A STORM FÉREG RÖVID ELŐÉLETE

Viharos események

Sorozatunk hatodik epizódjában ma az időjárás és a kártevők közti összefüggésekről esik szó a StormWorm, azaz a Viharféreg kapcsán. Az, hogy nem mindennapi ellenféllel van dolgunk, hamarosan kiderül a részletekből. A Storm, Small.DAM vagy Nuwar néven is ismert féreg minden idők talán leghatékonyabb kártevője.

Múlt időről sajnos szó sincs – a „kis aranyos" még mindig köztünk van, sőt hétről hétre hatékonyabb. Védekezni ellene csak megfontolt döntésekkel lehet. Ehhez viszont nem árt, ha megismerjük korábbi módszereit!

2007. január 17. „Sűrű sötét az éj, dühöng a déli szél..." (Arany János)

... Illetve viharok dúlnak, és ez remek alkalom egyes vírusírók számára, hogy újabb gyanútlan áldozatokra szabadíthassák rá kártevőiket. Több felvonásban érkezik a Viharféreg (**hopp.pcworld.hu/4223**), de a séma az unalomig ismert: az átlagfelhasználó kíváncsiságára apellál. Ilyen tárgysorú leveleket kaphattunk a Viharvírus, azaz StormWorm első felbukkanásakor:

- 230 halottja van az Európában dúló viharoknak
- Russian missile shot down Chinese satellite
- Russian missile shot down USA aircraft
- Sadam Hussein alive!
- Fidel Castro dead
- Hugo Chavez dead

A leleményes kártevőterjesztők minden alkalmat megragadnak, hogy a bekövetkezett tragédiákat, elemi csapásokat, valós vagy kitalált világpolitikai érdekességeket, szenzációkat, ünnepi évfordulókat stb. (**hopp.pcworld.hu/4224**) felhasználva minél több sebezhető számítógépet szerezzenek meg botnethadseregükhöz.

2007. január 21. A Viharféreg már rootkit technikát alkalmaz

Még korántsincs vége a Viharféreggel kapcsolatos történetnek – a kártevőt szorgosan fejlesztik tovább. Ismét egy komoly támadási hullám zajlott le (hopp.pcworld.hu/4224), és olyan új variánsok bukkantak fel, amelyek kernel módú rootkitek segítségével (hopp.pcworld.hu/4225) rejtik el futó folyamataikat, Registry-bejegyzéseiket, valamint aktív hálózati kapcsolatukat. A rootkit olyan eszköz (vagy eszközök gyűjteménye), amelynek segítségével titokban lehet vezérelni egy számítógépet. A rootkit kifejezést Windows-alapú rendszereken általában az olyan programok meghatározására szokták használni, amelyek futó folyamatokat, állományokat vagy rendszerleíró adatbázisbeli (Registry) kulcsokat rejtenek el az operációs rendszer, illetve a felhasználó elől. Az ilyen Windowsra telepített rootkit olyan funkciókat használ, amelyekkel ily módon nemcsak saját magát képes elrejteni, hanem további kártékony kódokat – például billentyűleütés-naplózót (keylogger), vírust, kémprogramot – is észrevehetetlenné tud tenni. A rootkitek nem szükségképpen csak rosszindulatú kódok elkészítéséhez használhatók, de az utóbbi időben mind gyakrabban vetették be ezt a rejtőzködő technikát a rossz oldalon. Ezzel a módszerrel a StormWorm szinte teljesen észrevétlenül tud tevékenykedni a fertőzött rendszereken, például nem jelenik meg a Feladatkezelőben, és futását, ténykedését is igyekszik leplezni.

Viharok, árvizek jönnek, különféle katasztrófák ütnek be, de a jelek szerint nem csak a helyszínen tartózkodók válnak áldozattá: a kíváncsi kattintgatók számítógépe is könnyen egyfajta csatatérré változhat

2007. február 28. Támadás blogokon és fórumokon keresztül

A blogvírus tulajdonképpen a Viharféreg egy specializálódott változata. Az eredeti StormWorm e-mailekhez csatolt fájlokban terjedt, ezek megnyitása után olyan rosszindulatú szoftvert telepítve a gépre, amely további támadások kivitelezését teszi lehetővé. Az új variáns is hasonló, ám tartalmaz egy új elemet: amikor a fertőzött gép tulajdonosa blogbejegyzést ír, vagy online üzenőfalon hagy üzenetet, minden egyes bejegyzésébe bekerül egy fertőzött weboldalra mutató link is.

