AEC Virus Eye

Obsah:

KAM KRÁČÍ ŠKODLIVÉ KÓDY?

PRVNÍ VIRUS PRO 64BITOVÉ SYSTÉMY

SÍŤOVÍ ČERVI STÁLE V KURZU: SASSER

SEMINÁŘE POŘÁDANÉ AEC A PC WORLDEM

www.aec.cz

Pro PC WORLD připravuje Tomáš Přibyl - tomas.pribyl@aec.cz

KAM KRÁČÍ ŠKODLIVÉ KÓDY?

Počítačové viry a další škodlivé kódy nejsou statickou záležitostí, ale naopak se velmi dynamicky vyvíjejí. Na tuto skutečnost samozřejmě musí odpovídajícím způsobem reagovat výrobci antivirových řešení a především samotní uživatelé, jinak se počítačová data ocitají v ohrožení.

Technikou, která je relativně novou a která zažívá nebývalý rozvoj v posledních měsících a letech, je využívání síťového prostředí pro šíření virů. Slovo „relativně" je v daném případě na místě, protože první síťový škodlivý kód se objevil už v roce 1988. Jmenoval se Worm (česky Červ), čímž dal vlastně za vznik celé kategorii pojmenování škodlivých kódů. Napsal ho jistý student Robert Morris, který chtěl na několika počítačích experimentálně odzkoušet šíření počítačového viru pomocí síťových prostředků. Jenomže pokus se mu kapku vymknul z ruky a došlo k napadení cca šesti tisíc počítačů (což v té době představovalo zhruba osm procent světové počítačové sítě). Robert Morris byl za svůj čin po zásluze odměněn – nedobrovolně musel ukončit studia a přídavkem dostal několik set hodin veřejně prospěšných prací.

Několik let jsme pak byli dalších síťových červů ušetřeni: internet byl příliš malý na to, aby se autor škodlivého kódu dokázal úspěšně skrývat a trest vyměřený Morrisovi měl dostatečně výstražný účinek (vida, jde to!). Až na samém konci devadesátých let se červi dočkali resuscitace. Nejprve v e-mailové podobě (např. Melissa), posléze byli schopni využívat pro svou distribuci lokální síť (Funlove aj.). A nakonec přišli i internetoví červi.

Jejich novou éru zahájil v červenci 2001 CodeRed, který využíval bezpečnostní chybu serverů s instalovaným prostředím IIS (Internet Information Server). Během jednoho jediného dne dokázal napadnout úctyhodných 340 tisíc počítačů na celém světě! Už nebylo třeba spouštět infikované soubory či spouštět napadené přílohy e-mailových zpráv. Díky využití bezpečnostního nedostatku stačilo mít „jen" zapnutý počítač s touto chybou. Mimochodem, je zajímavé, že CodeRed se světem pokouší šířit dodnes! To znamená, že dosud jsou na světě servery, jejichž administrátoři se neobtěžovali instalací příslušné záplaty (která byla už v době objevení CodeRedu několik týdnů k dispozici).

Další velký problém představoval na podzim 2002 objevivší se kód Opasoft. Ten v plné míře využíval výhod síťového červa, ale byl schopen napadat počítače (opět s bezpečnostní chybou) s instalovaným systémem Win 9X. To znamená, že začal představovat nebezpečí také pro řadové uživatele!

Dosud nejrychleji se šířícím kódem se stal v lednu 2003 Slammer. Během pouhopouhých deseti minut dokázal napadnout devadesát procent všech napadnutelných počítačů – těch bylo asi 75 tisíc. Během první minuty šíření přitom dokázal zdvojnásobit počet napadených počítačů během každý 8,5 sekundy! (Pro srovnání: populace CodeRedu se zdvojnásobila každý 37 minut!)

