A ransomware-ek evolúciója

CSIZMAZIA-DARAB ISTVÁN | 2016.05.20. | BIZTONSÁG

A felhasználók többségének akkor jut eszébe védekezni, ha már beütött a ménkű. Pedig folyamatos védekezésnél nincs hatásosabb. Csizmazia-Darab István írása.

Érdekes módon egy átlag felhasználónak legtöbbször egyáltalán nem izgatja magát azon, hogy vírussal fertőzött a gépe, mert például elhanyagolja a frissítéseket. Ám ha adatait – fájlokat, dokumentumokat, fényképeket – titkosítja egy zsaroló kártevő, szinte mindenkit azonnal érdekelni kezd a fertőzés és védekezés.

Az alábbiakban végiglépdelünk a zsaroló programok evolúciós állomásain, végül pedig a hatékony védekezéshez is szolgálunk néhány hasznos jó tanáccsal.

De mi az a ransomware?

Ransomware-nek – ezt a kategóriát magyarul zsaroló programnak szokás hívni – a váltságdíjat követelő kártevőnek nevezzük. Az ilyen programok titkosítják az eszközeinken található fájlokat, és utána váltságdíjat követelnek a rendszer vagy a fájlok feloldásáért.

Elsősorban e-mailek, csatolmányok (.zip, .exe) mellékleteiben, illetve fertőzött weboldalak fertőzött reklámjai (malwertising) terjesztik, de megtalálhatóak fájlcserélőkön az ún. warez programokban, de botnetek is terítik. Az sem ritka, hogy USB-s eszközökkel próbálják terjeszteni, ahogy az sem, hogy sebezhető vagy nyitott RDP-n (Remote Desktop Port) keresztül juttatják a célgépbe.

Ma már egész kis iparág alakult ki az ilyen programok körül. "Bagóért" kínálnak ransomware-készítő, -terjesztő készletek is nehezítik a helyzetet. Manapság már 400 dollárért is lehet kapni olyan Cryptolocker/Cryptowall kitet, melyhez teljes körű technikai támogatás jár.

A zsarolók általában 100-500 eurónyi összeget követelnek a titkosítás feloldásáért, ám a váltságdíjat szinte mindig a virtuális és nehezen lenyomozható bitcoinban kell fizetni. A lenyomozhatatlanságot segíti az is, hogy a károkozó távoli kommunikációs szervere (C&C) általában az anonimitást biztosító TOR hálózaton található, ami a hatóságoknak alaposan megnehezítik a felderítést.

