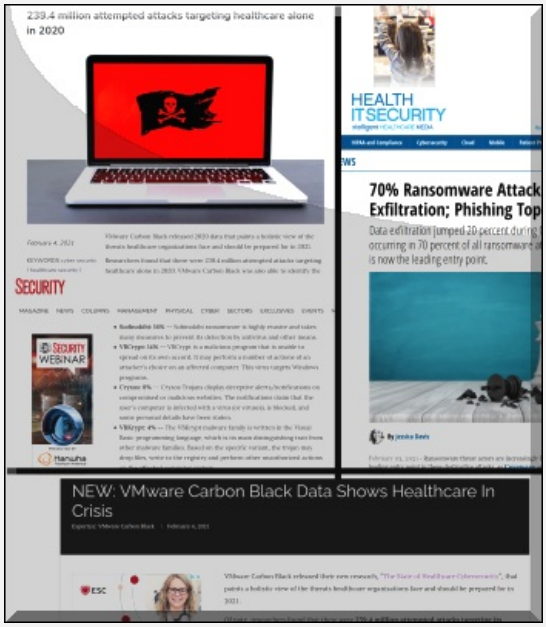
A robotszerű géphang elmondta, a dokumentumainknak reszeltek, és ideje fizetni, mert ha letelik a hét napos határidő, úgy duplázódik a váltságdíj. Az akkori összegekkel kalkulált válságdíj még "csak" 1.24 Bitcoin volt - 2016. tájékán ez körülbelül 500 dollár, nagyjából 140 ezer forint környékén mozgott.

2017-ben még az egyik legelterjettebb zsarolóvírus kártevőként volt jelen, aminek részben a RaaS, azaz Ransomware as a Service is oka volt, magyarán a bűnözők szolgáltatásként is árulták szerzeményüket. Ám utána pár évre már eltűnt a látókörünkből, jöttek az újak, TeslaCrypt és társai.

A látszólagos szünet után viszont új formában ismét felbukkant. A VMware Carbon Black biztonsági kutatói szerint **2020-ban az egészségügyi ellátást célzó, intézményeket fenyegető leggyakoribb ransomware fajtaként azonosították, 58% részesedést tudott kiharapni a tortából, aligha nem a három fejével ;-)**

A Cerber mellett **sajnos még egy rakás, a kórházakat, egészségügyi intézményeket támadó zsarolóvírust ismerhetünk, így az öt legjelentősebb között volt a Sodinokibi, a VBCrypt, a Cryxos és VBKrypt is. A beszámoló szerint 2020-ban hozzávetőlegesen 240 millió zsarolóvírus támadási kísérlet történt kizárólag az egészségügyi szektorban.**

Sajnos a kórházak a Covid járvány ellenére is kedvenc célpontjai maradtak a bűnözőknek, **kapott ransomware támadást az amerikai ExecuPharm gyógyszeripari óriáscég, de a csehországi Brno Covid centruma is, és még egy sor kórház is világszerte.**



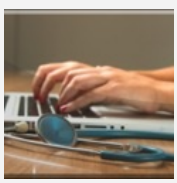
A megelőzés és védekezés még sosem volt ennyire fontos az élet minden területén, de az egészségüggyel kapcsolatos minden intézmény számítógépes rendszerén is.

És bár általánosságban látunk olyan eseteket, amikor nem is kis összegeket mégis csak kifizetnek a bűnözőknek, vannak olyan áldozatok is, **akik annyira nem fektetnek energiát a védekezésbe, incidens felderítésbe, megelőzésbe, auditokba, hogy az egyszeri váltságdíj rendezése után kis idő múlva aztán újból megtámadják, megzsarolják őket, és ismételten fizethetnek ugyanazoknak a bűnözőknek.**

Szólj hozzá!
Címkék: statisztika kórház egészségügy váltságdíj ransomware raas cerber zsarolóvírus

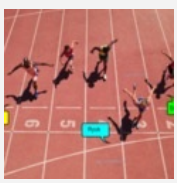
Ajánlott bejegyzések:


Sorozatosak


Kórház a


Offline


Ransomware


Világrekord,

lettek a kórházi támadások | vírus szélén | mennyország - egy rövid időre | helyzetjelentés | aminek mégsem örül senki

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó

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

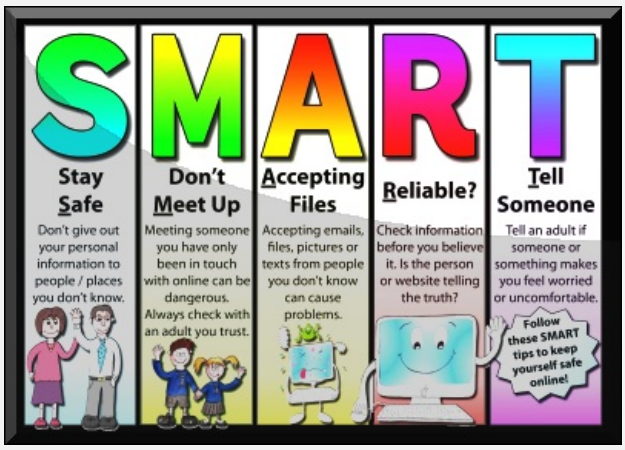
És ez az a nap!

2021. február 09. 11:33 - Csizmazia Darab István [Rambo]

Ötből egy gyerek nem érzi magát biztonságban az interneten - derül ki az InternetMost nevű kutatásból. Aktuális téma ez napjainkban, **nem csak azért mert a mai nap, február 9. a biztonságos internet világnapja, hanem azért is, mert a digitalizáció korábban eddig nem látott mértékben vált mindennapjaink részévé a 2020-as évben** a karanténhelyzet következtében..

Sokszor felnőttként is találkozhatunk a világhálón olyan tartalmakkal, vagy érhetnek minket olyan atrocitások az online térben, amelyekkel még sok évvel a hátunk mögött is nehéz megbirkózni. Nem beszélve az internethasználók legfiatalabb generációjáról, akik lelki fejlődésére nagyban kihathat egy-egy negatív tapasztalat. Ők a digitális bennszülöttek, akik **bár együtt nőnek fel a digitális technológiákkal, kíváncsiságuk és felelősségtudatuk hiánya miatt könnyen kerülhetnek veszélybe is.**

Az online biztonság kialakításában hatalmas felelőssége van a szülőknek is! **A Family Online Safety Institute (FOSI) friss jelentése szerint hozzáállásuk a témához korosztályonként változik.** Míg az ún. "baby boomer" generáció 57%-a véli úgy, hogy a gyermekek online biztonságát illetően a szülőké a legnagyobb felelősség, addig az X generációsok 43%-a és az Y generáció csupán 30%-a van hasonló álláspontonon.



A kutatás igazolja azt is, hogy a 7-11 éves gyerekek szüleire a leginkább jellemző, hogy valamilyen online biztonsági eszközt vetnek be a védelem érdekében, hiszen ennél a korcsoportnál a legnagyobb a valószínűsége annak, hogy nem a korosztályuknak megfelelő tartalmakkal találják szembe magukat az interneten.

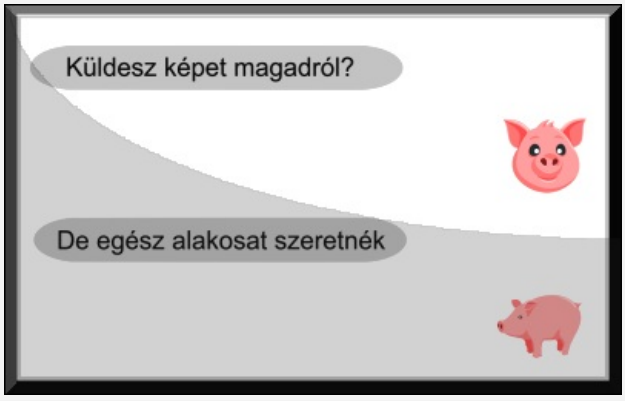
A különböző szülői eszközök használata mellett természetesen a biztonságtudatos nevelés és a példamutatás is kulcsfontosságú. **Beszélgessünk a gyermekekkel nyíltan és őszintén, így a koruknak megfelelő információkat átadva kialakíthatjuk biztonságtudatukat. Ehhez remek kiindulópontot nyújt az ESET családi oldala,** ahol a szülőknek szóló edukatív tartalmak mellett játékos videókat is találhatunk, amelyekkel közelebb hozhatjuk a gyermekekhez az internetes biztonság témakörét. Az ESET szakértői első lépésként az alábbi 4 gondolatébresztő tanácsot javasolják a szülők számára.

1. Nem a tiltás a megoldás!
Tartsuk szem előtt, hogy a fiatalok számára az internet már élettérré vált, és a járvány hatására még nagyobb szerepet kapott az életükben. Jelenleg az online tér a kapcsolattartás, a tanulás és a kikapcsolódás helyszíne is számukra, ennek minden előnyével és negatívumával együtt.

Közösen, a gyerekekkel együttműködve állítsunk fel szabályokat, amelyeket rendszeresen ellenőrizzünk is.

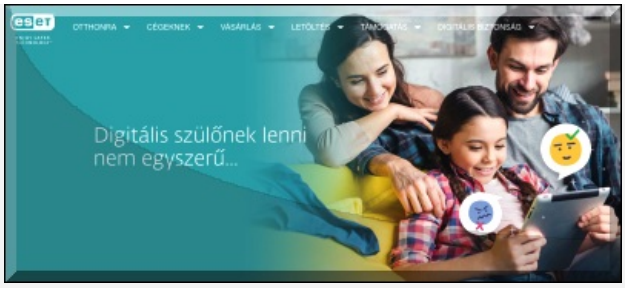
2. Óvatosan a közösségi médiával!
Bár a legtöbb social media felületen a regisztráció életkorhoz kötött (általában 13 év), hazánkban a 10-18 éves gyerekek 88%-a jelen van a közösségi oldalakon. Pedig nem véletlen a korhatár, hiszen ebben a korban már-már kialakul a gyerekek személyisége és az a képességük, hogy helyén tudják kezelni a külvilág visszajelzéseit.

Fontos azonban, hogy mindig nézzük át a különböző közösségi platformok által kínált adatvédelmi beállításokat, állítsuk privátra a gyerekek profiljait, illetve beszéljük át azt, hogy milyen információkat, tartalmakat szabad megosztaniuk magunkról ezeken a felületeken.



3. Vegyük észre a zaklatást!
Az UNICEF aktuális felmérése szerint Magyarországon a 10-18 éves gyerekek 20%-át érte már online bántalmazás (cyberbullying). Ennek felismerését nehezíti a szülők számára az, hogy a cyberbullying jelei könnyen összetéveszthetők a kamaszkori gondokkal, ezért sok szülő nem is szerez tudomást a problémáról. Intő jel lehet az étvágytalanság, alvászavarok, esetleg a súlyingadozás.

Online bántalmazásra utalhat továbbá az iskolakerülés, az érdeklődési kör elvesztése vagy a különböző közösségi profilok letörlése is.

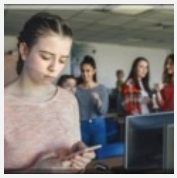


4. Programba zárt segítség
A különböző szülői felügyelet szoftverekkel gyermekbarát módon védhetjük meg a gyermekeket az internet káros oldalától, amikor épp nem lehetünk mellettük. Az ESET Parental Control alkalmazásával például megakadályozhatjuk a felnőtteknek szóló vagy erőszakos tartalmak elérhetőségét, illetve korlátozhatjuk, hogy milyen alkalmazásokat és mennyi ideig használhatnak a készülékükön.

A gyerekek kérhetik a letiltott weboldalak feloldását vagy éppen extra használati időt is igényelhetnek szüleiktől az alkalmazáson keresztül.

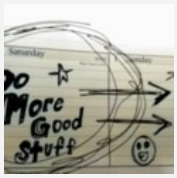
Szólj hozzá!
Címkék: biztonságos biztonság internet gyerekek tippek day megelőzés szülők zaklatás világnapja safer 2021.

Ajánlott bejegyzések:


Zaklatják a gyerekem


Fiatal vagy? Ezekre az online csalásokra figyelj!


7 tipp a mobilunk védelméhez



10 kiberbiztonságra veszélyes szokás

Ha eljön a személyiségtolvaj

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

A domainnév foglalás 22-es csapdája

2021. február 12. 10:38 - Csizmazia Darab István [Rambo]

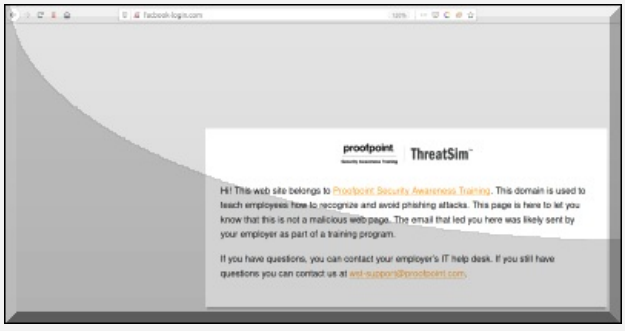
A biztonság klasszikus alappilléreit gyakran emlegetjük: védelmi program, hibajavító frissítések és biztonságtudatosság. Az utóbbiból pedig az a hasznos, ha az nem egy egyszeri, hanem rendszeres időközönként végzett képzésben ölt testet. **Az adathalászat elleni védekezést például nem lehet elégszer hangsúlyozni, amihez egyebek mellett a felhasználó óvatossága, tudatossága is egy nagyon fontos kellék.**

Most egy érdekes esetről olvashattunk, melynek lényege, hogy a Proofpoint cég rendszeres kiberbiztonsági képzést folytat különféle szervezetek számára, és ennek a teljes körű biztonsági képzésnek része az adathalászattal kapcsolatos tudatosság, és annak tesztelése is. **Ehhez le is foglaltak** szándékosan félregépelt (typosquatting) domain neveket, ám a Facebook ezt kifogásolta arra hivatkozva, hogy ezek az oktatási szándékkal félregépelt domainnevek (tadaaaaam!) zavaróan hasonlítanak a sajátjához, ami történetesen a védjegytörvény által védett.

Bár a webhely nem adathalászik, sőt meglátogatásakor azonnal közli: "Ez a webhely a Proofpoint Security Awareness Traininghez tartozik", a Facebook mégis panaszt nyújtott be ez ügyben az arizonai amerikai kerületi bíróságon.

Olyan domain címekről van szó, mint például "facbook-login.com", "facbook-login.net", "instagrarn.ai", "instagrarn.net", és instagrarn.org. Az ICANN, vagyis az Internet Corporation for Assigned Names and Numbers szervezet - amely egy magántulajdonban lévő, nonprofit vállalat - működteti a domainnév-rendszert (Domain Name System, DNS), így ez a vállalat felelős az internetes nevek és címek működését szabályozó irányelvekért.

A dolog mégsem annyira egyértelmű, hiszen **biztonságtudatossági tréningeken gyakran vannak ehhez hasonló feladatok, ahol észre kell venni az eltérést a valódi és a hamis webhely URL nevében, igaz kitalált példákon, mint amilyen a Google Phishing Quiz: Jigsaw oldala, ahol pont ezt kell begyakorolni, nagy biztonsággal felismerni.**



Furcsa egy helyzet, kicsit ahhoz hasonló, mint 2007. óta Németországban, ha valaki hacker eszközöket birtokol, akkor

már pusztán ezért büntethető.

Még nem tudni, mi lesz majd ennek a domain csatának a végeredménye, ám a címadásban említett Joseph Heller regényből származó örökbecsű mondatokat ettől függetlenül érdemes újra felidézni.

"*Csak egy csapda volt, és ez a 22-es csapdája volt, amely leszögezte, hogy bárki, aki közvetlen és valóságos veszélyben saját biztonságára gondol, az a döntésre képes elme természetes működéséről tesz bizonyságot. Orr őrült, tehát le lehet szerelni. Csak annyit kell tennie, hogy kéri a leszerelését, de ha kéri a leszerelését, akkor már nem lehet őrült, és további bevetésekre küldhető.*

Orr lehet őrült, ha további bevetésekre megy, és lehet egészséges, ha nem megy. Ha egészséges, akkor viszont mennie kell. Ha megy, akkor őrült, és nem kell mennie; de ha nem akar menni, akkor egészséges, és mennie kell. Yossariant mélységesen megrendítette a 22-es zárótételének abszolút egyszerűsége, és tisztelettel füttyentett."

Zárásképpen a cikk alatti kommentek némelyikéből is érdemes szemezgetni, például **van aki a védjegy miatt az ilyen oldalakat eleve tiltaná, hiszen a törvény valóban védi ezeket és büntetni hivatott sérelmes eseteket. De van olyan is, aki szerint a Facebook előbb kezdhetne birkózni azokkal az eleve csalásra használt hasonmás nevekkel, amelyek viszont nem hasonló felelős kezekben vannak.**

Mindenesetre az adathalászattal kapcsolatos óvatosságot, biztonságtudatosságot mindenkinek fejlesztenie kell magában, hiszen naponta kapunk olyan átveréseket például látszólag a bankunk nevében, hogy "Kattintson ide a bejelentkezéshez és a legfrissebb kamatlábak megtekintéséhez". **De a hamis számla kiegyenlítések megtévesztő magyar nyelvű változatai pl. Telenor, E.On, Elmű, T-Mobile, Nemzeti Közművek Zrt. is sajnos egyre gyakoribb vendégek a postafiókjainkban.**

2 komment
Címkék: facebook phishing adathalászat icann pereskedés proofpoint

Ajánlott bejegyzések:


Facebook


A bankos


Ingyenes

Adathalászat

Stop

egyperces | mindig kétszer csenget... | Omikron teszt vagy mégsem? | a Discordon | adathalászat

Kommentek:

kéki béla 2021.02.13. 17:52:26

Ez komoly? Hacker eszközök birtoklása büntethető a németeknél???
Nehogy valakinél linuxot találjanak! Nmap hacker eszköz vagy épp a horst vagy... Ja, nem a metasploit az már nincs csomagolva. De pentest tool nélkül mégis hogy lehet biztonságos rendszert építeni???

Válasz erre

gigabursch 2021.02.14. 16:01:13

Amerikába jöttem idevágó része...
Ahelyett, hogy odatenne egy gombot, hogy rossz helyre jöttél...

Anno a wigwam rock klub oldalát a wigwam.hu felől így lehetett elérni. Ha valaki rosszul gondolta a domaint.

Egyébiránt meg Túli kapja be!
Persze én könnyen vagyok, mert face negatív vagyok.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

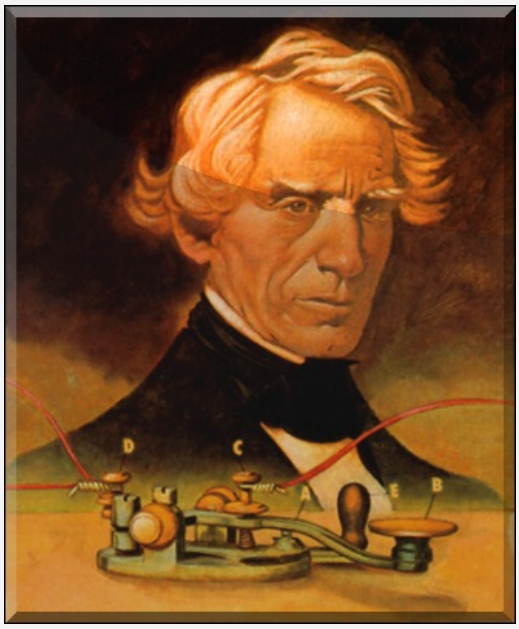
accountz

Belépés
Regisztráció

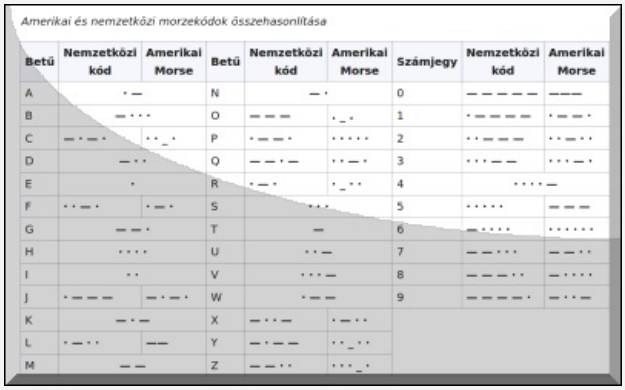
Felhőatlasz retro adathalászoknak

2021. február 16. 11:16 - Csizmazia Darab István [Rambo]

Sok meglepő dologgal találkozhattunk már az évek folyamán: a merevlemez cilindereit visszafelé eltitkosító Onehalf vírus, vagy éppen a nagy csinnadrattával beharangozott Windows Vista megjelenése után felbukkanó kártevő, amely az animált kurzorfájlok (.ani) kezelésével volt kapcsolatos, és a felfedezett hiba kihasználásával távoli kódfuttatást lehetett elérni a sebezhető rendszereken. **Az utazásnak azonban koránt sincs még vége, ezúttal a Morze ABC-nek jutott szerep egy adathalász támadásban.**



Samuel Finley Breese Morse, aki az elektromos jeltovábbításra képes távírót feltalálta 1837-ben, sosem gondolta volna, hogy élete főművét - amelyet például a Titanic óceánjáró 1912-es balesetében is használtak vészjelzés leadására - **itt és most a 21-ik században újabb aktív bevetésen porolják le,** és léphet elő, mint a Vadlibák mozifilm kiöregedett egykori veteránjai.

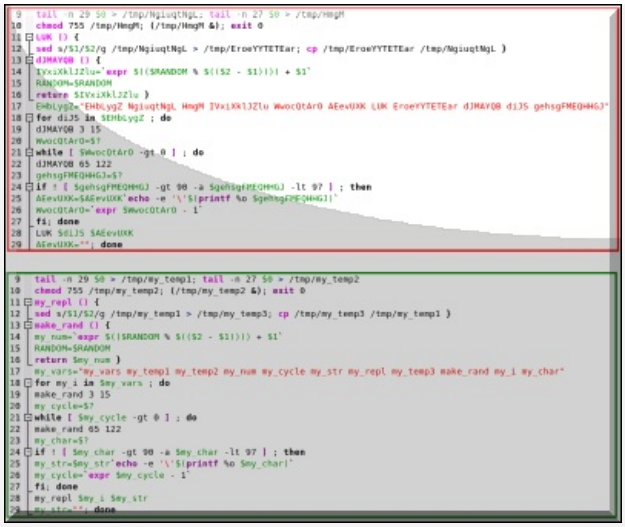


Amerikai és nemzetközi morzekódok összehasonlítása

Betű	Nemzetközi kód	Amerikai Morse	Betű	Nemzetközi kód	Amerikai Morse	Számjegy	Nemzetközi kód	Amerikai Morse
A	·−		N	−·		0	–––––	–––––
B	−···		O	–––	·–·	1	·––––	·––··
C	−·−·	··–·	P	·––·	·····	2	··–––	··–··
D	−··		Q	––·–	···–·	3	···––	···–·
E	·		R	·–·	·–··	4	····–	
F	··–·	·–·	S	···		5	·····	–––
G	––·		T	–		6	–····	·····
H	····		U	··–		7	––···	––··
I	··		V	···–		8	–––··	–····
J	·–––	–·–·	W	·––		9	––––·	–···
K	–·–		X	–··–	·––·			
L	·–··	––	Y	–·––	··–··			
M	––		Z	––··	···–·			

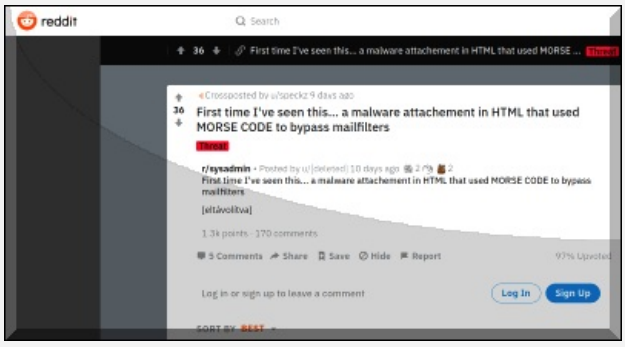
A Morze kód egy olyan kommunikációs módszer, amely a hagyományos latin betűs szöveget és számokat képes átalakítani kétállapotú jelek formájára: Ti a rövid, Tá a hosszú jel, és köztük igen lényeges, hogy legyen elegendő szünet.

A Bleeping Computer írt arról az adathalász támadásról, amelyben feltűnt az évszázados távíró kód.



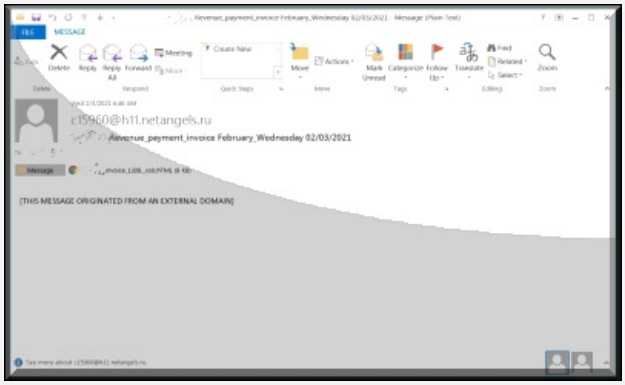
Idősebbek és katonaviseltek emlékezhetnek arra, hogy **a szkriptes kártékony kártevők igyekeznek elkódolni, összezavarni (obfuscation) a mindenki által látható, olvasható forráskódot, hogy a kártékony linkek ne legyenek már első látásra bárki által olvasható formában közszemlére téve.**

Nos ez eddig távírókód nélkül is remekül működött már évek, évtizedek óta. Leggyakoribb formában JavaScript, VBS (Visual Basic Script), Word Basic, illetve később VBA (Visual Basic for Applications) nyelveken találkozhattunk vele.



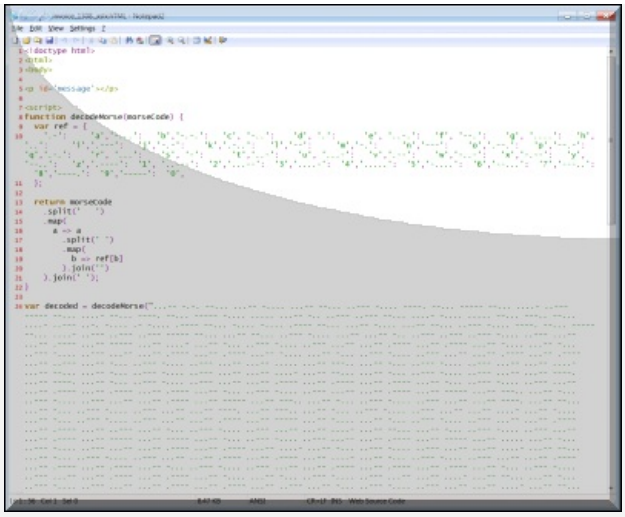
Mostani esetünkben viszont egy adathalász támadási kampány keretében **olyan kéretlen e-mail terjesztettek, amely látszólag saját cégünk nevére érkező, valamilyen legitim külső partnercég számláját tartalmazza.**

A melléklet azonban mégsem Excel tábla (ugye-ugye azt a fránya 26 éve alapértelmezetten kikapcsolt "ismert fájl típusok megmutatása" opciót minek is megváltoztatni, hiszen már a LoveLetter esetén is milyen remekül működött), csak annak látszik, hanem valójában egy HTML kód.



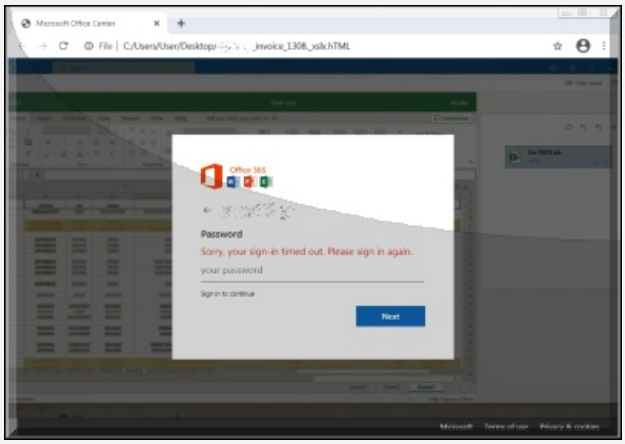
Ebben a hivatkozott kártékony **weboldal URL címében szereplő betűk és számok a Morze kód alapján a decodeMorse() függvény hatására veszik fel az értéket**.

A kódösszezavarás persze lehetett volna éppen bármi, ami az avatatlan áldozat elől képes eldugni az igazi link címét. A trükk felbukkanása viszont mindenképpen érdekessé és emlékezetessé teszi az incidenst.



Az akció végső célja pedig különféle webhelyek belépési accountjainak ellopása, így például többek közt az Office365 loginjének.

A kód feldob egy hivatalosnak látszó ablakot (ha nincs hozzá hivatalos logo, akkor éppen az Office365-öt), amely arról tájékoztat, hogy **állítólagos időtúllépés miatt újra be kell jelentkeznünk a rendszerbe, ám az adathalász ablakba begépelt login neveket és jelszavakat a kártevő összegyűjti és elküldi a távoli támadóknak.**

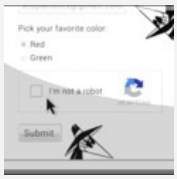


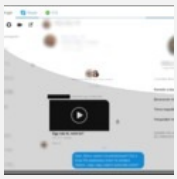
A beszámoló szerint több cégnél is bepróbálkoztak már ezzel a módszerrel, és a felbukkanó ablak sajnos sokakat valóban arra sarkall, hogy abba gondolkodás nélkül azonnal begépeljék az azonosítóikat.

A kódösszezavarási trükk viszont tényleg .--- --- .--. --- --.- .- :-)

2 komment
Címkék: javascript abc kód phishing morse adathalászat morze obfuscated obfuscation office365 kódösszezavarás

Ajánlott bejegyzések:


Mai szavunk pedig: reCAPTCHA


Facebook egyperces


A bankos mindig kétszer csenget...


Ingyenes Omikron teszt vagy mégsem?

Adathalászat a Discordon

Kommentek:

lcsaszar 2021.02.17. 13:17:12

Nem .--- --- .--. --- ..-. .- akart lenni?

Válasz erre

Gösser söralátét 2021.02.17. 16:49:46

@lcsaszar:

Bagatell. Egyre kevesebben értik ezt a nyalánkságot, guglival összeollózva meg nem kunszt összekeverni.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete.

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

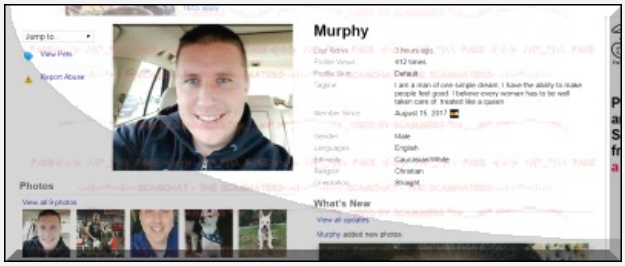
Modern románc, holdfény és tánc

2021. február 18. 11:55 - Csizmazia Darab István [Rambo]

A tavalyi esztendő fenekestül fordította fel az úgynevezett normális életünket. Ez az emberi kapcsolattartásainkban, pihenési szokásainkban, homeoffice-ba szorult munkavégzésünkben, online oktatásban, kijárási korlátozásokban új kihívást jelentő év az online leselkedő veszélyeket is megtolta, és igen, **a társkereséssel kapcsolatos csalások száma is jelentős növekedést mutatott. Egy megszívlelendő idézet Theodore Roosvelt-től: "A bölcsesség kilenctized része, hogy időben vagy bölcs".**

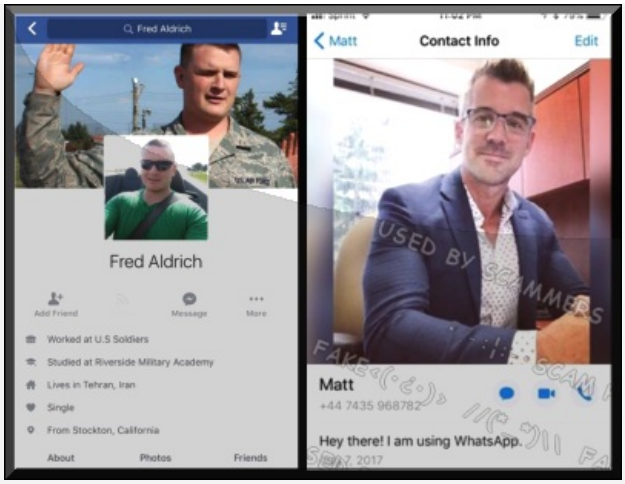
Jöttek mindenféle átverések 2020-ban, volt túlárazott, vagy nem is létező védekező eszközök (maszk, fertőtlenítő) fekete kereskedelme, és **az erre szakosodott hamis webáruházakon keresztül a személyes és banki adatok tömeges ellopása**. Volt magyar nyelvű, a magyar kormány nevében írt kéretlen levélben érkező átverés is, amelyben **a részletes személyes és banki információk megadása után kínáltak fel állítólagos 150 ezer forintos "segélyt" ismeretlen csalók.**

Persze nem kerülhettük el **a vakcinával és oltással kapcsolatos csalásokat sem, volt ezekben állítólagos azonnali oltási információ, fizetős lehetőség a várakozási listában való állítólagos előrébb jutásra**, de még feketepiaci oltóanyagot is kínálgattak a kéretlen üzenetekben.



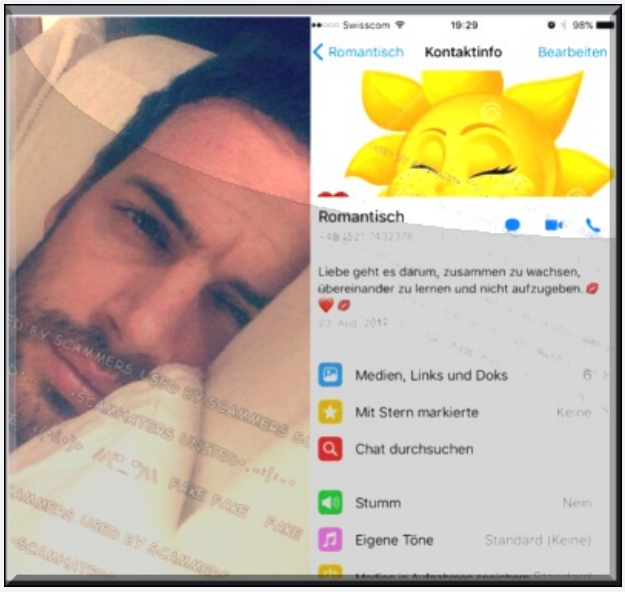
Természetesen a romantikus csalások sem szüneteltek, sőt a kijárási, utazási korlátozások miatt még a korábbinál nagyobb hangsúllyal lett az online virtuális tér az ismerkedés, a társkeresés elsődleges vagy egyetlen lehetséges terepe. A Szövetségi Kereskedelmi Bizottság (FTC) friss jelentése szerint tavaly rekordösszeget, 304 millió dollárt (hozzávetőlegesen 90 milliárd forint) sikerült a csalóknak bekasszírozni, ami 50%-os növekedés jelent az előző évhez viszonyítva.

Áldozatonként átlagolva így sem kevés ez, vagyis fejenként nagyjából 2500 dollárt, azaz körülbelül 740 ezer forint volt a veszteség, ami a 2016-hoz viszonyítva az akkori elszenvedett átlag kárértéknek a négyszerese.



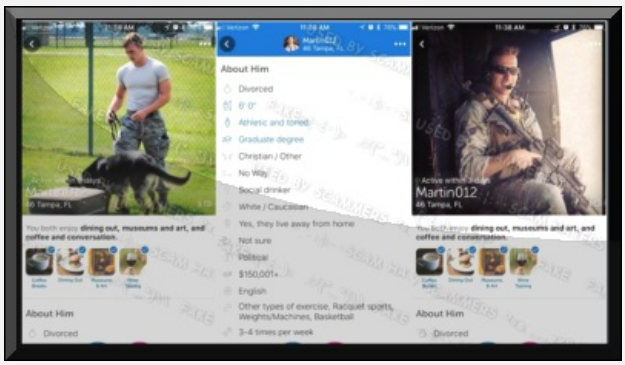
Aki még esetleg nem hallott volna a romantikus csalásokról, a még csak virtuálisan ismert leendő társunk tipikus jellegzetes élethelyzetről számol be az ismerkedés során: **külföldön szolgáló megözvegyült katona, fúrótornyon dolgozó jól kereső olajmunkás. A kezdeti levelezős szakaszban azonban éppen mindig az igazi, élőben remélt randi előtt fogy el a pénzük, vesztik el az állásukat, kapnak váratlanul magas összegű kórházi számlát, hal meg az apjuk, zárolják a számlájukat, szenvednek állítólagos balesetet, és ezeken a jogcímeken igyekeznek pénzzel lehúzni a neten kiszemelt jól szituált, egyedülálló nőket.**

A netes ismerkedés online szakaszában sok esetben arra is megkérik a partnert, hogy "akadályoztatásuk" miatt nyissanak helyettük, de a saját nevükre bankszámlát, vagy csak elkérik az áldozat részletes számla adatait.



Az FTC jelentése szerint a közösségi oldalakon, hamis profillal elkövetett romantikus csalások előfordulási aránya minden korcsoportban megnőtt, ám **a legmagasabb anyagi veszteséget mégis a 70+ korosztály szenvedte el, egyénenként átlagosan 9,475 USD, ez hozzávetőleg 2,8 millió forintnak megfelelő összeg.**

Kor alapján a 40-69 évesek a leginkább veszélyeztetett csoport, ők a bűnözők legkedveltebb célpontjai.



Hogy megvédjük magunkat a romantikus csalóktól, **mindig legyünk éberek és figyeljünk a hamis fotókra, gyanús kérésekre, kifogásokra, árulkodó jelek, amelyek arra utalhatnak, hogy átverés van folyamatban.**

Egy korábbi hasonló tematikájú posztunkban már részletes jótanácsokkal igyekeztünk szolgálni a megelőzéshez, ezt ezen a linken lehet elolvasni.

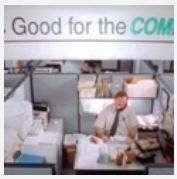
Szólj hozzá!
Címkék: online társkeresés ismerkedés csalás átverés randi romantikus welivesecurity.com

Ajánlott bejegyzések:

Amazónia veszélyes ragadozói ;-)

Celeb vagyok, fizess nekem!

Ingyenes Omikron teszt vagy mégsem?



Karácsonyi vásárlás biztonságosabban

Vakcinás csalások, szevasztok

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

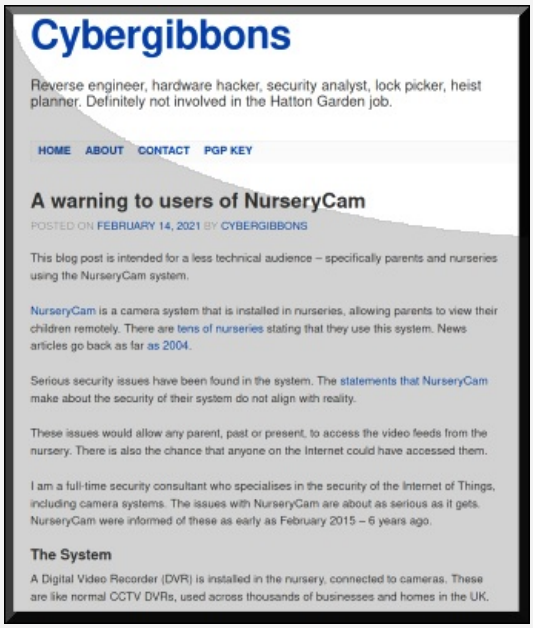
Óvodás módszerek

2021. február 23. 10:58 - Csizmazia Darab István [Rambo]

Az Egyesült Királyságban működő NurseryCam gyerekfelügyeleti szolgáltatását feltörték. Az ismeretlen támadó hozzáfért a felhasználók személyes adataihoz, beleértve a valódi név, felhasználói név, jelszó, e-mail cím mezőket is. **Az elsősorban óvodákban alkalmazott IoT szülői webkamera rendszer biztonságára már évek óta sok volt a panasz.**

A támadónak - aki egy évek óta ismert hibát használhatott ki - szinte az ölébe hulltak a bizalmas adatok. A hírről beszámoló cikkek alatt rendre azt lehet olvasni, már sokszor, például hat éve, 2015-ben is jelezték a fejlesztőknek, hogy orbitális hiányosságok vannak a biztonság területén. Bárki, aki bejelentkezett a Nurserycam DVR rendszerébe, admin joggal rendelkezhetett - ez biztosan nem fog bekerülni a profi felhasználói hitelesítések nagy aranykönyvébe.

A gyenge kialakítás miatt elvileg illetéktelenek bárkinek az élő kamerás felvételébe is belenézhettek, átirkálva az URL paramétereket. De a korábbi panaszok közt található az is, hogy például **a régebbi videókat tartalmazó FTP tárhelyük is sokáig hitesítés nélkül, nyilvánosan elérhető volt. Még a tavalyi évben is volt, aki biztonsági aggályokat jelentett a NurseryCam felé, ám ők sem kaptak érdemi választ.**



Cybergibbons

Reverse engineer, hardware hacker, security analyst, lock picker, heist planner. Definitely not involved in the Hatton Garden job.

HOME ABOUT CONTACT PGP KEY

A warning to users of NurseryCam

POSTED ON FEBRUARY 14, 2021 BY CYBERGIBBONS

This blog post is intended for a less technical audience – specifically parents and nurseries using the NurseryCam system.

NurseryCam is a camera system that is installed in nurseries, allowing parents to view their children remotely. There are tens of nurseries stating that they use this system. News articles go back as far as 2004.

Serious security issues have been found in the system. The statements that NurseryCam make about the security of their system do not align with reality.

These issues would allow any parent, past or present, to access the video feeds from the nursery. There is also the chance that anyone on the Internet could have accessed them.

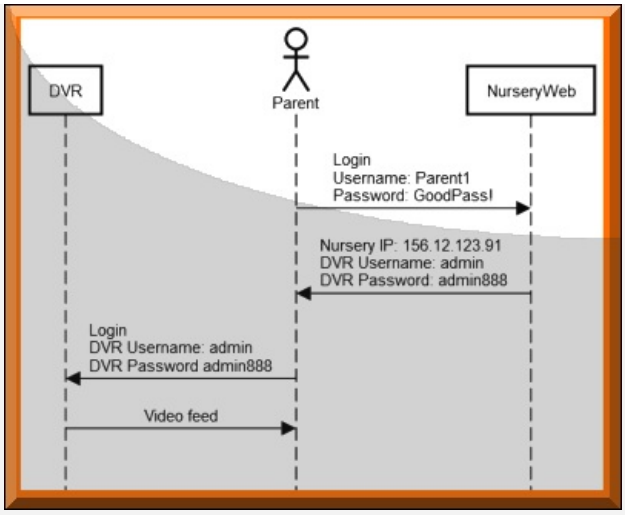
I am a full-time security consultant who specialises in the security of the Internet of Things, including camera systems. The issues with NurseryCam are about as serious as it gets. NurseryCam were informed of these as early as February 2015 – 6 years ago.

The System

A Digital Video Recorder (DVR) is installed in the nursery, connected to cameras. These are like normal CCTV DVRs, used across thousands of businesses and homes in the UK.

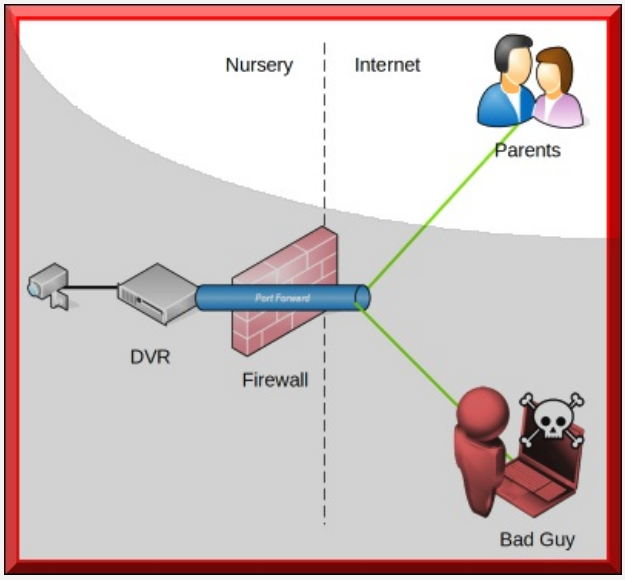
A mostani incidensnél **a támadó múlt pénteken felvette a kapcsolatot a céggel azzal, hogy 12 ezer NurseryCam felhasználó fiók részletes személyes adatát szerezte meg, amire azonnal lekapcsolták a szolgáltatást és értesítették a felhasználóikat.** Az Egyesült Királyságban bejegyzett vállalkozást két cég viszi, a FootfallCam Ltd és a Meta Technologies Ltd.

A kiszivárgott felhasználói adatok egy külsős szakértő ellenőrzése szerint tényleg valódiak. Úgy tűnik, a Brexit előtti GDPR nem működött megfelelően, hiszen itt nem pusztán csak bizalmas személyes ügyféladatokról van szó, hanem gyerekekről készült felvételekről is.



Gyenge termék, hiányos biztonság, gyengén teljesítő ügyfélszolgálat, és végül rossz reagálás az incidens nyilvánosságra kerülésénél - ez nem éppen optimális párosítás. *"Ügyfeleink biztonsága az első gondunk... Nagyon komolyan vesszük termékeink biztonságát...".*

Mindeközben viszont úgy tűnik, kiberbiztonság helyett látszólag inkább a PR-ba fektettek energiát. Ugyanis a cikkek tanúsága szerint jóval nagyobb erőfeszítéseket tettek a kritizálók Twitteren való letiltására, elhallgattatására, mint saját biztonsági problémáik orvoslására.



A biztonsági hibát jelző szakértő szavai egyértelműek: "*My Opinion: These issues are obvious and fundamental. They should not have existed in the first place.*" A társaság nyilvános bocsánatkérésében pedig ezt olvashatjuk: "*A NurseryCam őszintén elnézést kér minden szülői felhasználótól, valamint óvodától a bekövetkezett eset miatt, nagyon sajnáljuk*".

Hát az Egyesült Királyság Adatvédelmi Hivatala (ICO) talán fog majd valami bírságot kiróni a cégre. Addig is a veterán antivirus blog olvasó nagyot sóhajt, majd az x-re kattintva bezárja ezt a böngészőlapot ;-)

Szólj hozzá!
Címkék: webkamera rendszer óvoda szülői sebezhetőség adatlopás sérülékenység gyerekfelügyelet nurserycam

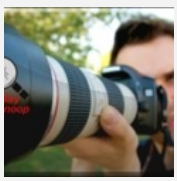
Ajánlott bejegyzések:


BlueFrag hiba az Androidon


Log4j sebezhetőség - hogyan tovább?


Exchange szerverek tűz alatt


Egyedül nem megy


Eltolás és zoomolás

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Persze hogy tudtam, csak nem sejtettem...

2021. február 25. 11:43 - Csizmazia Darab István [Rambo]

Érdekes eseményeknek lehetünk tanúi a Kia és a Hyundai Motor Company anyaszervezet környékén. A hírhedt DopplePaymer banda tagjai állítólag eredményes ransomware támadást hajtottak végre náluk, és **azzal fenyegetőznek, hogy nem fizetés esetén 3 héten belül publikussá teszik a kiszivárgott adatokat. A cég viszont azt állítja, náluk semmilyen zsarolóvírus támadás nem történt. Isten hozott a párhuzamos valóságok világában.**

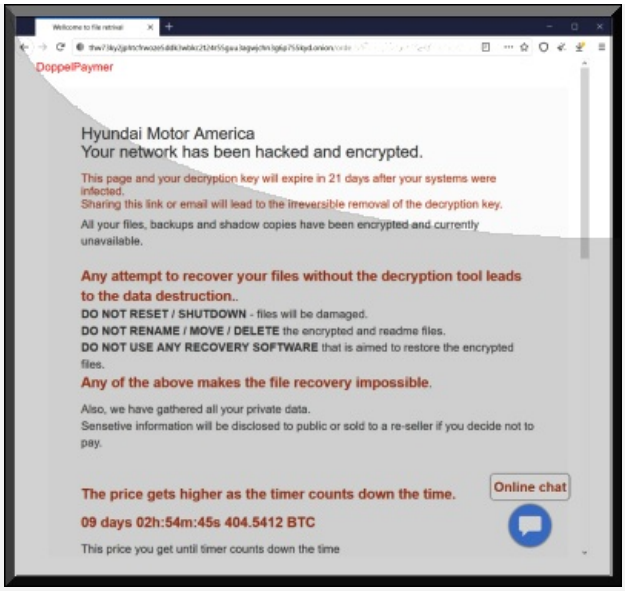
A Bleeping Computer az elsők között számolt be arról, hogy február 13-án kiesések történtek a Kia számítógépes rendszerében. A kereskedői platformok, a telefonos támogatói, valamint a mobilalkalmazásukkal kapcsolatos szolgáltatáskimaradást a cég belső hálózati szerver problémákkal magyarázta.

Ám egy új járművét átvenni próbáló arizonai ügyfél a kereskedésben azt a választ kapta 16-án, hogy már 3 napja állnak a számítógépes rendszerek zsarolóvírus támadás miatt.

Egy nappal később már olyan információról olvashattunk, hogy **a Hyundai Motor America anyacégtől állítólag 20 millió dollárnak (5.9 milliárd forint) megfelelő Bitcoint követeltek a bűnözők a dekódolásért és hogy az új módi szerint ne szivárogtassák ki az ellopott adatokat.** Ez viszont csak a tíz napon belüli kedvezményes fizetés összege (404 BTC), mert további késedelem esetén 600 BTC az emelt díj, ami viszont már 29 millió USD, nagyjából 8.6 milliárd HUF.

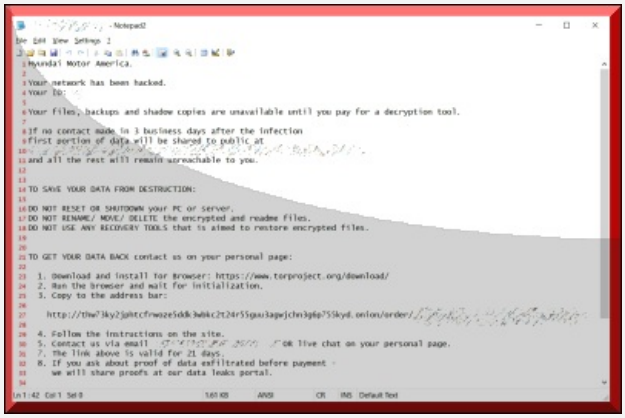
A ransom követelési dokumentumból az látszik, hogy **21 napot adtak arra, hogy kapcsolatba lépjenek velük a fizetéssel kapcsolatban.**

A bűnözői oldal ügyfélszolgálata e-mailben vagy akár chat üzenetben is kész erről kommunikálni, és ha szükséges, bemutatott bizonyítékokkal is szolgálnak arra, hogy valóban sikeres adatlopást hajtottak végre.



A Kia Motors America válasza minderre: "*KMA is aware of IT outages involving internal, dealer and customer-facing systems, including UVO. We apologize for any inconvenience to our customers and are working to resolve the issue and restore normal business operations as quickly as possible. We would like to thank our customers for their continued patience. At this time, we can confirm that we have no evidence of Hyundai Motor America or its data being subject to a ransomware attack.*"

Hát akkor ezek alapján most döntsük el, vajon történt-e incidens vagy sem? Egy ősi mondás szerint az idő mindent megold, lássuk hát, mit hoz az időmúlás ebben a konkrét történetben.



Ezen a héten hétfőn már arról olvashattunk, hogy a támadók a Hyundai Motor America és partnerei (pl. Hyundai Glovis) logisztikai műveleteivel kapcsolatos dokumentumokat töltöttek fel a netre. Ebből valószínűsíthető az a forgatókönyv, hogy nem történt váltságdíjfizetés a cég részéről. **Független IT security szakértők szerint szinte bizonyos, hogy zsarolóvírus támadás történt.**

A cég következetes tagadását azzal magyarázzák, hogy elvileg nem kötelesek nyilvánosságra hozni az incidens részleteit, hacsak az nem befolyásolja a részvényesek érdekét. Jó kérdés persze, hogy ezzel a látszólagos elzárkózással, hírzárlattal mennyiben használnak saját tőzsdei árfolyamuknak.

Március 6-án jár le majd a 21 napos határidő, meglátjuk, lesznek-e kiszivárogtatva további céges dokumentumok, vagy ez csak a támadók blöffje volt.

Addig is korábbi **összefoglaló ransomware kisokosunkat - benne a megtörtént vagy meg nem történt támadási formákról, ezzel kapcsolatos statisztikákról, valamint a védekezési, megelőzési lehetőségekről - az alábbi linken lehet olvasni.**

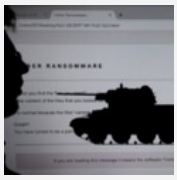
Szólj hozzá!
Címkék: leállás incidens america kia hyundai váltságdíj adatlopás adatszivárgás motors ransomware bitcoin zsarolóvírus doppelpaymer

Ajánlott bejegyzések:


Te nem kapod vissza, de mindenki más igen

Van másik!

"Illetéktelen fél korlátozott ideig hozzáférhetett fájlokhoz"


Ez most vajon akkor milyen ware?

5 ok, amiért a ransomware még sokáig velünk maradhat

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

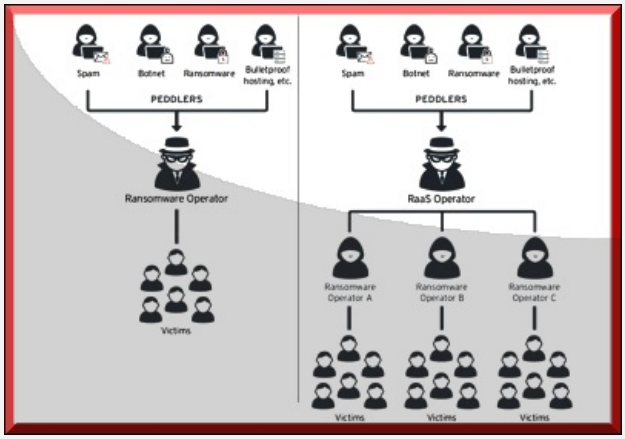
5 ok, amiért a ransomware még sokáig velünk maradhat

2021. március 02. 11:57 - Csizmazia Darab István [Rambo]

Zsarolóvírus fenyegetés - talán nincs is olyan ember, aki erről ne hallott-olvasott volna, vagy szerencsétlenebb esetben saját kárán tapasztalta volna meg azt, milyen is, amikor a számítógépes állományainkat titkosítják, és csak húzós váltságdíj ellenében ígérik be fájljaink feloldását.

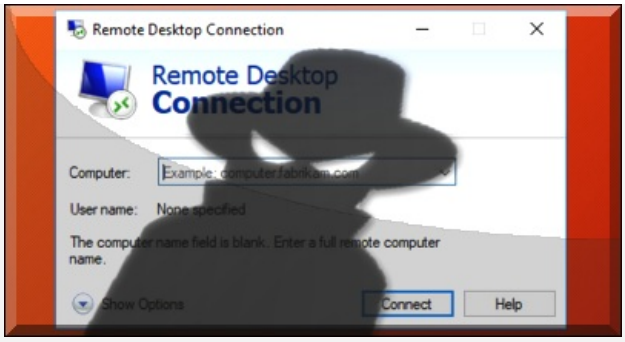
Egregor, Doppelpaymer, Ryuk - napjaink legagresszívabb ransomware fajtái, illetve terjesztő csapatai. Ezen kártevő típusról már sokszor írtunk, e fenyegetés alapvető tulajdonságairól többek közt itt is olvashatunk egy korábbi posztunkban. **Ma viszont arra keressük a választ, vajon van-e esély, hogy a zsarolóvírusok a közeljövőben már ne támadjanak minket. (És ha igen, akkor miért nem ;-)**

A rövid válasz erre, hogy "sajnos nincs", a hosszú válaszban pedig a miérteket az alábbi pontokban igyekszünk felvázolni. Akik szokták olvasni az ESET éves kártevő előrejelzéseit, azok láthatták, hogy a szakértők is folyamatos növekedést prognosztizálnak ebben az incidens típusban.



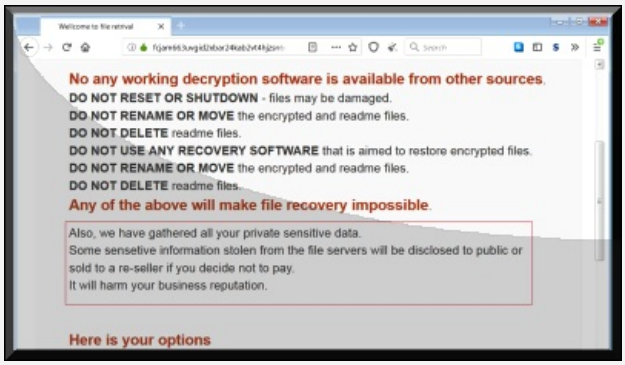
1. Jól működő gazdasági modell
Érdek a világ ura - tartja a mondás, és nincs ez másként a kártevők világában sem. **A 2013. óta zajló, fejlődő bűnözői üzleti modell abszolút életképes, és termeli a pénzt.** A támadók rosszindulatú programokat telepítenek és váltságdíjat követelnek, a pénz pedig gazdát cserél. **A ransomware-as-a-service (RaaS) segítségével kulcsrakész megoldásokat forgalmazó kiberbűnözők évről évre bebizonyítják, hogy komplett ökoszisztémát kiépítve folyamatosan képesek növekedni az üzletükben.**

Az általuk kínált szolgáltatás 7/24 supportot is tartalmaz, felhasználása pedig semmilyen különösebb szakértelmet nem igényel. A legfrissebb jelentések szerint a ransomware bandák legalább 350 millió dollárt kerestek 2020-ban, ami 311%-os növekedést jelent az előző évhez képest. **Jelentősen nőttek az átlagos céges váltságdíj összegek is, manapság ez 154 ezer dollár (46 millió forint) körül mozog, míg félévvel ezelőtt "csak" 111 ezer USD volt.**



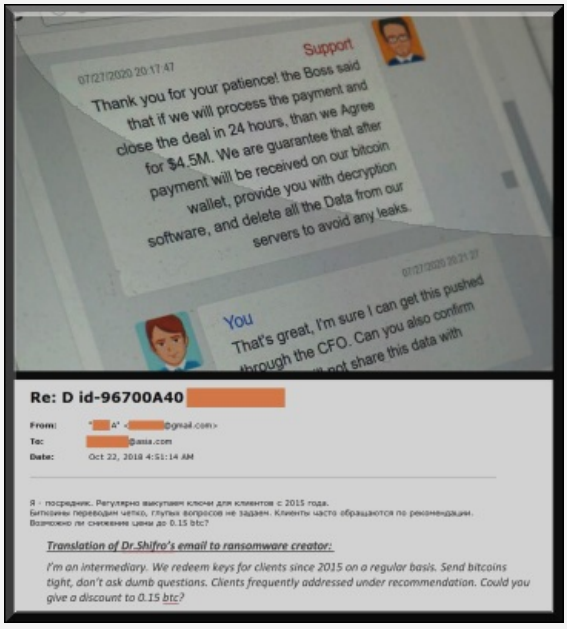
2. Védekezés, megelőzés gyerekcipőben
Bár már egy lassan kilenc éves kártevő típusról beszélünk, sajnos sok helyen még mindig hadilábon állnak a hatékony védekezési és megelőzési lépésekkel. A nyitott RDP (távoli asztal kapcsolat, Remote Desktop Protocol) sajnos bevált sikeres támadási vektornak bizonyult a ransomware környezetben.

De említhetjük a gyenge jelszavakat, az elhanyagolt biztonsági mentéseket, a szabályozatlan jogosultságokat, a nem frissített vagy hiányzó vírusvédelmet, az alkalmazói szoftverek és az operációs rendszer sérülékenységeit befoltozó rendszeres hibajavítások futtatásának elhanyagolását is. És ide tartozik a bekövetkezett támadások kommunikációja is, amely sajnos sok esetben egyedül csak a szimpla tagadást, a támadás hivatalos el nem ismerését jelenti, és iskolapéldája lehetne a "Hogyan ne kezeljünk informatikai incidenst?" témakörnek.



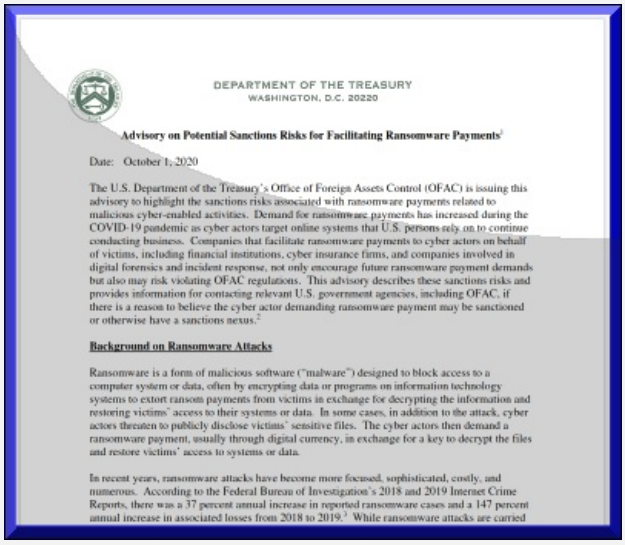
3. Egy szavam téged a padlóra küld
Vállalati környezetben elszenvedni egy ransomware támadást **alaphangon is óriási károkat okozhat.** Nemcsak maga a váltságdíj, hanem a szervezetek által nyújtott szolgáltatások leállásai, kiesett bevétel, a hírnév romboló rossz sajtó visszhang, a tőzsdei árfolyam esése és a szabályozási - például GDPR miatti - adatvédelmi bírságok is, plusz a helyreállítás költségei. **Ehhez járult még az az új típusú fenyegetés, ami már 1-2 éve tapasztalható: a váltságdíjat nem csak azért követelik, hogy feloldják a titkosítást, hanem hogy az ellopott bizalmas adatokat ne hozzák nyilvánosságra. Ez utóbbi ugyan néha csak blöff, de legtöbbször valós.**

Ahogy azt a számok is jelzik, ilyenkor az áldozatok elképesztő összegeket kifizetnek. Például a CWT Business Travel Management Company 2020. nyarán 4.5 mUSD, akkori árfolyamon nagyjából 1.3 milliárd forintnyi összeget fizetett ki a bűnözőknek. **Emiatt a legújabb trend alapján már kifejezetten a céges célpontok felső vezetőinek munkaállomásai felé irányulnak a támadások.** Innen ugyanis siker esetén valóban annyi és olyan érzékeny dokumentumot lehet megszerezni, amely a klasszikus elkódolásos zsarolás mellett sokkal fontosabb lesz az adott vállalatnak, hogy semmiképpen ne kerüljön nyilvánosságra.



4. Színre lép a ransomware bróker
Kezdetben a zsarolóvírusokat terjesztő bűnözői csapatok mellett feltűntek az olyan, függetlennek látszó segítő szervezetek, amelyek a kezdő váltságdíj fizetők "mi az a Bitcoin, hol tudnék ilyet venni?" kérdéseire adtak választ. **Ám számos esetben bebizonyosodott, hogy ezen "segítők" közül néhányan valójában a befolyt pénzen osztozó bűntársak voltak, történt is néhány ezzel kapcsolatos letartóztatás, vádemelés.** Később pedig hamis IT biztonsági ransomware tanácsadó cégek képében tűntek fel gyanús elemek. **A legitim, legális tevékenységet folytató valódi segítő vállakozások mellett például a Dr.Shifro nevű orosz kiberbiztonsági tanácsadó cégről gyanítják, hogy etikátlanul együttműködve kiszolgálja a zsarolóvírus terjesztőket.**

Bár látszólag törvényes vállalkozásnak tűnnek, és szolgáltatásaik között például a klasszikus tusztárgyaláshoz hasonlóan váltságdíj csökkentési tárgyalásokban való közreműködést is hirdetnek, ám üzletmenetük átláthatatlan, és a szakértők szerint több, mint gyanús a tevékenységük. Az már csak hab a tortán, hogy **2020-ban az amerikai kormány figyelmeztetést adott ki a növekvő ransomware kockázatokkal kapcsolatosan, és ebben arra hívják fel az állami cégek figyelmét, hogy a váltságdíj kifizetését elősegítő szereplők (ideértve a pénzügyi intézményeket, a kiberbiztosító cégeket, valamint a digitális kriminalisztikában és az incidensek elhárításában részt vevő azon társaságokat, amelyek a ransomware-fizetést kifejezetten ösztönzik) azt kockáztatják**, hogy emiatt szigorú büntetéseket rónak ki rájuk a hatályos előírások megsértése miatt.



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments[1]

Date: October 1, 2020

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this advisory to highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities. Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations. This advisory describes these sanctions risks and provides information for contacting relevant U.S. government agencies, including OFAC, if there is a reason to believe the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus.[2]

Background on Ransomware Attacks

Ransomware is a form of malicious software ("malware") designed to block access to a computer system or data, often by encrypting data or programs on information technology systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data. In some cases, in addition to the attack, cyber actors threaten to publicly disclose victims' sensitive files. The cyber actors then demand a ransomware payment, usually through digital currency, in exchange for a key to decrypt the files and restore victims' access to systems or data.

In recent years, ransomware attacks have become more focused, sophisticated, costly, and numerous. According to the Federal Bureau of Investigation's 2018 and 2019 Internet Crime Reports, there was a 37 percent annual increase in reported ransomware cases and a 147 percent annual increase in associated losses from 2018 to 2019.[3] While ransomware attacks are carried

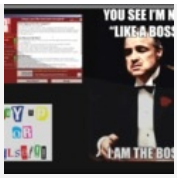
5. Biztosítás - félmegoldás
Korábbi posztjainkban már alaposan kitárgyaltuk, hogy a ransomware elleni biztosítás látszólag nem igazán vált be, sőt néha egyenesen kontraproduktív hatást gyakorolt, ugyanis az ilyen biztosítással rendelkező - főképp állami szervezetek, hivatalok, intézmények - ezzel sok esetben kényelmesen letudták a védekezést azzal, hogy baj esetén a biztosító majd úgyis fizet, és nem fordítottak elegendő figyelmet a technikai védelemre, szűrésre, megelőző pentestekre, illetve dolgozóik rendszeres biztonságtudatossági képzésére.

Ezzel összefüggésben pedig a bűnözök megtapasztalták, hogy az ilyen célpontok gyorsan és jól fizetnek, ezzel pedig végeredményben gyakorlatilag ráálltak az állami hivatalok nagyipari üzemszerű támadására.

A zsarolóvírusok elleni védekezés és megelőzés módjáról, minden ezzel kapcsolatos gyakorlati lépésről ezen a linken lehet részletesebben tájékozódni.

Szólj hozzá!
Címkék: modell trend üzleti céges publikus váltságdíj adatlopás célzott kiszivárogtatás ransom ransomware zsarolóvírus gdpr

Ajánlott bejegyzések:



[Ransomware a csúcs felé tör]

[Miért nem másolja egyszerűen vissza őket?]

["Illetéktelen fél korlátozott ideig hozzáférhetett fájlokhoz"]

[Te nem kapod vissza, de mindenki más igen]

[Ransomware napszemüvegben]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

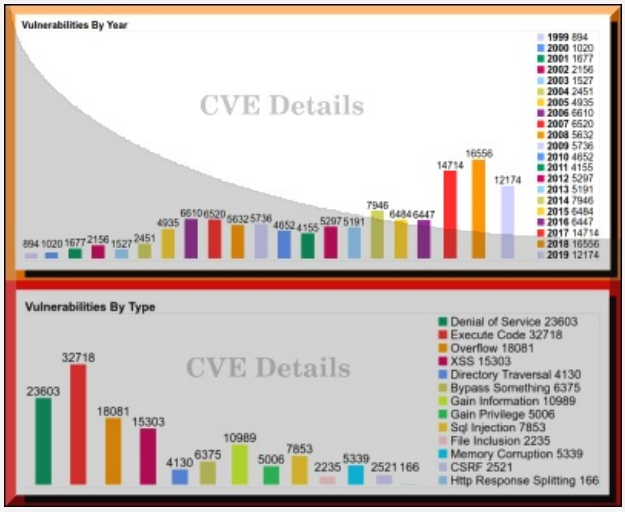
Belépés
Regisztráció

Egyedül nem megy

2021. március 04. 18:58 - Csizmazia Darab István [Rambo]

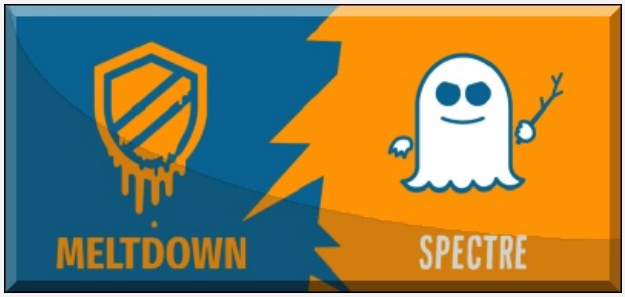
A sebezhetőségek hatékony felderítése kritikus fontosságú - ehhez gondoljunk csak például a mostani Microsoft Exchange nulladik napi hibára, **amit a hírek szerint a támadók aktívan ki is használtak**. Az Intel friss beszámolója szerint nagyjából fele-fele arányban találják meg házon belül, illetve külsős bug bounty felhívás keretében a sérülékenységeket.

Rengeteg helyen fut már hibavadász kampány, amelynek keretében az új, ismeretlen hibák felfedezőit a vállalatok a hiba jellegétől, súlyosságától függően jutalmazzák. Az teljesen biztos, hogy sokkal szerencsésebb, hatékonyabb, olcsóbb, ha ennek keretében derül ki hiányosság, mintha később élesben használnak ki ismeretlen biztonsági réseket.



A mostani 2020-as biztonsági beszámoló szerint **az Intel termékeiben bejelentett 231 sebezhetőség közül 109 problémát (47%) találtak a belső munkatársak, míg 105 darabról (45%) a hibavadász programban résztvevő külső kutatók** számoltak be. Részletes kimutatás nincs ezekről, de összességében 800 ezer dollárt fizettek ki a külsősöknek.

Ugyanez a számarány 2019-ben még kétharmadnyi volt: 70 belsős, 105 külsős felfedezéssel. Az mindenesetre elmondható, hogy az ilyen jellegű ráfordítás hasznos és megtérülő.



A külső kutatók általában a szoftver meghajtókra (grafikus, hálózati és Bluetooth) összpontosítottak, míg a belső munkatársak jobbára a bonyolultabb firmware vagy hardver sebezhetőségeket keresték. Az olyan hardveres biztonsági réseket, mint amilyen például a Spectre és a Meltdown tervezési hibák, viszont sajnos nagyon nehéz utólag javítani vagy csökkenteni a kockázatokat.

Összességében az Intel platformjai és szoftverei 2020-ban 6 kritikus, 80 magas besorolású, 131 közepes és 14 alacsony

súlyosságú sebezhetőséggel rendelkeztek.

Szólj hozzá!
Címkék: statisztika intel exploit sebezhetőség sérülékenység

Ajánlott bejegyzések:

Log4j sebezhetőség - hogyan tovább?

Exchange szerverek tűz alatt

Három éve jelent meg a WannaCry

Kr00K sebezhetőségre figyelmeztet az ESET

BlueFrag hiba az Androidon

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

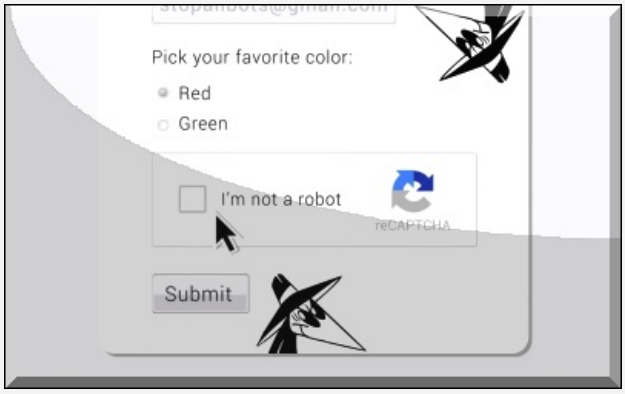
accountz

Belépés
Regisztráció

Mai szavunk pedig: reCAPTCHA

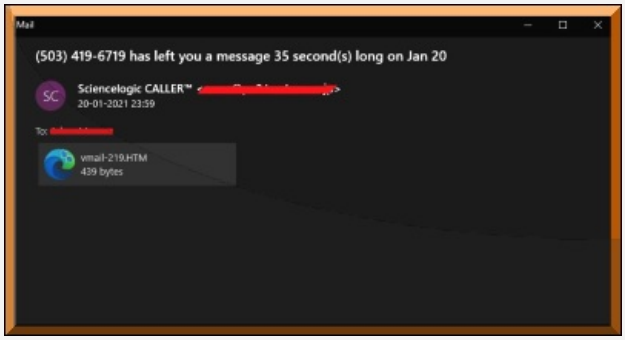
2021. március 09. 11:26 - Csizmazia Darab István [Rambo]

A Microsoft felhasználókat megcélzó új **adathalász támadás egy hamis Google reCAPTCHA rendszert használ arra, hogy megszerezze az átvert áldozatok Office 365 bejelentkezési** adatait.



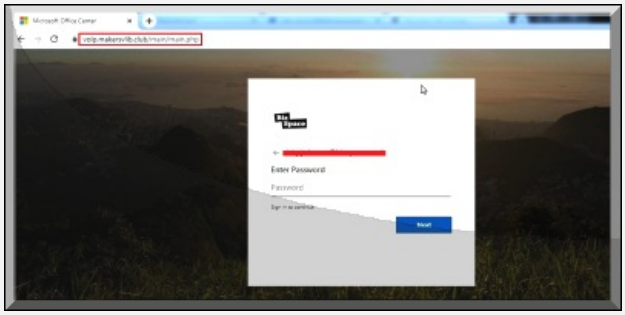
Az újabb kampány keretében **több ezer olyan spam levelet küldtek ki ismeretlenek, amelyek kifejezett célja az Office 365 rendszer hitelesítő adatainak ellopása**. A kéretlen levél azzal a trükkel operál, hogy kinézetre egy automatizálva kiküldött hivatalos levélnek látszik, amely a **mellékletben egy állítólagos hangposta üzenetre hivatkozik**, és ehhez valamilyen sorszámozott HTML fájlt találunk a csatolmányban.

Ha valaki erre rákattint, akkor indul el a captcha ellenőrzés, amely aztán **bejelentkezéshez már egy hamis, adathalász Office 365 oldalra továbbít.**



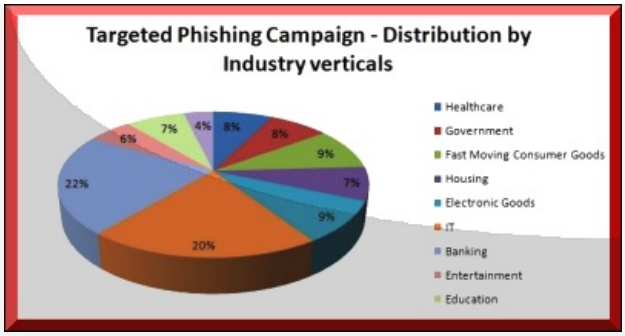
Biztonsági elemzők azt tapasztalták, hogy **ez a mostani kampány is egyértelműen magas beosztású üzleti vezetők, céges alelnökök, vállalati ügyvezető igazgatók felé irányult.**

A támadásoknak nagy valószínűséggel ugyanis az lehetett a célja, hogy érzékeny és értékes vállalati dokumentumok tudjanak megszerezni, amelyek birtokában egy zsarolóvírus támadás után - ha az adatok titkosításának feloldása miatt esetleg mégsem akarnának fizetni - a lopott dokumentumok nyilvánosságra kerülésének fenyegetésével mégis csak tudjanak váltságdíjat kizsarolni.



