SAJTÓKÖZLEMÉNY

Budapest, 2015. január 12.

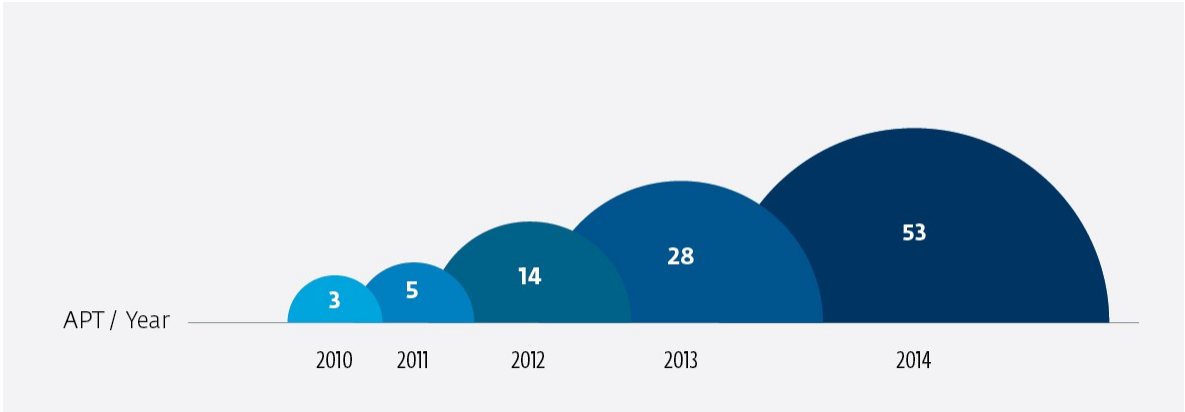
Célzott támadások, vírusos tévék és zsarolóprogramok sokasága jöhet idén

Az ESET kutatói összefoglalták a várható kiberbűnözési trendeket és elemezték a tavalyi év utolsó zsarolóprogramját

A vezető, proaktív védelmet kínáló biztonságtechnológiai vállalat, az ESET kutatói az előző évekhez hasonlóan elkészítették éves, a számítógépek elleni várható támadásokról szóló trendriportjukat. A tavalyi év során a legnagyobb figyelem az internetes adatvédelem mellett, az androidos eszközök elleni támadásokra és a high-tech malware-ek új hullámára esett. Idén sem kerülnek ezek az irányok a süllyesztőbe, de mellettük a célzott támadásokra, a fizetési rendszerekre és a dolgok internetéhez kapcsolódó támadásokra is érdemes lesz hangsúlyt fektetni. A zsarolóprogramok, mint a fogyasztói számítógépes bűnözés jelentős profitot termelő ágazata, már évek óta problémát jelent, ahogy az év végén felfedezett VirLock kártevő is.

Célzott támadások

Az elmúlt években, ha mást nem, egy leckét nagyon megtanulhattunk: azt, hogy a célzott támadások folyamatosan növekvő tendenciát mutatnak és ez alól az idei, 2015-ös év sem lesz kivétel. A közismert nevén Advanced Persistent Threats-ként (APT) ismert támadások a célpont kiválasztásánál, a támadás időtartalmában és a „lappangási" időszak hosszúságában térnek el a hagyományos kibertámadásoktól. Fontos azt is megjegyezni, hogy ezek a támadások célzott Social Engineering támadásokat hasznosítanak. Az APT adattár szerint az ilyen jellegű támadások az elmúlt pár évben megsokszorozódtak, 2010-től 2014-ig összesen 53 ismert támadást azonosítottak, és ezek mellett valószínűleg nagyon sok volt a még felfedezetlen kísérlet is. A területek alapján legfőbb azt láthatjuk, hogy jellemzően a pénzügyi és az üzleti szféra áll leginkább a célkeresztben, de időnként politikai motivációk is tetten érhetőek, vagy legalábbis gyaníthatók. Emellett aggasztó lehet, hogy folyamatosan növekszik az egészségügyi adatok elleni támadások száma is.



Fizetési rendszerek a célpontban

Az online fizetési rendszerek elterjedésével párhuzamosan az ezeket érő számítógépes támadások száma is növekszik. Az interneten keringő évről évre jelentősebb pénzösszegeknek köszönhetően a kiberbűnözők az idén is kiemelt erőfeszítéseket fognak tenni a fizetőrendszerek elleni támadásokba.