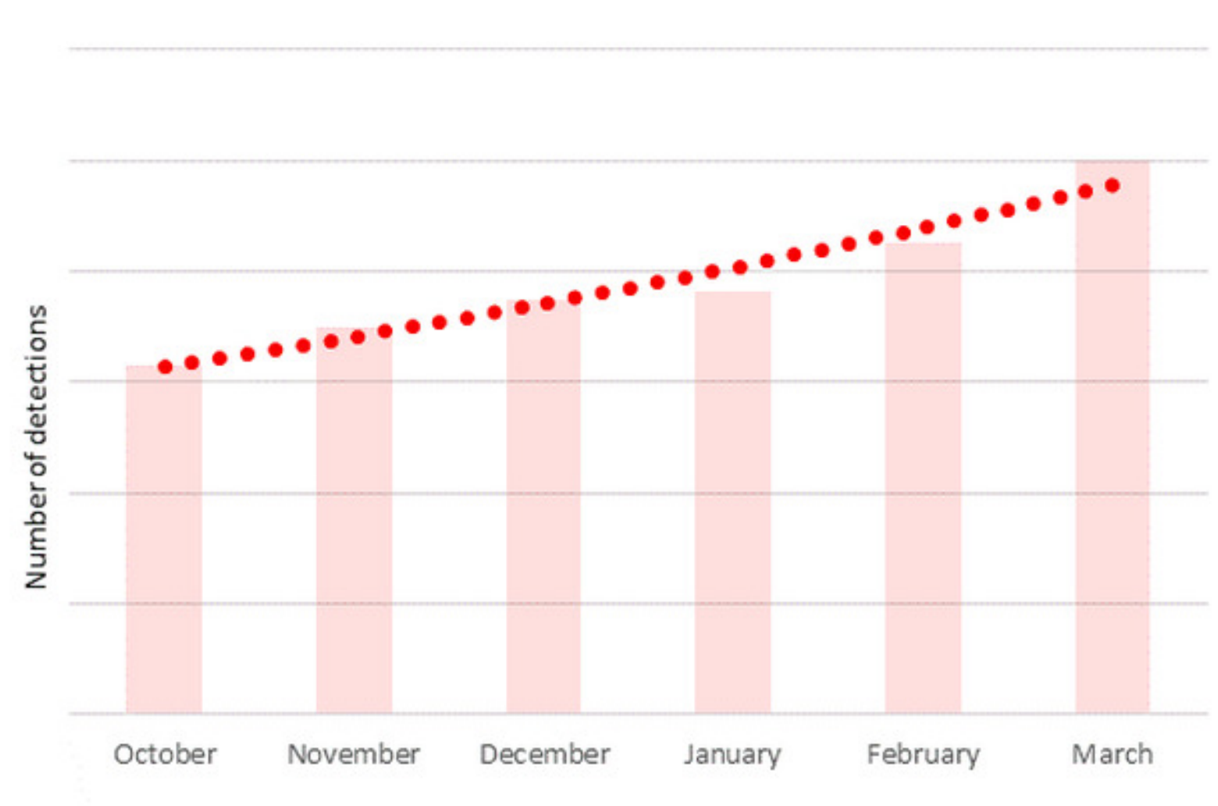
A váltságdíj megfizetésére jellemzően 48 vagy 72 órás határidőt adnak a támadók. Ha a határidő lejár, a zárolt adatok végleg elvesznek.

Az ilyen támadások célja egyértelműen a könnyű pénzkereset. A ransomware komoly pénztermelő ágazattá vált. A jó a megtérülési arányra jellemző, hogy az FBI szerint a ransomware-támadásokat végrehajtó bűnbandák havi bevétele egymillió dollár körül mozog – természetesen adómentesen. A jó megtérülés azonban az egész "iparágra" igaz. Az USA-ban már 2008-ban több pénzt termelt a bűnözőknek a kiberbűnözés, mint a drogkereskedelemből: egyes becslések szerint 105 milliárd dollárt kaszáltak.

Negyedszázada velünk élnek

Az első ransomware megszületését egy 1989-es esethez kötik. Egy cég AIDS-szel kapcsolatos információs floppylemezeket küldött szét huszonhatezer egészségügyi intézmény címére. A lemez egy aljas programozási trükkel operált, és egy saját algoritmus alapján folyamatosan titkosította a merevlemezen az állományokat és a könyvtárakat. A 99 újraindítást követően az elkövető kinyomtatott üzenetében egy panamai postafiókba kért váltságdíjat. Később sikerült elfogni készítőjét. Kiderült, hogy Joseph L. Popp, aki Panamában a PC Cyborg Corporation nevű céget jegyezte, közel egy évig készítette elő ezt az akcióját.

A detektált zsaroló programok mutatta trend az ESET LiveGrid adatai alapján



(Forrás: ESET)

A biznisz azonban az utóbbi pár évben pörgött fel igazán. A manapság ismert újszerű fenyegetést alkalmazó zsarolóprogramok mostani hullámának első darabja a CryptoLocker volt. A 2013. szeptemberében felbukkant károkozó 1024, később pedig 2048 bites egyedi aszimmetrikus RSA kulcsot alkalmazott, azaz más kulcs kell a titkosításhoz, és más a feloldáshoz. A titkosítás folyamán végigment minden felcsatolt meghajtón, USB tárolón, hálózati meghajtón, illetve megosztáson.

A következő jelentősebb kártevő a 2014. áprilisában felbukkanó CryptoWall volt. Ez 500 dollárnyi bitcoint követelt a titkosítás feloldásáért. Csak 2014 márciusától augusztusáig több mint 600 ezer PC-t fertőzött meg. Egyes statisztikák szerint ebben az időszakban 5.2 milliárd fájlt titkosított, és összesen 1,1 millió USD váltságdíjat zsebeltek be vele a bűnözők.