Problémem je, že antivirové programy si s podobnými kódy zpravidla nemohou poradit. Potíž není technického rázu, jde o princip: síťový červ doputuje do počítače po síti, přičemž „žije" pouze v paměti stroje. Pokud si nevytváří na disku konkrétní soubor, antivirové programy jej ignorují. I kdyby jej totiž z paměti nakrásně odstranily, ve zlomku sekundy je škodlivý kód v počítači znovu. Celý systém by pak skončil v nekonečné smyčce nahrávání a odstraňování červa.

Aby se tomu předešlo, je nutné „ucpat díru", kterou se červ do počítače dostává – zpravidla jde o nutnost aplikace bezpečnostní záplaty. Až pak ho lze v klidu odstranit s tím, že už se nevrátí. Ještě lepším řešením je ale implementace právě personálního firewallu: pokud je dobře nastavený a používaný, jakýkoliv síťový červ nemá šanci. Výrobci antivirových řešení si toto už dávno uvědomili, a tak začínají nabízet své programy s již implementovaným personálním firewallem (např. F-Secure AntiVirus).

Navíc je potřeba si uvědomit, že díky různým bezdrátovým a mobilním technologiím čím dále více počítačů opouští bezpečí chráněné sítě (za serverovým firewallem apod.), a jsou tak zranitelnější vůči útokům/infiltracím. Velmi názorným je případ již výše zmíněného internetového červa Slammer, který dokázal díky přinesenému (nechráněnému) počítači napadnout informační systém jaderné elektrárny Davis-Besse v Ohiu. V lednu 2003 zde na několik hodin vyřadil z provozu dva systémy podílející se na monitorování reaktoru!

Jak je možné, že do počítačové sítě tak klíčového objektu, jakým jaderná elektrárna bezesporu je, pronikl škodlivý kódy (na který už ostatně byla známá záplata)? Odpověď je až smutně jednoduchá: díky hrubé nedbalosti. Do lokální sítě si přinesl nezabezpečený počítač zaměstnanec subdodavatele od dodavatele – a neštěstí bylo hotovo. Inu, díky technologickému pokroku je čím dále těžší pohyb počítačů a jejich stav uhlídat…
Incident naštěstí neměl závažné důsledky (kromě výrazné negativní publicity), protože záložní informační systém zůstal červem nedotčen a navíc byl reaktor v inkriminované době odstaven.

Hrozby, které personální firewall dokáže eliminovat přitom nespadají pouze do oblasti útoků síťových červů. Brání počítač před napadením hackery, infiltraci škodlivého kódu z web stránky, zabraňuje neoprávněnému získání práv po síti, snižuje riziko bezpečnostního incidentu vinou lidské chyby, znesnadňuje odcizení informací… Jak už bylo výše uvedeno, význam personálního firewallu narůstá zvláště s rozmachem mobilních a bezdrátových technologií.

Zatímco antivirový program vyhledává konkrétní nebezpečné (nebo potencionálně nebezpečné) soubory a data (např. skripty ve web stránkách), úkolem firewallu je sledovat a zastavovat potencionálně nebezpečný provoz.

Podtrženo, sečteno: antivirový program je stále základním stavebním prvkem bezpečného systému. Díky technologickému posunu současných škodlivých kódů nicméně není univerzálním všelékem.

PRVNÍ VIRUS PRO 64BITOVÉ SYSTÉMY

Dne 27. května 2004 byl objeven a analyzován první známý počítačový virus pro 64bitové operační systémy. Spíše než o opravdovou hrozbu se ale zatím jedná spíše o tzv. „proof of concept" – tedy jakýsi „důkaz, že to jde".

Jedná se o „klasický" virus, který infikuje 64bitové spustitelné (64bit PE) soubory nacházející se v aktuálním adresáři a jeho podadresářích, odkud byl virus spuštěn. Infekce spočívá v přidání kódu viru na konec souboru. Podle tvrzení virových analyzátorů virus obsahuje chyby.

