Nyakunkon az ellenség

Egyre gyakrabban hallunk híreket vírustámadásokról, új és egyre veszélyesebb vírusok felbukkanásáról. Elemzésünkben a vírusvédelem különböző aspektusait járjuk körül, a 2F tapasztalataira alapozva.

Miért kell védekeznünk?

Nem árulunk el titkot azzal, hogy a víruskereső programok feladata a vírusos programok (valamint a trójaiak, dokumentum-makrók és társaik) felderítése és ártalmatlanná tétele. Ha csak annyit megteszünk, hogy használjuk, és rendszeresen frissítjük őket, máris sok veszélyforrást hatástalanítottunk: a flopikon és CD-ROM-okon terjedő, e-mailben érkező, letölthető fertőzéseknek vége. A gépünket fenyegető veszélyeknek azonban, sajnos, nem.

Számítógépünk képes az internetre csatlakozni, vagy már eleve egy cég hálózatába van kötve, ez pedig igen komoly veszélyforrás. Több tanulmány egybehangzóan állítja, hogy az adatokat ért támadások nagyjából 80 százalékáért saját munkatársaink a felelősek. A támadók véletlenül vagy szándékosan akaszkodnak mások gépére, hogy ott, szintén véletlenül vagy szándékosan, adatvesztést okozzanak. Néha elég egy lelkes kolléga, aki csak „segíteni" akart. De előfordulnak komolyabb esetek is, amikor szándékosan egymás adatait lopták, törölték alkalmazottak vagy egykori alkalmazottak. Közvetlenül az internetre csatlakozva pedig még hatványozottabban fordulhat elő ilyesmi.

Egy új korszak kezdete

Érdekes példa az alig pár hete megjelent *Slammer* (vagy *Sapphire*) vírus.

Az *SQL-Slammer* néven is ismeretes Sapphire féreg, amely január 25-én jelent meg az interneten, új korszakot nyitott a gyorsan terjedő internetes vírusok történetében. Egy neves elemzőcég felmérése szerint a megfertőződött SQL szerverek 90%-a a járvány első 10 percében esett áldozatul a Slammernek. Az általuk nemrég publikált jelentés szerint a Slammer féreg közvetlenül megjelenése után már minden 8,5 másodpercben megduplázta a fertőzött gépek összlétszámát, és három percen belül elérte aktivitása csúcspontját, amikor is másodpercenként 55 millió adatcsomagot küldött szét a Világhálón. A Slammer terjedése két nagyságrenddel (!) gyorsabb volt a 2001 nyarán megjelent *CodeRed* vírusénál, amely átlagosan 37 percenként duplázta meg a fertőzött gépek számát.

A 2F 2000 Kft. szolgáltatásai között kiemelkedő helyet foglal el az adatvédelem

A Sapphire férget készítő rosszindulatú hacker kifinomult, kézzel optimalizált gépi kódban írta meg a kártevőt. Emiatt annak mérete a memóriában mindössze 250 bájt (és az adathálózatban is csak 376 bájt), így szinte korlátlan példányszámban tud terjedni szerverről szerverre, a modern nagy sebességű hálózatokon keresztül. Mivel a féreg egyáltalán nem tartalmaz közvetlenül a gépeket pusztító rutint, a kódja igen kis méretű lehetett, és a további terjedés alapjául szolgáló fertőzött szerver-állománya is folyamatosan növekedett. A kisméretű, körülbelül 300 bájtos kártevő programkódja ugyanis annyira egyszerű, hogy csak a működéshez szükséges információkat hordozza.