A zsarolók is egyre gyorsabban fejlődnek

A ransomware-ek fejlődése eleinte lassú volt, később azonban felgyorsult. A CryptoWall után alig két hónappal, 2014 júniusában tűnt fel a CTB-Locker. Nevét a RSA-nál erősebb Elliptical Ccurve Cryptography (ECC) titkosítás után kapta: a CTB a Curve-Tor-Bitcoin rövidítése. Szintén adott lista szerinti kiterjesztésű állományokat keresett. A feloldásért már 8 bitcoint követelt.

A CTB-Locker újszerű módszerrel erősítette a fizetési hajlandóságot. Az áldozat tesztelhette, hogy valóban működik-e a visszaállítás: 5 tetszőleges állományt ingyen helyreállíthatott. A zsaroló egyébként 96 órát, azaz 4 napot adott a váltságdíj kifizetésére, és ha az nem érkezett meg, duplázta a követelt összeget.

Ebből is látszott a ransomware-ek fejlődése, hogy a CTB-Locker már nem csak a windowsos gépeket támadta. Lényegében minden alternatív platformon működött.

Szintén 2014 júniusában jelent meg a Simplocker, amely androidos eszközök SD-kártyáit titkosította. Szerencsére a legelső változatban volt egy durva kódolási hiba, így a jelszóhoz konstansként hozzá lehetett férni.

Egy elhagyott zsaroló

2015 februárjában járunk, amikor feltűnt TeslaCrypt. Ez az Adobe Flash egy meghatározott sebezhetőségét (CVE-2015-0311) használta ki, és 1,5 bitcoint követelt. Érdekessége főleg abban rejlik, hogy a szokásos állománytípusok titkosítása mellett a játékfájlok, játékállások fájljaira is veszélyt jelentett, emiatt az aggódó játékosok talán nagyobb arányban fizettek. Érdekesség, hogy épp a napokban derült ki, hogy a TeslaCrypt fejlesztői felhagytak a károkozó továbbfejlesztésével, sőt a mesterkulcsot is közzétették, aminek a segítségével el lehetett készíteni egy visszafejtő programot.

A fejlődés velejárója volt, hogy egyre gyakoribbak voltak az Android platformot támadó károkozók. A 2015 szeptemberében felbukkanó LockerPIN például képes volt megváltoztatni a készülékek PIN kódját, lezárta a készülék képernyőjét. A feloldásért 500 dollár váltságdíjat kért.