A blog az utóbbi idők slágerműfaja, az online naplók száma hihetetlen ütemben nő, így az ilyen veszélyek jelentősége is emelkedhet a jövőben.

2007. augusztus. Online Armageddon készül?

A McAfee kutatói jelentésükben egy olyan vészforgatókönyvet tártak a nyilvánosság elé, amelyben a becslések szerint mintegy 1,7 millió gép felett sikerül uralmat szereznie a zombigépekből álló StormWorm hálózatnak. Feltételezésük szerint ezt a lenyűgöző erőt nagy valószínűséggel célzottan, kiemelt célpontok ellen fogják felhasználni: nagy szolgáltatók, illetve kormányzati szervek ellen irányuló elosztott szolgáltatásmegtagadási támadásra (Distributed Denial of Service – DDoS), mint azt korábban már kipróbálták, igaz, kisebb léptékben (hopp.pcworld.hu/4226). Ez a korábbi becsléseknél jóval kiterjedtebb méretű hálózat, és emiatt

A StormWorm (más néven Nuwar) kezdeti terjedése a nagyvilágban – illusztráció az F-Secure weboldaláról

Íme egy zseniális ötlet a captcha védelem törésére: a feltörendő eredeti oldal kódellenőrző részletét beágyazzák egy szexoldalba, és mindig lesz néhány balek, aki önként és dalolva begépeli a hozzá tartozó szöveget

A YouTube-üzenetek szerint ilyet lehet nyerni. Szerintünk meg egy trójait a gépre

pusztító ereje is nagyobb lehet, illetve lesz.

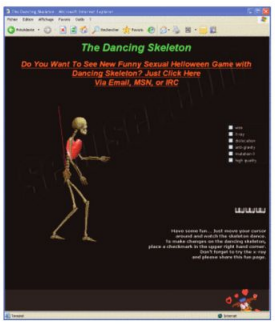
Ezzel ellentétes álláspontra helyezkedett az F-Secure. Ahogy Mikko Hyppönen kutatási igazgató fogalmazott: szerinte a fertőzött PC-k száma mindössze néhány tízezer lehet csak, és ezzel nem lehet jelentősebb károkat okozni.

A hónap vége felé aztán újabb fejlemény történt: a Sunbelt munkatársai webnaplókban, például a Google Blogger oldalain is észleltek több száz olyan, napi bejegyzésnek látszó, félrevezető üzenetet, amelyek különböző trükkökkel, például ingyenes szoftverletöltéssel kecsegtetve egy látszólag ártalmatlan URL-hivatkozásra irányították az olvasót, amely azonban egy trójai programot próbált az áldozatok gépeire letölteni.

Az, hogy a bűnözők egyre több helyen próbálják terjeszteni fertőző trójai programjukat, nem meglepő, hiszen minél több gépet sikerül uralmuk alá hajtani, annál nagyobb profitot tudnak termelni a hálózat fenntartójának, a „botnet-pásztornak", aki legtöbbször bérbe adja ezt az erőforrást spamlevelek terjesztéséhez, illetve DoS- vagy DDoS-támadásokhoz.

2007. szeptember. Támadás az NFL nevében

E-mailben érkeznek az üzenetek, bennük egy hamis National Football League (NFL, az amerikai futballszövetség, NFL) oldalra mutató linkkel. A megtévesztő weboldal egyáltalán nem tartalmaz semmilyen kártékony kódot. Ha azonban valaki rákattint bármelyik linkre vagy a képre, mindegyik a tracker.exe nevű trójai állományt tölti le egy másik szerverről.



Csontvázak minden mennyiségben: kelendő a jópofaság

2007. október. Színhely: a YouTube

Ide is befészkelte magát a StormWorm: az „Invite your friends" szolgáltatást felhasználva a spammerek leveleket próbáltak küldözgetni „Nyerj egy Halo3-at" szövegű levélben (ez egy Xbox játék), ám a mellékelt link ismét egy trójai programra mutatott. A jelentések szerint legalább 150 ezer ilyen levél ment ki hamis e-mail címekről, amelyeket a Gmail- és Hotmail-szolgáltatóknál, a képes kódbeíró (captcha) ellenőrzés kikerülésével regisztráltak. Szerencse a szerencsétlenségben, hogy ha friss adatbázissal rendelkező vírusirtót használtunk, akkor nem sikerült így megfertőzni a számítógépünket.