Jisté znaky naznačují, že Rugrat byl odvozen od „obyčejných" 32bitových virů z rodiny Chiton. Kód viru není šifrován a nepoužívá ani žádnou polyformní metodu. Obsahuje následující text:

Shrug - roy g biv
06/05/04
4U2NV

Tento virus neinfikuje žádné 32bitové aplikace (PE soubory) a nefunguje v klasických 32bitových operačních systémech (Windows 9x, NT, 2000 nebo XP) bez speciálního software zajišťujícího podporu 64bitových aplikací.

SÍŤOVÍ ČERVI STÁLE V KURZU: SASSER

Počátkem měsíce května 2004 se objevila také nová rodinka internetových červů Sasser.

Všechny tři varianty Sasser.A, B i C zneužívají ke svému šíření bezpečnostní chybu v LSASS.EXE, která byla zveřejněna Microsoftem v Security Bulletinu MS04-011 již někdy v polovině letošního dubna.

Sasser pracuje tak, že z infikovaného počítače otevírá různý počet spojení nebo na něm spouští různý počet procesů, s jejichž pomocí se snaží nalézt další infikovatelný počítač. Cílovým portem je port 445.

- Sasser.A – 128 spojení (threads);
- Sasser.B – 128 procesů;
- Sasser.C – 1024 procesů.

Rutina pro generování IP adres je nastavena tak, že červ vždy určitou část pokusů směřuje do lokální sítě daného infikovaného počítače, část do okolních sítí a část IP adres generuje zcela náhodně.

Pokud červ najde infikovatelný počítač se systémem Windows 2000 nebo XP způsobí na něm pomocí uvedené bezpečnostní díry „buffer overflow" v procesu LSASS.EXE. Potom na vzdáleném počítači dokáže na dálku ovládnout na TCP portu 9996 příkazovou řádku, vytvořit skript cmd.ftp a spustit jej. Tento skript přinutí vzdálený počítač ke stažení samotného souboru červa prostřednictvím FTP protokolu na TCP portu 5554 z prvotně infikované stanice a jeho spuštění.

Na infikované stanici se červ usazuje do systémového adresáře Windows jako „avserve.exe" (u verze „B" a „C" – „avserve2.exe"). Kromě toho ve stejném adresáři vytváří ještě jednu kopii s částečně náhodným názvem ve tvaru náhodné_číslo#_up.exe a v kořenovém adresáři C: soubor „win.log", který obsahuje IP adresu počítače (localhost). Spuštění při každém startu systému si zajišťuje vytvořením klíče v registru.

Vedlejším efektem činnosti červa Sasser je porucha činnosti LSASS.EXE, která vede k vynucenému restartu systému. Ten je provázen zobrazením následujícího dialogu:

Jako prevenci proti infekci použijte záplatu, kterou najdete na: http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

SEMINÁŘE POŘÁDANÉ AEC A PC WORLDEM

Ve druhé polovině května letošního roku se postupně v Košicích, Banské Bystrci a Žilině uskutečnil již třetí ročník AEC roadshow Slovensko – řady seminářů, která je věnovaná problematice počítačové bezpečnosti (viz snímek). Mediálním partnerem se stala právě redakce PC Worldu, odbornou záštitu převzala firma AEC zabývající se komplexními službami v oblasti počítačové bezpečnosti. Na seminářích zazněly příspěvky věnující se problematice počítačových virů, antivirové ochraně, elektronickému podpisu, šifrování a ICT bezpečnosti vůbec. Celkem všechny tři semináře navštívilo více než sto účastníků.

Přední česká společnost zabývající se otázkami informační bezpečnosti AEC Data Security Company uspořádala v Praze ve spolupráci s redakcí měsíčníku PC World několik seminářů zaměřených právě na otázky ochrany elektronických dat. Jeden z nich se uskutečnil na počátku května 2004, přičemž byl věnovaný nejen přednáškám o aktuálním stavu virových hrozeb a dalších nebezpečí přicházejících z internetu, ale také představení produktů finské společnosti F-Secure. Další seminář zaměřený na informační bezpečnost proběhl v úterý 1. června 2004 a orientovaný byl tentokráte na produkty společnosti Norman.

[KONEC magazínu AEC VIRUS EYE]