HOGYAN NE LEGYÜNK EGY BOTNET RÉSZE

Zombi-e vagy?

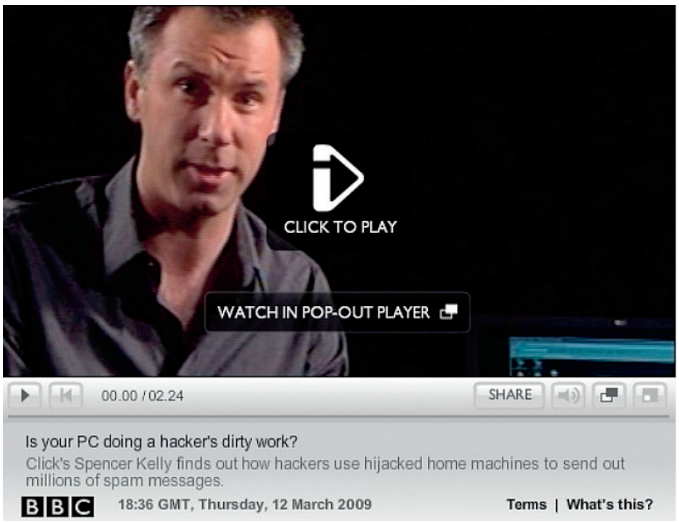
Kíváncsisággal vegyes borzongás fogja el a zombigép szó hallatán? Rettegve olvassa a botnet pásztorok aljas mesterkedéseiről szóló híreket? Most mindent elmondunk erről a témáról – hogyan fedezhetjük fel, ha netán bennünket is érint, továbbá jótanácsokkal is szolgálunk.

Maga a botnet kifejezés a robot network szavakból származik, és olyan hálózati gépek csoportját jelöli, amelyek automatikus működéssel előre meghatározott feladatot hajtanak végre, illetve a vezérlő gépről további utasításokat képesek fogadni. Bár elvileg ezt lehetne hasznos dolgokra is használni, ebben az esetben azonban sajnos nem erről van szó: a fertőzött gépek tünetmentesen és csendesen várják a távoli, különféle támadásokhoz használt utasításokat.

Táncóra idősebbeknek és haladóknak

Pillantsunk kicsit vissza az időben. A kártékony és/vagy kéretlen tartalmak elektronikus levél formájában való küldözgetését korábban is igyekeztek anonim módon végezni, ezért ezt nyitott proxyk segítségével vagy publikus levelezőszerverekről végezték. Ennek aztán az lett a hatása, hogy ezeket a szervereket szép lassan kitiltották a szűrésnél, így rendszeresen újakat kellett találni. Persze ehhez az is hozzátartozik, hogy ahol egy rendszergazda engedélyezte a nem saját domainből való levelek továbbítását is (open relay), az már eleve gondatlanul járt el. Mivel az is rendszeresen előfordult, hogy emiatt egy-egy cég levelezését teljesen letiltották a szolgáltatók, ennélfogva a visszakapcsolás után egy-egy ilyen szerveren gondosan befoltozták az ilyen réseket (hiányzó telepítés, precíz beállítások stb.), és ennek révén így ott már nem lehetett többé visszaélni a lehetőségekkel. A zseniális gondolat azonban megszületett a továbblépéshez – egy kicsit a trójai kémprogramok világát is idézve az olyan nagy elődök, mint például a Back Orifice, ihlették a megoldást: legyenek olyan fertőzött gépek, amelyre fel lehet telepíteni egy hátsó ajtót (backdoor), és később már egyszerűen be lehessen jutni rájuk. Ez a támadónak hasznos, hiszen észrevétlenül kutakodhat, bepillantást nyer az ott intézett ügyletekbe, illetve a tárolt anyagokba, és nem utolsósorban folyamatosan ellenőrizheti a teljes adatforgalmat és használhatja is a megtámadott gép erőforrásait. Amikor aztán jó pár éve már a távirányítást is kényelmes grafikus panelről intézhettük, eladható termék lett az ilyen szoftverekből, amit jó pénzért megvásárolhattak a bűnözők.

