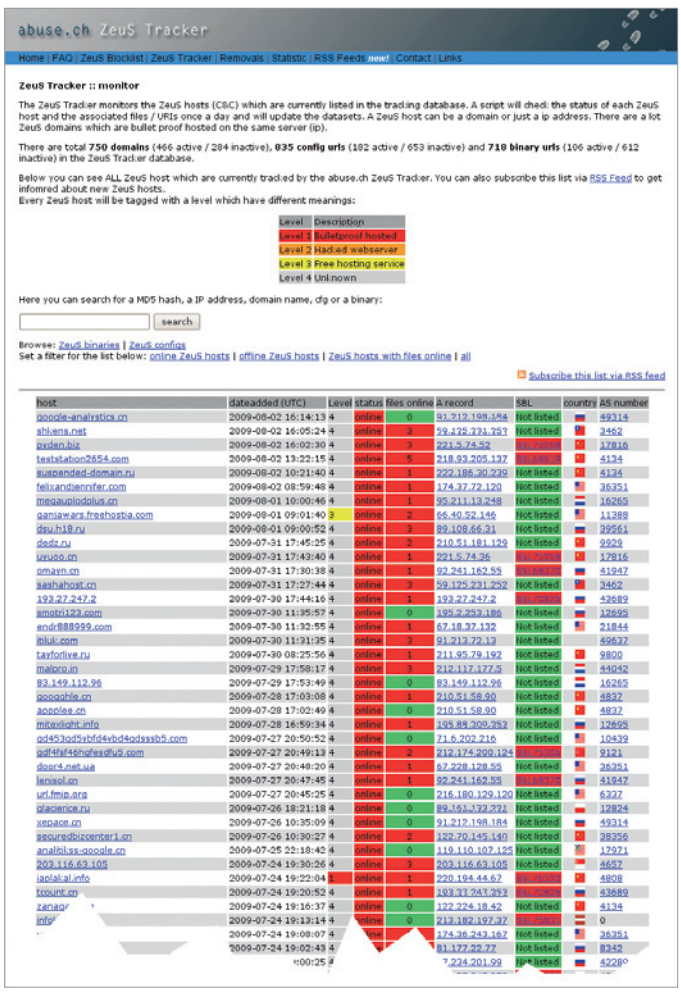
A TÍZMILLIÓ ZOMBI ORSZÁGA

A világ legnagyobb botnetjei

Sorozatunk huszonötödik epizódjában bemutatunk néhány jelentős bothálózatot, és kicsit körbenézünk, mely országok látszanak fő zombicélpontnak, és melyek tudták eddig több-kevesebb sikerrel elkerülni az ilyen tömeges fertőzést.

A botnetes támadásokról már szinte mindent leírtunk májusi *Zombi-e vagy?* című cikkünkben. Bár látszólag mindenki tudja a feladatát, a fertőzés mégis egyre jobban terjed. A havi kártevő-statisztikák is arról árulkodnak, hogy a Conficker féreg és társai számos országban masszívan trónolnak hónapok óta az élvonalban. A fertőzött gépeknek nemcsak a már unalomig ismert parancsok adhatók ki: spamküldés, részvétel DoS-, illetve DdoS-támadásokban, hanem a helyi adatok ellopásán kívül a kártevő frissítését (update), de akár önmegsemmisítést is (a telepített kártevőét, de a Windows rendszer tönkretételét is) vezényelhet a botnetgazda. Ez utóbbit igen ritkán szokták alkalmazni, időnyerés, esetleg nyomeltüntetés céljából tehetik meg. Ha például egy távoli paranccsal kitörlik a fertőzött zombigépek rendszerleíró adatbázisának (Registry) összes HKEY_LOCAL_MACHINE és HKEY_CURRENT_USER bejegyzését, ezzel összeomlasztják ugyan a gépeket, de a távvezérlést is elvesztik a gépek felett.



A svájci *Roman Hüssy* weblapja képes a Zeus trójai működését szolgáló szerverek nyomkövetésére. Sokan az áldozatok közül saját gépükön nem is vesznek észre semmit, pedig lehet, hogy eközben vállalkozásuk szervere éppen botnetet irányít

Begyűjtjük az első tízet

Júliusban tették közzé a NetworkWorld szakértői a tíz legnagyobb amerikai botnet adatait. Az adatokat a Damballa nevű biztonsági cég észleléseire, illetve becsléseire alapozva jelentették meg. Lehet, hogy idővel a kártevők havi toplistájához hasonlóan ebből is egy rendszeres, havi aktuális lista kerekedik majd? Meglátjuk, most pedig kezdjük is a sort!

