SAJTÓKÖZLEMÉNY

Budapest, 2014. november 3.

Hello Halloween: amit a botnetekről tudni kell

A zombik ünnepén érdemes megemlékezni az öt legfélelmetesebb zombi botnetről is, amelynek gyűjtését alább találhatják.

Mi is az a zombi botnet?

Zombi számítógépnek hívjuk azokat a gépeket, amelyeket bizonyos típusú távolról irányítható rosszindulatú programokkal fertőznek meg, így átveszik felettük az irányítást. A zombi hálózatok felépítése és károkozása akár egy poszt apokaliptikus filmes forgatókönyvvel is felér. Néhány ezek közül gyakorlatilag kiirthatatlan - mindig az árnyékban leselkedik egy "élőhalott", hogy egy újabb katasztrófát indítson el. Az ESET összeállította a véleménye szerinti öt legfélelmetesebb zombi hálózat listáját:

Storm – A legrégebbi malware a listán, az egyik legkorábbi botnet, amely olyan technikákat kezdett alkalmazni, amely a későbbi kártevők alapja lett. A gyorsan és nagymértékben terjedő kártevő tíz millió Windows rendszerű gépet fertőzött meg. Ez volt az első olyan nagyobb botnet is, amely anyagi jövedelmet hozott a tulajdonosainak.

Conficker – Fénykorában több millió Windows gépet fertőzött meg: egyes számok szerint több mint 15 milliót. A filmekben is, ha egy, az életünket kockáztató, elsöprő erejű katasztrófa közeleg, akkor egy szakértői csoport kialakítása a legkézenfekvőbb mód a védekezés elkezdésére. Itt sem volt ez másképpen: olyan nagymértékben terjedt a fertőzés, hogy megalakították a Conficker Working Group nevű csoportot, mely aztán felvette a harcot a károkozóval. Hat évvel az első felfedezése óta, még a mai napig léteznek megfertőzött számítógépek szerte a világban.

Zeus – Ez a malware nem egyszerűen csak egy sikeres botnet, hanem egy olyan kártevő is, amely online banki kódokat lopott különféle fertőzött mobil eszközökről (Symbian, Windows Mobile, Android és Blackberry). 2012-ben az US Marshals technikai csapata győzte le a botnetet. A kártevőt létrehozók nem tétlenkedtek: az eredeti botnetből elraktározva egy darabot újraélesztették Gameover Zeus néven, amelyet csak idén nyáron sikerült az FBI és partnereinek hatástalanítania. De még ez sem volt elég ennek a "ragadozónak": még egyszer feltámasztották a zombi hálózatukat. A tavalyi év Cryptolocker nevű vírusát is a Zeus különböző variánsai terjesztették.

Flashback – Azoknak az embereknek, akik abban a hitben éltek, hogy a Macintosh gépeket nem lehet vírussal fertőzni, ez a kártevő kisebb-nagyobb sokkot jelentett. Bebizonyosodott, hogy a Mac gépek is ugyanúgy "kaphatnak" vírust, sőt a megfertőzött gépek hatalmas botnetek részévé is válhatnak. Az Apple gépek nagy része, mintegy 600 000 számítógép fertőződött meg ebben a nagy erejű támadásban világszerte. Ez a botnet most éppen nem aktív, de bármikor azzá válhat.

Windigo – Látszólag ez a botnet is ugyanolyan, mint a többi: fertőzött gépekről lop el adatokat, vagy kéretlen leveleket küld szét a világba. Akár még kedvelhetnénk is ezt a zombit, mivel a többihez képest "csak" néhány tízezer gépet fertőzött meg. Viszont úgy néz ki, hogy a botnet alkotói szépen

lassan építik fel zombi hadseregüket, így egy időre mindig láthatatlanná válhatnak és megbújhatnak. A több tízezer Windigo által megfertőzött Linux alapú számítógép illetve szerver pedig addig is több millió emberhez juttatja el a vírust.

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