A jelenlegi botnetek tömeges elterjedésének pontos oka a nem frissített (vagyis kihasználható biztonsági réseket tartalmazó) Windows operációs rendszert futtató kompromittált számítógépek tömege. Sajnos a mai botnetes kártevők nemcsak megfertőzni tudják a gépeket, de féreg formájában terjesztik is magukat. A helyzet kialakulásához ugyanúgy hozzájárult az otthoni, olcsó szélessávú internet elterjedése, mint ahogyan kulcsszerepe volt a bevezetett spamellenes törvényeknek is, amire pontosan az ilyen anonimitást biztosító botnetekkel válaszoltak a cyberbűnözők.

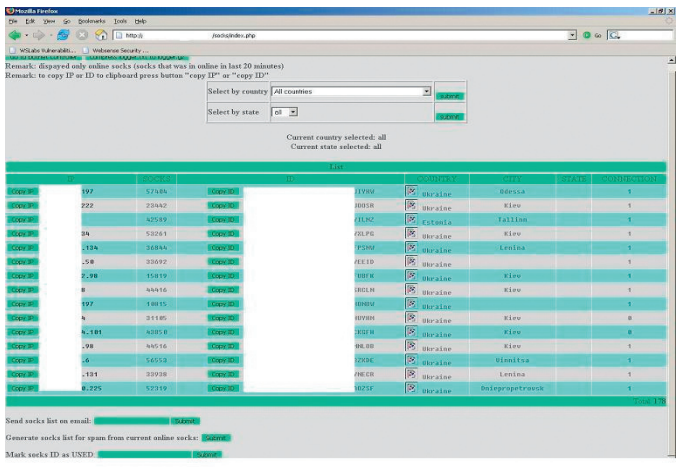


Felkavarta az indulatokat a BBC Click! című számítógépes műsora, amely azt mutatta be, mi történik akkor, ha valaki bérbe vesz egy 20 ezer gépből álló botnetet a bűnözőktől. A szerkesztők „megspammelték" saját postafiókjaikat, és mindössze néhány tucat géppel sikeresen térdre kényszerítettek egy webkiszolgálót

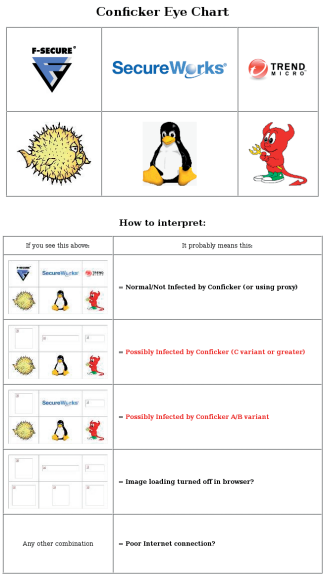
Kinövi magát az üzleti modell

Akik régebb óta figyelemmel kísérik az eseményeket, emlékezhetnek a Storm féreg esetére (er-

Mintha csak torrentezés közben a világ minden táján lévő adatcsomag-forrásokat nézegetnénk. Azonban senkit ne tévesszen meg a látvány, ez itt egy botnet vezérlő adminisztrációs felülete. Van itt japán, brazil, kínai és még ki tudja, hány országbeli zombigép



Így néz ki egy botnet webes irányítófelülete Firefox alatt. Kevés részletes nyilvános információ van erről, emiatt ilyen gyenge minőségű ez az ábra is. A lényeg azért látszik: IP-címek, országok, információ a csatlakozási állapotról, sőt különféle szűrési lehetőségek is a botmester rendelkezésére állnak