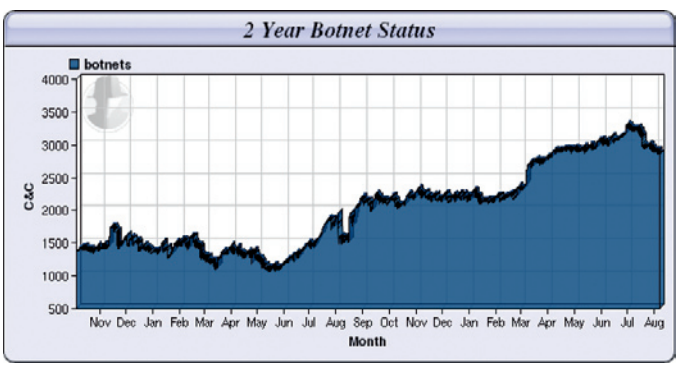
Az első helyen a Zeus nevű botnet áll, jelenleg 3,6 millió tagot számlál. E hálózat fő profilja a billentyűzetleütés-naplózás, amelynek segítségével az érzékeny adatokat, például felhasználói neveket, jelszavakat, számla- és hitelkártya-számokat gyűjt, ehhez banki belépő oldalakba helyez el hamis HTML-űrlapokat.

Második helyezett a Koobface, a maga nem csekély, 2,9 millió megfertőzött amerikai számítógépével. A Koobface sokaknak ismerős lehet, mostanában többször is szóba került a neve, hiszen a kártevő különféle variánsai a MySpace-en, a Facebookon, újabban pedig már a Twitteren is terjednek. A látszólag egy ismerőstől kapott üzenetben egy videofájlt ajánlanak fel megnézésre, ami rákattintás után egy állítólagos hiányzó kodeket kísérel meg letölteni, valójában viszont magát a Koobface kártevőt telepíti a gépre.

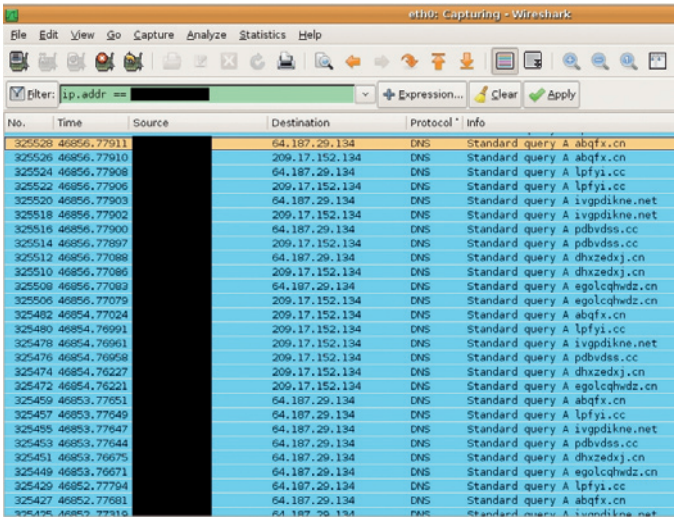
A harmadik helyen a TidServ szerepel másfélmillió zombiszámítógéppel. Főleg e-mailben terjed, lefülelése nem egyszerű, mivel rejtőzködésre rootkittechnikákat is használ. Sokszor érkezik együtt a különféle hamis antivírus programokkal.

A NetWorkWorld listáján negyedik a TrojanAVFakealert nevű hálózat, amely nevéhez híven főleg a hamis antivírus programokkal terjed. Ezek nem létező riasztásokkal próbálják megijeszteni a tapasztalatlan felhasználókat, és nemcsak megzsarolják őket az ígért teljes értékű fizetős változattal, hanem eközben megfertőzik a gépüket és azonnal át is veszik az uralmat felette. A jelentés szerint 1,4 millió számítógép szerepel ebben a hálózatban.