Az ilyen jellegű adatlopással kombinált ransomware incidensekben a kifizetett váltságdíjaknál pedig valóban az tapasztalható, **ha a cég meggyőződik arról, hogy a támadók igazat mondanak az ellopott dokumentumokkal kapcsolatban, és a tárgyaláskor valóban fel tudnak mutatni ellenőrzésképpen ilyeneket**, akkor a cégek elképesztően nagy összegű váltságdíjakat is hajlandóak kifizetni rövidtávú kármentés keretében.

Mint például ahogy az a CWT Business Travel Management Company esetében is történt.



Az elkövetők a hamis weboldalaknál úgy ügyeskednek, hogy maga a domain név az eredetinek tűnjön, ám a **.com helyett zömmel .xyz, .club vagy .online végződésű címeket használnak, amelyek mindegyike "egypálcás", azaz roppant olcsón, 1 dollár környéki összegekért lefoglalhatóak.** Az adathalászat ilyen módja igazából egy több hónapja zajló folyamat, és különféle állami intézmények, bankok felé irányult már hasonló, szintén kamu hangposta üzenetre hivatkozó kéretlen e-mail.

Iparági bontás szerint **az IT cégek/részlegek és a banki terület a legkedveltebb célpontok, de a többi ipari terület, a közigazgatás, az oktatási intézmények, az egészségügy, valamint egyéb állami hivatalok is** szerepeltek már áldozatként a korábbi támadási kísérletekben.

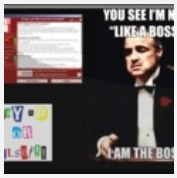
Szólj hozzá!
Címkék: microsoft céges phishing vállalati adathalászat célzott ransomware office365 zsarolóvírus

Ajánlott bejegyzések:


A bennfentes


5 ok, amiért a ransomware még sokáig velünk maradhat

Miért nem másolja egyszerűen vissza őket?



Ransomware a csúcs felé tör

Ha nem fizetsz, megfertőzzük a családodat

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

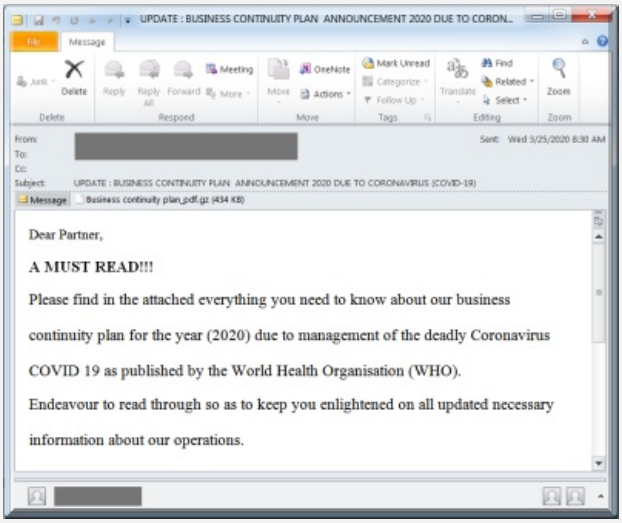
Vírushelyzet a vírushelyzetben

2021. március 16. 11:18 - Csizmazia Darab István [Rambo]

A furcsa címet az az ugyancsak furcsa helyzet inspirálta, hogy **napra pontosan éppen egy évvel ezelőtt kezdődött Covid-19 néven elhíresült pandémiás időszak**. Volt lezárás, bezárás, és minden lehetséges területen azonnali homeoffice, kijárási tilalom, lezárás, kontakt kerülés, online oktatás.

Ha átgondoljuk ezt az **egy esztendős évfordulót, és a magunk mögött hagyott időszakot, akkor rádöbbenhetünk, hogy mindez nemcsak gyökeresen, hanem vélhetően hosszútávra alakította át az életünket, emberi kapcsolatainkat, viszonyainkat, lehetőségeinket, napi rutinjainkat.**

Most csak röviden átfutjuk, hogy a számítógépes biztonság szemszögéből mik voltak a jelentősebb tényezők.



Mindig minden eseményhez - legyen az olimpia, földrengés, robbantás vagy lezuhant repülőgép - rövid időn belül megérkeztek a témához kapcsolódó átverések, spamek, adathalász próbálkozások. A koronavírus időszakra is ez volt a jellemző, hamis vagy nem létező maszkok, és egyéb védelmi eszközökkel köszönt be a fordulat, hogy aztán eljusson a feketepiacon kínált vakcinától, a vírustagadó fakenews híreket át a kórházak ransomware támadásokig, állítólagos fizetős előrébb kerülésig az oltási sorrendben.

Természetesen az adathalászat nem csak a hétköznapi felhasználókat, **hanem a céges munkatársakat is jócskán célba vette, visszaélve akár a WHO nevével is.**

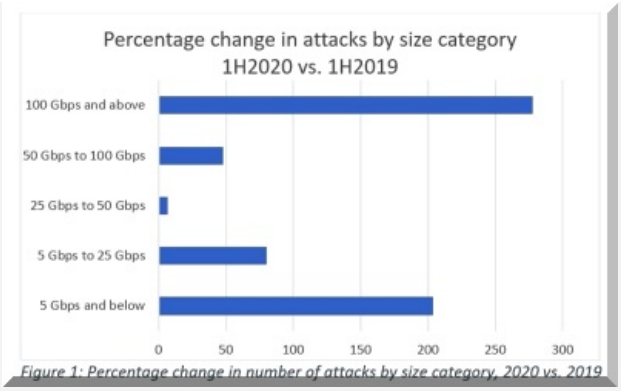


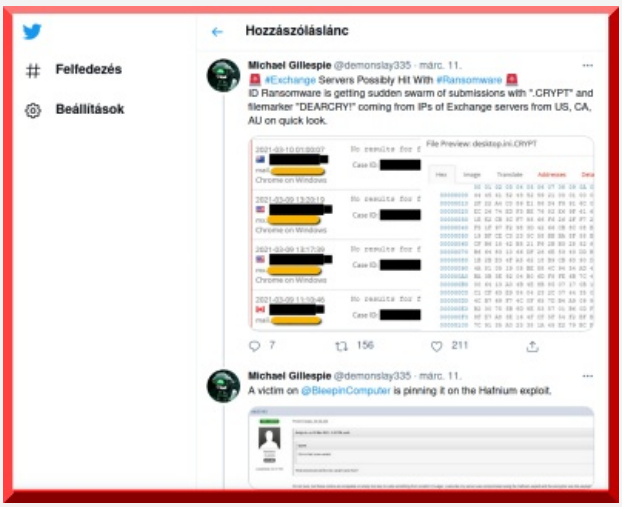
Figure 1: Percentage change in number of attacks by size category, 2020 vs. 2019

Évek óta aktívan jelenlévő fenyegetés a túlterheléses DoS, DDoS támadás, és ez a karanténos időszak csak még inkább sebezhetővé tette a cégek életét. A tapasztalatok szerint ezek az incidensek is növekvő mértékben jelentkeztek, de a zsarolóvírusos támadások is jelentős mértékben emelkedtek - beleértve persze itt nem csak a feloldókulcsért követelt váltságdíjat, de a nyilvánosságra hozatallal való fenyegetést is.

Érdekes módon itt mind a két incidens esetében kiemelkedő szerepet játszott a nyitott RDP (Remote Desktop Protocol, távoli asztal kapcsolat) protokoll, amin keresztül a támadások zöme bekövetkezett.

Egy külön fejezetet is megér az online konferenciákkal kapcsolatos helyzet is, amelyben persze olyan spamek is szerepeltek, amelyek vállalati vagy érdekes konferencia részvételt ígértek a mellékelt link segítségével. Alapvetően a kiszolgáló szoftverek voltak jobbára tűz alatt, amiben szerepelt többek közt a Microsoft Teams sebezhetőség és hibajavítás, de minden egyéb szoftver is jelentősebb terhelést, támadási próbálkozást kapott.

Ám kiemelkedett a mezőnyből a kifejezetten gyenge biztonságú, ám ingyenessége miatt mégis igen népszerű és elterjedt Zoom program. Itt aztán volt minden: beígért, de nem is létező end-to-end titkosítás (csak szerver oldali volt), API hiba, Kína felé továbbított adatforgalom, publikus netre felkerült sok ezer korábbi privát konferencia videó, na meg hogy illetéktelenek képesek voltak beletrollkodni trágár szavakkal, durva képekkel vagy videókkal az eseményekbe. Igaz, azóta már javítások is történtek.

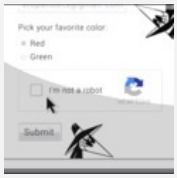


És hogy kerek legyen az év, **talán a legkellemetlenebb és derült égből jött hiba a Microsoft Exchange szerverek kritikus sebezhetősége** volt, amely egyaránt érintette és érinti számos ország vállalati és kormányzati infrastruktúráját. A támadók gyorsak voltak, és **rövid időn belül elkezdtek célzottan is keresni sérülékeny Exchange szervereket, továbbá a jelek szerint sajnos a ransomware bandák is komolyan rájátszottak erre az ígéretes területre.**

A pandémia, a karantén sajnos úgy tűnik, egyelőre továbbra is velünk marad, így informatikai szempontból biztosan nem mondhatjuk el, hogy már túl vagyunk a nehezén.

1 komment
Címkék: microsoft exchange évforduló karantén adathalászat ddos időszak pandémia homeoffice ransomware covid-19

Ajánlott bejegyzések:



Mai szavunk pedig: reCAPTCHA

Vakcinás csalások, szevasztok


Ingyenes Omikron teszt vagy mégsem?


Exchange szerverek tűz alatt

Sorozatosak lettek a kórházi támadások

Kommentek:

Antal Miklós 2021.04.14. 23:21:01

A néphülyítés ötven árnyalata – 1. rész: tutiblog.pestisracok.hu/hnd-a-nephulyites-otven-arnyalata-1-resz/

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

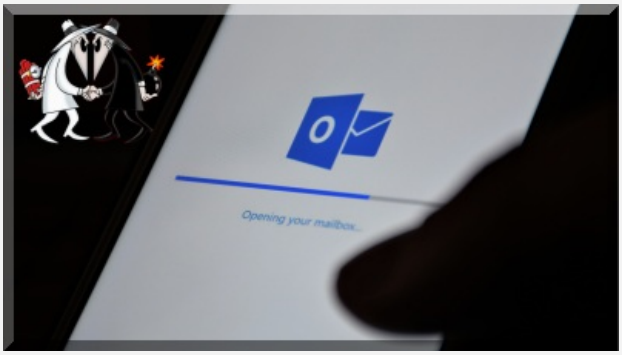
Exchange szerverek tűz alatt

2021. március 19. 09:55 - Csizmazia Darab István [Rambo]

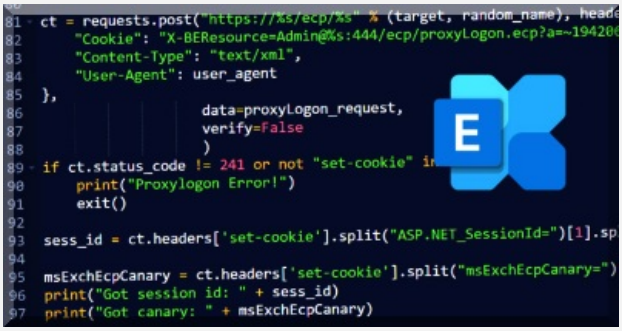
Az ESET kutatói **több, mint tíz különféle Advanced Persistent Threat (APT), vagyis fejlett és tartós fenyegetést jelentő csoportról számoltak be, akik a legújabb Microsoft Exchange biztonsági réseit használják ki** a levelezőszerverek támadásához. Az ESET több mint 5000 olyan levelezőszervert azonosított, melyek érintettek ebben a kártékony tevékenységben.

A támadások vállalkozások és kormányzatok szervereit érintik világszerte - köztük több olyan nagynevű szervezettel, mint például az Európai Bankhatóság. Ebből következik, hogy a fenyegetés nem korlátozódik a Microsoft által korábban jelentett Hafnium csoportra.

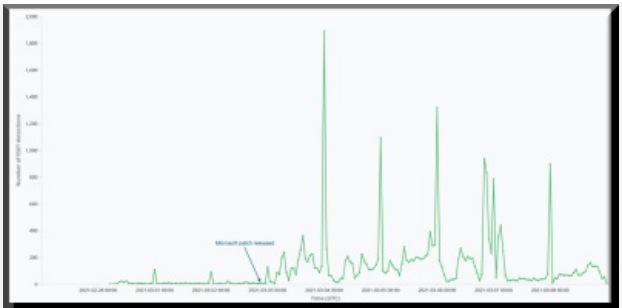
Március elején a Microsoft biztonsági javításokat tett közzé az Exchange Server 2013, 2016 és 2019 programokhoz, hogy kiküszöböljenek egy sor, az előzetes hitelesítésre és távoli kódfuttatásra (remote code execution, RCE) vonatkozó biztonsági rést. Ezek a biztonsági rések lehetővé teszik a támadók számára, hogy átvegyék az elérhető Exchange-szerverek feletti hatalmat, érvényes fiók-hitelesítő adatok nélkül - ami különösen sebezhetővé teszi az internethez kapcsolódó Exchange-szervereket.



„A biztonsági javítások közzététele utáni napon a korábbinál sokkal több fenyegetésre figyeltünk fel, amelyek tömeges mértékben támadták az Exchange szervereket. Érdekes módon mindegyikük kémkedésre szakosodott APT-csoport, kivéve egyet, ami a jelek szerint egy ismert kriptobányászati tevékenységgel áll összefüggésben. ***Elkerülhetetlen, hogy előbb-utóbb még több fenyegetés, köztük zsarolóvírussal támadó csoportok is hozzáférjenek ezekhez a sebezhetőséget kihasználó exploitokhoz.***



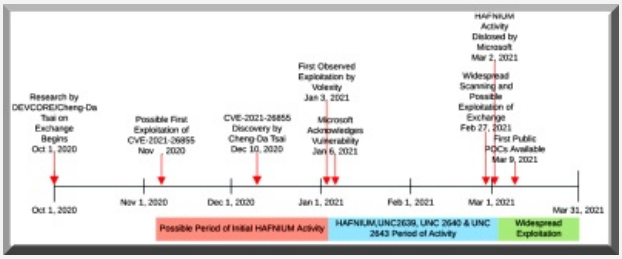
Az ESET kutatói megfigyelték, hogy néhány APT-csoport még a javítások kiadása előtt elkezdte kihasználni a sebezhetőségeket. ***Ez alapján elvethetjük annak lehetőségét, hogy ezek a csoportok a Microsoft frissítések kódjainak visszafejtésével hoztak volna létre egy exploitot.”*** **- nyilatkozta Matthieu Faou, az Exchange sebezhetőségi láncát vizsgáló kutatás vezetője.**



Az ESET óránkénti kimutatása a CVE-2021-26855 Exchange biztonsági résen keresztül hozzáadott webshell kódokról, az észlelések eloszlása országonként (2021.02.28. és 2021.03.09. között)

Az ESET telemetriai adatai alapján több mint 1**15 ország több mint 5000 egyedi szerverén észlelt webshell kódokat, vagyis olyan rosszindulatú programokat vagy szkripteket, amelyek lehetővé teszik a szerver távoli vezérlését a böngészőn keresztül.**

A kutatói team **több mint tíz különböző kiberbűnözői csoportot azonosított, amelyek vélhetően úgy használják ki a közelmúltban közzétett Microsoft Exchange RCE biztonsági réseket,** hogy rosszindulatú programokat, például webshell kódokat és hátsó ajtókat telepítenek az áldozatok levelezőszervereire. Ráadásul néhány esetben egyszerre több csoport is megtámadta ugyanazt a szervezetet.



Íme a beazonosított különböző kiberbűnözői csoportok és viselkedési mintáik:

 # Tick - kompromittálta egy IT-szolgáltatásokat nyújtó kelet-ázsiai székhelyű vállalat webszerverét. A LuckyMouse és a Calypso esetéhez hasonlóan a csoport valószínűleg még a biztonsági javítások kiadása előtt hozzáfért egy exploithoz.

 # LuckyMouse - kompromittálta egy közel-keleti kormányzati szerv levelezőszerverét. Az APT-csoport valószínűleg már a nulladik napon, legalább egy nappal a javítások közzététele előtt használt egy expoitot.

 # Calypso - kormányzati levelezőszervereket kompromittált a Közel-Keleten és Dél-Amerikában. A csoport valószínűleg már a nulladik napon hozzáfért az exploithoz. A rákövetkező napokban a Calypso üzemeltetői további kormányzati szervezetek és magánvállalkozások szervereit célozták meg Afrikában, Ázsiában és Európában.

 # Websiic - hét magánszférában lévő vállalat levelezőszerverét támadta meg Ázsiában (IT, telekommunikáció és mérnöki területeken) és egy kormányzati szervet Kelet-Európában. Az ESET Websiic névre keresztelte az új tevékenységcsoportot.

 # Winnti Group - kompromittálta egy olajipari vállalat és egy építőipari gépeket gyártó vállalat levelezőszervereit Ázsiában. A csoport valószínűleg még a javítások közzététele előtt hozzáfért egy exploithoz.

 # Tonto Team - kompromittálta egy beszerzési vállalat, illetve egy szoftverfejlesztésre és kiberbiztonságra szakosodott tanácsadó cég levelezőszervereit Kelet-Európában.

 # ShadowPad activity - kompromittálta egy ázsiai székhelyű szoftverfejlesztő cég és egy közel-keleti székhelyű ingatlancég levelezőszervereit. Az ESET észlelte a ShadowPad hátsó ajtók egyik variánsát, amit egy ismeretlen csoport hozott létre.

 # The “Opera” Cobalt Strike - körülbelül 650 szervert támadott meg, főleg az Egyesült Államokban, Németországban, az Egyesült Királyságban és más európai országokban, mindössze néhány órával a javítások közzététele után.

 # IIS backdoors - Az ESET webhéjakon keresztül telepített IIS hátsó ajtókat észlelt négy, Ázsiában és Dél-Amerikában található levelezőszerveren. Az egyik hátsó ajtó Owlproxy néven ismert.

 # Mikroceen - kompromittálta egy közüzemi vállalat levelezőrendszerét Közép-Ázsiában, a csoport által leginkább célzott régióban.

 # DLTMiner - Az ESET több olyan levelezőszerveren észlelte a PowerShell letöltők telepítését, amelyeket korábban az Exchange biztonsági rések kihasználásával támadtak. A támadásban használt hálózati infrastruktúra egy korábban jelentett kriptobányászati tevékenységhez kapcsolódik.

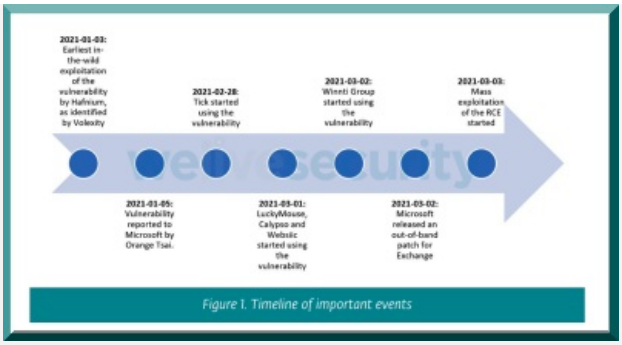


Figure 1. Timeline of important events

Nyilvánvaló, hogy haladéktalanul meg kell kezdeni az összes Exchange-kiszolgáló javítását. Ez még azokra a szerverekre is érvényes, amelyek nem kapcsolódnak közvetlenül az internethez. Kompromittálódás esetén a rendszergazdák feladata a webshell kódok eltávolítása, a hitelesítő adatok módosítása és a teljes átvizsgálás az esetleges további rosszindulatú tevékenységek felfedezése érdekében.

Ez az incidens nagyon jól példázza, hogy az olyan összetett alkalmazásoknak, mint a Microsoft Exchange vagy a SharePoint, nem szabadna védtelenül állniuk az internet előtt. **Az Exchange sebezhetőségét célzó támadások további technikai részletei a WeLiveSecurity "Exchange servers under siege from at least 10 APT groups" című blogposztjában olvashatók.**

Szólj hozzá!
Címkék: microsoft frissítés exchange exploit sebezhetőség sérülékenység kihasználás levelezőszerver

Ajánlott bejegyzések:


Microsoft Teams hiba és hibajavítás


BlueFrag hiba az Androidon


Log4j sebezhetőség - hogyan tovább?


Egyedül nem megy


Eltolás és zoomolás

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Leglegleg - 2020. a kibertámadások tükrében

2021. március 23. 10:31 - Csizmazia Darab István [Rambo]

Az FBI nyilvánosságra hozta a tavalyi év számítógépes bűnözéssel kapcsolatos statisztikai jelentését. **Az összesített kárérték 4.2 milliárd dollár volt,** de a bejelentett panaszok száma sem csekély, 791 ezer.

A bejelentések száma is óriási növekedést mutat az előző esztendőhöz viszonyítva, 69%-os emelkedés olvasható le belőle. A sokféle csalások közül is **hangsúlyosan jelen volt a mindenki életét megkeserítő COVID-19 járvány és az ezzel kapcsolatos megváltozott élet- és munkakörülmények.**

A járványt kihasználó incidensek száma az FBI Internetes Bűnügyi Panaszközpontja (IC3) szerint igen jelentős mennyiségű volt, 28 ezer ezzel kapcsolatos panasz érkezett hozzájuk különféle csalásokról, visszaélésekről. Sok volt az **állítólagos segélyt ígérő, illetve állítólagos pénzügyi támogatást ígérő átverés, ahol általában a személyes adatok megszerzése volt a bűnözők fő célja.**

Az ellopott személyazonosságokkal aztán további kellemetlenségeket tudtak okozni az áldozatoknak.

Természetesen **a vakcina megérkezése óta zajlanak az oltással, az oltási várólistára való azonnali felkerülés, a lista pozícióhoz képest állítólagos előrejutást "kedvezményes áron" ígérő akciók, illetve a vakcinák feketepiaca** is kialakult - ezeket már egységesen oltási csalásoknak is nevezhetjük.

A céges levelezéssel kapcsolatos 19 ezer csalási mellett kiemelten jelentkeztek az úgynevezett romantikus, vagy társkeresési átverések is. Ez utóbbinál profi bűnözők célzottan keresnek olyan jómódú, idős nőket, akik interneten akarnak ismerkedni, és különböző furfangos trükkökkel pénzt igyekeznek kicsalni tőlük.

A Szövetségi Kereskedelmi Bizottság (FTC) friss jelentése szerint **tavaly rekordösszeget, 304 millió dollárt (hozzávetőlegesen 90 milliárd forint) sikerült a társkeresési csalóknak bekasszírozni, ami 50%-os növekedés**

jelent az előző évhez viszonyítva.

A hamis support átverés is csúcsra volt járatva 2020-ban, eszerint az ilyen cselekmények által elkövetett összesített kárérték 146 millió dollár volt, amely ugyancsak nőtt a pandémia idején, egész pontosan 171%-os emelkedést mutat. Az ilyen csalások elkövetői azzal igyekeznek becsapni áldozataikat, hogy nem is létező technikai problémák megoldására e-mailben vagy telefonon ajánlják fel segítségüket. Az ürügy sokféle lehet, lejáró szoftverlicenc, állítólagosan veszélybe került e-mailfiók vagy bankszámla, amelynél személyes adatokat is igyekeznek megszerezni, de sok esetben kártevőt, vagy hátsóajtót telepíttetnek hibajavítás címén az áldozatokkal.

Ez nem csak az USA-ban, de világszerte komoly károkat okoz, például egy tavalyi brit statisztika szerint az átlagosan elszenvedett veszteség az ilyen eseteknél hozzávetőlegesen 2000 angol font, vagyis forintra átszámolva durván 760 ezer HUF volt, ami nem kevés.

A hamis supportos csalások jelentős része valamilyen bank, vagy pénzintézet nevében zajlik, újabban ez lehet akár virtuális valutával kapcsolatos pénzváltás, befektetés is. Sajnos az idősebb - feltehetően tehetősebb - réteget ez súlyosabban veszélyezteti, a számok itt arról tanúskodnak, hogy a 60-ik életév felett ez kiemelt kockázat.

Az összes károsultak 66%-a ebből az idősebb generációból kerül ki, és őket is sújtja legerőteljesebben. Ugyanis az összes ilyen jellegű elszenvedett kár több, mint 80%-a őnáluk jelentkezik.

Van természetesen friss adat **a zsarolóvírus okozta károkról is, amelyek 300 százalékkal emelkedtek az előző évhez képest, elérve a 29.1 millió dollárt.** Sajnos ezen a területen valóban elképesztő ütemű a károkozás, melyekért új fajta ransomware programok, illetve a Ransomware As A Service (RaaS) keretében bárki által, szakértelem nélkül is bérelhető lehetőségek a felelősek. Ezzel együtt az adathalász próbálkozások is folyamatosan ostromolják a felhasználókat.

Van tehát jelenlévő veszély és kockázat bőségesen, emiatt érdemes mind a cégek, mind a magánfelhasználók biztonsága érdekében a védekezés és megelőzése területén kiemelt erőfeszítéseket tenni a ki tudja még

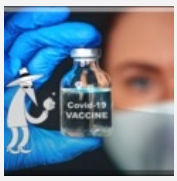
mennyi ideig tartó homeoffice, homeschool, és homemiegymás idején.

Szólj hozzá!
Címkék: statisztika jelentés fbi veszteség károk veszélyek összesítés welivesecurity.com 2020.

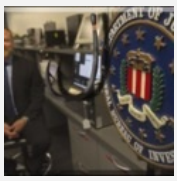
Ajánlott bejegyzések:

Ransomware helyzetjelentés

Nem életrevalók



Vakcinás csalások, szevasztok


Adathalászat - nem középiskolás fokon

Támadás, e-mail a neved

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

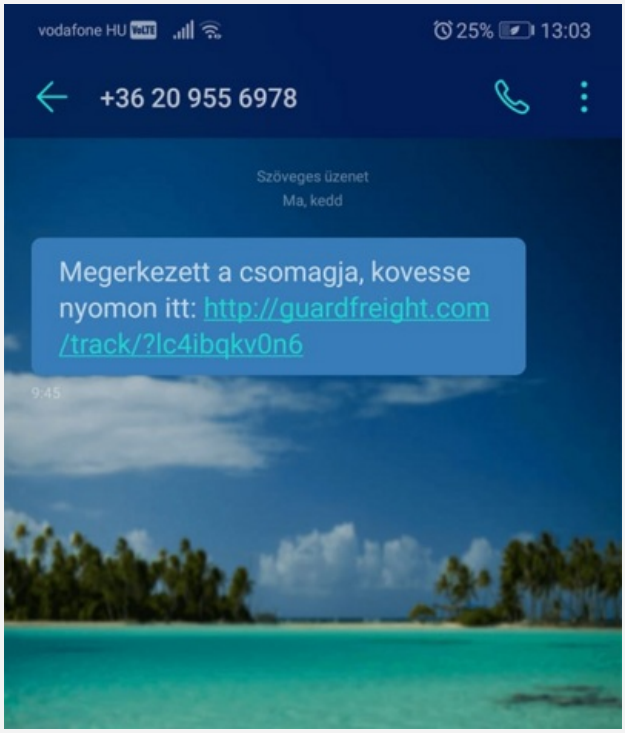
accountz

Belépés
Regisztráció

Megérkezett a csomagja - vagy mégsem?

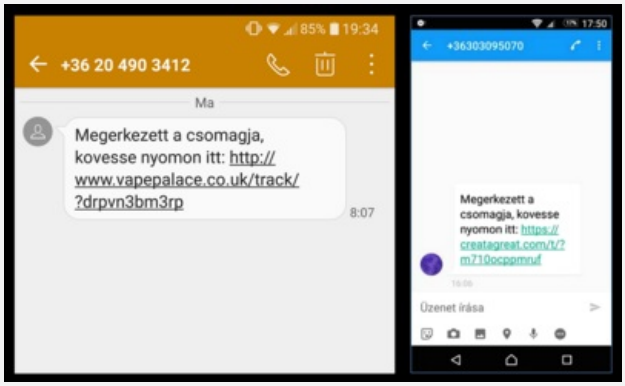
2021. március 25. 10:14 - Csizmazia Darab István [Rambo]

Kifogyhatatlan "vagy mégsem" rovatunk újabb átveréssel jelentkezik. Ezúttal - nyilván **a pandémia alatt felpörgött házhoz szállítások miatt is - egy olyan magyar nyelvű, de ékezetmentes SMS-ünk érkezhet, amely "Megerkezett a csomagja, kovesse nyomon itt: http://akarmi..." üzenetet tartalmaz. Elhinni, kattintani nem érdemes, sőt veszélyes**, további részletek a folytatásban.



A tapasztalatok szerint **több különféle számról is megy ez az sms, nyilván a csalók egész SIM kártya arzenállal rendelkeznek** amiatt, hogy a szolgáltató észlelve a tömeges küldéseket, nehogy könnyen letiltson egyetlen telefonszámot. Más korábbi csalásokban erre például úgynevezett SIMboxot használtak a bűnözők.

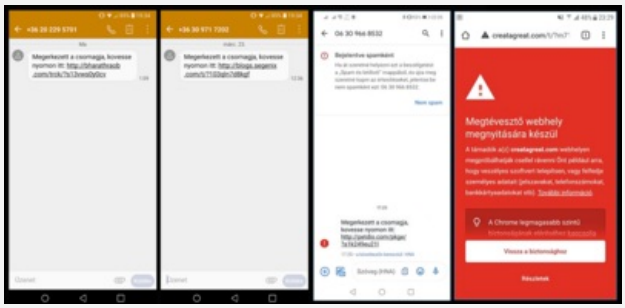
Olvasóink segítségével kaptunk pár ilyen üzenetet ábrázoló képernyőképet, ezekben a csalók linkjei már jórészt nem élnek. **Tehát ezek a kapott SMS-es 20-as és 30-as hazai számokról érkeztek, de nincs okunk kizárni, hogy 70-esről is mehetett ki ilyen.**



Az üzenet **minden esetben tartalmaz egy linket, amelyen egy androidos kártékony kód próbál meg letöltődni a telefonunkra**. A linkek domain neveire a csalók nem sok gondot fordítottak, vagyis meg sem próbálták valamilyen valid, legális, létező csomagküldő URL nevéhez hasonlót választani, hanem látszólag **ahány SMS, annyiféle egzotikus nevű weboldalra mutat.**

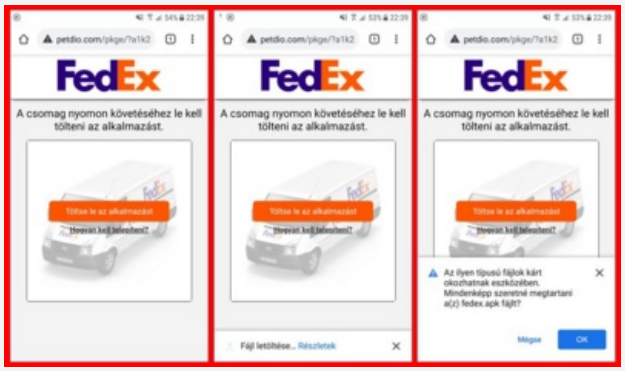
Bár van, amelyik linkben szerepel a "track" azaz nyomkövetés, de ha valaki jobban belegondol, miről szoktuk az adathalász próbálkozásokat könnyen felismerni, akkor a gyatra helyesírás, hiányzó ékezetek, idegen domain név, kattintható link küldése tételek ott is szerepelnek a bűnözők repertoárjában. **Az SMS megnyitás önmagában nem veszélyes, de a linkre kattintás után (amennyiben élő a link), ha letölti és utána telepíti az ottani kártékony .apk fájlt, az már az. A Készenléti Rendőrség Nemzeti Nyomozó Iroda (KR NNI) információ szerint a megfertőzött telefonokról a támadók hívásokat vagy szöveges üzenetek küldését is kezdeményezhetik, és**

ezzel további károkat is tudnak számunkra okozni.



Egyes esetekben már látszott, hogy **az adott számot spammelésért jelentették, illetve a fenti, biztonságtudatos odafigyelésen felül legbiztosabban a naprakész vírusvédelem fogja meg ezeket a próbálkozásokat**. Volt olyan lekattintás is, ahol a Chrome böngésző figyelmeztetett amiatt, hogy **az adott weboldalt már többen gyanúsnak jelentették.**

Az ESET Mobile Security program például "Android/TrojanDropper.Agent.HNJ" néven azonosított és blokkolt egy olyan fedex.apk nevű alkalmazást, amelyet egy ilyen gyanús linkről letöltöttek. **A kártevő egy távoli szerverre továbbítja a készüléken található összegyűjtött személyes adatokat, amelyek akár jelszavak, címjegyzékek, banki azonosító adatok is lehetnek.**



És itt beszúrhatjuk nyugodtan, az Androidos rendszereken **a naprakész vírusvédelem, az alkalmazások és az operációs rendszer biztonsági frissítéseinek mihamarabbi futtatása mellett kulcsfontosságú, hogy honnan és milyen programokat telepítünk.**

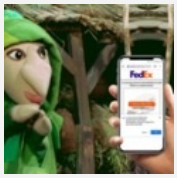
Normál helyzetben érdemes ragaszkodni a hivatalos Google Play áruházhoz, és blokkolni minden egyéb külső forrásból származó program telepítését (egyébként is ez az alapértelmezett állapot, ha valaki nem állítja át.)

A rengeteg próbálkozás miatt a rendőrség honlapján is megjelent már egy ezzel kapcsolatos általános figyelmeztetés. **Ha megfertőződött a telefon**, akkor gyári állapotra való visszaállítás biztos megoldás lehet, ám akkor minden adatunk törlődik, ezért ezt csak végszükség esetén érdemes alkalmazni. **Amit érdemes megtenni, hogy letöltünk egy vírusvédelmi programot és lefuttatunk egy teljes ellenőrzést. De ez a már korábban ellopott, illetéktelen kezekbe került adatainkat nem hozza vissza. Emiatt érdemes lehet a bankunkat is értesíteni a történtekről.**

Mit tehetünk viszont a megelőzésért? Mindig figyelmesen járjunk el a kéretlen üzenetekkel, ha nem vagyunk ügyfelek, nem is várunk küldeményt akkor ez fokozottan igaz, és gyanakodjunk, ha nem is hasonlít az URL cím a szolgáltatókéhoz. Tartsuk naprakészen, frissítve a készülékünket, és mindenképpen használjunk valamilyen komplex internetbiztonsági (vírusvédelmi) programot, valamint csak megbízható forrásból telepítsünk alkalmazásokat.

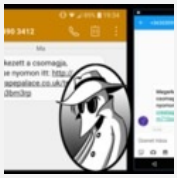
2 komment
Címkék: sms vagy csomag csalás átverés trójai android fedex adatlopás csomagküldő vagymégsem

Ajánlott bejegyzések:


Sárkány ellen sárkányfű


Ingyenes Omikron teszt vagy mégsem?


Nyerd meg az életed - vagy mégsem?


Csak a felszín más: csomagküldés helyett frissítés

Duplázd meg a pénzedet - vagy mégsem?

Kommentek:

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2021.03.26. 05:46:34

Újabb részletek az adatlopás részével kapcsolatban:
www.napi.hu/tech/csomagkuldos-kartevo-vigyazzon-ha-ezeket-az-alkalmazasokat-hasznalja.725836.html

Válasz erre

ebella 2021.03.28. 05:59:40

Nem akarok nagyon okosnak látszani, de soha nem nyitok meg olyan levelet, amiről nem tudom honnan jött. Naponta kapok nem is egy levelet, amit a szemétbe dobok azonnal: Nyertem. Sok pénzem gyűlt össze a kamatokból. A NAV visszatérít. stb. Mégha csomagot is várok, akkor is tudnom kell kitől rendeltem. Mire nyitnám meg az ismeretlen feladótól jövő" jelzést"? Ha az ember minden szemetet elolvasna, jó sok ideje menne el a teljesen felesleges olvasással. Az imént töröltem ki huszonegy levelet, ami tegnap dél óta jött. Mire olvastam volna el azokat?

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

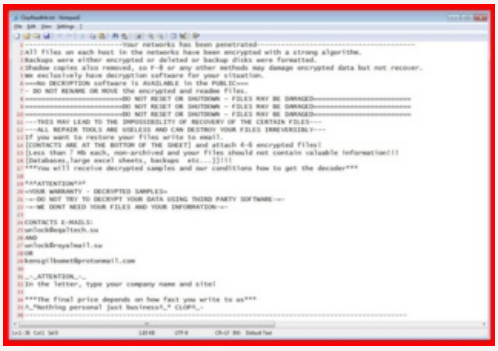
"Illetéktelen fél korlátozott ideig hozzáférhetett fájlokhoz"

2021. március 30. 13:12 - Csizmazia Darab István [Rambo]

A **Royal Dutch Shell elismerte, hogy a rendszereibe behatoltak és ott ransomware támadás történt.** Hivatalos nyilatkozatukban azt írták, hogy "Illetéktelen fél korlátozott ideig hozzáférhetett fájlokhoz." Ez annyira igaz, hogy **a bűnözők most nyilvánosságra is hozták az onnan ellopott munkavállalói útlevelek, valamint vízumok egy részét, hogy ezzel serkentsék az olajcéget a váltságdíj kifizetésére.**

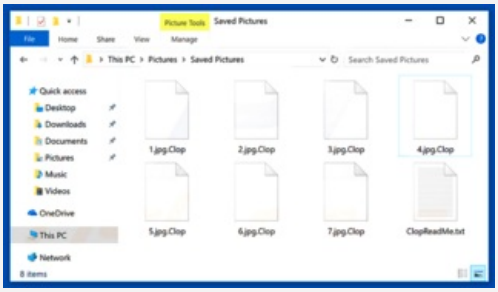
Még **a hónap elején történt incidensben a Clop zsarolóvírus fertőzte meg a rendszerüket, ám a vállalat igyekezett ezt kisebbfajta, jelentéktelen eseménynek beállítani,** és mindenkit azzal nyugtatott, hogy nincs konkrét bizonyíték arra, hogy a támadásnak a Shell alapvető informatikai rendszereire bármilyen hatása lenne, bár érzékeny és személyes adatok veszélybe kerülhettek.

Most viszont ehhez képest **fordulat, hogy a kiszivárgott adatok egy része napvilágra került. Szakértők szerint az ott használatos Accellion File Transfer Appliance alkalmazás egy sebezhetőségét használhatták ki a támadók.**



A publikussá tett anyagok között találhatóak az alkalmazottak amerikai vízumai, valamint útleveik beszkennel oldalai, valamint céges akták az amerikai és magyar irodáikból.

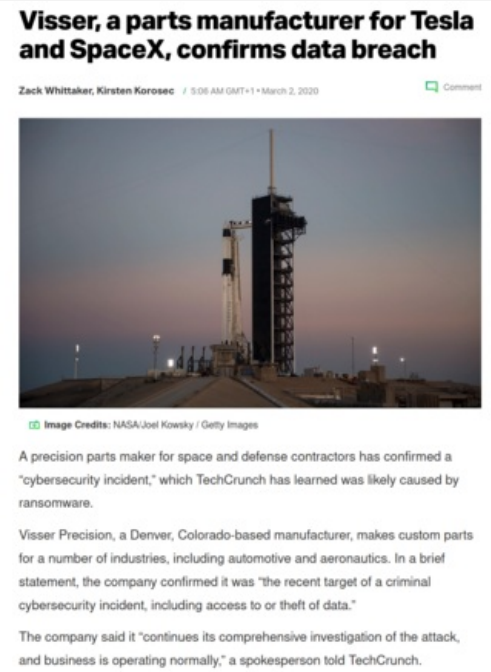
A vállalati ügyfelek elleni ransomware támadások sorában ez már sokadik ilyen jellegű incidens, ahol ha nem hajlandóak fizetni az elkódolt adatok helyreállító kulcsaiért, akkor ezt kiegészítik azzal a zsarolással, hogy a titkosítás előtt ellopott adatokat nyilvánosságra hozzák nemfizetés esetén.



A **Clop banda további jelentős áldozatairól is beszámolt a sajtó, ezek között találjuk a kanadai Bombardier repülőgépes céget, ahol katonai radarokkal kapcsolatos bizalmas információk szivárogtak ki, valamint a londoni The7stars hirdetési ügynöksége és a német Software AG** óriásvállalatot is.

A nagyvállalatokat célzottan támadó bűnözők szinte minden esetben azt állítják, hogy sikeresen loptak el adatokat, bár ez az esetek jó részében nem igaz. Ám **mivel nagy a tét, és a kockázat, szinte mindig elkezdődik egyfajta alkudozás a váltságdíj összegéről, hogy az esetlegesen illetéktelen kezekbe került adatok ne kerüljenek**

mégse nyilvánosságra.



Visser, a parts manufacturer for Tesla and SpaceX, confirms data breach

Zack Whittaker, Kirsten Korosec / 5:08 AM GMT+1 • March 2, 2020 Comment

Image Credits: NASA/Joel Kowsky / Getty Images

A precision parts maker for space and defense contractors has confirmed a "cybersecurity incident," which TechCrunch has learned was likely caused by ransomware.

Visser Precision, a Denver, Colorado-based manufacturer, makes custom parts for a number of industries, including automotive and aeronautics. In a brief statement, the company confirmed it was "the recent target of a criminal cybersecurity incident, including access to or theft of data."

The company said it "continues its comprehensive investigation of the attack, and business is operating normally," a spokesperson told TechCrunch.

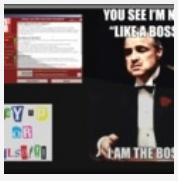
A tavalyi hasonló incidensek áldozatai között olyan jelentős vállalat neveket találhatunk, mint például a Tesla, a Lockheed-Martin, a Boeing vagy a SpaceX. Emlékezetes ugyanakkor, hogy éppen **a Clop csoport ténykedését vizsgálva jutottak biztonsági szakértők arra a következtetésre, hogy 2021-ben már kifejezetten a céges célpontok felső vezetőinek munkaállomásai felé irányulnak a támadások.**

Ugyanis innen jelentős mennyiségű érzékeny dokumentumot lehet megszerezni, amelynél a korábbi klasszikus csak elkódolásos zsarolás mellett már valóban sokkal fontosabb lesz az adott vállalatnak, hogy mégis fizessen.

Szólj hozzá!
Címkék: nyilvános céges támadás publikus shell váltságdíj adatlopás adatszivárgás ransomware zsarolóvírus clop

Ajánlott bejegyzések:

Te nem kapod vissza, de mindenki más igen



Ransomware a csúcs felé tör

5 ok, amiért a ransomware még sokáig velünk maradhat

Miért nem másolja egyszerűen vissza őket?

Van másik!

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

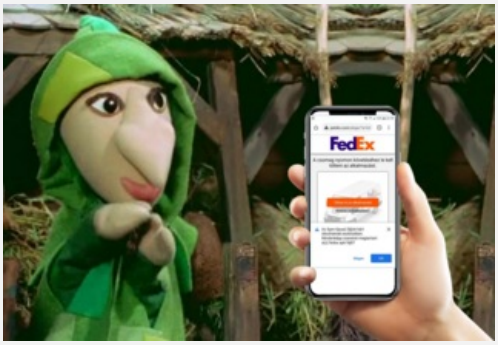
accountz

Belépés
Regisztráció

Sárkány ellen sárkányfű

2021. április 06. 12:23 - Csizmazia Darab István [Rambo]

A múlt heti Fedex nevével visszaélő "Megerkezett a csomagja, kovesse nyomon itt" SMS spam hullám komoly zűrzavarokat okozott, némely felhasználó esetében pedig konkrét, számszerűsíthető veszteséget is okozott. **A kártevő sikeres eltávolítását némiképp bonyolítja, hogy a korábban a Készenléti Rendőrség Nemzeti Nyomozó Iroda (KR NNI) munkatársai által is jó szívvel ajánlott FluBot Malware Uninstall nevű alkalmazás időközben sajnálatos módon eltűnt a Google Play áruházból. Mutatjuk, mi lehet a megoldás.**

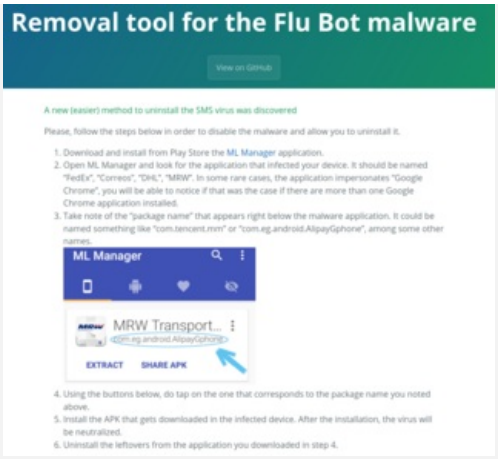


Elöljáróban arra érdemes kitérni, hogy **néhány korábbi cikk tévesen azt állította, hogy a Google saját piacterén található FluBot Malware Uninstall kártékony lenne**. Valójában viszont ez volt az ellenszer, ugyanis eltávolította a hamis fedexes vírusos alkalmazást, **amit éppen a gyanútlan áldozatok által megadott sok engedély miatt nehéz volt eltávolítani.**

A Google Playről való kikerülés okára a program készítője egy időközben eltávolított Twitter posztban utalt, "nehézfejűségre" utalva: "*The updates are both in queue for @GooglePlayDev to approve. Most likely, they won't reach the production state in Play Store until Monday or Tuesday, which means GitHub is the only place to get the latest version as of right now. Thanks for the unnecessary bureaucracy, Google!*" Érdekesség még, hogy **ez a tömeges SMS spam hullám a magyarországi terjedéssel egyidőben Németországban, valamint Lengyelországban is megjelent.**

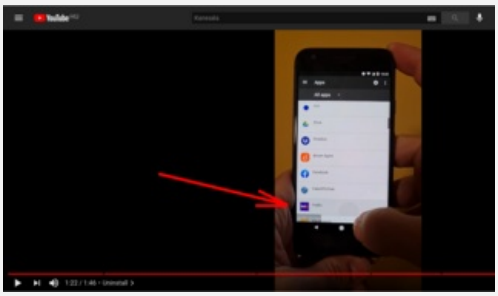
A hivatalos piactérről való eltűnés után **az eltávolító alkalmazás kikerült a Github weboldalra, ott forráskóddal együtt máig elérhető**. Igaz, ha valaki az SMS fertőzésből csak annyit jegyzett meg, hogy csak a Google Play oldaláról telepítsünk alkalmazásokat, külső forrásból soha, akkor most lehet, hogy gyanakodva vagy elutasítóan fogadta ezt a szintén csak külső forrásból letölthető, és kézzel telepítendő elviekben megbízható mentesítő programot is.

A Linuxct nevű fejlesztő emiatt aztán közreadott egy megkerülő (workaround) megoldást is, amelyben egy másik hivatalosan letölthető alkalmazás segítségével is meg lehet szabadulni a kártevőtől az útmutató lépéseinek segítségével.



Azt, hogy miért nehézkes a banki adatokat ellopó Flubot malware eltávolítása, arról a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet munkatársai által ehhez a témához készített podcast adásból lehet többet megtudni. **Ennek lényege, hogy ha valakinél korábban már eleve telepítve volt vírusvédelmi alkalmazás, az nem fertőződhetett meg ezzel az átveréssel. Kivétel az az eset, ha valaki a vírusvédelmi programok freemium változatát használta, és nem frissített vírusismereti adatbázist rendszeresen, az ingyenes verziókban ugyanis gyakori, hogy nem automatikusan frissül, hanem manuális kell azt mindig elvégezni.**

A Fedex vírus esetében a fő problémát az úgynevezett "Accesibility services" engedélyezése okozta, ugyanis ekkor ez az opció a védelmi programok elől elrejti a futó kártékony szolgáltatást, a kártevő hozzáfér a banki SMS-einkhez is, valamint a szokásos sima törlés uninstall ekkor nem működik.



Mi most viszont az ESET vírusvédelmi laborjának megbízható ismertetőjét mutatjuk, amely ennek a nehézkesen eltávolítható Flubot SMS kártevőnek a törlését mutatja be egyszerűen lépésről lépésre egy Youtube videó formájában.

Ennek lényege, hogy ha gyaníthatóan fertőzött a telefonunk, és a futó folyamatok között megtaláljuk a Fedexes vagy bármilyen más gyanús szervizt, akkor Safe módban kell újraindítani az eszközt, mert ebben csak a gyári alkalmazások élednek fel. Ekkor már lehetséges lesz a kártékony program eltávolítása.

Az emlegetett hazai anyagi károk között kétféle esetről is napvilágot láttak beszámolók. A Flubot telepítése után ugyanis minden a telefonunkon tárolt adatunkhoz hozzáfértek a bűnözők: az SMS-ek tartalma, a címjegyzék, kamera, mikrofon, bluetooth kapcsolat, jelszavaink, netbankhoz, kriptovaluta tárcánkhoz tartozó jelszavaink is, és a megfertőzött telefonokról hívásokat, SMS-ek (tovább)küldését is kezdeményezhették.

Emiatt aztán volt olyan magyar áldozat, akinek a bankszámláját is kifosztották, több millió forintos kárt okozva. Akit esetleg hasonló anyagi kár ért, az közvetlenül is jelentkezhet a rendőrség által megadott kiber@nni.police.hu e-mail címen.

Ám a járulékos károk ezzel még nem értek véget, ugyanis éppen a tömeges SMS küldések további anyagi veszteséget okoztak, mivel **a kiküldött SMS-ek pénzdíja mindig az áldozatokat terheli. Volt olyan áldozat, akinek a telefonjáról 4700 SMS üzenetet küldtek el, csak ez 35 forintjával számolva 160 ezer forintos plusz számladíjat jelent.**

Ettől csak egy előre beállított SMS küldési korlát menthet meg minket, illetve mivel **a saját fertőzött telefonon nem jelennek meg a kiküldött SMS üzenetek adatai, így kizárólag a szolgáltatók saját alkalmazásaiban (MyTelenor, Telekom, MyVodafone) lehet csak a valós forgalmi adatokat ellenőrizni.**

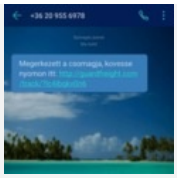
És végül még egy fontos tanulsága az esetnek. A kártevő eltávolítása - akár a fenti Safe módban való törléssel, akár a saját adatok mentése után a készülék gyári állapotába való visszaállítással végezzük - a már korábban ellopott személyes adatainkat nem hozza vissza, emiatt mindenképpen érdemes a bankunkat is értesíteni a történtekről. Ajánlott a telefonos alkalmazásainkban, szolgáltatásainkban használatos jelszavaink azonnali cseréje is, beleértve a banki felületekhez tartozókat is.

A sikeres megelőzés szempontjai pedig az alábbiak lehetnek:

- Mindig figyelmesen járjunk el a kéretlen üzenetekkel
- Ellenőrizzük, valóban attól a szolgáltatótól kaptuk-e az értesítést, amelytől csomagot várunk.
- Legitim forrásból telefonra szinte soha nem küldenek internetes linket.
- Adathalász intő jelek: gyenge helyesírás, hiányzó ékezet, sürgetés vagy ígéret, mellékelt link
- Gyanakodjunk, ha nem is hasonlít az URL cím a szolgáltatókéhoz
- Ha kérik, hogy kapcsoljuk ki a biztonsági figyelmeztetéseket a mobiltelefonunkon, az is gyanús
- Csak megbízható, hivatalos forrásból telepített alkalmazások pl. Google Play áruház
- Blokkoljunk minden egyéb külső forrásból származó program telepítést (ez az alapértelmezett állapot, ameddig valaki át nem állítja.)
- Alkalmazások és operációs rendszer biztonsági frissítéseinek gyakori és mihamarabbi futtatása
- Vírusvédelmi szoftver, amely automatikusan blokkolja a kártékony tartalmak elérését.

1 komment
Címkék: spam sms csalás átverés trójai mode eset uninstall banki fedex adatlopás safe csomagküldő eltávolítás

Ajánlott bejegyzések:



[Megérkezett a csomagja - vagy mégsem?]

[Egypálcás adathalász próbálkozások]

[Azt mondod Covid19, azt mondom spam]

[A bankos mindig kétszer csenget...]

[Ingyenes Omikron teszt vagy mégsem?]

Kommentek:

efi 2021.04.07. 17:29:34

És mire megyünk azzal, ha elküldjük az NNI-nek, hogy balekok voltunk?
Továbbá én csak prepaid előfizetést használok, ott soha nem fog előfordulni, hogy százezreket elsmsezik a telefon suttyomban.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

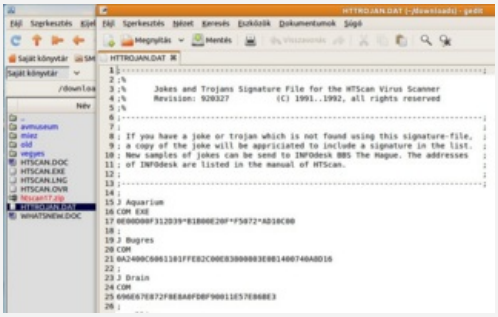
Titkosítok, tehát vagyok

2021. április 09. 11:55 - Csizmazia Darab István [Rambo]

Na jó, ez a témakör hatalmas, és **most csak egy icipici szeletét tárgyaljuk, de emellett előhúzunk néhány olyan előfordulást is a 35 éves vírustörténelem nagy kalapjából**, amire talán már csak a nagyon régi motorosok emlékezhetnek.

A vírusvédelem hőskorában - ezalatt most a 80-as évek végét értsük, a vírusirtók 1-2 havonta kaptak csak adatbázis frissítést, amiket az akkori MS DOS, sárga vagy zöld monokróm Hercules monitoros környezetben üzemelő gépeken, 1200, 2400 vagy 3600 baud-os betárcsázós modemmel (8 adatbit, 1 stop bit) léptünk be az olyan BBS oldalakra, mint például a VirNET. Ott szerepelt például a HTScan, **amiben még szövegfájlban mi magunk editálhattuk a szignatúra szekvenciákat, amik az adatbázis felismerésben működtek.**

Azóta persze már régóta tömörítve, kriptográfiai aláírással, titkosítva illik ilyen adatbázist készíteni, a lopás, illegális módosítás, célzott támadás megelőzése, a hitelesség megőrzése érdekében.



Ugyancsak a titkosítás témakörben említhetjük azt a bizonyos 2013-ban napvilágra került incidenst, amelynél Snowden jóvoltából az derült ki, hogy az RSA - ami ugyebár titkosítási termékeket fejleszt - az NSA kérésére szándékosan gyengített a titkosításon. **10 millió dollárért ugyanis egy jóval gyengébb, azaz könnyebben feltörhető véletlenszám-generátort tettek a BSAFE biztonsági eszköztárába**, amelyben egyes vélemények szerint a Dual_EC_DRBG modul backdoort is tartalmazott.

Ezt az etikátlan hozzáállást többen, köztük a vírusvédelemmel foglalkozó Mikko Hypponen is élesen kritizálta, például a Twitteren kijelentette, hogy "az egész iparág nevében szégyelli magát". Sőt később emiatt a 2013-as RSA konferencián való előadói szereplését is lemondta.

Ugyancsak furcsa eset volt, amikor a korábban népszerű és ingyenes TrueCrypt titkosító alkalmazással szemben is kételyek merültek fel még 2014-ban. Akkor egy közösségi összefogás révén lezajlott egy biztonsági audit, amely azzal zárult, hogy nincs hátsóajtó a programban, mindenki bátran továbbhasználhatja. Majd egyszercsak váratlanul megszűnt, az anonimitásukat megőrző fejlesztők lehúzták a rolót, **sokan NSA nyomást feltételeztek a háttérben.** Egy svájci domain még egy ideig biztatott a folytatással, de ma már ez az oldal is üresen tátong.

Sőt, a 2015-ös Potao nevű kártevőcsaládot, amellyel ukrán tisztviselők és újságírók után is kémkedtek, egy olyan orosz nyelvű hamisított weboldalról terjesztették, amelyről a Truecrypt fájl- és lemeztitkosító szoftver egy módosított, rosszindulatú trójai változatát lehetett letölteni. A TrueCrypt esetében is, és később a bűnözőktől lefoglalt iPhone telefonoknál is láttunk olyan eseteket, ahol például Nagy Britanniában az el nem árult jelszó több évnyi súlyos börtönbüntetést vont maga után.

A SkyECC végponttól végpontig titkosított üzenetküldő alkalmazást fejlesztő Sky Global cég vezetőit most tavasszal azzal vádolták meg, hogy tudatosan és szándékosan vettek részt egy olyan bűnözői vállalkozásban, amely megkönnyítette a kábítószerek terjesztését az általuk kínált titkosított kommunikációs eszközök értékesítésével és szolgáltatásával. Felelős lenne Bill Gates azért, hogy ki használja a Windowst? **És akkor a mostani hír, miszerint a belga rendőröknek "sikerült feltörni" a SkyECC csevegőalkalmazás titkosítását, és az így megszerzett információk birtokában 28 tonna kokaint foglaltak le.**

Mit jelenthet itt a "sikerült feltörés"? **Nagyon sokféle dolog vezethetett eredményre anélkül, hogy magát a matematikai alapon működő rendszert valójában fel tudták volna törni, sőt igen valószínű, ha ez történt volna, úgy mindezt nem is hozták volna nyilvánosságra, hiszen akkor a jövőben titokban lehallgathatnának bármit. Sokkal valószínűbb, hogy trójai alkalmazással, billentyűzetnaplózóval, kémprogrammal jutottak eredményre, vagy egyéb módon kiszivárgott jelszavakkal, kulcsokkal tudtak eredményt elérni, vagy akár hamis frissítő szervereket üzemeltettek - ezt sosem fogjuk megtudni.**

Időről időre felvetődik viszont, hogy a hatóságok beépíthessenek hátsóajtót a titkosító alkalmazásokba, ami nemcsak azt a veszélyt hordozza, hogy hamis biztonságérzetet nyújt a felhasználóknak, hanem azt is, amire **például Bruce Schneier és Richard Stallman is rendszeresen figyelmeztetnek, hogy a vírusterjesztő, kémkedő bűnözők is kihasználhatják azokat. Amire volt is már példa a rootkitek esetében, ahol a "láthatatlan" könyvtár szabad prédává vált a rejtett vírusoknak**, sőt ez akkoriban számos vírusvédelmi program előtt is észrevétlen maradt.

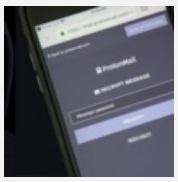
Nem is beszélve arról, hogy **a titkosszolgálatoktól történő zeroday exploitok lopása sem példa nélküli. Ilyen volt az EternalBlue és a DoublePulsar nevű támadó eszköz, amelyeket az NSA-tól lopott el a Shadow Brokers hackercsapat, és ezt használták fel a 2017-es világszerte hatalmas károkat okozó WannaCry kártevő terjesztésénél.**

Viszont ami számunkra kiemelendően fontos, hogy titkosítást nem csak a bűnözők használnak, sőt ennek alkalmazása nem csak hogy legitim, hanem egyenesen kívánatos, sőt egyenesen nélkülözhetetlen a magánélet, a céges információk, személyes adatok hatékony megóvása érdekében, nem is beszélve a GDPR által támasztott kötelezettségekről.

A palettán pedig számos megbízható lehetőség szerepel, a hétköznapi GPG-től a nagyvállalati központi menedzselésű programokig bezárólag, amiket érdemes használni.

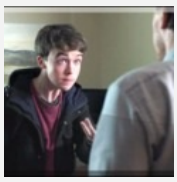
1 komment
Címkék: privátszféra truecrypt magánélet titkosítás feltörés gpg encryption skyecc

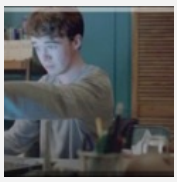
Ajánlott bejegyzések:


Bezzeg régen minden jobb volt?

GoDaddy - apák a pácban


Az online térben hagyott személyes adataink


Zsarolás hasra ütésre


Mai szavunk pedig: sextorsion

Kommentek:

Vaki Vaki 2021.04.11. 15:37:59

A TrueCrypt tovább él VeraCrypt néven.

Hogy ugyanazok fejlesztik-e, azt nem tudni, de megmaradt nyílt forrásúnak és nagyon biztonságosnak.

Mindenesetre hatalmas dicséret a TrueCrypt csapatnak, inkább eldobták a felépített brandet, a befektetett időt-pénzt, de nem feküdtek le az NSA "kérésének".

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

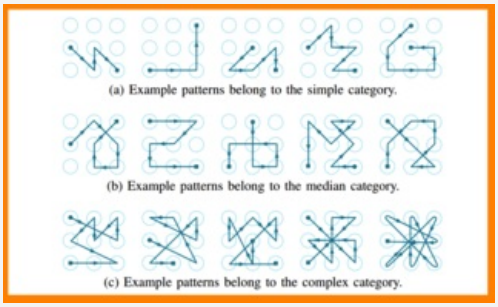
7 tipp a mobilunk védelméhez

2021. április 14. 11:44 - Csizmazia Darab István [Rambo]

Az elmúlt napokban komoly zűrzavart, több esetben anyagi kárt is okoztak a tömegesen kiküldött, csomag érkezéséről szóló csaló SMS-ek. Az incidens ráirányította a figyelmet arra, hogy **az okostelefonok esetében is kulcsfontosságú, hogy gondoskodjunk a megfelelő védelemről. Mik azok az óvintézkedések, amelyeket érdemes betartani a készülékünk, illetve a rajta tárolt személyes és banki adataink védelme érdekében?**

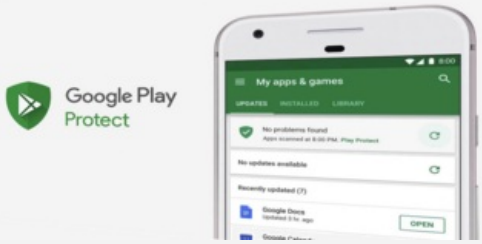
1. Biztonságos lezárás
Mindig zárjuk le biztonságosan készülékünket, és kerüljük az olyan egyszerű, de gyenge megoldásokat, mint például egy "L" alakú feloldóminta, vagy az „1234” jelszó beállítása. **Feloldóminta esetén rajzoljunk bonyolult alakzatokat, a feloldókód megadásakor pedig egyedi, minél hosszabb számsort adjunk meg.**

Ha van rá lehetőség, használjunk biometrikus jellemzőt is (például ujjlenyomatot vagy arcfelismerést) a jelszó vagy minta mellett.



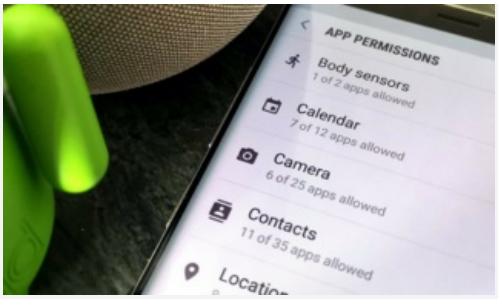
2. A hivatalos áruház használata
Akármennyire is csábítóan hangzik, hogy a hivatalos Google Play vagy App Store áruházon kívül más forrásokból is letöltsünk alkalmazásokat, ezzel az eszközünket szükségtelen kockázatoknak tennénk ki.

A nem hivatalos alkalmazásboltokat nem ellenőrzik olyan szigorúan és rendszeresen, mint a hivatalos verziókat, ezért nagyobb az esélye, hogy azokról rosszindulatú alkalmazásokat töltünk le.



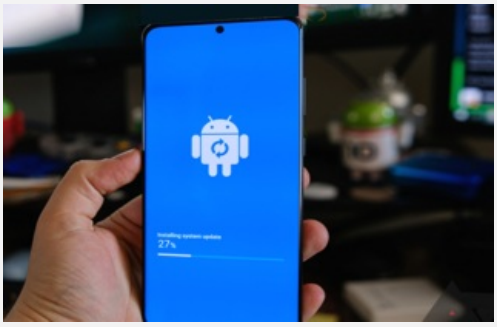
3. Alkalmazások engedélyei
Az alkalmazások telepítéskor különféle engedélyeket kérnek, amelyeket a figyelmetlen átgörgetés helyett érdemes átolvasni, és **ha valami gyanúsat észlelünk, akkor inkább keressünk egy másik applikációt. Ha mindent gondolkodás nélkül elfogadunk, akkor lehet, hogy ezzel lehetővé tesszük, hogy hozzáférjenek az eszközön tárolt adatainkhoz**, vagy pénzt csaljanak ki tőlünk, esetleg kémkedjenek utánunk.

Az ESET kutatói például pár évvel ezelőtt **felfedeztek egy magát ártalmatlan zseblámpa alkalmazásnak álcázó trójai programot, amely valójában banki azonosítókat próbált megszerezni.**



4. Biztonsági szoftver használata és javítások
Ma már az okostelefonokra hasonló veszélyek leselkednek, mint a számítógépekre, hiszen ugyanúgy vírustámadás áldozatává válhatnak, vagy akár illetéktelenek férhetnek hozzá a kameráikhoz. Az Android rendszerekre fejlesztett ismert, megbízható biztonsági szoftverek számos kellemetlenségtől kímélhetnek meg bennünket. **Védelmet nyújtanak a kiberfenyegetések és trójai fertőzések ellen, blokkolják a gyanús weboldalakat, biztosítják az érzékeny adataink védelmét, és segítséget nyújtanak az elveszett vagy ellopott eszközök megtalálásában is.**

A biztonsági program mellett **mindig telepítsük a készülékünkre a legfrissebb hivatalos alkalmazás és opererációs rendszer frissítéseket is, mivel azok gyakran tartalmaznak olyan biztonsági hibajavításokat is, amelyek segítenek a védekezésben.**



5. Titkosítás, biztonsági mentés
A biztonsági mentés lényege, hogy minden fontos fájlunkról (családi képek, dokumentumok, e-mailek) készítünk egy másolatot, amelyet az eszközünkön kívül tárolunk. A fájljaink ugyanis számos különféle módon megsérülhetnek vagy elveszhetnek. Például **a telefonunkat ellophatják, meghibásodhat vagy valamilyen baleset érheti (tűz, víz, leesés), de akár olyan rosszindulatú vírustámadás áldozatává is válhat, amely megrongálja vagy lezárja a rajta lévő fájljainkat.**

Ezekben az esetekben csökkentheti a bosszúságunkat, **ha legalább a rendelkezésünkre áll egy biztonsági mentés, amelyet az adatok helyreállításhoz használhatunk.**

6.Legyünk tisztában a veszélyekkel
Az okostelefonok esetében a kártevők és rosszindulatú alkalmazások mellett gyakori problémát jelent az adathalászat és a különféle átverések. Az adathalász csalások sokféle formában léteznek. Például kaphatunk fertőzött linkeket tartalmazó SMS-eket, amelyek rosszindulatú szoftvert tartalmazhatnak, vagy - ahogy a legutóbbi incidens során is láthattuk - egy kártékony alkalmazás letöltésére próbálnak rávenni.

A közelmúltban az is előfordult, hogy nemzetközi számokról hívták fel az áldozatokat - olyan országokból, amelyekkel a hívott félnek soha nem volt eddig kapcsolata. **Ha visszahívjuk a számot, extra magas számlaköltségeket okozhatnak nekünk**, ezért kétszer is gondoljuk meg, hogy visszahívunk-e külföldi, ismeretlen számokat. **Az elmúlt hetekben megjelent "Csomagja érkezett..." SMS FedEx csalássorozatban például a fertőzött telefonokról történt tömeges SMS küldések révén további anyagi veszteséget okoztak az áldozatoknak.**

7. Biztonságtudatosság, óvatosság
Az eszközeink biztonságát gyakran mi magunk veszélyeztetjük. **Hajlamosak vagyunk azt gondolni, hogy hétköznapi felhasználóként nem vagyunk elég érdekesek vagy értékesek a bűnözők számára, ezért nem tesszük meg a szükséges védelmi intézkedéseket. Ugyanakkor a legutóbbi SMS incidens is megmutatta, hogy a csalók nem konkrét célpontokat támadnak, hanem tömegesen próbálkoznak, remélve, hogy minél több gyanútlan felhasználót sikerül megtéveszteniük.**

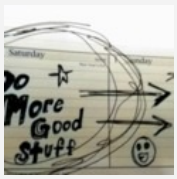
Ha felismerjük, hogy a veszély mindig fennáll, hosszú távon jobban járunk, mert az óvatossággal minimálisra csökkenthetjük a kockázatokat. A biztonsági mentések, a vírusvédelem és a képernyő lezárása mellett fontos, hogy biztonságtudatosan használjuk a telefonunkat. **Ha megfogadjuk ezeket a tanácsokat, készen állunk majd arra, hogy megfelelően kezeljük a váratlan helyzeteket.**

Szólj hozzá!
Címkék: biztonság trükkök tippek védelem megelőzés okostelefon tanácsok android eset védekezés

Ajánlott bejegyzések:

Az egyik COVID-19, a másik egy híján 20


Okoseszközeink biztonsága



10 kiberbiztonságra veszélyes szokás


Sötétben bújkáló shadowIT


Fiatal vagy? Ezekre az online csalásokra figyelj!

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

Az egyik COVID-19, a másik egy híján 20

2021. április 20. 10:12 - Csizmazia Darab István [Rambo]

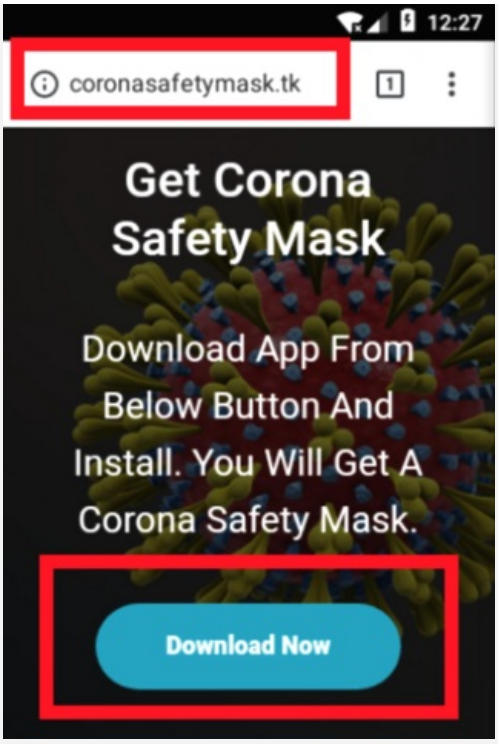
Az oltóanyagok létfontosságú lépést jelentenek a világ koronavírus-járvány elleni küzdelmében, ugyanakkor mindez visszaélésekre is lehetőséget ad a csalók és álhírterjesztők számára. Emiatt most éppen a Bitcoinnal fizethető hamis koronavírus-oltásokra épülő csalásra figyelmeztetnek a nemzetközi hatóságok. **Összefoglaltuk a leggyakoribb, vakcinával kapcsolatos tipikus átveréseket, amelyekkel megpróbálnak hozzáférni a személyes adatainkhoz vagy a pénztárcánkhoz.**

A közelmúltban az INTERPOL és az Egyesült Államok Belbiztonsági Minisztériuma is online terjedő hamis koronavírus-vakcinákkal kapcsolatos átverések veszélyeire figyelmeztettek - **a kiberbűnözők ugyanis egyre nagyobb mértékben próbálják kihasználni a nemzetek oltási programjaiban rejlő lehetőségeket.**

A COVID-19 vakcinák szigorú tudományos és hatósági folyamaton mennek keresztül és csak a nemzeti egészségügyi szolgáltatók forgalmazhatják és adhatják be őket. Ezért, ha belebotlunk egy olyan ajánlatba, ami online vakcinavásárlási lehetőséget ígér az egészségügyi szolgáltató általi hivatalos oltás helyett, akkor egész biztosan hamis termékről van szó.

A koronavírus-oltóanyagokkal kapcsolatos visszaélésekre az Európai Unió csalás elleni hivatala (OLAF) is figyelmeztetett: **csalók hamis vakcinamintákat ajánlanak eladásra, ám a kifizetést követően eltűnnek a pénzzel.**

Az ESET szakértői most bemutatnak néhány **tipikus koronavírus vakcinával kapcsolatos átverést, melyekkel a kiberbűnözők mostanában megpróbálják kicsalni a gyanútlan internetezők személyes információit és pénzét**, illetve alaptalan, hamis kijelentéseket terjesztenek az oltásokkal kapcsolatban.



Hamis piacterek - A kiberbűnözők új fokozatra kapcsoltak a magukat nemzeti vagy globális szervezeteknek kiadó hamis weboldalak létrehozásával, amelyek a COVID-19 oltások állítólagos előrendelését ajánlják fel Bitcoinnal történő fizetés esetén. Annak érdekében, hogy az átverés a lehető leghitelesebbnek tűnjön, **a csalók a koronavírus-vakcinák gyártásában részt vevő gyógyszeripari nagyvállalatok hivatalos logóit tüntetik fel.**

Az INTERPOL gyanúja szerint a hamis webhelyeket **adathalász támadásokhoz használják fel, valamint a gyanútlan áldozatok megkárosítására nem létező jótékonysági szervezetek nevében történő adománygyűjtéssel is próbálkoznak**. A pénzveszteségen túl a potenciális vásárlók számos más egyéb veszélynek is kiteszik magukat, ideértve az egészségügyi kockázatokat, **valamint a személyazonosság-lopást.**


COVID-19 Vaccine Business Proposal

Hello,

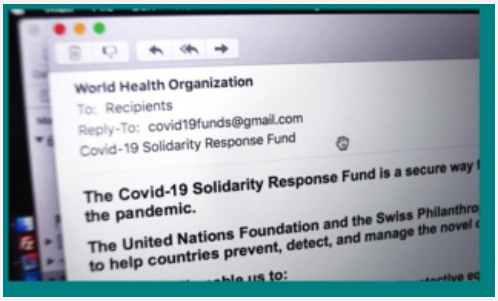
I am Elliot Grayson Research Assistant at Whitman Laboratories Ltd UK. One of the leading Bio Pharmaceutical companies in Europe. I have a business proposal concerning COVID-19 Vaccine for you which is worth a substantial amount and will save lives. I would be glad to receive your acknowledgement of this email so I can furnish you more with details of my proposal for your consideration. Please send your reply to my private email at: @protonmail.com

Please give me the opportunity to explain to you in detail what the business is all about by replying back to my private email as stated above. Note: You have the right to quit by the end of my detailed explanation and you don't feel like moving forward with me. But trust me, you won't regret it.

Elliot Grayson,
Whitman Laboratories Ltd.

Átverős üzleti ajánlatok - Az egyik gyakran alkalmazott taktika magukra a COVID-19 vakcinákra, vagy az előállításukra és tárolásukra használt technológiára fókuszál. **Ebben a levélben a kiberbűnöző a Whitman Laboratories brit gyógyszergyártó cég alkalmazottjának adja ki magát, azt állítva, hogy üzleti ajánlata van számunkra a vakcinával kapcsolatosan.** Az átverések megannyi jellemzőjét találhatjuk meg az e-mailben: csak akkor tudjuk meg az ajánlat részleteit, ha előbb válaszolunk a feladónak, ám maga a levél több nyelvtani hibát tartalmaz és a stílusa is merőben szokatlan egy üzleti levélhez képest.

Érdemes még megemlíteni, hogy **a COVID-19 oltóanyag értékesítéséről folytatott bizalmas tárgyalások szinte kizárólag közvetlenül a gyártók és a kormányok között zajlanak, ezért ha egy kutatási asszisztens céloz meg potenciális vásárlókat egy ilyen megkereséssel, annak minimum kétségeket kell** felvetnie a címzettekben.


World Health Organization
To: Recipients
Reply-To: covid19funds@gmail.com
Covid-19 Solidarity Response Fund

The Covid-19 Solidarity Response Fund is a secure way
the pandemic.