A Conficker Work Group munkacsoport weboldalán található ellenőrző link, amellyel megnézhetjük, fertőzött-e a gépünk. A vizsgálat a blokkolt tartalmak alapján hozza meg a döntést

ről részletesen sorozatunk *6. epizódjában* írtunk), vagy a később felbukkant Krakenre, amely rengeteg variánssal és titkosított kóddal rendelkezett. Híres-hírhedt még a Rustock és a szintén tömeges spamterjesztéséről ismert Srizbi is. Ma már a botneteket jobbára nem értékesítik, hanem bérbe adják. Sőt, nem is egyben az egészet, inkább csak darabokban. Miért jó ez? Nagyjából azért, hogy a leleplezés, lenyomozás esélye a minimális lehessen. A spamterjesztő egyszerűen kifizeti az összeget a vírus írójának vagy egy közvetítő üzletkötőnek, és már „dolgozhat" is. A rengeteg számítógép hatalmas teljesítményt és rendkívüli sávszélességet kínál. Emellett a botnet tagjai a dinamikus IP-címek miatt nehézkesen azonosíthatóak, ezért ez a szisztéma szinte teljes anonimitást biztosít a bűnözőknek.

Bemutató élő adásban

Márciusban a BBC Click műsorában egy különleges adást láthattunk. Ebben az újságírók részletesen bemutatták, hogy működik ez az egész. Az üzletet egy illegális chatszobában, orosz és angol nyelv keverékét használva lehetett nyélbe ütni, közvetítők segítségével. Ez biztosította, hogy mind az eladó, mind a vevő inkognitóban maradhasson. Kibéreltek egy 20 ezer gépből álló botnetet, és bemutatták, mire képes. A saját e-mail címeiket megbombázták spamekkel, és alig 60 gép segítségével eredményes DdoS-támadást intéztek a saját webszerverük ellen.

Bár az adás után sok támadás érte a műsor készítőit – erkölcsileg és jogilag is aggályos a bűnözőket támogató ilyen fajta tevékenység –, de kétségkívül szemléletesen és hatásosan juttatták el figyelmeztetésüket a nézőkhöz.

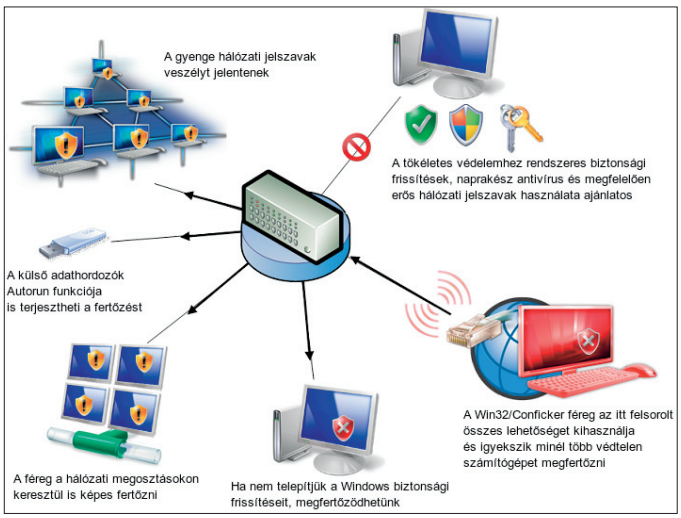
Miről vehetjük észre?

Egy felhasználó gépe anélkül lehet egy ilyen botnetes infrastruktúra része, hogy gazdája kérte vagy engedélyezte volna azt, illetve többnyire nincs is tudomása róla. Tegyük fel, olvassa most ezt a cikket, és szeretné kideríteni magáról, érintett-e. Szerencsére itt jobb a helyzet, mint a hipochonderek esetében, akik orvosi könyvet olvasva szinte mindent tünetet képesek felfedezni magukon. Gyanakodhatunk, ha abba a csoportba tartozunk, amely se nem frissít, se nem használ biztonsági szoftvereket. (Ha ezek hiányoznak, azonnal pótolni kell a mulasztást, majd a vírusirtó futtatásával győződhetünk meg gépünk pontos állapotáról.) Ezek megléte esetén pedig azt érdemes vizsgálni, illetve megfigyelni, nem lassult-e le túlságosan az internetkapcsolat sebessége.