Mivel a Sapphire féreg létezése a Windows memóriájára korlátozódik, a kód nem kerül kiírásra a háttértárolókon. A ma létező víruskereső szoftverek rajtuk kívülálló okokból nem képesek a teljes rendszermemóriát ellenőrizni, így a Sapphire hatékony felismerését nem lehet beépíteni az adatbázisaikba. A megfelelő védelmet

Mobil tartalomszűrő

Az *F-Secure Corporation* bejelentette az *F-Secure Mobile Filter* termékét, a világ első tartalombiztonsági megoldását a vezeték nélküli letöltő-rendszerekhez. A termék tartalomszűrési lehetőséget kínál a szolgáltatók számára a kártékony szoftverek és az inkompatibilis Java alkalmazások kiszűrésére, még mielőtt azok letöltődnének a mobiltelefonokra. A megoldás a szűrési feltételek automatikus frissítésének a szolgáltatását is tartalmazza. Emellett a szolgáltató rugalmasan definiálhat szabályokat a nem kívánt tartalom blokkolásához.

Az F-Secure Mobile Filter Java bájtkódelemzést és víruskeresést végez az inkompatibilis Java szoftverek és más káros tartalmak kiszűrésére a hálózaton, még a letöltés előtt. A transzparens proxy felépítés megkönnyíti az integrációt a letöltő-platformokkal, a szolgáltató oldalán található felhasználói felület pedig lehetővé teszi a nemkívánatos funkciók és akár az egyes inkompatibilis Java függvények kiszűrését is. Az *F-Secure Anti-Virus Research* központ automatikus, napi 24 órás szolgáltatást nyújt a tartalomelemző adatbázis frissen tartásához.

az operációs rendszer és az alkalmazások gyártói által kiadott biztonsági frissítések telepítése és a tűzfalak megfelelő konfigurálása jelenti.

Okulva a korábbi vírusok írói által elkövetett hibákból, a Sapphire féreg a rendszer órajelciklusát használja a célpontként szolgáló véletlen IP-címtartományok generálására, így bár az erőforrásokat nagyon pazarló módon, de korlátlan mértékben tud terjedni. Ennek egyik mellékhatása, hogy a kiküldött csomagok gyakran „multicast packet" típusú címmel rendelkeznek, vagyis a legrosszabb esetben egyetlen csomag is egy egész alhálózatnyi kiszolgálót fertőzhet meg! Ez a technika eddig ismeretlen volt.

A Slammer vírusról szóló jelentésben a *CAIDA* munkatársai kifejtik, hogy ez a féreg alapul szolgálhat olyan jövőbeli változatok kifejlesztéséhez, amelyek még gyorsabban terjednek, és nagyobb káoszt hagynak maguk után. „Ha a Slammer írói elterjedtebb szoftvert vagy biztonsági hiányosságot választanak célpontjuknak, és pusztító rutinnal egészítik ki a féregvírust, minden bizonnyal sokkal komolyabb kárt okozhattak volna" – áll az elemzésben.

A Microsoft 2002 júliusa óta ismerte azt az SQL 2000 biztonsági hibát, amelyet a Sapphire kihasznált, és amelyre a javítás meg is jelent júliusban. Sajnos jellemző, hogy mind a különböző operációs rendszerekre, mind pedig az alkalmazásokra kiadott hibajavító biztonsági javításokat NEM futtatják le a rendszergazdák, csak miután azok hiánya problémát okozott.

A Slammer írói – valószínűleg szándékosan – kihagyták a büntető rutinjukat, igazság szerint a tömeges fertőzésen túlmenően jelentős adatvesztést okozó pusztítást is véghez tudtak volna vinni. Az is szándékosnak látszik, hogy éppen a hétvégére időzítették a támadást, amikor a munkavállalók és a számítástechnikai szakemberek jó része nincs a munkahelyén.

A Slammer leglényegesebb tulajdonsága, hogy viszonylag könnyen lehet védekezni ellene – de nem víruskeresővel. A víruskeresők ugyanis merevlemezünk állományait vizsgálják folyamatosan, ez a vírus azonban sohasem ölt állományformát. Jelen lehet a gép memóriájában és a hálózaton is, fájlként azonban sosem találjuk. Fertőzési módja a számítógépeket feltörő crackerek, illetve az egymás adatait lopkodó kollégák módszereit idézi: a hálózatot felhasználva támadja és fertőzi meg célpontjait, a víruskeresők számára mindvégig láthatatlanul.