2007. november. Halloween e-mail és táncoló csontváz

A biztonsági cégek figyelmeztetnek, hogy a „Happy Halloween" és „Dancing Bones" címmel érkező levelek linkjei a híres-hírhedt StormWorm trójaira mutatnak, ezért semmiképpen ne kattintsunk rájuk. A levelekben egy link található, ám az ígért telepítőfájl helyett egy trójai program töltődik le gépünkre.

Újabb átverés: nehéz egy sportrajongótól elvárni, hogy ne kattintson kedvenc oldalán – legalábbis amit annak hisz

Szaporodnak a kártevők letöltésére szakosodott weboldalak

2007. december. Ünnepi nagyüzem

2007 végén a Storm elsősorban az ünnepekkel kapcsolatos üzenetek révén igyekezett terjedni, például a happycards2008.com vagy newyearcards2008.com nevű trójai állományok formájában. Ezek mellett a Mrs. Clause, egy Mikulás-ruhás, vetkőző hölgyeket bemutató ingyenes képernyővédő – amely valójában egy trójait tartalmazó letöltés – is sokakat megtéveszthetett. Az volt az igazán meghökkentő ebben az esetben, amit az F-Secure weblogjában olvashattunk: a vizsgált merrychristmasdude.com fertőzött oldal minden másodpercben másik IP-címhez tartozó szerverről töltődött be, ily módon nehezítve a védekezést, illetve a nyomozást.

Az évnek még mindig nincs vége: órákkal a Benazir Bhutto, korábbi pakisztáni miniszterelnök elleni merénylet után már akcióba lendültek a kártevőkészítők. Megjelentek az olyan linkek a különböző blogoldalakon, amelyek a gyilkosságról készült videót ígérték, ámde – minő meglepetés! –, az egy Active-X csomagot hiányol, azonban ennek letöltése helyett a link egy trójaira mutat.

2008. Mi várható, mire lehet képes egy ekkora botnet?

A StormWorm botnet számítási kapacitása állítólag vetekszik a világ szuperszámítógépeinek teljesítményével. Egyesek 50 millióra, míg az óvatosabbak 1-2 millióra becsülik a számítógépek számát ebben a botnethálózatban. Micsoda óriási számítási teljesítmény! A titkosszolgálatok joggal aggódhatnak. Itt azért átértékelődik a különféle erősségű kódok feltöréséhez szükséges időmennyiség kérdése is, és persze a rainbow-táblák generálása is fel-

December egyik slágere volt a fürdőruhás lányokkal ékesített mikulásos képernyővédő, jár a pluszpont a rosszfiúk csapatának – ötletekért nem kell a szomszédba menniük

Benazir Bhutto halála is kapóra jött a csalóknak

gyorsítható ilyen irdatlan erőforrások birtokában.

„Teljesítményben a botnet csúnyán lenyomja a szuperszámítógépeket. Nagyon ijesztő, hogy ekkora számítási kapacitás áll a bűnözők rendelkezésére, de nem nagyon tehetünk ellene semmit" – összegezte a helyzetet az InformationWeek-nek Matt Sergeant, a MessageLabs spamellenes részlegének műszaki igazgatója.

Az információs hadviselés kulcsfontosságú, ahogy azt Bruce Willis Die Hard 4.0 című filmjében is láthattuk. Emlékezetes, hogy 2007 májusában az észtországi IP-címek ellen Oroszország indított támadást – gyanítható, hogy ezt a módszert fogjuk még tapasztalni különböző konfliktusokban. Nagyon jó előadást láthattunk erről a témáról a 2007-es Hacktivity konferencián Muha Lajostól (Gábor Dénes Főiskola) „Kiberháború az orosz–észt viszony kapcsán" címmel.

A Sans Institute (ISC) kutatói szerint azonban lehet, hogy a virtuális gépekkel való elemző támogatás veszélybe kerülhet, ugyanis az új Storm féreg – amelynek készítői szemlátomást találékony elmék – felismeri a virtuális környezeteket, és ezek alatt nem fertőz. A cikk (**hopp.pcworld.hu/4222**) szerint a Microsoft Virtual PC-je, valamint a talán leghíresebb, több különféle platformon is elérhető VMware program eshet így ki a virusvédelmi fegyvertárból. A virtuális környezet „leleplezése" olyan illegális utasítások végrehajtásával történik, amely a fizikai hardveren hibaüzenetet generál, míg a virtuális gépben nem. A kártevő készítői ezzel igyekeznek lassítani és gátolni a víruslaborok eredményes munkáját – és sajnos gyaníthatóan az újabb vírusokban is szerepel majd ez a trükk.