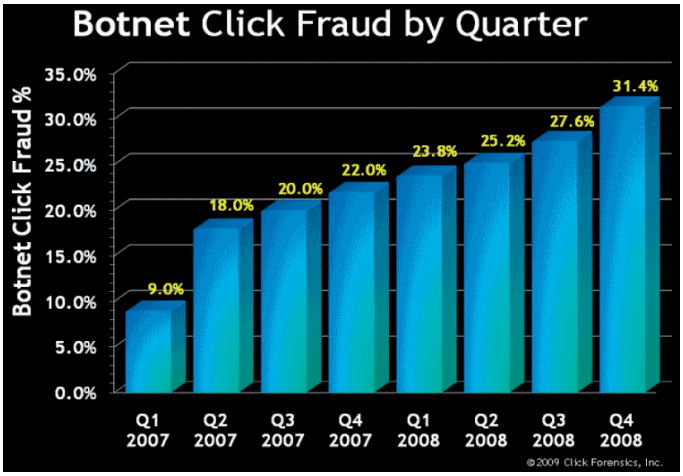
Ennek persze számos más oka is lehet, de ezek között szerepel az is, ha egy botnet már egyéb rejtett feladatokkal emészti fel a sávszélességünk tetemes részét. Ugyancsak egyszerűen kivitelezhető módszer, ha a Feladatkezelőt (Task Manager) meghívjuk, és amikor éppen semmilyen feladatot vagy letöltést nem végez a gépünk, ellenőrizzük a hálózati forgalmat. Ha az általunk vélt csendes időszakban is masszív adatforgalmat tapasztalunk, ez is intő jel lehet arra nézve, nem mi irányítjuk saját számítógépünket.

A sokmillió conficker fertőzés miatt azt is érdemes lehet ellenőrizni, hogy a mi gépünkön dolgozik-e valamilyen féregváltozat. Ehhez az egyik legegyszerűbb teszt a Conficker Working Group weboldalán (**conficker workinggroup.org**) található tesztoldalt lefuttatni, amely azon alapul, hogy a kártevő blokkolja a vírusvédelmi cégek weblapjait. Ha nem jelenik meg minden ábra maradéktalanul, akkor érdemes lehet fertőzésre gyanakodni.

Baj esetén használhatjuk az olyan egyedi mentesítő segédprogramokat, mint például az ingyenes ESET Conficker Removert (**www.eset.hu/viruslabor/ingyeneseltavolitok**). Vigyázzunk, csak megbízható gyártó weboldaláról letöltött alkalmazásban bízzunk, mert e témában is elindultak a kéretlen levelek, amelyekben ingyenes Conficker-mentesítőt hirdetnek, azonban ehelyett a kétes letöltési link további kártevőket szabadít a számítógépünkre.



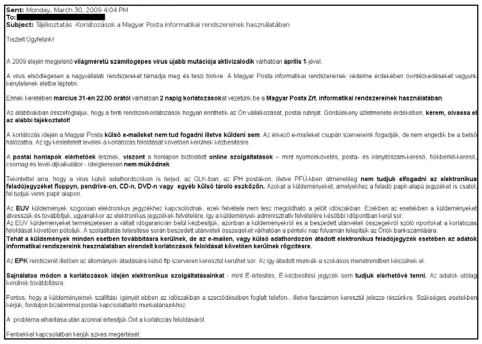
A Microsoft ábrája a Conficker féreg működéséről. A külső eszközök csatlakoztatásakor automatikusan elinduló Autorun folyamatok komoly biztonsági kockázatot jelentenek



A botnetek segítségével elkövetett kattintási csalások száma évről évre emelkedik. A reklámokkal kapcsolatos visszaélés lényege, hogy ilyenkor nem élő hús-vér internetezők látogatják az oldalt, hanem csak automatikus szkriptek növelik a kattintások számát, vagyis a csalás miatt bár a látogatások száma magas, a hirdetők reklámjait a kutya sem nézi meg