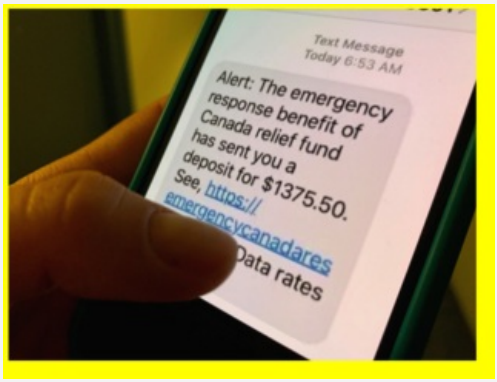
The United Nations Foundation and the Swiss Philanthro
to help countries prevent, detect, and manage the novel

Hamis COVID-19 információk - Egy másik népszerű taktika során a csaló egy olyan ismert egészségügyi hatóságnak adja ki magát, amelyik közvetlen kapcsolatban áll a járványkezeléssel.

Az Egészségügyi Világszervezet (WHO) a koronavírushoz kapcsolódó különféle átverésekben leggyakrabban megszemélyesített hatóságok közé tartozik. A csalók - akik a WHO képviselőinek és alkalmazottainak adják ki magukat - hamis alkalmazásokat vagy fontos információnak beállított álhíreket terjesztenek.

Tobzódás az összeesküvés-elméletekben - A koronavírus helyzet sajnos remek lehetőséget nyújt az olyan e-mailek terjesztésére is, **amelyek azt állítják, hogy a linkre kattintva megtudhatjuk az „eltitkolt igazságot". Ehhez általában egy valós hírt vagy videót is prezentálnak a saját narratívájuknak megfelelően.** De az is gyakori módszer a valóban elhangzott állítások szándékos félreértelmezése és olyan szintű manipulatív átszerkesztése, hogy a végeredménynek már szinte semmi köze nincs az eredeti hírhez. **Mindennek célja, hogy az embereket rávegye a mellékelt linkre való kattintásra.**

Egy másik hasonló típusú e-mail **a Microsoft egyik újonnan bejegyzett szabadalmáról szól. Témája a szabadalom számában megtalálható sátáni szimbólumok, de a Szellemi Tulajdon Világszervezete (World Intellectual Property Organization, WIPO) oldalán történő gyors keresés után kiderül, hogy a találmány nem ördögtől való.** A redmondi székhelyű techóriás egy olyan kriptovaluta rendszert szabadalmaztatott, ami testaktivitási adatokat használ fel. **Ezen e-mailek ugyan nem tartalmaznak vírusokat, de a tartalmuk ettől még tipikus álhír, úgyhogy bár ijesztő**, egyelőre mégsem kell tartanunk a bennük megjósolt végítélet napjától.

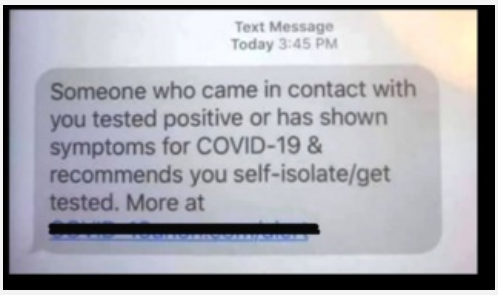


Akkor végül tekintsük át, hogyan maradhatunk biztonságban? Mivel sokan továbbra is türelmetlenül várjuk az oltásukat, **összegyűjtöttünk pár hasznos tippet, melyekkel elkerülhetjük, hogy kiberbűnözők csapdájába essünk**. Ne legyen kétségünk afelől, hogy amint egyre több embert oltanak be, a csalók egyre intenzívebben folytatják majd félrevezető kampányukat, ezért érdemes megfogadni a biztonságunk zálogát jelentő tanácsokat.

- Ne kattintsunk olyan linkekre és ne töltsünk le olyan fájlokat, amelyeket ismeretlen vagy nem hitelesíthető címről érkező e-mailben kaptunk.

- Ha az e-mail állítólag egy hivatalos szervezettől érkezett, látogassunk el a weboldalukra, majd vegyük fel velük a kapcsolatot a hivatalos elérhetőségeiken, hogy kiderüljön, valóban tőlük származik-e a levél. A levélre rá is kereshetünk az interneten, hátha egy már jól ismert, tipikus spam körlevél.

- Vigyázzunk az olyan üzleti ajánlatokkal, amelyek túl jónak tűnnek ahhoz, hogy igazak legyenek - különösen akkor, ha nem hitelesített küldőtől érkeztek.



- Használjunk megbízható, többrétegű biztonsági megoldást a digitális eszközeinken - beleértve az okostelefonokat és a tableteket is -, amely a vírusvédelem mellett kiszűri a spam leveleket és az adathalász weboldalakat is.

- Az oltással kapcsolatos naprakész információkért forduljunk a helyi egészségügyi hatósághoz és a hivatalos kormányzati forrásokhoz.

- Gyanakodva álljunk hozzá minden olyan kéretlen levélhez, amely vakcinákat akar eladni - főleg, ha kriptovalutás fizetést vagy személyes adatokat kérnek érte.

- A bizalmas adatokat tartalmazó felhasználói fiókjainknál engedélyezzük a kétlépcsős hitelesítést.

Szólj hozzá!
Címkék: tippek átverés vakcina megelőzés tanácsok védekezés covid-19 covid

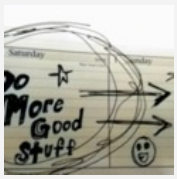
Ajánlott bejegyzések:


Fiatal vagy? Ezekre az online csalásokra figyelj!


7 tipp a mobilunk védelméhez


Ingyenes Omikron teszt vagy mégsem?

Vakcinás csalások, szevasztok



10 kiberbiztonságra veszélyes szokás

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Egypálcás adathalász próbálkozások

2021. április 22. 19:02 - Csizmazia Darab István [Rambo]

A nemrég lezajlott SMS csalásból remélhetőleg senkinek nem az marad meg a fejében, hogy "FedEx-re nem kattintunk", hanem hogy mindig óvatosak, gyanakvóak és biztonságtudatosak maradunk és soha semmi olyanra nem kattintunk, ami bárhonnan is jön, bármire is hivatkozik, de furcsa, gyanús, hihetetlen, hiteltelen.

A címben használt "egypálcás jelző" a színvonaltalan, stílustalan, mélyen szánalmas, gyér, gyatra minőségű, az elvárható nívót alulról meg sem közelítő minőséget jellemzi a korabeli index Zsargon gyűjteményéből kölcsönözve. Néhány szemléletes kéretlen üzenet példáján mutatjuk, nem ördöngösség a csalások valós időben való leleplezése.

Első munkadarabunk **egy webmailes belépési linket tartalmazó angol nyelvű levél, eszerint a levelezési jelszavunk állítólag 24 órán belül lejár** (na persze), ám ha kattintunk a mellékelt ausztrál linkre, akkor természetesen változatlanul használhatjuk a fiókunkat továbbra is a korábbi, megszokott régi jelszavunkkal. Az üzenet szigorú határidőt is szab (a klasszikus recept szerint kell ugye a sürgetés-fenyegetés vagy valamilyen vonzó ingyen ajándék felkínálása), ez pedig esetünkben 72 óra, azaz három nap.

Vegyük észre, hogy **az igazi oldallal szemben itt egy szedett-vedett doménről jön az adathalász próbálkozás, ahol az URL címben van beparaméterezve az e-mailcímünk**. Ha begépeljünk jelszavunk helyett a "A jó moszkvai nagynénikédet!" szöveget, úgy a "Server Timeout!" üzenetet kapjuk, mintha nem sikerült volna a belépés, közben viszont már a csalóknál landolna a név-jelszó páros. **A levél többször is, különböző feladókkal is megérkezett**, és nyilvánvalóan nem egy sales@mingfa.cf vagy egy info@astoca.gq feladó fog értesíteni minket levelezésügyileg, mint "IT SERVICE DESK".

Következő történetünk egy "Sikeresen bejelentkezett, a készülék összes adata átmásolásra került. Olvassa el a benne lévő utasítások" tárgysorú levél formájában kopogtat. Érdemes idézni a teljes szöveget is, eszerint lásd a mellékelt képernyőképet. Az ilyen típusú fenyegetések nem számítanak újdonságnak, sőt elég uncsi is már. Tulajdonképpen egy igazi állatorvosi lóval van dolgunk, hiszen az összes árulkodó jellemzőt magán hordozza.

Gyatra helyesírás, amely arra utal, hogy a hol tegezős, hol magázós szöveg valamilyen nyers-fordítóval lett "hunglish" nyelvre átültetve. Jön a fenyegetés, az állítólagos titokban rögzített képeket és videókat (sok sikert a leragasztott kamerához) a váltságdíj nem fizetése esetén elküldi a szintén állítólag ellopott címjegyzékünkre. Nos addig álljon a feladó féllábon, amíg az 1100 dollárnyi (333 ezer HUF) kért Bitcoint várja a megadott tárcájába.

És végül következzen egy T-Mobile által küldött levélnek még véletlenül sem kinéző próbálkozás. Nyertünk - és kapunk 90 dollárt, amint kitöltjük az elégedettségi kérdőívet. Akkor nézzük a feladót, tegye fel nyugodtan a kezét, akinek így szoktak érkezni mobilszolgáltatótól a levelei: "Mobile Survey T-mobile <79Z5HBE0SF.690SN9079LHU1XXJJ7UF.RYATT@lghrib.com>" Hát nem éppen hivatalosnak tűnő forma, és ugyanez elmondható a mellékelt linkről is.

A bit.ly líbiai link-rövidítő szolgáltatás által elfedett hivatkozás már nem él, **valószínűleg elegendő számú panasz érkezett mostanra, hogy lelőjék a vélhetően adathalász oldalt**. Ugyancsak beszédes **a nyeremény kép alá valószínűleg véletlenül belekerült levezési töredékek is: az biztosra kijelenthető, hogy ilyet semmilyen hivatalos nyeremény játék végére nem illesztenek be.**

Egy szó mint száz, érdemes minden korosztálynak csiszolgatnia a felismerést, ugyanis **pici rutinnal könnyen ki lehet szúrni a gyenge minőségű átveréseket. Ezek azonnali törlése sok későbbi gondtól óvhat meg bennünket, és nem gyarapítjuk saját jogon a haveibeenpwned.com már amúgy is hatalmas 11 milliárdos adatbázisát.**

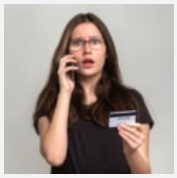
1 komment
Címkék: spam csalás átverés próbálkozás gyenge adathalászat adatlopás

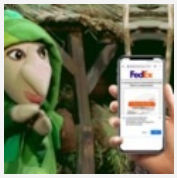
Ajánlott bejegyzések:


Azt mondod Covid19, azt mondom spam


A bankos mindig kétszer csenget...


Ingyenes Omikron teszt vagy mégsem?


Továbbra is célkeresztben a banki adataink


Sárkány ellen sárkányfű

Kommentek:

Head Honcho 2021.04.23. 04:30:09

Senki sincs biztonságban. :)

444.hu/2021/04/22/allami-es-onkormanyzati-szerveket-zsaroltak-hamis-maszturbalos-videokkal

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

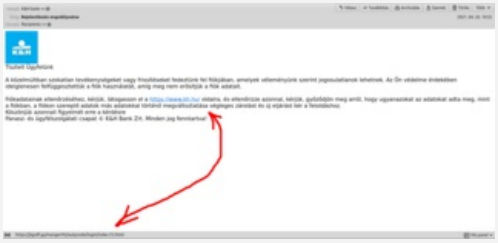
Továbbra is célkeresztben a banki adataink

2021. április 27. 19:40 - Csizmazia Darab István [Rambo]

Nem a Fedex nevével visszaélő SMS csalás az egyetlen, amely a felhasználók banki adatainak ellopására pályázik. Igaz, az ilyen visszaélések döntő többsége külföldön, zömmel angol nyelvterületen zajlik, de immár **egyre többször fordul elő nálunk Magyarországon is.**

A Flubotos eset óta is már volt példa magyar nyelven történő és a bankok nevével történő telefonos visszélésékre, például **az OTP nevében hívnak csalók hideghívással véletlenszerű számokat. A kamu telefonhívások során a csalók magukat banki ügyintézőnek, vagy banki csalások elleni nyomozónak adják ki, és adatellenőrzésre hivatkozva próbálnak személyes adatokat bediktáltatni** az áldozatokkal, jellemzően pontos születési adatokat, banki azonosítókat.

Érdekes módon az átverésben használt telefonszám számszerűen is hasonlóságot mutat az OTP Bank valódi ügyfélszolgálati elérhetőségével. Ezzel kapcsolatban a Nemzeti Kibervédelmi Intézet egy külön figyelmeztetést is kiadott.

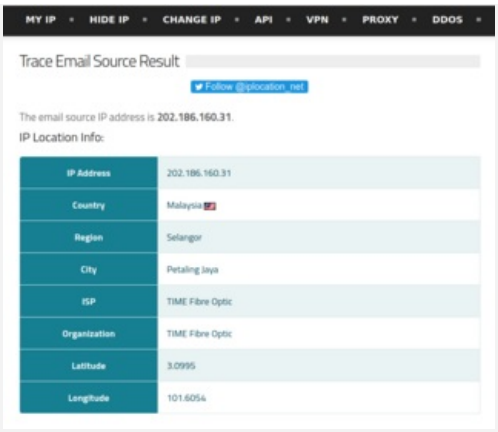


A mostani újabb esetben a K&H bank nevében érkezik a kéretlen e-mail üzenet. Ha e-mail trace segítségével megvizsgáljuk a fejlécet, akkor látható, hogy valójában egy malájziai IP címről lett elküldve. **Az üzenet természetesen egy linket is tartalmaz, melyre kattintva egy mobilbank belépési hasonmás adathalász oldalra jutunk, az ide begépelt azonosítók azonnal a bűnözők kezébe kerül.** Cikkünk írásakor ez a konkrét URL cím már nem élt, valószínűleg a bejelentések miatt lekapcsolták. A levél teljes szövege a következő:

"*Tisztelt Ügyfelünk*

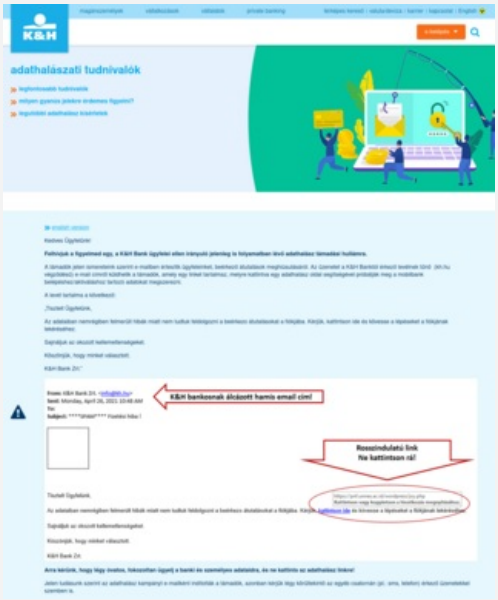
A közelmúltban szokatlan tevékenységeket vagy frissítéseket fedeztünk fel fiókjában, amelyek véleményünk szerint jogosulatlanok lehetnek. Az Ön védelme érdekében ideiglenesen felfüggesztettük a fiók használatát, amíg meg nem erősítjük a fiók adatait.

Fiókadatainak ellenőrzéséhez, kérjük, látogasson el a https://www.kh.hu/ oldalra, és ellenőrizze azonnal, kérjük, győződjön meg arról, hogy ugyanazokat az adatokat adta meg, mint a fiókban, a fiókon szereplő adatok más adatokkal történő megváltoztatása végleges zárolást és új eljárást kér a feloldáshoz.
Köszönjük azonnali figyelmét erre a kérdésre
Panasz- és ügyfélszolgálati csapat © K&H Bank Zrt. Minden jog fenntartva!"



Itt is vegyük észre a számtalan árulkodó jelet. **Például nem is nekünk írtak személyesen, hanem a címzett mezőben a Recipients szerepel, vagyis ez egy tömegesen kiküldött spam**. A megfogalmazás láthatóan hivataloskodó, ám szerfelett zavaros. Például nem tudják pontosan megmondani, hogy szokatlan tevékenységeket vagy frissítéseket fedeztek-e fel a fiókunkban, de azért közben Fülig Jimmy, Török Szultán és Tuskó Hopkins üzeni, hogy ***"Köszönjük azonnali figyelmét erre a kérdésre".***

A csalásokra oly jellemző sürgetés, fenyegetés sem marad ki az eszköztárból: *"Az Ön védelme érdekében ideiglenesen felfüggesztettük a fiók használatát, amíg meg nem erősítjük a fiók adatait. ... a fiókon szereplő adatok más adatokkal történő megváltoztatása végleges zárolást és új eljárást kér a feloldáshoz."*



De épp elég, ha **csak az egérkurzort mozgatjuk az állítólagos K&H bank fiókellenőrzési oldalának linkje fölé, hogy rögtön láthassuk, egy teljesen idegen domain neve szerepel itt** a hivatalos magyar banki URL helyett: "https://jigsdf.ga/mangerHU/autpcode/login/index%20(1).html".

Persze intő jel ide, árulkodó jel oda, **a legjobb mégis az lenne, ha már az adatok jogosulatlan telefonos bekérése, vagy egy bank nevében írt és mellékelt linket is tartalmazó, személyes belépési adatokat kérő üzenet már önmagában is megnyomná mindenki fejében a vészcsengőt: hogy hoppá, ez biztosan nem valós, na kedves csalók, ehhez korábban kellene felkelnetek. Sajnos biztonságtudatosságban egyelőre még nem igazán tartunk itt.**

Szólj hozzá!
Címkék: bank csalás átverés k&h adathalászat adatlopás nki

Ajánlott bejegyzések:


A bankos mindig kétszer csenget...


Ingyenes Omikron teszt vagy mégsem?


Fogják a pénzünket és futnak

Egypálcás adathalász próbálkozások


Azt mondod Covid19, azt mondom spam

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

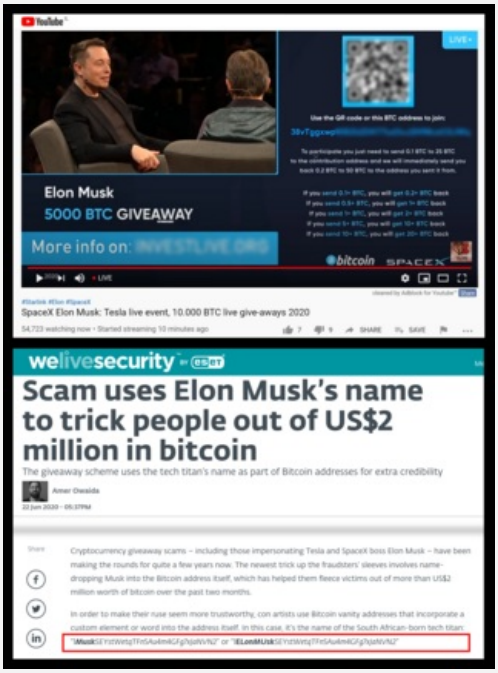
Celeb vagyok, fizess nekem!

2021. május 03. 11:33 - Csizmazia Darab István [Rambo]

Vagy mégsem és egyéb rovatunkban már sok olyan incidenssel találkozhattunk, ahol a csalók híres és gazdag emberek nevével visszaélve próbáltak pénzt kihúzni a gyanútlan áldozatokból. Most **négy olyan jellegzetes csalási sémát mutatunk, ahogy az átverés mögött bujkáló bűnözők az ismert, népszerű emberek álcája mögé bújnak.**

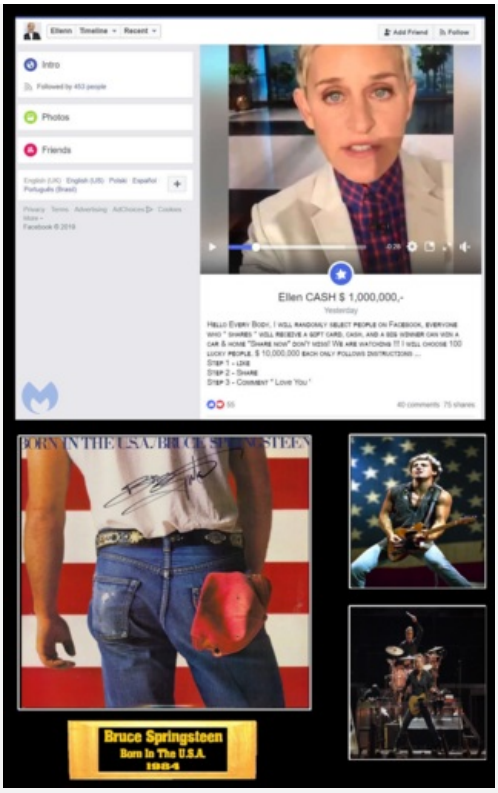
Az első említett módszer a kriptovaluta ajándékok ígérete. Az ilyen évek óta zajló típusú átverésnél vagy egy híresség nevében létrehozott kamuprofillal, vagy magának a híres embernek a feltört Twitter vagy YouTube profillal tevékenykednek. Az elkövetők magukat híres embereknek - pl. Elon Musk/Tesla, Vitalik Buterin/Ethereum, John McAfee, Warren Buffet, vagy valamilyen fejlesztői csoportnak - kiadva olyan bejegyzéseket tesznek közzé, amelyben a követőiknek Bitcoinok, és Ethereumok szétosztását ígérik.

Néha a hamis profilok neveiben olyan adathalász oldalakra jellemző pici betűhibákat is látni (typosquatting), mint például "WarrenBuffert", "BillGavtes", stb. Még arra is volt eset, hogy magába a Bitcoin tárca nevébe építették be Elon Musk nevét.



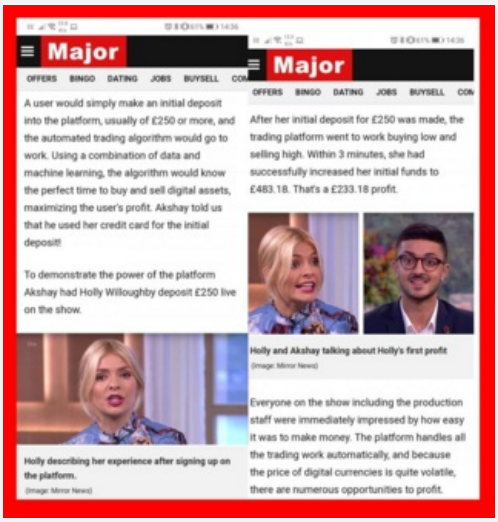
Ugyancsak gyakori mód, hogy a híresség nevében legtöbbször valamilyen kamuprofillal (betűhibás elütésű írásmóddal, vagy valójában csak rajongói oldal segítségével) közzétesznek valamilyen videót, ahol beígérnek olyasmit, hogy például az első 1000 hozzászóló 1000 dollárt fog kapni. A nyereményre vágyó balekok aztán kapnak egy üzenetet, amely további utasításokat tartalmaz az állítólagos nyeremény igényléséről, amely magában foglalhatja **egy adott kártékony webhelyre mutató linkre való kattintást és bizalmas személyes adataik kitöltését, illetve különféle költségekre hivatkozva előzetes pénzküldést a számlájukról.**

Kicsit a 419-es nigériai csalásra hasonlít a dolog, előbb vagy személyes adatot, vagy kisebb összegeket "kell" adni ahhoz, hogy mi majd megkaphassuk a hatalmas nemlétező nyereményt, csodás ;-)



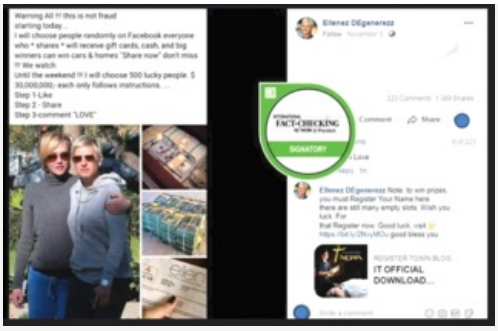
A hírességek időnként tényleg jótékonykodnak - gondoljunk csak Andre Agassira, a Bill és Melinda Gates alapítványra, vagy egyik kedvenc színészünkre, Keanu Reevesre. **Azonban a neten szerveződő adománygyűjtések vagy pénzkérések jelentős része valamilyen csalás köré szerveződött történet.** Ne hagyjuk, hogy ilyenkor pusztán a sajnálat, az érzelmeink vezéreljenek bennünket, gondolkodjunk józanul, és mindig kérdezzünk rá, pontosan mi is a neve, címe, és telefonszáma az alapítványnak, például kérjük írásos tájékoztatást a programjukról.

Mindig ellenőrizzük le az adott szervezet korábbi történetét, de az is jó ötlet, ha a hivatalos adománygyűjtők listáján is megkeressük őket. **Gyakran teljesen banális sztorikkal is sikert érnek el, például egy Bruce Springsteen profil mögé bújt csaló arra hivatkozva, hogy állítólagos válása kapcsán ideiglenesen zárolták a vagyonát, egy éven keresztül sikeresen csalt ki nagyobb pénzösszegeket a rajongóktól.**



És végül, de nem utolsó sorban a hamisan megszemélyesített celeb biztathat állítólagosan jól jövedelmező befektetésekre is. Ezek a csalások sem új keletűek, de az internet, a villámgyors hírközlés világában teljesen új közegben kell eldöntenünk: elhisszük-e, hogy valóban Elon Musk fektetett jelentős összegeket Bitcoinba (igen, így történt) vagy csak fakenews a dolog. **A módszer lényege, hogy gyanútlan embereket tudjanak becsapni a villámgyors meggazdagodás ígéretével különféle befektetési programokba.**

A hamis webhelyek sokszor már mentesek a gyanús helyesírási hibáktól, és meglepően hitelesnek tűnnek. **A celeb a hamis riportokban elmagyarázza, hogyan tudott akár percek alatt hihetetlen nyereséget elérni, és arra biztatja a követőit, hogy akár nem túl jelentős kezdőtőkével is vágjanak bele.**

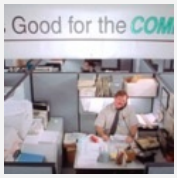


Mit tehetünk megelőzésképpen? Az a bizonyos biztonságtudatos hozzáállás, amely az éber, egészséges gyanakvásra épít, az mindenképpen nélkülözhetetlen. Soha ne válaszoljunk pénzküldési kérelemre, vagy küldjünk pénzt olyan személy számlájára, akit nem ismerünk és akiben nem bízunk meg. Sose fogadjunk el olyan ajánlatot, amelyben látatlanban előlegfizetést, vagy azonnali szerződéskötést igényel, hanem mindig konzultáljunk a családunkkal, szakemberrel, saját ügyvédünkkel.

Utasítsunk el minden a kéretlen kommunikáció útján érkező közvetlen ajánlatot, legyen az akármilyen kedvezően hangzó. Ellenőrizzük le, ha egy "híresség" felveszi velünk a kapcsolatot, igazi-e a profilja. A jótékonysági szervezeteket és befektetési lehetőségeket pedig egy gyors Google-kereséssel csekkolhatjuk le, hogy valódiak-e.

Szólj hozzá!
Címkék: celeb online csalás átverés híresség adathalászat óvatosság 419 nigériai gyanakvás biztonságtudatosság welivesecurity.com

Ajánlott bejegyzések:



Karácsonyi vásárlás biztonságosabban

Amazónia veszélyes ragadozói ;-)

Ingyenes Omikron teszt vagy mégsem?

Modern románc, holdfény és tánc

Vakcinás csalások, szevasztok

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Az elveszett jelszavak fosztogatói

2021. május 06. 13:39 - Csizmazia Darab István [Rambo]

Ma van a Jelszó Világnapja (World Password Day), amelyet 2013. óta minden esztendő május első csütörtökén tartanak világszerte. Célja, hogy **felhívja a figyelmet a tudatos jelszóhasználat fontosságára, ugyanis az évek során végzett kutatásokból kiderül, hogy a felhasználók még mindig nem fordítanak kellő figyelmet erre a témára.**

Életünk nagy részét az online térben töltjük, itt dolgozunk, bankolunk, posztolunk a közösségi média oldalainkra, vásárolunk, vagy éppen tanulunk. **Egy átlagos felhasználónak ma már több tucat online fiókja van, amelyekben rengeteg személyes és pénzügyi adatot tárol. A felhasználóknak túl sok, akár több száz jelszót kell megjegyezniük, ezért sajnos legtöbbször az eredetivel majdnem megegyező, vagy könnyen kitalálható karaktereket állítanak be.**

A hackerek pedig abból indulnak ki, hogy a felhasználók kényelmesek, így **sokszor mindenféle nehézség vagy trükk nélkül feltörik a gyenge jelszavakkal bíró felhasználói fiókokat.**

Az Egyesült Királyság Kiberbiztonsági Központjának (NCSC) friss felmérése szerint **a megkérdezettek 15%-a a házi kiskedvence nevét használja jelszóként, 13%-uk egy számukra fontos személyes dátumot, további 6%-uk pedig a kedvenc sportklubjának a nevét adja** meg belépési kódként.

A jelszavak tudatos használata érdekében érdemes a szakértők tippjeit megfogadni, melyekkel nem csak magunkat védhetjük meg, hanem az egyre növekvő online bűnözés ellen is tehetünk egy lépést. A világnap alkalmából az ESET kiberbiztonsági szakértői segítenek a biztonságos jelszóválasztásban.

Használjunk egyedi és erős jelszavakat!

Talán sokan egyetértünk abban, hogy egy erős és biztonságos jelszó létrehozása nem olyan bonyolult és mindenkinek meg kellene tennie, azonban több statisztika, felmérés és adatvédelmi incidens megmutatta már, hogy kevesen fogadják meg ezt a tanácsot. A NordPass minden évben nyilvánosságra hozza a leggyakrabban használt jelszavak listáját, melyből kiderült, hogy **2020-ban a felhasználók körében továbbra is a könnyen kitalálható számkombinációk, például az „123456”, „123456789” és az „12345678” voltak a legnépszerűbbek.**

Ezek az azonosítók nem nyújtanak megfelelő védelmet, ugyanis az első öt helyen szereplő jelszónak több mint 4,5 millió felhasználója van, és több mint 38 millió adatsértési eset kapcsolódik hozzájuk együttesen.

Bízzuk a munkát a jelszógenerátorra!
Új jelszavak létrehozásánál mindig törekedjünk arra, hogy nehezen kitalálható azonosítókat alkossunk. Kerüljük a szótárban szereplő szavakat, a könnyen kitalálható kifejezéseket, és az olyan személyes adatokat, mint például a családtagjaink neve.

Ebben segíthet nekünk az ESET ingyenes jelszógenerátora, amely az általunk választott karakterszám alapján elkészíti számunkra a megfelelő jelszót. Linuxos böngészőben pedig a BitWarden is egy kényelmesen használható kiegészítő.

Kerüljük a jelszavak újrafelhasználását!
A német Hasso-Plattner-Institute **1 milliárd felhasználói fiókkal végzett kutatása szerint a felhasználók 20%-a ugyanazt a jelszót használja több fiókjához is, míg a felmérésben résztvevők 27%-a közel azonos jelszavakat ad meg az általa kezelt profilokhoz**. Mivel évről évre több fiókot kezelünk, egyre nehezebb minden profilunkhoz erős jelszót kitalálni és megjegyezni. Jó megoldás erre egy jelszókezelő program, amellyel akár bonyolultabb jelszavakat is tárolhatunk.

Ez tulajdonképpen egy digitális széf, amelyben könnyedén elhelyezhetjük a különböző helyeken használt jelszavakat, csupán a mesterjelszót szükséges megjegyeznünk. Így nem kell azon aggódnunk, hogy fogunk-e emlékezni a jelszavainkra, és a ritkán használt fiókjaink esetében sem kell percekig törnünk a fejünket, hogy vajon milyen kódot adtunk meg korábban.

Éljünk a többfaktoros hitelesítés lehetőségével!
Egyre több felületen nyílik lehetőség a többfaktoros hitelesítés alkalmazására, amely egy extra biztonsági réteget jelent a felhasználók számára, mivel a jelszó megadása mellett egy extra azonosítást is kér a belépéshez.

Leggyakoribb módja az SMS-ben vagy e-mailben kapott kód megadása, ám ezeknél még biztonságosabb módszer a dedikált hitelesítő alkalmazás vagy hardveres megoldás, például hitelesítési tokenek használata.
Így az olyan esetekben, amikor nem mi kezdeményezzük a belépést, rögtön értesülhetünk arról, hogy illetéktelen személy próbál behatolni a fiókunkba és azonnal megtehetjük a megfelelő intézkedéseket.

Legalább negyedévente cseréljünk jelszót!
Tanácsos rendszeresen megújítani az összes fontos jelszavunkat, főleg abban az esetben, ha egy adott eszközt más felhasználókkal közösen használunk. **Akkor is érdemes megváltoztatni a kódjainkat, ha rosszindulatú szoftvert észlel a vírusirtónk.**

A haveibeenpwned.com weboldalon le tudjuk ellenőrizni kiszivárgott és nyilvánosságra került jelszavainkat. **Ebben az évek óta gyűjtött hatalmas adatbázisban immár több, mint 11 milliárd lopott név-jelszó páros található.** A jelszavak biztonságának visszatérő problémáját könnyebben megoldhatjuk, ha megfogadjuk ezeket a jótanácsokat. A jelszavainkat soha ne adjuk meg másoknak, ám a biztonsághoz vezető ezen lépéseket, tippeket bátran osszuk meg gyermekeinkkel, családtagjainkkal, barátainkkal is!

1 komment
Címkék: jelszó password világnap adatlopás adatszivárgás worst haveibeenpwned

Ajánlott bejegyzések:

Nem életrevalók

Jelszóválasztásban a helyzet változatlan

GoDaddy - apák a pácban

Stop adathalászat


100 millió helyett "csak" 40 lett, maradhat?

Kommentek:

Antolion 2021.05.09. 17:50:19

Miért kell nekem a Usernek más(ok) miatt kínlódnom? Itt nem a hackerekre hanem igenis a "szakemberekre" gondolok. Természetes, használok jelszavakat, melyek: legyenek bonyolultak, (megjegyezhetetlenek) gyakran változtassam őket, mindenhez külön. A posthoz megnéztem, 24 jelszót használok FB-tól a Vízművekig. Ki helyett kelljen még dolgoznom? A windows szinte minden frissítése hibákat generál, felelős nincs, kártérítés nincs...

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

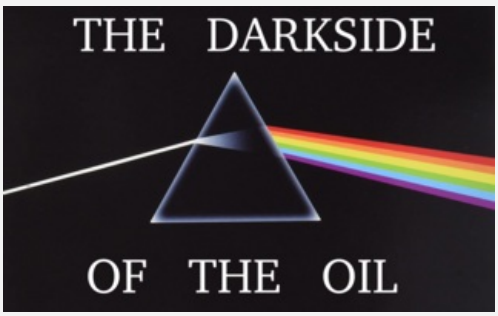
accountz

Belépés
Regisztráció

Fizess vagy einstandoljuk a kőolajvezetékedet!

2021. május 11. 10:42 - Csizmazia Darab István [Rambo]

Kibertámadással céloztak már kórházra, de okoztak hatalmas áramszünetet Ukrajnában, és emellett semmisítettek meg rendőrségi videófelvételeket, de kőolaj szállítására való csővezetéket eddig még nem igen bénítottak meg, legalábbis ennyire látványosan biztosan nem. **A zsarolóvírus doxinggal kombinált módszerével élve a DarkSide nevű banda most az USA Colonial Pipeline vezetékére mért brutális, címlapokra kerülő csapást.**

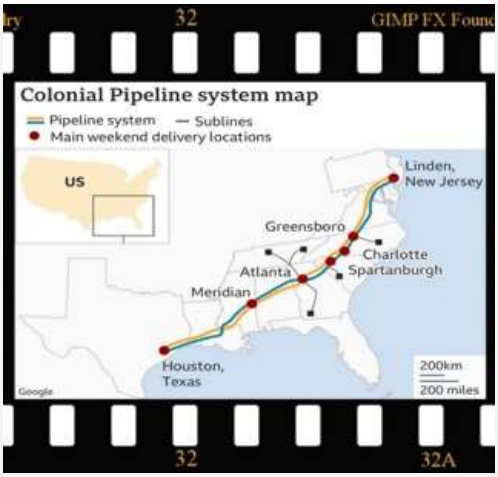


Nem öröm a ransomware sehol sem, ha például egy kórházban üt be a mennykő, akkor ott jönnek a leállások, **az egész foglalási rendszer borul, műtétek maradnak el, és a helyreállításig marad kökorszak: a papír és ceruza, a telefon meg a faxolás.**

Még nem látni pontosan, milyen hatása lesz ennek a mostani támadásnak, de mindenesetre nagyon látványos, és **félő, hogy meghozza a bűnözők kedvét az ehhez hasonló további akciókhoz.**

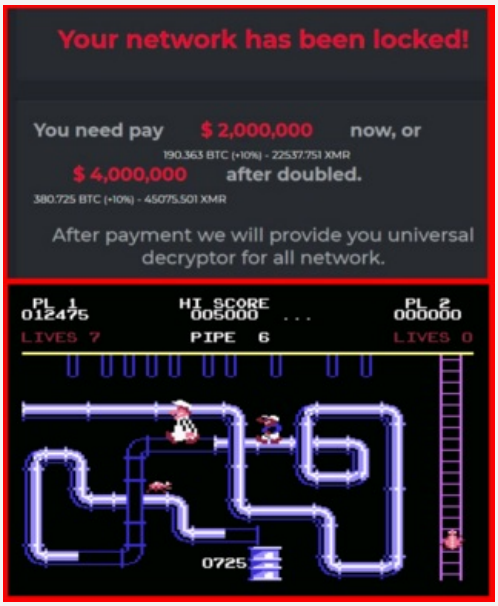
A napi 100 millió gallon (kb. 378 millió liter) kapacitású olajvezeték, amely a texasi Houston és New York között található, napok óta áll, ugyanis **kiberbűnözők megtámadták és megbénították a számítógépes rendszert és ezzel egyúttal leállt a keleti partot ellátó vezetéken történő üzemanyag szállítás is. Az üzemeltetők beszámolója szerint május 7-e, péntek óta tart az üzemzavar**, melynek elhárításánál kiberbiztonsági szakértők, valamint az FBI specialistái is dolgoznak.

Független elemzők szerint hatalmas olajmennyiség ragadt a texasi oldalon, ami miatt ideiglenes hiány is felléphet, bár egyelőre az üzemanyag árak még nem emelkedtek az incidens hatására.



Az eddig napvilágra került információk szerint a DarkSide nevű, gyanítható kelet-európai, talán oroszországi illetőségű banda lehet az elkövető, ezt nyilvánosan magukra is vállalták. Ez a csapat **viszonylag új, három év alatt összesen pár tucat ransomware akciót hajtottak végre, és fő motivációjuk az anyagi haszonszerzés.**

A doxing lényege, hogy nem csak az adatok elkódolásáért kérnek váltságdíjat, hanem azzal is fenyegetőznek ilyenkor, hogy nemfizetés esetén nyilvánosságra hozzák az ellopott érzékeny, bizalmas adatokat, ami jelen esetben igen jelentős mennyiség, nagyjából 100 GB-nyi lehet.



A londoni székhelyű kiberbiztonsági cég, **a Digital Shadows szerint támadást a koronavírus-járvány segíthette elő, mivel a pandémiás helyzetben több mérnök otthonról, távolról is hozzáfér a csővezeték vezérlő rendszereihez, és vélhetően az ő bejelentkezési adataik ellopásával kezdődhetett ez az incidens.** A Digital Shadows kutatása szerint ez a számítógépes bűnözői banda **valószínűleg orosz nyelvterületen található, mivel látványosan elkerülik a poszt-szovjet utód államokban lévő vállalatok megtámadását,** ideértve Oroszországot, Ukrajnát, Fehéroroszországot, Grúziát, Örményországot, Moldáviát, Azerbajdzsánt, Kazahsztánt, Kirgizisztánt, Tádzsikisztánt, Türkmenisztánt és Üzbegisztánt, a feltételezésre azonban egyelőre semmilyen bizonyíték nincs.

A DarkSide saját állítása szerint (aztán vagy elhisszük, vagy sem) nem támad meg a kórházakat, szociális intézményeket, oktatási illetve kormányzati célpontokat, és bevételének egy részét állítólag jótékonysági célokra fordítja, mint valami újkori Robin Hood.

A Colonial Pipeline azt ígérte, hogy ennek a hétnek a végére előreláthatóan nagyrészt már helyreállhat a normál üzem, és nem kényszerülnek tartósan közúti, vasúti szállítmányozásra. Az Egyesült Államok kritikus infrastruktúráján történt eddigi legsúlyosabb kibertámadásnak egyelőre nem látni a végét, **a cég nem közölte, hogy fizetett-e váltságdíjat, vagy hogy folytatnak-e tárgyalásokat, alkukat a bűnözőkkel, illetve a DarkSide sem nyilatkozott egyértelműen ez ügyben, ami azt valószínűsíti, hogy már fizettek, vagy még jelenleg is folyhatnak a háttérben a tárgyalások.**

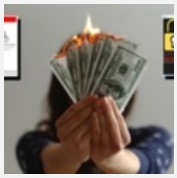
Brian Krebs biztonsági szakértő szerint **az állami intézményeknek, a kritikus infrastruktúrákat üzemeltető cégeknek jóval több támogatásra lenne szüksége** az ilyen incidensek elkerülése, illetve megelőzése érdekében, és ezzel az állítással nem igazán lehet vitatkozni.

3 komment
Címkék: usa olaj kőolaj texas állami váltságdíj intézmény darkside csővezeték ransomware pipeline colonial zsarolóvírus doxing

Ajánlott bejegyzések:

Offline mennyország - egy rövid időre

Van másik!


Fejemen olvad a vaj, engem nem érhet baj


Váltságdíjat kínálnak a váltságdíjszedő bandáért

Tesz-e Oroszország a ransomware ellen?

Kommentek:

horrorpornó bábszínház 2021.05.13. 11:30:31

Szerintem azért is büntetés járna, ha valaki annyira pocsékul ír, mint te.

Válasz erre

]{udarauszkasz 2021.05.13. 12:13:54

Ha mar annyira szuperintelligens Robin Hoodok, azert azzal tisztaban kene lenni, hogy az olajarak emelkedesehez ok is hozzajarultak ezzel.
Az egesz vilag osszefugg, tobbek kozott miattuk lesz rekorddraga a benzin.

Válasz erre

A Joda visszatér 2021.05.13. 16:49:59

@horrorpornó bábszínház:

-Gergő, megcsináltad az angol házit?

-Si, tanár úr..

:D

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

A mint adathalászat

2021. május 13. 17:27 - Csizmazia Darab István [Rambo]

A sokakat homeoffice alá terelő több, mint egy éve zajló pandémia erőteljesen átalakította a munkavégzést. **Ennek nyilván előnyös és hátrányos oldalai is voltak-vannak, és persze a megnövekedett kockázatok, az intenzívebb támadások is velejárói a helyzetnek**. Elég csak a Solarwinds123 jelszóválasztásra, vagy a Colonial Pipeline mérnökök ellopott jelszavaira gondolni.

Egy a közelmúltban végzett kormányzati felmérés szerint volna még mit javítani a brit munkavállalók adatvédelemmel, adathalászattal kapcsolatos biztonságtudatosságán. **A 2021-es kutatás adatai azt mutatják, a vállalkozások 80%-a nem teszteli a dolgozók ez irányú tudását, 57%-uk nem rendelkezik kiberbiztosítással, és ami talán a Covid időszak legnagyobb hiányossága, hogy mindössze a cégek negyede rendelkezik az otthoni munkavégzéssel kapcsolatos biztonsági előírásokkal, beleértve ebbe a személyes eszközök otthoni használatának szabályozását is.**

Pedig a sokadik hullám után várhatóan minden vállalatnál ki fog alakulni valamilyen hosszútávú hibrid megoldás, amely az irodai és a homeoffice választható vagy elvárt arányát fogja meghatározni.

A fenti felmérést végző Keller Lenkner adatvédelmi cég **olyan vállalatokat és vállalkozásokat képvisel, mint például a Ticketmaster, az Equifax, az Equiniti, a TeamSport, a British Airways, a Dixons Carphone, vagy a Police Federation of England and Wales.**

De ha már brit példát hoztunk, akkor folytassuk is ott, miszerint **egy brit szakszervezet bocsánatkérést követel a West Midlands Trains vasúttársaságtól amiatt, hogy a céges biztonságtudatossági teszt lebonyolításakor olyan adathalász teszt levelet küldtek körbe a dolgozóknak, amelyben a Covid-19 járványon átesett munkatársaknak bónusz jutalmat ígértek.**

A levelet **látszólag a West Midlands Trains (WMT) pénzügyi és bérszámfejtési osztályáról küldték, és ebben azt írták 2500 munkatársnak, hogy egyszeri kifizetést ajánlanak fel számukra, hogy ezzel köszönetet**

mondhassanak az elmúlt mintegy 12 hónapban végzett kemény munkájukért. A levél végén arra kérték őket, hogy kattintsanak a mellékelt Microsoft Office 365 linkre, amely állítólag a WMT ügyvezető igazgatójának, Julian Edwardsnak a személyes üzenetéhez vezet.

Természetesen hullottak a kattintások, és az így becsapott dolgozók egy olyan emailt kaptak, amelyben arra hívták fel a figyelmüket, hogy **ez egy IT-biztonság tesztelésére szolgáló levél volt, és a jövőben legyenek óvatosabbak, valamint alaposabban gondolják át, hova gépelik be a céges bejelentkezési adataikat.**

A szakszervezet azonban durva és elítélendő viselkedésként elítélte a tesztet, és bocsánat kérésre szólította fel vasúttársaságot. **A szimulált adathalász támadások célja azonban minden cégnél az informatikai biztonság tudatosítására szolgál az alkalmazottak körében, és máshol is hasonló módszerekkel ellenőrzik az éberséget.**

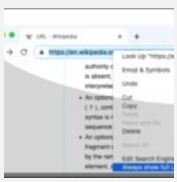
Emlékezetes, hogy tavaly decemberben a GoDaddy domainnév kezelő cégnél olyan e-mailt küldtek körbe, amelyben 650 dolláros üdülési bónuszt ígértek az alkalmazottaknak. Ezt bár vehetik rossz néven, de minden ilyen teszt célja, hogy felhívja a figyelmet a vállalatokat sújtó egyre gyakoribb adatsértésekre, incidensekre és felkészítse a dolgozókat gyanakvóbb, biztonságtudatosabb hozzáállásra

Szólj hozzá!
Címkék: teszt brit felmérés adathalászat vasúttársaság wmt biztonságtudatosság

Ajánlott bejegyzések:


Ingyenes Omikron teszt vagy mégsem?

Celeb vagyok, fizess nekem!


Adathalászat kontra halőr


A support csalók nem pihennek

Banki adatok online elszipkázása

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Siker, pénz, csillogás: Visszatérítés az adószámlán

2021. május 17. 11:45 - Csizmazia Darab István [Rambo]

Mai posztunkban örömhírrel foglalkozunk: **a NAV rendszere arról értesített bennünket, hogy adó-visszatérítésre vagyunk jogosultak, így váratlan helyről, váratlan jogcímen áll pénz a házhoz, vagy mégsem?**

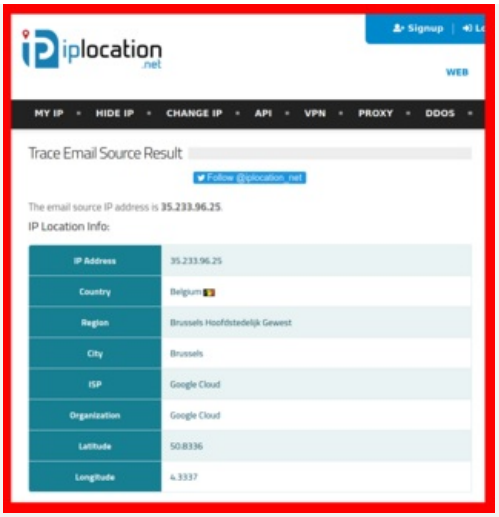
Először is egy fontos alaptétel: sosem lesz vége a vagy mégsem rovatnak, hiszen a csalók részéről sincs vége az átverési kísérleteknek. Ezt akkor gyorsan le is tudtuk, **nézzük a mai "munkadarabot", melyben a NAV arról tájékoztat minket, hogy "Visszatérítést kap, amelyet a nav.gov biztosítás nem teljesített. Műveletkezelő rendszerünk észleli, hogy jogosult-e erre a kifizetésre."**

Bár látszólag magyar nyelven van, de azért a nyelvtani fogalmazáson érzünk némi nemű Fülig Jimmy és Tuskó Hopkins jellegű utóízt. A kéretlen levélnek az sem szolgál előnyére, hogy **bár azt egy hazai állami hivataltól kaptuk, a feladója mégis egy németországi sazihazi KUKAC t-online PONT de. Pedig jöhetett volna a hivatalos Ügyfélkapun is.**

Ha valaki nagyon akkurátus, és a fejlécet bedobja egy online e-mail trace dobozba, akkor pedig az is előbukkan, hogy a levél küldése éppenséggel egy brüsszeli, azaz Belgiumban található IP címről történt. Nézzük akkor a lehetséges jó oldalait a levélnek, még ha hihetetlenek is ezek. **Először is hivatalosnak látszó referencia számot kaptunk, miénk az A8005W ügyirat, vagyis nincs itt semmi légből kapottság.** A hivatkozott nav.gov pedig tényleg a nav.gov.hu oldalra mutat, igaz csak az alsó linknél.

Aztán lássuk a nekünk járó pénzt, az is csábító: 63688.73700HUF. **Látszik, hogy kihegyezett mérnöki precíz pontossággal kalkulálták ki ezt nekünk, nyoma sincs benne a gépjármű súlyadónál tapasztalt lekezelő és ormótlan ezresre kerekítésnek, mert mi ezt a mostani szép pontos összeget megérdemeljük. Nem? De ;-)**

A gyors online pénzhez jutáshoz nincs is másra szükség, mint a NAV oldalon begépelni a személyes és banki adatainkat. Ja hogy nincs biztonságos HTTPS kapcsolat? És hogy ez valójában nem is a NAV oldala, hanem csak annak látszik, miközben ez a "zebdal7wa PONT com" URL című webhely? Ilyen apróságokon nehogy már fennakadjunk, hiszen mi pénzt akarunk, itt és most, de ízibe.

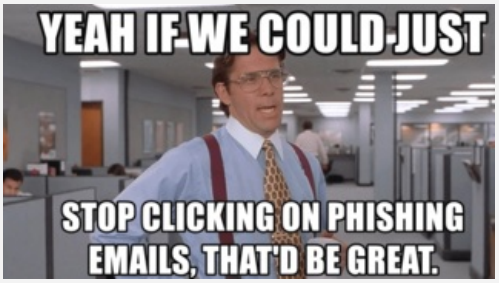


Az űrlap töltögetés a teljes név, adóazonosító jel, e-mail cím (ezt miért is, hiszen megkaptuk az elektronikus levelet?), telefonszám, valamint a pontos lakcímünk irányítószámmal ékesített formájában való begépelgetést kéri, ami már csak azért is furcsa, hiszen egy adóhivatal szinte többet tudhat rólunk, mint mi saját magunkról.

Na de a pénz az pénz, na meg "time is money", és **máris a bankkártya adataink megadása című fejezethez érkezünk, és akkor foglaljuk össze, mit tudunk eddig. Brüsszeli IP címről egy német nímand ír nekünk egy kéretlen e-mailt, amelyben a NAV nevében ingyen pénzt ígér, csak előtte be kell gépelnünk részletes személyes adatainkat, valamint bankkártya információinkat. Vajon vissza is lehet ezzel élni?**

Nem sikerül elképzelni azt a figyelmetlen, fogalmatlan (clueless) embert, aki ennyi brutális intő, evidens figyelmeztető jel ellenére is beleesik ebbe az átlátszó csapdába, és reméljük, hogy ezek száma tényleg konvergál a nullához. A sikeres boldog élet záloga egyes buddhista tanok, no meg a mindfulness prófétái szerint is a pillanat teljes megélése, a szemlélődő jelenlét, a droidszerű rutin tevékenységek helyetti aktív itt és most figyelem.

Akkor tehát összpontosítsunk ezzel az emelkedett szemlélettel a banki adatok kitöltésre. Vajon miért is kellene a bankkártyánk háromjegyű CVV biztonsági kódját megadnunk, hiszen itt mi kapunk pénzt? Nem lenne elég ehhez a számlaszámunk vagy a kártyaszámunk? Ha valóban nekünk akarna valaki utalni, akkor a válasz igen, de.



Az oldal a banki adatok begépelése után rendre timeout hibaüzenetet jelenít meg, ekkor dörzsölik az adathalászok tenyerüket, és valós adatok begépelése esetén hamarosan csörög is nekik a kassza, miközben az áldozat számlája hamar kiürülhet. **Vagyis a pénzhez jutás ígérete igaz ugyan, csak éppen nem mi kapunk a NAV-tól, hanem a bűnözök csapolják le azt a hiszékeny emberektől. Nem osztogatnak, hanem fosztogatnak.**

Az adathalász oldalt lejelentettük a hatóságoknak, ez a konkrét oldal a mai, hétfő napon már nem volt elérhető. Ám a módszer nagyon is életképes, és bármikor, bármilyen hasonló formában szembejöhet velünk, **így az óvatosság, a biztonságtudatosság nélkülözhetetlen.**

2 komment
Címkék: adatok phising adathalászat banki adóhivatal adóvisszatérítés nav

Ajánlott bejegyzések:


Fizessük számlánkat egyszerűen, egy kattintással


NAV adó-visszatérítés 2. felvonás

Banki adatok online elszipkázása


NAV adó-visszatérítés vagy mégsem?


A bankos mindig kétszer csenget...

Kommentek:

Head Honcho 2021.05.18. 11:03:41

Mivel félelmetes a sötétség a fejekben, szinte biztos, hogy lesz, akinél sikerrel járnak majd.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker

2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

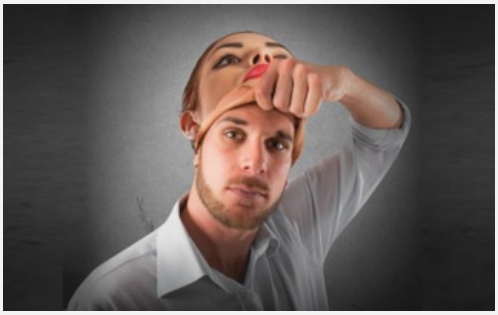
Az online térben hagyott személyes adataink

2021. május 20. 08:29 - Csizmazia Darab István [Rambo]

Valószínűleg mindenki számára ismerősen cseng a "digitális lábnyom" kifejezés, de vajon ismerjük a pontos jelentését? A digitális lábnyomunkat alkotják többek között a közösségi médián megosztott tartalmaink, a különféle online fizetési tranzakcióink, helyelőzményeink, e-mailjeink, az azonnali üzenetküldő platformokon keresztül küldött üzeneteink és az útlevélhasználatunk is.

Attól függően, hogy **mennyire figyelünk oda adataink biztonságára az interneten, és mennyi információt osztunk meg magunkról a közösségi média oldalakon, ezeket az adatokat összegyűjthetik és felhasználhatják arra, hogy egy átfogó személyleírást készítsenek rólunk. Kiberbűnözők kezébe kerülve az adataink különféle rosszindulatú célokra is felhasználhatók, vagy akár el is adhatják őket a dark weben. Információinkkal könnyedén visszaélhet egy online zaklató vagy csaló is, például tudtunk nélkül megszemélyesítve minket.**

Jó hír, hogy pár egyszerű lépéssel minimalizálhatjuk ezeket a kockázatokat, és csökkenthetjük digitális lábnyomunkat. Ettől még nem kell mindentől elzárkózva remetévé válnunk, elegendő, ha hozunk pár okos döntést, és egyensúlyt teremtünk adataink védelme és kényelmünk között.



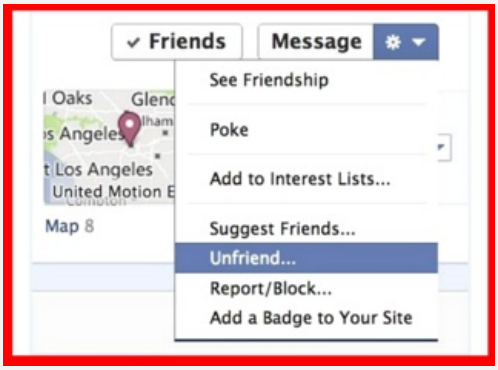
Első lépésként ellenőrizzük közösségi média profiljainkat és az adatvédelmi beállításokat. Nézzük meg, hogy ki tekintheti meg profiljainkat és milyen információkat láthat belőlük. Ehhez át kell bogarásznunk a különféle adatvédelmi beállítások listáit (amelyek ráadásul minden közösségi oldalon más helyen találhatók) de mindenképp megéri a fáradtságot. Ellenőrizzük az összes múltbéli és frissebb bejegyzésünket is - valószínűleg senkinek sem kell tudnia, hogy 12 évvel ezelőtt hol vacsoráztunk a barátainkkal.

Ez a feladat hosszadalmas lehet, főleg ha sok évnyi posztot kell utólag átnéznünk, de a dolog jó oldala, hogyha egyszer végigcsináljuk, biztosan elgondolkodunk azon, hogy a jövőben mit osztunk meg világgal. Ez a tisztogatás ráadásul azt is megakadályozhatja, hogy a nem kívánatos régi bejegyzéseink kísértsenek minket a jövőben, például egy állásinterjú során.

Ne hagyjuk ki a szelektálásból ismerőseink listáját sem, hiszen nem mindegy, kinek adunk betekintést a magánéletünkbe. Kezdjük azoknak az idegeneknek az eltávolításával, akikre már nem is emlékszünk, majd folytassuk

azokkal az ismerősökkel, akiket nem ismerünk túl jól és azokkal, akikkel sose szoktunk beszélni. Felmerülhet bennünk a kérdés, hogy "de mit árthat az, ha idegenek is látják a bejegyzéseimet?" - nos, ilyenkor érdemes átgondolni, hogy a posztjaink milyen sokat elárulhatnak rólunk.

Ezt bizonyítja az az eset is, amelyben bűnözők különböző híresség Instagram-fiókjait figyelték meg azzal a céllal, hogy megismerjék a szokásaikat, programjaikat, és ezen információk alapján kirabolhassák otthonaikat.

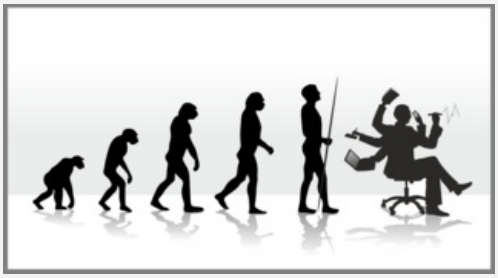


Ellenőrizzük az összes felhasználói fiókunkat - és tisztítsuk meg őket. Valószínűleg valamennyien regisztráltunk már olyan webshopokra, amelyeket csak egyszer vagy kétszer használtunk, vagy valamilyen fitnesz applikációra, főző alkalmazásra, esetleg játékra és így tovább. Nagy valószínűséggel ezek mindegyike különféle információkat tárol rólunk, a nevünktől kezdve a születési dátumon át egészen a telefonszámunkig.

A legtöbben a kényelem érdekében általában egyszeri bejelentkezéssel történő azonosítás (SSO, Single Sign On) segítségével - például a Facebook vagy Google fiókunkkal -, vagy az e-mail címünkkel regisztrálunk. Valószínűleg senki sem vezet fejben vagy fizikálisan egy listát az összes szolgáltatásról, webshopról vagy alkalmazásról, amelyre az évek során feliratkozott - ilyenkor segíthet az SSO opció a visszaemlékezésben.

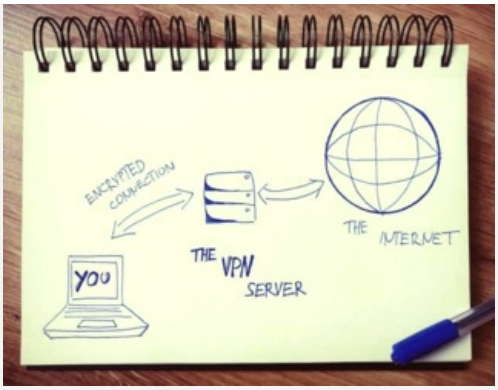
Akár a Google, a Facebook vagy az Apple fiókunkat használtuk ezeknél a bejelentkezéseknél, mindegyikük lehetőséget nyújt arra, hogy megnézzük azoknak a harmadik féltől származó alkalmazásoknak a listáját, melyeknek valaha hozzáférést adtunk a fiókunkhoz. Erről a listáról törölhetjük azokat a fiókokat, amelyeket már nem használunk.

Ha a regisztrációk során az e-mail címünket használtuk, akkor e-mail fiókunkban kereshetünk rá az összes általunk használt szolgáltatásra. Ehhez elegendő, **ha a beérkező levelek (vagy a már elkülönített HÍRLEVELEK) mappájában rákeresünk az olyan kifejezésekre, mint a "leiratkozás", a "bejelentkezés", vagy az "üdvözlünk".**



Tegyük rendbe hírlevél feliratkozásainkat is! Legtöbben egy regisztráció során nem olvassuk el az apró betűs részeket, csak automatikusan rákattintunk arra a gombra, amely a leggyorsabban végigvezet minket a regisztrációs folyamaton. Emiatt végül e-mailek százai érkeznek postaládánk Promóciók mappájába, amelyeket valószínűleg sosem fogunk elolvasni. Érdemes ezekről leiratkozunk, és **egy külön e-mail címet létrehoznunk, amit csak az egyszeri vásárlásokhoz használunk.**

Ez két előnnyel is jár: így a fő e-mail fiókunk megmarad a fontos dolgoknak, másrészt egyszerűbben áttekinthetjük az összes egyszeri online vásárlásunkat, míg az adataink biztonságban maradnak. Ha pedig egy olyan dologra szeretnénk feliratkozni, amelyet csak egyszer tervezünk használni, akkor alternatív megoldásként használhatunk másodlagos e-mailcímet, vagy pedig ideiglenes e-mail szolgáltatásokat is a valódi fő levelezési címünk helyett. Az "eldobható e-mail cím" vagy "ideiglenes e-mail cím" kifejezésre keresve több ilyen szolgáltatót is találhatunk.



További bónusz tipp lehet az extra biztonság érdekében, ha VPN-t használunk, azaz virtuális magánhálózatot. A VPN-ek titkosított alagutakként működnek internetes forgalmunk számára. Segítségükkel böngészési szokásaink rejtve maradnak a kíváncsiskodó szemek előtt, és megakadályozzák azt, hogy nyomon követhetőek legyünk. Az ESET szakértői arra is felhívják a figyelmet, hogy **az Európai Unió lakosaként jogunkban áll élni az "elfelejtés" lehetőségével**. Például mindössze egy kérelem kitöltésével utasíthatjuk a Google-t bizonyos személyes adataink eltávolítására, de használhatjuk a Google Adatvédelmi Áttekintőjét és egyéb eszközeit is arra, hogy ellenőrizzük, milyen adatainkat követik nyomon, és ezeket akár el is távolíthatjuk.

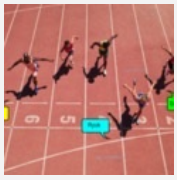
Ha pedig ezen már túl vagyunk, miért ne végeznénk el a Facebook adatvédelmi ellenőrzését is? **A Facebookról és más közösségi média-hálózatokról, például a Twitterről le is tölthetjük az általuk tárolt összes információnk másolatát, ha szeretnénk**. Összefoglalva tehát, még akkor is, ha a digitális lábnyomunk minimalizálása eleinte nehézkesnek tűnik, megéri az erőfeszítést. Később hálásak leszünk az így megszerzett privát szféráért.

Szólj hozzá!
Címkék: adatvédelem digitális privátszféra beállítások megelőzés lábnyom védekezés rendrakás ESET

Ajánlott bejegyzések:


Mindent IS visz...


Fiatal vagy? Ezekre az online csalásokra figyelj!


Világrekord, aminek mégsem örül senki

Az egyik COVID-19, a másik egy híján 20


7 tipp a mobilunk védelméhez

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Kormányzatok célkeresztben

2021. május 25. 09:55 - Csizmazia Darab István [Rambo]

Az ESET átfogó riportot készített **a kormányzatokat világszerte érintő kiberbiztonsági kihívásokról, melyben a Luckymouse APT-csoport legújabb támadási kampányát is megvizsgálja.** A kutatás összhangban áll az Európai Bizottság, a CERN és az Europol védelmi stratégiai perspektívájával, amelyet az European Cybersecurity Day online konferencián mutattak be.

A kiberbűnözők különösen nagy hatékonysággal célozzák azokat a kritikus fontosságú infrastruktúrákat, melyek védelme a kormányzatok felelőssége. **Az Európai Unió és világszerte a kormányok kiberbiztonsági stratégiáját nemcsak a digitális működésre való áttérés teszi próbára, hanem a kiberkémkedés, a zsarolóvírusok és ellátási lánc elleni támadások is.**

A legkomolyabb kihívást a kormányok számára azonban az Advanced Persistent Threat (APT), vagyis a fejlett és tartós fenyegetést jelentő, feltűnés nélkül munkálkodó szervezett csoportok támadásai jelentik.

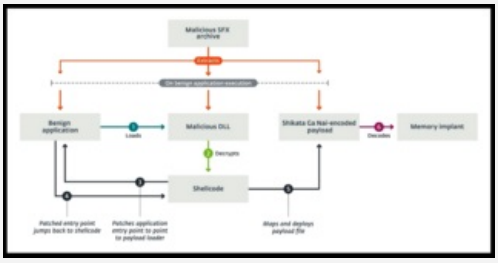
Az év elején egy jól ismert, LuckyMouse névre keresztelt APT-csoport (más néven Emissary Panda, APT27) új támadási kampányba kezdett, mellyel a Microsoft Exchange Server számos zero-day (azaz nulladik napi) sebezhetőségét használta ki. Az ESET által **„EmissarySoldier" (titkos küldetésű katona) névre keresztelt kampány célja, hogy a Közel-Kelet több kormányzati hálózatán és Közép-Ázsia szervezeteinek hálózatain kémkedjen.** A csoport a rosszindulatú SysUpdate eszköztárát használja fel a gépek kompromittálására, melynek első mintáit 2018-ban fedezték fel, ám azóta különböző fejlesztési szakaszokon ment keresztül, és fokozatosan integráltak különféle funkciókat az eszközkészletbe.

Az APT csoportok - például a LuckyMouse - által használt eszközök fejlődése komoly probléma. A támadások során a kormányzás olyan feladatai kerülnek veszélybe, mint az állampolgárok, az üzleti környezet és a más nemzetállamokkal ápolt kapcsolat stabilitásának biztosítása. **A LuckyMouse és más APT csoportok - köztük állami szereplők és partnereik - olyan széles körben elterjedt együttműködési platformokat céloznak meg, mint a Microsoft SharePoint vagy más digitális szolgáltatások.**

Ám a LuckyMouse tevékenysége csupán a jéghegy csúcsa. A kormányzatokat célzó fenyegetések nagy része szervezett bűnözői csoportoktól ered, akik egyre inkább hajlandóak együttműködni a közös céljaik elérése érdekében. A digitális

szolgáltatások használatának növekedésével az ellátási lánc fenyegetettsége is nőtt.

Az ESET 2020. utolsó negyedévében olyan sok ellátási lánc elleni támadási kampányt fedezett fel, mint amennyit pár évvel ezelőtt a teljes biztonsági szektor egy teljes év alatt észlelt. Az ilyen típusú támadások során az ellátási lánc kevésbé biztonságos elemeinek célzott támadásával próbálják megkárosítani a kiszemelt iparági szervezetet.



A 2020-as és 2021-es években számos kutatási együttműködés érett be, ideértve az Európai Nukleáris Kutatási Szervezettel (CERN), a Europollal és a Francia Nemzeti Kiberbiztonsági Ügynökséggel (ANSSI) történő közös munkát is. Az ESET European Cybersecurity Day virtuális eseményen és **a jelentésben megosztott meglátások közül több is azt hangsúlyozza, hogy a kormányok és az IT-infrastruktúrájuk elsődleges célpontoknak számítanak.**

A riport kiemeli annak szükségességét, hogy a kiberbiztonsági cégek, szakértők továbbra is támogassák a kormányokat a biztonsági hiányosságaik megszüntetésében és az APT csoportok taktikái, technikái és működésük nyomon követésében a rendelkezésükre álló különböző végponti észlelésre és reagálásra képes megoldások által.

Az elmúlt év eseményei komoly változásokat hoztak, és **már nincs választási lehetőség a kormányzati IT-csapatok számára, muszáj a védelemre fokozottan figyelni.** A legjobb biztonsági technológiákra, termékekre és élvonalbeli kutatásokra van szükséges ahhoz, hogy a kormányzatok képesek legyenek lépést tartani az egyre nagyobb kihívásokkal.

A LuckyMouse APT-csoport tevékenységét is részletesen bemutató „ESET industry report on government: Targeted but not alone„ című riport a WeLiveSecurity.com oldalról tölthető le.

Szólj hozzá!
Címkék: kormányzat infrastruktúra kritikus apt támadás kibertámadás ESET welivesecurity.com

Ajánlott bejegyzések:


Kiberkockázatok - miért nehéz velük lépést tartani?


Heten, mint a gonoszok


Török, zúzok, felülírok, nyávogok


Unortodox támadások jönnek

Kr00K sebezhetőségre figyelmeztet az ESET

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei

Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Ez történik a weben egy perc alatt

2021. június 01. 13:27 - Csizmazia Darab István [Rambo]

Jó régen jelentkeztünk már ezzel a rovatunkkal, így most érdekes lesz megfigyelni, mi és hogyan változott a bő másfél év távlatában. **A növekedés - legyen szó akár a röpke 60 másodperc alatt küldözgetett fájlokról, az egy perc alatt lezajló kattintásokról, vagy a kártékony kódok megemelkedett számáról - persze látatlanban bátran borítékolható.**

Kellemes kis összefoglaló ez az egyperces műfaj, legyen szó **akár a DOMO Data Never Sleeps kimutatásáról, vagy akár a Lori Lewis féle Internet Minute összefoglaló ábráról**. Ha a DOMO-s infografikákat nézzük, akkor már a 2010-es 1.0-hoz képest a 2013-as 2.0-ás is "kis lépés egy embernek, de nagy lépés az emberiségnek" érzés foghat el minket a számok emelkedése láttán.

De hasonló léptékű növekedés volt látható a 2017-es 5.0-ás akkori állapot a korábbi, 2016-os 4.0-ás pillanatkép között is.

Rátérve a friss kimutatásokra, nézzük akkor, hogy a mai ismereteink szerint a világszerte 4.66 milliárd internetező mit hozott össze ezekben.

A legfrissebb 8.0 és a 2018-as 7.0 is mutat jellegzetes átalakulásokat. Itt **nem csak a számszerű emelkedés, hanem az új kategóriák felbukkanása, korábbiak csökkenése, eltűnése, vagy ellenkezőleg, erőteljes előretörésére láthatunk példákat.**

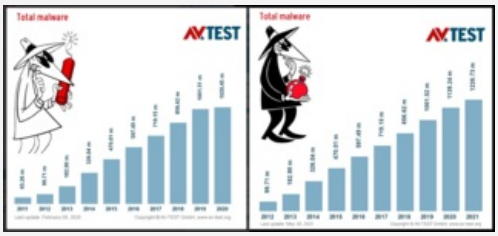
500 óra videót töltenek fel ez alatt az egy perc alatt, 41 millió Whatsapp üzenet keletkezik, és az Instagramon 347 ezer sztori landol. **Új kategóriák is megjelentek a pandémia miatt, például 208 ezer Zoom meeting, vagy az 52 ezer Microsoft Teams kapcsolódás is erről árulkodik, de az internetes vásárlás is csúcsrajárt az utóbbi időben.**

Például a vizsgált átlagos egy percünk elég volt ahhoz, hogy az Amazon 6659 csomagot kézbesítsen, a vásárlók 1 millió dollárt költsenek online, vagy Doordash rendszerében 555 ételrendelés történjen. A kimutatások a korábbi verzió infografikájához képest itt nem minden esetben összehasonlíthatóak, más

mértékegységben, más szolgáltatók egységeit mutatja, de azért a változások nagyjából így is érzékelhetőek.

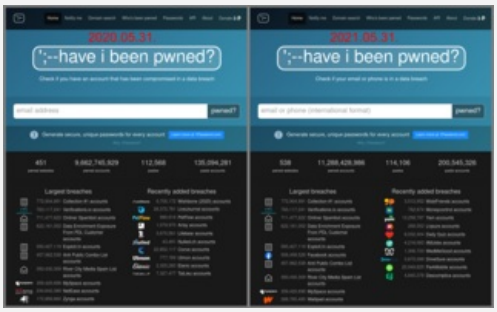
Ha másodikként az Internet Minute ábráit nézzük, akkor itt már elég egységes, szabatos kategóriák szerepelnek, amiknél könnyebb az időmúlással párhuzamokat vonni. A tavalyi, 2020-as adatokhoz képest például 19 millió szöveges üzenet helyett már 21 milliós számot látunk az idei értékeknél.

Látványos emelkedés van TikTok fronton, ott az 1400 letöltött tartalom helyett már 5000 történik. Ugyanilyen emelkedés volt a Messenger/Whatsapp üzenetek számaiban, 59-ről 69 milliósra hízott a mennyiség, de a társkereső Tinderben az oldalra húzások is megsokasodtak, a korábbi egy perces adat 1.6 millióról 2 millióra duzzadt.



És végül nézzük meg a feketeleves részét is a megnövekedett forgalomnak. **Az AVTest weboldal összesítője szerint az egyedi kártékony kódok mennyisége a tavalyi 1 milliárdról 1.22 milliárdra nőtt.**

De természetesen ahogy a fenti adatokban, úgy ezen a téren sem várt senki csökkenő számokat, sajnos ez a realitás.

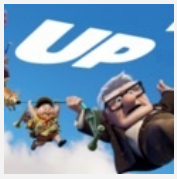


Zárásképpen pedig rápillantunk a Wayback Machines segítségével a haveibeenpwned oldalára, mit mutatott egy esztendeje és mit láthatunk rajta most. Az ellopott, kiszivárgott jelszavak száma a korábbi 9.6 milliárdról 11.2-re változott, tehát erős, egyedi, rendszeresen változtatott jelszó ügyeben is van még mit fejlődnünk, a két-, illetve többfaktoros autentikáció elterjedtebb használatáról nem is beszélve.

Összességében számok nőttek, pandémia nélkül is toltuk a netet, de a kényszerű karantén alatt még inkább. Ahogy John Rambo fogalmazott a First Blood részben: sok katonából sok halott lesz, úgy a világszerte egyre növekvő internethasználó, egyre több netre kapcsolt kütyü miatt nő a forgalmazás, de jó lenne, ha mindeközben a vírusfertőzések, az ellopott jelszavak és veszélybe került személyes adatok mennyisége ehhez képest viszont végre csökkenhetne. Ha majd egyszer így lesz, természetesen arról is nagyon szívesen adunk hírt.

Szólj hozzá!
Címkék: statisztika internet net never ez egy perc történik minute domo sleeps

Ajánlott bejegyzések:



5.2 milliárd netező 1 perce

Ez történt 2019-ben egy perc alatt a weben

Sötét jelen: agresszív zsarolóvírusok, tömeges bruteforce

Fiatal vagy? Ezekre az online csalásokra figyelj!