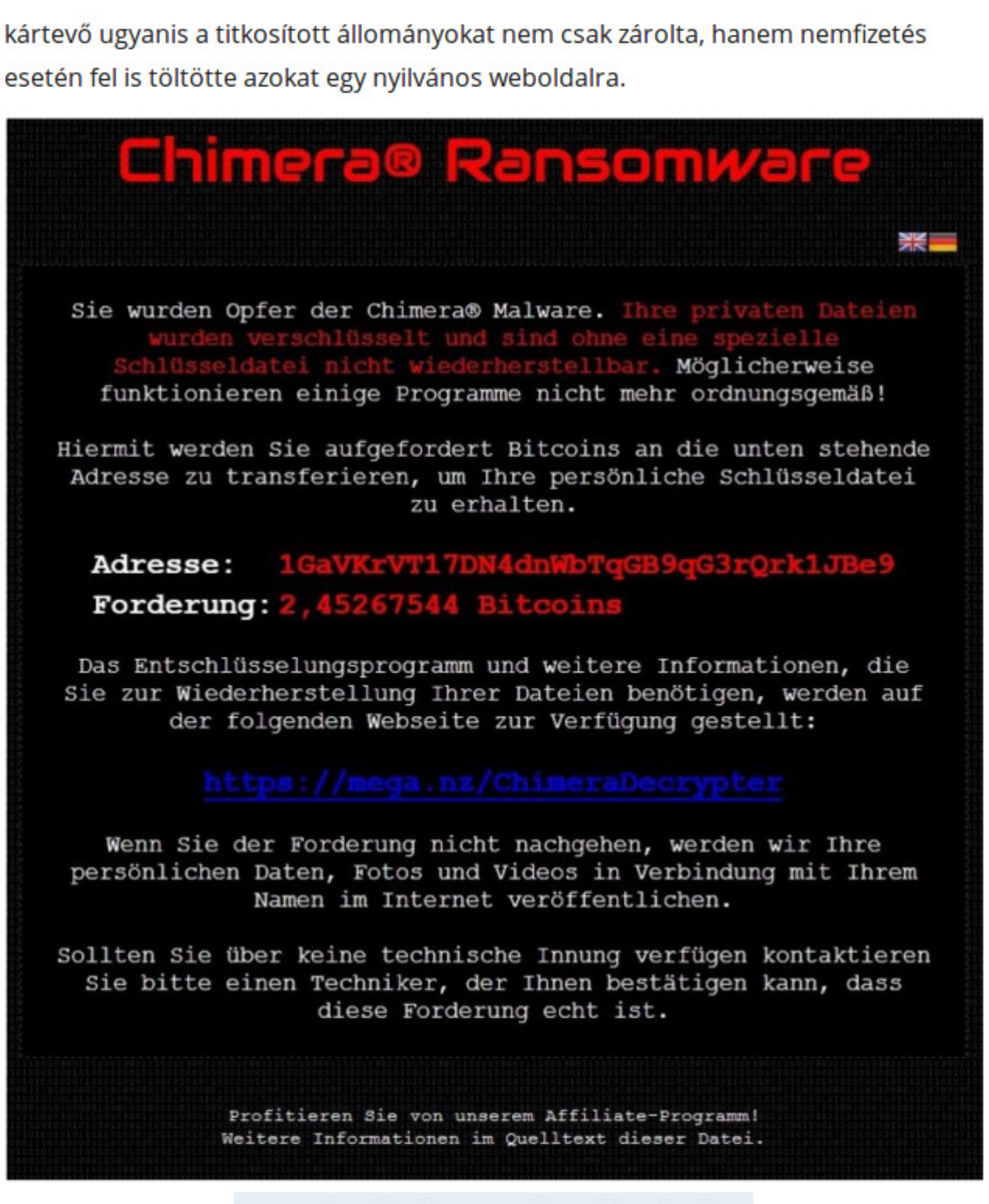
A tavalyi év egyik legkellemetlenebb darabja azonban a Power Worm volt. Az októberben készült ransomware a 2 bitcoint követelt a feloldásért, ami után jött a kellemetlen meglepetés. A zsaroló kártevő ugyanis hibásan volt megírva, így hiába fizetett valaki, esélye sem volt arra, hogy adatait visszanyerje.

A folyamatos fejlesztés eredményeképpen tavaly a korábbi kártevők új változatai is felszaporodtak. Például 2015 novemberében jött a CryptoLocker 4.0, amely már nemcsak a fájlok tartalmát, hanem a fájlneveket is titkosította. Így viszont azt sem lehetett már felmérni, hogy pontosan mi veszett el, ahogy az a lehetőség is elveszett, hogy az ingyenes teszt visszaállítással a legértékesebb fájljainkat visszaszerezzük.

Mérföldkő: Linux.Encoder.1

Tavaly novemberben fontos mérföldkőhöz ért a ransomware-világ: megjelent a Linux.Encoder.1. Ez ugyanis a LAMP (Linux, Apache, MySQL, PHP) webszervereket támadta – azaz a zsarolók itt már vállalati rendszereket ellen támadtak. A Linux.Encoder.1 380 dollárnyi bitcoint követelt a titkosítás feloldásáért. A program azonban szerencsére kezdetleges volt, így rövid idő után készült hozzá univerzális visszakódoló, amellyel fizetés nélkül helyre lehetett állítani az állományokat.

A Chimera, amely decemberben jelent meg, azonban már profi volt, ráadásul kétféle módon is zsarolta a vállalatokat. A TOR hálózaton keresztül kommunikáló kártevő ugyanis a titkosított állományokat nem csak zárolta, hanem nemfizetés esetén fel is töltötte azokat egy nyilvános weboldalra.



