SAJTÓKÖZLEMÉNY

Budapest, 2015. január 21.

Év eleji rohamot indított a váltságdíjszedő kártevő új változata
Magyarországon és a régióban is érdemes odafigyelni és frissíteni a biztonsági programokat

A tavalyi év utolsó hónapjában nem volt jelentős változás vírusfronton

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, amelyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. A decemberi toplista mellett egy hazánkban is jelentős januári veszélyre figyelmeztet a cég. A napokban ugyanis egy váltságdíjszedő és fájljainkat titkosító kártevő vadonatúj változatát jelentették Magyarországról, valamint a kelet-közép európai régió több országából is. A naprakész ESET biztonsági programmal rendelkező felhasználók gépe már megfelelő védelemmel van ellátva.

A decemberi nemzetközi kitekintés előtt mindenképpen meg kell említeni, hogy a napokban **a váltságdíjszedő és fájljainkat titkosító kártevőből egy vadonatúj változat jelent meg Magyarországon.** A fertőzésről először január 19-én kettő órakor kapott bejelentést az ESET magyarországi csapata, akik azonnal elkezdték a probléma vizsgálatát. A begyűjtött minták alapján az ESET szakértői megállapították, hogy a fájlok elkódolásáért a Win32/Filecoder.DA.Gen malware legújabb verziója felelős, amely CTB-Locker néven is feltűnhet. A biztonságtechnológiai vállalat központjában haladéktalanul elkészítették a kártevő felismerésére szolgáló mintát, amit még aznap délután publikáltak[1] a frissítési szervereken, így a védelem már megérkezett a felhasználók számítógépeire. Mivel a fájlok dekódolása jelenleg sajnos nem megvalósítható, így az offline backupból való visszaállítás javasolt a biztonsági mentésből, amennyiben már fertőződött a gépünk. A szakemberek ezen felül felhívják a figyelmet az érintett Windows rendszerek azonnali frissítésére és a felhasználók oktatásra, arra vonatkozóan, hogy soha ne nyissanak meg ismeretlen mellékletet, csak miután megbizonyosodtak annak valódiságáról. A biztonsági program finomhangolásaként javasolt az ESET Live Grid és a Kiterjesztett heurisztika a fájlok futtatásakor funkciók bekapcsolása, azokon a gépeken, ahol ez esetleg jelenleg nem aktív.

Decemberi vírustoplista

Negyedik hónapja vezeti a listát a HTML/Refresh. 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. A lista első felében nem történt változás, a hátsó szekcióból kiesett a HTML/ScrInject, míg az egyetlen újonc a nyolcadik helyen felbukkanó LNK/Agent.AV trójai. Ez tulajdonképpen egy olyan kártékony link hivatkozás, amelyik különféle parancsokat fűz össze és futtat le észrevétlenül a háttérben. Működését tekintve hasonlít a régi autorun.inf mechanizmusára. Változatlanul listatag az INF/Autorun vírus, amely az előző hónaphoz képest egy pozícióval még javított is rajta. Az, hogy hét esztendős kártevők egyáltalán szerepeljenek egy 2015-ös listában, egészen elképesztő, hiszen a külső adathordozókon terjedő Autorun vírus biztonsági frissítései már hosszú évek óta rendelkezésre állnak. Nyilvánvalóan a már tavaly óta nem támogatott, de még mindig rengeteg helyen használt és elhanyagolt javításokkal rendelkező Windows XP is alaposan kiveszi ebben a részét.

A banki átverésekről

Az ESET Radar Report e havi kiadásában ezúttal olyan új átverésekre hívják fel a figyelmet, amelyben a csalók egyenesen a bank csalásellenes osztálya nevében (vagy éppen a rendőrség nevében) telefonálnak, és azt

[1] a frissítést elérhetővé tették a 11038 számú vírusdefiníciós adatbázisban 2015.01.19-én 16:10-kor

állítják, hogy gyanús aktivitást észleltek az érintett bankszámláján. Ilyen hívások esetében sokan nem is gyanakszanak, mivel személyes adataik (név, telefonszám) a hívó fél tulajdonában vannak. A forgatókönyv természetesen a szokásos, "ellenőrzésképpen" elkérik a PIN kódunkat. Sose felejtsük el, hogy egy bank sohasem, tényleg hangsúlyozzuk: sohasem fogja kérni, és nem is kérheti tőlünk a PIN kódunkat, sem levélben, sem telefonon, sem pedig személyesen. A csalók az átvert áldozatnak azt mondják, hogy kiküldenek egy futárt a "kompromittált" bankkártya begyűjtésére. Ez is egy teljességgel szokatlan lépés, aminél mindenkinek gyanút kellene fognia, hiszen jobbára inkább azt kérik, hogy mi vigyük be azt egy bankfiókba, semmint hogy ilyen költséges futáros módszert választanának. A bankok sosem jönnek a lakásunkba, a rendőrség sosem jön házhoz azért, hogy "kicserélje" az állítólag hibás, sérült bankkártyát. Bár ezek a próbálkozások angol nyelvterületen történtek, annyira elképesztőek és nyilvánvalóan csalárd szándékúak, hogy Magyarországon remélhetőleg senki nem dőlne be hasonló trükköknek. Sajnos sok korábbi, szakállas trükk, kilátásba helyezett nyeremény reményében is jócskán szedett áldozatot a magyar felhasználók között is, ezért minden helyzetben érdemes óvatosnak és biztonságtudatosnak lennünk.