Ransomware helyzetjelentés

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

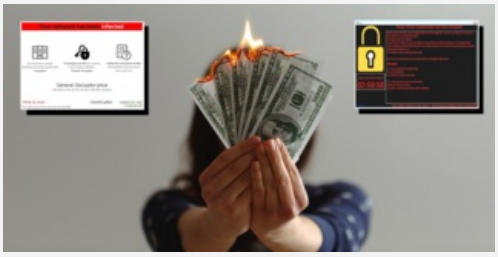
accountz

- Belépés
- Regisztráció

Fejemen olvad a vaj, engem nem érhet baj

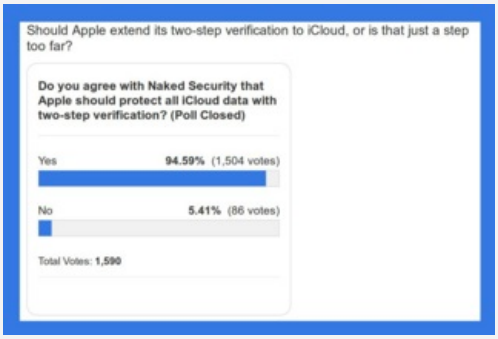
2021. június 07. 09:58 - Csizmazia Darab István [Rambo]

P. Mobil rajongók előnyben, legalábbis ami a címadást illeti. Persze ez csak egy alkalmi cím, ám ha tovább nézünk, a Colonial Pipeline csővezetéket ért **ransomware támadás és a végül kifizetett 4,4 millió dollár váltságdíj esetét, sokakban felmerülhet a kérdés, mi vezetett idáig, egyáltalán hogy történhetett meg ez?**



Nem lehet, hogy talán éppen az az elképesztő csoda, hogy csak most került arra a sor, hogy egy ilyen komoly incidens megtörténjen? **Volt már pár olyan támadás, adatszivárgás, ahol világosan bebizonyosodott, durva mulasztások következték ki a pokolba vezető utat.**

Emlékezzünk például a LinkedIn 2012-es adatlopási ügyére, ahol 6.5 millió felhasználó adata került illetéktelen kezekbe, és az derült ki, hogy **az üzemeltetők magánál a jelszó hashek kódolt tárolásánál az úgynevezett SHA-1 algoritmust szimplán használva nem támaszkodtak olyan megbízható kiegészítő technikákra, mint például a jobban véletlenszerűsítő, ezáltal a feltörésnek jóval ellenállóbb úgynevezett Salted eljárás**, megnövelve ezáltal a jelszó hash hosszát, és egyúttal a bonyolultságát is.



Hasonló hibák kerültek a felszínre a 2014-es fappening esetnél is, ahol számtalan híresség - például Jennifer Lawrence, Kate Upton, Kirsten Dunst, Avril Lavigne - meztelen képe jelent meg váratlanul a Reddit és a 4chan oldalain. **A támadásnál valószínűsíthetően a Find My iPhone szolgáltatásban rejlő gyenge-pontot használták ki, és ennek segítségével tudtak hozzáférni a fiókokhoz. Míg a jelszópróbálgatási limit például az iCloud rendszerben már korábban is be volt állítva, sajnos a támadás idején a Find My iPhone funkcióra viszont nem. Persze utóbb aztán az Apple aktiválta a brute-force elleni védelmet a Find My iPhone szolgáltatásra is, csak hát ugye későn.**

Végül aztán - vége jó, minden jó - kétlépcsős azonosítást kaptak az iCloud backupok is, valamint e-mail értesítést is bevezettek, melyben a felhasználóknak azonnal jelzik, ha valaki megpróbálja megváltoztatni az Apple ID jelszavukat, vissza akarja állítani az iCloud adataikat vagy amikor éppen először jelentkeznek be egy új eszközön a felhasználói fiókjukba.

A sort a végtelenségig lehetne folytatni, például a Target áruház lánc elleni akcióval, ahol a 2013. év végi incidensben a beszámoló szerint 70 millió ügyfél személyes adata és mintegy 40 millió hitel- és bankkártya adata került rossz kezekbe. **Az adatlopások nyilvánosságra kerülése után az üzleteikbe aztán már azonnal chipes kártyaolvasókat telepítettek, hogy elkerüljék az ismételt támadásokat**.

De itt állhat még az Equifax eset is, ahol hitelminősítéssel foglalkozó cég informatikai olyan súlyos incidenst szenvedett el, amelynek során 143 millió személyes adat kiszivárgott ki, köztük banki adatok is. A kritikus besorolású, távoli kódfuttatást lehetővé tevő CVE-2017-5638 **sérülékenység hibajavítás futtatásának elmaradása nagyban befolyásolta az adatlopást, pedig az Apache Struts sebezhetőségre kiadott javítófolt már 2017. március 7-én megjelent, a hibajavítás elvégzése hónapokig mégsem történt meg. Sőt, 2015. előtt egyáltalán nem is létezett náluk vállalati előírás a hibajavításokkal kapcsolatban feladatokkal-felelősségekkel,** és a későbbi úgynevezett Equifax Patch Management Policy finoman fogalmazva is erősen hiányos volt.

Innen dobbantunk akkor a mai témára, ami pedig a Colonial Pipeline csővezetékrendszer üzemeltetőjét ért kibertámadással kapcsolatos. Erről külön posztban mi is beszámoltunk, de ami érdekesebb, hogy **a cég vezetése most először ismerte el nyilvánosan, hogy valóban fizettek a zsarolóknak. Elmondásuk szerint az adott helyzetben nem igen tudtak mást választani, így május 7-én a váltságdíjat a bitcoinban átutalták**. Sajnos azonban a cserébe kapott visszafejtő eszköz olyannyira lassú volt, hogy helyette a inkább saját korábbi biztonsági mentéseikből állították helyre a rendszert.

Az egész incidens kiindulópontja az lehetett, hogy **a mérnökök által távmunkában felügyelt vezérléshez tartozó VPN fióknál nem használtak többtényezős hitelesítést, és ez a kompromittálódott hozzáférés került aztán a rosszindulatú hackerek kezébe. Azt egyelőre nem tudni, hogy a felhasználói accountot ellopták vagy feltörés vezetett eredményre. Mindenesetre a Bloomberg értesülése szerint a jelszót a darkweben az ottani kiszivárgott jelszavak gyűjteményében fedezték fel.**

Most az események után azt látni, hogy világszerte megugrott a kiberbiztosítások iránti igény, ám nem szabad elfelejteni, hogy hasonlóan a GDPR követelményeinek való megfeleléshez, ahol **sokan kizárólag csak a precíz jogi megfogalmazással készült jogi szövegekig jutottak, és a technikai védekezésre, végpontvédelemre, titkosításra, stb. egyáltalán nem fordítottak figyelmet, úgy hasonlóan itt sem lesz elegendő szimplán csak a biztosítások megkötése a megelőzésre és a kibervédelemre fordított erőforrások nélkül, ezzel mintegy "letudva" a feladatot.**

Sőt ez vissza is üthet, hiszen láthatóan a ransomware elleni biztosítással rendelkező cégek, állami hivatalok sokkal engedékenyebben fizettek váltságdíjat az átlag piaci szereplőkhöz vagy magánemberekhez viszonyítva, és erre a támadók is ráéreztek. Úgy tűnik, sok esetben éppen emiatt fokozódott a célzott támadás az állami közintézmények, kórházak, iskolák, önkormányzatok ellen. És most már a "Hack the Planet" jegyében jönnek az

olajvezetékek, húsipari üzemek, és minden egyéb IS.

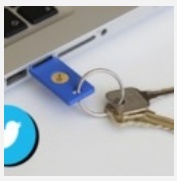
Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: apple account biztosítás ellopott húsipar hitelesítés mulasztás váltságdíj target ransomware pipeline jbs autentikáció equifax colonial kétfaktor kéttényezős zsarolóvírus többfaktoros

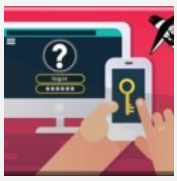
Ajánlott bejegyzések:

Offline mennyország - egy rövid időre

Fizess vagy einstandoljuk a kőolajvezetékedet!



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



iPhone mint biztonsági kulcs Chrome-hoz

Váltságdíjat kínálnak a váltságdíjszedő bandáért

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia-Darab István
@antivirusblog

Riasztás az interneten terjedő, zsaroló hangvételű levelekkel kapcsolatban: buff.ly/3pYqghq

5m

Csizmazia-Darab István
@antivirusblog

Remember Norton 360's bundled cryptominer? Irritated folk realise Ethereum crafter is tricky to delete: buff.ly/32YuAV8

Embed View on Twitter

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

Kémek krémje

2021. június 10. 09:30 - Csizmazia Darab István [Rambo]

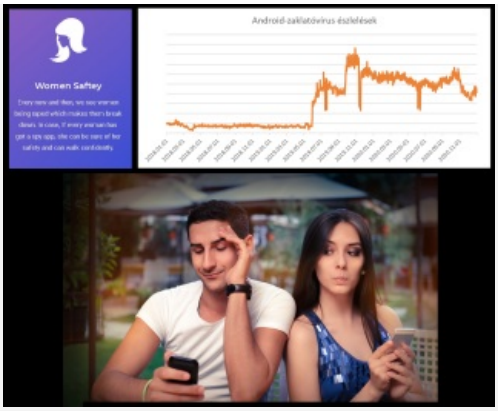
Az ESET kutatása szerint **a leggyakrabban használt androidos megfigyelő-kémkedő alkalmazások olyan sebezhetőségekkel vannak tele, amelyek nem csak az áldozatokra nézve jelentenek súlyos fenyegetést, de ezenfelül a zaklatók adatait és biztonságát is nagyban veszélyeztetik.**

A mobilos megfigyelő-kémkedő alkalmazás, más néven "spouseware", azaz "házastárs vírus" egy **olyan rejtett megfigyelő szoftver, amelyet a zaklató az áldozat tudta nélkül titokban telepít rá annak eszközére. Ehhez az elkövetőnek általában rövid időre fizikailag is hozzá kell férnie az áldozat eszközéhez, ezért a zaklatók gyakran az áldozat közeli családtagjai, esetleg ismeretségi vagy munkahelyi köréhez tartoznak.**

"*A mobilos megfigyelő appos kémkedés egyre gyakoribb fenyegetés, amelyet legálisan értékesítenek különböző webhelyeken. A telemetriai adatok szerint a megfigyelő-kémkedő app-észlelések száma 2020-ban mintegy 48 százalékkal emelkedett a 2019-es évhez képest. Kutatásunkban több, mint 80 ilyen androidos megfigyelő-kémkedő app családot vizsgáltunk meg, a biztonsági problémákra és a kódjukban lévő kihasználható adatvédelmi hibákra összpontosítva*." - magyarázta Lukáš Štefanko, az ESET kutatója.

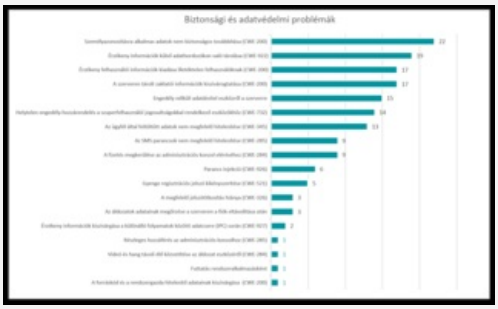
A megfigyelő-kémkedő app - többek között - **leköveti az áldozat eszközének GPS-helyzetét, az áldozat beszélgetéseit, képeit és a böngészési előzményeit is. Emellett az összes adatot tárolja és azokat a kémkedő részére titokban továbbítja** - ezért döntött úgy az biztonsági cég, hogy alaposabban megvizsgálja, miként kezelik az alkalmazások készítői az így megszerzett személyes adatokat. A gyártók úgy tudnak észrevétlenek maradni és elkerülni azt, hogy megfigyelő-kémkedő appként jelöljék meg a termékeiket, hogy **sok esetben gyermekek, alkalmazottak vagy nők számára védelmet nyújtó "ártalmatlan" alkalmazásként aposztrofálják ezeket a programokat.**

Ugyanakkor a weboldalaikon sokszor megjelenik a "kémkedés" szó is, tehát nem olyan nehéz megtalálni ezeket az online eszközöket - még csak nem is kell hozzá darkwebes vagy illegális oldalakat böngésznünk. **Az alábbi képernyőkép az egyik legkellemetlenebb példája annak, amikor egy alkalmazás hamisan azt állítja, hogy a nők biztonsága érdekében kémkedik utánuk. A leírás szerint a nyomonkövetésükkel megelőzhető a nők megerőszakolása.**



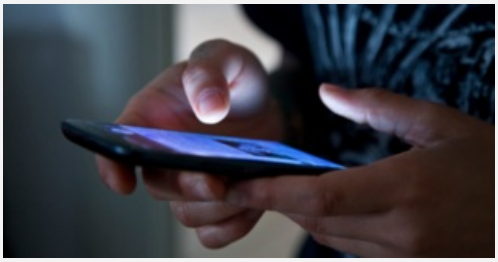
Mivel a megfigyelő-kémkedő alkalmazások etikailag megkérdőjelezhető viselkedésre ösztönözhetnek, a legtöbb mobilbiztonsági megoldás nemkívánatosként vagy károsként jelöli meg azokat. Tekintettel arra, hogy ezek az alkalmazások több információt gyűjtenek, tárolnak és továbbítanak, mint bármelyik másik, az áldozatok által telepített alkalmazások közül, a kutatók kíváncsiak voltak arra, hogy hogyan védik ezt a hatalmas mennyiségű, különösen bizalmas adatot.

A kutatók manuálisan vizsgálták meg 86 különböző gyártó 86 androidos megfigyelő-kémkedő applikációját: **elemzésükben zaklatónak nevezik a megfigyelő-kémkedő appot telepítő, majd távolról megfigyelő és irányító személyt; a célszemélyre, akit a zaklató a vírussal titokban megfigyel, a leírásban áldozatként hivatkoznak. Támadónak pedig azt a harmadik felet nevezik, akiről általában sem a zaklatónak, sem az áldozatnak nincs tudomása**. Ez a külső kibertámadó képes távolról kiaknázni a megfigyelő-kémkedő appok vagy más megfigyelő-szolgáltatások biztonsági- vagy adatvédelmi réseit, sebezhetőségeit.



Az elemzés során a kutatók számos súlyos biztonsági és adatvédelmi problémát azonosítottak, **amelyeket kihasználva egy külső támadó át tudja venni az irányítást az áldozat eszközei felett, továbbá a zaklató fiókja felett is. Emellett könnyen megszerezheti az áldozat adatait, hamis bizonyítékokat tölthet fel az eszközére, amivel gyanúba keverheti, vagy távoli kódfuttatással akár tetszőleges parancsokat is végrehajthat a gyanútlan áldozat okostelefonján.**

Az 58 Android-alkalmazás közül összesen 158 biztonsági és adatvédelmi problémát fedeztek fel, amelyek komoly fenyegetést jelentenek **nem csak az áldozatra nézve, de még a zaklató, sőt esetenként maga az alkalmazás gyártója is bizonyos mértékű kockázatnak van kitéve.**



Az ESET a biztonsági rések 90 napon belüli koordinált nyilvánosságra-hozatalával kapcsolatos irányelveinek megfelelően többszörösen is értesítette ezekről a problémákról az érintett gyártókat. **Sajnos ezek közül eddig mindössze hat gyártó javította ki az alkalmazásaikban észlelt problémákat.**

Negyvennégy gyártó egyáltalán nem válaszolt a megkeresésekre, hét pedig megígérte, hogy hamarosan megoldja a problémákat egy közelgő biztonsági javító frissítéssel. Emellett volt egy olyan gyártó is, amelyik úgy döntött, hogy egyáltalán nem javítja ki a jelzett problémákat.

A kutatás figyelmeztetésként szolgálhat a stalkerware szoftverek felhasználói számára, mivel **házastársaik, szeretteik, munkatársaik titkos alkalmazásokkal való ellenőrzése nemcsak etikátlan, de ráadásul ezzel még el is lophatják a résztvevők személyes és bizalmas információit, illetve kibertámadás és csalás áldozataivá is válhatnak.**

Mivel szoros kapcsolat állhat fenn a zaklató és az áldozat között, a zaklató privát információi is könnyen kiszivároghatnak. A kutatásból emellett még az is kiderül, hogy néhány megfigyelő-kémkedő app az alkalmazást használó zaklató adatait is eltárolja, valamint azután is tovább gyűjti az áldozatok adatait, hogy a zaklató már kérte az adatok törlését.

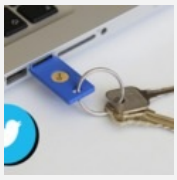
Mindez csak egy kis részlete a kutatás tanulságainak, a teljes átfogó jelentés, angol nyelven az alábbi linkre kattintva érhető el.

1 komment
Címkék: biztonság adatvédelem megfigyelés kémkedés welivesecurity.com stalkerware

Ajánlott bejegyzések:


Kiberkockázatok - miért nehéz velük lépést tartani?


Amazónia veszélyes ragadozói ;-)


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

Átvészelt homeoffice


Egyéb (járulékos) veszélyek

Kommentek:

Bandibacsi34 2021.06.11. 09:12:21

Jatek a szavakkal. A zaklato az, aki zsarol az informaciokkal. Az "aldozat" az megfigyelt(ennek pozitiv okai is lehetnek pl kiskoru eseten ne keveredhessen rossz tarsasagba(drogosok, prostitualt futtatok, rejtőzködő kejgyilkosok stb. stb es ne tuntethessek el (VV Fanni) nyomtalanul), akire valószínűleg gyanakszik a masik fel(pl. pumpolja penzert mikozben masnak teszi szet a labat, ami kb olyan, mintha a kozos vallalkozasbol valaki kilopna a penzt. Harmadik fel is hekkelgetheti a dolgokat, de azok valoszinuleg celzott tamadasok. Nem tudom mi ezzel a baj. A Facebookon es hasonlo appokon vilag allambacsi(FBI, CIA es hasonloak) kemkednek. Most "loptak el" (vagy ugy csinaltak par milliard jelszot www.gizchina.com/2021/06/08/the-largest-data-leak-including-8-4-billion-passwords-is-online/, amirol kuss van.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Van másik!

2021. június 15. 09:42 - Csizmazia Darab István [Rambo]

A régesrégi bohóctréfa poénja szerint mindig van egy másik, ami esetünkben viszont egyáltalán nem tréfa dolog. Hiszen **nagyon úgy tűnik, hogy a Colonial Pipeline és a JHS húsfeldolgozó elleni doxinggal ékesített ransomware támadás sajnos csak a kezdet, a bemelegítés, a próba volt.**

Mint az közismert, az idei májusi hónapot még sokáig fogják emlegetni a Colonial Pipeline csővezetékrendszer üzemeltetői. A zsarolóvírus támadás a mérnökök által távmunkában felügyelt vezérléshez tartozó gyengén védett, és emiatt kompromittálódott jelszavakkal indult, mellyel aztán **egy több hetes, az Egyesült Államok keleti partján jelentkező üzemanyaghiányt és hatalmas veszteséget okozó időszak vette kezdetét.**

Bár a cég megfizette a 4.4 millió dollárnyi (1.27 milliárd HUF) váltságdíjat, a válság így is elhúzódott, mert a cserébe kapott visszafejtő eszköz olyannyira lassú volt, hogy helyette inkább saját korábbi biztonsági mentéseikből állították helyre a rendszert.

Közben lezajlott ugyan egy JBS elleni hasonló támadás is. A JBS a világ egyik legnagyobb húsfeldolgozó vállalata, amelynek székhelye Brazíliában található, és világszerte több, mint 250 000 alkalmazottja van. **A JBS USA elismerte, hogy célzott és szervezett kibertámadás áldozatai lettek, és az észak-amerikai és ausztrál informatikai rendszerek kiesése miatt vészhelyzet, káosz, áruhiány alakult ki.**

Itt is kifizették a váltságdíjat, ami 11 millió dollárnyi (3.17 milliárd forintnak megfelelő) kriptovaluta volt. Bár mindkét akció mögött oroszországi bűnözői köröket sejtenek, ezt nagyon nehéz lesz bizonyítani.

Ám közben a színfalak mögött egy másik csővezeték hálózat zsarolóvírussal való megtámadása is megtörtént, amiről csak most utólag kerültek fel információk. Eszerint a houstoni székhelyű LineStar Integrity Services hálózatát nagyjából a Colonial Pipeline incidenssel egyidőben támadták meg, erről az esetről azonban eddig sehol nem olvashattunk.

A mostani beszámolók szerint itt is hasonló - doxinggal, azaz adatlopással és kiszivárogtatással való fenyegetéssel kiegészülő - ransomware akció zajlott le. I**tt 70 GB bizalmas adatok sikerült ellopniuk az elkövetőknek, amelyet később részben feltöltöttek a darknetre.**

A Distributed Denial of Secrets weboldal jelzése szerint 37 GB nyilvánossá tett adat jelent meg, köztük **73 ezer e-mail üzenet, valamint 19 GB forráskód és adatállomány**. A támadást egy Xing Team nevű, vélhetően kínai bűnözői csapat követte el a Mount Locker ransomware program segítségével.

Bár a LineStar egy aránylag kisebb vállalat, **szakértők szerint erősen aggasztó, hogy az innen ellopott adatok között sok olyan bizalmas technikai információ lehet, amely később könnyen hasonló támadások előkészítéséhez, illetve végrehajtásához vezethet. Vagyis a címre visszautalva félő, hogy lesz másik, sőt egyre több másik.**

Szólj hozzá!
Címkék: váltságdíj adatlopás adatszivárgás csővezeték ransomware darknet zsarolóvírus doxing linestar

Ajánlott bejegyzések:

Fizess vagy einstandoljuk a kőolajvezetékedet!

"Illetéktelen fél korlátozott ideig hozzáférhetett fájlokhoz"


Persze hogy tudtam, csak nem sejtettem...


Te nem kapod vissza, de mindenki más igen

5 ok, amiért a ransomware még sokáig velünk maradhat

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.
VVV 03.
VVV 04.
VVV 05.
VVV 06.
VVV 07.
VVV 08.
VVV 09.
VVV 10.
VVV 11.
VVV 12.
VVV 13.
VVV 14.
VVV 15.
VVV 16.
VVV 17.
VVV 18.
VVV 19.

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

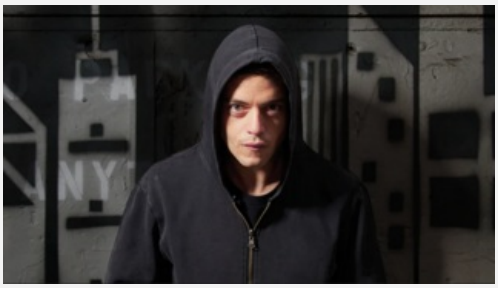
accountz

Belépés
Regisztráció

Diplomatákat támad a BackdoorDiplomacy

2021. június 17. 16:20 - Csizmazia Darab István [Rambo]

Az ESET Research által felfedezett **új APT-csoport, a BackdoorDiplomacy elsősorban közel-keleti és afrikai külügyminisztériumok hálózatába próbál bejutni, de az is előfordul, hogy telekommunikációs vállalatok kerülnek a támadások célkeresztjébe**. A folyamat során a kiberbűnözők a szervereken futó programok sebezhetőségeit kutatják fel és használják ki annak érdekében, hogy hátsó ajtót telepíthessenek ezekre.



A BackdoorDiplomacy esetében a támadást az ESET által Turian névre keresztelt hátsó ajtón (backdoor) keresztül indították. A hátsó ajtó szoftver lehetővé teszi a hackerek számára, hogy a titkosítási módszereket megkerülve távolról belépjenek a rendszerbe, ahol titokban érzékeny adatokat, jelszavakat és más fontos bizalmas információkat gyűjthetnek és lophatnak el a felhasználóktól.

A BackdoorDiplomacy képes felismerni a cserélhető adathordozókat, főleg az USB flash meghajtókat, melyek tartalmát a fő meghajtó lomtárába másolja át.

A BackdoorDiplomacy ugyanolyan taktikákat, technikákat és eljárásokat használ, mint más hasonló ázsiai székhelyű kémkedő csoportok. Jean-Ian Boutin, az ESET fenyegetéskutatási vezetője szerint **a Turian valószínűleg egy fejlettebb verziója a Quarian nevű hátsó ajtónak, mely utoljára 2013-ban mutatott aktivitást szír és amerikai diplomáciai célpontok ellen.**

A Turian hálózati titkosítási protokollja szinte teljesen megegyezik más ázsiai központú bűnszervezetek által használt, Calypso, illetve Whitebird nevű hátsó ajtó program titkosítási protokolljával. Érdekesség, hogy a Whitebird-öt a BackdoorDiplomacy-val egyidőben (2017-2020) alkalmazták szintén diplomáciai szervezetek elleni támadások során Kazahsztánban és Kirgizisztánban.

A BackdoorDiplomacy korábban több afrikai ország külügyminisztériumában, valamint Európában, a Közel-Keleten és Ázsiában is indított támadásokat. Továbbá célpont volt számos afrikai telekommunikációs társaság és legalább egy közel-keleti jótékonysági szervezet is.

Az elkövetők minden esetben hasonló támadási taktikákat, technikákat és eljárásokat (TTP) használtak, de még a közeli földrajzi régiókban is rendszeresen módosították az alkalmazott eszközöket, ami nagyban megnehezítheti a csoport nyomon követését.

A bűnözői csoport Windows és Linux alapú szervereket egyaránt támad, leginkább olyan internetes portokon keresztül, ahol valószínűsíthetően gyenge a fájlfeltöltési biztonság, illetve javítatlan biztonsági rések találhatóak a rendszerben. Az áldozatok egy részét olyan adatgyűjtő fájlokon keresztül célozták meg, amelyeket cserélhető adathordozók (valószínűleg USB flash meghajtók) keresésére terveztek.

A beépülő modul rendszeresen megvizsgálja az ilyen meghajtókat, és a cserélhető adathordozók behelyezésének észlelésekor megkísérli az összes rajta található fájl jelszóval védett archívumba való másolását.

A kártevő képes továbbá az áldozat rendszerinformációinak ellopására, titokban képernyőképek készítésére, illetve tetszőleges fájlok írására, áthelyezésére vagy törlésére is. A csoport kártékony tevékenységéről további részletek az ESET "BackdoorDiplomacy: Upgrading from Quarian to Turian" című angol nyelvű blogcikkében olvashatók bővebben.

Szólj hozzá!
Címkék: spyware calypso diplomácia kémkedés bűnbanda eset BackdoorDiplomacy turian

Ajánlott bejegyzések:


Mennyi? 23. Mi 23? Miért mi mennyi?


Sötétben bújkáló shadowIT


Váltságdíjat kínálnak a váltságdíjszedő bandáért


Nyerd meg az életed - vagy mégsem?


Sötét jelen: agresszív zsarolóvírusok, tömeges bruteforce

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

FinTech: az előretörés ideje

2021. június 23. 07:53 - Csizmazia Darab István [Rambo]

A koronavírus-járvány hatására életünk számos oldala lassult le, akadt vagy szűnt meg teljesen - ugyanakkor vannak területek, melyek sokkal gyorsabban fejlődtek, mint azt bárki várta volna. **Az elmúlt évre reflektálva az ESET az egyik ilyen gyorsan fejlődő terület, a pénzügyi technológiát, azaz a FinTech helyzetét vizsgálta.**

A felmérésnél több, mint 10 ezer fogyasztót és senior üzleti vezetőt kérdeztek meg az Egyesült Királyságban, az Egyesült Államokban, Ausztráliában, Japánban, Mexikóban és Brazíliában. A kutatás a FinTech-kel kapcsolatos tapasztalatokat, az ezzel kapcsolatos megoldások jövőjét és a kiberbiztonsági szokásokat vizsgálta. Mivel a lezárások hatására életünk számos területe költözött az online térbe, így nem meglepő, hogy a FinTech alkalmazások használata is megnőtt.

Az ESET felmérésének fogyasztói szegmenséből kiderült, hogy globálisan **a felnőtt fogyasztók 51%-a 1-5 féle FinTech alkalmazást használ, ideértve a digitális pénztárcákat, a költségvetés-tervező alkalmazásokat és a virtuális bankokat. Mindössze egyharmaduk (33%) válaszolta azt, hogy nem változtak a bankolási szokásaik a koronavírus miatti lezárások idején.**

Annak ellenére, hogy több FinTech alkalmazást is használnak, **világszerte csak a fogyasztók fele (49%) telepített minden eszközére biztonsági szoftvert, így a másik felük védtelen a pénzügyeiket célzó kibertámadásokkal szemben. 42 százalékuk nem használ jelszókezelőt, amely segítene az erős és egyedi jelszavak létrehozásában-kezelésében**, illetve a hitelesítő adatok kitöltésének és a brute force-támadások megakadályozásában.

A kiberbiztonság terén a fogyasztók továbbra is kockázatos magatartást tanúsítanak, például nyilvános WiFi hotspotokhoz csatlakozva hajtanak végre pénzügyi tranzakciókat.

Ahogy a FinTech alkalmazások használata egyre fontosabbá és széleskörűbbé válik, elengedhetetlen, hogy a

kiberbiztonsági gyakorlatok lépést tudjanak tartani ezzel - ellenkező esetben a magánszemélyek és a vállalkozások is azt kockáztatják, hogy kiszolgáltatottá válnak a támadásoknak. A FinTech-be történő befektetés vonzó lehetőség a vállalkozások számára is, mivel **a technológia számos előnnyel jár: többek között kevesebb költséget, könnyű használatot és a piacra történő egyszerűbb belépést kínál.**

A vállalkozások döntő többsége (81%) egyetért abban, hogy a koronavírus-járvány még szükségesebbé tette a pénzügyek fokozott védelmét. Ezen felismerés ellenére csaknem egyharmaduk (28%) nem fektet be aktívan a pénzügyek védelmének megerősítését célzó új technológiákba, vagy legalábbis nem tudatosan.

Ami a jövőbeli terveiket illeti, a senior üzleti vezetők több, mint kétharmada (68%) arra számít, hogy vállalataik FinTech-befektetései növekedni fognak a 2021-es és 2022-es évben. A vállalkozások fele már online fizetésfeldolgozó és könyvelési megoldásokat használ pénzügyeinek kezeléséhez, harmaduk pedig fontolgatja a szabályozási technológia (RegTech), a bankfiók nélküli bankok és a biztosítási technológia (InsurTech) alkalmazását.

Az üzleti működést világszinten átalakító különböző pénzügyi technológiák a következők:

- Online fizetésfeldolgozók: az ESET kutatásából kiderül, hogy az online fizetésfeldolgozás a vállalatok által legnagyobb mértékben használt pénzügyi technológia, a vállalatok 56 százaléka alkalmazza. A fizetésfeldolgozók irányítják a hitel- vagy bankkártya tranzakció folyamatát, továbbítják az ügyfelek kártyaadatait a vállalkozások bankjainak.

- Online határokon átnyúló fizetés: szintén egy rendkívül fontos technológia a globális e-kereskedelem szempontjából. Egyre gyakrabban fordul elő, hogy a tranzakció címzettje és kedvezményezettje külön országokban tartózkodnak, ezért fontos, hogy a vállalkozások képesek legyenek határokon átívelve utalni - ez egyike a megannyi területnek, ahol a FinTech egyre gyorsabbá és biztonságosabbá teszi a pénzügyi folyamatokat.

- Online számlázás: **a világ vállalatainak csaknem fele (44%) használ online számlázást.** Ez a technológia leegyszerűsíti a számlázási folyamatot, lehetővé téve a vállalkozások számára a pénzforgalom hatékonyabb nyomon követését.

- Biztosítási technológia (InsurTech): az InsurTech egy rendkívüli gyorsasággal növekvő szektor, **a vállalkozások 33 százaléka használja jelenleg és 32 százalékuk fontolgatja a jövőbeni alkalmazását**. Az új típusú - például az intelligens eszközök által gyűjtött - adatok felhasználásával az InsurTech lehetővé teszi a vállalatok számára, hogy igazán testreszabott biztosítási irányelveket hozzanak létre.

- Szabályozási technológia (RegTech): a RegTech automatizálással oldaná meg a szabályozással kapcsolatos vállalati kihívásokat. A szektor úttörői arra használják ezt a technológiát, hogy a szabályozásokkal kapcsolatos monitoringot, riportálást és megfelelőséget biztosítsanak a vállalkozások számára.

A senior üzleti vezetők 45%-a úgy véli, hogy az online fizetésfeldolgozók hozzájárulhatnak a profitnöveléshez, ezáltal segítve a vállalatokat a talpra állásban egy sokak számára rendkívül nehéz év után. A fogyasztók úgy tervezik, hogy a világjárványt követően is többet fognak online vásárolni, vagyis a kiskereskedők több

pénzügyi tranzakciót fognak online feldolgozni, amihez megfelelő és biztonságos technológiára lesz szükségük.

Amint ezek a friss példák is szemléltetik, a pénzügyi technológiát sokféleképpen alkalmazzák szerte a világon, és szerepe a globális üzleti életben csak növekedni fog az elkövetkező években, ezért minden eddiginél fontosabbá válik majd ezen pénzügyi megoldások megfelelő kibervédelme.

Szólj hozzá!
Címkék: statisztika kutatás felmérés eset pénzügyi fintech kibervédelem

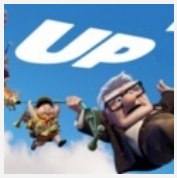
Ajánlott bejegyzések:


Sötét jelen: agresszív zsarolóvírusok, tömeges bruteforce


Ransomware helyzetjelentés

Támadás, e-mail a neved

Oly távol vagy tőlem, és mégis közel



5.2 milliárd netező 1 perce

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

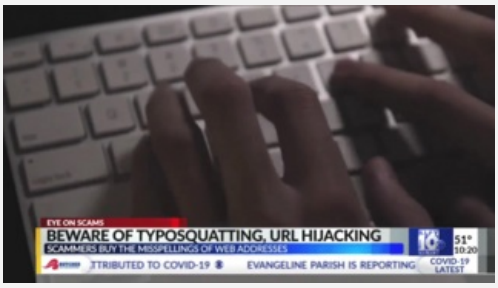
Hol jársz, hová mész?

2021. június 29. 07:24 - Csizmazia Darab István [Rambo]

A cím arra próbál utalni, hogy böngészés közben nem mindig vagyunk tudatában annak, vajon tényleg jó helyen járunk-e éppen. Mobileszközön pedig, ahol a kis méretű kijelző ráadásul az URL felismerést is nehezíti, még plusz nehezítést jelent az asztali gépekhez viszonyítva. Következzen néhány jótanács, mire érdemes figyelni.

Beszéltünk már többször is arról, hogy az **adathalász oldalak esetében gyakori az olyan próbálkozás**, mint például ha csak egyetlen, hasonló kinézetű betű eltérés van a hamis és az eredeti oldal címe között (typosquatting), ilyen karakterek például a nagy O betű és nulla, vagy a kis L betű és egyes. Ennél is furmányosabb az úgynevezett Internationalized Domain Name (IDN) homograph attack, **amikor más idegen nemzetiségű, például az orosz ABC betűiből alkotnak a támadók látszólag mégis latin karakterű hamis domaint.**

Itt alaposan meg kell nézni a címet, mert ami majdnem az, az nem az. Hasznos lehet például, ha a ShowIP is mutatja a webhely címét, vagy **fut a háttérben a vírusvédelem mellett egy Netcraft jellegű böngésző kiegészítő.**

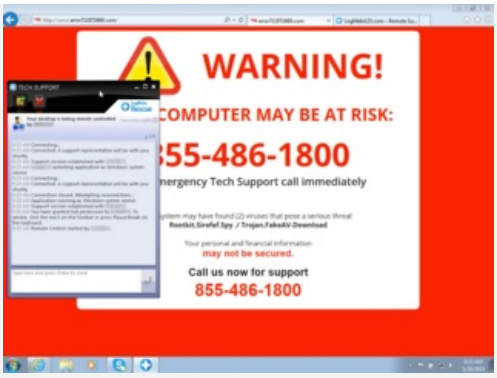


A gyanús URL címeket előzetesen akár meg is vizsgáltathatjuk online webes ellenőrzés segítségével. Erre alkalmas eszköz többek közt a Google Safe Browsing site status vagy pedig egy jól irányzott VirusTotal linkhivatkozás ellenőrzés.

De jó szolgálatot tehet egy WHOIS vagy Domaintools lekérdezés is, amely felsorolja a keresett domain részletes adatait, például hogy ki birtokolja azt, mikor és hol regisztrálták, és hogyan lehet kapcsolatba lépni a tulajdonossal. Itt az egyik fontos információ, amelyre érdemes figyelni, hogy a domain vajon frissen van-e regisztrálva, ami szintén jelezheti, hogy az rosszindulatú lehet.

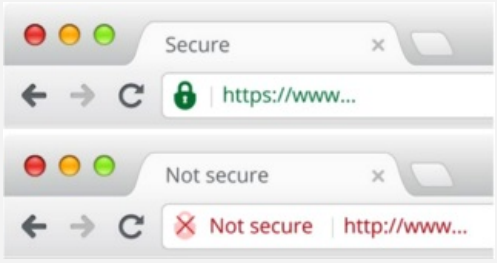
Ugyancsak hasznos lehet, ha egy hivatalosnak látszó oldal esetében **ellenőrizzük, hogy vannak-e adatvédelmi irányelvek?** Ezeknek kötelezően meg kel(ene)l jelennie a törvényesen működő szervezetek, ügyfélszolgálatok, hivatalok webhelyén, a hiányuk viszont megint csak komoly intő jel lehet. Az adatvédelmi előírások azt tartalmazzák, hogyan védi és kezeli az adott weboldal a felhasználói adatokat, azokhoz ki férhet hozzá, hol tárolják, és azt is, hogy szükség esetén hogyan kezdeményezhetjük innen saját adataink törlését.

Az adatvédelmi szabályok megsértését az Európai Unió által bevezetett adatvédelmi rendelet (GDPR) súlyos szankciókkal bünteti, például 10 millió EUR vagy a szervezet éves forgalmának 4%-át kitevő bírság kiszabásával.



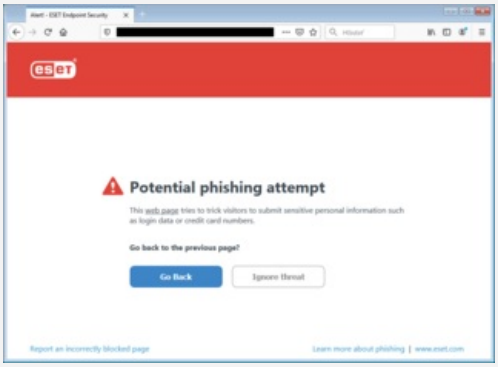
A törvényesen működő vállalkozások nem gördítenek akadályokat a közvetlen kapcsolatfelvételre, van személyesen felkereshető lokális irodájuk, posta címük, telefonos és e-mailes elérhetőségük, vagy e-mail cím hiányában legalább egy webes üzenetküldő űrlap alkalmazást használnak erre.

Ha a megkeresésekre nem kapunk választ, esetleg a hívott számon idegen akcentusú, gyanúsan amatőr viselkedésű, részletes személyes adataink iránt viszont nagyon is érdeklődő személyek jelentkeznek be, **akkor joggal gyanakodhatunk csalásra**. Ilyenkor egy netes kereséssel érdemes hivatalos elérhetőségeket után kutatni, és inkább azon a telefonszámon felvenni a kapcsolatot az adott szervezettel.



Erről is sokszor beszéltünk már, például a karácsonyi vásárlások kapcsán: legyen SSL, lakat, https, érvényes tanúsítvány. **Figyelve az URL-t, a hihető árat, az ellenőrizhető és leinformálható kereskedőt, ellenőrizve az érvényes tanúsítványt, az SSL/TLS kapcsolat meglétét (kis lakat a címsorban), illetve emellett ellenőrizhetjük a keresőben a gyanús weboldal reputációját.**

Ha ezzel kapcsolatban például csupa panaszkodó találatot kapunk, akkor az is egy hasznos visszajelzés arra, hogy ne mi legyünk az éppen soron következő balek.



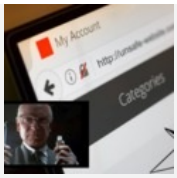
És végül, de semmiképpen nem utolsó sorban legyen mindig naprakész a szoftver környezet, beleértve ebbe nem csak az operációs rendszert, hanem minden alkalmazói programozt is. **Statisztikai tény, hogy a kártevők igen nagy százalékban javítatlan biztonsági rések, sebezhetőségek kihasználásával terjednek, jórészt automatikus kereséssel futtatva. Vagyis ilyenkor nem számít, hogy mi fontos vagy átlagemberek vagyunk-e, hanem csak az, hogy idejében lefuttattuk-e már a hibajavítást vagy sem.**

Természetesen egy hatékony vírusvédelmi program sem hiányozhat ma már, és jó hír, hogy **egy korszerű internetbiztonsági csomagban már rég nem csak egy egyszerű vírusirtó ketyeg, hanem olyan különféle integrált modulok dolgoznak**, mint Exploit Blocker, Botnet elleni modul, hálózati támadások elleni védelem, a biztonságos bankolást biztosító környezet, de természetesen a zsarolóprogramok illetve az adathalászat elleni védelem sem hiányzik a beépített védelmi eszköztárból.

Szólj hozzá!
Címkék: tippek hamis url böngészés phishing adathalászat webhely homograph typosquatting welivesecurity.com

Ajánlott bejegyzések:

[Stop adathalászat]



[Biztonságos? Biztonságos?]

[Ingyenes Omikron teszt vagy mégsem?]

[Vakcinás csalások, szevasztok]

[Fizessük számlánkat egyszerűen, egy kattintással]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

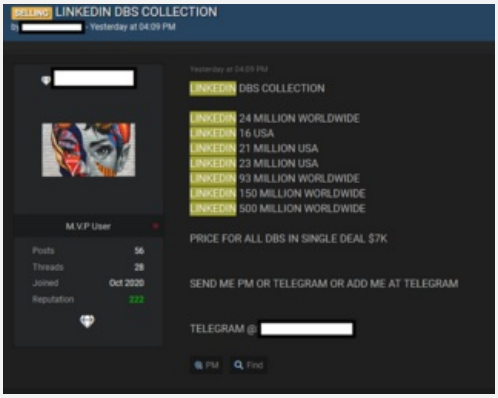
Megint jőnek, szivárogtatnak...

2021. július 02. 10:57 - Csizmazia Darab István [Rambo]

Csak éppen senki nem mondja nekik, hogy csendesebben vigadjanak. **Ismét itt egy újabb nagy csomag lopott/kiszivárgott LinkedIn account, számszerűsítve egész pontosan 700 millió, ami nem csak gombócból sok**. Idén már másodszor történik ilyen, a korábbi esetben 500 millió felhasználói adatot kínáltak eladásra. Szóval nem csak a Facebook szenved az ilyesmitől.

Június 22-én egy TomLiner nevű GOD User rangú felhasználó bocsátotta áruba a fent említett 700 millió LinkedIn accountot, amelyek tartalmazzák a teljes nevet, a felhasználó nemét, e-mail címeket és telefonszámokat, valamint részletes információkat a felhasználók szakmai tapasztalatairól.

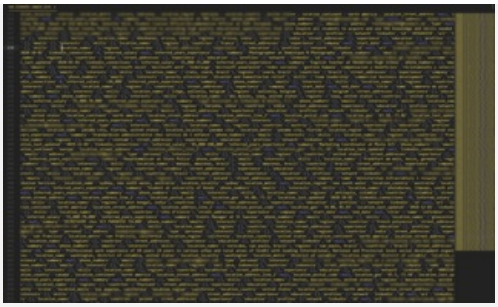
Ez elég nagy szám, **ha a hivatalosan is közölt LinkedIn taglétszámmal vetjük egybe, ami most éppen 756 millió, vagyis ha igaz a dolog, akkor szinte az egész (92%) adatbázist jelentheti.**



Nyomatékképpen **egy millió adatrekordot publikussá is tettek mintának, ezt pedig azután biztonsági kutatók alaposan átvizsgálták és elemezték. A Privacy Sharks munkatársai szerint a fájl valóságos adatokat tartalmaz**, és még arra sem utalnak egyértelmű jelek, hogy esetleg trükközésből valamilyen korábbi adatsértés állományát turbózták volna fel az eladók. A pár hónappal korábbi, 500 millió rekordot tartalmazó adatbázisért négy számjegyű összeget kértek amerikai dollárban.

A Privacy Shark a mintaadatok elemzését még etikusnak tartja, ám a teljes adatbázis megvásárlásától elzárkóztak, mert nem kívánják pénzzel támogatni a bűnözést.

A kutatók weblapján olvasható a LinkedIn-nel folytatott levelezésük is, sajnos ebben ismét az ilyenkor szokásos lepattintó hozzáállás köszön vissza az üzemeltetők részéről.

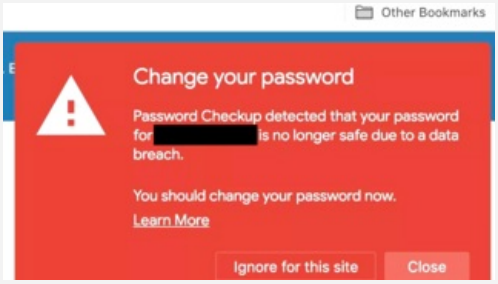


Emlékezetes, hogy a 2012-es LinkedIn adatszivárgásnál "csak" 6.5 millió felhasználó adata került illetéktelen kezekbe, ám nem ez volt a történetben a nagy érdekesség.

Hanem egyrészt az, hogy a jelszó hashek kódolt tárolásánál az úgynevezett SHA-1 algoritmust szimplán használva nem támaszkodtak olyan megbízható kiegészítő technikákra, mint például a jobban véletlenszerűsítő, ezáltal a feltörésnek jóval ellenállóbb úgynevezett Salted eljárás, megnövelve ezáltal a jelszó hash hosszát, és egyúttal a bonyolultságát is.

Másrészt az is fontos momentum volt az incidens utóéletében, hogy 2 teljes évnek kellett ahhoz eltelnie, hogy az üzemeltetők orvosolva a korábbi helyzetet jelentős biztonsági fejlesztéseket (bejelentkezéssel kapcsolatos kontroll, a jelszóváltoztatásról külön e-mailes emlékeztető értesítés, és saját adataink mentési lehetősége) végezzenek el és jelentsenek be.

Remélhetőleg a GDPR bevezetése után **már sehol nem lesz ilyen brutálisan hosszú időablak a hiányzó biztonsági javításokra.**

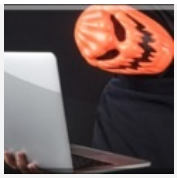


Ha valaki úgy gondolja, hogy az adatai akár személyes mulasztás miatt, akár valamilyen szolgáltató elleni a támadás részeként adatszivárgás részét képezik, **akkor fontolja meg jelszavának azonnali megváltoztatását.**

A megfelelően erős, vagyis nehezen feltörhető és egyedi jelszavak generálásához és nyilvántartásához a legjobb, ha erre alkalmas külön jelszókezelőt vagy az ezt a funkciót is ellátó vírusvédelmi alkalmazást használunk. **Ne feledkezzünk el a többtényezős hitelesítés engedélyezéséről sem, ami a szokásos SMS-en kívül a még biztonságosabb hardver token vagy mobilalkalmazás használatával történhet, ez szintén erősen ajánlott.**

Szólj hozzá!
Címkék: incidens linkedin jelszavak adatlopás adatszivárgás welivesecurity.com

Ajánlott bejegyzések:



[Halloween, helló adatok]

[GoDaddy - apák a pácban]

[Stop adathalászat]

[100 millió helyett "csak" 40 lett, maradhat?]

[Persze hogy tudtam, csak nem sejtettem...]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

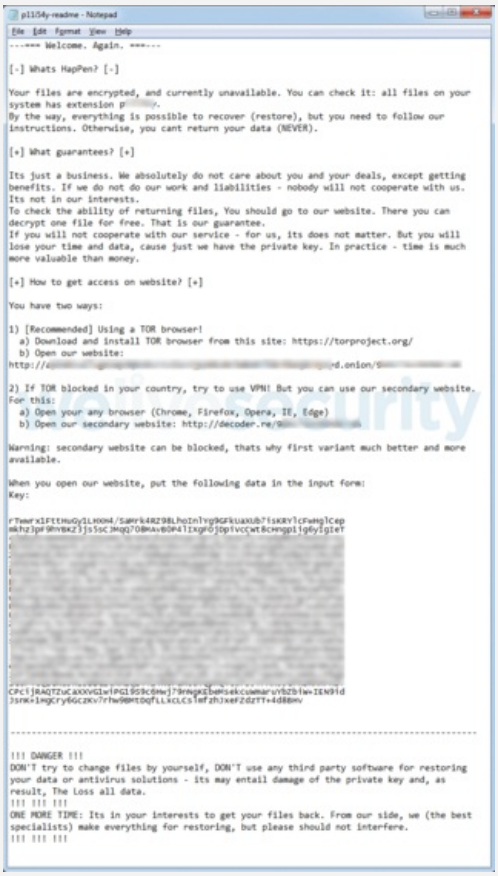
A Kaseya három napja

2021. július 06. 17:09 - Csizmazia Darab István [Rambo]

Épp csak felocsúdtunk a SolarWinds történetből, máris itt az újabb nagyszabású eset. **A Kaseya távmenedzsment szolgáltató elleni incidens rengeteg ügyfélnek okozott kellemetlen perceket, és kőkemény ransomware támadást.**

Mint az közismert, azok a cégek, amelyek rendszereik kezeléséhez, frissítéséhez a Kaseya ügyfelei voltak, nehéz helyzetbe kerültek, ugyanis egy átfogó támadás miatt **a REvil ransomware-banda, más néven Sodinokibi zsarolóvírus támadást hajtott végre és 70 millió dollárnak megfelelő kriptovalutát követel az üzemeltetőktől váltságdíjként.**

A beszámolók szerint a háttérben megindulhatott valamilyen alkudozás az árról, egyes vélemények szerint a Reutersnek és a Krebs Stamos Groupnak **sikerülhet lejjebb tornászni a kezdeti induló 70 milliós számot akár 50 millió környékére is egy univerzális dekódoló kulcsért.**

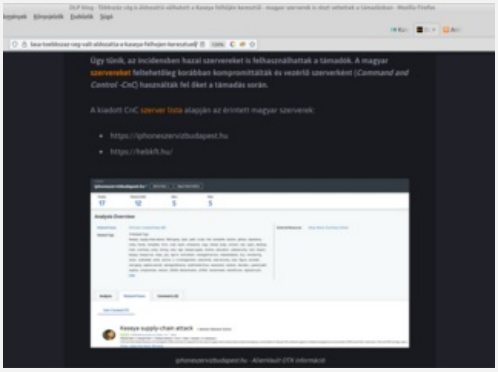


Világszerte 800 és 1500 közötti vállalkozást érinthet az incidens. Az éppen július 4-ét ünneplő **USA mellett több más európai ország, például Svédország is érintett, ott a Coop-szupermarketek százainak kellett bezárnia, mert a pénztárgépeik nem működtek.**

Emellett Új-Zélandon 11 iskola és több óvoda hálózata is leállt, ezt a támadók állítólag véletlen balesetnek, nem szándékos járulékos kárnak minősítették.

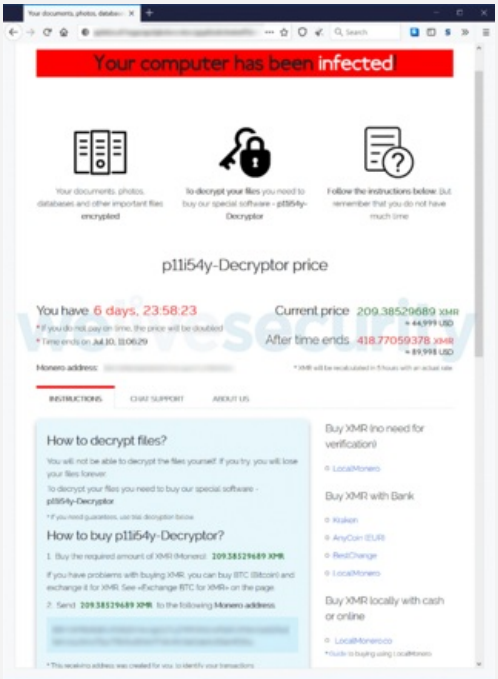
[A dlp.hu információi szerint magyar kompromittálódott szervereket is használhattak C&C szerverként a támadásban](). Ami viszont annak fényében, hogy **Magyarország évek óta rendszeresen előkelő helyet foglal el a botnet-tag zombigépek nemzetközi statisztikákban**, sajnos nem annyira meglepő.

A Kaseya egy idő után ugyan hivatalosan is értesítette a lehetséges áldozatokat, ám a ransomware lefutási idejéhez képest ez biztosan késedelmes lehetett.



[Az ESET telemetriai adatbázisa szerint a támadásban szereplő kártevő változat először július 2-án 15:22-kor volt megfigyelhető](), **ezt a vírusvariánst a védelem Win32/Filecoder.Sodinokibi.N trójaiként azonosítja és blokkolja.**

Az észlelések több különböző térségből is mutattak aktív fertőzéseket, **túlnyomó többségben az Egyesült Királyságból, Dél-Afrikából, Kanadából, Németországból, az Egyesült Államokból és Kolumbiából.**



Az USA Colonial Pipeline vezetékére mért hasonló csapás esetében [bár a vállalat május 7-én kifizette az 5 millió dollárnyi váltságdíjat](), **azonban a cserébe kapott visszafejtő eszköz olyannyira lassú volt, hogy helyette inkább a saját korábbi biztonsági mentéseikből állították helyre a rendszert.** Ennek fényében nagyon is kérdéses, hogy a Kaseya esetében mi lesz a további fejlemény, de nyilván hamarosan, idővel majd ez is kiderül.

Az biztos, hogy a korábbi Colonial Pipeline, az ACER, [a JBS húsüzem incidens]() és **a mostani Kaseya elleni akció után ez egyértelmű hadüzenet, várhatóan egyre gyakoribb és erőteljesebb csapásmérésekkel.**

[Szólj hozzá!]()
Címkék: [c&c]() [botnet]() [váltságdíj]() [revil]() [ransomware]() [welivesecurity.com]() [kriptovaluta]() [zsarolóvírus]() [sodinokibi]() [kaseya]()

Ajánlott bejegyzések:

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

[Offline mennyország - egy rövid időre]

[Amikor a hóhért akasztják...]

[Felebarátod váltságdíját ne kívánd!]

[Ransomware napszemüvegben]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Régen minden jobb volt? Hitelesítés történelem dióhéjban

2021. július 09. 11:34 - Csizmazia Darab István [Rambo]

Egyik első Hacktivity látogatásom során - amely még a szép emlékű Fonó Budai Zeneházban zajlott, **volt 2009-ben egy érdekes előadás a szerzői jogokról, amely visszanyúlva az időben, olyan történelmi példákkal, és párhuzamokkal volt illusztrálva, mint a Biblia sokszorosításának joga, vagy később a könyvnyomtatási jog. Bodó Balázs volt az előadó, és a címe ez volt: "Csigát eszik, filmet tölt le, börtönbe megy - ki az?". Nos valami hasonlóról lesz szó most itt is.**

Egy érdekes történelmi összefoglaló jelent meg ezzel kapcsolatban, nézzünk akkor ebben pár jellegzetes régi mérföldkövet, honnan indultunk a mai helyzetig. Történészek és régészek szerint régi, 100 ezer évvel ezelőtt létező kultúrákban **az ékszerek jelezték a kiválasztott személy különleges státuszát, gazdagságát, hitelesítették származását.**

Az ilyen tárgyakhoz való kötődés, azonosítóként való használat eredményezte aztán később a katonai dögcédulákat is, a kutyák nyakában szereplő azonosítót, igazolványokat.

Nagy ugrással Krisztus előtt 1046-ig nyúlik vissza a tetoválás kifejezetten azonosításként való felhasználása, amikor is **a kínai Zhou-dinasztia idején a kínai hatóságok tetoválásokat használtak a foglyok megjelölésére.**

Azonban a legklasszikusabb identitás céljából használt látványos tetoválás **a maori kultúrában található, ahol Új-Zéland őslakosai testét és arcát jellegzetes, teljesen egyedi minták díszítik.** Maga a tetoválás elképesztően széleskörűen elterjedt lett, a korábbi börtöntetoválások, a jakuzák teljes testet borító jelentéssel bíró mintázatok alkalmazása ma már szimpla divattá vált, és persze minőségileg is óriásit fejlődött.

Az összeállítás megemlíti **az első útlevélként szolgáló személyazonossági okmány megjelenését, amelyet V. Henrik angol király uralkodása alatt hoztak létre, az 1414. évi** biztonságos magatartásról szóló törvény nyomán.

Ennek bevezetése szolgált az angol állampolgárok külföldi országokban való biztonságos utazására, ennek során az ellenőrző pontokon való áthaladáskor történő igazolásra.

Lassan elérkezünk napjainkhoz is, de ha valakinek feltennénk a kérdést, **vajon a személyi azonosító számok vajon mióta is léteznek, kevesen tippelnének 1829-re**. Pedig pontosan ebben az évben fogadta el a brit parlament azt a Fővárosi Rendőrségi Törvényt, amely lehetővé tette, hogy **személyes adatokat kezdjenek el tárolni az egyénekről, az aktákat pedig egyedi azonosító számmal kapcsolták a személyekhez.**

Jó száz évvel később pedig, **1936-tól az Egyesült Államok elkezdte forgalomba hozni a társadalombiztosítási igazolványokat**, ezt a példát pedig később számos más ország is követni kezdte.

És már itt is vagyunk a biometrikus azonosítóknál. **Sir William Herschel tisztként Indiában szolgált a brit hadsereg tagjaként, és felismerte, hogy az ujjlenyomatok egyediek és tartósak.**

1858-ban ő alkalmazta ezt először, ahol az akták a helyi munkaszerződésekben a munkavállalók ujjlenyomat mintáit is eltárolták. Később aztán persze a bűnüldözésben is kulcsszerepet kaptak már az ujjlenyomatok.

Az első számítógépes jelszóhoz érkeztük, **ennek dátuma 1961. Ezt pedig a Massachusettsi Műszaki Intézetben (CTSS) fejlesztették ki, szerepe pedig az volt, hogy az akkori úgynevezett időosztásos (time-sharing) rendszereken megossza a számítógép erőforrásait több felhasználó, illetve munkafolyamat között**. A jelszavakat manapság mint gyenge-pontot látjuk sokszor, támadható, feltörhető, illetve ha nem kellően erős és egyedi, akkor ellophatják, kiszivároghat.

A Have I Been Pwned adatbázisában ma már 11.4 milliárd kompromittált jelszó szerepel, az újságok főcímei pedig tele vannak informatikai incidensekkel. A szomorú helyzeten többek közt a Worst Password összefoglalókra is hivatkozó **praktikus jelszóválasztási tanácsokkal védekezhetünk, beleértve ma már a többfaktoros autentikációt is.**

Végül, de nem utolsósorban **a biometrikus azonosítás modern formái is jelen vannak életünkben, nagyjából 2004. óta történtek itt jelentős fejlesztések, például az USA néhány államában ekkor hoztak létre globális, az egész államokra kiterjedő tenyérlenyomat adatbázisokat.**

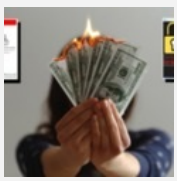
2010-től India is alkalmazott ilyet hitelesítési, illetve csalásmegelőzési céllal. **Ma már a legtöbb okostelefon képes arcfelismerésre, ujjlenyomat olvasásra, és ezzel digitális azonosításra.**

És ha már régi hacker élményekkel kezdtük, zárjunk is azzal. Szintén emlékezetes volt a 2012-es és 13-as, MOM Kultúrházban rendezett Hacktivity, ahol **Fehér András, Kapitány Sándor és Otti Csaba mutattak be olyan elképesztően egyszerű trükköket, amellyel simán átverhetőek voltak a biometrikus azonosítások, felejthetetlen például többek közt a színes nyomtatón frissen kinyomtatott arcképpel való sikeres azonosítás.**

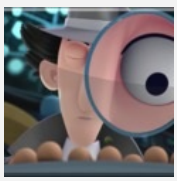
Szólj hozzá!
Címkék: biztonság történelem jelszó áttekintés hitelesítés biometria melegvan autentikáció

Ajánlott bejegyzések:


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


Fejemen olvad a vaj, engem nem érhet baj


Egyéb (járulékos) veszélyek


Májusi kétfaktor aranyat ér

10 kiberbiztonságra veszélyes szokás

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

- RSS 2.0
  bejegyzések, kommentek
- Atom
  bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

Tesz-e Oroszország a ransomware ellen?

2021. július 13. 10:35 - Csizmazia Darab István [Rambo]

Jó kérdés - mondhatná erre bárki. És valóban izgalmas kérdés, annak ellenére, hogy bár nyilván nem minden zsarolóvírus érkezik innen, de azért a számítógépes bűncselekmények terén, **újabban főképp a ransomware fronton a gyanítható orosz szál azért nagyon is ott van a szeren.**

A "két ember beszélget" kezdetű mondat valószínűleg alig érdekel valakit, **de ha ez a két ember történetesen nem más, mint Joe Biden és Vlagyimir Putyin, akkor ez a beszélgetés máris azonnal érdekesebb lehet, ha pedig ráadásul a zsarolóvírus támadások kérdése is szóba kerül ebben a telefonbeszélgetésben, akkor különösen.**

Ebben a bizonyos beszélgetésben úgy került terítékre az ügy, hogy a SolarWinds, Kaseya, Colonial Pipeline, JBS húsfeldolgozó elleni doxing és egyéb ügyek kapcsán is sejthető, **érzékelhető volt egy oroszországi támadó szál - például a Kaseya incidensnél a REvil (Ransomware Evil) -, míg az ellen oldalon Egyesült Államokbeli, gyakran európai vállalkozások is szenvedtek tetemes károkat a másik oldalon.**


CNBC

MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV WATCHLIST PRO

POLITICS

Biden presses Putin to disrupt cybercriminals in Russia as U.S. grapples with latest ransomware attacks

PUBLISHED FRI, JUL 9 2021 1:03 PM EDT | UPDATED SAT, JUL 10 2021 2:39 AM EDT

Christina Wilkie
@CHRISTINAWILKIE

SHARE

KEY POINTS

- President Joe Biden pressed Russian President Vladimir Putin in a phone call Friday to take action to stem recent ransomware attacks from Russia-based groups.
- "I made it very clear to [Putin] that the United States expects, when a ransomware operation is coming from their soil even though it's not, not, sponsored by the state, that we expect them to act," Biden said Friday afternoon at the White House.
- The call came just days after a massive new cyberattack by the group REvil, believed to be based in Russia.

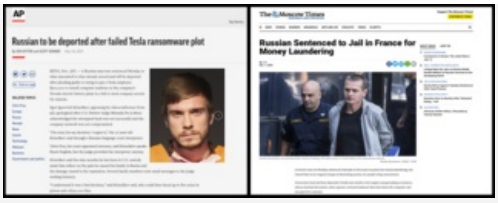
TRENDING

U.S. President Joe Biden speaks before signing an executive order in the State Dining Room of the White House in Washington, D.C., U.S., on Friday, July 9, 2021.

WASHINGTON – President Joe Biden pressed Russian President Vladimir Putin in a phone call Friday morning to take action to stem recent ransomware attacks from Russia-based groups.

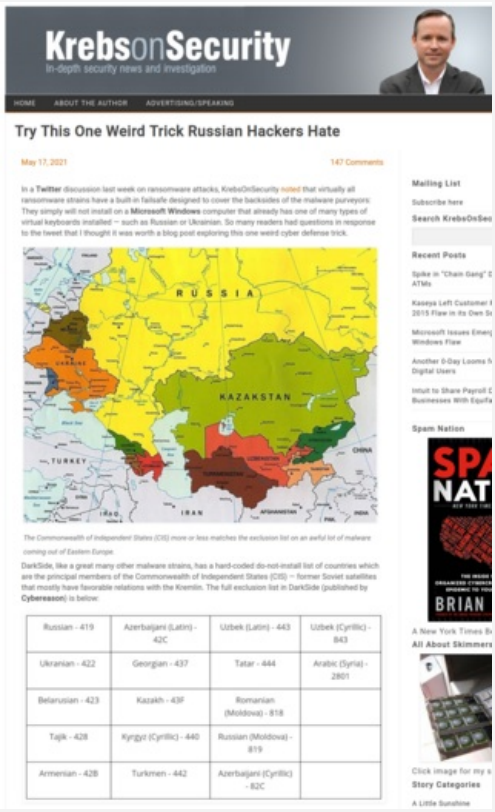
Az USA elnökének kérése pedig az volt, hogy **Oroszország tegyen sokkal határozottabb lépéseket az országuk területéről induló, ide köthető bűnözői csoportok leleplezésére, elfogására, megbüntetésére. A cél az lenne, hogy a hatóságok nagyobb és koordinált együttműködésben, vegyes bizottságot létrehozva, az USA kibervédelmi egységeinek észlelési bizonyítékainak átadásával rábírja Oroszországot a váltságdíjat kizsaroló bűnözők elleni tényleges fellépésre.**

Mint az közismert, a magyar iszlamista terrorista elfogásához is pontosan hasonló, a CIA által a magyar hatóságoknak átadott információk vezettek a leleplezéshez és a letartóztatáshoz.



Lehet-e bizonyítani konkrét országok érintettségét a ransomware támadásokban? **Nem lehetetlen, de valóban nagyon nehéz.** Gyanítani ugyanakkor könnyű. **Például a pénzek útjának követésével, hacker csoportok kitartó megfigyelésével, támadási módszerek jellegzetességeinek azonosításával, a C&C szerverek lenyomozásával is erősödhet a gyanú, ilyen például Észak-Korea államilag támogatott ténykedése zsarolóvírus ügyekben. A WannaCry esetében például egyértelműen az észak-koreai Lazarus csoportot tartják felelősnek.**

Orosz érintettségeket keresgélve a Google-ban is találhatunk pár ilyen hírt. 2021. márciusban például Egor Igorevich Kriuchkovot ítélték el, mert a Tesla szerverein próbált ransomware programot terjeszteni. 2020. decemberében ítélték 5 év börtönre Franciaországban azt az Alexander Vinniket, aki 135 millió EUR értékben hajtott végre zsarolóvírus támadásokat 2016. és 2018. között. **A néhány felderített és lezárt eset nyilvánvalóan csak a jéghegy csúcsa.**



Mindez a Biden-Putyin találkozón is szóba került abban a kontextusban, hogy ha olyan zsarolóvírussal találkozunk, amely az orosz nyelvű operációs rendszer beállítása esetén nem támad, akkor nehéz ezt az eredetet mással magyarázni. **Itt a blogon is írtunk például a Cerber kártevő visszatéréséről, amely indításkor ellenőrizte ezt, és a volt Szovjetunió tagköztársaságainak számítógépeit nem fertőzte meg.**

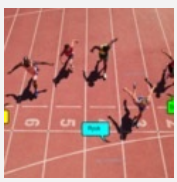
Biden a beszélgetésben azzal is érvelt, hogy a "megtűrt" bűnözői számítógépes csoportok jelenléte az orosz hálózatokon egyik országnak sem lehet hosszútávú érdeke, és mostantól határozott intézkedéseket vár el az orosz féltől, ha konkrét támadásokról minden technikai információt, segítséget átad. Meglátjuk, a szavakon túlmenően jelent-e ez bármi jót, vagy valódi előrelépést a jövőre nézve. Majd az idő eldönti...

21 komment
Címkék: együttműködés usa oroszország bizottság putyin megelőzés vegyes fellépés váltságdíj biden ransomware zsarolóvírus

Ajánlott bejegyzések:


Váltságdíjat kínálnak a váltságdíjszedő

Offline mennyország - egy rövid


Világrekord, aminek mégsem örül

Fizess vagy einstandoljuk a


Felebarátod váltságdíját ne kívánd!

bandáért időre senki kőolajvezetékedet!

Kommentek:

birka menet 2021.07.14. 23:34:37

Illibernyák ruszkiéknál ha nem ruszki célpont ellen végzel cyber támadást, akkor a törvény nem büntet. Ezzel államilag el is van intézve, hogy ruszkiék a világ legnagyobb nemzetközi cyber bűnözői.

Válasz erre

Ekrü 2021.07.15. 07:03:08

@birka menet: Mert gondolod ,hogy az amerikaiaknak nincsenek meg a saját cyber bűnözői ? Vagy a németeknek meg a franciáknak?A kínaiaknak?
A különbség csak annyi,hogy az oroszt fél kevésbé képmutató és nem sírja tele vele a világot ha egy-egy támadást nem tud kivédeni....

Válasz erre

nemecsekerno_007 2021.07.15. 08:35:51

@birka menet: Ja, Edward Snowden is azért lakik Moszkvában mert szereti a vodkát. :))))))

Válasz erre

MaxVal BircaMan KözÍró • http://bircahang.org 2021.07.15. 08:36:24

Felszólítom a USA elnökét, tegyen lépéseket az agymosó hollywoodi propaganda ellen!

Válasz erre

chrisred 2021.07.15. 10:11:15

@MaxVal BircaMan KözÍró: Tenne, ha a hollywoodi filmgyártás állami ellenőrzés alatt állna.

Válasz erre

MaxVal BircaMan KözÍró • http://bircahang.org 2021.07.15. 10:13:34

@chrisred:

S az orosz hackerek állami ellenőrzés alatt vannak?

Válasz erre

chrisred 2021.07.15. 10:16:15

@MaxVal BircaMan KözÍró: A GRU minden bizonnyal igen.

Válasz erre

MaxVal BircaMan KözÍró • http://bircahang.org 2021.07.15. 10:18:11

@chrisred:

Tehát minden orosz hacker a GRU alatt működik?

Válasz erre

chrisred 2021.07.15. 10:19:36

@MaxVal BircaMan KözÍró: Bőven elég lenne azokat megfékezni, akik igen.

Válasz erre

MaxVal BircaMan KözÍró • http://bircahang.org 2021.07.15. 10:21:54

@chrisred:

Ahogy Biden is csak az állammal együttműködő hollywoodi cégeket zárja be.

Válasz erre

chrisred 2021.07.15. 10:33:14

@MaxVal BircaMan KözÍró: Vedd úgy, hogy megtörtént, az összes álllammal együttműködő hollywoodi cég be van zárva.

Válasz erre

MaxVal BircaMan KözÍró · http://bircahang.org 2021.07.15. 10:37:14

@chrisred:

Ez nem látszik.

Válasz erre

chrisred 2021.07.15. 10:47:58

@MaxVal BircaMan KözÍró: Persze, hogy nem látszik, nincs olyan hollywoodi cég, ami a szövetségi államnak alárendelve működne.

Válasz erre

MaxVal BircaMan KözÍró · http://bircahang.org 2021.07.15. 10:50:57

@chrisred:

Nyíltan nyilván nincs. De nyíltan GRU-hacker sincs.

Válasz erre

chrisred 2021.07.15. 11:27:39

@MaxVal BircaMan KözÍró: Minek titkolna ilyesmit bárki is?

Válasz erre

élesi 2021.07.15. 11:43:07

@chrisred: www.youtube.com/watch?v=SPuvX6MspFU

Válasz erre

chrisred 2021.07.15. 11:56:52

@élesi: Köszönöm, megvagyok nélküle.

Válasz erre

MaxVal BircaMan KözÍró · http://bircahang.org 2021.07.15. 12:03:59

@chrisred:

Mert így szokás.

Válasz erre

chrisred 2021.07.15. 12:40:11

@MaxVal BircaMan KözÍró: Attól függ, hol.

Válasz erre

birka menet 2021.07.15. 20:47:03

@MaxVal BircaMan KözÍró:

Hahaha, nagyon megszivatott téged chrised, te félkegyelmpü bulgár barom!

Válasz erre

MaxVal BircaMan KözÍró · http://bircahang.org 2021.07.16. 09:40:52

@birka menet:

Hol, mikor?

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó

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 ransomware-nek nincs No-go zóna

2021. július 19. 11:24 - Csizmazia Darab István [Rambo]

Noha az idők során fejlődött valamelyest mind az egyéni biztonságtudatos hozzáállás, mind a cégek kibervédelmi felkészültsége, **ám ez korántsem elégséges mértékű**. A korábbi "hiszen ez egy biztonságos platform, nem?", vagy éppen a "mi csak okosan netezünk" felhasználói érvelés mellett sajnos lépten-nyomon gyakori még a vállalati "mi egy ki cég vagyunk, ugyan ki támadna éppen minket?" típusú hamis vélekedés.

Az elmúlt időszak hangos volt a nagyszabású zsaroló támadásoktól, például a SolarWinds, Colonial Pipeline, JBS, Kaseya incidenstől. Ám a statisztikák is visszatükrözik ezt a növekedést, a Crowdstrike adatai szerint az elmúlt hat hónapban világszerte megugrott az ilyen támadások gyakorisága.

Emellett a követelt váltságdíjak mértéke is jelentősen megnőtt, amit a bűnözők követelnek az ellopott adatokat visszafejtő kulcsokért és hogy az ellopott bizalmas információkat ne töltsék fel publikusan a netre.

A Cyber Security Cooperative Research Centre (CSCRC) szervezet nemrég közzétett jelentése szerint a számítógépes bűnözés 1 billió dollárba került a világgazdaság számára. **A kutatás kitér Ausztráliára is, amely például a JBS húsipari konszern elleni támadás során 47 ausztráliai létesítményt is érintett,** de emellett sok már jelentős eset is történt, például 2020. tavaszán a Toll Holdings logisztikai társaság ellen, illetve idén márciusban a média területén tevékenykedő Nine Entertainment ellen.

De **a friss, világszerte több mint 1500 Kaseya-szolgáltatást igénybe vevő vállalatot érintő incidensben is legalább öt ausztrál informatikai szolgáltató céget** találunk.

A Crowdstrike egy tavalyi felmérésben 200 ausztrál vezető IT-döntéshozót és biztonsági szakembert kérdezett meg a

helyi legfontosabb ipari szektorokban. A válaszokból az derült ki, hogy **a megkérdezett ausztrál szervezetek kétharmada szenvedett már el ransomware támadást az előző 12 hónapos időszakban.**

A megtámadott szervezetek egyharmada kifizette a váltságdíjat, amely átlagosan 1.25 millió dollár volt - derült ki mindez a felmérésből. Vagyis **csak az itt megkérdezett cégek összesen legalább 55 millió dollár váltságdíjat fizettek a bűnözőknek**. A biztonsági cég szerint a fizetés egyértelmű bátorítás a bűnözők felé, amely csak ront a helyzeten, és gyarapítja a hasonló incidenseket.

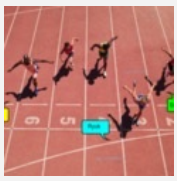
Ha van egyáltalán tanulság, akkor az, hogy még mindig sok a felkészületlen vállalat, vállalkozás. A zsaroló vírus bejutását leggyakrabban nem NASA-t feltörő profi hackerek, hanem automata szkripteket futtató bűnözői csoportok okozzák. Ahol nem az a kérdés, hogy én vagyok-e Boris Johnson, vagy Joe Biden, hanem nyitva az RDP port vagy sem, le lettek futtatva a megjelent hibajavítások vagy sem, rákattintanak-e a munkavállalók a gyanús e-mailekre, linkekre vagy sem.

És persze az incidensek kötelező bejelentése is hasznos lépés lenne, mert a fű alatt milliárdok úsznak el, és adatok tömkelege kerül illetéktelen kezekbe. Mert nem lehet mindenre mentség, hogy akkor jönne a leállás, termelés kiesés. A helyzet mindenesetre roppant nehéz, de mégis csak kellene vele valamit kezdeni.

Szólj hozzá!
Címkék: statisztika ausztrália tapasztalatok váltságdíj ransomware zsarolóvírus

Ajánlott bejegyzések:

Ransomware helyzetjelentés


Világrekord, aminek mégsem örül senki

A Cerber visszatér


Váltságdíjat kínálnak a váltságdíjszedő bandáért

Kik, hol és mire költik a beszedett váltságdíjainkat?