Chimera® Ransomware

Sie wurden Opfer der Chimera® Malware. Ihre privaten Dateien wurden verschlüsselt und sind ohne eine spezielle Schlüsseldatei nicht wiederherstellbar. Möglicherweise funktionieren einige Programme nicht mehr ordnungsgemäß!

Hiermit werden Sie aufgefordert Bitcoins an die unten stehende Adresse zu transferieren, um Ihre persönliche Schlüsseldatei zu erhalten.

Adresse: 1GaVKrVT17DN4dnWbTqGB9qG3rQrk1JBe9
Forderung: 2,45267544 Bitcoins

Das Entschlüsselungsprogramm und weitere Informationen, die Sie zur Wiederherstellung Ihrer Dateien benötigen, werden auf der folgenden Webseite zur Verfügung gestellt:

https://mega.nz/ChimeraDecrypter

Wenn Sie der Forderung nicht nachgehen, werden wir Ihre persönlichen Daten, Fotos und Videos in Verbindung mit Ihrem Namen im Internet veröffentlichen.

Sollten Sie über keine technische Innung verfügen kontaktieren Sie bitte einen Techniker, der Ihnen bestätigen kann, dass diese Forderung echt ist.

Profitieren Sie von unserem Affiliate-Programm!
Weitere Informationen im Quelltext dieser Datei.

Ha nem fizetünk, a Chimera mindent nyilvánosságra hoz

Az idén áprilisban megjelent Samsam szintén a vállalati körre specializálódott: javítatlan Red Hat JBoss vállalati szervereket keresett, és azokat fertőzte meg. Ennek során RSA kulcspárt generált. A feloldásért 1 bitcoint követelt gépenként, és a beszámolók szerint rengeteg vállalat, közintézmény (például kórház) szerepelt az áldozatok között.

A Locky, amely idén februárban jelent meg, Word dokumentumban, a fájlba ágyazott makró segítségével terjedt. Ha a felhasználó engedélyezte a makrók futását, fertőzött. A Word és Excel fájlokat titkosította, és közben eltávolított minden árnyékmásolatot (VSS, Volume Snapshot Service). Plusz "szolgáltatásként" ha talált a gépen bitcoinos pénztárca fájlt (wallet.dat), azt is megrongálta, hogy a váltságdíjat fizető csak bitcoin vásárlásával tudjon fizetni.

Nincs védett platform!

Két hónapja megjelent az első valódi zsaroló Macintosh OS X-re. A KeRanger a Transmission nevű torrentkliensben terjedt el annak hivatalos weboldalról úhy, hogy Transmission 2.90-es verziójának március 4-i kiadását ismeretlenek eltérítették, és egy hamis verzióra irányították a letöltőket. Mivel a kártékony csomag rendelkezett érvényes fejlesztői aláírással, így a 10.8-al bevezetett Apple Gatekeeper Execution Prevention védelmi technológia sem volt képes megállítani.

A sötét oldalon gőzerővel folyó fejlesztések egyik érdekes terméke a Cerber (Kerberosz, a görög mitológiában az alvilág kapuját őrző háromfejű kutya). Ez szintén márciusban bukkant fel. Az AES titkosítást használó zsaroló programnál 1,24 bitcoin volt a váltságdíj, ami nem fizetés esetén hét nap után duplázódott. A Cerber a fenyegetést is kimaxolta: egy robotszerű géphang 12 nyelven (: angol, francia, portugál, török, német, kínai, lengyel, spanyol, japán, olasz, arab, holland) mondott el egy fizetésre felszólító hangüzenetet. A másik izgalmas momentumként a károkozó ellenőrzi, hogy a számítógép a Szovjetunió utódállamaihoz tartozik-e. Ugyanis az ottani gépek ellen nem indít támadást, azaz nem titkosít.