Az antivírus blog decemberi fontosabb posztjai között a Regin nevű újabb állami kémprogram felbukkanása apropóján összegyűjtöttünk néhány hasznos tanácsot, amikkel egy hétköznapi felhasználó a lehetőségekhez képes magát és adatai is megóvhatja.

A karácsony közeledtével az internetes webáruházak témáját is érintettük. A statisztikák szerint a "kik vásárolnak leginkább online" kérdésre elsősorban a magasabb keresetű, és egyetemi végzettséggel rendelkező középkorú nők vezetik a statisztikát. Biztonsági szempontból pedig az lehet különösen érdekes, hogy a tavalyi adatok szerint a beérkező rendelések nagyjából ötöde - 18 százaléka - már mobileszközközről származik.

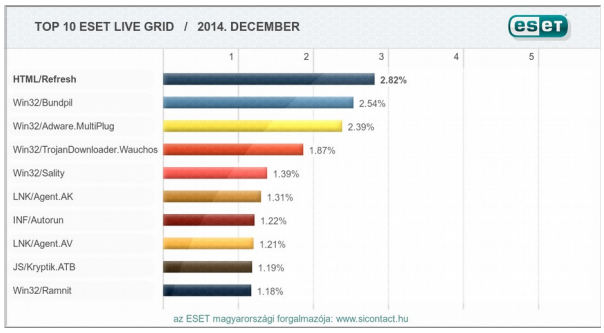
Emellett tanulságos történetről olvashattunk az Android háza tájáról. Három rejtett előfizetéssel trükköző brit céget is megbüntettek, mert a vizsgálat szerint különféle Androidos alkalmazásokba olyan rosszindulatú funkciót rejtettek, amelyek révén az áldozat drága emelt díjas szolgáltatásokra iratkozott fel tudtán kívül.

Szerencsére a privát szféra megóvása lassan mindenki gondolkodásába beépül. Sajnos szinte mindenki tapasztalt már saját példáján vagy ismeretségi körében olyan incidenseket, lopásokat, amelyek esetleg elkerülhetőek lettek volna egy biztonságtudatosabb hozzáállással. Ennek kapcsán ismertettünk pár, könnyen megfogadható tippet, amelyek betartásával segíthetünk személyes adataink, személyazonosságunk hatékonyabb védelmében.

Végül arról is beszámoltunk, hogy az ESET kanadai kutatói alaposan megvizsgálták a tavalyi év elején megjelent TorrentLocker nevű zsarolóprogram működését. A malware legutolsó változata legalább 40,000 rendszert fertőzött meg pár hónap alatt, és leginkább az európai országokban szedte áldozatait. Szomorú újdonság, hogy a korábbi szerencsés helyreállítási kísérletekkel szemben a TorrentLocker áldozatai sajnos már nem tudták visszaállítani a dokumentumaikat az elkódolt fájljaik és az egyszerű szöveges állományának kombinálásával megszerzett kulcsfolyam segítségével.

Vírustoplista

Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2014 decemberében a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 17.12%-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. HTML/Refresh trójai
Elterjedtsége a decemberi fertőzések között: 2.82%
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

02. Win32/Bundpil féreg
Elterjedtsége a decemberi fertőzések között: 2.54%
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

03. Win32/Adware.MultiPlug adware
Elterjedtsége a decemberi fertőzések között: 2.39%
Működés: A Win32/Adware.MultiPlug egy olyan úgynevezett nemkívánatos alkalmazás (Potential Unwanted Program, PUP), amely a felhasználó rendszerébe bekerülve különféle felugró ablakokban kéretlen reklámokat jelenít meg az internetes böngészés közben.
Bővebb információ: http://www.virusradar.com/en/Win32_Adware.MultiPlug.H/description

04. Win32/TrojanDownloader.Wauchos trójai
Elterjedtsége a decemberi fertőzések között: 1.87%
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

05. Win32/Sality vírus
Elterjedtsége a decemberi fertőzések között: 1.39%
Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.
Bővebb információ: http://www.virusradar.com/Win32_Sality.NAR/description

06. LNK/Agent.AK trójai
Elterjedtsége a decemberi fertőzések között: 1.31%
Működés: A LNK/Agent.AK 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.AK/description

07. INF/Autorun vírus
Elterjedtsége a decemberi fertőzések között: 1.22%
Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.
Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

08. LNK/Agent.AV trójai
Elterjedtsége a decemberi fertőzések között: 1.21%
Működés: A LNK/Agent.AV trójai egy olyan kártékony link hivatkozás, amelyik különféle parancsokat fűz össze és futtat le észrevétlenül a háttérben. Működését tekintve hasonlít a régi autorun.inf mechanizmusára.
Bővebb információ: http://www.virusradar.com/en/LNK_Agent.AV/description

09. JS/Kryptik trójai
Elterjedtsége a decemberi fertőzések között: 1.19%
Működés: A JS/Kryptik egy általános összesítő elnevezése azoknak a különféle kártékony és olvashatatlanná összezavart JavaScript kódoknak, amely a különféle HTML oldalakba rejtetten beágyazódva észrevétlenül sebezhetőségeket kihasználó kártékony weboldalakra irányítja át a felhasználó böngészőprogramját.
Bővebb információ: http://www.virusradar.com/en/JS_Kryptik/detail

10. Win32/Ramnit vírus
Elterjedtsége a decemberi fertőzések között: 1.17%
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

**

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.