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

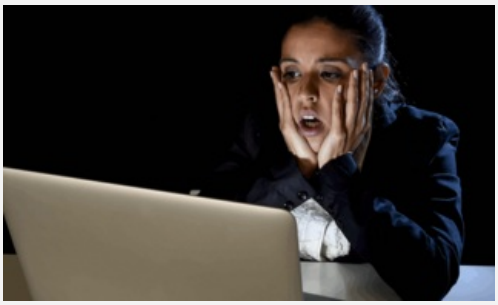
Mai szavunk pedig: megszemélyesítéses csalás

2021. július 22. 09:03 - Csizmazia Darab István [Rambo]

Valószínűleg mindenki hallott már arról social engineering technikáról, melynek célja, hogy megtévesztéssel az embereket rávegye, hogy érzékeny információkat áruljanak el magukról. Az ESET kiberbiztonsági vállalat most **a kiberbűnözők egy másik kevésbé ismert, de mostanában egyre gyakoribb támadási technikájára, a megszemélyesítésre hívja fel a figyelmet.**

A módszer során **a támadók egy megbízható személynek (például kollégának, üzleti partnernek) adják ki magukat annak érdekében, hogy becsapják az áldozatokat, és olyan tevékenységekre vegyék rá őket, amelyek aztán bajba sodorhatják őket vagy munkáltatójukat.**

Jellemző példa, hogy a támadó a kiszemelt cég v**ezérigazgatójának adja ki magát (annak távollétében), és a nevében azonnali csaló tranzakciókat és megrendeléseket** hagy jóvá.



Hogyan ismerhetjük fel, ha egy kollégánk nevében valójában egy kiberbűnöző veszi fel velünk a kapcsolatot? Megszemélyesítésről akkor beszélünk, ha egy bűnöző valaki másnak adja ki magát - ebben az esetben annak érdekében, hogy információt szerezzen vagy hozzáférhessen egy személyhez, céghez vagy bizalmas számítógépes rendszerhez.

Céljuk elérése érdekében **a kiberbűnözők többek között telefonhívásokon, e-maileken vagy üzenetküldő alkalmazásokon keresztül lépnek kapcsolatba áldozataikkal.** Sok esetben a támadók a kiszemelt vállalat felső vezetőinek nevével állítanak be e-mail címet, így olyan levelet tudnak küldeni, mely teljesen úgy néz ki, mintha azt valóban az adott vezető írta volna.

Szinte hihetetlen, hogy manapság mennyi vállalati információ érhető el publikusan az olyan platformokon, mint a LinkedIn. A vállalatok teljes felépítése és az alkalmazottak névsora egyaránt könnyedén összegyűjthető róla. **A kiberbűnözők az így megszerzett információkat felhasználhatják arra, hogy az egyik kolléga nevében valamilyen ürüggyel megkérjék a vállalat egy másik alkalmazottját arra, hogy bizalmasan indítson el egy átutalást, fizessen ki egy számlát vagy küldjön el pár fontos adatot, és erről ne szóljon egyelőre senkinek.**

Egy ilyen célzott és testre szabott támadás rendkívül veszélyes lehet a vállalatok számára, mivel adatlopásokat és pénzügyi veszteséget is okozhat.

A TEISS adatai szerint a megszemélyesítéssel kapcsolatos online támadások világszerte elterjedtek és **cégmérettől függetlenül bármekkora vállalkozásra fenyegetést jelenthetnek. Az esetek száma 2019-ben csaknem 70%-kal emelkedett az előző évhez képest.** A biztonsági megoldások megvédenek a technikai támadásoktól, de a megszemélyesítés módszerei **inkább az emberi megtévesztésre, pszichológiai módszerekre támaszkodnak, és az emberek túlzott bizalmát használják ki.**

Ezért kiemelten fontos a munkavállalók ilyen irányú **biztonságtudatossági képzése is**. Íme, néhány hasznos tanács az ESET kiberbiztonsági szakértőitől, melyek segítségével csökkenthetjük az ilyen pszichológiai megtévesztések kockázatát, és kiszűrhetjük a rosszindulatú próbálkozásokat:

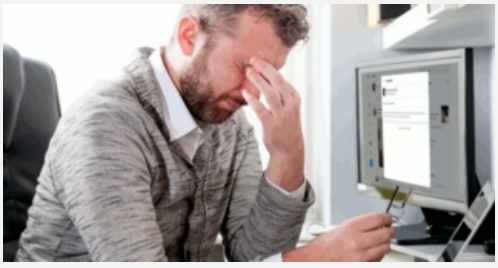

THE WALL STREET JOURNAL.

Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies

1. Tanuljuk meg felismerni a megszemélyesítés technikáját használó hamis üzeneteket
Ne feledjük, a tudatosság kulcsfontosságú! Minél többet tudunk a megszemélyesítés eszközeiről, annál könnyebben felismerhetjük azokat. Nézzük meg, hogyan működnek a megszemélyesítő e-mailek! Sok bűnöző a sürgősség és a félelem érzését próbálja kiváltani célpontjában, ami arra készteti az áldozatot, hogy gondolkodás nélkül kapkodva elvégezze a kért feladatot. A bűnözők kívánsága sokszor tartalmaz valami szokatlant és gyanúsat. Hivatkozhatnak például olyan szerződésekre vagy tranzakciókra, amelyekről még nem is hallottunk, vagy olyan ügyfelekre, akiket nem ismerünk. **A kiberbűnözők általában nagyon rövid határidőt adnak a szükséges feladat elvégzésére és arra kérnek, kezeljük bizalmasan az adott utasítást.** Az üzenetek gyakran tartalmaznak nyelvtani hibákat és sokszor hibásan alkalmazzák a vállalat arculatát is. A megszemélyesítésekben igazán jártas támadók azonban nagyon valóságosnak tűnő e-maileket is készíthetnek, amelyek végén szerepel a levelet küldő alkalmazott hivatalos fényképe vagy aláírása is. Tehát ha az üzenetben szereplő kérést furcsának találjuk, akkor legyünk gyanakvóak, még akkor is, ha az e-mail sablon valódinak tűnik, és teljesítés előtt tájékozódjunk már csatornákon, vagy kérjük egy másik felső vezető jóváhagyását.

2019. tavaszán például egy meg nem nevezett angol energetikai cég vezérigazgatója 220 ezer eurót utalt át egy ismeretlen magyar beszállító számlájára, ahol a megtévesztésben a vállalat németországi vezetőjének hangját utánozták le sikerrel. A hanghamisításban a főnök azonnali átutalást rendelt el, és a hangját a csalók annyira jól utánozták le, hogy az akcentus, a beszéd szokásos hanglejtése, sebessége is tökéletes volt. A mintegy 72 millió forintnak megfelelő összeget az ismeretlen elkövetők a magyar számláról azonnal továbbutalták egy mexikói számlaszámra.



2. Gondoljuk át az összefüggéseket!
Néha túl elfoglaltak vagyunk és szinte gondolkodás nélkül hozunk döntéseket. **Ám inkább szánjunk rá néhány extra másodpercet, és mérlegeljük, hogy az adott üzenet nem furcsa-e! Miért éppen ez a kolléga kéri az összeg**

átutalását vagy épp ezeket az érzékeny adatokat? Minden olyan szokatlan dolgot, amely eltér a vállalat hagyományos üzleti folyamataitól, tekintsünk figyelmeztető jelnek! Még akkor is lehetünk csalás áldozatai, ha az e-mail egy olyan nyilvánvalóan megbízható egyéntől származik, mint a vezérigazgatónk. Legyünk éberek, és ellenőrizzük az esetleges kéréseket más kollégákkal is.

Előfordulhat, hogy az internetes bűnözők azt is tudják, hogy valaki épp szabadságon van, és úgy viselkednek, mintha helyettesítenék őt. Ilyen esetben ellenőriztessük a kérdéses információkat a felettesünkkel vagy munkatársainkkal.

3. Ellenőrizzük alaposan az e-mail címet
Üzleti e-mailt kaptunk egy személyes fiókból? Még akkor is, ha az e-mail cím látszólag olyan személyhez tartozik, akit ismerünk, inkább az illető hivatalos e-mail címére válaszoljunk.

Ne feledjük, a hackerek olyan e-mail címet is használhatnak, amely első látásra hivatalos vállalati e-mail címnek tűnhet, de a domain neve tartalmaz kisebb eltéréseket. Melyek a leggyakoribb ilyen eltérések az e-mail címekben? Gyakran kicserélnek egy betűt egy rá hasonlítóval; például az „m” helyett „rn”-t használnak, vagy más betűeltéréseket tartalmaz - ezt a módszert hívják „typosquatting”-nak.

4. Ellenőrizzük az illetőt egy másik, alternatív kommunikációs csatornán keresztül is
Gyanítjuk, hogy esetleg csaló üzenetet kaptunk? **Hívjuk fel a feladót, vagy vegyük fel vele a kapcsolatot egy másik kommunikációs csatornán keresztül és kérdezzünk rá az adott üzenetre!** Ne felejtsük el, hogy nem az e-mail az egyetlen kommunikációs csatorna, melyet a hackerek a megszemélyesítéshez használhatnak. Olyan népszerű üzenetkezelő alkalmazásokon keresztül is kapcsolatba léphetnek velünk, mint például a WhatsApp. Tehát ha gyanús WhatsApp üzenetet kapunk, akkor is írjunk a feladó vállalati e-mail címére egy üzenetet, vagy hívjuk fel telefonon.

Alternatív megoldásként természetesen személyesen is megkérdezhetjük az illetőt. **Ne féljünk attól, hogy valakit megzavarunk a munkában, még akkor sem, ha épp nagyon elfoglalt. Ha szemtől szembe mindig nem is léphetünk kapcsolatba a vezetőnkkel, beszélhetünk a helyettesével vagy másokkal, akik várhatóan tájékozottak lesznek az adott üggyel kapcsolatban.** Például egy nagy összegű, sürgős határidejű számlafizetésről biztosan tud a pénzügyi igazgató vagy az ügyvezető igazgató is, így nyugodtan rákérdezhetünk náluk is.

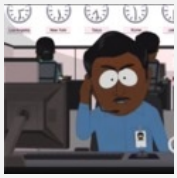
5. Hozzunk létre „Külső” címkét
A „Külső” címkék segítségével megjelölhetjük azokat az e-maileket, amelyek a vállalati domainen kívülről érkeznek. **Ezek a címkék figyelmeztetik a címzetteket, ha egy adott levél nem a szervezeten belülről származik, és segíthetnek azonosítani azokat az e-maileket, amelyek az adott domaint próbálják meg valamiképp hamisítani (például a fent említett „m” és „rn” esetben).**

A fent említett ajánlások ugyan extra időt igényelnek, de biztosak lehetünk benne, hogy a befektetett időnk bőven megtérül, hiszen lehet, hogy pont ezáltal óvjuk meg munkahelyünket egy célzott kibertámadástól. **A támadók azzal is**

próbálkozhatnak, hogy egy rosszindulatú mellékletre vagy linkre való kattintásra ösztönözzenek minket, ezért ne felejtsünk el egy olyan átfogó biztonsági megoldást találni, amely képes hatékonyan észlelni és blokkolni mind a szervereken, mind pedig a végpontokon ezt a fajta veszélyt is.

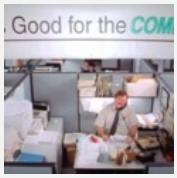
3 komment
Címkék: social csalás átverés veszteség anyagi engineering megszemélyesítés impersonating

Ajánlott bejegyzések:


A support csalók nem pihennek


A bankos mindig kétszer csenget...


Ingyenes Omikron teszt vagy mégsem?



Karácsonyi vásárlás biztonságosabban

Adathalászat a Discordon

Kommentek:

MaxVal BircaMan KözÍró · http://bircahang.org 2021.07.23. 07:54:06

Munkahelyen megadom az adataimat annak, akik azt mondja, a kollégám. Nem az én bajom ez.

Saját adataimat viszont sose adom meg senkinek.

Válasz erre

ebella2 2021.07.23. 10:20:42

@MaxVal BircaMan KözÍró: Ez kicsit zavarosra sikeredett.

Válasz erre

MaxVal BircaMan KözÍró · http://bircahang.org 2021.07.23. 11:21:44

@ebella2:

Zavaros, de igaz.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

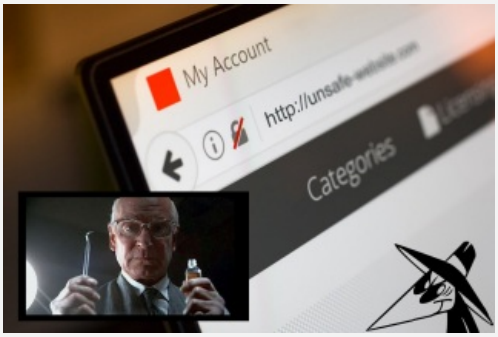
accountz

Belépés
Regisztráció

Biztonságos? Biztonságos?

2021. július 27. 11:11 - Csizmazia Darab István [Rambo]

A fenti kérdés sokaknak lehet ismerős valahonnan. Naponta valószínűleg több tíz, de akár több száz webhelyet is felkeresünk. **Honnan vehetjük észre, hogy az általunk látogatott oldalak "biztonságosak-e", nem pedig az adatainkra vadászó webhelyek?** Az ESET szakértői összegyűjtötték, mire érdemes figyelni, hogy könnyen felismerjük a különbséget a biztonságos és a csaló weboldalak között.



Homoglifa, avagy elgépelt URL-ek és kétértelmű karakterek
A homográf típusú támadások a kiberbűnözők leggyakoribb megtévesztő taktikái közé tartoznak. Ennek lényege, hogy **a hamis weboldalakat olyan domain neveken regisztrálják, amelyek nagyon hasonlítanak ismert, megbízható oldalakéhoz, ezek pedig kinézetre összetéveszthető karaktereket tartalmaznak.** Ilyen például az, ha a „microsoft.com” helyett „rnicrosoft.com”-ot használnak, ahol az „m” betűt „rn” karakterekkel helyettesítik.

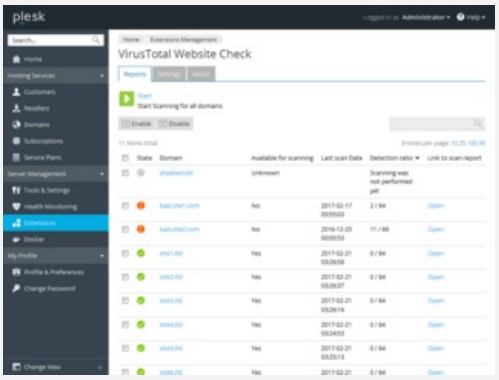
Előfordulhat az is, hogy **az „o” betű helyett a görög eredetű omicront, azaz „o”-t használják** a domain névben: itt például a „facebook.com” címben a második „o” helyére az omicron lépett, ám kinézetre szinte nincs is különbség.

"Typosquatting", vagyis a szándékos elírással történő megtévesztés
Ahol is a támadók népszerű weboldalak neveihez nagyon hasonló domain neveket regisztrálnak, például **„google.com” helyett "gogle.com" vagy "goooogle.com" címeket**. Érdemes megemlíteni, hogy **a példában szereplő, tévesen írt változatokat a Google biztonsági okokból megvásárolta, így ezek szerencsére automatikusan átirányítanak az eredeti oldalra, azonban még így is sokféle hamis változat bukkanhat fel.**

A hamis oldalak általában megtévesztésig hasonlítanak az eredetire, ezért legyünk nagyon óvatosak, és mindig ellenőrizzük, hogy tényleg a helyes oldalon járunk-e. Szerencsére **több olyan biztonsági programot is találunk, amelyek felismerik a homográf támadásokat, és figyelmeztetnek,** ha egy gyanús weboldalt próbálunk meg elérni.

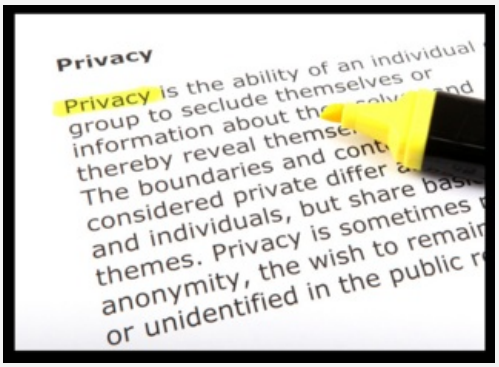
Rosszindulatú webhelyek ellenőrzése
Ma már számos megoldást találunk arra, hogy egy weboldal hitelességét ellenőrizni tudjuk. A Google Biztonságos Böngészés felületén lehetőségünk van az adott **weboldal URL címének beillesztésével ellenőrizni, hogy a keresett webhely biztonságos-e.**

Egy másik hasonló felület a VirusTotal URL ellenőrzője, amely elemzi a webhely címét, és összeveti több tucat felsőkategóriás víruskeresővel, illetve webhely-szkennelő eszközzel, így **igen pontos adatokat tud adni nekünk arról, ha esetleg mégis rosszindulatú felülettel van dolgunk.**



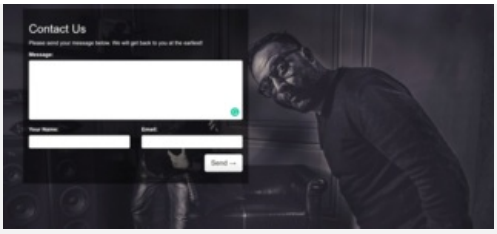
Hiányzó adatvédelmi szabályzat - árulkodó jel lehet
Ha bizonytalanok vagyunk egy oldal hitelességét illetően, mindig ellenőrizzük, hogy a felületen található-e adatvédelmi szabályzat. Az adatvédelmi törvények értelmében ugyanis **minden weboldalnak rendelkeznie kell(ene) olyan szabályzattal, amelyben elmagyarázzák, hogyan védik és kezelik a felhasználók személyes adatait.**

Ha egyáltalán nem találunk erre vonatkozó információkat a honlapon, úgy joggal kérdőjelezhetjük meg az adott weboldal megbízhatóságát.



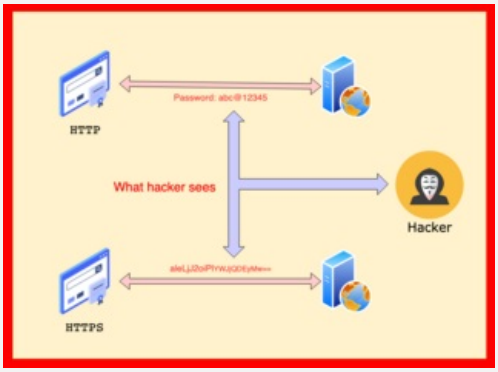
Elérhetőségek - erre is szükség lehet
Minden törvényes vállalatnak, amely kapcsolatot szeretne fenntartani az ügyfelekkel, el kell helyeznie az elérhetőségeit a weboldalán. Ez lehet egy kapcsolatfelvételi űrlap, telefonszám vagy közvetlen e-mail cím.

Ha viszont nem találunk semmit, az már önmagában is gyanús, ahogyan az is, ha a megadott telefonszám huzamosabb ideig nem kapcsolható, vagy olyan személy veszi azt fel, aki egyáltalán nem tűnik illetékesnek. Ilyen esetekben érdemes elgondolkodnunk azon, hogy itt esetleg csalással van dolgunk.



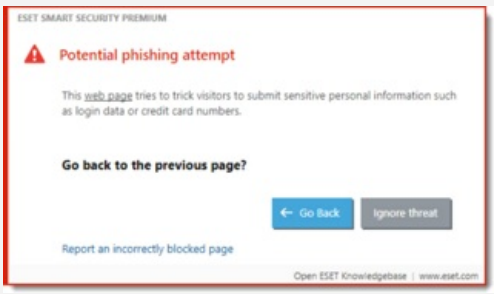
"S" mind Sándor a HTTPS-ben
Egy széles körben elterjedt módszer a weblapok biztonságának ellenőrzésére a HTTPS protokoll vizsgálata. A HTTPS-t gyakran a biztonság kulcselemeként tartják számon, a valóság azonban ennél árnyaltabb. Valójában **ez a protokoll csak azt biztosítja, hogy a webszerver és a felhasználó böngészője közötti kapcsolat titkosított**, azaz védettséget nyújt a lehallgatástól. Nem ad választ azonban arra a kérdésre, hogy bár a webhelyhez titkosított kapcsolaton keresztül csatlakozunk, valóban egy hivatalos weboldalon vagyunk-e, vagy csak egy hamis, adathalász verzióba botlottunk.

Manapság a számítógépes bűnözők ugyanolyan könnyen szerezhetnek érvényes SSL/TLS tanúsítványt a hamis webhelyeikhez, mint egy törvényes vállalkozás. Ezért ezt a módszert érdemes úgy kezelni, mint egy kirakós darabkáját, amely csupán egy nagyobb puzzle része. Ami a tanúsítványokat illeti, érdemes egy pillantást vetni arra is, hogy milyen szolgáltatásokat kínál a weboldal, és melyik szervezet adta ki az SSL vagy TLS tanúsítványát. **Ha a webhely által kezelt adatok érzékenyek, de a kiadott tanúsítvány olcsó vagy ingyenes, akkor érdemes behúzni a vészféket**. A tanúsítvány érvényességéről, és a kiállító szervezetről bővebb információt a böngésző címsorában található lakat ikonra kattintva kaphatunk.



Megbízható biztonsági szoftverek
Egy naprakész, megbízható biztonsági program használatával további nagy lépést tehetünk a kiberfenyegetésekkel szemben. **A biztonsági szoftverek általában beépített szkennelési technikával elemzik a weboldalakat, és rosszindulatú tartalmakat keresnek. Ha ilyet észlelnek, nyomban jelzik a veszélyt, majd letiltják a webhelyhez való hozzáférést és a rosszindulatú tartalmak letöltését megóvva ezzel a felhasználót.**

Az élvonalbeli biztonsági megoldások emellett általában **adathalászat elleni védelemmel is rendelkeznek, megakadályozva a jelszavak, banki adatok és más érzékeny információk megszerzésére irányuló kísérleteket.** Amikor megpróbálunk hozzáférni egy adott URL-címhez, a biztonsági szoftver összehasonlítja azt az adathalász webhelyek adatbázisával, egyezés esetén pedig azonnal megszünteti a hozzáférést, és figyelmezteti a felhasználót a veszélyre. **A most felsorolt biztonsági tippek betartása mellett érdemes óvakodni még a gyanús hirdetésektől, valamint a helyesírási hibáktól hemzsegő weboldalaktól is.**



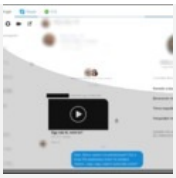
Összegezve tehát az online biztonságunk megőrzése érdekében legyünk mindig nagyon körültekintőek, hiszen a kiberbűnözők **egyre fejlettebb technikákat vetnek be a megtévesztésünk érdekében.**

Szólj hozzá!
Címkék: weboldal biztonság url ellenőrzés böngészés phishing kártékony adathalászat

Ajánlott bejegyzések:

[Hol jársz, hová mész?]

[A bankos mindig kétszer csenget...]



[Facebook egyperces]

[Ingyenes Omikron teszt vagy mégsem?]

[Adathalászat a Discordon]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

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

2021. július 30. 13:20 - Csizmazia Darab István [Rambo]

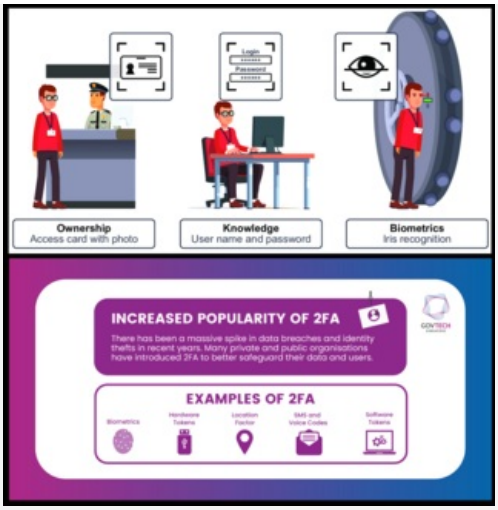
Ha a mai napon megnézzük a haveibeenpwned.com weboldalt, azt láthatjuk, hogy 11,420,802,014 azaz 11.4 milliárd kiszivárgott, ellopott jelszónál tartunk. Ennek részben az is az oka, hogy jelszóválasztásban a helyzet változatlan, azaz egyforma és primitív jelszavakat használnak sajnos még rengetegen. **Pedig lehetne javítani a helyzeten, csak használni kéne a 2FA megoldásokat.**

Foglalkoztunk más sokat ezzel a témával, de most csak két posztot emelünk ki ezek közül, az egyik, amely a hitelesítés rövid történelmi összefoglalója volt, hogyan zajlott ez a dolog fejedelmi gyűrűktől egészen a biometrikus azonosításig. A másik pedig egy olyan összefoglaló volt, mik azok a módszerek, amelyekkel a jelszavak, belépési accountok védelmét nagyban tudjuk erősíteni.

Nincs újdonság a Nap alatt, **ezek a kétfaktoros azonosítás, a személyes USB kulcs, az egyszer használatos OTP (One Time Password), a biometrikus módok és a virtuális token.**

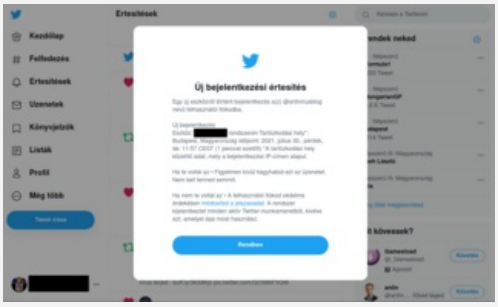
Ezek közül most a 2FA lesz a mai téma, amely többféle módon is megvalósítható. Legegyszerűbb, és legtámadhatóbb fajtája az egyszeri hitelesítő kód szöveges SMS-ben, amely bár vírussal eltéríthető, az eszköz ellopása esetén illetéktelenül felhasználható, illetve SIM kártya cserés támadásnál az eszköz a felhasználó tudta és engedélye nélkül megváltoztatható, de a semminél még így is erősebb védelmet nyújthat. Ennél haladó csoportosabb és biztonságosabb a dedikált biztonsági eszköz, illetve a biometrikus azonosító használata.

A lényeg mindenesetre, hogy amellett amit tudok (név-jelszó páros) szükség van még valamire, amit birtoklok (például USB hitelesítő kulcs), kiegészítve azzal, ami vagyok, azaz a saját testem egyedi jellemző jellegzetes része (írisz, arc, tenyér, véna, ujjlenyomat, hang, fülkagyló, stb.)



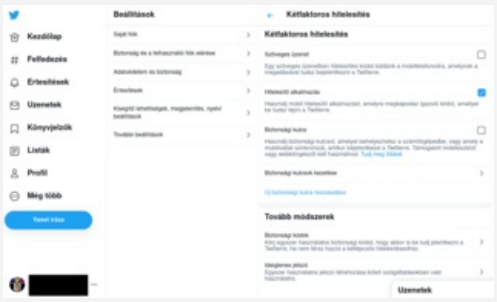
Egy a közelmúltban megjelent átláthatósági jelentésből - amelyet a Twitter készített - **az derült ki, hogy sajnos kéttényezős hitelesítés hiába létezik már évek óta, a felhasználóknak mindössze 2.3 százaléka élt ezzel a lehetőséggel**.

Pedig Twitter fronton nem ismeretlen a fiók feltörés, és az áldozat nevében posztolás, gondoljunk csak Russell Crowe ausztrál színészre, akinek meztelen nőket töltöttek a támadók a lapjára, vagy Sepp Blatter volt FIFA elnök korrupciót látszólag beismerő vallomását hamisították oda, de emellett a Financial Times, a Huffington Post, sőt maga Obama elnök is járt már pórul.



Az üzemeltetők látnak ugyan valamifajta kismértékű növekedést, de áttörést nyilván az hozhatna, ha alapértelmezetten más területekhez hasonlóan kötelezővé tennék vagy ha a felhasználói biztonságtudatosság szintje valamilyen rejtélyes ok folytán váratlanul és rövid időn belül az egekbe szökkenne.

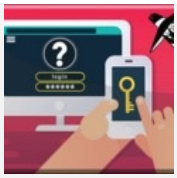
Vélhetően az első változat indulna nagyobb eséllyel a valóság talaján maradva, míg az utóbbira csak elég kedvezőtlen feltételekkel lehetne fogadni a londoni bukméker irodákban.



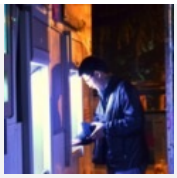
Ha megvizsgáljuk, melyik 2FA módszert használják a leggyakrabban, akkor azt látjuk, hogy a legkevésbé biztonságos szöveges SMS vezeti a rangsort, **de összességében is túl kevesen élnek a kétfaktoros azonosítás lehetőségével, ezért a dolog népszerűsítésével, felhasználóbarátabb megoldásokkal kellene/lehetne még tenni az ügy érdekében.**

Szólj hozzá!
Címkék: biztonság jelszó hitelesítés autentikáció 2fa welivesecurity.com kétfaktor kéttényezős

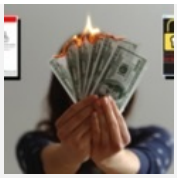
Ajánlott bejegyzések:



[iPhone mint biztonsági kulcs Chrome-hoz]



[Régen minden jobb volt? Hitelesítés történelem dióhéjban]



[Fejemen olvad a vaj, engem nem érhet baj]

[Májusi kétfaktor aranyat ér]

[10 kiberbiztonságra veszélyes szokás]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

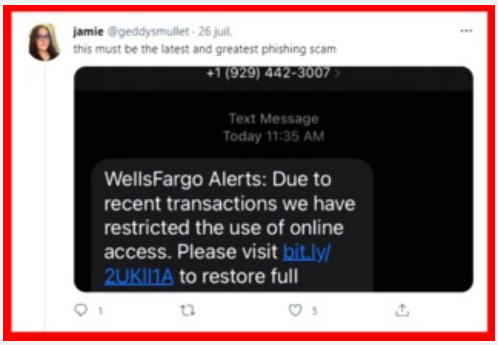
Amazónia veszélyes ragadozói ;-)

2021. augusztus 03. 13:42 - Csizmazia Darab István [Rambo]

Az Amazon webáruház roppant népszerű, na meg a pandémia időszaka is jól felpörgette az online kereskedelmet olyannyira, hogy sokan, akik még kezdetben idegenkedtek ettől a vásárlási formától, ma már szépen belerázódtak, és gyorsnak, kényelmesnek, praktikusnak tartják. Mint minden online vásárlásnál, **az előnyök mellett itt is lehetnek veszélyek, ezekből mutatunk pár mostanában jellemző csalást, átverést, trükköt.**

Az Amazon a világ legnagyobb online piactere, amely 2020-ban 386 milliárd dollár bevételt könyvelhetett el, emellett 200 millió előfizetője van az Amazon Prime szolgáltatására az USA-ban.

A hatalmas ügyfélkör természetesen vonzza a kiberbűnözőket is, akik folyamatosan újabb trükkökkel próbálkoznak bepalizni a gyanútlan áldozatokat.



Mindenki kapott már különféle adathalász leveleket, így az sem lehet meglepő, ha az Amazon nevében érkezik ilyen. Ezek jórészt a fiók hitelesítő adatokat próbálják ellopni, illetve "természetesen" a személyes és banki adataink is érdekesek a támadók számára. **Kaphatunk például olyan levelet látszólag az Amazon ügyfélszolgálatától, miszerint állítólag valaki az imént a nevünkben vásárolt, és a mellékelt linkre kattintva ellenőrizhetjük vagy tilthatjuk le ezt.**

Ezek a hivatkozások aztán átirányíthatnak minket egy hasonmás adathalász oldalra, vagy valamilyen kémprogrammal, illetve egyéb kártevővel fertőzhetik meg a gépünket. Itt **a védekezés az alapos odafigyelés a linkekre, a biztonságtudatos hozzáállás, de persze hasznos az adathalászat ellen is védő antivírus, illetve az ilyen célra használatos böngészőkiegészítők.**

Az említésből nem hiányozhatnak **az úgynevezett ajándékkártya csalások sem, ez is egy régóta űzött átverési forma már**. Itt elképesztően széles a repertoár, e-mail üzenetben, de **az Amazon nevében jelentkezve akár telefonon is megpróbálhatnak rávenni bennünket ilyen ajándékkártyák vásárlására, sürgetéssel vagy büntetéssel való fenyegetéssel állítólagos adategyeztetést kérhetnek, vagy olyan esetek is vannak, amikor egy valamilyen hivatal a kitalált bírság összegét Amazon ajándék kártyával fizetve is elfogadja.**

Ilyen természetesen nincs, ha valódi a büntetés, azt mindig pénzben kell befizessük. Talán ez az a forma, amit leginkább

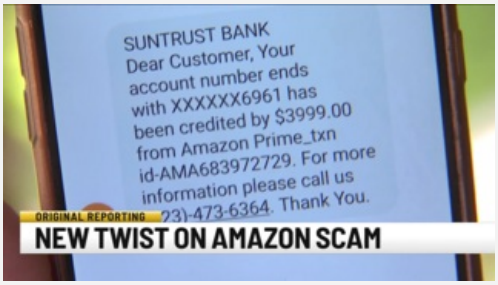
kiszúrnak a felhasználók, és észreveszik, hogy valami nagyon nincs rendben a kamu történetben. Áldozatok persze ennek ellenére sajnos itt is előfordulnak.

Említettük, hogy a banki adatainkra is fenik a fogaikat a csalók, így ez a terület is biztosan támadás elé kerül. **Itt elirányíthatnak bennünket az Amazon saját biztonságos fizetési platformjáról, vagy megpróbálnak minket valamilyen kedvezménnyel rávenni, hogy máshol történjen a fizetés. Ezekre sokszorosan ráfizethetünk, hiszen se a terméket nem kapjuk meg, hivatalon jogorvoslat híján pedig a pénzünket sem tudjuk visszaszerezni. Sőt ha könnyelműen személyes, valamint banki adatokat is megadtunk, akkor később még további bosszúságok, anyagi károk is bekövetkezhetnek.**

Ugyanez vonatkozik az állítólagos nyereményjátékokra is, ahol "csak" az adatainkat kell mindehhez megadni. Az Amazonos vásárlásnál pedig **legyen gyanús a Western Union, MoneyGram és hasonló pénzátutalási kérés.**

Hideg hívásokkal is szembesülhetünk, amikor **véletlenszerűen tárcsázva keresnek meg bennünket telefonon azzal, hogy valamilyen adatvédelmi probléma van a fiókunkkal és azonnali adategyeztetés szüksége, vagy elveszett az állítólagos csomag, most próbál egy csaló vásárolni a nevünkben, és a fiók letiltásához az összes személyes és banki adatunkat, jelszavunkat be "kell" diktálnunk a telefonba.**

Hasonlóan a banki csalásokhoz, helyes, ha az ilyen próbálkozásoknál azonnal gyanút fogunk, megszakítjuk a hívást, és nem esünk bele a támadók csapdájába.



Összefoglalva, Murphy örökbecsű törvényét érdemes segítségül hívni, miszerint: "Bízz embertársadban, de azért emeld meg a kártyapaklit." Óvatosságba, éber odafigyelésbe, biztonságtudatos hozzáállásba még senki nem halt bele, viszont jó eséllyel kerülte el pénztárcájára, személyes adataira veszélyes gyanús szituációkat.

Sose hagyjuk sürgetni magunkat, és minden kéretlen üzenet vagy telefonhívás érkezésekor legyen helyén az eszünk.

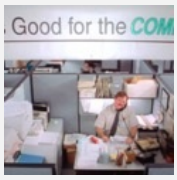
És a végére egy érdekes idézet a megtévesztésről:

"*- Én vagyok, mon generál.*
- Mit kíván?
- Hallottam a hírt, hogy ezen az állomáson önnek is ellopták az irattáskáját, altábornagy úr.
- Megtévesztettek...
- Egy kitűnő tiszt azt mondotta bírói székéből: hogy egy katona nem tévedhet!
- Ezt én mondtam - felelte sápadtan, de keményen az altábornagy.
- Elveszítettem a menyasszonyomat, az ön leányát, és elveszítettem a tiszti kardbojtomat... Ezért a mondatért.
- Magamat sem fogom felmenteni!
A rongyos, portól szürke közlegény egy lépést tett beljebb:
- Ha velem is altábornagy koromban történik a hiba, talán kisebb katasztrófa lett volna a nyugdíjazásom.
- Miért jött ide?
- A távíró szétvitte a hírt mindenfelé... A város környékén táboroztam és idesiettem, hogy a szemébe nézzek altábornagy úrnak. Hogy a legalázatosabban megkérdezzem: hogy történhetett ez?
- Engem... megtévesztett egy ember kapitányi ruhában és megtévesztett az, hogy a csendőr őrmesterrel beszélget... Ez annyira valószínűvé tette...
- Excellenciás uram! Ha a katona fakoronákat lát a távolban, gondoljon arra, hogy egy ütegállás is lehet ott, elmaszkírozva.
Az altábornagy mozdulatlanul hallgatta a saját szavait!"

(Rejtő Jenő: Járőr a Szaharában)

Szólj hozzá!
Címkék: vásárlás biztonság online amazon csalás tippek átverés fizetés webáruház óvatosság welivesecurity.com

Ajánlott bejegyzések:



Karácsonyi vásárlás biztonságosabban

Celeb vagyok, fizess nekem!

Modern románc, holdfény és tánc

Ha eljön a személyiségtolvaj


A bankos mindig kétszer csenget...

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

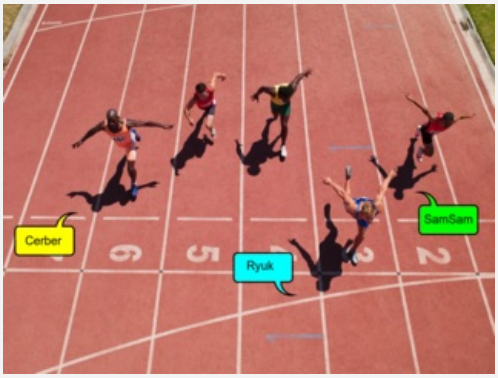
accountz

Belépés
Regisztráció

Világrekord, aminek mégsem örül senki

2021. augusztus 06. 11:07 - Csizmazia Darab István [Rambo]

Rekord mennyiségű zsarolóvírus támadást regisztráltak a 2021-ben, és ezen belül is az év második negyedévében volt a valaha legnagyobb mennyiségű ransomware incidens. Az utóbbi időszakban a ransomware elsődleges fenyegetésnek bizonyult, **a képzeletbeli tabellát a Ryuk vezette, ebből az FBI információ szerint már 100 különböző vírustörzs kering világszerte.**



Az idézett friss felmérésből kiderült még az is, hogy az internetes szervezett bűnözés e területén a dobogós helyeket az élen álló Ryuk mellett **a második helyezett Cerber, valamint a harmadik pozíciót elfoglaló SamSam birtokolja. Az említett statisztika adatai szerint a ransomware mennyisége az első negyedévi 115.8 milliós számhoz képest a második negyedévre már 188.9 millióra** ugrott.

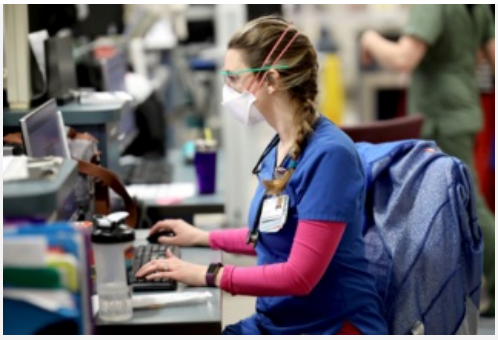
Az országok szerinti fertőzöttség az USA-ban a legnagyobb, a második legtöbb fertőzést elszenvedő ország pedig az Egyesült Királyság - itt nyilvánvaló hogy egy adott országbeli áldozatok kedvezőbb anyagi helyzete vonzza a bűnözőket, mert ott érdemesebb váltságdíjat kérni. A kutatók szerint erőteljes emelkedés tapasztalható a kormányzati ügyfeleket megcélzó ransomware kísérletekben, és ezen belül is **a legutóbbi hónapokban az oktatási szektor szenvedett el jelentős károkat.**

Érdekes, vagy inkább szomorú helyzet alakult ki **Olaszországban, ahol a tömeges ransomware fertőzések miatt egyes helyeken - pl. Lazio - leállt a teljes közigazgatási rendszer, beleértve az oltással kapcsolatos ügymenetet is**. Egészségügyi vezetők az olasz közigazgatást megbénító valaha volt legsúlyosabb kibertámadásnak nevezték.

Az ANSA nevű olasz hírügynökség pedig azt közölte, hogy a külföldről érkezett kibertámadás vizsgálatában az FBI és az Europol szakértői is részt vesznek, magát a támadást pedig terrorcselekményként értékelik.

A pandémia időszaka alatt a kórházak és az egészségügyi infrastruktúrák amúgy is a legsebezhetőbb célpontok közé számítottak, és sajnos nem is kerülte el őket a támadás.

Emlékezetes, hogy a tavalyi évben számos incidens történt: például az amerikai ExecuPharm gyógyszeripari óriáscég ellen, megtámadták a csehországi Brno Covid centrumát, de németországi kórházak is áldozatul estek.



És akkor itt értünk el a "mit is lehet tenni?" kérdéshez, amivel kapcsolatban Dél-Korea láthatóan már erőteljes lépésekkel készülődik, felmérve a lehetséges óriási kockázatokat. Az itt meghirdetett gyakorlati lépések jól hangzanak, például **kiterjesztik a kisvállalkozások támogatását, hogy segítsenek nekik elhárítani a ransomware fenyegetéseket.**

Ennek keretében adatmentési, titkosítási és helyreállítási rendszereket kínálnak számukra, hogy megvédhessék belső hálózataikat, bizalmas adataikat, és hogy segítsék rendszereik visszaállítását egy esetleges zsarolóvírus támadás során.

Emellett **ingyenesen biztosítanak ransomware elleni védelmi szoftvereket az orvosi klinikáknak, illetve felülvizsgálják a kritikus infrastruktúra helyzetét.** Erre az Egyesült Államokban nemrég lezajlott Colonial Pipeline elleni zsarolóvírus támadás, és az azt követő országos leállás az üzemanyag ellátásban lehet egy mindenki számára komoly intő példa.

Az biztos, hogy a védekezéshez mindig a megelőzés a létező legjobb stratégia.

Szólj hozzá!
Címkék: statisztika olaszország dél-korea megelőzés védekezés váltságdíj ransomware zsarolóvírus

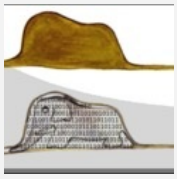
Ajánlott bejegyzések:


Ransomware helyzetjelentés


A ransomware-nek nincs No-go zóna

Tesz-e Oroszország a ransomware ellen?

A Cerber visszatér


Adatokkal jóllakó kígyó

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

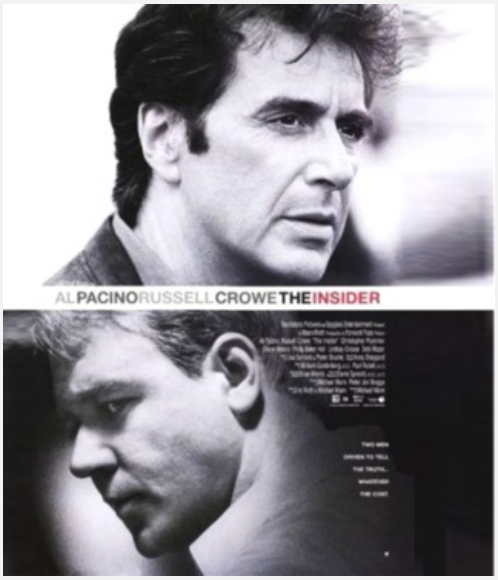
accountz

Belépés
Regisztráció

A bennfentes

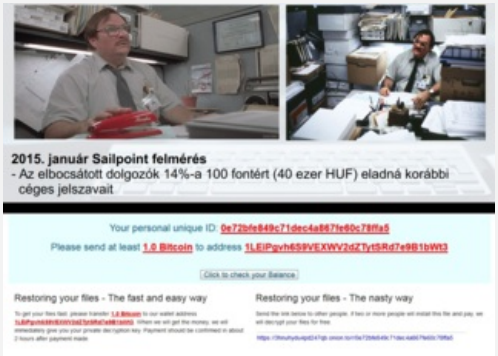
2021. augusztus 10. 08:54 - Csizmazia Darab István [Rambo]

Anno az egyik legjobb mozifilm volt, amelynek szereplői Al Pacino és Russell Crowe voltak, de innen csak a címet kölcsönöztük. **Viszont milyen összefüggés lehet a bennfentesek és a zsarolóvírusok között?** Ezzel foglalkozik a mai poszt.



Ha valaki még emlékszik **a 2015-ös Sailpoint felmérésre, abban arról olvashattunk, hogy az elbocsátott brit munkavállalók 14%-a már 100 fontért (40 ezer HUF) is eladná korábbi céges jelszavait.**

Ez amiatt lehet necces szituáció, mert egy másik, HelpNetSecurity jelentés szerint a korábbi IT munkavállalók 25%-a azóta is régi jelszavával hozzáfér a hálózatához, sőt 16%-nak az összes eddigi korábbi munkahelyéhez van még az élő hozzáférése.



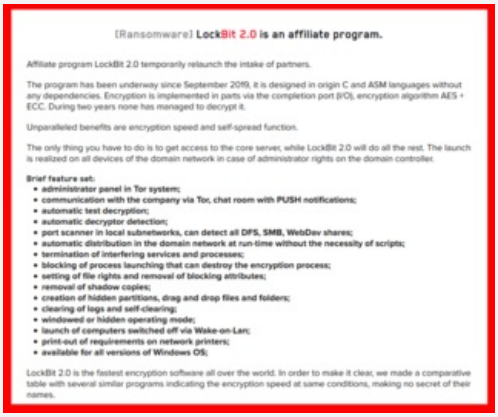
A komolyabb fajsúlyú adatsértések, incidensek rendre gyenge vagy eltulajdonított belépési adatok miatt következnek be, de **emellett még szóba jöhet a belső szál is, amely szintén gyakori.**

Itt a sértett munkavállaló bosszúból vagy a bűnözőktől kapott pénzért ad el bizalmas adatokat, hozzáféréseket, jelszavakat.

Emberi tényező ügyben már korábban is sokszor rezgett ez a bizonyos etikai léc - már ha létezik manapság egyáltalán ilyesmi.

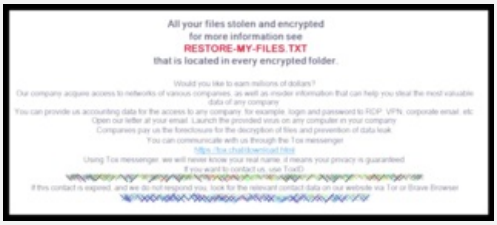
Az egyik ilyen emlékezetes előzmény volt, amelynél a 2016-os Popcorn Time Ransomware nevű kártevő változat, amely egy Bitcoin (akkoriban kb. 770 USD) váltságdíj fizetés ellenében azt az ajánlatot tette, hogy ha az

áldozat sikeresen megfertőzte a zsaroló vírussal két ismerősét, akkor ő ingyen kaphatott helyreállító kulcsot.



Most viszont a Lockbit zsarolóvírust fejlesztő és terjesztő bűnözői csapat, amely 2019. szeptemberében kezdett jelentős RaaS (Ransomware as a Service) tevékenységbe, **a 2021. júniusban debütáló Lockbit 2.0 kártevő kapcsán új gyenge-pontok után kutat, és ez a régi-új gyenge pont jelen esetben (vagy mindig is) a felhasználó maga.**

A kártevőt terjesztő banda a korábbi közvetítői, alvállalkozói hálózati láncot teljesen kihagyva immár közvetlenül sértett munkavállalókat, bennfenteseket toboroz, és jelentős pénzjutalmat ígér azoknak, akik cégük RDP, VPN, levelező szerver, és egyéb belső vállalati rendszereikhez hozzáférést, jelszavakat adnak a bűnözőknek. A toborzók a pénz mellé teljes anonimitás ígérnek a besúgónak, aki majd ártatlan arccal nézheti végig, ahogy a céges rendszerük beleáll a földbe.

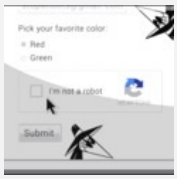


Pedig amúgy sem egyszerű felvenni a harcot a ransomware támadásokkal, egyre több lépés szükséges a hatékony vállalati védelemhez, megelőzéshez, **például rendszeres hibajavító frissítés, napi biztonsági mentés, RDP tiltás, naprakész antivírus, 2FA/MFA használata, megfelelő biztonsági és hálózati beállítások, biztonságos jelszavak, kidolgozott policy, adminisztrátori jogosultságok korlátozása, biztonságtudatosság, érzékeny adatok nyugalmi állapotban történő titkosítása, biztonsági naplózás, rendszeres munkavállalói képzések, hálózatok szegmentálása, stb.**

Sajnos úgy tűnik, a zsarolóvírusok frontján - lásd Colonial Pipeline, JBS, Kaseya - egyre több incidensre számíthatunk, "a nemzetközi helyzet fokozódik".

Szólj hozzá!
Címkék: céges belső munkavállalók vállalati sértett belsős ransomware bennfentes zsarolóvírus lockbit

Ajánlott bejegyzések:


Mai szavunk pedig: reCAPTCHA


Te nem kapod vissza, de mindenki más igen

"Illetéktelen fél korlátozott ideig hozzáférhetett fájlokhoz"

5 ok, amiért a ransomware még sokáig velünk maradhat

Miért nem másolja egyszerűen vissza őket?

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

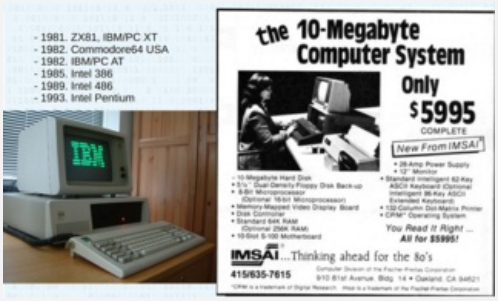
accountz

Belépés
Regisztráció

Péntek 13 egykor és ma

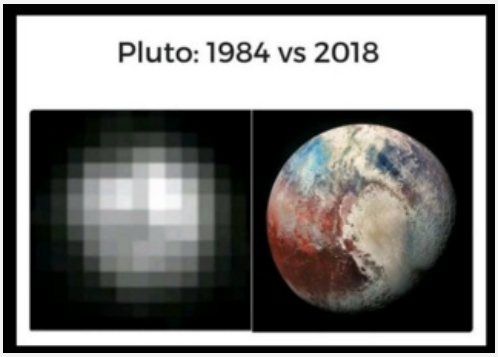
2021. augusztus 13. 10:17 - Csizmazia Darab István [Rambo]

Egy kerek évforduló okán - 40 éve jelent meg az első IBM PC személyi számítógép - **érdemes egy picit visszafelé tekinteni, honnan indultunk. Annyira hihetetlen események követték ki az eddigi utat, hogy szinte fakenews érzése lehet az embernek.**



Akármilyen hihetetlen, az első néhány évben úgy lehetett PC-t használni, hogy az ég kék, a fű zöld volt, madarak csiripeltek, és semmilyen vírus nem fenyegette a gépünket. A széles körű áttörés, amelynek aztán a mai napig isszuk a levét 1986-ban volt, amikor sajnos a Brain személyében megjelent az első IBM PC kompatibilis, szabadon terjedő vírus.

Aki bővebben is kíváncsi erre a fejlődési időszakra, vagy csak nosztalgiázni akar, annak ezt Az IKT fejlődésének nem várt árnyoldalai című összefoglalót ajánljuk, már ami a technikai fejlődést illeti. A vírustörténelemről, a kártékony kódok evolúciójáról pedig a Kódok Harca előadás beszél elég részletesen.



Na de mi is ez a cím, **puszta babonaság-e szerencsétlennek tartani ezt a gyanúsan hangzó dátumot? (spoiler alert: igen, az).** Ám nem mindig volt így, ahogy ezt azok a szakemberek, akik már a 80-as, 90-es időszakban is számítógépes munkát végeztek saját bőrükön is megtapasztalhatták. Írtunk erről korábban már a blogban is.

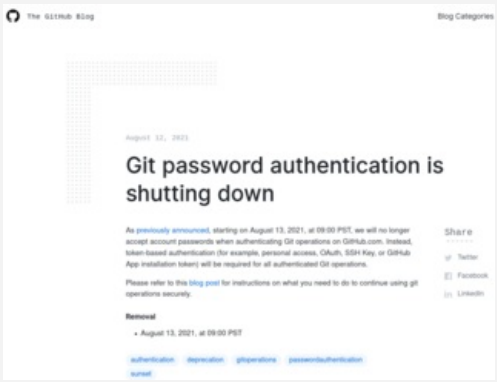
Elképesztő módon **egyedi nevezetes dátumokhoz is készültek vírusok, amik aztán az adott napon állományokat tudtak megfertőzni és jóvátehetetlenül felülírni**.

Akkoriban még **volt olyan vélekedés is, miszerint ha péntek éppen 13-ra esik, akkor emiatt senki ne kapcsolja be a számítógépét. Ami persze már akkor is tarthatatlan volt például a közműszolgáltatók, repterek, tőzsdék, kórházak, bankok, hadsereg, adóhatóság részéről.**

De persze igen hamar jöttek a kijózanító 14 szombat és egyéb kártevővariánsok, tehát mindenki belátta, igazi hatékony megoldásra volt szükség vírusvédelem formájában.

És hogy stílszerűen emlékezzünk újra a 13-a péntekre, amikor a fekete macska valójában azért kel át az úttesten, mert odaát van dolga, **a GitHub kihasználta ezt az évfordulót, és erre időzítve jelentett be változást.**

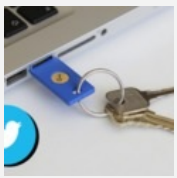
A platformon mától már nem elégséges a kevésbé biztonságos sima jelszavas hitelesítés, hanem a felhasználóknak mostantól hitelesítési tokeneket (OAuth, SSH kulcs vagy GitHub App) kell használniuk a GitHub műveletek jóváhagyásához.

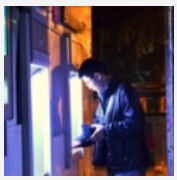


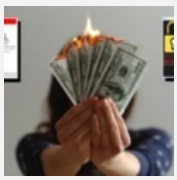
Na ugye, hogy történhetnek jó dolgok is az ilyen megtépázott emlékű napokon?

Szólj hozzá!
Címkék: vírus ibm péntek 13 hitelesítés token github

Ajánlott bejegyzések:


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


Régen minden jobb volt? Hitelesítés történelem dióhéjban


Fejemen olvad a vaj, engem nem érhet baj


Üdvözlünk Sin City-ben

Vakcinás csalások, szevasztok

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Kiberkockázatok - miért nehéz velük lépést tartani?

2021. augusztus 17. 08:43 - Csizmazia Darab István [Rambo]

Vajon miért olyan nehéz sok cég, vállalat, szervezet számára védekezni, lépést tartani az egyre fejlődő vírusokkal és hatékonyan kezelni a kiberkockázatokat? Mondunk rá 5 okot...

A pénzügyi szolgáltató vállalatok hosszú ideje a kiberbűnözők népszerű célpontjai. **Ezek a pénz mellett rengeteg bizalmas ügyféladatot is kezelnek, amelyeket a bűnözők különféle átverésekhez** tudnak felhasználni, vagy épp eladják azokat az internet fekete piacain.

A Verizon 2020-as adatsértési jelentéséből kiderül, hogy **a pénzügyi ágazatot csak az elmúlt évben több mint 1500 incidens érte, köztük 448 megerősített adatlopással.**

A régóta velünk lévő kiberfenyegetések mellett a legtöbb vállalatnak még a távoli munkavégzésre való gyors átállással is meg kellett küzdenie. A váltás rendkívül rövid időn belül ment végbe, így a cégeknek kevés ideje maradt a megfelelő kiberbiztonsági intézkedések bevezetésére, valamint arra, hogy felkészítsék az alkalmazottakat a rájuk leselkedő fenyegetésekre.

Bár a járványhelyzet azóta javult, a távmunka velünk marad - és felkerült azon kihívások listájára, melyekkel a vállalatoknak számolniuk kell, amikor kidolgozzák a kiberbiztonsági terveiket és irányelveiket. Az ESET kiberbiztonsági szakemberei összegyűjtöttek öt jellemző nehézséget, ami miatt a vállalatok folyamatosan küszködnek a megfelelő kiberbiztonsági körülmények kialakításával.

1. Szakemberhiány
Sok vállalat vadászik akár tapasztalt, akár feltörekvő kiberbiztonsági szakemberekre, hogy segítsenek nekik a különböző fenyegetések elleni védelem kialakításában, ám egyszerűen **nincs elegendő jelölt.** Bár a kiberbiztonsági munkaerőhiány évek óta először mutat csökkenő tendenciát, globális szinten még mindig 3.12 millióval kevesebb szakember van a szükségesnél.

A globális szakemberhiány pótlásához az Egyesült Államokban 41 százalékkal, **világszerte pedig 89% kellene növekednie a foglalkoztatásnak.** Tehát a legjobb és legtehetségesebb kiberbiztonsági szakemberek megszerzéséhez a vállalatoknak versenyképes fizetéseket és inspiráló munkalehetőségeket kell kínálniuk.

2. Elégtelen költségvetés
Szintén kiemelt probléma, hogy a kiberfenyegetések leküzdéséhez nem elegendő a vállalatok kiberbiztonságra elkülönített költségvetése. Az Ernst and Young tanácsadó cég által végzett felmérésben a megkérdezett szervezetek **87%-a válaszolta azt, hogy nincs elegendő büdzséjük a kiberbiztonság és ellenálló képesség vágyott szintjének eléréséhez.**

Az erőforrások hiánya miatt a vállalatok nem tudnak elegendő kiberbiztonsági szakembert alkalmazni vagy olyan technikai intézkedéseket bevezetni, amelyek ellenállóvá tennék őket a különböző kiberfenyegetésekkel szemben.

3. A saját kiberbiztonság túlbecsülése
A vállalatok egyik gyakori hibája a saját kiberbiztonsági intézkedéseik túlértékelése. Bár azt gondolhatják, hogy mindenre fel vannak készülve, egyáltalán nem biztos, hogy a legjobb biztonsági rés kezelési irányelveket alkalmazzák. **Erre jó - ugyanakkor sajnálatos - példa a BlueKeep biztonsági rése a Windowsban.**

A Microsoft mindenkit felszólított a 2019 májusában kiadott javítás letöltésére, majd egy hónappal később a Nemzetbiztonsági Ügynökség is kiadta saját figyelmeztetését - azonban júliusban még mindig több mint 805 ezer gép volt kiszolgáltatva annak a biztonsági hibának, ami a novemberi első BlueKeep-támadásokhoz vezetett. Egy ilyen **súlyos sebezhetőség javításának semmilyen körülmények között sem szabadna hat hónapon át** húzódnia.

4. Tájékoztató tréningek hiánya
Egy másik gyakori ok, amely aláássa a vállalat kiberbiztonságát, ha az alkalmazottak nem részesülnek megfelelő kiberbiztonsági képzésben. A koronavírus okozta távmunkára való áttéréssel **csak tovább nőtt annak kockázata, hogy az alkalmazottak egy átverés miatt rosszindulatú programokat töltenek le vagy kiadják a vállalati hitelesítő adataikat.**

A Ponemon Intézet tanulmánya szerint bár megugrott a vállalatok által észlelt kibertámadások (ideértve az adathalász és az emberi megtévesztésre építő social engineering támadásokat is) száma a járvány ideje alatt, **a válaszadók 24 százalékuk érezte úgy, hogy szervezeteik nem biztosítottak számukra megfelelő tréninget a távmunkával kapcsolatos kockázatokról.** Aggasztó adat, hogy a tanulmány szerint a vállalatok több mint fele nem rendelkezik a távoli munkát végzőkre vonatkozó biztonsági szabályzattal.

5. A kiberbiztonság fontosságának alulértékelése
Egyes szervezetek alábecsülik a kiberbiztonság értékét, ehelyett más, általuk érdemesebbnek tartott területekbe fektetnek, például a terjeszkedés finanszírozásába vagy új termékek fejlesztésébe. Amellett érvelnek, hogy a költségek meghaladják az előnyöket, például **a kiberbiztonsági intézkedések anyagi vonzata felülmúlja az adatsértésből eredő esetleges veszteségeket.**

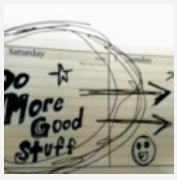
Bár a lehetséges pénzbüntetések és pénzveszteségek rövidtávon alacsonyabbak lehetnek, a vállalat hírnevének csorbulása hosszútávon nagyobb kieséshez vezethet, ideértve az ügyfelek bizalmának elvesztését is, ami a bevételi forrásokat is sújtja. **Ráadásul egy támadás során a kiberbűnözők akár szellemi tulajdonhoz is hozzáférhetnek, amelyet aztán a dark weben árusíthatnak az ügyféladatokkal együtt.** Éppen ezért a kiberbiztonság fontosságát nem szabad alulértékelni, mivel az mind a vállalat, mind az ügyfelek védelmét szolgálja.

Kibertámadás esetén a fent említett tényezők bármely kombinációja jelentős kárt okozhat egy szervezet működésében. Jó hír, hogy a pénzügyi szolgáltató vállalatok vezetői elkezdték komolyan venni a kiberbiztonsági aggályokat. A McKinsey globális menedzsment tanácsadó cég által megkérdezett igazgatói bizottságok 95%-a azt állítja, **hogy évente legalább négyszer megvitatják a kiber- és a technológiai kockázatokat.**

Az ESET szakértői ehhez hozzáteszik, hogy **a felsővezetés tudatosságának növelésével párhuzamosan megfelelő összegeket kell fektetni a kiberbiztonsági megoldások használatába, valamint a dolgozók színvonalas képzésébe is.**

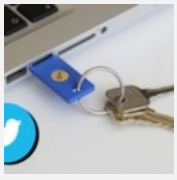
Szólj hozzá!
Címkék: biztonság kockázat vállalati kiberbiztonság ESET welivesecurity.com

Ajánlott bejegyzések:

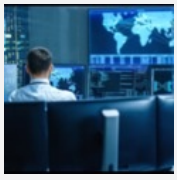


10 kiberbiztonságra veszélyes szokás


Amazónia veszélyes ragadozói ;-)


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


Kémek krémje


Kormányzatok célkeresztben

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

100 millió helyett "csak" 40 lett, maradhat?

2021. augusztus 19. 08:49 - Csizmazia Darab István [Rambo]

Újabb nagyszabású adatvédelmi incidens érte a T-Mobile-t. Ha megnézzük az előzményeket, azt láthatjuk, hogy **már korábban is több ízben, például 2019. novemberében, 2018. augusztusában és 2015-ben is jelentettek be hasonló incidenseket.** 2015-ben 15 millió mobilos ügyfél adatai kerültek illetéktelen kezekbe.

A friss eset úgy kezdődött, hogy 15-én vasárnap megjelent egy Motherboard cikk arról, hogy a T-Mobile vizsgálja egy darknetes fórumbejegyzés valóságtartalmát, **miszerint egy ismeretlen hacker 100 millió, az ő szerverükről lopott ügyféladatot bocsátott áruba.**

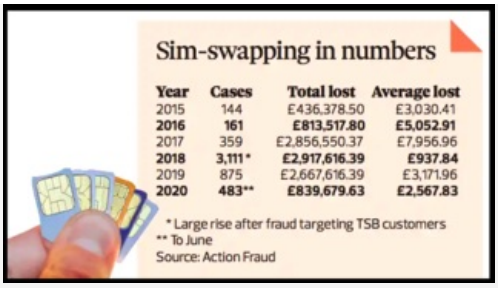
Az eladó 6 Bitcoint, azaz körülbelül 80 millió forintnak megfelelő összeget kér az adatbázisért. Egy nappal később, 16-án a T-Mobile megerősítette, hogy igen, **valóban támadás áldozatai lettek, és illetéktelenek jogosulatlanul hozzáfértek az adataikhoz.**

A T-Mobile az Egyesült Államok egyik legnagyobb szolgáltatója az AT&T és a Verizon mellett, miután felvásárolt a Sprintet. **Ez pedig 4 év alatt már a hatodik adatvédelmi incidensük. Az ellopott adatok közé tartoznak a teljes név, születési dátum, társadalombiztosítási számok, telefonszámok, a lakcímek, az egyedi IMEI-számok és a jogosítványadatok is, ezek pedig részben már meglévő, illetve korábban, valamint megrendelés alatt álló ügyfelek személyes adatai voltak.**

A Vice az adatok egy részének vizsgálata után úgy nyilatkozott, hogy azok pontosak és valódinak tűnnek.

A korábbi állítólagos 100 milliós szám elég durván hangzik, hiszen ez kvázi az USA teljes lakosságának egyharmada lenne. **A 40 millió mindazonáltal így is hatalmas adatmennyiség**. A T-Mobile nem közölt részleteket arról, hogy a támadók hogyan férkőzhettek az adatokhoz, csak annyit írtak, hogy lezárták ezt az illegális hátsóajtós belépési pontot.

Hivatalos közleményük szerint a társaság folyamatosan egyeztet a bűnüldöző szervekkel, miközben folytatják a nyomozást, és kivizsgálják az incidens körülményeit. A vállalat két év ingyenes személyazonosság-védelmi szolgáltatást ajánlott fel az érintett ügyfeleknek, hogy ezzel segítsenek biztosítani kompromittálódott személyes adataik védelmét.



Már a puszta személyes adatok is igen érzékeny információnak számítanak, de ha egy mobil szolgáltató esik áldozatul ilyennek, akkor gyakran még durvább következményei is lehetnek. **Emlékezetes, hogy a T-Mobile 2021. februárjában is elismert egy adatlopást/szivárgás, amire úgy derült fény, hogy az ügyfelek tömegesen szenvedtek el SIM cserés támadásokat.**

Az ilyen fajta támadások alkalmasak arra, hogy az eredeti tulajdonos tudta és engedélye nélkül a támadók SIM kártya cserét kezdeményezzenek a mobilszolgáltatónál **megszemélyesítve a gyanútlan áldozatot. Majd miután már ők kapják a 2 faktoros banki SMS-eket, leürítik az bankszámláját, miközben az eredeti ügyfél telefonja elnémul és lekapcsolódik a hálózatról.**

1 komment
Címkék: személyes t-mobile incidens backdoor adatlopás adatszivárgás hátsóajtó kibertámadás darknet

Ajánlott bejegyzések:

GoDaddy - apák a pácban

Megint jőnek, szivárogtatnak...

Van másik!


Persze hogy tudtam, csak nem sejtettem...


Hogy ne kezeljünk informatikai incidenst?

Kommentek:

Omnilox 2021.08.19. 23:26:43

Idézek a posztban linkelt egyik posztból: "A csalóknak valójában elég három adatunkat ellopniuk és máris képesek eltulajdonítani a személyazonosságunkat - ráadásul sokak esetében ez a három adat a Facebook profilon is megtalálható."

Így nekünk esélyünk sincs. A T-nek nem is érdeke, hogy elővigyázatos legyen, nekik elég bemondani egy-két megszerezhető adatot a személyazonosság igazolásául, elég bemondani a személyi igazolvány számát annak személyes bemutatása helyett, elég egy tanúzott iratról csak egy fényképet belüldeni az irat helyett, és biztosan tudnánk még találni szándékosan meggyengített pontokat a rendszeren. Senki nem szeret az ügyes-bajos dolgai miatt ügyfélszolgálatokra járni, kilincselni, ezért a T azt találta ki - nem csak ők -, hogy az ügyfél kedvében fognak járni, és engednek a biztonságból. Az ügyfelek többsége ezzel teljesen elégedett lesz, akit meg az engedékenység révén vernek át, úgysem tud mit kezdeni, merthogy ők fel tudják mutatni a szentséges ÁSZF-et, annak igazolásául, hogy ők mindenben ártatlanok, mert elfogadtam a lényegében az 'ÚGYIS MEGSZÍVATUNK' szlogennel egyenértékű szerződési feltételeket, hát hogy ne fogadtam volna el, különben telefon nélkül maradok, hiszen a szolgáltatási feltételekben való "kartellezés", összeegyeztetés nem tilos, és minden telefonos cég ugyanazt az 'ÚGYIS MEGSZÍVATUNK' feltételeket kínálja egyetlen opcióként.

Én próbáltam olyat kérni tőlük, hogy jegyezzék fel, hogy a nevemben csak személyesen én intézkedhetek, vállalva a kényelmetlenséget. Ilyenre nincs lehetőség, ennyi volt a válasz.

Egyszer a nevemben vett tőlük valaki egy telefont. Kellett hozzá simlisség az átvevőponton is, de elég volt a szokásos, mindenhol megadandó személyi adatokon kívül az igazolványszámom is. Ennyi kellett ahhoz, hogy több százezres kárt okozhasson valaki a mit sem sejtő ügyfélnek. A T leszarta az egész ügyet, átpasszolta a papírokat egy behajtónak, a pénzüket így ők megkapták, és többé semmilyen együttműködésre, a rendőrségi nyomozásban való együttműködésre nem voltak hajlandóak. Igazi "multi".

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei

Biztonságos bankolás
Deliága Éva gyermekpszichológus
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Fogják a pénzünket és futnak

2021. augusztus 24. 08:42 - Csizmazia Darab István [Rambo]

Úgy tűnik, csúcsra járnak a pénzügyi megtévesztések. Csalók telefonálnak a bankok nevében, és próbálják bekérni a bankkártya adatokat, és folyamatosan érkeznek az átverések SMS-ben valamint e-mailben is. **Egy ilyen most a mi postaládánkba is beesett.**

"Kedves ügyfél!

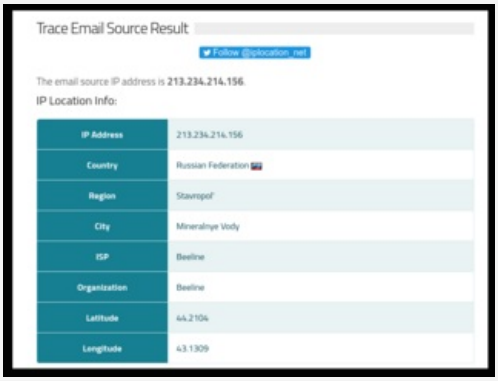
Nemrégiben szokatlan tevékenységeket vagy frissítéseket fedeztünk fel fiókjában, amelyekrol úgy gondoljuk, hogy jogosulatlanok. Az Ön biztonsága érdekében ideiglenesen felfüggesztettük ennek a fióknak a használatát, amíg nem igazolja fiókadatait.

A fiókadatok ellenorzéséhez kérjük, látogasson el a https://www.cib.hu/ oldalra, és azonnal ellenorizze, gyozodjön meg arról, hogy ugyanazokat az adatokat adja meg, mint a fiókban, a fiók adatainak más információkkal történo megváltoztatása végleges eredményt eredményezhet zárolást, és új eljárást kér a feloldáshoz.

Köszönjük az ügyre való gyors figyelmét"

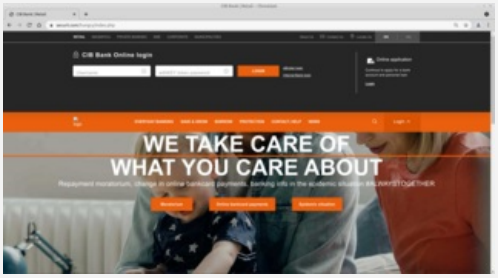
Tuskó Hopkins és Török Szultán ismét visszatért, hogy újfent csúfot űzzön a szép magyar nyelvből - ez már első pillantásra tisztán látszik. **Ahogy az is, hogy a www.cib.hu az NEM egyenlő a hxxp://zoisys.com/index.php weboldallal. És itt akár be is fejezhetnénk a posztot.**

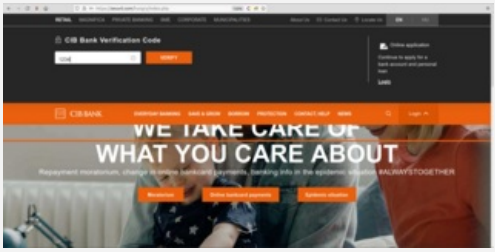
Ha az üzenet forrást leellenőrizzük, akkor azt láthatjuk, hogy **mindezt Oroszországból küldték szeretettel.** De ha már itt vagyunk, lapozzuk át, és lássuk, mi volt az elkövetők zseniális haditerve! **Egy ellenőrző oldal következik, hiába no, lám milyen kedves és alapos emberek ezek a bankárok ;-)**

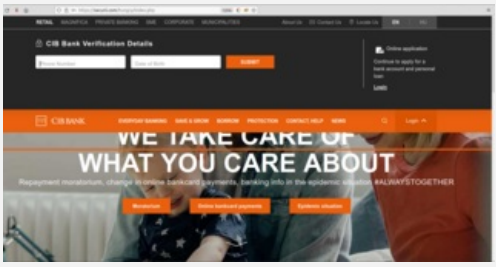


Végül is nem kérnek sok mindent. Ja de. Felhasználó név, jelszó, CIB bank ellenőrző kód, mobiltelefon szám, születési dátum - majd ha valaki ezeket begépelte a bűnözők adathalász ablakába, akkor a rosszindulatú weboldal rögtön átirányítja a látogatót a valódi CIB bankos webhelyre, ahol úgy tűnhet, mintha az előző belépési kísérlet valami miatt sikertelen lett volna, és most újra kezdhetjük a gépelgetést.

A valóság azonban az, hogy éppen átadtuk a banki adatainkat a támadóknak, és kezdhetünk aggódni.

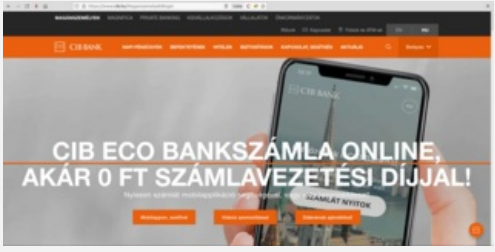






Megint csak intő jelek sokasága, íme a csaló és a valódi webhely.

A bank igazi oldala NEM a "securii.com/hungry/index.php", ahol vicces módon nem is a "Hungary" azaz Magyarország, hanem a "hungry" azaz éhes szó szerepel az URL hivatkozásban. Ki mivel álmodik ugyebár...



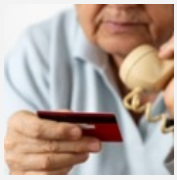
Természetesen a bank is rövid úton közzétette a saját figyelmeztetését, amit itt lentebb láthatunk.

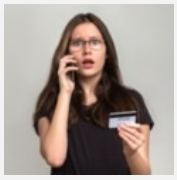
Ám ettől a mostani esettől függetlenül általános érvényű tanács, hogy kéretlen üzenetben, levélben, SMS-ben, telefonhívásban a bank sosem kéri jelszavainkat, belépési azonosítóinkat, ezt telefonba sem diktáltatja be velünk, továbbá semmilyen banki biztonsági osztály nem kér arra minket, hogy állítólagos csalás miatt gyorsan utaljuk el a számlánkról a pénzünket egy általuk bediktált "biztonságos" másik számlára.

Ehhez most már mindenkinek fel kellene nőnie, mert sajnos nem babra megy a játék, valódi károk, igazi tragikus veszteségek történnek valóságos magyar átlagemberekkel.

1 komment
Címkék: bank csalás átverés adathalászat cib

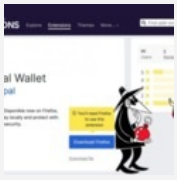
Ajánlott bejegyzések:


A bankos mindig kétszer csenget...


Továbbra is célkeresztben a banki adataink


Ingyenes Omikron teszt vagy mégsem?

Adathalászat a Discordon



Bízz embertársaidban, de emeld meg a kártyapaklit!