A vírusírók is hibázhatnak

A március a ransomware-ek nagy hónapja volt. Akkor jelent meg ugyanis a Petya trójai, amely újabb fejlődési állomást jelez. Már nem csak titkosított, hanem a teljes meghajtót vette célba. Módosította a meghajtón az MBR-t (Master Boot Record), és titkosította az MFT-t (Master File Table). A feloldásért 0,9 bitcoint követelt. Szerencsére készítője a kevésbé biztonságos Salsa10 algoritmust használta a titkosításhoz, így lehetett készíteni ellene egy univerzális visszaállító segédprogram. Az ingyenes program, amely a GitHubról letölthető, azonban elég "pilótavizsgás", így csak a gyakorlottabbaknak ajánlható.

Csizmazia-Darab István
Az IT-biztonsági szakértő a Sicontact munkatársa. Évek óta vezeti a sikeres Antivírus blogot. A cikk a CIO Hungaryn május 5-én elhangott előadás cikké formált változata.

Hasonlóképpen járt a Jigsaw is, amely szintén áprilisi termés. A horrorfilmekből visszaköszönő alakkal jelentkező kártevő 0,4 bitcoint követelt. A károkozó egy kegyetlen játékkal próbálta gyorsítani a fizetést: 60 percenként fájlokat törölt: az első órában egyet, a másodikban kettőt, aztán négyet, és így tovább a kettő hatványai szerint. A Windows újraindítását extra büntetéssel sújtotta: ilyenkor egyszerre törölt 1000 fájlt véglegesen. Szerencsére azonban a Jigsaw írója sem végzett tökéletes munkát, így elkészülhetett ellene az univerzális helyreállító, a JigSawDecrypter, amely számos helyről letölthető.

Fertőzött hirdetések JavaScript kódjával terjedt (malvertising) összeállításunk utolsó darabja, a Cyber.Police, amely szintén a múlt hónapban jelent meg. Az Android rendszereket támadó károkozó újított a váltságdíj terén: nem bitcoint kért a képernyőzár feloldásáért, hanem két 100 dolláros Apple iTunes ajándékkártya-kódot. A Cyber.Police ugyan eltávolítható gyári resettel, de ez adatvesztéssel jár, már ha nincs rendszeres mentésünk képeinkről, videóinkról, adatainkról.

Frissesség, éberség... ez nem stréberség

Mit lehet tenni, ha egy ilyen kártevő bejut a gépünkbe? Mindenekelőtt a megelőzésre kell koncentrálni. A fertőzés esélye jelentősen csökkenthető ugyanis, ha az operációs rendszerünket és alkalmazásainkat gondosan és időben frissítjük, haladéktalanul telepítjük a megjelenő biztonsági javítófoltokkal, valamint valamilyen külső gyártótól származó teljes körű internetbiztonsági csomagot – vírusirtót, tűzfalat, kémprogram elleni modult stb. – használunk.

Hasznos tud lenni az is, ha szokásunká válik, hogy óvatosan, azaz biztonságtudatosan kezeljük a spameket, e-mailek mellékleteit. Emellett technikai trükköket is bevethetünk, például a letilthatjuk a %APPDATA%, %TEMP% programfuttatást, a tűzfalon blokkolhatjuk a TOR forgalmat, vagy letilthatjuk a távoli asztal kapcsolatot (RDP).

Fontos az is, hogy a biztonsági szoftverekből a legújabb termékverzió fusson, megfelelően konfigurálva. Érdemes beállítani az olyan szolgáltatásokat – az ESET-nél például a felhőalapú Live Gridet –, amelyek segítségével a számítógépek ellenőrzése és az új kártevők felismerése még gyorsabbá és hatékonyabbá válik. A LiveGrid egyébként aktívan blokkolja a zsarolóprogramok folyamatát is.

Fizessünk?

Essen pár a szó a váltságdíjról is. A biztonsági cégek ezt – az emberrablási esetekhez hasonlóan – nem javasolják. Mivel ilyenkor bűnözőkkel üzletelünk, nincs garancia nincs arra, hogy egyáltalán kapunk valamilyen működőképes visszaállító kódot. A legtöbb esetben a fizetés után nem érkezik semmi. Éppen ezért a legfontosabb a megelőzés, amihez hozzátartozik a rendszeres adatmentés is. Enélkül nagyon kicsi az esélyünk az adatvesztés elkerülésére.