Ötödik helyen találjuk a Trojan/Downloader.Agent botnetet, amelyben a Damballa szakértői 1,2 millió számítógépet sejtenek. Ez egy igazi pénzszerző kártevő,



Ha egy viszonylag hosszabb időszakot, például két évet vizsgálunk, jól látszik a botnetek számának erőteljes emelkedése



A hálózati forgalom TCP/IP-csomagjait vizsgálva a Confickerre jellemző forgalom látszik a Wireshark ablakában

az irányítója titkosított parancsokkal kommunikál, és főleg reklámokra történő kattintási manőverekben használatos visszaélésekre használják.

Hatodik helyen található az úgynevezett Monkif, amellyel az amerikai számítógépek közül 520 ezer fertőződött meg. Ezzel a kártevővel szoktak kéretlen reklámokat megjelenítő, úgynevezett BHO-programokat (Browser Helper Object) feltölteni az áldozatok gépére.

A hetedik helyezett a 480 ezer számítógépet bitorló Hamweq. Az Autorun funkció segítségével igyekszik másolatait minden elérhető meghajtóra eljuttatni. Külön Registry-bejegyzésekkel gondoskodik a kód automatikus lefuttatásáról, amikor az explorer.exe folyamat éppen elindul. A fertőzött gépen a botmester tetszőleges parancsokat futtathat, és bármibe bele tud nézni.

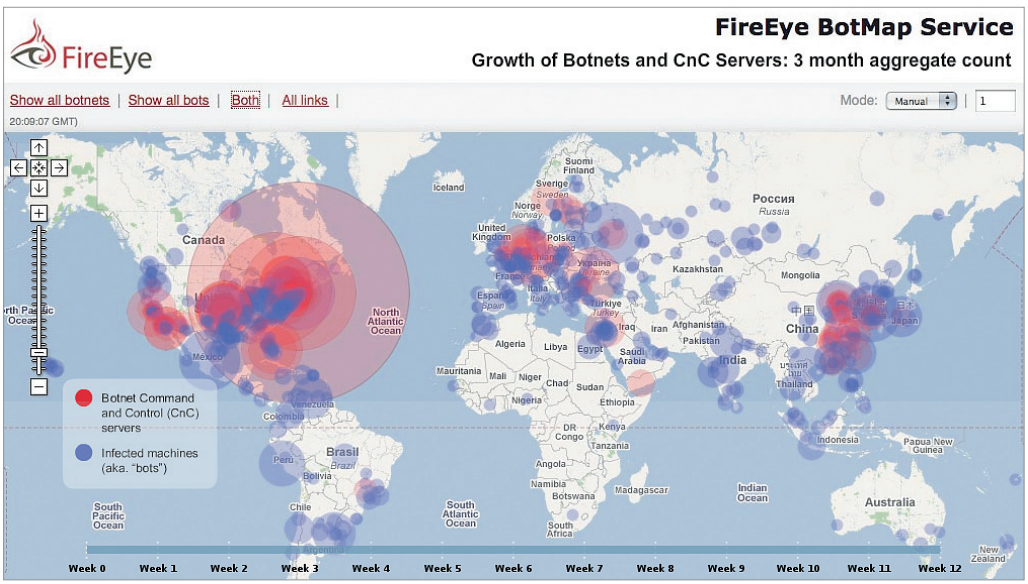
Nyolcadik utasunk a Swizzor, a lista 370 ezer fertőzött gépet tulajdonít neki. Fő célja kéretlen reklámokat és különféle trójai programokat telepíteni a számítógépre. Az ESET havi magyarországi statisztikái szerint a Swizzor itthon is minden hónapban az első tízben volt, februárban pedig első helyezettként szerepelt.

Egy botnet elterjedtségét demonstráló világtérkép. (A Prevx ábrája a saját májusi adataik alapján.) Jól látszik, hogy Kanada mintha ellenszert vett volna be, míg Európa vastagon érintett az USA-val együtt

Kilencedik, de még mindig jelentős méretekkel rendelkezik a Gammina botnet, melllette a 230 ezres számot olvashatjuk. Ez a kártevő az online játékok belépési jelszavaira specializálódott, az ezekhez tartozó belépési nevet, jelszót és számlaadatokat igyekszik megszerezni. Rootkittechnikával megpróbál elrejtőzni a megfertőzött gépen, akár külső USB-eszközökkel is terjed, és talán leghíresebb húzása az volt, amikor 2008 nyarán a Nemzetközi Űrállomás két számítógépét is megfertőzte.