Kommentek:

ebella 2021.08.27. 03:59:57

Nekem is írogatnak, telefonaálnak legalább kéthetente, évek óta. Leteszem, vagy/és nem reagálok. "Aki hülye, az is marad." Mert minek csinálnák, ha eredménytelen? Biztos találnak balekot.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

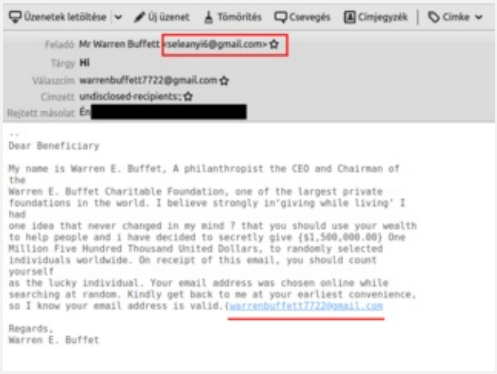
Elon Musk és Warren Buffett írt nekünk

2021. augusztus 27. 12:08 - Csizmazia Darab István [Rambo]

Kevés nagyobb megtiszteltetés képzelhető el, mint hogy ilyen jeles nevezetes személyek levelet írjanak egyenesen nekünk. Igaz, rémlik valami, hogy régebben Bill Gates is írt már egyszer, hogy elosztogatná számunkra a vagyonát, csak írjunk neki vissza egy e-mailt, **ám ez most teljesen más. Legalábbis reméljük. Nagyon-nagyon. Vagy mégsem?**

Az immár 90 esztendős befektetési bankár, Warren Buffett levele egyenesen az Egyesült Államokból érkezett, ezt a trace adatok ellenőrzése is megerősítette. **Kicsit vesztett ugyan az üzenet a személyességéből azáltal, hogy nem mi vagyunk benne az egyedüli címzett**, hanem az "undisclosed-recipients:;" csoportnak küldték, **de biztosan csak sietett az öreg, szeret ő minket.**

Lám csak, hogy a saját nevét is elírta puszta véletlenségből, hiszen a Buffett két ef és két té betűvel írandó, itt pedig valamiért Buffet szerepel, **de hát tegye fel a kezét, aki még soha életében nem ütött félre hasonló betűhibát, na ugye hogy ugye**. Furcsa módon viszont nem Csizmazia úrnak szólít, ehelyett a nagyon hivataloskodó Tisztelt Kedvezményezett szerepel az üzenet elején, **de hát vélhetően sok volt a dolga, és most kivételesen biztos nem ért rá kedveskedni.**


Üzenetek letöltése | Új üzenet | Tömörítés | Csevegés | Címjegyzék | Címke

Feladó: Mr Warren Buffett <seleanyi6@gmail.com>
Tárgy: Hi
Válaszcím: warrenbuffett7722@gmail.com
Címzett: undisclosed-recipients:;
Rejtett másolat: Én [redacted]

Dear Beneficiary

My name is Warren E. Buffet, A philanthropist the CEO and Chairman of the
Warren E. Buffet Charitable Foundation, one of the largest private foundations in the world. I believe strongly in'giving while living' I had
one idea that never changed in my mind ? that you should use your wealth to help people and i have decided to secretly give ($1,500,000.00) One Million Five Hundred Thousand United Dollars, to randomly selected individuals worldwide. On receipt of this email, you should count yourself
as the lucky individual. Your email address was chosen online while searching at random. Kindly get back to me at your earliest convenience, so I know your email address is valid.(warrenbuffett7722@gmail.com

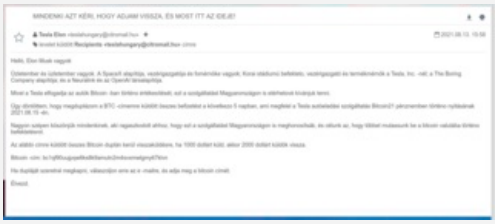
Regards,
Warren E. Buffet

Az igazi jóhír azonban csak most következik, hiszen **kapunk másfél millió ropogós amerikai dollárt, háromszoros hurrá. Csodajó, hogy éppen a mi e-mail címünket választotta ki ehhez**, pedig 4.66 milliárd intermetfelhasználó sorakozik világszerte, mindegyik vagy féltucat különböző e-mailcímmel. **De hát éppen mi voltunk ezek a nagyon szerencsések.**

Semmi más teendőnk nincs már hátra, mindössze válaszolni kell a warrenbuffett7722 KUKAC gmail PONT com címre. Jé, hogy egy ilyen nagy embernek ilyen mukinyulas sorszámozott Google címe legyen, semmi saját domain, meg hasonló? **És ugye, hogy itt már szépen két té-vel írja, szóval tud az öreg, jön a pénzünk hamarosan. Vagy nem.**

Elon Musk levele is nagyon kedves, sőt az első nagy meglepetés, hogy ékes magyar nyelven ír nekünk, mindezt pedig egy szuperbiztonságos citromail-es e-mail címről teszi - teslahungary KUKAC citromail PONT hu - ennél hivatalosabb és professzionálisabb forrásból mindezt nem is tehetné.

A személyre szóló címzést sajnos itt is bebuktuk, mert itt is befigyel a "Recipients". Ám az üzenet tárgya már sokkal bíztatóbb: "Mindenki azt kéri, hogy adjam vissza, és most itt az ideje!". Jöjjön hát a teljes levél!



"*Helló, Elon Musk vagyok*

Üzletember és üzletember vagyok. A SpaceX alapítója, vezérigazgatója és fomérnöke vagyok; Korai stádiumú befekteto, vezérigazgató és termékmérnök a Tesla, Inc. -nél; a The Boring Company alapítója; és a Neuralink és az OpenAI társalapítója.

Mivel a Tesla elfogadja az autók Bitcoin -ban történo értékesítését, ezt a szolgáltatást Magyarországon is elérhetové kívánjuk tenni.

Úgy döntöttem, hogy megduplázom a BTC -címemre küldött összes befizetést a következo 5 napban, ami megfelel a Tesla autóeladási szolgáltatás Bitcoin21 pénznemben történo nyitásának 2021.08.15 -én.

Nagyon szépen köszönjük mindenkinek, aki ragaszkodott ahhoz, hogy ezt a szolgáltatást Magyarországon is meghonosítsák, és célunk az, hogy többet mutassunk be a bitcoin valutába történo befektetésrol.

Az alábbi címre küldött összes Bitcoin duplán kerül visszaküldésre, ha 1000 dollárt küld, akkor 2000 dollárt küldök vissza.

Bitcoin -cím: bc1qf90uujpqw6ks8k9amutn2m4svxmwlgmy67klvn

Ha dupláját szeretné megkapni, válaszoljon erre az e -mailre, és adja meg a bitcoin címét.

Élvezd."

Ez az, igen, lássuk mit is kell tenni az élvezéshez, ha valaki "üzletember és üzletember". Küldeni kell neki pénzt a megadott Bitcoin címre, és várni, hogy az majd duplán érkezzen vissza. Hát ez könnyű feladat lesz. Reméljük, hogy bár kicsit kicsúsztunk az 5 napos ünnepi határidőből, de azért jön majd vissza a dupla pénz, és mi leszünk az igazi telemázlisták: dupla vagy minden.

Na jó, visszazökkehetünk a kevésbé lelkes és biztonságtudatos üzemmódba. Szóval ehhez hasonló csaló levelek, átverős üzenetek folyamatosan jönnek, és mindenkinek érdemes lenne **legalább egy "hihető vagy nem hihető" kérdést feltennie magának, mielőtt elhisz, válaszol, átutal. Mert nem csinálnák, ha nem érné meg nekik, és mindig van, aki sajnos bedől, aki szívesen duplázna.**

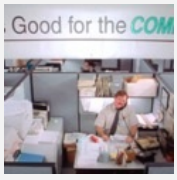
Szólj hozzá!
Címkék: spam tesla csalás átverés warren buffett vagymégsem musk elon biztonságtudatosság

Ajánlott bejegyzések:

Duplázd meg a pénzedet - vagy mégsem?


Földgázszámla vagy mégsem?


Ingyenes Omikron teszt vagy mégsem?



Karácsonyi vásárlás biztonságosabban

Celeb vagyok, fizess nekem!

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

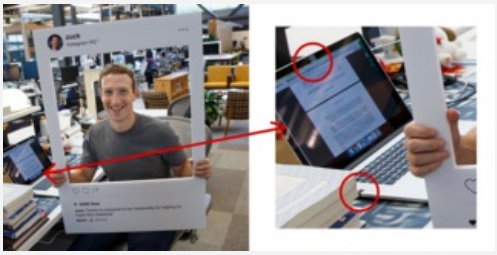
Fontos-e letakarni gyermekeink webkameráját?

2021. szeptember 03. 13:38 - Csizmazia Darab István [Rambo]

Laptopok, okostelefonok, játékkonzolok és táblagépek - **az okoseszközök többségének már van beépített kamerája**. A technológia fejlődésének köszönhetően ma már nem számít, hogy egy barátunk az utca, vagy a világ másik végén él, a webkameráink segítségével bármikor beszélgethetünk (majdnem) szemtől szemben.

A videohívások, a szelfik, a vlogolás, valamint telefonjaink és számítógépeink apró kamerái olyan könnyűvé teszik a kapcsolattartást, amennyire csak lehet. **Ezt a fajta szabadságot pedig különösen élvezik a gyerekek és a tizenévesek.** Viszont nem csak az emberi kapcsolatok profitálnak ebből a technológiából - a szélhámosok is gyorsan felismerték, hogyan használhatják ki, hogy kémkedésre alkalmas eszközök kerültek asztalainkra és zsebeinkbe.

Emiatt ami a múltban még paranoiának tűnhetett, ma már teljesen ésszerűnek bizonyul: néhány évvel ezelőtt, amikor Mark Zuckerbergről készült egy fotó, amelynek hátterében a leragasztott webkamerás laptopja is látható volt, senki sem gondolta, hogy túlzásba esett volna.



Éppen ellenkezőleg, **kifejezetten ajánlott a webkamerák körültekintő használata**, mivel minden csatlakoztatott eszköz potenciális célpontot jelent a támadók számára. Rosszindulatú kódok használatával a kiberbűnözők betörhetnek egy általuk kiválasztott eszközbe, és saját céljaikra használhatják annak kameráját vagy mikrofonját.

Az ESET szakértői arra hívják fel a figyelmet, hogy ezzel a technikával a támadók az áldozatok tudta nélkül be- és kikapcsolhatják a kameráikat, így kémkedve életük legbensőségesebb helyzetei után. **Motivációik változatosak: egyesek egyszerűen csak izgalmasnak találják, hogy titokban másokat figyelhetnek, mások viszont pénzt akarnak kizsarolni az áldozataiktól.** Ha a sértett nem csinálja azt, vagy nem fizeti meg azt az összeget, amit a kémkedők követelnek, a róluk készült videókat vagy képeket közzéteszik az interneten.

Már maga az ötlet is hátborzongató, pláne ha belegondolunk, hogy a támadók gyerekeket is megpróbálhatnak ily módon kihasználni. Elővigyázatos szülőként érdemes megfogadnunk a szakértők alábbi tanácsait:

- Tanítsuk meg gyermekeinknek, hogy ha nem használják a webkamerájukat, mindig takarják le azokat. Így ha támadók fel is törik azt, többnyire használhatatlan lesz számukra. Erre a célra már öntapadós webkamera takarókat is vásárolhatunk, amelyeket egyszerűen csak el kell húznunk, ha használni szeretnénk a kamerát.

- Győződjünk meg arról, hogy gyermekeink webkameráinak alapértelmezett beállítása a „kikapcsolt”.

- Használjunk megbízható, naprakész internetbiztonsági megoldást, amely szoftveres szinten képes védeni a webkamerákat, például figyelmeztet, ha egy program hozzá szeretne férni a webkameránkhoz, és lehetővé teszi a letiltását.

- Győződjünk meg arról, hogy gyermekeink ne rakjanak olyan helyre webkamerát vagy kamerával ellátott okoseszközt, ahol azok intim helyzeteket rögzíthetnek, amelyekkel a csalók visszaélhetnek.

- Tanítsuk meg gyermekeinknek, hogy semmi olyat ne tegyenek egy fedetlen webkamera előtt, amit akkor sem tennének, ha valaki nézné őket.

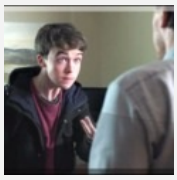
- Mutassunk jó példát gyermekeink számára, és tartsuk be mi is ezeket a szabályokat!

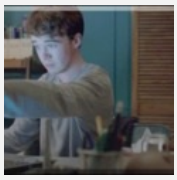
Az [ESET családi oldalán gyermekeknek szóló játékos videókat is találunk], amelyekkel az egész család együtt ismerheti meg a legfontosabb IT biztonsági témákat.

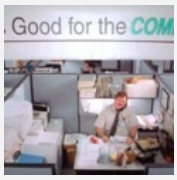
A vírusvédelemben pedig most **segítséget nyújt az iskolakezdési akció is, melynek keretében 1 helyett akár 3 eszközt védhetünk a támadások ellen**, ezzel is nagyobb biztonságban tudva családtagjainkat. További részletek a weboldalon: https://www.eset.com/hu/iskolakezdesi-akcio-2021/

47 komment
Címkék: család webkamera kukkolás akció kamera zsarolás gyermekek kockázat iskolakezdés veszélyek

Ajánlott bejegyzések:


Zsarolás hasra ütésre


Mai szavunk pedig: sextorsion



Karácsonyi vásárlás biztonságosabban


Kiberkockázatok - miért nehéz velük lépést tartani?


Leglegleg - 2020. a kibertámadások tükrében

Kommentek:

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.04. 13:14:49

És mi van a BIOS-ban letiltott kamerákkal? (Notebook)
Op.rendszerbő tudná engedélyezni egy malware?

Hát a mobilokkal, amiknek elég macerás eltakarni a kameráját, ha rendeltetésszerűen használom a készüléket?

Válasz erre

steery 2021.09.04. 13:34:57

Hatékonyabb lenne törvényi szabályozással rákényszeríteni az összes számítógép, laptop és mobiltelefon gyártót, hogy tegyenek a készülékeikre egy mechanikus kapcsolót, tolózárat, amivel a kamera és a mikrofon is fizikailag kikapcsolható és ez a kapcsoló állásán könnyen felismerhető, jól látható. A fizikai megszakítás az egyetlen dolog, amit nem lehet meghekkelni a távolból. Ugyanis a kamerára ragasztott papírcetlik egyrészt leeshetnek, másrészt a mikrofon ettől még nyugodtan használható hallgatózásra. Csodálom, hogy sehol nincs még ilyen törvény, holott a probléma már

lassan 20 éve létezik.

Válasz erre

MaxVal BircaMan KözÍró · http://bircahang.org 2021.09.04. 14:26:03

Nem szabad bedőlni a pedofilhisztinek. Lélegezz szabadon, ne légy liberális.

Válasz erre

kuki123 2021.09.04. 14:28:06

Nagyobb multi cégeknél, főleg fejlesztő részlegeken évek óta, sőt legalább 10 éve már le kell ragasztani a kamerát, Laptopon, mobilon, adathordozó nyílást(SSD/HDD/micro sdcard/usb) leragasztják stb.

Válasz erre

kuki123 2021.09.04. 14:28:52

@Le a spammerekkel: kutya gumit nem ér.
Ha valaki fel akarja törni feltöri

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.04. 14:35:36

@kuki123: ezt most melyikre? A mobilra vagy a BIOS tiltásra?

Válasz erre

kuki123 2021.09.04. 14:37:08

@MaxVal BircaMan KözÍró:
Igen és a védekezés adatbiztonság mennyire fontos, nagyon fontos

de a pedo hiszti egy vicc én is így gondolom.
Tegyük fel látja a pedo a kamerán a gyereket, mit lát?
Semmit a gyerek arcát, ha csak nem a felnyitott laptop előtt vetkőzik át...
Nyilván lecsukja ha nem játszik rajta...
A sima asztali gép kamera már más helyzet az fix...hát ...igen azt talán többet lát.
De az látni fogja a feleséget is meztelenül...nekem le van ragasztva laptopon,

A mobilon is ügyelek arra, hogy csak akkor használjam ha fel van öltözve..ha olyan van wifi kikapcsolva, időnként resetálva..
De pl céges alkalmazás is simán lehallgathat.
A múltkori izraeli kémkedés botrányon meg se lepődtem.
Az okos telefonok biztonsága szart se ér.
Ön ámítás, csak a basic szintet üti meg, hogy X ember ne férjen hozzá, hacker vagy aki ezzel foglalkozik az lazán.
Hemzseg a kiskapuktól az android os

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.04. 14:38:13

@MaxVal BircaMan KözÍró: a "szabadon" = liberális, te ostoba, hazátlan pöcs!

Válasz erre

Örömhernyó 2021.09.04. 14:41:38

@steery: A "probléma" nem létezik. Az a baj, hogy a meztelenséget, szexualitást démonizálják.

Mechanikus kapcsoló, tolózár...
Utcán is burkában vagy nikábban kellene járniuk a gyerekeknek, az a biztos!
Rólam annak idején, gyerekkoromban készültek meztelen képek, zavart később, de nyilván azért, mert káeurópai nevelést kaptam, a szexről, meztelenségről elég korlátolt nézeteket hallottunk.
Aki gyerekekre izgul, az az utcán is megnézi, lefotózza, nem kell neki a meztelenség, azt hozzá tudja képzelni, hisz minden gyerek teste elég hasonló.
Aki felnőtt nőkre izgul és elég perverz, annak se kell feltétlenül a meztelenség, megnézi magának a ruhába öltözött

nőket és simán kiveri rájuk a farkát.

Nekem mutogathatnak meztelen gyerekekről készült fotókat, semmi hatással nincs rám. Aki meg pederaszta vagy pedofil, az az utcán látott gyerekelre is felizgul.

Egy marginális kérdés, valójában álprobléma "megoldására" találsz ki kissé túltervezett "megoldásokat". Mindenre alkossanak törvényt! Az a biztos.

Válasz erre

MaxVal BircaMan KözÍró · http://bircahang.org 2021.09.04. 14:41:55

@Le a spammerekkel:

Ezt rosszul tudod.

Válasz erre

MaxVal BircaMan KözÍró · http://bircahang.org 2021.09.04. 14:43:03

@Örömhernyó:

Na most, egy pedónak van egy rakás LEGÁLIS tartalom a neten és a tv-ben, szóval biztos nem fog vebkamerákat hekkelni.

Válasz erre

Bircanyíró 2021.09.04. 14:52:24

Létezik bármilyen statisztika arról, hogy világszerte eddig hány esetben fordult elő illetéktelen hozzáférés magánszemélyek webkamerjához? Gyanítom, hogy statisztika ide vagy oda, ez a szám rettenetesen alacsony, talán nem is látszik! A Pentagon és CIA hálózatába is történtek már sikeres hacker-betörések, pedig azokat elég komoly tűzfalrendszerek védik. De mondok más példát: néha a lottón is nyernek szerencsés emberek milliárdokat! Mindezzel azt akarom mondani, hogy attól, hogy valami elméletileg és technikailag lehetséges - sőt néhány konkrét példa is van rá - attól még a bekövetkezés esélye lehet olyan irgalmatlanul csekély, hogy foglalkozni is kár vele. Tehát attól, hogy A Pentagon hálózatába is betörtek már, egyáltalán nem következik, hogy ez a te otthoni gépeddel is meg fog történni, az, hogy valaki nyert a lottón, nem jelenti azt, hogy ha veszel egy szelvényt (vagy akár ezret), akkor te is nyerni fogsz. Ugyanígy van a webkamerával is: az elméleti és technikai lehetőség megvan ugyan, de az esély hogy veled ez megtörténik, majdnem egyenlő a nullával. A baj az, hogy a bulvármédia kártékony hatása miatt az emberek mára teljesen elvesztették a realitásérzéküket!

És mielőtt valaki azt mondaná, hogy oké, de a csekély esély is esély, tehát védekezni kell ellene! Az ilyen mentalitásúaktól azt kérdezem, hogy a házukból való kilépés előtt vesznek-e fel bukósisakot, vagy be mernek-e ülni egy autóba, vagy zuhanyoztak-e már a fürdőkádban biztonsági felszerelés nélkül? Csak azért kérdem, mert az esélye annak is megvan, hogy valakinek a fejére esik egy tetőcserép, karambolozni fog, vagy elcsúszik a kádban és kitöri a nyakát! Sőt, meggyőződésem, hogy ezek sokkal gyakrabban történnek meg, mintsem hogy valakit a webkameráján át kukkoljanak illetéktelenek!

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.04. 15:11:27

@Bircanyíró: konkrét statisztikát nem ismerek. Rengeteg médindzsunka kamera eleve backdoorral érkezett/érkezik, ezeket nagyon hackelni sem kell, elég ha a támadó tudja, milyen címen érhető el.
Konkrét esetről tudok: Budapesten sok éve volt néhány publikus forgalomfigyelő kamera.
Ezeket kb. mind leszarták az üzemeltetők, így egy vagy két év elteltével rongyosra hackelték és vírusterjesztésre használták őket a rosszfiúk.

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.04. 15:12:08

@MaxVal BircaMan KözÍró: nem, ezt ti hazaáruló nácik próbáljátok úgy beállítani, ahogy te is, de az hazugság.

Válasz erre

Bircanyíró 2021.09.04. 15:17:17

@Le a spammerekkel: PUBLIKUS forgalomfigyelő kamerát említesz, ráadásul néhány éves sztorit! Ez bizony az én véleményemet tűnik alátámasztani, nevezetesen hogy MAGÁNFELHASZNÁLÓ, otthoni privát gépén nem túl sűrűn

fordul elő, hogy illetéktelenek buzerálják a webkamerát. Egyébként ha a webkamerához hozzáférnek, akkor akármi máshoz is, tehát nem csak a kamerát kellene leragasztani, hanem a billentyűzetet, sőt a bekapcsológombot is! :-)

Válasz erre

MaxVal BircaMan KözÍró · http://bircahang.org 2021.09.04. 15:19:42

@Le a spammerekkel:

Akkor elmagyarázom. A liberalizmus egy ideológia, s nem azt jelenti, hogy szabadság.

Érted, Soros-troll?

Válasz erre

Bircanyíró 2021.09.04. 15:22:00

@MaxVal BircaMan KözÍró: a fasizmus is egy ideológia, érted újfasiszta bértollnok?

Válasz erre

MaxVal BircaMan KözÍró · http://bircahang.org 2021.09.04. 15:34:07

@Bircanyíró:

Bértollnok még sose voltam.
Egy időben fasiszta voltam, már nem vagyok az.

Igen, a fasizmus egy ideológia.

Válasz erre

Bircanyíró 2021.09.04. 15:51:43

Munkásságodat ismerve kellően autonómnak tűnsz, hogy akár el is higgyem neked, miszerint nem vagy igazi bértollnok, DE mindazzal, amit a blogtérben művelsz mégis úgy tűnik, hogy egészen határozottan egy bizonyos irányvonal szekerét tolod, mindenütt jelen lévő hozzászólásaiddal folyton ugyanabba az irányba "manipulálod", a vitákat, terelésekkel, csúsztatásokkal nyilvánvalóan az antiliberális, nacionalista kurzus érdekeit szolgálod, akkor is ha nem bíztak meg ezzel és nem fizetnek ezért. Ugyanakkor gyanút ébresztő az a munkaóra, amit a blogtérben töltesz, ugyanis ha nem ebből élsz, akkor ott a kérdés, hogy miként marad időd bármi másra?

Válasz erre

Bircanyíró 2021.09.04. 16:05:53

@MaxVal BircaMan KözÍró: Az előzőt válaszként akartam küldeni, de talán így sem félreérthető hogy kinek szól...

Válasz erre

MaxVal BircaMan KözÍró · http://bircahang.org 2021.09.04. 16:17:15

@Bircanyíró:

Mindenki egy bizonyos áramlatot támogatva ír.

Tudsz olyan közírót mondani, aki reggel liberális, este fasiszta, közben meg dél körül kommunista?

Nem az lenne a gerinctelenség, ha valaki irányvonal NÉLKÜL írna?

Válasz erre

MaxVal BircaMan KözÍró · http://bircahang.org 2021.09.04. 16:18:11

@Bircanyíró:

"folyton ugyanabba az irányba "manipulálod", a vitákat, terelésekkel, csúsztatásokkal"

Ahogy minden közíró teszi, minden irányzatból, nem?

Válasz erre

MaxVal BircaMan KözÍró · http://bircahang.org 2021.09.04. 16:19:02

@Bircanyíró:

" az antiliberális, nacionalista kurzus érdekeit szolgálod"

Az antiliberális igaz. A nacionalista nem. Antinacionalista vagyok.

Válasz erre

MaxVal BircaMan KözÍró · http://bircahang.org 2021.09.04. 16:22:50

@Bircanyíró:

"gyanút ébresztő az a munkaóra, amit a blogtérben töltesz, ugyanis ha nem ebből élsz, akkor ott a kérdés, hogy miként marad időd bármi másra"

Ha akarsz időt valamire, beosztod az idődet, s lesz rá időd. Mindennel így van ez. A dohányos pl. mindig talál időt dohányzásra, az alpinista hegymászására, a zenebolond meg zenehallgatásra.

Egy rakás dolgot nem csinálok, amit az átlagember csinál. Pl. nem hallgatok modern zenét, nem nézek sóműsorokat, nem olvasok bulvármédiákat, nem dohányzom, nem nézek pornót, nem bulizok, nem iszom alkoholt, nem sportolok, stb. Így sok időm marad.

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.04. 19:10:19

@MaxVal BircaMan KözÍró: hazátlan hazaáruló, faszságot írtál, mint mindig.

Válasz erre

MaxVal BircaMan KözÍró · http://bircahang.org 2021.09.04. 19:14:16

@Le a spammerekkel:

Lám, ellenérved nincs.

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.04. 19:21:42

@Bircanyíró: nem érted. Ezek sima web kamerák voltak, csak ipari külsővel.
A lakásokban előforduló kamerák jó része ugyanígy nincs megfelelően védve.
És a kamerák feltörése nem úgy megy, mint az NCIS-ben, hogy valaki veri a billentyűket, aztán "sikerült főnök!", hanem malware-ek segítségével, amik kihasználják a böngésző egy ismert sérülékenységét, hozzáférve a kliens op.rendszeréhez, ott már két pillanat megtalálni a kamerát és rákapcsolódni.
Nem triviális feladvány, de a mai gépekkel elég gyorsan kivitelezhető, ha nincs rendesen karbantartva a gép/mobil.

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.04. 19:22:22

@MaxVal BircaMan KözÍró: egy hazátlan hazaárulónak? Minek? Neked sincs.

Válasz erre

Almandin 2021.09.04. 19:27:19

@kuki123: Ez rémisztő. Elvileg engem már akkor lefotóztak pucéran. Ugyanis sokszor zenét hallgatok a laptopomon, közben elmegyek zuhanyozni, majd a szobában öltözöm fel. Szörnyű a gondolat, hogy a privát szférámba leskelődnek idegenek.

Válasz erre

Almandin 2021.09.04. 19:30:51

@Örömhernyó: Nem ismered a kukkolók lelki világát. Amúgy nemcsak a gyerekek vannak veszélyben. A kukkolót a leskelődés, a tiltott dolog izgalma vezeti. Másrészt ha valakit lefotóznak meztelenül a gépe előtt, akkor meg is zsarolható, tehát sokan ezzel keresnek pénzt sajnos.

Válasz erre

Almandin 2021.09.04. 19:34:11

@steery: Ebben teljesen igazad van.

Válasz erre

MaxVal BircaMan KözÍró · http://bircahang.org 2021.09.04. 19:34:47

@Le a spammerekkel:

Nekem van, troll. Erre a hétre se kapsz bónuszt a gazdádtól...

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.04. 19:48:10

@MaxVal BircaMan KözÍró: kár, hogy hazaárulóságod még sosem prezentálta. A mocskolódásod nem érv, szarember!

Válasz erre

MaxVal BircaMan KözÍró · http://bircahang.org 2021.09.04. 19:56:50

@Le a spammerekkel:

Mit kellene konkrétan prezentálni?

Válasz erre

Who111 2021.09.05. 08:25:06

A kamerának mikrofonja is van ám. Csaxóltam... A legegyszerűbb egy kétáramkörös kis mechnikus kapcsoló, egy a kamerának, egy a hangnak. A tudomány mai állása szerint szakadt drótban nem megy áram. Ezt az egyet nem lehet szoftverből megoldani. Ezért az a legbiztonságosabb számítógép, aminek a netkábele ki van húzva. (Idézet a WiFi előtti időkből...)

Válasz erre

eßemfaßom meg áll · https://antivaxxer.blog.hu 2021.09.05. 10:11:22

@Bircanyíró: "a vitákat, terelésekkel, csúsztatásokkal nyilvánvalóan az antiliberális, nacionalista kurzus érdekeit szolgálod," Pont annyira mint amennyire Brendel szolgálja a európai értékrendű progresszívek érdekeit. Kb mint ablakos tótnak a hanyattesés olyan hasznosak ezek azoknak akiket támogatni szeretnének.

Válasz erre

eßemfaßom meg áll · https://antivaxxer.blog.hu 2021.09.05. 10:12:46

@MaxVal BircaMan KözÍró: Szerintem mindenki sejtette eddig is, hogy igen szar életed van.

Válasz erre

eßemfaßom meg áll · https://antivaxxer.blog.hu 2021.09.05. 10:19:00

@Almandin: "Másrészt ha valakit lefotóznak meztelenül a gépe előtt, akkor meg is zsarolható, tehát sokan ezzel keresnek pénzt sajnos."
Sokkal egyszerűbb elküldeni egymilliárd mailcímre, hogy "En egy hekker vagy aki feltörte te kamera és készít felvétel ahogy te masturbation. A felvétel elkuldom minden ismerősöd ha nem kuldesz nekem 0,002 BTC erre a cim:"

Válasz erre

MaxVal BircaMan KözÍró · http://bircahang.org 2021.09.05. 10:36:11

@eßemfaßom meg áll:

Kiváló életem van.

Válasz erre

Örömhernyó 2021.09.05. 10:36:59

@Almandin: "Másrészt ha valakit lefotóznak meztelenül a gépe előtt, akkor meg is zsarolható, tehát sokan ezzel keresnek pénzt sajnos."

Hogyan is zsarolható meg valaki, akit lefotóztak meztelenül?
2021-ben valaki még szégyelli, hogy van teste és néha meztelen?
Ha engem lefotóznának meztelenül, első körben felháborodnék, mert erre neveltek, aztán belegondolnék és a képeimet nem szégyellném jobban, mintha mondjuk előnytelen arckép készült volna rólam titokban.
Hogy te is értsd: Ha arról készül titokban felvétel, hogy autókat rongálok, felgyújtok egy hajléktalant, bankot rabolok, akkor azzal zsarolható vagyok. Ha a meztelen testemről készül titokban felvétel, azzal nem vagyok zsarolható.

Azok az emberek, akik zsarolhatónak érzik magukat a meztelen képeikkel, valami lelki betegségben szenvednek. Ez nem jelenti, hogy titokban lehessen másokat fotózni.
Engem mondjuk az is irritál, ha engedély nélkül bárhol kép készül rólam, ruhában. A képen megörökített meztelenségem a felháborodásomhoz nem sokat tenne hozzá.

Más: ma már olyan deepfake technikák vannak, amivel komplett videókat, filmeket lehet kreálni valakiről. Hanggal, beszéddel, bármit az illető szájába lehet adni.
A gyerekek meg aztán teljesen ugyanúgy néznek ki meztelenül serdülőkor előtt, ha egyet láttál, kb. az összeset láttad. Tudom, voltam gyereky fürödtem meztelenül, majd alig ruhában más gyerekekkel (a sötét, kegyetlen, embertelen szocializmusban ez normális volt, senkit se botránkoztatott meg).

Egy pedó az utcán, ruhában látott gyerekre is kiveri. A médiában rengeteg csinos kisfiú és kislány szerepel sorozatokban, a Disney csatorna nézőinek szerintem jelentős része pedó.

Ami a kukkolót vonzza az a tiltott gyümölcs, hogy a kultúránkban szokatlan, tabu a meztelenség. Finneknél az egész család együtt szaunázik, sőt kollégákkal együtt ülsz szaunában egy szál semmiben. A vidéki afrikaiaknál, pápuknál, amazóniai indiánoknál a csöcsök a térdeket verdesik, senkinek nek jut eszébe kukkolni. Nem lenne baj, ha felnőne az emberiség.

Válasz erre

eßemfaßom meg áll · https://antivaxxer.blog.hu 2021.09.05. 11:45:08

@MaxVal BircaMan KözÍró: Igazad van, ez csak a "kiváló" definíciójának kérdése.

Válasz erre

MaxVal BircaMan KözÍró · http://bircahang.org 2021.09.05. 12:32:03

@eßemfaßom meg áll:

Nyilván a szó liberális értelmében életem nem kiváló. Amire büszke vagyok.

Válasz erre

sóhegy049 2021.09.05. 18:53:28

3 réteg fekete szigszalag, mikrofonaljzatba egy üres jack-dugó és VPN.

Válasz erre

Örömhernyó 2021.09.06. 06:10:02

@sóhegy049: Amúgy ennyi. VPN, Tor, üres jackdugó, kamerára egy sötét matrica vagy szigszalag.

Válasz erre

Luna Bell 2021.09.06. 12:33:10

I am professional blogger and I am also search engine optimization consultant at transmediadesign.org/.

Válasz erre

Almandin 2021.09.06. 21:36:23

@Örömhernyó: A logikád szerint akár ki is mehetnénk pucéran az utcára, mert "nem kell szégyellni a meztelen testet". Nos, még a legprimitívebb őserdei népek is viselnek ágyékkötőt, egyszerűen nem illik pucéran járni. Szeméremérzet is van a világon. Én se szégyellem a saját testemet, de nem is mutogatom mindenkinek.
Ehhez mit szólsz, szerinted ez is normális, csak a rendőrök fújták fel?
velvet.hu/elet/2021/09/05/a-strandon-elegitette-ki-magat-egy-no-mindossze-20-masodperc-alatt/?utm_source=index.hu&utm_medium=doboz&utm_campaign=link

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.06. 21:41:43

@Almandin: csakhogy az őserdei népek praktikus okokból hordanak ruha jellegű dolgokat, nem a valláskárosult neveltetésük miatt.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Ha szólsz a rendőröknek, akkor véged!

2021. szeptember 07. 17:15 - Csizmazia Darab István [Rambo]

Ha ransomware támad meg cégeket, vállalatokat, akkor **három féle kárt is képesek okozni: hosszas leállás a szolgáltatásban, titkosítják az adatokat, és ha nem fizetnek a feloldókulcsért, akkor kiteszik, kiszivárogtatják a netre a bizalmas dokumentumokat.**

A vállalkozásoknak **az a legjobb, ha a védekezésben és megelőzésben utaznak**: napi rendszeres biztonsági mentés, automatizált patch menedzsment, naprakész vírusvédelem, biztonságos hálózati (RDP, stb.) beállítások, erős jelszavak és hitelesítés, 2FA/MFA alkalmazása, biztonsági policy,
adminisztrátori jogosultságok korlátozása, biztonságtudatossági képzések, érzékeny adatok nyugalmi állapotban történő titkosítása, hálózatok szegmentálása, és hasonlók.

Ha pedig már helyzet van, általában értesítik a hatóságokat is, illetve sok esetben alkalmaznak ransomware brókereket, akik helyettük tárgyalnak a bűnözőkkel, és igyekeznek lealkudni a fizetendő váltságdíj összegét - ilyen volt például 2020-ban a CWT Business Travel Management Company zsarolóvírus incidens, **ahol 30 ezer számítógép lett fertőzött, 2 TB adatot sikerült a támadóknak ellopni, és végül 4.5 millió dollárnak megfelelő Bitcoint fizettek ki.**

Állítólag meg is kapták a helyreállításhoz szükséges kulcsokat, valamint egy olyan ígéretet, hogy nem teszik közzé a bizalmas vállalati fájlokat. (no comment)

És akkor ide kapcsolódik a mai hírünk is, miszerint a Ragnar Locker zsarolóvírus banda is tisztában van a fenti helyzettel, forgatókönyvekkel, ezért most egy olyan fenyegetést tettek közzé, amelyben azt írják, hogy ha az áldozataik közül valaki kapcsolatba lép a rendőrséggel, bűnüldöző szervekkel, akkor haladéktalanul közzéteszik az ellopott bizalmas érzékeny adatokat.

A fenyegetés azokra az áldozatokra is vonatkozik, akik nem fordulnak a hatóságokhoz, de adatmentési szakértőket bíznak meg az adatok visszafejtéséhez, illetve ilyen szakértőket kérnek fel a tárgyalási folyamat sikeres lefolytatása érdekében. Minden ilyen említett esetben a csoport bosszúból azonnal közzéteszi az áldozattól megszerzett teljes adatcsomagot saját darknetes .onion webhelyén.

Úgy tűnik tehát, **igyekeznek minden olyan "zavaró körülményt" kiiktatni, ami árthat a zsaroló üzletüknek, vagy a hatóságok érdeklődését túlzottan rájuk irányíthatja.**

A Ragnar Locker ransomware korábbi áldozatai között olyan jelentős szervezeteket találunk, mint a Capcom szerencsejátékban érdekelt cég, a Campari italgyártó vállalat, vagy a tajvani ADATA adattároló gyár.

29 komment
Címkék: fenyegetés váltságdíj ransomware locker zsarolóvírus ragnar

Ajánlott bejegyzések:


Váltságdíjat kínálnak a váltságdíjszedő bandáért

Kik, hol és mire költik a beszedett váltságdíjainkat?


Offline mennyország - egy rövid időre


Amikor a hóhért akasztják...


Ransomware helyzetjelentés

Kommentek:

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.08. 06:27:17

@blogger: mostanában nem nagyon reagálsz a felvetődő kérdésekre...
Pl. jelen esetben az automatizált patch management alatt mit értesz?
Mert így első olvasatra nekem az jön le, hogy minden javítást, kérdés nélkül feldobni az összes gépre... az meg, különösen ha windows-ról van szó, nem biztos, hogy jó ötlet. :)

Válasz erre

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2021.09.08. 11:53:10

@Le a spammerekkel: SZia! Nyilván ez nem mindenhol jó, például kritikus infrastruktúráknál, bankoknál tesztkörnyezetben kell tesztelni ezeket, de még mindig számos magánszemély, kkv nem foglalkozik vele, sőt néha nagyok sem. Például a 143 milló adatlopásos Equifax esetben, bár az USA három nagy hitelminősítő közül az egyik, az incidensig nem is volt felelőle a frissítéseknek, nem is végeztek ilyet, és a forensic vizsgálat azt mutatta, egyértelműen emiatt futottak bele az adatlopásba: az Apache Struts sebezhetőségre kiadott javítófolt már 2017. március 7-én megjelent, a hibajavítás elvégzése hónapokig mégsem történt meg. Vagyis figyelmet kell rá fordítani, nyilván nem bambán, és nem mindenhol végezhető előzetes tesztek nélkül.
www.theregister.com/2017/09/14/missed_patch_caused_equifax_data_breach/

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.08. 13:10:42

@Csizmazia Darab István [Rambo]: az az Equifax... hát az már a NAB+ kategória...
Én kisebb, bár kritikus szoftvereket használó cégnélvoltam sokáig. Azt hiszem, egyszer kellett egy windows update, ami sok gépet használhatatlannátett, hogy attólkezdve szigorúancsak tesztelve...
És még így is sikerült olyanba belefutni (nem windowson), hogy teszten jó volt, csak az élest fektette meg a tizedik user belépése után :D (adatbázis szerver valami op.rendszerbe integrált lockolási mechanizmust használt és azon változtattak valamit, ami tömeges deadlockokhoz vezetett... az egy izzasztó hét volt :D)

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.08. 13:12:51

Franc ebbe a bloghu-ba, hogy nem lehet szerkeszteni... samsung billentyűzet a szóközöket nyeli le, gboard meg a teljes kommentet ha egy "."-ot írok rossz helyre... és csak itt. (Droid+firefox)

Válasz erre

munkanélküli informatikus 2021.09.08. 22:45:27

Én még nem hallottan olyan zsarolóvírusról, amely többet tett volna a fájlok titkosításánál. Ahánnyal csak találkoztam, az mind egyszerűen letitkosította a fájlokat a számítógép összes meghajtóján (és persze a többi gépen is, ha elég hülye volt a rendszergazda.... a "betű alapú" meghajtó megosztás hálózatban amatőr hiba!) és ezzel egyidőben a vírus megadja a feloldókulcs hozzáférésének módját. Ezek a vírusok meg sem próbálnak a fájlokról másolatot készíteni egy távoli helyre (ami egyrészt lebukás veszélyes lenne, másrészt technikailag is lehetetlen, több okból is). Tehát aki olyat ír le, hogy a zsaroló vírusok írói a fájlokban lévő információk nyilvánosságra hozatalával zsarolják a számítógépek gazdáit, az még életében nem látott zsaroló vírust.

Válasz erre

munkanélküli informatikus 2021.09.08. 23:04:22

@Le a spammerekkel:
A windows frissítés olykor nagyobb bajt okoz, mint amekkora bajt a frissítés szolgáltatás letiltása okozott volna :)

Válasz erre

CoolKoon 2021.09.08. 23:45:55

Nos igen, "hálás" téma ez. Én személy szerint a bankokat ilyen szempontból egy kicsit sem sajnálom, törjék fel, töröljék le, lopják el jó sok pénzüket, mert azok úgyis nagy ívből tesznek gyakorlatilag minden sebezhetőség kijavítására, aki pedig figyelmeztetni próbálja őket, azokat egyenesen a rendőrségen is feljelentik (tehát magyarán ott rohadjanak meg ahol vannak). A többi cégnél érdemes lenne a megfelelő csatornákon rendszeres felvilágosítási kampányt végezni, de persze Mo-n ilyen soha de SOHA nem lesz, lásd a Tré-Systems meg a Telekom esetét (=tökkelütött idióták által vezetett haveri cégek, ergo a holdudvar "szagértői" is vsz. hasonlók lehetnek).

A Ragnar Locker esete eléggé érdekes amúgy. Vagy szorul a nyakuk körül a hurok, vagy nem megy a bolt, mert a patkányszerű fenyegetésből ítélve mintha a végét járnák. Egyrészt ugyanis ha fölérendelt helyzetben lennének, akkor nem lenne szükségük a fenyegetőzésre, másrészt pedig ezzel gyakorlatilag minden potenciális áldozatnak azt üzenik, hogy bármit is tesznek (ha az FBI-nak szólnak, ha szakértőket fogadnak!), akkor is nyilvánosságra hozzák az összes ellopott adatot. Ezzel pedig gyakorlatilag még inkább arra ösztönzik a cégeket, hogy ne fizessenek nekik, hiszen mindenképpen fel kell bérelniük valakit aki elvégzi a rendszereik auditálását és megfelelő tanácsokkal/intézkedésekkel elejét veszi egy újabb támadásnak.

Válasz erre

CoolKoon 2021.09.09. 00:21:30

@munkanélküli informatikus: "A windows frissítés olykor nagyobb bajt okoz, mint amekkora bajt a frissítés szolgáltatás letiltása okozott volna :) " - Sajnos ez nem ennyire egyszerű. Az ISO 27001 nevű ocsmány förmedvény például kimondottan előírja a rendszeres frissítéseket, méghozzá záros időn (asszem a nyilvánosságra hozatalától számított két héten) belül. A frissítések külön tesztelése pedig meglehetősen időigényes dolog.

"Tehát aki olyat ír le, hogy a zsaroló vírusok írói a fájlokban lévő információk nyilvánosságra hozatalával zsarolják a számítógépek gazdáit, az még életében nem látott zsaroló vírust." - Ezeknek a támadásoknak az a lényege, hogy adatlopással egybekötött zsarolóvírus-támadások szoktak lenni, tehát mire a cég rájön, hogy baj van, addigra az adatai valószínűleg a támadónál vannak.

Válasz erre

Kedélyes Paraszt 2021.09.09. 07:00:47

@CoolKoon: a 27001emlékeim szerint nem ír elő záros határidőt, főleg nem 2 hetet. Max ajánlja. A jelenlegi környezetemben kb egy hónap alatt fut át a Windowsos rendszerek (szerverek és munkaállomások) patchelése a kiadástól kezdve. Sok-sok év alatt néhány esetben futottunk bele, hogy tömeges hibát okozott (talán 2-3 alkalom), amikor is vissza kellett vonni egy patchet. Olyan, hogy esetileg valakinél nem működött valami, az is csak olyan 10-es nagyságrendileg. Szóval, ha engem kérdeznek, én mindenféleképp javaslom a rendszeres patchelést.

Válasz erre

]{udarauszkasz 2021.09.09. 07:04:47

@CoolKoon: Bocs,hogy bele amatorkodom,de ha egy zsarolo szervezet adatokat lop (jo sok terabyteot)az nem tunik fel senkinek,aki egy kicsit is monitorozza a forgalmazast?

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.09. 07:13:43

@CoolKoon:

"Én személy szerint a bankokat ilyen szempontból egy kicsit sem sajnálom, törjék fel, töröljék le, lopják el jó sok pénzüket, mert azok úgyis nagy ívből tesznek gyakorlatilag minden sebezhetőség kijavítására, aki pedig figyelmeztetni próbálja őket, azokat egyenesen a rendőrségen is feljelentik "

Ergo életedben nem jártál normális bank informatikai rendszereinek a közelében sem. Nekem volt szerencsém többhöz is. Ez így egy egetverő hazugság, nem több.
A pénzügyi szektorban (ahol jártam) kényesen ügyelnek, legalábbis ügyeltek a biztonsági kérdésekre. És én nem tudok olyan esetről, hogy ha károkozás gyanúja nélkül jelzett valaki egy hibát, akkor a bank a rendőrséghez fordult volna.
Az más kérdés, hogy a rendszer feltörésére irányuló kísérleteket feljelentéssel honorálják.

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.09. 07:18:46

@]{udarauszkasz: hogy gondolod a monitorozást, amivel észlelhető, hogy napi pár megabájttal többet forgalmaz egy-egy munkaállomás valami legális felhőszolgáltató vagy mondjuk a cloudflare irányába?
Ha meg MitM-t játszanak és elemzik a kimenő forgalom tartalmát... az nem tudom, mennyire vállalható úgy hardveresen, mint jogilag.

Szóval nem költői a kérdés: hogy gondolod, hogy gondoljátok?

Válasz erre

gigabursch 2021.09.09. 08:22:40

@Le a spammerekkel:
Ízlés nem vita tárgya, de ha van böngésző, amit rühellek az pont a FF.

Válasz erre

gigabursch 2021.09.09. 08:29:02

A cikk belseje is néhol zavaros, de a cím...

Szóval, helyesen:
Ha szólsz a rendőröknek [vessző(!)] véged.

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.09. 09:17:24

@gigabursch: más droidos böngésző nem rendelkezik olyan szolgáltatásokkal, mint a noscript, ublock0 stb.

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.09. 09:18:52

@gigabursch: már megint itt van, hogy nem lehet szerkeszteni. :(

Szóval FF - én is rühellem, mióta dobták a korábbi verziót, de lásd fenn, nincs más...

Válasz erre

]{udarauszkasz 2021.09.09. 10:04:16

@Le a spammerekkel: LED Keyboard megy nalam,az nem szivat.

Válasz erre

]{udarauszkasz 2021.09.09. 10:10:53

@Le a spammerekkel: gondolom,azert egy rencergizda csak latja,hogy egyszercsak megindultak a terabajtok valami cloud fele,esetleg egy valami ismeretlen iranyba.
Meg en,mint mezitlabas juzer is ki tudom szurni otthon,ha valami nem franko a nettel. Egy idoben volt olyan,hogy torrent kozben szinte teljesen megallt a net. Kiderult,hogy a kliens nyitott valami kismillio portot (tcp asszem) aztan a kliens csere utan nagyjabol normalizalodott a helyzet.
Nektek,mint hivatasos infosoknak gondolom,csak van tobbfajta eszkozotok erre

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.09. 11:22:45

@]{udarauszkasz: épp az a gond ezzel, hogy ha elég sunyi a kis spyware, akkor szép lassan csordogál kifelé az infó, akár hónapokon át. Azt elég nehéz kiszűrni, ha látszólag legális irányba küldik. (Nem igazán értek hozzá, meg tippeket sem akarok adni a tréfás kedvű kollégáknak, szóval inkább nem mennék részletekbe)

Válasz erre

GyMasa 2021.09.10. 00:12:17

@munkanélküli informatikus:
Igen, ez nekem is feltünt...
Főleg, hogy egy adatlopás az egy jól előkészített és valószínúleg sokáig tartó akció.
Csak a 2TB adat feltöltése lenne vagy 4,5 nap, ha egy teljes, 1Gbites uplinkje van a cégnek.
Az pedig bizonyosan szemet kell, hogy szúrjon a rendszergazdának.
Ha meg lemegy 100Mbitre, akkor 45 nap, de még az is túl feltűnő adatforgalom szerintem.

Válasz erre

CoolKoon 2021.09.11. 22:38:34

@Le a spammerekkel: "És én nem tudok olyan esetről, hogy ha károkozás gyanúja nélkül jelzett valaki egy hibát, akkor a bank a rendőrséghez fordult volna." - Valóban. A "normál" ügymenet úgy működik, hogy hogyha valaki jelez egy hibát, akkor nagyívből leszarják. Aztán ha az illető (a saját szakállára) akciózni kezd, na akkor megy a rendőrségi feljelentés, természetesen a hibák kijavítása nélkül. És persze a volt kollegáim (középszerű informatikusok mind) közül nagyon sok pont bankokba ment dolgozni. De persze, ez az egész csak kitaláció, én se létezek, és a magyar banki rendszerek a legbiztonságosabbak a világon (hmm, vajon a FIPS tanúsítványaik a rendszerük összes elemére vonatkozik?)...

Válasz erre

CoolKoon 2021.09.11. 22:45:15

@]{udarauszkasz: Ami azt illeti, nem szokás a hálózati adatforgalmat valós időben figyelni, mivel fölösleges. Persze, hébe-hóba megnézi az ember (na meg persze akkor ha gond van), de alapesetben nem figyeli minden nap. Az adatlopási támadások pedig nem feltétlenül úgy működnek, hogy az illető egyszerre fog megpróbálni feltölteni 2 TB adatot valahova, hiszen tudja, hogy az jó eséllyel azonnal feltűnne. Az ilyen eseményekről szóló hírekben gyakran visszatérő elem, hogy mire külső szakértőkkel vizsgáltatják meg a rendszereiket kiderül hogy már hetek, sőt hónapok óta folyhatott a támadás. Annyi idő alatt pedig elég kényelmesen ki lehet csempészni egészen nagy adatmennyiséget is, elég nagyot ahhoz hogy a cégnek fájjon is.

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.12. 01:56:23

@CoolKoon: miből gondolod, hogy leszarják? Elég rég kiszálltam a területről, de amíg ott dolgoztam... maradjunk annyiban, hogy nem szarták le, max. a téma érzékenysége miatt nem volt visszajelzés.

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.12. 02:29:47

@CoolKoon: kurvajó... már sokadjára fordul elő, hogy gépelek egy félórát és hirtelen minden ok nélkül eltűnik az egész. Az előző mobillal nem volt ilyen gond...

Megpróbálom újra: azzal nem értek egyet, hogy ne lenne értelme "valós időben" monitorozni a forgalmat.
Megfelelő szoftverrel azért bizonyos dolgokat elég jól ki lehet szűrni.
Sőt... Igaz, ez a saját hálómon történt, de ilyesmiből született rendőrségi feljelentés is. :D
Feltűnt, hogy kissé gyakorivá vált pár dél-amerikai cím felkeresése, miközben tudtam, hogy szándékosan nem járok arra és látszott a logokból, hogy egy elég jól behatárolható időszakra esett a forgalom indulása abba az irányba. A szolgáltató javasolta, hogy tegyek feljelentést arra az esetre, ha törvénysértő dologra használná valaki a hálózatomat, hogy legalább nyoma legyen a hackelésnek.
Pár nappal később persze kiderült, hogy egy régóta használt tool közelmúltban telepített új verziója pofázik valamit "haza". Azóta se tudom, hogy telemetria, valami benne felejtett, fixen beírt cím vagy tényleg malware volt, az biztos, hogy egy szimpla uninstall után megszűnt a gyanús forgalom. (Visszaraktan, újra kezdődött, úgyhogy repült az egész)
Viszont ez csak akkor feltűnő, ha gépenként lehet elemezni a forgalmat és nem valami népszerű felhős szolgáltatást használ a szivárogtató malware...

Válasz erre

CoolKoon 2021.09.12. 11:44:53

@Le a spammerekkel: "A szolgáltató javasolta, hogy tegyek feljelentést" - Muhahahaha már látom hogy a hazai rend őrei hogy fognak dél-amerikai szarfészkekben drogkartellek által üzemeltetett rendszerek IP címei után kutakodni meg érdeklődni :D

"Viszont ez csak akkor feltűnő, ha gépenként lehet elemezni a forgalmat" - Pontosan. Ez max. egy tízfős cégnél járható út, ennél fölfelé már nagyon is nyomós oknak kell lennie ahhoz, hogy "rádolgozzanak" a hálózati adaforgalomra.
Mellesleg ha már itt tartunk igen, van még egy kategória, ahol nagyon figyelik a hálózati forgalmat: az olyan cégeknél, ahol az internetezési szokások miatt boszorkányüldözést folytatnak. Viszont ilyen cégeknél nem jó dolgozni, és igazából ezek általában magasan tesznek az IT biztonságra, a forgalom figyelését csak az alkalmazottak sanyargatására használják.

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.12. 12:17:24

@CoolKoon: ugye te a fidesz IT-s "szakembereinek" sorát gyengíted? Remélem, ennyire buta alakokat máshol nem találni...
Az egy dolog, hogy rendünk őrei kb annyira voltak képben,mint te, de ugye az esetleges feltörés esetén arra kell a feljelentés, hogy a saját seggem valamennyire fedezve legyen, ha valóban betört valaki a hálózatra és bűncselekmény végrehajtásához használta.

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.12. 12:21:30

@CoolKoon: többezres cégnél is működik ilyen felügyelet, nem csak home lan esetében. Csak ott már szoftver riaszt. A riasztásokat kell humán erőforrásnak kezelnie. Egyelőre.

Válasz erre

CoolKoon 2021.09.12. 13:31:08

@Le a spammerekkel: "ugye te a fidesz IT-s "szakembereinek" sorát gyengíted?" - Idióta....a Fidesz IT "szakemberei" olyan cégekben ülnek, mint a Tré-Systems meg a Telekom, de ahogy így elnézlek, téged is onnan szalajthattak...

"Az egy dolog, hogy rendünk őrei kb annyira voltak képben,mint te" - lol na pont erről beszéltem...

"arra kell a feljelentés, hogy a saját seggem valamennyire fedezve legyen" - Érdekes, nálunk is volt gyanús forgalom, aztán mégsem lett belőle feljelentés. Az egyik kollégának a telefonján "rakoncátlankodott" valami szar. Visszarakta az egészet gyári beállításokra és annyi. A feljelentés sokkal gyanúsabb forgalomnál szokás csak, de hát te tudod. Végül is rájöttél erre magad is, miután elmentél a rendőrségre és elámultál a magas szintű technikai tudásuktól :D

"többezres cégnél is működik ilyen felügyelet, nem csak home lan esetében" - Igen, a fenti okokból (=az alkalmazottak figyelése érdekében). Aztán ezenek az adatoknak a felhasználásával szűrik a céges internet-hozzáférést valami eszement módon. A kimenő oldalon lévő anomáliák figyelését végző rendszerek pedig szerintem csak nagyon-nagyon feltűnő dolgok esetén riasztanak, mivel kisebb gyanús forgalmat egyszerűen nincs esélyük kiszűrni, és bárki bármit is állít, a DPI se csodaszer, az is igazából csak az alkalmazottak nyaggatására jó.

Válasz erre

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.12. 14:27:01

@CoolKoon: szóval tényleg fidesznyik "szakember" vagy. Bizonyítéknak ennyi elég is. :D

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Ransomware helyzetjelentés

2021. szeptember 09. 12:09 - Csizmazia Darab István [Rambo]

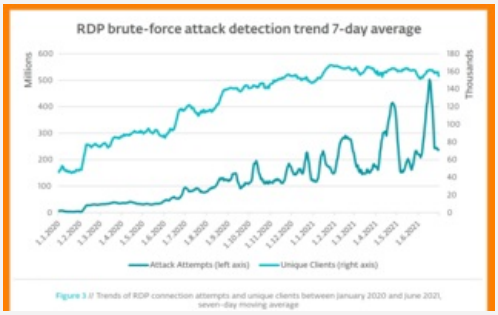
Az ESET közzétette **legújabb, zsarolóvírusokról szóló jelentését**, amely azt vizsgálja, hogyan válnak egyre veszélyesebbé a zsarolóvírusok a bűnözők technikai fejlesztései és egyre újabb megtévesztéses trükkjei által.

Emellett kiemelte a támadók által használt leggyakoribb technikákat, **három legelterjedtebb támadási vektorra fókuszálva: Távoli Asztali Protokoll (Remote Desktop Protocol, RDP), e-mail mellékletek és az ellátási lánc.**

A zsarolóvírussal támadó csoportok a zsarolási és terjeszkedési eszköztáruk bővítésére használták ki a koronavírus-járványt, például a Távoli Asztali Protokollt futtató, nyilvánosan elérhető és rosszul konfigurált rendszereken keresztüli behatolásokra összpontosítva. **A telemetriai adatok szerint az RDP mára az egyik leggyakoribb támadási formává vált: a 2020. januárja és 2021. júniusa közötti ilyen észlelések száma meghaladta a 71 milliárdot.**

Az e-mailhez csatolt rosszindulatú fájl mellékletekkel ellentétben az RDP-n keresztüli támadások a legitimitás álcájával tudnak kicselezni számos észlelési módszert, mivel **a vállalkozások kevésbé tudatosak ezzel a fenyegetéssel kapcsolatban.**

A telemetriai adatok azt is feltárták, hogy a **főként vállalati hálózatok fájl- és nyomtatómegosztására használt Server Message Block (SMB) protokollt támadási vektorként is lehet használni, és ezen keresztül is sikeresen be lehet juttatni a zsarolóvírust a szervezetek hálózatába**. 2021 januárja és áprilisa között az ESET biztonsági megoldásai több mint 335 millió nyilvános SMB elleni brute force (próbálgatásos módszerű) támadást akadályoztak meg.

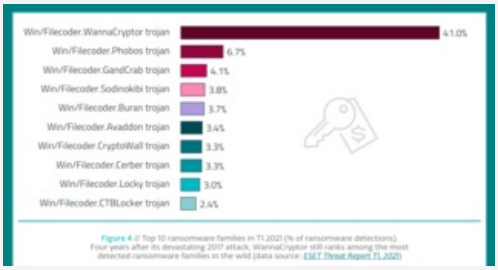


Ahogy a zsarolóvírus-támadások egyre célzottabbakká válnak, elengedhetetlen, hogy a vállalkozások tisztában legyenek a kiberbűnözők legújabb módszereivel és készen álljanak azok kezelésére, elhárítására.

2020. kezdete óta többször is bebizonyosodott, hogy betartott szabályokkal, a távoli hozzáférés megfelelő beállításaival, kétlépcsős belépéssel kombinált erős jelszavakkal, illetve rendszeres biztonsági frissítésekkel sikeresen fel lehet venni a harcot a zsarolóvírusokkal. A **jelentés az RDP és más kiberhigiéniai tényezők megfelelő beállítása mellett egy fejlett végponti detektálásra és reagálásra képes eszköz alkalmazását is javasolja a vállalkozásoknak.**

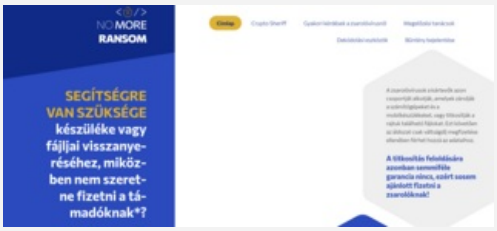
A riport kiemeli a Kayesa valamint a Colonial Pipeline rendszerét érintő közelmúltbeli nagy horderejű támadásokat is, illetve, hogy **világszerte milyen óriási költségeket jelentenek a vállalkozásoknak a zsarolóvírus-támadások.** A tanulmány szerzői a váltságdíj fizetési dilemmát is megvitatják a fent említett esetek fényében.

Érveik szerint bár a váltságdíj kifizetésével talán visszaszerezhető a fájlok egy része, nincs rá semmifajta garancia, hogy kiberbűnözők ténylegesen hajlandók vagy képesek is helyreállítani az adatokhoz való teljes hozzáférést, **a követelt kriptovaluta pedig segíti őket a jövőbeli névtelen bűncselekmények további finanszírozásában** – ezért folyik jelenleg is vita az ilyen jellegű kifizetések illegálissá tételéről.



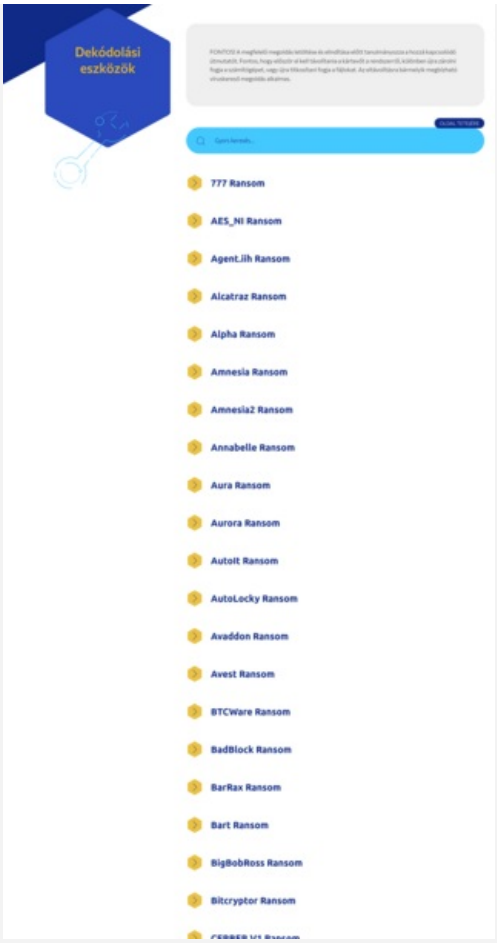
Elengedhetetlen, hogy a szervezetek rendelkezzenek a szükséges ismeretekkel a zsarolóvírus-színtér legújabb fejleményeivel kapcsolatban, hogy a kiberhigiéniára, az optimális beállításokra, rendszeres mentésekre és a megbízható biztonsági intézkedésekre alapozva építhessék ki védelmüket.

A No More Ransom elnevezésű, 2016-ban induló kezdeményezés a végrehajtó szervek és az IT biztonsági vállalatok közös összefogásával született, célja a zsarolóvírusok áldozatainak segítése a fájlok helyreállításában.



Azóta, hogy **2018-ban az ESET is csatlakozott ehhez a kezdeményezéshez, már öt zsarolóvírus-kezelő eszközét bocsátotta** a nyilvánosság rendelkezésére, amelyek több, mint 25 ezer embernek segítettek.

A kiberbiztonsági vállalat brute-force támadások elleni biztonsági technológiája kifejezetten sikeres védelmi mechanizmusnak bizonyult: **2020 januárja és 2021 áprilisa között a csaknem 1 millió ügyfeleket célzó, megközelítőleg 55 milliárd támadási kísérletet észlelt és blokkolt. Ezen felül eddigf több, mint 300 ezer internetező töltötte le** az egyik nyilvánosan elérhető zsarolóvírus-eltávolító eszközüket is.

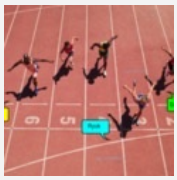


Indulása óta a No More Ransom több mint hatmillió embernek segített ingyenesen helyreállítani a túszul ejtett fájljait, amely közel egymilliárd euró megszerzésében akadályozta meg a zsarolóvírussal támadó bűnözőket. A kezdeményezés jelenleg 121 különféle ingyenes eszközt kínál, ezek 151 zsarolóvírus család dekódolására képesek, és 170 védelmi partnert egyesítenek a köz- és a magánszektorból.

A portál 37 nyelven - köztük magyarul is - érhető el, az új No More Ransom weboldal pedig modernebb és felhasználóbarátabb, és folyamatosan friss információkkal és tanácsokkal szolgál a zsarolóvírusokról, illetve a támadások megelőzéséről.

Szólj hozzá!
Címkék: statisztika jelentés éves eset váltságdíj ransomware zsarolóvírus no-more-ransom

Ajánlott bejegyzések:


Világrekord, aminek mégsem örül senki

A ransomware-nek nincs No-go zóna

A Cerber visszatér

Oly távol vagy tőlem, és mégis közel


COVID-19 nyomkövető vagy mégsem?

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

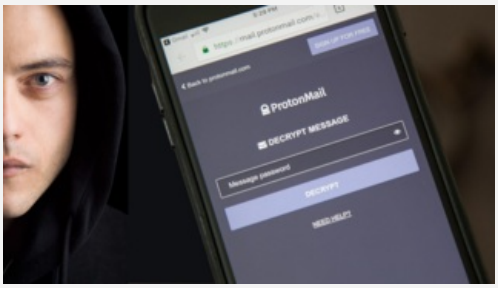
accountz

Belépés
Regisztráció

Bezzeg régen minden jobb volt?

2021. szeptember 14. 07:43 - Csizmazia Darab István [Rambo]

Semmi sem állandó, csak a változás maga - szól Hérakleitosz idézete, aki vajmi keveset sejthetett arról, hogy itt és most milyen kontextusban fogjuk őt idecitálni. Volt már korábban egy olyan markáns céges üzenet az Apple részéről, amit érdemes volt a Wayback Machine internetes archívumából előkeresve szembeállítani az éppen aktuális állapottal. **Ezúttal megint valami nagyon hasonló megváltozásos esetnek lehetünk a tanúi.**

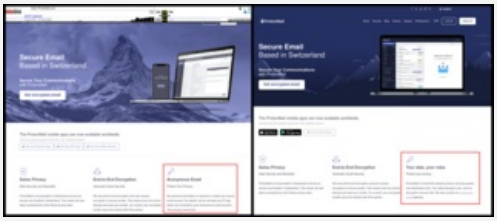


Az emlegetett korábbi marketingüzenet az volt, amikor az Apple honlapján eredetileg szereplő "***It doesn't get PC viruses***. *A Mac isn't susceptible to the thousands of viruses plaguing Windows-based computers. That's thanks to built-in defenses in Mac OS X that keep you safe, without any work on your part.*" üzenet átváltozott "***It's built to be safe***. *Built-in defenses in OS X keep you safe from unknowingly downloading malicious software on your Mac.*" megmondásra. Vagyis az "*Itt nincsenek vírusok*" helyett "*A rendszert úgy alakították ki, hogy az biztonságos legyen.*" lett az új szlogen.

Az ok pedig az volt, hogy a korábbi ritka esetek után egy kritikus Java sebezhetőséget széleskörben kihasználó kártevő 2012-ben mintegy 600 ezer OSX gépet megfertőzve **kártékony botnet hálózatot tudott létrehozni.**

A mostani eset is egy hasonló akkor és most párhuzamra épül, ahol a svájci titkosított ProtonMail üzemeltetők eredeti "*By default, we do not keep any IP logs which can be linked to your anonymous email account. Your privacy comes first.*" üzenetét váltotta le a "*ProtonMail is email that respects privacy and puts people (not advertisers) first. Your data belongs to you, and our encryption ensures that.*" Magyarán a "*Nem tároljuk el az ön IP címét*" *helyett lett a "A ProtonMail tiszteletben tartja a magánélet védelmét, és az embereket helyezi előtérbe, nem a hirdetőket.*"

Mindez igazából azt jelzi, hogy a TheRegister értesülése szerint a Proton jogilag kötelező érvényű végzést kaphatott a Svájci Szövetségi Igazságügyi Minisztériumtól, aminek állítólag ellenvetés vagy fellebbezés nélkül kötelessége volt eleget tennie.



Tehát nem igaz, hogy nem őrzik meg az IP címeket, legalábbis mostantól már biztos nem, és ezek indokolt esetben kiadhatók.

Emlékezetes, hogy a jelenleg 50+ millió felhasználóval rendelkező titkosított levelezést biztosító cég **egy évvel azután indult, hogy Edward Snowden megtette a nagy hatású kiszivárogtatását**, amiből többek közt az is kiderült, hogy a titkosszolgálatok minden korábbi elképzelést felülmúlóan tömegesen hozzáfértek mindenfajta elektronikus kommunikációnkhoz.

A titkosított levélküldési rendszernek hirdetett [ProtonMail szolgáltatás mindenesetre](#) most változott, de legalább nem megszűnt, mint korábban a Lavabit [vagy lemeztitkosítást fejlesztő TrueCrypt](#).

Igaz, az is megjelent vele kapcsolatban, hogy [a ProtonMail állítólag kapcsolatban állt/áll a CIA-vel, és hátsóajtót biztosít a számukra, erről többek közt Bruce Schneier](#) is írt a blogjában.

Egyébként ha furcsaságokat keresgélünk a titkosítás világában, számtalan érdekes történést találhatunk. Amikor 2013-ban kiderült, hogy **az RSA - ami ugyebár titkosítási termékeket fejleszt - az NSA kérésére szándékosan gyengített a titkosításon, és 10 millió dollárért egy jóval gyengébb, azaz könnyebben feltörhető véletlenszám-generátort tettek** a BSAFE biztonsági eszköztárába, akkor a szakma látványosan felháborodott.

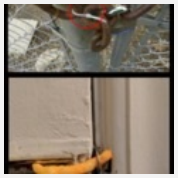
Ezt például [Mikko Hypponen is élesen kritizálta, a Twitteren kijelentette, hogy "az egész iparág nevében szégyelli magát"](#). Sőt később emiatt a 2013-as RSA konferencián való előadói szereplését is lemondta.

A friss esetek közt válogatva pedig az volt egy izgalmas sztori, amikor **idén kiderült, hogy a bűnözők által széles körben használt ANOM elnevezésű titkosított üzenetküldést biztosító alkalmazást valójában az amerikai szövetségi nyomozóiroda (FBI) fejlesztette és üzemeltette két éven át.**

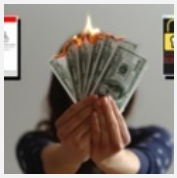
A fedett művelet során több, mint [800 gyanúsított letartóztatására került sor, köztük maffiózók, kábítószer kereskedők és egyéb bűnözői csoportok](#) buktak le a lehallgatott kommunikáció következtében.

[5 komment](#)
Címkék: [apple](#) [fbi](#) [truecrypt](#) [levelezés](#) [nsa](#) [titkosítás](#) [rsa](#) [végpont](#) [ipcím](#) [snowden](#) [protonmail](#) [anom](#)

Ajánlott bejegyzések:


[Titkosítok,](#)


[Váltságdíjat](#)


[Fejemen](#)


[Leglegleg -](#)

[Vakcinás](#)

tehát vagyok | kínálnak a váltságdíjszedő bandáért | olvad a vaj, engem nem érhet baj | 2020. a kibertámadások tükrében | csalások, szevasztok

Kommentek:

Androsz · http://migransozo.blog.hu 2021.09.15. 15:38:25

Illik embernek nézni azt is, aki nem olvas angolul, és ha már angol idézeteket használok, akkor le is fordítom azokat. Megtehetném helyetted, de inkább meghagyom a teret a javításra, úgy lenne az igazi.

Válasz erre

eplethy 2021.09.16. 12:15:52

@Androsz: Nem nem! Nem lefordítjuk az internetet, hanem megtanulunk angolul! Ők is emberek ettől még, nem értem ez hogy jön ide.

Válasz erre

eplethy 2021.09.16. 12:17:03

Ráadásul nem szöveget, képet kéne fordítani??? Hagyjuk már...

Válasz erre

Androsz · http://migransozo.blog.hu 2021.09.16. 15:40:25

@eplethy: Te ne életcélt adj az embereknek, ne hosszútávú programot tervezz nekik, hanem érthető olvasnivalót. Az nem értelmes hozzáállás, hogy mindenki tanuljon meg angolul, aztán majd visszajöhet, elolvasni a te izgalmas posztodat. Most nem mindenki beszél angolul azok közül, aki idetéved téged elolvasni, és a viselkedésed, a hozzáállásod kicsit gyerekes felvágásnak tűnik, hogy te milyen ügyesen olvasol már angolul, a magyar fordítása már nem is szükséges. A posztot nem magadnak írod. Vagy ha mégis, akkor ez rólad mesél.

Nem a képeket kellene lefordítanod, hanem azokat az angol idézeteket, amelyeket bevettél a szövegbe. Mondtam: illik lefordítani. Vagy törődsz az udvariassággal, vagy nem, engem nem érdekel tovább.

Válasz erre

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2021.09.17. 11:35:38

@Androsz: Szia. Beszúrtam a fordításokat, amiket javasoltál.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Szerva itt, letartóztatás ott

2021. szeptember 21. 14:44 - Csizmazia Darab István [Rambo]

Sajnos valóban nagyon ritka alkalom, hogy arról olvashatunk, ha egy bűnözői hálózatot lekapcsolnak. Ám most mindenki örömére ez történt, és a lekapcsolása alatt **az Europol és az olasz Eurojust aktív közreműködésével történő 106 gyanúsított letartóztatását kell érteni.**

A kiterjedt nemzetközi bandának olyan mostanában széles körben elterjedt bűncselekmények róhatók fel, mint az adathalászat, amelynek segítségével a kártékony hasonmás oldalakkal szerzik meg az áldozatok belépési jelszavait és személyes adatait.

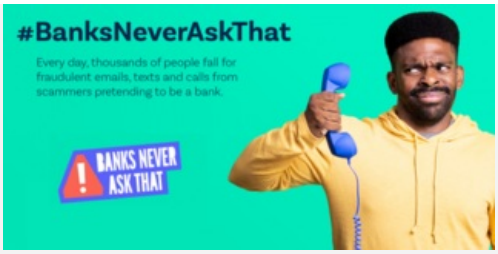
Számos ilyen incidens tud nagyon komoly veszteségekkel is járni, például emlékezetes lehet sokaknak az idén márciusban felbukkant Fedex-es átverési hullám, amelyben a személyes adatok ellopása egyes esetekben még az áldozatok bankszámlájának kiürítéséhez is elvezetett.

Ezzel át is értünk a következő módszerhez, hiszen az adathalászat mellett az **egyre többször felbukkanó SIM kártya cserés támadást is nagyban űzték a csapat tagjai.**

Ez egy olyan egyre inkább terjedő csalási forma, ahol a célszemélyről begyűjtött, kiszivárgott, ellopott személyes adatok birtokában, pontosan ezekkel visszaélve az ügyfél nevében SIM kártya cserét kezdeményeznek a mobilszolgáltatónál, és **onnantól kezdve már ők kapják a banki kétfaktoros jóváhagyó és tájékoztató SMS üzeneteket.**

A céges e-mailek kompromittálása pedig egyenes út lehet az úgynevezett főnöki utalás nevű csaláshoz. Ennek során alapos belső információkkal rendelkezve a főnök nevében (például feltörve a levelezését) **arra utasítják a pénzügyi osztály vezetőjét, hogy bizalmasan kezelve azonnal hajtson végre egy nagy összegű átutalást, vagy egyenlítsen ki egy olyan számlát, aminek a bankszámlaszáma más, mint korábban.**

Legtöbbször utólag derül csak ki, hogy csalók ezt a mesét használták a vállalati számla megcsapolására, és igen nagy összegű károkat tudnak ezzel okozni.



A főnöki utalás módszere is sokat csiszolódott az idők folyamán, és így **már nem csak e-mail útján, hanem telefonos hívással is történhet ilyen.**

Egy szintén címlapokra került 2019-es esetben például **egy angol energetikai cég vezérigazgatója azonnal átutalt 220 ezer eurót egy ismeretlennek, mert azt hitte, hogy pár perccel korábban a cég németországi igazgatója kérte erre**, pedig ez csak egy megtévesztésig hasonló, számítógéppel szimulált hang volt.