Zárásképpen hadd villantsak fel egy szokatlan szempontot. Csányi Vilmos etológus egyik kedvenc példájával élve: ha a távoli marslakók vizsgálnák a földlakók mostani, zsaroló programmal kapcsolatos helyzetét, akkor szemúk előtt szépen kirajzolódna az evolúció. Mert mit is próbált már évek óta minden IT-biztonsági szakértő megértetni a felhasználókkal? Hogy legyen mentés. Ez a figyelmeztetés azonban sokszor süket fülekre talált.

A mostanra már több ezer fajtát, variánst felvonultató zsaroló kártevők azonban – és ezt látják a marslakók a távolból – képesek voltak arra, hogy rábírják a felhasználókat, hogy fontos állományaikat rendszeresen mentsék külső adathordozóra. Jó esetben más kárán, kevésbé jó esetben a saját kárukon tanulták meg mindezt. Földlakóként elszenvedni ezeket a megpróbáltatásokat nem kellemes, de távolról nézve a fejlődés látható: egyre többen megértik a gondos mentés fontosságát.

ENNYI NEM ELÉG? IRATKOZZON FEL HÍRLEVELÜNKRE! Megosztom Share Tweet

HIRDETÉS

IBM QRadar – az IT-biztonság központi agya

A Biztonsági Intelligencia egyszerre kínál megoldást a magasan képzett emberi erőforrás szűkösségére és a kifinomult, folyamatosan változó online támadások megbízható kivédésére.

A HÓNAP TÉMÁJA

Ezért sikeresek még mindig a mainframe-ek

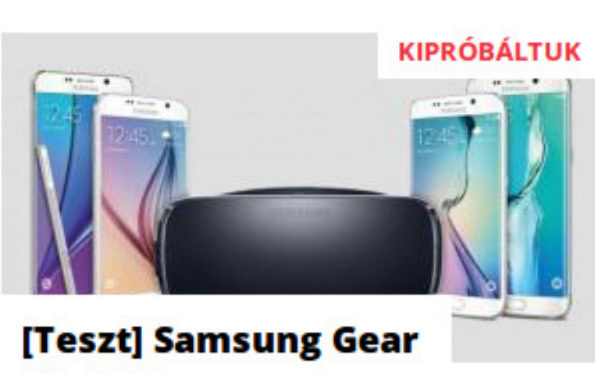
Az elmúlt fél évszázadban sorra érték a kihívások a platformot, népszerűsége azonban továbbra is töretlen. Utánajártunk az okoknak.

A MELLÉKLET TÁMOGATÓJA AZ INTERCOMPUTER

VENDÉG CIKK

Ez nagyon sok pénzbe fájhat a magyar vállalatoknak

Minden eddiginél több szoftvergyártói audit vár rájuk. Az IPR-Insights felmérése a magyar piacról.



KIPRÓBÁLTUK

[Teszt] Samsung Gear VR: fullba nyomja a virtuált

A két új csúcsmodell nem változtat, legfeljebb csiszol a bevált recepteken.

Bitport
Tetszik az oldal 2,7 ezer kedvelés
Az ismerőseid közül te lehetsz az első, akinek ez tetszik.

BIZTONSÁG

Magyarországon is készülnek a Dell-EMC fúzió lezárására

A jövőálló technológiák mellett az EMC-fúzióról is beszéltek a Dell európai vezetői a Be/Future Ready/'16 nemzetközi eseménysorozat budapesti állomásán.

Ön sem informatikus, de munkája során az információtechnológia is gyakran befolyásolja döntéseit? Ön is informatikus, de pénzügyi és gazdasági szempontból kell igazolnia a projektek hasznosságát? Mi közérthetően, üzleti szemmel dolgozzuk fel az infokommunikációs híreket, trendeket, megoldásokat. A Bitport ötödik éve közvetít sikeresen az informatikai piac és a technológiát hasznosító döntéshozók között.

© 2010-2016 Bitport.hu Média Kft. Minden jog fenntartva.

KÖVETKEZŐ RENDEZVÉNYÜNK

CIO Hungary 2016: a digitális transzformáció