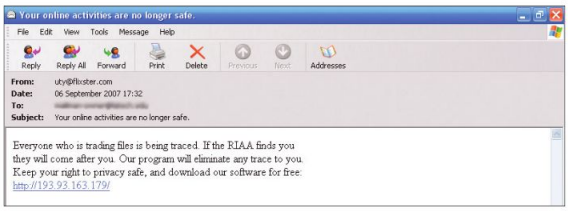
Ha hiányzó kodekcsomagot vagy Active-X modult javasolnak letöltésre, legyünk résen!

Segít-e a homokozó?

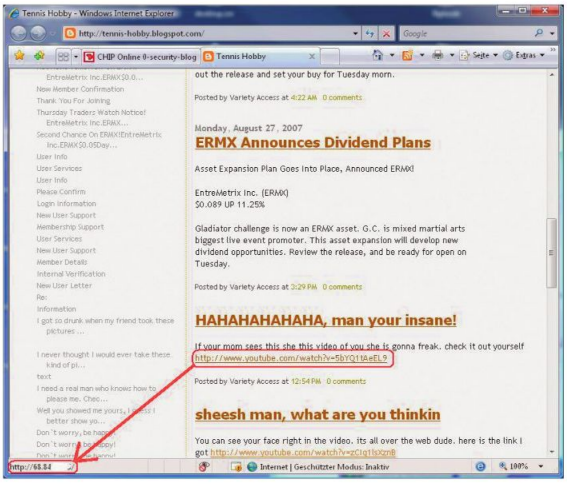
Igen hasznos módszer a kártevők feldolgozásánál, hogy elemzésükkor egy virtuális gépen történik a tesztelés, amely azt vizsgálja, hogy milyen bejegyzéseket, állományokat hoz létre, milyen internetes aktivitást mutat, hogyan történik maga a fertőzés. Ezzel kevésbé veszélyes terepen lehet adatokat gyűjteni a kártevőkről, ráadásul a vizsgálat gyorsan és olcsón végezhető.

The Show Must Go On

Énekelte a Pink Floyd, na meg a Queen, és így is van, az élet nem állhat meg, megy tovább, mindkét oldal tanul a történésekből, és



Fenyegető vagy csalogató levélből mindig van raktáron, a könnyelműek elcsábítására



A StormWorm által írt blogbejegyzésben szereplő linknél vegyük észre, hogy az valójában nem a YouTube oldalra mutat, hanem valamilyen kétes IP címmel jelölt weboldalra vezet

mind a „rosszfiúk", mind a védelmi programok fejlesztői folyamatosan csiszolják, javítják a technikákat. A jövőben majd okostelefonjaink, GSM- vagy autós navigációs rendszerünk, esetleg a Skype Vo-IP-s kapcsolatunk kerül sorra, és sajnos bizton állíthatjuk, a kártevők fejlődése itt sem fog megállni. A Skype 3.2 verziója már lehetővé teszi, hogy Pay-Palon keresztül pénzt utaljunk. Valószínűleg már lezajlottak az előkészületek a csalással szerezhető könnyű pénzkeresetet remélők oldalain. Létesültek már oldalak a felfedezett és kihasználható sebezhetőségek adásvételére is, és úgy tűnik, a sérülékenységek száma szűnni nem akaró áradatként egyre csak gyarapodik.

A hamis játéktöltő oldal gyereknek és felnőttnek egyaránt vonzó célpont lehet

Cikkünk végére értünk: kicsit stirlitzesen így lehetett dióhéjban összefoglalni a Viharféreggel kapcsolatos tavalyi történéseket. Biztos, hogy 2008-ban is hallani fogunk róla, sokak szerint ugyanis ez az eddigi legsokoldalúbb, legjobban rejtőzködő és legmegtévesztőbb kártevő.

Talán nem túlzás azt állítani, hogy a hollywoodi forgatókönyvírók újabb sztrájkja után akár a StormWorm brigádot is fel lehetne fogadni ötletgyárnak, ugyanis a megfelelő csali kiötlésében szemlátomást mindig aktívak és sziporkázók.

***

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

www.eset.com/threat-center/blog
www.f-secure.com/weblog
www.viruslist.com/en/weblog
www.symantec.com/enterprise/security_response/weblog
theinvisiblethings.blogspot.com
blog.metasploit.com