106 ARRESTED IN A STING AGAINST ONLINE FRAUDSTERS

20 September 2021

Press Release

EUROPOL

About € 10 million was stolen in just a year

The Spanish National Police (Policía Nacional), supported by the Italian National Police (Polizia di Stato), Europol and Eurojust, dismantled an organised crime group linked to the Italian Mafia involved in online fraud, money laundering, drug trafficking and property crime. The suspects defrauded hundreds of victims through phishing attacks and other types of online fraud such as SIM swapping and business email compromise before laundering the money through a wide network of money mules and shell companies. Last year alone, the illegal profit is estimated at about € 10 million.

Overall results:

- 106 arrests, mostly in Spain and some in Italy
- 16 house searches
- 118 bank accounts frozen
- Seizures include many electronic devices, 224 credit cards, SIM cards and point-of-sale terminals, a marihuana plantation and equipment for its cultivation and distribution.

This large criminal network was very well organised in a pyramid structure, which included different specialised areas and roles. Among the members of the criminal group were computer experts, who created the phishing domains and carried out the cyber fraud, recruiters and organisers of the money muling, and money laundering experts, including experts in cryptocurrencies. Most of the suspected members are Italian nationals, some of whom have links to mafia organisations. Located in Tenerife (Canary Islands, Spain), the suspects tricked their victims, mainly Italian nationals, into sending large sums to bank accounts controlled by the criminal network. They then laundered the criminal proceeds through a wide network of money mules and shell companies.

A mostani incidensnél őrizetbe vette személyek többségét Spanyolországban, kisebb részüket pedig Olaszországban tartóztatták le. A hatóságok szerint a jól szervezett banda központja Tenerifén üzemelt, és több száz áldozatuk volt. A károsultak elsősorban olasz állampolgárok voltak, de spanyol, angol, német illetve ír áldozataik is voltak. Az ügy kivizsgálása során összesen 16 házkutatást végeztek és 118 bankszámlát befagyasztottak.

A rendőrök számos elektronikus eszközt, 224 hitelkártyát, SIM-kártyákat foglaltak le, de emellett a helyszínen marihuánaültetvényt és a hozzá tartozó mezőgazdasági berendezéseket is találtak. **Az olasz rendőrség értesülése szerint sikeres volt az akció, és éppen idejében történt, mert a klasszikus forgatókönyv szerint az ellopott pénzeszközöket nehezen lenyomozható kriptovaluta vásárlásra tervezték felhasználni, illetve további bűncselekményekbe fektették volna, például kábítószerbe valamint a fegyverkereskedelembe.**

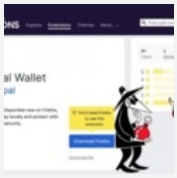
Szólj hozzá!
Címkék: csalás átverés letartóztatás interpol adathalászat átutalás őrizetbevétel simswap főnöki

Ajánlott bejegyzések:


A bankos mindig kétszer csenget...


Ingyenes Omikron teszt vagy mégsem?

Adathalászat a Discordon



Bízz embertársaidban, de emeld meg a kártyapaklit!


Fogják a pénzünket és futnak

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

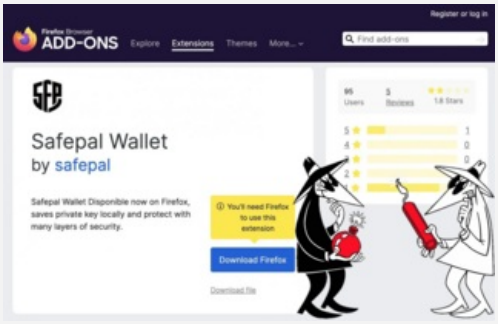
accountz

Belépés
Regisztráció

Bízz embertársaidban, de emeld meg a kártyapaklit!

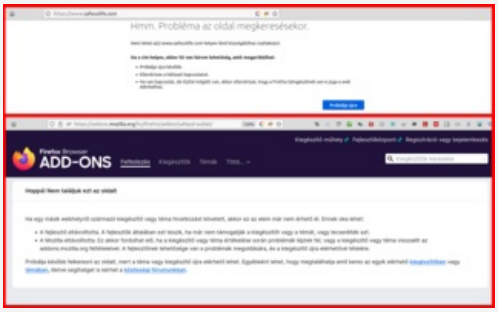
2021. szeptember 28. 11:04 - Csizmazia Darab István [Rambo]

Néhány órával a telepítés és a bővítménybe való bejelentkezés után azt láttam, hogy a pénztárca egyenlegem 0 dollárra csökkent - **panaszolta egy érintett felhasználó, aki a rosszindulatú Firefox bővítményt futtatta**. Hát ebből már jól látszik, hogy ez sajnos nem egy sikertörténet lesz.



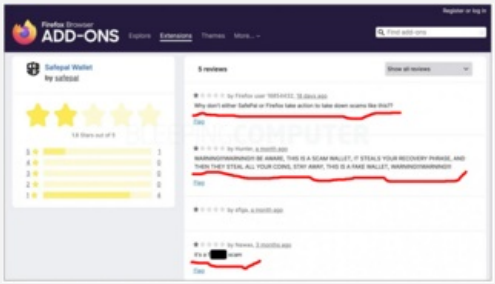
Beszámolók szerint a "Safepal Wallet" elnevezésű rosszindulatú Firefox-bővítmény átverte a felhasználókat, és kiürítette pénztárcájukat. Hét hónapig viszont zavartalanul volt letölthető a Mozilla bővítmény kínálatban. **A Safepal egy kriptovaluta pénztárca alkalmazás, amely rengeteg különböző fajtájú virtuális fizetőeszköz biztonságos kezelését ígérte**, többek közt a Bitcoint, az Ethereumot és a Litecoint.

A BleepingComputer észrevétele szerint a lelepleződés után a rosszindulatú böngészőbővítményt levették ugyan, de az adathalászatot kiszolgáló kártékony weboldal változatlanul működik még. **A mi mai posztunk írásakor azonban a safeuslife.com oldalt már azóta szerencsére lelőtték.**



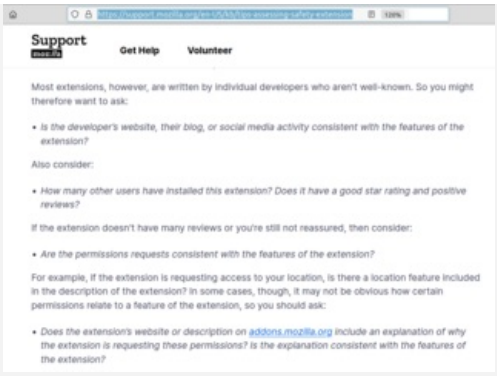
A kiegészítő állítólag 2021. február 16. óta volt elérhető. Egy pórul járt felhasználó bejelentése után biztonsági felülvizsgálatot ígértek, majd 5 nap múlva kivették a letölthető bővítmények közül. A károsult a rendőrséghez is fordult, ám ők azt mondták, nem tehetnek semmit. **Mivel a Safepal máig jelen van mind az Apple Store, mind pedig a Google Play hivatalos webáruházban**, és az ottani felhasználói értékelések szerint megbízhatóan végzi a dolgát.

Így az tűnik a legvalószínűbb forgatókönyvnek, hogy a Mozilla kiegészítő készítői egész egyszerűen ellopták a Safepal nevet, a logót és a leírást, majd a cég nevében egy hamis, kártékony kiegészítőt fejlesztettek és nyújtottak be. A céljuk nyilvánvalóan a megbízható név mögé bújva **a gyanútlan áldozatok megkárosítása volt, az ellopott helyreállítási kulcsok segítségével.**



Ha van tanulság, akkor az egyrészt az, hogy **a pénzünket nem szabad akárkire, akármilyen ellenőrizetlen alkalmazásra rábízni**. Másrészt amint azt egy korábbi, androidos appok területén tapasztalható kaotikus állapotokkal kapcsolatos posztunkban írtuk: **nagyon kell figyelni a gyanús alkalmazásokra.**

A Google Play esetén például rengeteg esetben található volt teljesen azonos néven rengeteg népszerű játék, divatos alkalmazás, ahol könnyű volt eltéveszteni, melyik az igazi, melyik a csaló. Vagyis arra is **mindig kiemelten kell figyelni, melyik az eredeti app, ellenőrizni, ki a fejlesztő, és megnézni az értékeléseket.**

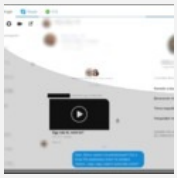


Időközben a Mozilla frissítette a bővítményekkel kapcsolatos közleményét, amelyben kiemelten felhívja a felhasználók figyelmét ezekre az értékelésekre, a fejlesztő webhelyének ellenőrzésére.

Remélhetőleg emellett a saját maga figyelmét is felhívja, hogy fogadjon be és tegyen fel a kínálatba nem megfelelő bővítményeket. Hát reménykedjünk ebben, azt végül is szabad ;-)

2 komment
Címkék: firefox böngésző csalás átverés mozilla bővítmény kártékony adathalászat rosszindulatú wallet bitcoin kriptovaluta ethereum

Ajánlott bejegyzések:


Facebook egyperces


Azt mondod Covid19, azt mondom spam


A bankos mindig kétszer csenget...


Ingyenes Omikron teszt vagy mégsem?

Adathalászat a Discordon

Kommentek:

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.09.29. 13:57:12

Ha már hamisítás...
A netpincérről rendeltem volna, de nem tudom a jelszavam.
Kértem újat, a kapott link a ablink.info.netpincer.hu oldalra vitt, ott viszont a browser hisztizni kezdett, hogy nem biztonságos a kapcsolat, mert a szerver tanúsítványa a sendgrid.net domainhez tartozik.
Hm. Ilyenkor mi a teendő? A sendgrid.net számomra ismeretlen.

Válasz erre

Omnilox 2021.09.29. 16:28:07

@Le a spammerekkel: Harmadrendű aldomain, ez elég ritka. Gyanakodva kezelném, mert ilyen aldomaint a DNS szerverekre bejutva is lehet regisztrálni, eltérítve a felhasználót egy tetszés szerinti oldalra. Lehetetlennek tűnhet, de már nem az, sajnos. A sendgrid.net egyébként kétesélyes, mert a Google és a Yandex szerint e-mail küldő oldal, lehet valóban kapcsolatban a netpincér jelszómegújító funkciójával, nem szükségképpen reklámoldal. A Firefox NoScript bővítménye fedezékében megpróbáltam megnézni a linket, de csak ennyi nem elég, ennek a végén nincs weboldal. A Google erre a címre ételfutárok reklámjait dobta fel, ezért szerintem el lehet fogadni a tanúsítványt.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

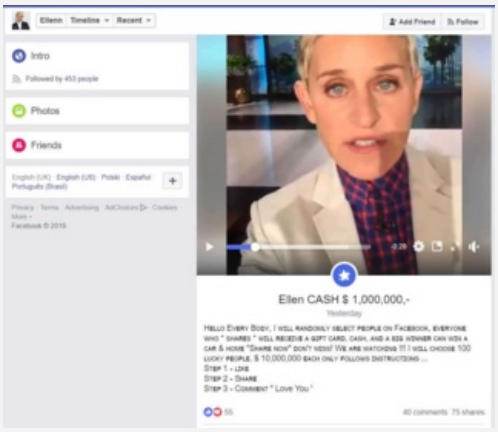
Fiatal vagy? Ezekre az online csalásokra figyelj!

2021. szeptember 30. 09:45 - Csizmazia Darab István [Rambo]

A hamisított designer termékektől a "túl szép ahhoz, hogy igaz legyen" típusú állásajánlatokig - **íme, öt gyakori trükk, melyekkel a csalók a kamaszok pénzét és személyes adatait próbálják megszerezni.**

A bizalom és a fiatalsággal járó naivitás teszi a csalók egyik első számú célpontjává a tizenéveseket, hiszen kamaszként még könnyebben hiszünk másoknak. Ha szülőként olvassuk ezt a cikket, érdemes megosztanunk az itt leírt tanácsokat a gyermekeinkkel is, a biztonságos online jelenlét érdekében.

Nézzük, **melyek a legnépszerűbb, tiniket célzó csalási módszerek, és hogyan védekezhetünk ellenük** az internetbiztonsági programokat fejlesztő ESET szakértői szerint!



1. Csalások a közösségi médiában
Mivel a közösségi média a tinédzserek digitális játszótere, nem meglepő, hogy a csalók ott próbálják meg lépre csalni őket, ahol az idejük legnagyobb részét töltik. A közösségi médiás átverések a legkülönfélébb formákban érkeznek, így nincs egyetlen, minden esetben alkalmazható univerzális megoldás. **Az egyik gyakori csapda hírességekről szóló, sokkoló címekkel ellátott bulvárcikknek álcázza magát, viszont aki rákattint a linkre, egy kártékony weboldalra kerül.**

A csalók közvetlenül is kapcsolatba léphetnek áldozataikkal olyan üzenetek formájában, **amelyek különféle versenyekben és nyereményjátékokban való részvételre invitálják őket.** A megosztott link ez esetben is egy hamis weboldalra vezet, amely megfertőzi az eszközüket kártékony programokkal, vagy megpróbálja kicsalni tőlük a bizalmas személyes adataikat.

2. Leárazott luxustermékek
Egy másik népszerű internetes csalási forma a közösségi médiában megosztott hamis hirdetés, amely nevetségesen alacsony áron kínál luxuscikkeket. Hogy ajánlataik kellőképpen vonzóak legyenek a tizenévesek számára, a csalók

megpróbálnak a kamaszok körében kifejezetten népszerű márkákat és árukat kínálni – **a limitált kiadású cipőktől kezdve a kamu Ray-Ban online webshopokon át az olyan márkás ruhákig, amelyeket egyébként nem engedhetnének meg maguknak a zsebpénzükből vagy a részmunkaidős fizetésükből.**

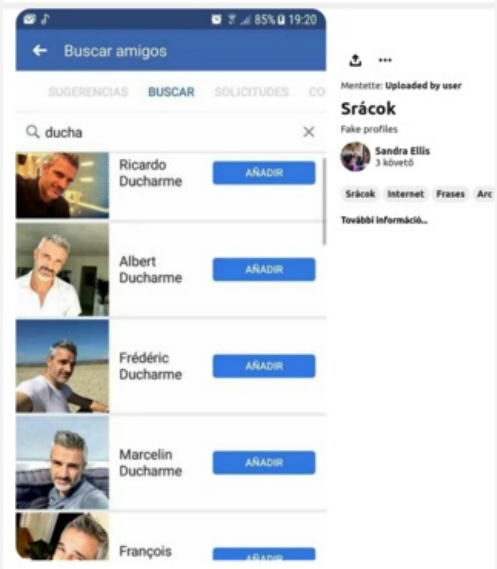
Az átverés egy hamis webáruház létrehozásán alapul, amely széles választékot kínál a fent említett termékekből, azonban a vásárlás után a megrendelők vagy egy hamisított terméket kapnak, vagy semmit sem. A legrosszabb esetben pedig a bankkártya adataink ellopásával le is nullázzák az egyenlegüket.

3. Ösztöndíjas csalások
A tandíj és a továbbtanulással járó költségek fedezésében segíthetnek az ösztöndíjak – a kiberbűnözők pedig az anyagi támogatást kereső diákokra vadásznak különféle hamis ösztöndíjak ajánlásával – elsősorban az angol nyelvterületen élőknél.

Ezek a nem létező ösztöndíjprogramok gyakran kötelezik a kérelmezőt egy regisztrációs díj kifizetésére, azonban ezt a pénzt a csaló teszi zsebre. **Az átverés "ösztöndíj-tombola" formájában is érkezhet, amely az adóköltségekre hivatkozva követeli meg a résztvevőtől egy előzetesen előre fizetendő "feldolgozási díj" vagy "kifizetési díj" átutalását.**

4. Hamis munkaajánlatok
Nem könnyű tinédzsernek lenni, hiszen a divatos ruhákat, bulikat, utazásokat, tanulmányokat nem lehet csak a zsebpénzből fedezni – éppen ezért keresnek sokan részmunkaidős állást. **A fiatal álláskeresők átveréséhez a kiberbűnözők hamis állásajánlatokkal kecsegtetik őket, amelyek többnyire eleve túl jól hangzanak ahhoz, hogy igazak legyenek.**

A csalók hiteles állásajánlat-gyűjtő helyeken posztolnak hamis munkalehetőségeket, amelyek általában otthoni könnyű munkavégzést lehetővé tévő, kifejezetten jól fizető pozíciót ígérnek. Azonban ezek célja nem a foglalkoztatás, hanem a célpontok személyes adatainak kicsalása, melyeket később egyéb átverésekhez tudnak majd felhasználni – **például az áldozat nevére történő bankszámla megnyitásához vagy a személyazonosságukkal történő okirat hamisításához.**



5. Álprofilos átverések
A szerelmi csalók már nem csak a társkereső oldalakon tevékenykednek – gyakran a közösségi médiát is fürkészik, ahol

kiszemeltjeikkel privát üzeneteken keresztül lépnek kapcsolatba.
A csaló sok esetben olyan személynek adja ki magát, akit a célpont nagy valószínűséggel vonzónak talál. Ezután addig udvarol, amíg el nem éri a célját, például, hogy pénzt csaljon ki az áldozatától.

Sajnos a kiberbűnözők a legvisszataszítóbb taktikáktól sem riadnak vissza, ezért az is előfordulhat, hogy áldozataikat intim képek küldésére ösztönzik, majd azzal zsarolják őket, hogy megosztják ezeket a szeretteikkel és/vagy a nyilvánossággal, amennyiben az áldozat nem fizet nekik.

Szerencsére vannak olyan módszerek, amelyekkel hatékonyan lehet védekezni.

- Ha egy olyan állásajánlattal találkozunk, amely csábítóan hangzik, de vannak aggályaink, **keressünk rá a cégre, hogy találunk-e valami gyanúsat**. Ne felejtsük el, hogy a bérkifizetéshez szükséges személyes adatokat mindenhol csak a felvétel után kell megadni.

- Ugyanez vonatkozik az ösztöndíjakra is – **mindig győződjünk meg az állítólagos ösztöndíjat kínáló szervezet hitelességéről, akár internetes kereséssel, akár az iroda közvetlen felkeresésével**. És soha ne fizessünk be előre semmiféle "feldolgozási" vagy "előleg" díjat.

- Az internet egyik alapszabálya: „**Ha valami túl szépnek tűnik ahhoz, hogy igaz legyen, akkor valószínűleg nem igaz.” Tehát ha egy nevetségesen leárazott, limitált kiadású márkás termékkel találkozunk,** akkor szinte biztosak lehetünk benne, hogy átverésről van szó. Amennyiben ennek ellenére sem tudjuk kiverni a fejünkből az ajánlatot, akkor alaposan ellenőrizzük le a szállítót, hogy találunk-e bármi gyanúsat.

- Az idegenektől érkező kéretlen levelek esetén mindig nagyon gyanakvónak kell lennünk, pláne ha egy kétes ajánlat, gyanús csatolmány vagy link is érkezik az üzenettel együtt. Minden esetben a legjobb lépés teljesen figyelmen kívül hagyni a levelet és nem rákattintani az ismeretlentől érkezett linkre vagy mellékletre.

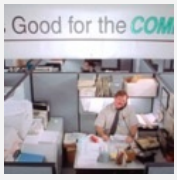
- Amennyiben **egy idegen chatüzenetekben próbál kapcsolatba lépni velünk és rövid időn belül szerelmet is vall, villognia kell a belső vészjelzőnknek**, hogy ez nem életszerű. Egy gyors, kép alapján (Reverse Image Search, pl. TinEye) történő kereséssel hamar kiderülhet, hogy valamilyen hátsó szándékkal másnak adják-e ki magukat.

Szólj hozzá!
Címkék: internet csalás tippek átverés fiatalok megelőzés közösségi oldalak védekezés

Ajánlott bejegyzések:

Az egyik COVID-19, a másik egy híján 20

Ha eljön a személyiségtolvaj



Karácsonyi vásárlás biztonságosabban


Amazónia veszélyes ragadozói ;-)


7 tipp a mobilunk védelméhez

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

Amikor a hóhért akasztják...

2021. október 04. 11:24 - Csizmazia Darab István [Rambo]

Sajnos túl jó üzletnek számít a zsarolóvírus, sőt már **évek óta elérhető bérelhető szolgáltatás, RaaS azaz Ransomware as a Service formájában is**. Ám az élet nem habos torta, ahol nem mi vagyunk, ott az ellenség - amint az a Tanúban is elhangzik. **Ahogy a Darkneten is lehet, hogy az éppen felbérelhető bérgyilkos egy fedett nyomozó, vagy egy bűnözők által kedvelt ANOM nevű titkosított üzenetküldő valójában meg az FBI-tól származik. A mai történetünk is hasonló húrokat pendít meg.**

Revil, vagyis Ransomware Evil - van-e, ki e nevet nem ismeri? Mint az közismert, ez a bűnözői csapat állt az Acer, és a Kaseya felhőalapú felügyeleti szolgáltató elleni zsarolóvírus támadások mögött.

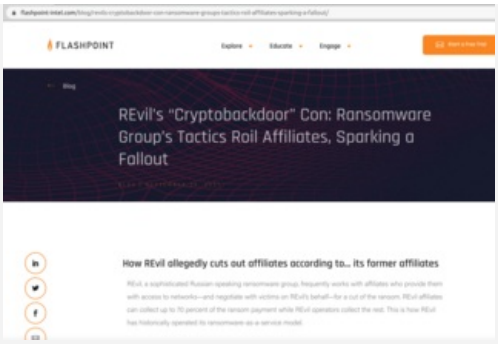
A csoport egy jó ideje adja bérbe a ransomware erőforrásait más elkövetőknek, cserébe pedig ezekből a harmadik felek általi támadásokból származó Bitcoin kifizetésekből is részesülnek, amiket az áldozatok fizetnek a bérlőknek a ransomware dekódoló kulcsokért. **Eddig legalábbis papír forma szerint így zajlott a dolog, ám most úgy tűnik megváltozott a modell.**

Talán sokan emlékeznek arra az összeállításunkra, amely az androidos megfigyelő-kémkedő alkalmazásokról szólt. **Ezekről a mobilos megfigyelő-kémkedő alkalmazásokról - amelyeket a zaklatók szoktak letölteni és használni áldozataik ellen** - az derült ki, hogy számos súlyos biztonsági rést tartalmaznak, melyek révén távoli támadók, vagy éppen maga a szoftverek fejlesztői nem csak az áldozat, hanem a megfigyelő ellen is tudnak kémkedni.

Vagyis itt a fagyi nem kicsit nyalt vissza.

Ezzel analóg módon most az derült ki, hogy Revil csapat nem elégedett meg a normál részesedéssel a váltságdíjakból, hanem nagy valószínűséggel **elhelyeztek a programjukban egy olyan hátsóajtót is, ahol a ransomware tárgyalásokat is figyelemmel kísérhették.**

És ha elengedő nagy váltságdíjjal kecsegtetett egy üzlet, ők maguk közvetlenül felvették a kapcsolatot az áldozatokkal, és ők kasszírozták be a feloldó kulcsért járó összeget kizárva így saját bérlőiket.



Egy beszámoló szerint például már éppen nyélbe ütöttek volna egy 7 millió dollárnak megfelelő összegű "üzletet" a RaaS-t használó bűnözők, mikor a zsarolási történet varázsütésre egyszer csak véget ért. Utólag pedig azt gyanítják, a fenti ok vezethetett a váratlan végkifejlethez. **Több fórumon, több különböző incidens kapcsán egybehangzóan megismétlődött ez a vélelmezett forgatókönyv.**

Mondhatjuk erre, hogy csalót becsapni ugyan nem vétek, de a felhasználók szintjén ez már teljesen irreleváns, hiszen itt szinte mindegy, végül ki kopasztja meg az áldozatot, számunkra mindkettő egyformán bűnöző. Emiatt a védekezést és megelőzést továbbra is érdemes magas szinten tartani: végpont és szervervédelem, frissítések, rendszeres mentés, autentikáció, titkosítás, többtényezős hitelesítés és hasonlók - ahogy azt már többször is írtuk. **Aki pedig a címképet esetleg nem ismerné, annak mindenképpen érdemes megnéznie A kilenc 9 királynő című zseniális mozifilmet.**

Szólj hozzá!
Címkék: trükk csalás átverés backdoor váltságdíj hátsóajtó revil ransomware zsarolóvírus

Ajánlott bejegyzések:

Kik, hol és mire költik a beszedett váltságdíjainkat?


Offline mennyország - egy rövid időre


A Kaseya három napja


Váltságdíjat kínálnak a váltságdíjszedő bandáért


Ransomware helyzetjelentés

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

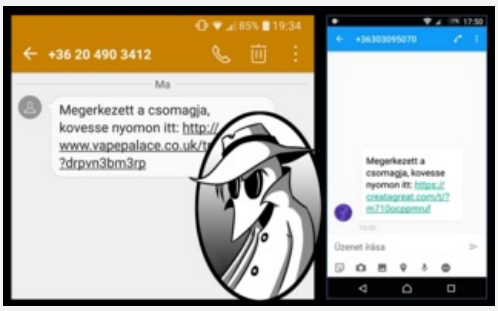
accountz

Belépés
Regisztráció

Csak a felszín más: csomagküldés helyett frissítés

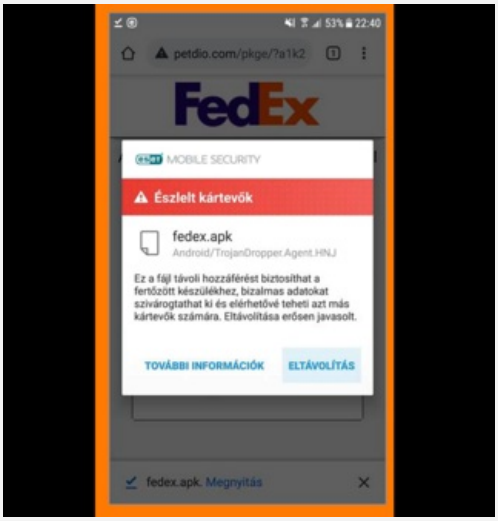
2021. október 11. 10:50 - Csizmazia Darab István [Rambo]

Biztosan sokan emlékeznek arra az **androidos kártevőre, amely a Fedex nevében idén márciusban árasztotta el Magyarországot a "Megerkezett a csomagja, kovesse nyomon itt" kezdetű, magyar telefonszámokról érkező SMS üzenetekkel.**



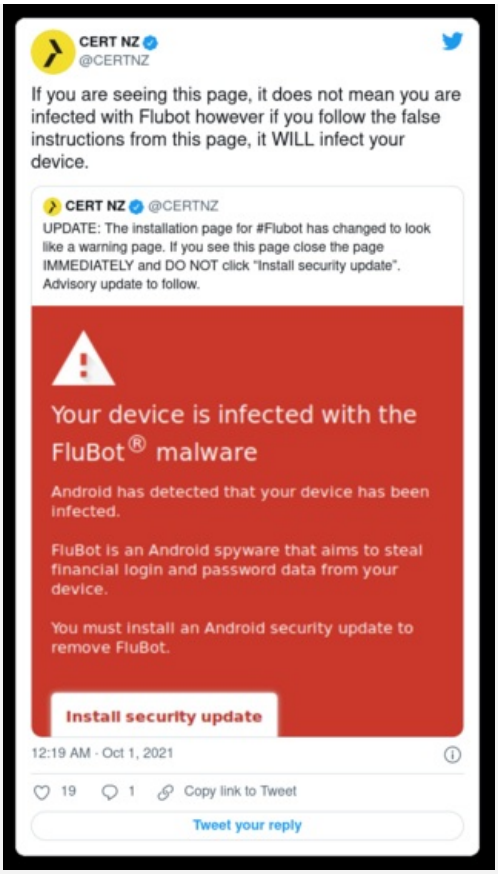
A Flubot malware nem volt előzmények nélkül, a rendelkezésre álló adatok szerint **már 2020. novemberében fertőzött Spanyolországban.** A tavaszi magyarországi kampánnyal egyidőben pedig rajtunk kívül még Lengyelországban, Németországban és Olaszországban is lecsapott. Ott és akkor levontuk a tanulságokat, miszerint **nem töltünk le kéretlen SMS-ben érkező, hivatalos piactéren kívüli alkalmazást, nem telepítjük ezeket és nem adjuk meg neki az összes létező rendszerengedélyt.**

Aki ezt mégis megtette, az egyrészt elbukta az összes személyes adatát, rossz esetben a bankszámlájához is hozzáfértek, illetve emellett járulékos kárként a telefonjáról küldözgetett SMS üzenetek díját is a károsultnak kellett állnia.



Mai történetünk viszont arra mutat rá, hogy újracsomagolva bármikor felbukkanhatnak korábbi kártevők, és a Flubot esetében sincs ez másként. Beszámolók szerint **ezúttal azzal bukkan fel kéretlenül egy üzenet, hogy a készülékünk állítólag megfertőződött a Flubot vírussal, és ahhoz hogy ezt eltávolítsuk, a kéretlen ablakban felajánlott linkre kattintva kellene egy úgynevezett biztonsági frissítést letölteni és lefuttatni.**

Ahol ugyanaz a forgatókönyv, mint a Fedex nevében elkövetett csalásnál: engedélyeznünk kellene az ismeretlen forrásból származó alkalmazások telepítését, ezeknek az összes igényelt engedély meg kellene adni - beleértve az "Accesibility services" engedélyezését is.

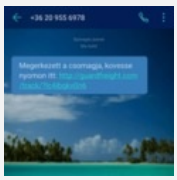


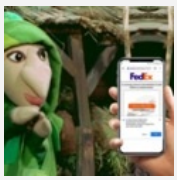
A flubot kártevő fejlesztői **elsősorban hitelesítő adatok, fizetési információk és egyéb érzékeny adatok fertőzött eszközökről történő ellopására készítették a programjukat.**

Vagyis a védekezés, megelőzés, a biztonságos környezet továbbra is a vírusvédelem + rendszeres frissítések + biztonságtudatos alkalmazás telepítés + egészséges gyanakvás elemekből áll össze, ebben nem történt semmi változás.

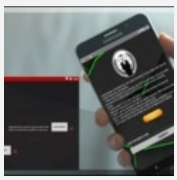
Szólj hozzá!
Címkék: mobil frissítés sms malware telepítés csalás átverés android kártevő flubot

Ajánlott bejegyzések:


Megérkezett a csomagja - vagy mégsem?


Sárkány ellen sárkányfű


Üdvözlünk Sin City-ben


Naprakész koronavírus infó, vagy mégsem?


Koronavírus spamek, hoaxok, átverések

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia-Darab István
@antivirusblog

Riasztás az interneten terjedő, zsaroló hangvételű levelekkel kapcsolatban: buff.ly/3pYqghq

5m

Csizmazia-Darab István
@antivirusblog

Remember Norton 360's bundled cryptominer? Irritated folk realise Ethereum crafter is tricky to delete: buff.ly/32YuAV8

Embed View on Twitter

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

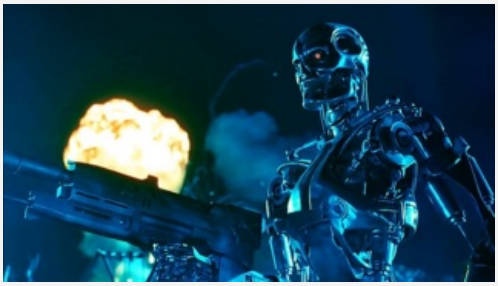
accountz

Belépés
Regisztráció

Sötét jelen: agresszív zsarolóvírusok, tömeges bruteforce

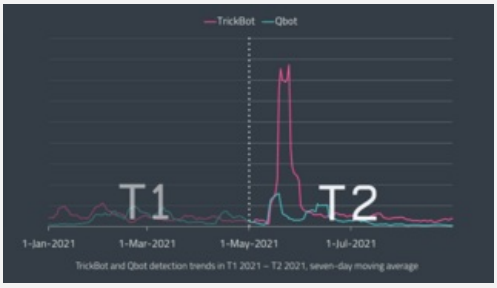
2021. október 15. 09:02 - Csizmazia Darab István [Rambo]

A kiberbiztonsági megoldásokat fejlesztő **ESET közzétette a 2021-es esztendő második harmadát vizsgáló vírusriportját**, amely összefoglalja észlelőrendszereinek legfontosabb statisztikáit és kutatási eredményeit. **Ebben több aggasztó tendenciát is kiemel, köztük a mind agresszívabb zsarolóvírus-taktikákat, az egyre intenzívebb brute-force támadásokat, valamint a gyakori megtévesztő adathalász-kampányokat, melyek tömegesen célozzák meg az otthonról dolgozókat.**



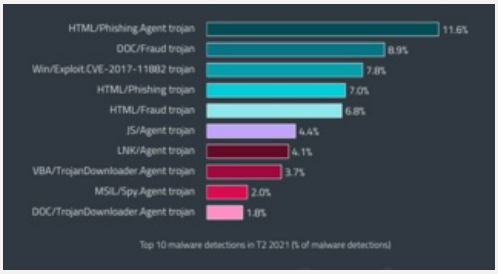
Az elmúlt hónapokban több jelentős zsarolóvírus-támadás is történt, köztük minden idők eddigi legnagyobb összegű váltságdíj követelésével. Az Egyesült Államok legnagyobb kőolajvezetékét üzemeltető vállalata, a Colonial Pipeline működését leállító támadás és a Kaseya VSA felhős IT-menedzsment szoftver sebezhetőségét kihasználó, ellátási láncot érintő támadás sokkhatása a kiberbiztonsági iparágon túl is érezhető volt.

Úgy tűnik, hogy a kiberkémkedés helyett mindkét esetben az anyagi haszonszerzés volt az elsődleges cél - **a Kaseya-támadás elkövetői 70 millió dolláros váltságdíjat szabtak meg, ami az az eddig ismert legmagasabb ilyen követelés.**



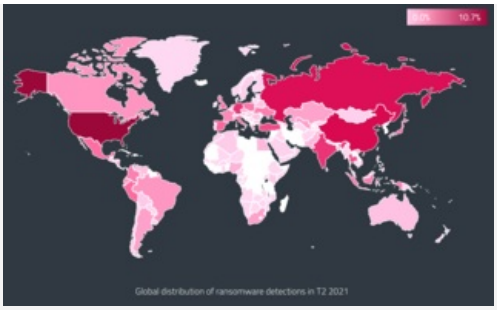
Roman Kováč, az ESET vezető kutatója szerint a zsarolóvírussal támadó bűnbandák néha hoppon maradtak, például egyes nagy hatású ügyekbe a bűnüldöző szervek is bevonásra kerültek, és ilyenkor több elkövetői csoport is váltságdíj nélkül visszavonulásra kényszerült. **Egy másik fronton meredek emelkedést lehetett tapasztalni, például a TrickBot kártevő a jelek szerint új erővel tért vissza a tavalyi leállítása után.**

Fő funkciója eredetileg a banki adatok és egyéb hitelesítő adatok ellopása volt, ám az új változat üzemeltetői számos továbbfejlesztett moduláris kártékony funkciókkal is kibővítették. **A friss statisztikában pedig már látszik, hogy 2021-ben a TrickBot már megduplázta** az ezzel kapcsolatos észlelések számát.



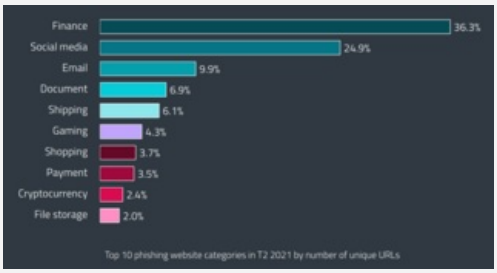
Az év második harmadában tovább nőtt a jelszófeltörő támadások száma, amelyek gyakran szolgálnak ugródeszkaszerűen a zsarolóprogramos támadások kezdeti lépéseként. A **május és augusztus közötti időszakban az ESET 55 milliárd brute-force támadást észlelt a nyilvános Távoli Asztali Kapcsolat (Remote Desktop Protocoll, RDP) szolgáltatások ellen** (ami 104%-os növekedést jelent az év első harmadához képest).

Az egyedi felhasználókra jutó átlagos napi támadások számában is elképesztő növekedést észlelt a telemetria: míg 2021 első harmadában 1392 volt gépenként a napi támadási kísérletek száma, ez a második harmadra megduplázódott, napi 2756 támadási próbálkozással.



Az év második harmadát vizsgáló vírusriport exkluzív kutatásai többek között **új jelenségekről is beszámolnak, egyebek közt a rendkívül nagy figyelmet kapó DevilsTongue kémprogrammal kapcsolatban, amelyet az emberi jogok védelmezői, disszidensek, újságírók, aktivisták és politikusok elleni kémkedésre használnak; valamint a Dukes APT csoport új adathalász** kampányáról, amely továbbra is elsődleges fenyegetést jelent a nyugati diplomaták, civil szervezetek és agytrösztök számára.

A riportban **külön fejezet ismerteti az ukrajnai kormányzati szervezeteket célzó**, rendkívül aktív Gamaredon kiberbűnöző-csoport által alkalmazott újabb támadó eszközöket.



A friss vírusriport ezenkívül egy olyan **új, többplatformos APT csoport tevékenységét is bemutatja, amely a Windows és Linux rendszereket egyaránt megcélozza**, emellett megemlít számtalan biztonsági problémát az androidos zaklatóvírus alkalmazásokban.

Továbbá terítékre kerültek a beszámolóban az IIS (Internet Information Services) szervereket célzó olyan kártevő programok is, amelyek változatos formában jelentenek biztonsági kockázatot. **A teljes, részletes vírusriport az alábbi linken olvasható.**

Szólj hozzá!
Címkék: statisztika vírus malware riport eset 2021

Ajánlott bejegyzések:

Oly távol vagy tőlem, és mégis közel

Ransomware helyzetjelentés


FinTech: az előretörés ideje

Vajon 2021-ben tovább nő a zsarolóvírusok száma?

Támadás, e-mail a neved

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

Stop adathalászat

2021. október 18. 13:46 - Csizmazia Darab István [Rambo]

A ransomware mellett a másik leggyakoribb támadási vektor az adathalászat. Bizony, ennek még Steve Jobs is bedőlt, és simán rákattintott a látszólag az Amazon weboldalának látszó linkre. **Csokorba szedtük, mik azok a tipikus jelek, amikre mindenkinek érdemes figyelnie**, hogy elkerülje adatainak le- és elhalászását.

Colonial Pipeline - van aki e nevet nem ismeri? Az idén májusban történt zsarolóvírusos kibertámadás kiinduló pontja az volt, hogy **a csővezeték felügyeletét és vezérlését a mérnökök távmunkában végezték, és az ehhez tartozó gyengén védett jelszavak illetéktelen kezekbe kerültek.**

Emiatt egy több hetes, az Egyesült Államok keleti partján jelentkező üzemanyaghiányt és hatalmas veszteséget okozó időszak vette kezdetét, ahol **a bajba került cég 4.4 millió dollárnak megfelelő (akkori áron kb. 1.27 milliárd HUF) kriptovalutát fizetett ki a bűnözőknek, részint hogy az adatait helyreállíthassa, részint pedig, hogy az ellopott bizalmas információkat a támadók ne töltsék fel** publikus weboldalakra.

A Welivesecurity cikke arra is kitér, hogy **az általuk készített adathalászat felismerő teszt kitöltési eredményei szerint jelentős különbségek mutatkoznak az életkor függvényében**. Az ESET Phishing Derby nevű weboldal statisztikája szerint **a fiatalabb, 18-24 év közötti résztvevők közül jóval többen, 47%-os eredménnyel azonosították helyesen a valódi és a csaló weboldal mintázatokat, míg ezzel szemben a 65 pluszos korosztályból már csak mindössze 28% volt az, aki ugyanezzel a feladattal sikeresen meg tudott birkózni.**

Az eredmények alapján 25-44 közti korosztály 45%-os, míg a 45-64 évesek pedig 36%-os eredményt értek el az adathalászat felismerésében.

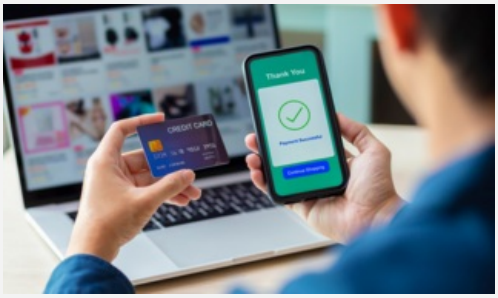
Itt a kiberbiztonság hónapja, ennek jegyében nézzük hát akkor ezek után azokat a bizonyos intő jeleket, amikkel mind a magánfelhasználóknak, mind a céges alkalmazottaknak tisztában kell lenniük. Természetesen egy háttérben futó antivírus is a segítségünkre van ebben, de mi most a szabad szemmel is jól látható elemekre fókuszálunk.

- ügyfél vagyok-e egyáltalán, amikor érkezik egy kéretlen megkeresés? Sokan ennek hiányában is kattintanak kíváncsiságból, figyelmetlenségből

- a kéretlen üzenet nem egy kizárólag csak nekünk szóló levél, hanem egy tömegesen kiküldött körlevél (Undisclosed Recipients), aminek rajtunk kívül még számtalan címzettje van

- nyelvtani és helyesírási hibákkal van tele a kéretlen levél. Ezek sokfélék lehetnek, kezdve az ékezetek hiányától, a tegezés és magázódás váltogatásától kezdve a Tuskó Hopkins, Török Szultán és Fülig Jimmy féle helyesírásig, ami gyakran valamilyen nyersfordítás, pl. Google Translate eredménye

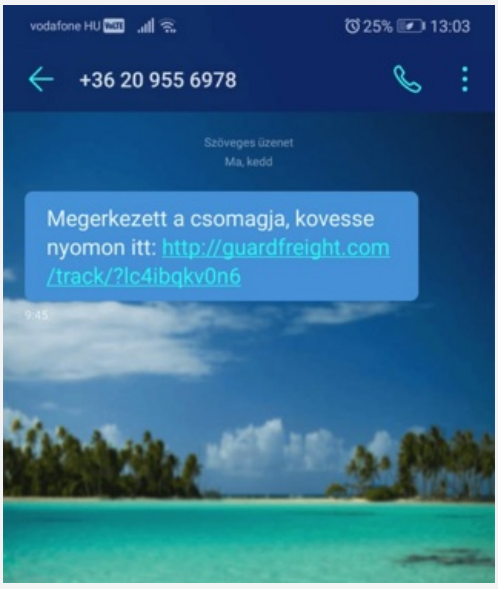
- sürgetés, ijesztgetés - ez is egy gyakori jelenség, hogy állítólagosan be nem fizetett számla miatt felszólítás érkezik, vagy zárolják a számlánkat, ha nem lépünk azonnal. Ebben egy jó adat social engineering, azaz megtévesztés, pszichológiai nyomás alkalmazása is rejlik, ugyanis a statisztikák azt bizonyítják, hogy a pánikoló felhasználó hajlamos gyorsan rosszul dönteni: kattint, fizet, személyes adatot megad, csak hagyják békén, oldódjon meg gyorsan a nem is létező probléma.



- nem is az a valódi feladó - mindig alaposan meg kell nézni, ki küldte az adott üzenetet. Ha már a domén név sem stimmel, akkor nyugodtan törölhetjük a kéretlen üzenetet, de érdemes azt is megnézni, nincs-e benne szándékos hasonmás betűhiba (typosquatting), vagy más idegen nemzetiségű karakterből álló (például az orosz ABC betűiből) hamis domén (homograph)
https://antivirus.blog.hu/2021/06/29/hol_jarsz_hova_mesz

- mellékelt linkre való kattintást kérnek - itt is érdemes a fentiek alapján ellenőrizni, illetve sose kattintsunk mellékelt linkre, ha az kéretlenül érkezik. Ez jó esetben csak valamilyen reklám oldalra, űrlap kitöltögetésre visz, rossz esetben kártékony weboldalra, amely lehet adathalász oldal, vagy vírust tartalmazó hivatkozás.
https://antivirus.blog.hu/2021/05/13/a_mint_adathalaszat

- fertőzött fájlmellékletet kapunk - ez is egy gyakori forgatókönyv, például számlának hazudva. A melléklet pedig lehet .EXE, .PDF vagy valamilyen Microsoft Office formátumú állomány. Ha kéretlenül jön, akkor nem szükséges rákattintani. Gyakori módszere a bűnözőknek, hogy magából a levélből ne derüljön ki semmi, hanem a mellékletre hivatkoznak, hogy ott kapjuk meg az érdemi információt. A valóság pedig, hogy ezek többnyire olyan preparált, sebezhetőséget tartalmazó fájlok, amik révén megfertőzhetik a számítógépünket. Jó ötlet, ha gyanakszunk, akkor bedobni a kérdéses fájlt a Virustotal oldalára, ahol 70 különféle antivirus motor vizsgálja párhuzamosan az állományt.



Sajnos sokan bedőlnek ezeknek a kísérleteknek, gondoljunk csak az idei márciusi Fedex nevével visszaélő csalásra. Ott kéretlen SMS-ben kaptak sokan "Megerkezett a csomagja, kovesse nyomon itt: http://akarmi..." üzenetet, **melyre rákattintva kártékony alkalmazást telepítettek a telefonukra, a kért engedélyeket gondolkodás nélkül megadták, és ezzel anyagi kárral is járó adatlopást, fertőzést szenvedtek el.**

Pedig az adathalászat felismerése, megelőzése korosztálytól függetlenül mindenkinek feladja a leckét, és jó lenne, ha ebben mindenki azt mondhatná: Tanár úr kérem, én készültem.

1 komment
Címkék: tippek jelek phishing adathalászat adatlopás adatszivárgás welivesecurity.com

Ajánlott bejegyzések:

[Ingyenes Omikron teszt vagy mégsem?]

[Hol jársz, hová mész?]

[Ha eljön a személyiségtolvaj]

[A bankos mindig kétszer csenget...]

[Megint jőnek, szivárogtatnak...]

Kommentek:

gigabursch 2021.10.18. 17:34:54

S akkor a telefonos műsort ne hagyjuk ki.
Lásd: Személyiség tolvaj.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

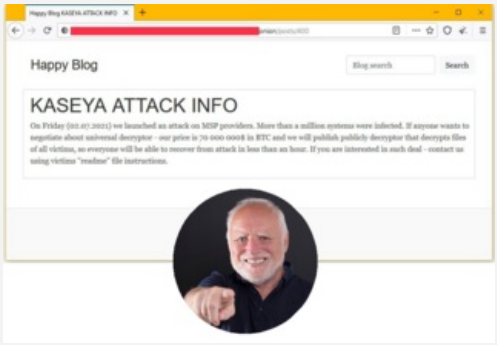
accountz

Belépés
Regisztráció

Offline mennyország - egy rövid időre

2021. október 26. 14:14 - Csizmazia Darab István [Rambo]

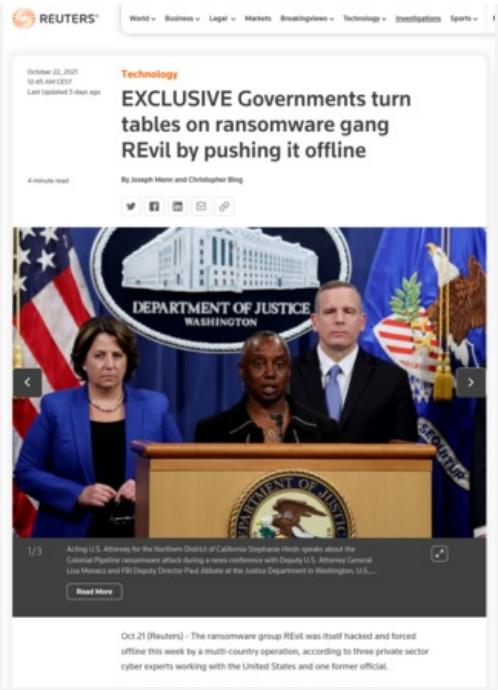
Megkönnyebbülést érezhetnek a ransomware fenyegetések miatt a felhasználók, **pár napja ugyanis elnémult a híres-hírhedt REvil bűnözői csoport**. Eddig csak találgatások voltak az okokról, ám **időközben már a miértekre is fény derült.**



Hatalmas horderejű, mindennapi életünkre is **jelentős hatású, valamint elképesztő mértékű követelt váltságdíj jellemezte** azokat az utóbbi időben bekövetkezett zsarolóvírus támadásokat, amelyek sok ember életét keserítették meg.

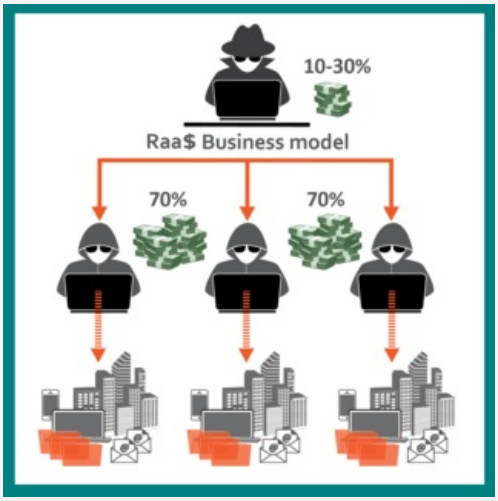
A Colonial Pipeline csővezeték rendszere elleni incidens hosszú leállást, és **pánikszerű üzemanyaghiányt okozott az USA keleti partján**, a JBS húsfeldolgozót (11 millió dollárnyi követelt váltságdíj) célzó támadás következménye szintén **áruhiány és ellátási nehézségek lettek**, míg a **Kaseya felhőalapú távmenedzsment szolgáltató egy szintén egy hosszas leállást** okozó ransomware támadással volt kénytelen szembenézni. A Colonial Pipeline (4.4 millió dollárnyi követelt váltságdíj) és a Kaseya (70 millió dollárnyi követelt váltságdíj) esetében is az elkövető a REvil banda volt.

Amint az a friss beszámolókból kiderült, nemcsak a korábbi Happy-blog vált elérhetetlenné október 17-étől, hanem **a bűnüldöző szerveknek ezen a héten sikerült hozzáférniük a REvil számítógépes hálózati infrastruktúrájához, és ezen szerverek felett részleges irányítást tudtak szerezni.**



A REvil bűnbanda már korábban is eltűnt egy időre, legutóbb júliusban tartottak egy rövidebb szünetet. **Visszatérésükkor erőteljes, agresszív terjeszkedésbe kezdtek, például 90%-os jutalék felajánlása és hasonló gyanús jelek mutatkoztak, melyeket a biztonsági szakemberek is furcsának találtak.**

Később jött aztán az a hír, amely szerint egy rejtett hátsóajtót tartalmaz a bérbe adott kártevő, amelyen keresztül a REvil fejlesztők a jelentős váltságdíj fizetéssel kecsegtető zsarolások végjátékát egyszerűen elveszik a bérlő bűnözőktől, és ezzel hoppon maradtak a RaaS ügyfelek. **Akiket persze nem sajnálunk, de a modell hitelességét és jövedelmezőségét így a bűnözői oldalon is sokan elkezdték megkérdőjelezni.**

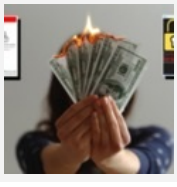


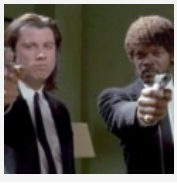
Lényeg a lényeg, ugyan egyelőre egy oroszországi zsarolóvírus csapattal most kevesebb van, de a többi banda ilyenkor szokás szerint idővel átveszi a helyeket, jelen esetben a DarkSide csoportnál látni erőteljes pénzmozgásokat. **Az sajnos viszont biztos, hogy amikor nem tartóztatnak le senkit, és csak időlegesen tudnak irányítást átvenni bizonyos kártékony szerverek felett, az nem jár végleges győzelemmel, és az akciót csak átmeneti sikerként könyvelhetjük el.**

A REvil most látszólag kiszállt, később vissza is térhetnek mondjuk új néven, meg más is helyükre léphet, sőt ez így együtt is lehetséges. Addig is marad nekünk felhasználói oldalon a vírusvédelem, a rendszeres frissítés, az alapos konfigurálás, a rendszeres adatmentés és hasonló megelőző jellegű lépések.

Szólj hozzá!
Címkék: offline fellépés váltságdíj revil ransomware hatósági pipeline raas colonial zsarolóvírus kaseya

Ajánlott bejegyzések:


A Kaseya három napja | Fejemen olvad a vaj, engem nem érhet baj | Fizess vagy einstandoljuk a kőolajvezetékedet! | Váltságdíjat kínálnak a váltságdíjszedő kandáért | Kik, hol és mire költik a beszedett váltságdíjainkat?

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

- RSS 2.0
  bejegyzések, kommentek
- Atom
  bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

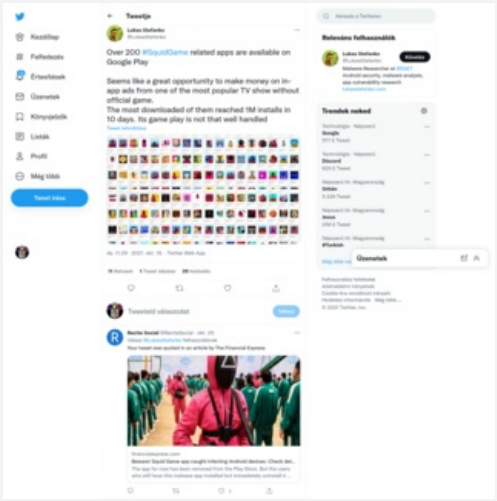
Nyerd meg az életed - vagy mégsem?

2021. október 28. 10:58 - Csizmazia Darab István [Rambo]

A Netflixen futó és felkapottnak számító **Squid Games sorozat** **a kártevőterjesztők figyelmét is felkeltette. Érdemes óvatosnak lenni a Google Playen, és egyéb helyeken.**

Mindig van valamilyen apropó - legyen az lezuhant maláj repülőgép, olimpiai játékok, földrengés, cunami, robbantás egy maratonfutáson vagy bármi - kis késéssel máris megérkeznek a hírt meglovagló átverések, csalások, számítógépes kártevők.

Nincs ez másként most sem, és az androidra telepítendő programok esetében most sem árt a biztonságtudatos hozzáállás, hogy ki tudjuk szúrni a gyanús appokat.



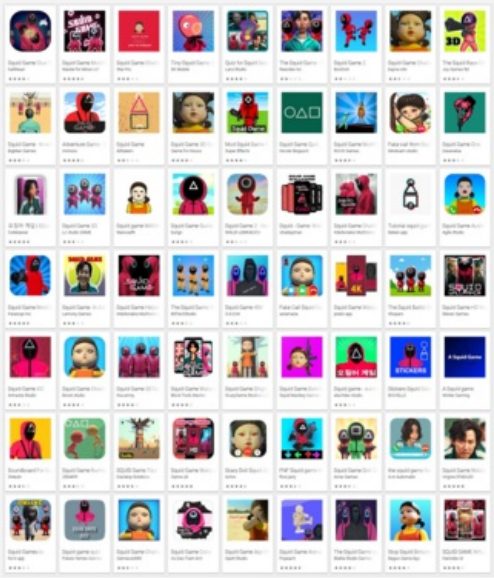
Lukas Stefanenko, az ESET szakértője hívta fel a figyelmet egy Twitter posztban arra, hogy már 200 felett találhatók különféle, az elnevezésben a Squid Gamesre hivatkozó alkalmazások, amelyek játékok, háttérképek és hasonlók, ám köztük számos applikáció kártékony volt.

Például az egyik **"Squid Wallpaper 4K HD" nevű háttérkép program a már 2016 óta ismert Joker kártevőt** tartalmazta.

A Joker egy elég alattomos kártékony kód, látszólag legitim alkalmazásban rejtőzik, ám a telepítés után titokban beregisztrálja a felhasználókat különféle drága előfizetési szolgáltatásokra, emellett képes ellopni az SMS-üzeneteket, a partnerlistákat valamint a részletes eszközadatokat is.

Sajnos ezek a próbálkozások évről évre rendszeresen elő szoktak fordulni, **általában egy már a Google Play kínálatában szereplő korábban tiszta alkalmazás rosszindulatú frissítésében, de sok esetben más, egyéb**

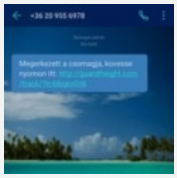
ellenőrizetlen piactér, illetve letöltési oldal kínálatában.



A legjobb amit tehetünk, ha használunk valamilyen vírusvédelmet az androidos eszközeinken is, maradunk az ellenőrzöttebb hivatalos piactéren, de még ott is odafigyelünk arra, pontosan mit telepítünk, mire adunk engedélyeket, és mindig átgondoljuk, hogy érkezett-e egyáltalán csomagunk, meg minden ilyesmi ;-)

Szólj hozzá!
Címkék: squid meg az vagy joker twitter games trójai android eset mégsem életed vagymégsem lukas nyerd stefanenko

Ajánlott bejegyzések:



Megérkezett a csomagja - vagy mégsem?

Ingyenes Omikron teszt vagy mégsem?

COVID-19 nyomkövető vagy mégsem?

Duplázd meg a pénzedet - vagy mégsem?

Unortodox támadások jönnek

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

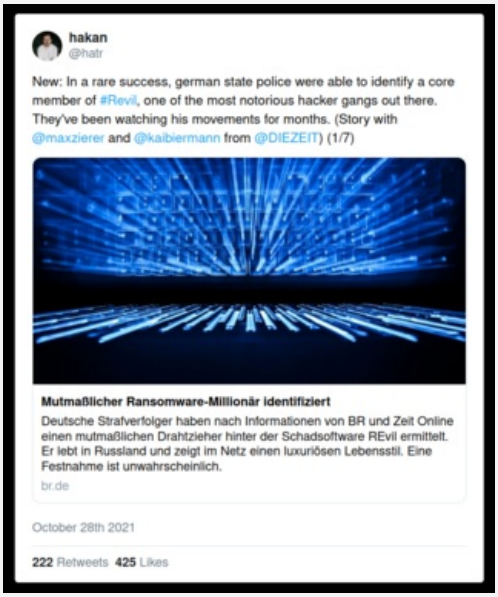
Kik, hol és mire költik a beszedett váltságdíjainkat?

2021. november 02. 15:59 - Csizmazia Darab István [Rambo]

Érdekes beszámoló jelent meg a német sajtóban arról, hogy **a REvil banda egyik beazonosított tagja milyen életszínvonalon éli a mindennapjait - köszönhetően** a zsarolóvírus biznisz gigantikus bevételeinek.

A Nikolay K-nak nevezett illető a REvil tagja, amely bűnözői csapathoz olyan korábbi kiemelkedő ransomware támadások köthetők, mint a JBS Húsfeldozó, az Apple, illetve a Kaseya elleni incidens. A Bayerischer Rundfunk és a Zeit Online riporterei hónapokat töltöttek el a gyanúsított digitális nyomainak felkutatásával. **Ezalatt találtak például olyan érintett kriptovaluta számlát, amelyre a vizsgált időszak alatt hat részletben több mint 400 000 eurót (144 millió forintnyi összeget) utaltak Bitcoinban.**

A német rendőrség állítólag tisztában van a gyanúsított valódi személyazonosságával és pontos tartózkodási helyével, amely valahol Dél-Oroszországban van. Nikolay ott egy úszómedencés házban él, egy drága BMW autóval közlekedik, és a 70 ezer eurós (kb. 25 millió forintos) karóra virít a csuklóján.



Korábbi nyaralásait sem aprózta el, a közösségi oldalak tanúsága szerint olyankor napi 1300 euróért bérelt jachtot (közel félmillió HUF), ötcsillagos szállodákban fordult meg Dubajban, a Maldív szigeteken vagy éppen a törökországi Antalyán. **A gyanúsított az interneten büszkélkedett vagyonával, és jelenleg kriptovaluta befektetőnek adja ki magát.** A német hatóságok már hónapok óta figyelik, és lenyomozták a személyazonosságát, amely egyértelmű kapcsolatot mutatott az illető és a REvil banda tevékenysége között.

A stuttgarti rendőrség abban bízik, hogy egyszer kimozdul a Krim-félszigetről, és egy olyan, Németországgal érvényes kiadatási szerződéssel rendelkező országba utazik majd, ekkor végre vádat emelhetnek majd ellene.

Sajnos igen ritka, hogy valódi nagyhalak letartóztatására is sor kerüljön. Bár időnként történnek kisebb súlyú őrizetbevételek, sokszor csak a közvetlen végrehajtók, egyszerű közreműködők akadnak fenn a rostán.

Az október 17-i REvil szerver lelövésekor például az egyik vezetőjük, 0_neday idejében észlelte az ellenük indított

akciót, azonnal felismerte a veszélyt, és nyomban háttérbe vonult az XSS fórumbeli posztja után. **Várhatóan Nikolay K is lesz annyira óvatos, hogy ezek után esze ágában sem lesz egyhamar elhagyni Oroszország területét.**

1 komment
Címkék: banda nyomozás váltságdíj gyanusított revil ransomware nikolay kriptovaluta zsarolóvírus

Ajánlott bejegyzések:


A Kaseya három napja


Váltságdíjat kínálnak a váltságdíjszedő bandáért

Offline mennyország - egy rövid időre


Amikor a hóhért akasztják...

Ransomware helyzetjelentés

Kommentek:

ROTFL Manó 2021.11.03. 20:22:07

Az válTságdíj, nem válságíj!

Ráadásul a hibás címet a Zindex főoldala is átvette.

(A válságdíjjat a FED költi el...)

:-D

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

VVV 25.
VVV 26.
VVV 27.
VVV 28.
VVV 29.
VVV 30.
VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

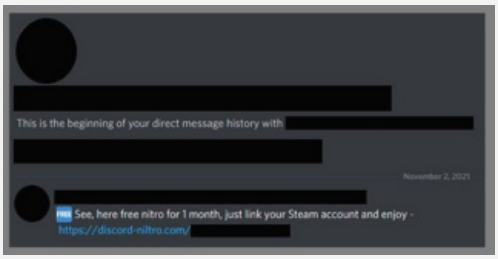
Adathalászat a Discordon

2021. november 04. 12:44 - Csizmazia Darab István [Rambo]

Nem kivételek a játékplatformok, sem a legnépszerűbb játékos chat alkalmazások, itt is simán belefuthatunk átverésekbe, mindenféle csalásokba.

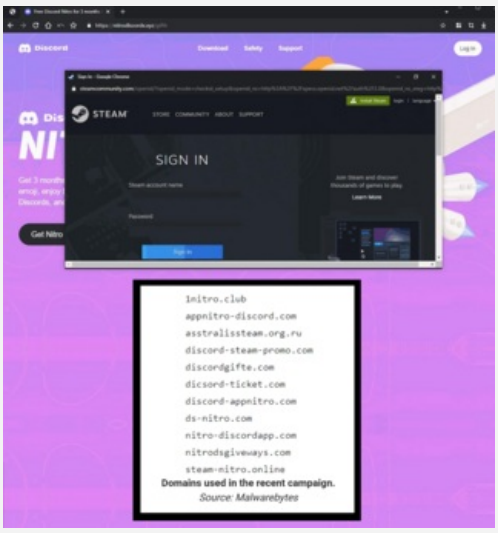
A Discord Nitro a chat szolgáltatás extrákkal ellátott fizetős prémium szintje rendszeres felhasználók számára. **A mostani csalás ingyenes Nitro előfizetést ígér csaliként, és arra igyekszik rábírni a gyanútlan áldozatot, hogy kapcsolja össze Discord és a Steam fiókját.**

***"Nézd, itt egy ingyenes egy hónapos nitro, csak írd be a Steam belépésed és élvezd azonnal!"* - szól az üzenet, és ehhez "természetesen" egy adathalász linket is felkínál.** Promóció helyett azonban ha valaki a hamis Steam belépési oldalba begépeli az accountját, akkor az adatok rögtön mennek a csalók szerverére.



A Bleeping Computer és a Malwarebytes is beszámolt erről a phishing támadásról, ahol **a csalók egy érdekes módszerrel furmányosan még arról is gondoskodtak**, hogy a hamis oldalon a belépési adatok első begépelésekor egy kamu hibaüzenet jelenjen meg arról, hogy a fióknév vagy a jelszó helytelen, majd újra bekérik a név-jelszó páros beírását.

Ezzel mintegy minőség-ellenőrzik, nem történt-e véletlen gépelési hiba a számukra értékes adatok megadásakor.



Így a sokadik adathalász támadásnál már illik észrevenni a jellegzetes szokásos jeleket. Csali: ingyenes valami ígérete, vagy fenyegetés, hogy egy meglévő valamink elveszik, zárolják, stb. Mellékelt linket adnak: a kéretlen üzenet a "gyors ügyintézés érdekében" kattintható hivatkozást is mellékel, így ha valaki siet, figyelmetlen, nyerni akar, akkor erre gyorsan kattint, ám ezzel már robog is ezerrel az adathalász hasonmás oldalra.

Egy korábbi posztunkat most belinkeljük, ahol minden adathalászatra utaló intő jelet, gyakori módszert és

megelőzési tippet szép részletesen felsorolunk.

Megosztom tumblr. Tweet Pin it Tetszik 0

Szólj hozzá!
Címkék: kampány csalás átverés nitro steam phishing adathalászat jelszólopás discord

Ajánlott bejegyzések:

A bankos mindig kétszer csenget...

Ingyenes Omikron teszt vagy mégsem?

Vakcinás csalások, szevasztok

A csaló számlák helyes időzítéséről

Facebook egyperces

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Váltságdíjat kínálnak a váltságdíjszedő bandáért

2021. november 09. 15:28 - Csizmazia Darab István [Rambo]

Napjaink egyik legelterjedtebb támadási formája a ransomware. Ha döcögősen is, **de elindult egyfajta nemzetközi összefogás a legkártékonyabb csapatok kiszorítására**, ezek egyike a DarkSide.

Ha azt nézzük, honnan lehetnek ismerősek, akkor rögtön beugrik a Colonial Pipeline csővezeték elleni idén májusi támadás.

Itt egy **több hetes, az Egyesült Államok keleti partján jelentkező üzemanyaghiányt és hatalmas veszteséget tudtak okozni az elkövetők, és a cég végül kifizette a 4.4 millió dollárnyi** (akkori áron kb. 1.27 milliárd HUF) váltságdíjat.

Felmerült aztán, hogy tesz-e Oroszország a feltételezett orosz elkövetők ellen lépéseket, és mindez **szóba került júliusban Joe Biden és Vlagyimir Putyin közti beszélgetés során is.**

Míg végül októberben a bűnüldöző szerveknek sikeresen leállították a REvil zsarolóvírus banda szervereit, és ezzel **egy látványos ellencsapást mértek a bűnözőkre.**

Most pedig tovább emelik **az amerikai hatóságok a tétet: 10 millió dollárt ígérnek** a nyomravezetőknek a DarkSide ransomware bandavezérekkel kapcsolatos információkért.

A Külügyminisztérium közleménye szerint minden olyan személyekről szeretnének információt kapni, **akik kulcsfontosságú vezető szerepet tölthettek be a DarkSide ransomware nemzetközi szervezett bűnözői csoportban.**

További részeredménynek számít, hogy júniusban az ukrán és a dél-koreai rendőrség segítségével fél tucat embert letartóztattak azzal a gyanúval, hogy a Cl0p ransomware banda tagjai voltak. Az Interpol akkori akcióját **30 hónapos nyomozás előzte meg, és az Europol mellett vírusvédelmi cégek is segítettek** a nyomok felderítésében.

Nehéz megtippelni, mennyire lesz hatékony az egységes nemzetközi fellépés, de annak mindenesetre örülni lehet, hogy legalább elkezdődtek az ilyen országhatárokon átívelő koordinált ellenakciók.

Szólj hozzá!
Címkék: fbi csapat letartóztatás nemzetközi interpol fellépés banda bűnbanda váltságdíj darkside europol ransomware zsarolóvírus

Ajánlott bejegyzések:

Kik, hol és mire költik a beszedett váltságdíjainkat?

Offline mennyország - egy rövid időre

Tesz-e Oroszország a ransomware ellen?

Fizess vagy einstandoljuk a kőolajvezetékedet!


Felebarátod váltságdíját ne kívánd!

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Gyermek + okosóra = biztonság?

2021. november 11. 14:38 - Csizmazia Darab István [Rambo]

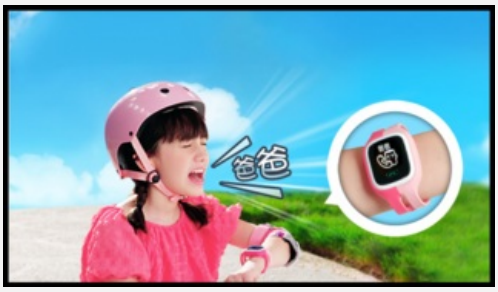
"Szólj, ha megérkeztél". Olyan mondat ez, amelyet minden gyerek hallott már a szüleitől attól függetlenül, hogy iskolába, edzésre, különórára, a barátaihoz vagy a nagyszüleihez ment éppen. **Ma már a digitális vívmányok rengeteg lehetőséget kínálnak arra, hogy aggódó szülőként nyomon követhessük gyermekeink aktivitását. Ilyen az okosóra is, amely a biztonság elősegítése mellett sajnos néha veszélyforrást is jelenthet a gyerekek számára.**

Egyre több szülő dönt az okosóra vásárlás mellett. Nem meglepő, hiszen segítségükkel nyomon követhetjük gyermekeink tartózkodási helyét, kommunikálhatunk is velük, lényegében - digitális formában - velük lehetünk mindenhol. A biztonsági programokat fejlesztő ESET szakemberei szerint viszont egyáltalán nem mindegy, hogy milyen eszközt választunk erre a célra.

Mire érdemes figyelni, ha okosóra vásárláson gondolkodunk? A tervezett vásárlás előtt érdemes alaposan tájékozódni az adott termékről. Nem csak az óra tudása, hanem **a biztonságos működést biztosító funkciók megléte is kulcsfontosságú**, ezt általában csak a közepes és magasabb árfekvésű termékek tartalmazzák.

Az alábbi jó tanácsok segítségével nagyobb eséllyel választhatjuk ki a legbiztonságosabb termékeket.

1. Gyűjtsünk információt!
A felhasználói vélemények mindig nagy segítséget jelenthetnek, ha egy termék megbízhatóságáról szeretnénk visszajelzést kapni. Keressünk rá a márkanévre, sőt a modell nevére, és illesszünk mellé olyan szókapcsolatokat, mint például a "biztonsági rés", hogy megtudjuk, milyen biztonsági funkciókat tartalmaz.



2. Járjunk utána, hogy a gyártó mennyire tartja fontosnak a kiberbiztonság kérdését!
Amennyiben az eszköz és a szerver közötti kommunikáció nem titkosított, akkor tartózkodjunk a termék megvásárlásától. Az okosórák szerverekkel vannak összekötve. **Azonban, ha az eszközök nem rendelkeznek megfelelő biztonsági háttérrel, a hackerek könnyedén hozzáférhetnek a gyermekekkel kapcsolatos információkhoz. Még az is előfordulhat, hogy a biztonsági réseket kihasználva a kiberbűnözők egyenesen a gyerekekkel veszik fel a kapcsolatot.** Így a védelmük és biztonságuk helyett éppen az ellenkezőjét érjük el, és kockázatnak tesszük ki a legkisebbeket.

2019-ben kiderült, hogy az SMA-WATCH-M2 okosórát gyártó kínai cég több mint 5000 gyermek adatait tette hozzáférhetővé világszerte annak következtében, hogy nem fordított kellő figyelmet saját szervereinek

biztonságára. A kiszivárgott adatok alapján rekonstruálhatóvá váltak kiskorúak, többek között egy 10 éves német lány, Anna mindennapi szokásai is. A hiba miatt a GPS meghatározás alapján nem csak az általa használt útvonalakat, hanem a pontos lakcímét is ki lehetett deríteni. Ez sajnos nem egyedi eset, 2019 elején ugyanis az Európai Bizottság még a Safe-KID-One okosóra visszahívását is elrendelte, szintén hasonló adatvédelmi és biztonsági aggályok miatt. Érdemes tehát figyelmesen elolvasni a gyártó honlapján található adatvédelmi szabályzatot, utánajárni az adott márkának, és az ahhoz köthető vállalatról is minél többet megtudni.

3. Keressünk biztonsági réseket!
Fontos azt is megvizsgálnunk, hogy történt-e adatvédelmi incidens a termékkel vagy a gyártó céggel kapcsolatban. Amennyiben igen, sokat elárul a cégről, hogy miként reagált a visszaélésekre. Jó jelnek bizonyul, ha a cég körültekintően járt el, elismerte és átlátható módon kommunikált az incidensekkel kapcsolatban.

Mivel a biztonsági résekkel való visszaélés viszonylag gyakran fordul elő elengedhetetlen, hogy a gyártó képes legyen gyorsan reagálni ezekre. **Fontos továbbá, hogy a kiszemelt szoftver frissíthető legyen, és a vállalat rendszeresen biztosítsa ennek lehetőségét.** Ennek hiányában inkább válasszunk másik terméket vagy márkát.

4. Nézzük a márkanevet!
Tartózkodjunk a kevésbé ismert márkák vásárlásától, ha nem tudjuk ellenőrizni, miként védik adatainkat, illetve hol tárolják (hová töltik fel) ezeket. Ugyan spórolhatunk egy olcsóbb eszköz vásárlásával, azonban ezzel azt kockáztatjuk, hogy a későbbiek során illetéktelenek kezébe kerülhetnek az adataink.

Az olcsó okosórák gyakran gyenge minőségűek, a technikai paraméterek terén egy elvárható szakmai minimum sem teljesül bennük, **sőt komoly adatvédelmi aggályok is felmerülnek velük szemben. Például teljesen szét kell szedni őket a SIM kártya behelyezéshez, de a biztonsági funkciók is sokszor teljesen hiányoznak ezekből a gyengébb termékekből. Ez gyakorlatilag azt jelenti, hogy titkosítatlan, bárki által olvasható clear textben** utaznak a bizalmas információink, jelszavaink a neten.

5. Mindig frissítsük az eszközt!
A gyártó mellett nagyon fontos, hogy mi is rendszeresen frissítsük az eszközön található szoftvert! A biztonsági frissítések különböző hibajavításokat is tartalmaznak, amelyek igyekeznek biztonságosabbá tenni az eszközöket. Ha ezt nem tesszük meg, a hackerek kihasználhatják a javítatlan biztonsági réseket és hozzáférhetnek a készüléken lévő adatokhoz.

6. Fontoljuk meg, milyen funkciókra van szükségünk!
Szeretnénk okosórán keresztül kommunikálni, esetleg videó- vagy telefonhívást is kezdeményeznénk gyermekünkkel? Ezesetben keressünk olyan eszközt, amely beépített kamerával, hangszóróval és mikrofonnal is rendelkezik.

Esetleg elég lehet egy egyszerű SOS segélyhívó funkcióval ellátott modell is, amely vészhelyzetben felveszi a kapcsolatot az általunk előre meghatározott személlyel? **Mennyire fontos számunkra a "geofencing", azaz a biztonsági zónák kijelölése? Ezzel a funkcióval értesítést kaphatunk arról, ha gyermekünk elhagy egy bizonyos területet (pl. iskolát).**

Mielőtt okosórába fektetünk, alaposan gondoljuk át, hogy milyen szintű kontrolt szeretnénk a segítségével gyakorolni. Tartsuk szem előtt, hogy minél több funkcióval rendelkezik egy okosóra, annál kevesebb időt fog kibírni az akkumulátora töltés nélkül. Míg egyes modelleket szinte minden nap fel kell tölteni, addig más készülékek akár hetekig is használhatók feltöltés nélkül. Gondoljunk arra is, hogy minél több lehetőséget kínál egy adott eszköz, annál több biztonsági rés keletkezhet rajta, ami potenciális veszélyforrást jelenthet, és megkönnyítheti a kiberbűnözők hozzáférését az adatokhoz.