Végül, de nem utolsósorban a Conficker áll a tizedik helyezettként a maga 210 ezer amerikai számítógépével. A Conficker is ismerős lehet a magyar havi listákról, a júniusi és júliusi top 10-et még vezette is. Sokféle fertőzési mechanizmussal dolgozik, ebből csak egy a tavaly októberben már befoltozott biztonsági résen való bekúszása. Emellett a fertőzés a gyenge adminjelszavak elleni támadással, valamint az automatikus futtatási lehetőségén keresztül is terjed. Többek közt a Waledac kártevő terjesztésére is felhasználták a botnet irányítói.

Mit mondhat nekünk ez lista? Talán megfelelően demonstrálja azokat a kerülendő veszélyeket, amelyeken a legtöbb képzetlen vagy gyanútlan felhasználó fennakad. Ijesztő is lehet egy ilyen hatalmas erőforrásra támaszkodó sötét erő. Persze mutathat feladatokat a szakemberek számára is, sőt kell is, hogy mutasson, mert hatékony ellenlépések nélkül ez a helyzet vagy megmarad, vagy még rosszabbodni is fog.



Egy másik világtérkép egy másik cég elemzései alapján. Itt szintén alig van pötty Ausztráliában, miközben tudjuk, hogy minden ötödik ottani gép egy botnet tagja. Emiatt külön felvilágosító programot is hirdettek a gépek megtisztítására

Kicsi a bors, de vannak barátai

A toplista vége felé elhelyezkedő botneteket sokan hajlamosak alábecsülni azzal, hogy „Ugyan kérem, mi ez a pár százezer a millióhoz képest?"

Az ESET kutatói eljátszottak a botnetes Waledac kártevővel, és a forgalom elemzésével méregették a botnet spamkibocsátási képességeit. A Latin-Amerikában végzett tesztelés szerint már egyetlen botfertőzte számítógép is másod-

A Facebook és MySpace közösségi oldalakon terjedő Koobface féreg a futtatása során vicces képet jelenít meg, viszont a hatásai már nem is olyan viccesek. Csak az Egyesült Államokban 2,9 millió számítógép tartozik e hálózatba

percenként két spamlevelet, illetve egy teljes nap alatt pedig mintegy 150 ezer kéretlen reklámlevelet képes kibocsátani. A szándékosan megfertőzött laboratóriumi PC a Bálint-napi kártevővel állt be a botnetek sorába, majd ennek kapcsán nyílt alkalom a hálózati forgalom alaposabb vizsgálatára is. A Waledac számos tekintetben felülmúlja a korábbi Storm képességeit, és annak reinkarnációjának tartják.

Sebastian Bortnik egy blogbejegyzésében a Waledac kártevővel üzemelő botnet méretét 20 ezer gépre becsüli, teljesítőképességét pedig napi 3 milliárd kiküldhető spamre teszi. Természetesen ezek a becsléseken alapuló botnetes elméleti teljesítmények valójában tényleg csak elméletiek, hiszen a botnetet általában sosem használják teljes üzemidőben és teljes kapacitással, bár ennek technikailag semmi akadálya nem lenne.

Az elemzés emellett azt is kimutatta, hogy a Waledac valóban a Storm utódjának tekinthető, és fejlesztésénél figyelembe vették az elődjavítandó hibáit is, például amíg a Storm csak 64 bites RSA-kódolási algoritmust használt, a Waledac már ebben is előrelépett, és minden tekintetben folyamatosan továbbfejlődött az év eleji Bálint-naptól egészen a július 4-i Függetlenség Napja ünnepekig.

Hegyek, völgyek, tájak, országok

Vajon mi lehet a pontos oka annak, hogy vannak országok, amelyek vastagon és hónapok óta érintettek a botnetes problémában, és vannak, amelyek viszonylag sikeresebben ellenállnak? Ha csak a Conficker férget nézzük a havi toplistákban, gyanítható sok országban van kiterjedt bothálózat. Az ESET havi statisztikai adatai szerint ilyen például az USA, Brazília, Indonézia, Irán, Új-Zéland, Pakisztán, Románia, Oroszország, Szerbia, Ukrajna és Zimbabwe.

Az USA-ban sok a pénz, sokan használnak hitelkártyákat, sok az óvatlan felhasználó, és rengeteg ember él ott, valószínűleg ezért érdemes a nagy számok törvénye miatt is próbálkozni a bűnözőknek.