Ugyanebbe a sorba tagozódik be az online valuta (bitcoin) ellen elkövetett támadások is. A legújabb ilyen támadások már nem csak a veszélybe került felhasználók online pénzét képesek ellopni a tárcáikból, hanem a botnet hálózatok révén rejtett bányászatot is folytatnak a megfertőzött zombigépek kapacitását kihasználva.

A dolgok internetével is ismerkednek a bűnözők

Ne gondoljuk azt, hogy azok az új eszközök, amelyeket összekötünk az internettel, és amelyek adatait ott tároljuk, előbb vagy utóbb ne kerülnének a kiberbűnözők kereszttüzébe. Az Internet of Things trend biztos melegágya lesz a támadók kíváncsiságának, hiszen már tavaly is több bizonyítékát láttuk ennek az iránynak. Támadásokat intéztek többek között számos okostévé, okostelefonok biometrikus rendszerei, spammeltek a hűtőszekrényből álló botnetek, sőt a Google Glass ellen is volt támadás. Sajnos azt lehet tapasztalni, hogy a gyártók és fejlesztők egyelőre sajnos még kevéssé foglalkoznak itt érdemben a biztonsággal. Pedig mindenképp érdemes lenne, hiszen ezeknek az eszközöknek elterjedésével ez a terület is egyre nagyobb figyelmet fog kapni.

Zsarolóprogramok, a tavalyi VirLock esete

Végül említsük meg a zsarolóprogramokat, amelyek a malware fejlesztők egyik kiemelt fenyegetése, az egyik legfontosabb eszköze lehet a következő években is. Az ilyen ransomware - gondoljunk csak a tavalyi CryptoLockerre - számos felhasználó adatát semmisítette meg, emellett pedig közvetlen anyagi kárt is okozott a védelmi pénzekkel. Sajnos azt látni, a zsarolóprogramok folyamatos továbbfejlesztése egyre nagyobb kihívás elé állítja a vírusvédelmeket és a felhasználókat. Ennek egyik legjobb példája a 2014 végén megjelenő VirLock (Win32/VirLock) névre hallgató zsarolóprogram. Elemzése során az ESET kutatói azzal szembesültek, hogy az új verziós zsarolóprogram már nem csak zárolja az áldozat eszközének képernyőjét, hanem egyúttal az első alakváltó, polimorf vírus, amely emellett megfertőzi a felhasználó fájljait. Jó hír lehet viszont, hogy a VirLock által megfertőzött fájlok visszaállításához az áldozatok letölthetik az ESET önálló mentesítő segédprogramját.

„Technikai szempontból a legérdekesebb része a VirLock vírusnak, hogy polimorf, azaz új testet tud ölteni a fájlok megfertőzéséhez és mindannyiszor megváltoztatja alakját, akkor, ha valaki megnyitja. Sőt az elemzés során az is kiderült, hogy több szintű titkosításra is képes, ami arra utal, hogy a malware szerzője nagyon is ért a kódoláshoz.” – mondta Robert Lipovsky, az ESET malware kutatója.

Emellett az Android platform is további "kiemelt figyelemre" számíthat a vírusírók részéről. A mobilos kártevők száma évről évre folyamatosan és meredeken emelkedik köszönhetően az Android rendszer széleskörű elterjedtségének. A kártevők azonban nem csak számszerűleg, hanem technikailag is folyamatosan fejlődnek. Emlékezetes lehet például, hogy korábban a ransomwarek két nagyobb klasszikus csoportját tudtuk megkülönböztetni: léteztek a képernyőzárolók és külön a fájltitkosítók. Azonban tavaly például már e kettő tulajdonság egy hibridje is felfedezhető volt, ilyen vírus volt például az ESET által tavaly év elején felfedezett Android/Simplocker. Ez a fájlokat már nem csak elkódolta, hanem emellett a képernyőt is zárolta egy a zsarolást tartalmazó üzenettel.

A VirLock vírusról olvasható elemzés itt olvasható:
http://www.welivesecurity.com/2014/12/22/win32virlock-first-self-reproducing-ransomware-also-shape-shifter/

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