A Microsoft is felvette a kesztyűt

A Microsoft hivatalos rosszindulatú szoftvert eltávolító programjával (MSRT) is sok esetben védekezhetünk, és mivel a biztonsági rések miatt a cég renoméja is csorbul, nem kevesebb, mint 250 ezer dollárt ajánlottak fel vérdíjként a Conficker féreg készítőinek kézre kerítéséért idén februárban. Ez pestiesen szólva, de értékét tekintve az egész világon is már „van az a pénz"-kategória, ami miatt talán egyszer lesz érdemi információ. Igaz, a bejelentőnek nemcsak azzal kell majd törődnie, mihez kezd a majdnem 54 millió forintnak megfelelő összeg-



A Magyar Posta nem bízta a véletlenre. A közlemény arról tájékoztatja az ügyfeleket, hogy az április 1-jére jósolt Conficker-támadás miatt két teljes napra drasztikus korlátozást rendeltek el, ez idő alatt még e-maileket sem fogadtak

gel, hanem azzal is számot kell vetnie, hogy egy ilyen maffiaszerű cselekményben résztvevő és hihetetlen profi tudású elkövetőkre tett terhelő vallomásával képes lesz-e titokban maradni élete hátralévő részében, ergo tudja-e majd bosszúmentesen élvezni is ezt a díjat.

Egységfrontba tömörült biztonsági cégek

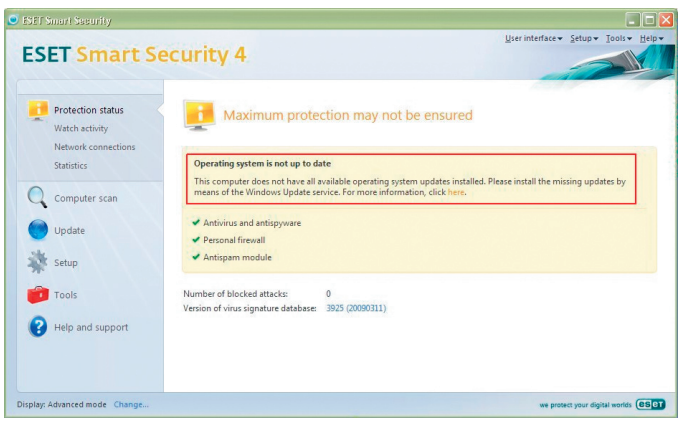
Több külön szervezet is alakult a helyzet súlyosságára való tekintettel. Az egyikben például olyan neves cégek sorakoztak fel a már említett Conficker Working Group zászlaja alatt, mint például az F-Secure, Cisco, ICANN, ESET, Kaspersky, McAfee, Microsoft és még sokan mások. Céljuk, hogy küzdjenek a botnetek ellen.

Amikor a felhasználók felől nézzük, az a jó módszer, hogy mindenki frissítse a gépét, használjon tűzfalat, valamint antivírus szoftvert és kémprogram-irtót. Megóvta magát ezzel? Igen. Megszűntek ettől a világban a támadások? Nem. Nos, pontosan emiatt gyűltek össze a szakemberek, hogy a hálózati forgalom elemzésével, víruscsapdának használt számítógépek (honeypotok) adataival, a kártevő példányainak visszafejtésével szerzett részletesebb információkkal maguk a vezérlő szerverek és a kártékony kódok készítői, használói ellen tudjanak hatékonyan fellépni, illetve a jelenséget megszüntetni.

Elmaradt a világvége április elsején

A legújabb Conficker-variáns, az úgynevezett Conficker.X visszafejtése során a kutatók azt látták a forráskódban, hogy 2009. április elsejére várható egy nagyobb volumenű támadás. Ehhez a botnetgazdák egy 50 ezres domainállományból választanak ki 500 véletlenszerű szervert, amelyek segítségével igyekeznek a fertőzött gépeket vezérelni, további kártékony kódok letöltésére és támadásokban való részvételre rávenni.