Ezzel szemben vannak azok az országok, ahol pedig még az első húszban sem szerepel a Conficker féreg egyetlen variánsa sem. Az ilyen szerencsésebb helyek közt találjuk Bahreint, Dániát, Máltát, Kanadát, Hollandiát, Norvégiát és Svédországot. Utóbbiak viszonylag a valóságban is gazdag országok. Mi lehet itt a magas biztonsági faktor oka? Alacsony lehet a lopott Windows operációs rendszer aránya, és talán mindenkinek van legális antivírus program telepítve a gépén, esetleg képzettebbek a felhasználóik és talán mindenki tudja, hogyan védekezzen?

A felhasználók helyzetét nehezíti, hogy sok esetben a számítógép forgalmazója spórolásból nem ad valódi telepítőlemezt a megvásárolt géphez, hanem a vásárlóra bízza, hogy az előtelepített Windowsból maga készítsen lemezt. Ám ez a lustaság és a hozzá nem értés miatt sokszor elmarad, így rendszerösszeomlás vagy zombifertőzés esetén nincs mihez nyúlni

Eljön-e John Connor?

Ha ilyen ütemben fejlődik a számítástechnika, mindenki otthonról bankol majd, és a gazdagabb országokban növekedik a számítógép vezérelte intelligens otthonok száma, akkor egyre jobban a Terminátor filmek Skynetjére fog hasonlítani az a totális ellenőrzés, amellyel a számítógépes bűnözők gépek millióit tarthatják majd kontroll alatt. A probléma orvoslására azonban új módszereket kell bevetni, mert a figyelmeztetések, újságcikkek önmagukban jól láthatóan nem képesek a jelenség felszámolására. Míg egy defektes kereket a sofőrök azonnal észlelnek, és kicserélik, addig a gépén élősködő zombit sokszor nem is érzékeli a tulajdonosa, vagy érdektelenségből nem javítja, és ezzel rászabadítja a botnetet a többiekre. És ez az, amit megengedhetetlen.

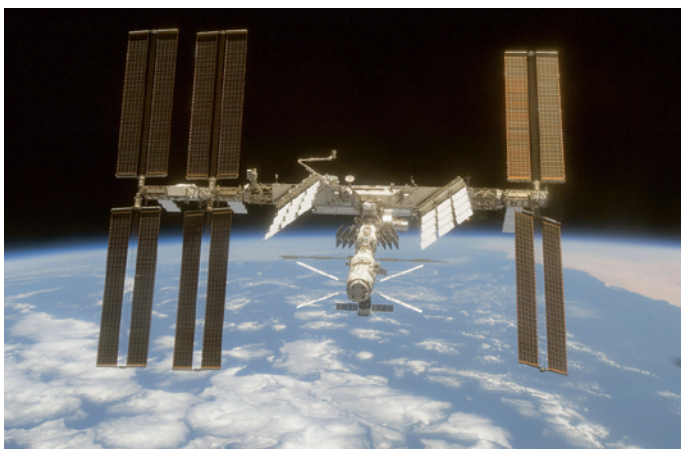
A helyzet felemás. Egyes vélemények szerint az internetszolgáltatóknak kellene aktívabban segíteni a botnetes fertőzéseknél, de ezt csak a forgalom ellenőrzésével, szűrésével tehetnék. Közben pedig, ha mondjuk P2P-forgalomra szűrnek, akkor meg utáljuk őket, és azt gondoljuk, nincs is joguk a forgalom figyelésére.

Mindenesetre, ha valakinek nagyon lelassult a gépe, és tudtán kívül egy zombihadsereg katonája, a fenti adatokból megértheti, hogy hová is tűnik az elhappolt sebesség és teljesítmény. Az amerikai kormánynak a Sandia National Laboratories kutatói eközben olyan rendszert fejlesztenek, amellyel szimulálható lesz az internetes jelenségek működése. A MegaTuxnak keresztelt projektben egy Dell szuperszámítógépet készítenek fel egymillió operációs rendszer virtualizált futtatására, és ez a botnetes kártevők vizsgálatában vadonatúj és igen hatékony szimulációs terep lehet.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**).

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu



Két noteszgép is megfertőződött 2008 augusztusában a Nemzetközi Űrállomáson. A BBC akkori értesülései szerint az asztronauták a laptopjaikon semmilyen antivírus programot nem használtak