SAJTÓKÖZLEMÉNY

Budapest, 2014. december 17.

Európa a bitcoint követelő zsarolóprogram árnyékában

Az ESET kutatói elemezték a rosszindulatú programcsalád működését.

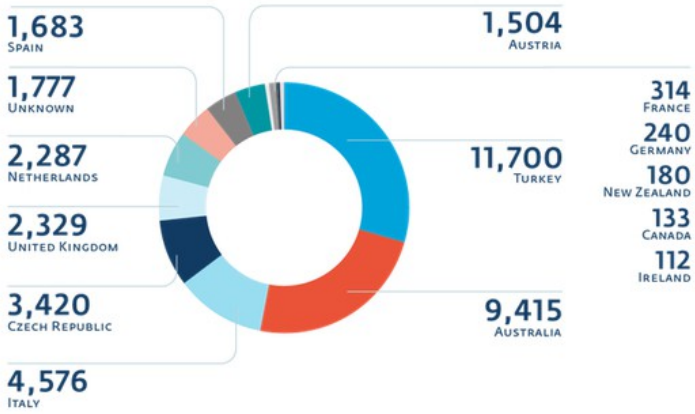
A vezető, proaktív védelmet kínáló biztonságtechnológiai vállalat, az ESET kanadai kutatói megvizsgálták az először az év elején megjelenő TorrentLocker nevű zsarolóprogram működését. A malware legutolsó változata legalább 40 000 rendszert fertőzött meg pár hónap alatt, leginkább európai országokban szedve áldozatait. Az ESET biztonsági kutatói most elkészítették a zsarolóprogramra vonatkozó kutatás háttéranyagát, amely a malware viselkedésének vizsgálatát és részletes elemzését tartalmazza.

Az ESET Win32/Filecoder.DI névvel illeti a TorrentLocker most elemzett verzióját. Az elnevezés a malware korai korszakából ered, hiszen a program ezt a "Bit Torrent Application" elnevezésű registry kulcs bejegyzést használta konfiguráció beállításainak tárolására.

Hogyan működik a zsarolóprogram?

Az ESET összefoglalója szerint a TorrentLocker hét különböző módon terjedt és a telemetriai mérésnek köszönhetően kiderült, hogy a malware első nyomai 2014 februárjában bukkantak fel. A rosszindulatú program folyamatosan fejlődik, legfejlettebb változata augusztustól szedte áldozatait.

A zsarolóprogramnak ez a változata dokumentumokat, képeket és egyéb fontos fájlokat titkosít a felhasználó eszközén és váltságdíj fejében engedélyezi a hozzáférést a fájlokhoz. Jellegzetessége, hogy a váltságdíjat kizárólag virtuális valutában lehet kifizetni és akár 4 bitcoint (ez nagyjából 1180 euró vagy 1500 dollár) is követelhet. Az utolsó kampányban a TorrentLocker 40 000 számítógépet fertőzött meg és több mint 280 millió dokumentumot titkosított. A célzott országok zöme európai volt, de a fertőzés Kanadában, Ausztráliában és Új-Zélandon is megjelent. Szerencsére „csak" 570 áldozat fizette ki a váltságdíjat, így összesen 585,401 bitcoin ütötte a TorrentLocker mögött álló emberek markát.



"Azt gondoljuk, hogy a TorrentLocker mögött álló személyek ugyanazok, akik a Hesperbot nevű banki trójai család mögött álltak. - mondta Marc-Etienne M. Léveillé, az ESET kanadai kutatója. *„A TorrentLocker-ben a támadók reagáltak az online biztonságtechnikai jelentésekre, hiszen megkerülik az ilyen típusú kártevők felismerésére szolgáló eljárásokat és megváltoztatták az AES (Advanced*

Encryption Standards) titkosítási módszerüket CTR-ről (Counter mode) CBC típusúra (Cipher block chaining mode), annak hatására, hogy ismertté vált egy módszer a kulcsfolyamuk megszerzésére. Ennek következtében a TorrentLocker áldozatai már nem tudják visszaállítani a dokumentumaikat az elkódolt fájljaik és az egyszerű szöveges állományának kombinálásával megszerzett kulcsfolyam segítségével."

Hogyan terjed a fertőzés?