Mire jó a tűzfal?

Hogyan védekezzünk akkor? Mit tehetünk a Slammerhez hasonló járványok, a gépünket célzó ismerősök és kollégák, ismeretlenek ellen? A megoldás a hálózati forgalom elemzése. Ezt legtöbbször a tűzfalak végzik, amelyek a vállalati hálózatok kiés bejövő forgalmát ellenőrzik. Saját kollégáink ellen azonban nem védenek meg, és ugyanez a helyzet akkor is, ha például egyszerű internet-felhasználóként otthonunkból kapcsolódunk a hálózatra. Nincs mit tenni, saját gépünk védelmére egyedi tűzfal kell. Ezeknek két fő fajtája is ismeretes, a vállalati és otthoni felhasználás igényeihez igazodva. A személyi tűzfalak a nagy és bonyolult vállalati tűzfalak védelmét adják – egyetlen gépnek. Feltelepítve a felhasználó szabályozhatja, ki és hogyan férhet a gép adattaihoz, erőforrásaihoz. Mivel beállítása a felhasználó aktív közreműködését igényli, a dokumentáció tanulmányozására nagy szükség lesz.

A Vírus Híradó portál hiteles és naprakész tájékoztatást nyújt a vírusokról, és hasznos információkkal látja el a PC-felhasználókat

Vállalati környezetben az igények és az elvárások is mások az effajta eszközökkel szemben. Itt rendszerint elosztott tűzfalakat használnak. Ezek hasonló elven működnek, mint a személyi tűzfalak, ám felügyeletüket, beállításukat, karbantartásukat a vállalat rendszergazdája végzi. Ily módon a felhasználók védetté válnak egymással és a külső veszélyekkel szemben, miközben egyáltalán nem kell bonyolult hálózati fogalmakkal megismerkedniük, érthetetlen műszaki kérdésekre hasukra ütve válaszolniuk.

Az elosztott és a személyi tűzfalak egy lépéssel tovább viszik a számítógépek védelmét. A statikus, állományokban kereső vírusvédőkre továbbra is szükség lesz – ám a dinamikus, a hálózatot aktívan felhasználó támadások, fertőzések ellen csakis ezekkel védekezhetünk hatékonyan.

Fórján Tamás, Csizmazia István
2F 2000 Kft.

Veszélyesebb vírusok 2003-ban

Veszélyesebb és nehezebben detektálható vírusok megjelenését helyezte kilátásba 2003-ra *Kimmo Alkio,* az *F-Secure Corporation* alelnöke.

2002-ben új típusú fenyegetések jelentek meg: a vírusok terjedése Linux rendszereken, a nyílt forráskódot kihasználó támadások, az otthoni számítógépekbe való betörések egyre gyakoribbá válása és az ázsiai vírusírók egyre növekvő aktivitása rengeteg munkát adott az adatbiztonsággal foglalkozó cégeknek.

Az új technológiák, a sok platform, valamint a mobil- és a vezeték nélküli eszközök rohamos terjedésével együtt nő a potenciális támadások száma is.

Mindezek a fenyegetések nagy lehetőséget, komoly piaci potenciált tartogatnak a biztonsági cégek számára. Kimmo Alkio szerint azonban a megfelelő megoldás kiválasztásánál ma már egyre nagyobb szerepet kapnak a könnyen menedzselhető, „mobil vállalati" biztonsági rendszerek, és egy ilyen komplex biztonsági szolgáltatás esetében a márkanév és a hozzá fűződő tapasztalat is egyre inkább meghatározó szempont.

Az F-Secure – melynek magyarországi disztribútora a *2F 2000 Kft.* – 10%-os piaci részesedéssel bír a magyar piacon.

A hazai felhasználók informálása érdekében a 2F 2000 Kft. munkatársai 2002 novemberében elindították a *Vírus Híradó* portált **(www.virushirado.hu),** amely magyar nyelven nyújt hiteles és naprakész tájékoztatást a vírusokról, s hasznos információval látja el a PC felhasználókat.