Az április elsejei látványos akció elmaradt ugyan, de a veszély egészen biztosan nem hárult el. Lehet, hogy kivárnak, amíg a kiemelt figyelem lankad, lehet, hogy éppen a médiavisszhangot kezdik majd felhasználni hamis Conficker-irtó szoftverek tömeges terjesztésére, egyelőre csak találgathatunk. Mindenesetre a visszajelzések egyértelműen arról tanúskodnak, hogy a készítők igazi profik, és vélhetően sok borsot fognak még az orrunk alá törni.



Az ESET Smart Security külön üzenettel figyelmeztet, hogy nem töltöttük le és telepítettük az összes Microsoft Windows biztonsági javítást

Ahol tesznek is ellene

Ausztráliában már minden hatodik számítógép egy botnethálózat tagja. Emiatt indítottak Zombi Tudatossági Hét néven kampányt a Sophos közreműködésével, amelynek legfőbb célja, hogy felhívja a figyelmet erre a káros jelenségre, erősítse a felhasználók biztonságtudatosságát és segítséget nyújtson a fertőzött gépek megtisztításában.

Becslések szerint csak a Conficker féreg által rutinszerűen megfertőzött, és ezáltal botnet tagjává tett számítógépek száma világszerte meghaladja a 10 milliót. Egy ilyen megfertőzött számítógép aktívan részt vesz a spamküldésekben, webhelyek elleni DdoS-támadásokban anélkül, hogy a tulajdonos szélessávú internetkapcsolatában bármilyen jelet, vagy érdemi lassulást észlelne.

A tapasztalatok szerint nemcsak a kisebb vállalatok, vállalkozások számítógépei, hanem a gyors és állandó internetkapcsolatok miatt kifejezetten a magánemberek vannak egyre nagyobb veszélyben. Kellő szakmai ismeretek hiányában, illetve szakértő ismerős, barát, alkalmazott, rendszergazda, családtag hiányában könnyű bekerülni a szórásba.

Egy OECD-tanulmány szerint a fertőzött botnetes gépek száma évről évre meredeken emelkedik, emellett a fertőzött weboldalak száma is egyre növekszik. A rosszindulatú webhelyek többsége továbbra is kínai, illetve amerikai szervereken hostolt oldal. Az eseményszervezők reményei szerint most igyekeznek minél többeket támogatni abban, hogy kikerüljenek a botnetekből, illetve felvilágosítással és gyakorlati ismeretekkel segítenek a megelőző védekezésben.

Mindenki tegye a kötelességét!

Amíg a Windows-felhasználók nincsenek tudatában a veszélynek, nem igazán fog változni semmi. Még a pesszimista becslés szerint is legalább 5000 új kártevőt írnak naponta erre az operációs rendszerre, és ez az iram még a legfejlettebb heurisztikát is alaposan megdolgoztatja. A legcélravezetőbbnek az tűnik, hogy maguk a felhasználók legyenek képzettebbek, biztonságtudatosabbak és kevésbé lusták. Magyarul a legrövidebb időn belül rendszeresen frissítsék az operációs rendszert a megjelent biztonsági javításokkal – például telepítsék a Conficker miatt is érintett MS08-067-es biztonsági frissítést –, illetve használjanak naprakész antivírus szoftvert és kémprogramok elleni védelmet, valamint kétirányú szűrésre beállított tűzfalat. Legyenek tudatában, mivel jár egy webes linkre való kattintás, és az milyen automatikusan lefutó/települő kártevőket hozhat a rendszerbe.

Ezzel ugyan még nem élveznek 100%-os védelmet, de már mindent megtettek, ami rajtuk múlott, és így minimalizálták a támadás esélyét. Ha ezt mostanra már mindenki megtette volna, ez a cikk és maguk a botnetek sem születtek volna meg jelenlegi ma ismert formájukban.

***

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

KAPCSOLÓDÓ WEBOLDALAK

A ESET magyar nyelvű víruslexikona: **www.eset.hu/virus**
A Bonni Egyetem webes Conficker-tesztje: **hopp.pcworld.hu/5676**
A Conficker Working Group webes Conficker-tesztje: **hopp.pcworld.hu/5844**
ESET Conficker Remover letöltés: **www.eset.hu/viruslabor/ingyeneseltavolitok**