A későbbi áldozat egy fertőzött dokumentumot tartalmazó kéretlen e-mailt kap. A mellékelt fájl megnyitása általában egy ki nem fizetett számlát, csomagok nyomon követését vagy kifizetetlen gyorshajtási büntetést tartalmaz. Az e-mail hitelességét erősíti, hogy az áldozat közvetlen környezetéből származó üzleti vagy kormányzati honlapokat utánoz. Ha olyan áldozat olvasta az emailt, aki nem a célországból kattintott a linkre és kezdeményezte az oldal letöltését, akkor automatikusan a Google search oldalra irányította a kártevő. *„Az áldozatok becsapásának érdekében a támadók CAPTCHA képeket is illesztettek a levelekbe, így keltve hamis biztonságérzetet."* – magyarázza Léveillé.

A kutatás és a malware bemutatása WeLiveSecurity.com blogon érhető el:
http://www.welivesecurity.com/2014/12/16/torrentlocker-racketeering-ransomware-disassembled-by-eset-experts/

A részletes elemezés (white paper) pedig itt olvasható:
http://www.welivesecurity.com/wp-content/uploads/2014/12/torrent_locker.pdf

Az ESET-ről:
A több mint 25 éves, díjnyertes NOD32 technológiát kifejlesztő ESET a proaktív védelem úttörője, az üzleti és otthoni biztonságtechnikai szoftvermegoldások nemzetközi szállítója. A vállalat piacvezető a fenyegetések észlelésében és megelőzésében. Az 1987-ben megjelent ESET NOD32 Antivirus világelső az elnyert Virus Bulletin "VB100" díjak számát tekintve, illetve a vizsgálatok 1998-as fennállása óta eddig minden szabadon terjedő vírust vagy férget észlelt és kivédett. Az ESET NOD32 Antivirus, ESET Smart Security és az ESET Cyber Security (biztonsági megoldás Mac-re), valamint a mobiltelefonok és táblagépek védelmét biztosító ESET Mobile Security a legajánlottabb biztonsági megoldások közé tartoznak, a termékekben milliók bíznak meg világszerte. A vállalat központja Szlovákiában, Pozsonyban található, regionális terjesztési központokkal rendelkezik San Diegóban (USA), Buenos Airesben (Argentína) és Szingapúrban, valamint irodái vannak São Paulóban (Brazília) és Prágában (Csehország). Az ESET több mint 180 országban, köztük Magyarországon, rendelkezik kiterjedt partneri hálózattal. További információ: www.eset.hu

A Sicontactról:
A Sicontact Kft. az egyik legjelentősebb, IT biztonsággal foglalkozó hazai szoftverdisztribútor. Mottója és küldetése, ami köré termékportfolióját kialakította: „biztonság a digitális világban". A Sicontact Kft. Magyarországon az ESET NOD32 technológiára épülő termékeivel mind a lakossági, mind a vállalati szegmensben meghatározó piaci szereplő. A cég 2007-ben megszerezte az ESET ausztriai képviseletét, így azóta regionális piaci szereplőként tevékenykedik. A Sicontact kizárólagos magyarországi disztribútora a Unified Threat Management (UTM) hálózatbiztonsági eszközök terén piacvezető Cyberoam termékeinek, valamint portfóliójában megtalálható a helyi és távoli rendszerdiagnosztika, a hálózatfigyelés, a távvezérlés és a licencmenedzsment terén kiemelkedő képességekkel rendelkező AIDA64 szoftver is.

A Sicontact Kft. több ízben elnyerte a kitüntető Business Superbrands díjat. Az ESET Smart Security programcsomagot többször is az év antivírus megoldásának választották. A Sicontact Kft. az ESET szoftvereit a lehető legrugalmasabb konstrukciókban kínálja. Az ESET biztonsági szoftverek licencelése során a gyorsan változó körülményeket is figyelembe veszi, így például az ESET szoftverek a licencidőszak alatt bármikor újratelepíthetők az adott számítógépre, továbbá az unilicenc konstrukció keretében a munkaállomásokon a megvásárolt ESET licenccel egyaránt használhatók a Windows, Linux és Mac operációs rendszerre fejlesztett ESET termékek, így az operációs rendszer cseréje esetén nem szükséges új licencet vásárolni. A Sicontact Kft. az ESET szoftverekhez és a Cyberoam termékeihez díjmentes terméktámogatást és távsegítséget biztosít, mind az otthoni, mind a vállalati felhasználók számára, így az ügyfelek jelentős időt és pénzt takarítanak meg.

További információ:
Benedikt Károly
+36-30-984-4904
LWp Kommunikáció
karoly.benedikt@lwpk.hu