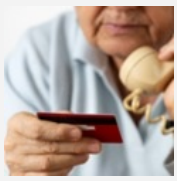
Ha olyan okosórára esik a választásunk, amely számos fejlett funkcióval rendelkezik, bizonyosodjunk meg arról is, hogy megfelelő biztonsági szinttel és rendszeres hibajavító frissítésekkel rendelkezik. Összességében tehát az okosórák nagy segítséget jelenthetnek, ha helyesen választunk. Szülőként sok szempontot kell mérlegelnünk, és minél több időt szánunk erre, annál nagyobb a valószínűsége, hogy a leginkább megfelelő eszközt találjuk meg gyermekünk számára.

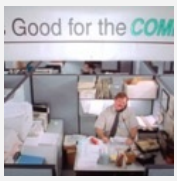
Szólj hozzá!
Címkék: vásárlás biztonság választás szülő gyermek okosóra smartwatch

Ajánlott bejegyzések:


Amazónia veszélyes ragadozói ;-)

8 tipp az online vásárláshoz


A bankos mindig kétszer csenget...



Karácsonyi vásárlás biztonságosabban


Kiberkockázatok - miért nehéz velük lépést tartani?

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

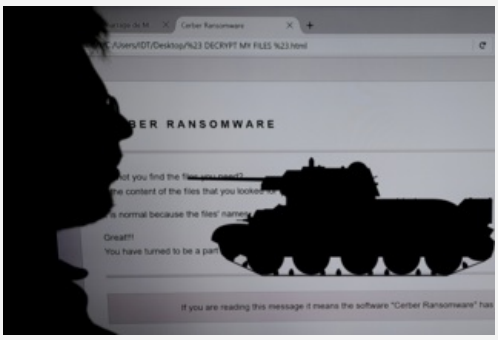
accountz

Belépés
Regisztráció

Ez most vajon akkor milyen ware?

2021. november 16. 10:31 - Csizmazia Darab István [Rambo]

A klasszikus ransomware, azaz zsarolóvírus definíciója szerint ezek olyan kártékony szoftverek, melyek zárolják az eszközöket, titkosíthatják az eszközökön lévő adatokat annak érdekében, hogy váltságdíjat csikarjanak ki a felhasználótól. A doxing képében pedig az alapképletet megfejelve újabban már az is a fenyegetés része, hogy nemfizetés esetén bizalmas adatokat szivárogtatnak. **Na de mi van olyankor, ha egyáltalán nem is kérnek pénzt?**

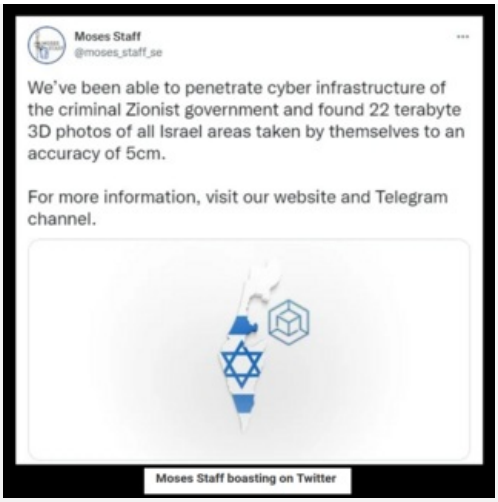


Darwin díjas ransomware témakörben már szerepelt egyszer egy összefoglaló. Ezek azok az esetek voltak, ahol a kártevő készítő tervébe valamilyen hiba csúszott. Ezek egyike például a 2015-ös Power Worm zsarolóvírus, amely Windows alá készült. Bár az adatokért cserébe 2 Bitcoint kértek, de egy programozási hiba következtében ezt ha akarták volna, sem tudták megtenni.

Ugyanis **hibásan volt megírva a zsaroló program, emiatt a mégis fizetőknek sem volt lehetőségük adataik visszanyerésére. Ráadásul a kártevő elemzésekor a biztonsági kutatók azt észlelték, hogy az eredetileg csak Microsoft Word és Excel állományokat veszélyeztető kártevő hibás titkosító algoritmusa miatt számtalan más fájlkiterjesztést is elkódolt a helyreállítás esélye nélkül**.

Ugyancsak hasonló digitális harakirivel ért fel 2016-ban a GitHubról származó RANSOM_CRYPTEAR.B egyik átirata, az úgynevezett "Hidden Tear" is, de szintén a helyreállításra esélyt sem adó támadás volt a 2017-es BTCware/Nuclear incidens is.

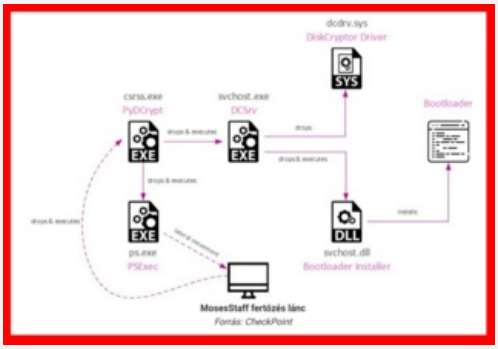
Ahol szintén a bűnözői oldal programozási hibájából adódóan a 10 MB méret feletti állományoknál egyáltalán nem működött a helyreállító kulcs, így garantált volt az adatvesztés.



Moses Staff boasting on Twitter

Mostani esetünkben is jelen van az adatokba való agresszív belegyalogolás, vagyis itt az elkódolás, titkosítás nem azért történik, hogy majd az áldozat esetleg fizessen, hanem **a masszív célzott károkozás a motiváció, a helyreállítás esélye nélkül. Ezúttal egy új hackercsoport, a Moses Staff vállalta a felelősséget számos, a közelmúltban izraeli szervezetek elleni támadásért. Mivel a szándék a rongálás volt, így joggal feltételezhető a politikai motiváció.**

A támadók az elmúlt hónapokban több olyan támadást hajtottak végre, amiben beszivárogtak izraeli rendszerekbe, ott elkódolták az adatokat, de mindezt váltságdíj követelés nélkül, ám az ellopott másolatokat rosszindulatúan kiszivárogtatták a nyilvánosságnak.



Szakértők úgy találták, hogy **a titkosítást egy a GitHubról származó PyDCrypt nevű program egyéni átiratával végezték**. Az alapos elemzés szerint a támadók nem igazán voltak profik, így szerencsére **a titkosított fájlok bizonyos körülmények között mégis visszaállíthatók**, mivel a titkosítási séma szimmetrikus kulcsgenerálást használ.

Politikai célok bár viszonylag **ritkán, de azért már többször is előfordultak a kártevő történelemben. Ilyen volt például a 2015-ös Potao incidens**, ahol egy oroszországi weboldal trójaival fertőzött TrueCrypt fájl- és lemeztitkosító szoftvert terjesztett, amivel ukrán tisztviselők és újságírók után kémkedtek.

De **a hírhedt 2010-es Stuxnet is kifejezetten politikai célzattal készült, ott a cél az iráni Bushehr atomerőmű urániumdúsító berendezéseinek szabotálása volt**. A kártevőt az USA és Izrael közösen fejlesztette ki, és a sikeres támadás után 2010. novemberében Irán leállította az urándúsítóit, miután a centrifugák 20%-a leégett, megsemmisült.

Szólj hozzá!
Címkék: izrael incidens politikai támadás adatszivárgás ransomware zsarolóvírus adatrombolás

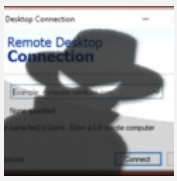
Ajánlott bejegyzések:


Te nem kapod vissza, de mindenki más igen

"Illetéktelen fél korlátozott ideig hozzáférhetett fájlokhoz"


Persze hogy tudtam, csak nem sejtettem...

Van másik!



Felkészülés meghatározatlan ideig tartó RDP-re

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker

2. A Gmail-es jelszavak kiszivárgása
3. Lakásvásárlás, de csak ha OTP-s vagy
4. Túlélési tippek Windows XP-hez
5. Társkeresős csalások szevasztok

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

Mindent IS visz...

2021. november 18. 11:44 - Csizmazia Darab István [Rambo]

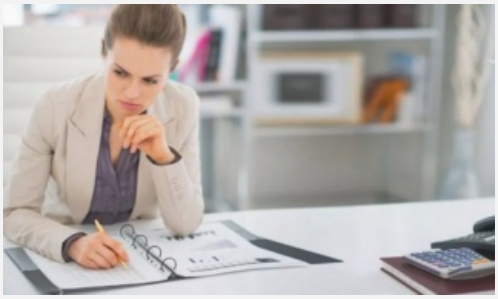
Egy kutatás szerint a kilépő vagy elbocsátott munkavállalók közel fele titokban letölt, elment, továbbküld vagy kiszivárogtat munkával kapcsolatos dokumentumokat, mielőtt elhagyja régi munkahelyét. Ennek részben az is az oka, hogy becslések szerint az irodai dolgozók 72%-a tévesen úgy gondolja, hogy a munkahelyükön általuk létrehozott adatok az övék.

Az ESET szakértői szerint a járványra adott intézkedések - **az ellátási láncok és partnerségek kiterjesztése, valamint a távmunka és a felhő-infrastruktúra bevezetése - minden korábbinál kiszolgáltatottabbá tették a cégeket a külső és belső fenyegetésekkel szemben. A távozó alkalmazottak - akár szándékosan, akár véletlenül - jelentős károkat okozhatnak** a vállalat pénzügyeire és jó hírére nézve.

A belső incidensek költségei 2018 és 2020 között 31%-kal ugrottak meg; a kár megközelíti a 11 és fél millió amerikai dollárt. Ebből is látszik, hogy a hatékony kiléptetés minden biztonsági stratégia alapvető részét kell, hogy képezze - sajnos mégis túl gyakran figyelmen kívül hagyják.

A vállalat támadási felületeit általában a külső fenyegetések szemszögéből vizsgálják, pedig maguk az alkalmazottak is fenyegetést jelenthetnek. Ma már sok szervezetnél gyakorlatilag bárhonnan, bármilyen eszközről hozzá lehet férni a felhőalapú alkalmazásokhoz, adattárolókhoz és egyéb vállalati hálózati erőforrásokhoz. A produktivitás fenntartása miatt ez elengedhetetlen volt a pandémia idején, de **a megfelelő kontroll hiányában az alkalmazottak így könnyebben kijátszhatják az adatvédelmi szabályzatot.**

Sajnos a kutatások azt mutatják, hogy **a szervezetek 43%-a egyáltalán nem rendelkezik olyan szabályzattal, amely megtiltja a dolgozóknak, hogy távozáskor magukkal vigyék a munkahelyi adatokat.** Még ennél is aggasztóbb, hogy például **az Egyesült Királyságban csak a vállalatok 47%-a vonja vissza az épülethez való hozzáférést a kilépési folyamat során, és csak 62% kéri vissza a vállalati eszközöket a kilépett dolgozóktól.**



A felmérések adataiból emellett az is kiderül, hogy a munkavállalók közel fele (45%) letölt, elment, továbbküld vagy kiszivárogtat munkával kapcsolatos bizalmas dokumentumokat, **mielőtt elhagyja a munkahelyét. Ez leggyakrabban a tech, a pénzügyi és a tanácsadói szektorokban fordul elő.**

Milyen károkat okozhat mindez? Akár amiatt viszik magukkal az adatokat a kilépő dolgozók, hogy az új munkaadó

kedvében járjanak, akár azért, hogy bosszúból ellopják vagy töröljék azokat, ez súlyos következményekkel járhat a szervezet számára. Az adatsértés a következőkhöz vezethet:

• Vizsgálati, kármentesítési és tisztítási költségek
• Csoportos keresetekből eredő jogi költségek
• Hatósági bírságok
• Márka- és hírnévkárosodás
• Elveszített versenyelőny

Egy hitelszövetkezeti alkalmazott a közelmúltban bűnösnek vallotta magát abban, hogy 21 GB bizalmas adatot semmisített meg a kirúgását követően. Annak ellenére, hogy egy kollégája megkérte az IT részleget a kirúgott alkalmazott hálózati hozzáférésének azonnali letiltására, ez mégsem valósult meg időben, így az illető a korábbi felhasználónevét és jelszavát használva távolról még hozzá tudott férni a fájlszerverhez és mintegy 40 percet töltött adatkárosítással.

A hitelszövetkezetnek 10 ezer amerikai dollárba került ez a jogosulatlan behatolás és a dokumentumok elvesztése. A fent említetthez hasonló eseteket sokkal jobban lehetne kezelni, ha az érintett szervezetek hatékonyabb kiléptetési folyamatokat vezetnének be. **Ennek a folyamatnak már jóval azelőtt el kell kezdődnie, hogy a munkavállaló jelezné felmondási szándékát vagy elbocsátják.**

- Világosan kommunikáljuk a szabályzatot!
Ha egyértelmű és írásos formában is elérhető irányelvekkel segítünk a munkavállalók számára megérteni a szellemi tulajdonjog határait, sok későbbi kellemetlenséget spórolhatunk meg. Egyértelmű figyelmeztetéseket is mellékeljünk arról, hogy mi történik, ha egy munkatárs megszegi a szabályzatot.

- Vezessük be a folyamatos nyomon követést!
Ha egy alkalmazott a vállalat elhagyása előtt információkat akar lopni, akkor valószínűleg már jóval azelőtt nekikezd, hogy értesítené a HR-t a munkahelyváltásról. Ezért a szervezeteknek olyan felügyeleti technológiákat kell bevezetniük, amelyek folyamatosan rögzítik és jelzik a gyanús, szokatlan tevékenységeket - természetesen a helyi adatvédelmi törvények betartásával és a munkavállalók etikai aggályainak figyelembevételével.

- Legyen kéznél egy szabályzat és egy előre meghatározott folyamat!
Tervezzük meg előre a munkafolyamatokat: míg szinte minden szervezetnek van beilleszkedési protokollja, sokan elfelejtik ugyanezt megtenni a távozó alkalmazottak esetén.

A következőket érdemes belevenni a kilépési protokollba:

• Az összes alkalmazáshoz és szolgáltatáshoz való hozzáférés visszavonása és a jelszavak visszaállítása
• Épület-hozzáférések visszavonása
• Kilépési beszélgetés a gyanús viselkedés ellenőrzésére
• Egy utolsó vizsgálat futtatása a felügyeleti/naplózási eszközökön a szokatlan tevékenységre utaló nyomok észlelése érdekében.
• Gyanús tevékenység észlelése esetén a HR/jogi osztály felkeresése
• A fizikai vállalati eszközök maradéktalan visszakérése
• E-mail-továbbítás és fájlmegosztás megakadályozása
• A licencek újbóli kiosztása más felhasználóknak

Ahogy a szervezetek készülnek a járvány utáni világra, az ügyfelekért folytatott verseny minden eddiginél élesebbé válik. Kevesen engedhetik meg maguknak, hogy az értékes szellemi tulajdonuk a távozó alkalmazottakkal együtt elhagyja a vállalatot, vagy, hogy egy súlyos biztonsági résből eredően pénzügyi és hírnévbeli károkat szenvedjenek el.

A kiléptetés csak egy kis darabkája ennek a vállalatbiztonsági kirakósnak - ám egy nagyon is fontos darabja.

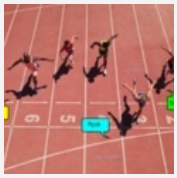
Szólj hozzá!
Címkék: adatvédelem céges szabályzat megelőzés vállalat alkalmazott elbocsátás adatvesztés védekezés adatlopás adatvagyon távozó

Ajánlott bejegyzések:

Az online térben hagyott személyes adataink

Ha eljön a személyiségtolvaj

Fiatal vagy? Ezekre az online csalásokra figyelj!



Világrekord, aminek mégsem örül senki

Az egyik COVID-19, a másik egy híján 20

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

GoDaddy - apák a pácban

2021. november 23. 10:38 - Csizmazia Darab István [Rambo]

A GoDaddy **a világ egyik legnagyobb domainregisztrátora és webhosting cég**, világszerte több mint 20 millió ügyfélnek nyújt különféle szolgáltatásokat. Na de mi történik akkor, ha pont a suszter cipője lyukas?

Vonzó célpont egy ilyen cég, és már jó pár támadáson, támadási kísérleten vannak túl az évek folyamán. A mostani friss esetnél a vállalati WordPress környezetbe hatoltak be illetéktelenek.

Bár a támadást november 17-én észlelték, **a vizsgálatok alapján arra lehet következtetni, hogy a támadók már szeptember 6-a óta hozzáférhettek a hálózatához és a kompromittált rendszerek** adataihoz.

A támadók **egy feltört jelszó segítségével admin jogot szereztek, és ezzel jogosulatlanul hozzáférhettek rengeteg bizalmas adathoz. A jelenlegi beszámolók szerint 1.2 millió ügyfél adatához, azonosítókkal, e-mail címekkel, a regisztráció idején generált rendszergazdai jelszavakkal.**

Ezen felül aktív fiókok sFTP belépési név-jelszó párosok, adatbázis login adatok lehetnek érintettek. Ráadásul az aktív ügyfelek egy részének esetében az SSL privát kulcsot is ellophatták, ami roppant kínos.

A vállalat a támadás észlelésekor azonnal értesítette a hatóságokat, valamint saját ügyfeleit is tájékoztatta, segélyvonalakat állított fel. **Az érintett felhasználók jelszavait resetelték, illetve az SSL támadás kockázata miatt az adott felhasználók részére folyamatban van új tanúsítványok kiadása és telepítése.**

Alig egy éve történt, amikor meg éppen 28 ezer SSH bejelentkezés kiszivárgása miatt magyarázkodhattak, így ennek fényében a cég mostani közleménye, miszerint: "*We will learn from this incident and are already taking steps to strengthen our provisioning system with additional layers of protection.*" - azaz hogy **tanulunk az incidensből és megerősítjük a védelmünket - mindenképpen elmarad egy ilyen kaliberű szereplő esetében az elvárható biztonságtól, és sajna ez nem igazán Daddy Cool.**

5 komment
Címkék: ssl incidens wordpress feltörés godaddy adatlopás sftp adatszivárgás godaddy.com domainregisztrátor webhoszting

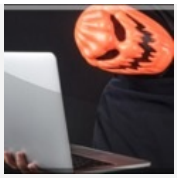
Ajánlott bejegyzések:

[100 millió helyett "csak" 40 lett, maradhat?]

[Megint jőnek, szivárogtatnak...]

[Persze hogy tudtam, csak nem sejtettem...]

[Hogy ne kezeljünk informatikai incidenst?]



[Halloween, helló adatok]

Kommentek:

steery 2021.11.24. 16:23:49

És ezek csak azok az esetek, amik nyilvánosságra kerülnek. Az okosabb hekkerek, ha bejutnak egy rendszerbe, azt igyekeznek addig titokban tartani, amíg nem tudnak a hozzáférésükből maximális pénzügyi hasznot realizálni. És ez nem jelent feltétlenül adatkereskedelmet, lopást és zsarolást. Az is lehet, hogy csak belelátnak a cég pénzügyeibe és eladják az infókat egy konkurens cégnek, ami így rájuk licitálhat, keresztbe tehet az üzleteiknek, elszipkázhatja az ügyfeleiket vagy olcsón felvásárolhatja a konkurenciát. És sosem fog kiderülni, hogy ez miként volt lehetséges?

Válasz erre

Studiosus 2021.11.24. 17:07:00

godaddy kb. háromszor olyan drága, mint bármi más, még a domain titkosításért is fizetni kell, ami máshol alap. az elején még nagyon jók és olcsók voltak, úgy kb. 20 éve, de azóta elszáguldott mellettük a világ. meg a pöcs elefántra vadászgatott, szóval teljesen vállalhatatlan is lett. béke poraira.

Válasz erre

gigabursch 2021.11.24. 18:16:00

Már a neve alapján se foglalkoznék egy ilyen céggel.

Válasz erre

éppnászos 2021.11.24. 19:07:20

www.youtube.com/watch?v=QtxlCsVKkvY

Válasz erre

Head Honcho 2021.11.28. 10:05:42

www.youtube.com/watch?v=lhm2YIZ1dco

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

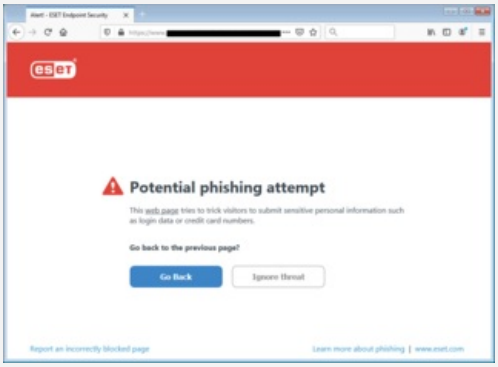
Karácsonyi vásárlás biztonságosabban

2021. november 30. 11:35 - Csizmazia Darab István [Rambo]

Közeleg az ünnepi időszak, amikor sokan vesznek maguknak és szeretteiknek ajándékot, és bár eddig is megvoltak az online lehetőségek, a pandémia miatt ezerszeresen **inkább a neten vásárolunk, mint boltokban maszkban császkálva**. Bár ez a téma évről évre terítékre kerül, de ilyenkor mindig **érdemes lehet kicsit leporolni, felfrissíteni, hogy mikre érdemes odafigyelni.**

Az egyik alap a biztonságos netkapcsolat. Ami vásárláskor lehet az otthoni saját internetes elérésünk, vagy mobileszköz esetén a saját adatforgalmunkat használni. Vásárláskor, pénzügyeink intézésekor kerüljük a nyilvános wifi hotspotokat, amelyek lehallgathatják a forgalmat, ellophatják a bizalmas adatainkat.

Nyitott wifi esetében - ha esetleg mégis erre kényszerülnénk, a VPN azaz a Virtual Private Network megoldások segíthetnek a titkosított és biztonságos adatforgalom biztosításában.



A másik alappillér magának a használt eszköznek a biztonságos állapota. Ez bármi lehet: asztali gép, noteszgép, tablet, ám ma már leggyakrabban az okostelefonunkról történnek a rendelések.

Itt a védelemhez olyan elemekkel járulhatunk hozzá, mint a naprakész vírusvédelmi megoldás használata, a biztonsági javítófrissítések rendszeres letöltése és futtatása, erős jelszavak használata, több tényezős hitelesítés alkalmazása, biometrikus azonosítás - például ujjlenyomat alapján. **A vírusvédelem nem csak a kártevőktől, hanem többek közt az adathalász támadásoktól is megvédik a felhasználókat.**

A biztonságos fizetési metódus is a fontos láncszem a vásárlásaink során. **Egy hatékony vírusvédelmi megoldásban többek közt netbank- és tranzakcióvédelem is található, emellett a más említett kétfaktoros autentikáció, valamint a fizetésközvetítők (PayPal, Revolut) használata, illetve a hasonlóképpen egy virtuális bankkártya használata is igen jó ötlet.** Ez utóbbi esetében egy ilyen külön internetes vásárlásokhoz való elektronikus (unembossed card) virtuális kártya számát bárhol bátran megadhatjuk, akár még a három jegyű CVV ellenőrző kóddal együtt is.

Ha erre az alszámlára csak a vásárlás előtt közvetlenül a netbankunkon utaljuk a vásárláshoz szükséges pontos összeget, akkor ez csak pár percig lesz az egyébként üres virtuális számlánkon, így ezzel a módszerrel nem tudnak

tőlünk lopni, és így az "igazi" bankkártyánk adatait sosem kell a weboldalakon megadnunk. Ma már egyébként az ilyen online terheléseket is a legtöbb esetben egyedileg kell a banki appokban jóváhagynunk, ez pedig mindenképpen pozítiv fejlemény.

Nem elhanyagolható a biztonságtudatos hozzáállás sem, amely óvatossággal, egészséges gyanakvással segít elkerülni a csalásokat, átveréseket. Ezek egész évben próbálnak minket megtéveszteni, a Black Friday, Cyber Monday és hasonló akciós időszakokban erőteljesen igyekeznek becsapni bennünket.

A tapasztalat, a józan ész és megfontoltság sokat segíthet, például ha kifejezetten drága luxustermékeket hirdetnek 90%-os árcsökkentéssel, akkor érdemes résen lenni, és nem bedőlni. Ez kicsit arról is szól, hogy igyekszünk megbízható webáruházakból, bejáratott ismert webshopokból rendelni-vásárolni, és nem hiszünk el minden popup ablakban vagy Facebook üzenetben felbukkanó hirdetési akciót.

Összességében a megelőzés, védekezés szempontjából nem nagyon változott semmi, **és mégis minden megváltozott. A biztonsági szabályok, tippek jórészt maradtak, ám a lezárás, bezárás, homeoffice, távolságtartási korlátozások miatt minden korábbi időszakhoz képest hatalmas arányban tevődött át** a hétköznapi emberek vásárlása az online térbe.

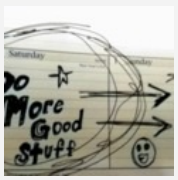
A csalók pedig változatlanul próbálkoznak, sőt. **Ez pedig azt jelenti, hogy a fenti tanácsokkal mindenkinek dolga van, vagy dolga lenne.**

Szólj hozzá!
Címkék: vásárlás karácsony akció xmas csalás átverés védelem megelőzés óvatosság biztonságtudatosság welivesecurity.com

Ajánlott bejegyzések:

Amazónia veszélyes ragadozói ;-)

Celeb vagyok, fizess nekem!



10 kiberbiztonságra veszélyes szokás

Ha eljön a személyiségtolvaj

Ingyenes Omikron teszt vagy mégsem?

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász
NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

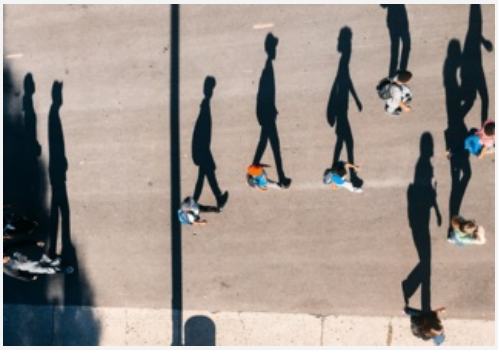
Sötétben bújkáló shadowIT

2021. december 02. 10:09 - Csizmazia Darab István [Rambo]

A táv- és hibrid munkavégzés terjedése új kihívás elé állítja az IT csapatokat: **az alkalmazottak által használt olyan szoftverek és eszközök, melyek az IT csapat ellenőrzési körén kívül esnek, komoly fenyegetést jelenthetnek a szervezetre nézve**. A kérdés az, hogy mit tehetünk ellene, amikor még azt is nehéz felmérni, milyen mértékű a probléma.

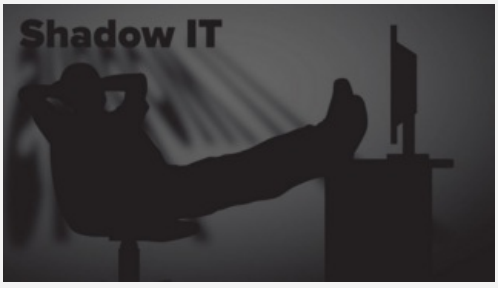
Az árnyékinformatika – más néven shadow IT - a gyűjtőneve minden olyan alkalmazásnak, hardvernek és informatikai megoldásnak, amelyet az alkalmazottak az IT csapat jóváhagyása és ellenőrzése nélkül használnak. Ezek lehetnek vállalati szintű megoldások is, ám a leggyakrabban magánfelhasználásra szánt technológiákról van szó, amelyek komoly veszélynek tehetik ki a szervezetet:

• Magánfelhasználói szintű fájltároló, illetve megosztó, amelyet a dolgozók a hatékonyabb együttműködés érdekében használnak.
• Produktivitás- és projektmenedzsment-eszközök, amelyek szintén támogathatják az együttműködést és a napi feladatok elvégzését.
• Üzenetküldő és e-mail alkalmazások a munkahelyi és magán kommunikációhoz.
• Felhőalapú IaaS (Infrastructure as a Service) és PaaS (Platform as a Service) rendszerek, amelyek nem engedélyezett erőforrások tárolására is használhatók.



Mi az oka a shadow IT jelenségnek? Az ESET szakértői szerint az árnyékinformatika létrejötte mögött általában az áll, hogy **az alkalmazottak megkerülik a szerintük nem eléggé hatékony vállalati IT-eszközöket, amelyekről úgy gondolják, hogy gátolják produktivitásukat.**

A világjárvány hatására **sok szervezet kénytelen volt engedélyezni, hogy a dolgozók a személyes eszközeiket használják az otthoni munkavégzéshez**, ez pedig egyúttal megnyitotta az utat a nem engedélyezett alkalmazások letöltése előtt is.

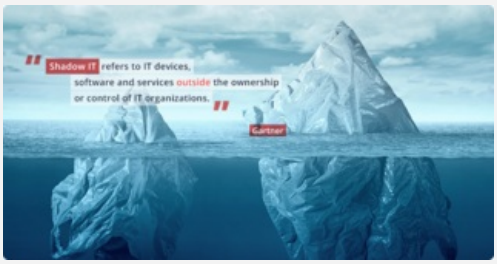


Súlyosbító tényező, hogy **sok alkalmazott nem ismeri a vállalati biztonsági szabályzatot vagy éppen az IT csapatok vezetői maguk voltak kénytelenek felfüggeszteni a szabályokat a home office átállás során.**

Egy nemrégiben készült kutatásban a megkérdezett IT csapatok 76%-a elismerte, hogy a pandémia idején a biztonság háttérbe szorult az üzletmenet folytonosságának javára, míg **91%-uk szerint nyomás nehezedett rájuk, hogy csökkentsék a kiberbiztonság színvonalát.**

A home office emellett megnehezíti az új eszközök jóváhagyását, és hajlamosabbá teheti a dolgozókat a biztonsági szabályok figyelmen kívül hagyására. **Egy 2020-as globális tanulmány szerint az otthonról dolgozók több mint fele (56%) használ nem munkahelyi alkalmazást a vállalati eszközén, és 66%-uk töltött fel erre vállalati adatokat.**

Közel egyharmaduk (29%) válaszolta, hogy **úgy érzi, „megúszhatja" a nem munkahelyi alkalmazás használatát, mert nem találja hatékonynak** az IT által támogatott hivatalos megoldásokat.



A saját eszközök mellett annak is megvan a maga veszélye, hogy bizonyos vállalkozások ellenőrzés nélkül tárolnak erőforrásokat IaaS vagy PaaS vállalati felhőalapú szolgáltatásokon. Sokan félreértik a felhők megosztott felelősség modelljét, és azt feltételezik, hogy a szolgáltató (CSP) gondoskodik a biztonságról.

Pedig valójában az alkalmazások és az adatok biztonságának megőrzése az ügyfélszervezet feladata – de amiről nem tud, azt nem képes megvédeni sem.

Egy 2019-es kutatás szerint az amerikai munkavállalók 64%-a létrehozott legalább egy olyan fiókot, **amiről nem szólt az IT-nek**. Egy másik felmérésből kiderült, hogy **a távolról dolgozó alkalmazottak 65% használt olyan eszközöket a járványt megelőzően, amelyeket az IT nem hagyott jóvá.**

Ugyanez a tanulmány rámutat egy érdekes jelenségre, mégpedig arra, hogy az árnyékinformatika iránti hajlandóság az életkorral változik: **az idősebb baby boomerek mindössze 15% él vele, szemben a fiatal ezredfordulós generáció 54%-val, akik ezt hajlamosak sokkal lazábban kezelni.**

De miért veszélyes ez? A potenciális kockázatot jól példázza az az amerikai kontaktkutató vállalat esete, amely az év elején 70 ezer ember adatait hozhatta nyilvánosságra, miután az alkalmazottak jóváhagyás nélkül használtak Google-fiókokat az információk megosztására.

Íme, néhány példa az árnyékinformatika veszélyeire:

• Az IT ellenőrzésének hiánya: így a szoftverek biztonsági frissítések nélkül vagy rosszul konfiguráltan (pl. gyenge jelszavakkal) működnek, ami támadásoknak teheti ki a felhasználókat és így a vállalati adatokat.
• Nincs vállalati vírusirtó vagy egyéb biztonsági megoldás az árnyékinformatikai eszközök vagy a vállalati hálózatok védelmére.
• Nem lehet ellenőrizni a véletlen vagy szándékos adatszivárgást/adatmegosztást.
• Problémák a megfeleléssel és auditálással.
• Adatvesztés veszélye: az árnyékinformatikai alkalmazások és adatok nem részei a vállalati biztonsági mentésnek.
• Pénzügyi és reputációs károk egy súlyos biztonsági incidens, például adatszivárgás miatt.

Hogyan kezeljük az árnyékinformatikát? Érdemes megfontolni a következő lépések megtételét:

• Egy átfogó árnyékinformatikai szabályzat létrehozása, benne az engedélyezett és nem engedélyezett szoftverek és hardverek egyértelmű listájával, valamint az engedélykérés folyamatának leírásával.
• Az alkalmazottak ösztönzése az átláthatóságra, edukációval és őszinte, kétirányú párbeszéd kezdeményezésével értetve meg velük az árnyékinformatika lehetséges hatásait, kockázatait.
• Az alkalmazottak visszajelzésének meghallgatása arra vonatkozóan, hogy mely eszközök hasznosak, illetve hatékonyak a számukra és melyek nem. Talán itt az ideje felülvizsgálni a szabályzatot a hibrid munkavégzés hozta új korszaknak megfelelően, hogy jobban egyensúlyba kerülhessen a biztonság és a kényelem.
• Felügyeleti eszközök használata a vállalaton belüli árnyékinformatika-használat és a kockázatos tevékenységek nyomon követésére, hogy idejében fel lehessen ismerni a szabályszegőket.

Az árnyékinformatika egyértelműen megnöveli a vállalat támadási felületét és komoly kiberbiztonsági kockázatot rejt magában. A probléma eredményes megoldásához az IT-nak szorosabb és hatékonyabb együttműködést kell kialakítania a munkavállalókkal.

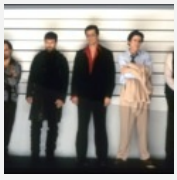
1 komment
Címkék: tippek eset vállalati védekezés shadowit árnyékinformatika

Ajánlott bejegyzések:


7 tipp a mobilunk védelméhez


Fiatal vagy? Ezekre az online csalásokra figyelj!

Az egyik COVID-19, a másik egy híján 20


Tőrbeejtett adataink


Digitális ajándékok Karácsonyra

Kommentek:

Amicus 2021.12.04. 11:32:52

Ez egy nagyon izgalmas téma, viszont az IT-nak azzal is foglalkoznia kell, hogy miért alakult ki a ShadowIT? Sokszor ez a belső IT működési problémáira is utal (lásd nem szolgálja ki megfelelően a felhasználókat), persze lehet, hogy csak a könnyebb, egyszerűbb utat választották az üzleti területek és ezért kerülik meg az IT-t. Szóval érdemes óvatosan megközelíteni és lehet, bizonyos esetekben nem is kell teljesen megszüntetni, de szabályozni és elvárásokat

megfogalmazni mindenképpen kell.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

Ingyenes Omikron teszt vagy mégsem?

2021. december 07. 11:57 - Csizmazia Darab István [Rambo]

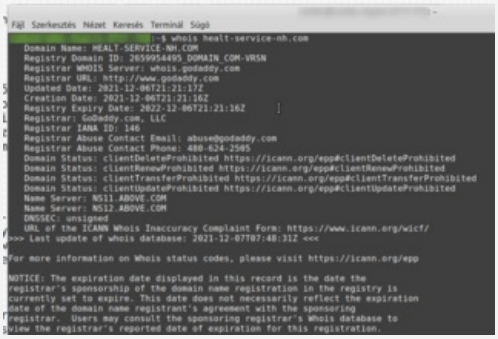
Történjen a világban, egy biztos, rövid időn belül megjelenik a hozzákapcsolódó átverés, kéretlen phishing levél. Nincs ez másként a pandémiás időszak legújabb felvonásában sem. **Az Omikron koronavírus-variáns felbukkanása után máris terítik a bűnözők az ezzel kapcsolatos adathalász kampányokat.**

A soha véget nem érős Vagy mégsem? rovatunk legújabb epizódjában olyan adathalász támadásokat mutatunk, amelyekben a bűnözők éppen erre hivatkozva személyes adatokat igyekeznek megszerezni és ellopni.

Ebben a próbálkozásban **az Egyesült Királyság Nemzeti Egészségügyi Szolgálatának (NHS) nevével visszaélve olyan hamis üzeneteket küldenek, amely azt ígéri az áldozatoknak, hogy ingyenes Omikron PCR tesztet kaphatnak.**

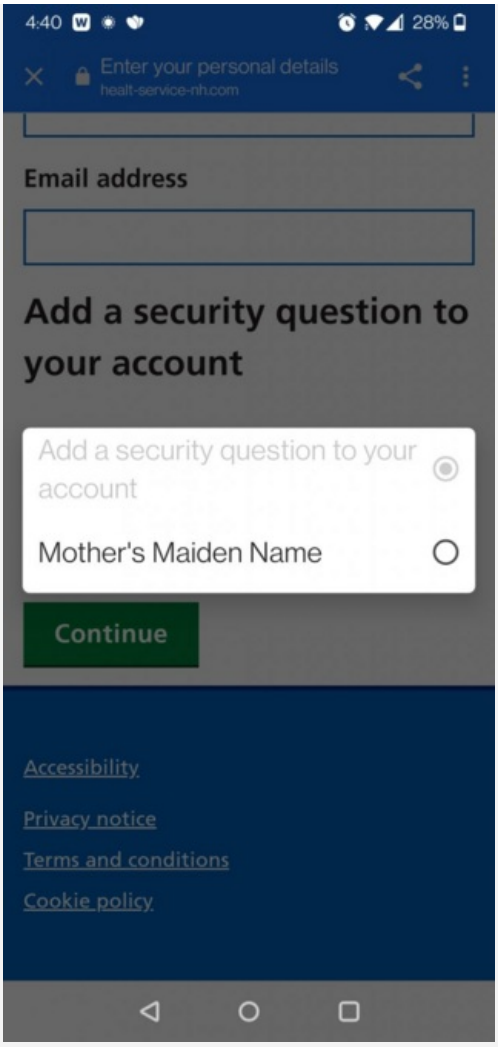
A levél **megtévesztően azt is állítja, hogy az új változatot nem észlelik a korábbi COVID-19 variánsokhoz használt tesztkészletek, erre csak az új tesztek alkalmasak**, ami persze nem igaz.

Az üzenet kattintás után átirányít egy hamisított NHS weboldalra, ahol **bekérik a látogató teljes nevét, születési dátumát, lakcímét, mobilszámát és e-mail címét - vagyis minden olyan információt, amellyel a csalók később megszemélyesítéses támadást hajthatnak végre.**



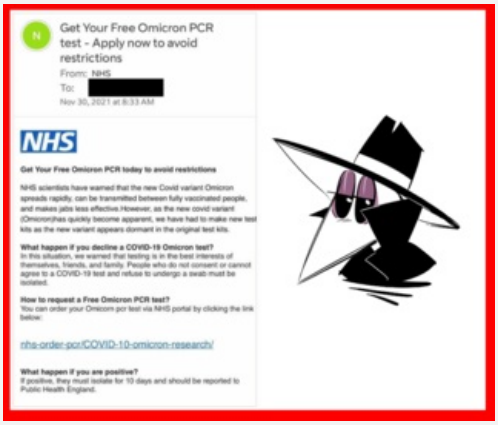
Az már csak hab a tortán, hogy **az "ingyenes" tesztért 1.24 angol fontot mégis kér állítólagos szállítási díjra hivatkozva. A kamu hasonmás weboldalt (healt-service-nh.com) pedig a whois lekérdezés alapján frissen regisztrálták** ehhez az átveréshez.

Ugyanezzel a módszerrel **több különböző, kisebb módosításokkal rendelkező verzió is megjelent a megtévesztő e-mailből.**



Az elkövetők leleményességére utal, hogy a **szállítási díj fizetésénél annak állítólagos biztonságosabbá tételére hivatkozva kérnek egy biztonsági kérdést és választ is.**

Ahol az alapértelmezett - és emiatt valószínűleg sokak által választott - opció az anyja neve lesz, emiatt pedig még precízebb lesz az ellopott bizalmas személyes adatok köre.



Az elkerülés, megelőzés érdekében változatlanul **a nagyobb odafigyelést javasoljuk, sose kattintsunk kéretlen üzenetek linkjeire, vagy csatolt mellékleteire, ne dőljünk be az ingyenesnek hirdetett dolgoknak, és bánjunk sokkal biztonságtudatosabban saját személyes adatainkkal.**

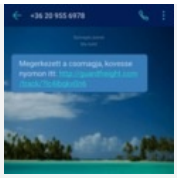
Szólj hozzá!
Címkék: teszt ingyenes vagy csalás átverés phishing adathalászat mégsem omikron adatlopás vagymégsem variáns welivesecurity.com covid-19 covid

Ajánlott bejegyzések:

[Vakcinás csalások, szevasztok]

[Duplázd meg a pénzedet - vagy mégsem?]

[A bankos mindig kétszer csenget...]



[Megérkezett a csomagja - vagy mégsem?]

[Földgázszámla vagy mégsem?]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

A bankos mindig kétszer csenget...

2021. december 09. 16:43 - Csizmazia Darab István [Rambo]

Az idei évben egyre erőteljesebben **terjed az az átverési forma, ahol csalók telefonon hívogatják az embert és különböző Magyarországon tevékenykedő bankok alkalmazottaiként mutatkoznak be**. Mutatjuk a különféle furmányos trükkjeiket és persze **adunk a védelemhez, megelőzéshez tippeket, tanácsokat is**, mert az ünnepi időszakban még több ilyen kísérletre számíthatunk.

A kamu telefonhívás alaptörténete, hogy egy magát a bankunk ügyintézőjeként bemutatkozó illető (pl. Nagy Dominika) arról tájékoztat minket, hogy valószínűleg bajban vagyunk, mert illetéktelenek megszerezhették a személyes és banki adatainkat, és vásárlásokat kezdeményeztek a számlánk terhére.

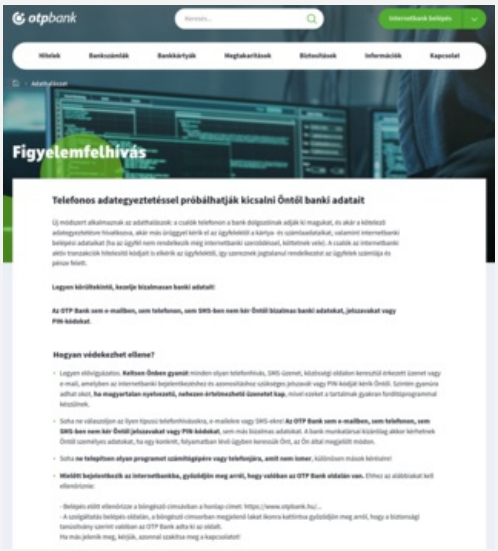
Felajánlja a segítségét, hogy blokkolja ezeket az állítólagos vásárlásokat, ehhez mindössze egyeztetésre kéri be az összes személyes adatunkat, valamint banki adatainkat, kártyaszámunkat, lejárati dátumot, PIN kódunkat, 3 jegyű CVV biztonsági kódunkat, internetes banki belépési név-jelszó párosunkat. A telefonáló lehet nő vagy férfi is, ám sok esetben érezhető akcentussal, vagy tájszólással beszél, és egy betanult szöveget olvas fel gépiesen egy állítólagos 90 és egy 150 ezer forintos vásárlásról. Egy ilyen próbálkozás, ahol a csaló az OTP nevével él vissza, itt hallgatható meg.

Ahogy hallható, **gyakran már azon elbuknak, hogy nem is tudják kit hívnak, mert hideg hívásokkal próbálkoznak, arra számítva, hogy a hívott fél majd bemutatkozik**. A visszakérdezések sokszor kizökkentik a csalót a szerepéből, elbizonytalanodik vagy bontja a vonalat. Ha az első akadályon túljutottak, és sikerül megijeszteni az áldozatot, ám ő jelzi, hogy nem is az adott bank ügyfele, erre is van válaszuk, tudjuk, és máris átkapcsoljuk a ... bankhoz, ehhez még háttér irodazajt is bejátszanak.

A bekért adatokat arra a mesére hivatkozva kérik el, hogy letiltással megvédjék az ügyfél bankszámláját, ami persze nem igaz, hiszen azért kérik el az adatokat, hogy gyorsan leürítsék róla a pénzt.

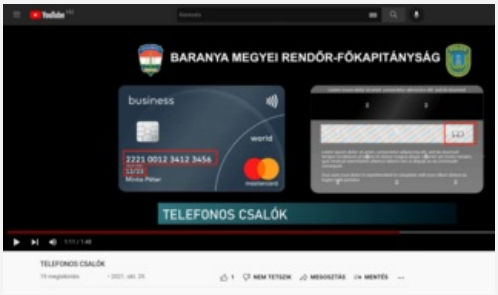
A mese részeként időnként az is megtörténik, hogy a pénzösszeg állítólagos megóvása érdekében **bediktálnak egy ismeretlen, másik úgynevezett "biztonsági számlaszámot", és azt kérik, ideiglenesen oda utalja át az áldozat a pénzét, mert azon biztonságba helyezik, amíg a felderítés, és a nyomozás zajlik**. Akár az állítólagos letiltás, akár a kamu továbbutalás történik, kérnek egy negyedóra türelmet, hogy addig senki ne lépjen be a banki alkalmazásba, mert az "technikai zavart" okozhat.

Ám ennek igazi oka, hogy ezalatt lopják el az áldozat pénzét. **Az a forgatókönyv is előfordulhat, hogy a megijesztett áldozattal feltelepíttetnek a mobilra, tabletre, számítógépre egy olyan távmenedzsment szoftvert (pl. AnyDesk, Teamviewer), amelynek segítségével távoli teljes eléréshez jutnak, és onnan minden szükséges személyes és banki adatot el tudnak lopni**, sajnos ilyen konkrét magyarországi esetről is jelent már meg beszámoló.



A bankok alaphelyzetben elég jól védettetek, **ezért igyekeznek a csalók a könnyebb utat választani, ez a gyengébb láncszem pedig maga a gyanútlan felhasználó**. Ezek a fajta átverések egész Európában elterjedtek, és sajnos Magyarországon is egyre gyakrabban találkozhatunk vele.

A leckét sajnos mindenkinek muszáj megtanulnia, mert ilyen csalás esetén egyértelműen az ügyfél hibájából keletkezik a kár, és ezt a bankok nem térítik meg.



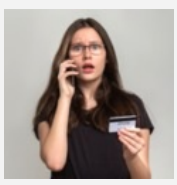
Akkor térjünk rá a védekezés-megelőzés részre. Először is a bankok sosem (never-ever) kérik el tőlünk a banki adatainkat, kártyaszámunkat, lejárati dátumot, PIN kódunkat, 3 jegyű CVV biztonsági kódunkat, internetes banki belépési név-jelszó párosunkat telefonon keresztül, ez legyen egy örök érvényű figyelmeztetés az agyunkban. Ilyet csak adathalász támadók tesznek.

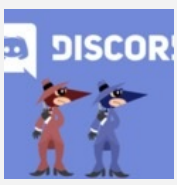
Ismeretlen hívásnál gyanakodjunk, és ellenőrizzük le a hívó felet. Ha nem látszik a hívó száma, eleve gyanús, de **ha bármi bizonytalanság felmerül, életszerűtlen a történet, fura a telefonáló, azonnal bontsuk a vonalat és mi magunk hívjuk a bankunkat a hivatalos telefonszámon. Az ORFK azt kéri, minden áldozat mihamarabb tegyen feljelentést, ez segíti hasonló bűncselekmények megelőzését.**

1 komment
Címkék: biztonság bank csalás átverés phishing vishing adathalászat pénzintézet adatlopás telefonhívás

Ajánlott bejegyzések:


Ingyenes Omikron teszt vagy mégsem?


Továbbra is célkeresztben a banki adataink



Adathalászat a Discordon


Fogják a pénzünket és futnak

Egypálcás adathalász próbálkozások

Kommentek:

éppnászos 2021.12.10. 13:47:53

Ha banktól hívnak, az mindenképp csalás lesz

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

- RSS 2.0
- bejegyzések, kommentek

Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

SÜTI BEÁLLÍTÁSOK MÓDOSÍTÁSA

5.2 milliárd netező 1 perce

2021. december 13. 13:15 - Csizmazia Darab István [Rambo]

Évről évre rendszeresen követjük azokat az izgalmas statisztikákat, amelyeket a DOMO ad ki Data Never Sleeps címmel. Az idei legfrissebb adatok arról is tanúskodnak, hogy **a törvényszerű szokásos kiszámítható emelkedések mellett a pandémia hova csatornázott be kiugró növekedéseket.**

Először is azt kell megállapítsuk, a készítők sokat dolgoznak azon, hogy minél nehezebben lehessen összehasonlítani a korábbi verziók adatait az aktuálissal.

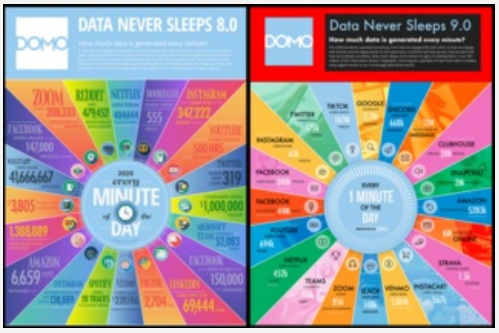
Ez sokkal többet jelent, mint új szolgáltatók vagy szolgáltatások felbukkanása, inkább valamilyen Murphy törvényes szabályszerűséget követve ("A méreteket mindig a legkevésbé használható mérték egységekben adják meg. A sebességet például öl per miatyánkban.") csak arra az egy verziójú ábrára érvényes egyedi, a későbbiekkel már összehasonlíthatatlan mértékegységű adat szerepeltetését jelenti.

A szükséges, de nem elégséges zsörtölődés után nézzük akkor az új adatokat. A teljes és részleges lezárás, a homeoffice alaposan felforgatta a szokásainkat, kezdve mondjuk az online konferenciázással, az MS Teams, Cisco Webex, Zoom, és hasonló alkalmazások segítségével történő rendszeres kapcsolattartásra, ebben biztosan történt növekedés: **2020-ban 60 másodperc alatt 208 ezer résztvevő, míg 2021-ben egy perc leforgása alatt 856 perc webinar zajlott világszerte ;-)**

Ami még Zoom ügyben viszont még fontos, a korábbi rengeteg biztonsági incidens miatt azóta az üzemeltetők már sokat faragtak a biztonságon, többek közt legutóbb az automatikus frissítési lehetőséget hegesztették bele.

YouTube fronton is komoly emelkedés következett be, **mára 694 ezer óra anyagot közvetít a platform percenként.**

De jól látható a fejlődés abból a párhuzamból is, hogy **míg 2020-ban percenként 2704-en telepítették fel a TikTokot, úgy 2021-ben már 167 millió videót néztek az egységnyi 60 szekundum alatt. Kis lépés ez ugyan egy embernek, ám nagy lépés az emberiségnek és az egymással könnyen összevethető statisztikáknak ;-)**



Hideg fejjel még pár nagy volumenű érték a 9.0-ás kimutatásból, mi történik a neten 1 perc alatt: 575 ezer Twitter poszt, 283 ezer USD elköltése az Amazon áruházban, **240 ezer kép megosztása a Facebook illetve Meta univerzumában, 5.7 millió Google keresés, 668 ezer Discord üzenet küldése, 2 millió Snapchat üzenet, és 100 ezer felhasználó csatlakozása a Teams** rendszerére.

Az emberiség 65%-a online van, és a fenti elérések jelentős része már mobileszközökről történik a Statista adatai szerint. A 2022-es évre is legalább hasonló mértékű növekedést prognosztizálnak a szakértők.

Végezetül pillantsunk rá az AV Test weboldalra, mekkora az egyedi kártékony kódok számossága ezen a fagyos

decemberi napon. **Ez a december 12-i napon 1 milliárd 306 millió volt. A haveibeenpwned.com weboldal tanúsága szerint pedig 11.7 milliárd kiszivárgott belépési adat került illetéktelen kezekbe.**

Mind az egyperces számok, mind ezek az kártékony támadásokkal kapcsolatos értékek jelzik, hogy jövőre is sok teendőnk lesz még az internetes biztonság javítása területén.

Szólj hozzá!
Címkék: statisztika internet net never egy data perc történik minute domo sleeps

Ajánlott bejegyzések:


Ez történik a weben egy perc alatt


Ez történt 2019-ben egy perc alatt a weben


Sötét jelen: agresszív zsarolóvírusok, tömeges bruteforce


Fiatal vagy? Ezekre az online csalásokra figyelj!

Ransomware helyzetjelentés

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

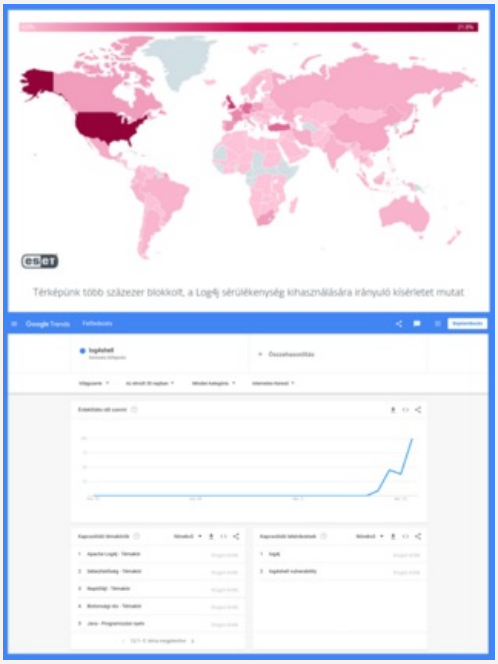
Log4j sebezhetőség - hogyan tovább?

2021. december 16. 10:40 - Csizmazia Darab István [Rambo]

A napokban derült fény a világszerte mindenütt jelenlévő Log4j segédprogram kritikus hibájára, amely megrázta az egész kiberbiztonsági iparágat. **A Log4j nyílt forráskódú Java-alapú naplózási szoftvert globális szinten számtalan vállalat és kormányzati szerv használja.**

Amióta **a sérülékenység kihasználásához szükséges kód felkerült az internetre, a hackerek tömegével próbálják kijátszani a rendszereket**, miközben a kiberbiztonsági szakemberek minden erejükkel igyekeznek biztonsági frissítésekkel és más védelmi intézkedésekkel védekezni a támadások ellen.

Az ESET által közzétett térképen jól látható, mely országokban hajtották végre a legtöbb Log4j sérülékenységet kihasználó támadási kísérletet, ezekből több százezer blokkolt kihasználási kísérlet történt.



A fenyegetés az Egyesült Államokban, az Egyesült Királyságban, Törökországban, Németországban és Hollandiában van a leglátványosabban jelen. Roman Kováč, az ESET vezető kutatója úgy nyilatkozott a vizsgálatok eredményéről, hogy **az észlelések mennyiségé alapján egy jelentős problémával állunk szemben, amely sajnos nem fog egyhamar megszűnni.**

A támadók számos módszerrel próbálják kihasználni a sérülékenységet, de **nem minden kísérlet rosszindulatú, hiszen köztük kutatók, információbiztonsági cégek és a penetrációs tesztelők védelmi célokból is tesztelik ezeket a sebezhetőségeket.**

A Log4j segédprogram kritikus hibájáról [további részleteket az ESET magyar nyelvű weboldalán](), illetve az ESET [angol összefoglaló videójából]() lehet többet megtudni.

3 komment
Címkék: java támadás exploit sebezhetőség sérülékenység log4j log4shell

Ajánlott bejegyzések:


Exchange szerverek tűz alatt


Egyedül nem megy


Három éve jelent meg a WannaCry


Kr00K sebezhetőségre figyelmeztet az ESET


BlueFrag hiba az Androidon

Kommentek:

Le a spammerekkel · http://ketkerekenoutival.blog.hu/ 2021.12.16. 21:35:27

Az megvan, hogy nem minden verzió érintett? Vagy ez csak UL?

Válasz erre

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2021.12.17. 11:29:25

Szia!

A beszámolók szerint 2.x verziók, vagyis több is érintett. Sőt a már forgalomban nem lévő, de vélhetően valahol még futattott 1.x is a terepasztalon van.
bitport.hu/ujabb-problemakat-talaltak-az-apache-log4j-ben

Ma elég részletesen körbejárták ezt a dolgot a Millásreggeliben, szerintem holnapra már fent lesz a podcast is.

Válasz erre

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2021.12.17. 17:08:33

Na ki is jött a podcast: Log4Shell, jegybankok és devizák - Millásreggeli Frész Ferenccel:
millasreggeli.hu/podcast/log4shell-jegybankok-es-devizak/

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció

Ha eljön a személyiségtolvaj

2021. december 21. 11:26 - Csizmazia Darab István [Rambo]

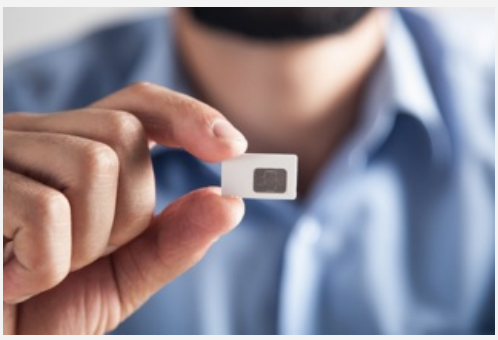
Ha ellopják a bizalmas személyes adatainkat - jelszavak, lakcím, születési információk, banki adatok, stb. - akkor a legrosszabb forgatókönyv az, ha a csalók bennünket megszemélyesítve leürítik bankszámlánkat, adót igényelnek vissza, a nevünkben hitelt vesznek fel, autót lízingelnek, az egészségügyi számlánkra nagy értékű műtéteket számolnak el, bűncselekmények elkövetésekor a mi adatainkat diktálják be, és még hosszan lehetne sorolni az esetleges negatív következményeket. **A személyazonosság-lopás korai figyelmeztető jeleinek észlelésével és biztonságtudatos hozzáállással minimalizálhatjuk a kockázatokat.**

Mindannyian egyre több időt töltünk online, tanulással, munkával, kikapcsolódással, online vásárlással. **Ennek a viselkedésbeli változásnak egy járulékos következménye, hogy még több személyes adatunkat és bejelentkezési hitelesítő adatainkat osztjuk meg azokkal a vállalatokkal, amelyektől rendelünk, vásárolunk, különféle szolgáltatásokat veszünk igénybe.**

A kiberbűnözők viszont mindent megtesznek, hogy ellopják ezeket az adatokat részben ezektől a szervezetektől, részben közvetlenül tőlünk. Mire figyeljünk, hogyan előzhetjük meg mindezt?

Az egyik ilyen intő jel a szokatlan banki terhelések. Nem mi kezdeményeztük, nem értjük az okát, és legyen az bármilyen apró összeg, azonnal érdemes felvenni a kapcsolatot a bankunkkal. A lopott banki adatoknál például szokás próbaképpen kis összegekkel terhelni, helyes-e az ellopott PIN kód, például negyed dollár utalása a Vörös Keresztnek. A bűnözők az ellopott de ellenőrzött kártya adatokért jóval többet kapnak a feketepiacon.

A biztonságos karácsonyi vásárlások kapcsán már kivesézték az optimális fizetési megoldásokat, vagyis ha virtuális kártyával fizetünk, van azonnali egyenlegértesítőnk, mindig használunk kétfaktoros autentikációt, erős jelszavaink vannak, nem osztjuk meg másokkal a banki és egyéb személyes adatainkat, akkor ezt az akadályt sikeresen legyőzhetjük.



Hasonlóan riasztó esemény lehet, ha a mobiltelefonunk elnémul, vagy levelezésünkbe, online szolgáltatásainkba többé már nem tudunk belépni. A mobiltelefon leállása SIM kártyacserés támadásra figyelmeztethet. SIM-eltérítésnek, SIM-megosztásnak, SIM-cserének is hívják, ha a kiberbűnözők először célzottan adatokat gyűjtenek a kiszemelt áldozatról, majd a nevükben eljárva SIM kártyacserét kezdeményeznek a mobil szolgáltatónál. Szerencsére a sok ilyen visszaélés miatt a szolgáltatók azóta már szigorítottak ezen a folyamaton.

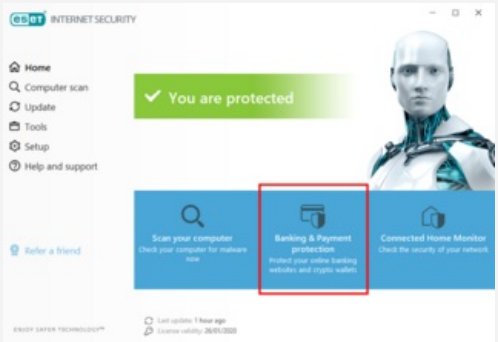
Online account pedig esetében érdemes lehet jelszavaink biztonságát is áttekinteni, incidens esetén azonnal változtatni. Mindenhol legyen egyedi, erős azaz betűket, számokat és szimbólum karaktereket egyaránt tartalmazó hosszú jelszavunk. Minden helyen alkalmazzunk többtényezős hitelesítést: biometrikus (pl. arc, ujjlenyomat) azonosítást, egyedi SMS küldést, vagy egyéb dedikált hitelesítő alkalmazást. Rendszeres időközönként - akár tapasztaltunk gyanús dolgokat, akár nem - mindenképpen cseréljük a legfontosabb fiókjaink jelszavait.

Bár ez a fajta visszaélés inkább az angol nyelvterületen elterjedt, **ha valamilyen magyarországi TB vagy adózási ügyben szokatlan esemény, történés látható, amelyet nem mi kezdeményeztünk, vagy nem tudunk belépni, elvégezni korábban problémamentes szokásos online feladatokat, bevallásokat, akkor is gyanakodhatunk adatlopásra.**

A csalók szívesen használnak lopott társadalombiztosítási számokat és egyéb személyes adatokat hamis bevallások, adó-visszatérítések benyújtásához, illetéktelenül megszemélyesítve az áldozatot. Egyébként érdekes módon magyar nyelvű adathalász próbálkozások már több éve előfordulnak nálunk is. **Az egészségügyi adatokkal való visszaélésekről itt írtunk bővebben, ez is egyelőre jó részt inkább a külföldi, magánegészségügyi szolgáltatásokkal kapcsolatosan jelent visszatérő problémát.**

És végül az is egy intő, sőt fejbekólintó jel lehet, ha bár anyagilag legjobb tudásunk szerint jól állunk, mégis adósságbehajtók jelentkeznek. Ez egyértelműen utalhat a nevünkben elkövetett pénzügyi visszaélésekre, és az ilyen esetekben csak idő kérdése, hogy nálunk kopogtassanak.

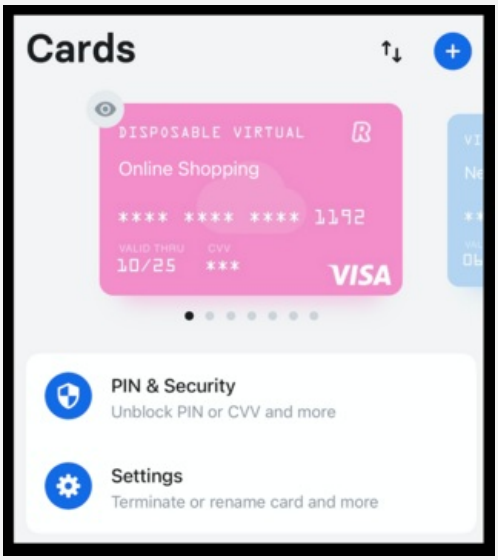
Első lépésként haladéktalanul vegyünk fel a kapcsolatot a bankunkkal, egyeztessük velük a gyanús tranzakciókat, kérjünk tőlük vizsgálatot. Ha csalók megpróbálták meg minket megkárosítani - akár sikeresen, akár sikertelenül - minden esetben haladéktalanul tegyünk feljelentést a rendőrségen.



Személyiséglopással kapcsolatos "megelőzésügyi" jótanácsainkat a fentieken túl még pár hasznos dologgal azért ki tudjuk egészíteni. **Nagyon fontos hogy a telefonunkat, számítógépünket fizikailag is óvjuk ellopás, elvesztés, illetéktelen használat ellen. Pénzügyek, hivatalos ügyek, vásárlások alkalmával mindig saját megbízható eszközünkről lépjünk be, és csak biztonságos internetkapcsolattal tegyük ezt, vagyis otthonról vagy telefonunk adatforgalmáról. Sose intézzünk pénzügyeket, netes vásárlást nyitott wifiről, nyitott hotspotról. Minden készülékünkön fusson naprakész vírusvédelmi program, és rendszeresen frissítsük mind az operációs rendszerünket, mind a felhasználói programjainkat a megjelent hibajavító frissítésekkel.**

Legyen mindenhol erős, egyedi jelszavunk, kétfaktoros autentikációval megerősítve. Legyünk biztonságtudatosak, ne dőljünk be az adathalász és egyéb csalásoknak, használat után mindig jelentkezzünk ki a banki szolgáltatásokból. Hasznos, ha aktiváltatjuk bankunknál az SMS vagy push üzenet alapú azonnali egyenlegértesítést, mert így értesülünk a számlánkon zajlódó összes pénzmozgásról, és sokkal könnyebben

felfigyelhetünk az esetleges gyanús tevékenységekre.

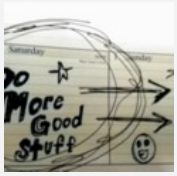


Ugyancsak hasznos biztonsági lépés, ha az internetes vásárlásokhoz virtuális kártyát igénylünk, amelynek a számát bátran megadhatjuk, akár még a három jegyű CVV ellenőrző kóddal együtt is. Ám erre az alszámlára érdemes csak a vásárlás előtt közvetlenül a netbankunkon átvezetni a vásárláshoz szükséges pontos összeget, ami így csak pár percig lesz az egyébként üres virtuális számlánkon. Ezzel a módszerrel nem tudnak tőlünk lopni, és így az "igazi" bankkártyánk adatait sosem kell a weboldalakon megadnunk.

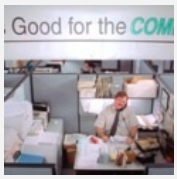
Ezt a legtöbb magyarországi banknál kérhetjük, de akár a Revolut virtuális kártyája is egy lehetséges megoldás lehet erre a célra. **Néha ellenőrizzük jelszavaink biztonságát a haveibeenpwned.com oldalon, és ha esetleg érintettnek látszunk, vegyük azt komolyan, és azonnal cselekedjünk. Emellett biztonságtudatos szokás, ha tudatosan és folyamatosan törekszünk arra, hogy minél kisebb digitális lábnyomot hagyjunk magunk után.**

4 komment
Címkék: csalás tippek identity megelőzés visszaélés theft adatlopás személyiséglopás welivesecurity.com

Ajánlott bejegyzések:


10 kiberbiztonságra veszélyes szokás


Ingyenes Omikron teszt vagy mégsem?



Karácsonyi vásárlás biztonságosabban

Stop adathalászat


Fiatal vagy? Ezekre az online csalásokra figyelj!

Kommentek:

Motorogre 2021.12.22. 16:18:12

fontos a folyamatos figyelemfelhívás értékeinkre, köszönjük a posztot.
Bár jól hangzik hogy a szolgáltatók szigorítottak a SIM-kártya cseréjén (ahogy a poszt közli), mégis hiányolom hogy adjon iránymutatást, mit tehet a felhasználó saját maga, ha pl. ilyet észlel ! És persze ez munkaszüneti napon késő éjjel történik ...
A többi tanács követhető, a jelszavainak mindenki maga URA, még éjjel is tud változtatni ...

Válasz erre

Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2021.12.22. 17:44:53

A SIMkártyás csalások többnyire céges előfizetőknél okoztak bajt, ott a gépről ellopott aláírási címpéldánnyal már jó eséllyel lehetett kártyacserét kezdeményezni, például ez is egy ilyen eset volt:
24.hu/belfold/2020/06/08/sim-cseres-atveres-csalas-adathalasz-telekom-otp-bank-lakashirdetes/

Idén szeptembertől végre szigorítottak valamennyit ezen a procedúrán:
index.hu/belfold/2021/09/28/nemzeti-media--es-hirkozlesi-hatosag-sim-kartya-csereje-uj-szabalyok/

Válasz erre

kvp 2021.12.22. 20:47:36

@Motorogre: "Bár jól hangzik hogy a szolgáltatók szigorítottak a SIM-kártya cseréjén (ahogy a poszt közli), mégis hiányolom hogy adjon iránymutatást, mit tehet a felhasználó saját maga, ha pl. ilyet észlel !"

Telefonszolgaltato felhivasa, szam tiltasa. Ha banki vagy barmilyen szolgaltatoi regisztraciohoz is hasznaltuk a szamot, akkor a bank es a tobbi szolgaltato felhivasa, account-ok zarolasa. Majd szemelyesen elmenni es uj sim-et kerni (ha van ra lehetoseg uj szammal), ezutan az uj szamot regisztralni az osszes erintett szolgaltatasnal es mindenhol jelszot is cserelni. Ez sokszor szemelyes megjelenest igenyelhet. (facebook eseten ez utobbi nehez, de egy bank eseten be tudunk menni)

Idealis esetben lehetoseget kellene adnia a szolgaltatonak arra, hogy letiltsuk a nem szemelyes kartyacseret, szemelyes esetben pedig alairas, arckep es szemelyi igazolvany ellenorzest kerjunk.

Válasz erre

Motorogre 2021.12.23. 06:08:18

@kvp: köszönöm. Ugye még nem próbáltad szombat éjjel ...
más: a személyes pénzintézeti cselekményeimnél kifejezetten kérdezem, hogy húzzam-e le a maszkot egy pillanatra az azonosításomhoz - a legtöbb esetben fel se néz az ügyintéző, csak az átadott két okmányt bámulja.
Értem én, hogy a személyes eljárásnál nincs hitelesebb - de lehetne ezt fejleszteni, akár a szolgáltatónál a szerződéskötéskor leadott titkos kóddal stb. - de ne az én dilettáns ötleteim szerint haladjon a világ, dolgozzák ki a szakemberek.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

vírustámadásokról, számítógépeink biztonságáról.

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

rambo archiv

- Rambo archívum

linkz

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

pcw cikkz

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

VVV 31.
VVV 32.
VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

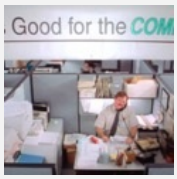
Kellemes Karácsonyi Ünnepeket!

2021. december 23. 06:35 - Csizmazia Darab István [Rambo]

Boldog Karácsonyi Ünnepeket kívánunk blogunk minden látogatójának!

Szólj hozzá!
Címkék: karácsony xmas boldog 2021.

Ajánlott bejegyzések:



Karácsonyi vásárlás biztonságosabban

Vírusmentes Boldog Új Évet 2021.

Kellemes Karácsonyi Ünnepeket!

Digitális ajándékok Karácsonyra

Vírusmentes Boldog Új Évet 2022.

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

NetAcademia Elemzés, kutatás-fejlesztés

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés
Regisztráció

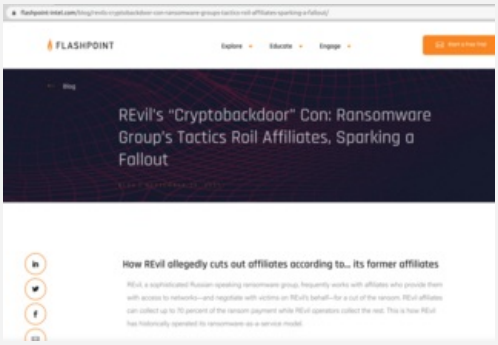
Vírusmentes Boldog Új Évet 2022.

2021. december 28. 11:04 - Csizmazia Darab István [Rambo]

Rövid idő van már csak hátra az idei esztendőből, így **a hagyományos jókívánságok mellett nagyon röviden visszatekintünk az év első három legfelkapottabb témájára**, amiket a legtöbben olvastak.

A harmadik legolvasottabb posztunk az az októberi cikk volt, amely szerint a Revil, vagyis Ransomware Evil csoport - akiket ismerhetünk például az Acer vagy a Kaseya elleni támadásról - már egy jó ideje bérbe adja a ransomware erőforrásait más elkövetőknek, cserébe pedig ezekből a harmadik felek általi támadásokból származó Bitcoin kifizetésekből is részesülnek. **Csakhogy volt ebben egy rejtett stikli is, ahogy Rejtő Jenő mondaná: a szerencse forgandó, de nem akkor, ha Tuskó Hopkins keveri a kártyát.**

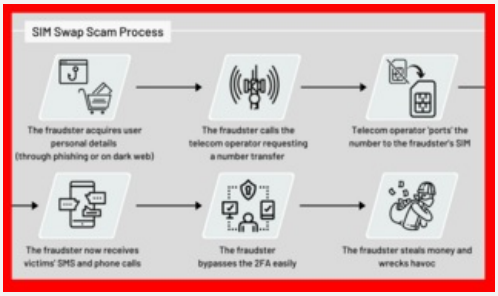
Itt ugyanis az derült ki, hogy a Revil csapat nem elégedett meg a normál részesedéssel a váltságdíjakból, hanem nagy valószínűséggel **elhelyeztek a programjukban egy olyan hátsóajtót is, ahol a ransomware tárgyalásokat is figyelemmel kísérhették, és ha elengedő nagy váltságdíjjal kecsegtetett egy üzlet, kizárva saját bérlőiket titokban ők maguk közvetlenül vették fel a kapcsolatot az áldozatokkal, és ők kasszírozták be a feloldó kulcsért járó összegeket.**



A második helyezettünk az a beszámoló lett, amelyből kiderült, hogy a Ragnar Locker zsarolóvírus banda egy olyan fenyegetést tett közzé, amelyben azt írják, hogy ha az áldozataik közül valaki kapcsolatba lép a rendőrséggel, bűnüldöző szervekkel, vagy adatmentési szakértőket bíznak meg az adatok visszafejtéséhez, illetve ilyen szakértőket kérnek fel a tárgyalási folyamat sikeres lefolytatása érdekében, akkor **a csoport minden ilyen esetben bosszúból haladéktalanul publikusan közzéteszi az ellopott bizalmas érzékeny adatokat.**

És végül a favorit, top #1 bejegyzés a SIM kártyacserés támadásról készült. Ennek lényege, hogy a bűnözők először célzottan adatokat gyűjtenek a kiszemelt áldozatról. Amikor már elegendő személyes információ van a kezében, a csaló kapcsolatba lép a kiszemelt áldozat mobiltelefon-szolgáltatójával, és a megszerzett személyes adatok segítségével megszemélyesíti a telefon valódi tulajdonosát, majd SIM kártyacserét kezdeményez, ezzel pedig átveszik az irányítást az áldozat mobiltelefonja felett, az eredeti SIM pedig elnémul.

Az ilyen típusú támadások esetében általában az a cél, hogy hozzáférjenek a célpont online fiókjaihoz, beleértve akár a bankszámláinak kiürítését is.



Nem maradt más hátra, mint hogy **Mindenmentes Boldog Új Évet kívánjunk, menteset mind a hagyományos COVID típusú omikron és egyéb variánsos, mind pedig a számítógépes vírusoktól, kártevőktől, kibertámadásoktól.**

Egészséget, boldogságot, sikert, belső békét minden Kedves Olvasónknak. 2022-ben is megyünk majd tovább, szokás szerint folytatjuk a 2007-ben elkezdett munkát.

Szólj hozzá!
Címkék: újév buék köszöntés boldog újesztendő 2022.

Ajánlott bejegyzések:

Vírusmentes Boldog Új Évet 2021.

Kellemes Karácsonyi Ünnepeket!

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

top 5z

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

about

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

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

rambo archiv

Rambo archívum

linkz

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

pcw cikkz

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

biztonság

Nincs megjeleníthető elem

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

- Belépés
- Regisztráció