AEC Virus Eye

Obsah:

www.aec.cz

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

ŠPINAVÉ TRIKY POČÍTAČOVÝCH VIRŮ

Počítačové viry bohužel nejsou statickou záležitostí, ale nesmírně dynamicky se vyvíjejí. Jejich programátoři přicházejí se stále novými nápady, jak „oblafnout" uživatele či výrobce antivirových programů. Většina těchto nápadů je víceméně primitivní (nebo poněkud fádně okopírovaná z jiných virů), ale některé rozhodně stojí za pozornost. Podívejme se nyní na několik podobných „inovací", jimiž hackeři vybavili počítačové viry v poslední době.

Já jsem to opravdu nebyl!

Máte kvalitní antivirovou ochranu, pravidelně ji aktualizujete, správně používáte (nebo si to alespoň myslíte). O spolehlivosti zabezpečení se pravidelně přesvědčujete, protože antivirový software zachytává příchozí/vstupující viry a pravidelně o tom podává hlášení. A najednou vám začnou chodit e-mailová varování, že šíříte virus. Jednou jsou slušnější, jednou jsou méně slušná. Jak je to možné? Co se děje?

Málokdo u uživatelů informačních technologií si totiž uvědomuje, e-mailová adresa „odesílatele" nemusí vůbec nic vypovídat o tom, kdo je skutečným odesílatelem (spíše by se mělo napsat: z jehož počítače se virus rozesílá). Pro virus je totiž úplně jednoduché adresu odesílatele změnit; nejčastěji je použita jiná - již existující.

V praxi to pak vypadá tak, že virus napadne počítač pana A. Pan A je šetrný nebo nezkušený, takže nepoužívá antivirovou ochranu. Výsledkem je, že se virus rozešle na všechny strany – nejčastěji k získání seznamu kontaktů použije třeba e-mailový adresář pana A. Všem těmto „obětem" pak přijde v elektronické poště virus. Jenomže ne každý je šetrný nebo nezkušený, takže antivirová ochrana většinu těchto virů zachytí. Lidé pak mohou zpětně pana A varovat: pozor, rozesíláte viry!

A teď si představte navlas stejnou situaci jen s tím rozdílem, že virus při odchodu z počítače změní adresu odesílatele. Takže místo pana A tam podvodně uvádí jako odesílatele paní B (její adresu si mohl najít třeba v adresáři pana A). Následně dochází k situaci, kdy se světem šíří virus, který se tváří jakoby jej odesílala paní B (přestože tak činí počítač pana A – samozřejmě bez jeho vědomí). Paní B přitom může být klidně na dovolené – virus pouze použil její jméno.

Antivirové programy pak hlásí, že od paní B chodí viry. Lidé se ji následně pokoušejí varovat nebo spílají (záleží na nátuře). A když se paní B vrátí z dovolené, nestačí se divit.

Přitom je prakticky bezmocná, neboť je nesmírně obtížné zjistit, ze kterého počítače se virus skutečně šíří. Výsledkem je, že paní B je stále zasypávána e-mailovými varováními, kdežto skutečného viníka (pana A) nikdo neupozorní.

Infikovaný obrázek?

Mohou či nemohou elektronické obrázky obsahovat virus? Na tuto otázku nelze odpovědět prostým „ano, mohou" nebo „ne, nemohou". Odpověď je krapet složitější.

Dá se říci, že samotný obrázek aktivní virus obsahovat nemůže. Obrázek je ve své podstatě souborem dat, která grafický editor či prohlížeč pouze ZOBRAZÍ, ale NEVYKONÁ JE. Jinými slovy – kniha s návodem na výbušninu vám neexploduje v ruce při četbě. Pokud chcete kýženého výsledku (exploze) dosáhnout, musíte výbušninu dle návodu vyrobit.

Pozor! Je zapotřebí mít na paměti, že teď hovoříme o „čistých" obrázkových formátech (GIP, JPG, BMP…). Některé speciální aplikace už do obrázku umožňují vkládat doplňkové funkce, které se následně chovají jako regulérní počítačový program – a tyto samozřejmě virus obsahovat můžou. Toto ale už nejsou „čisté" obrázky (jedná se např. o aplikace AutoCAD či Corel Draw!).

Nedávno se ovšem objevil škodlivý kód Perrun, který byl údajně schopen infikovat i nejrozšířenější formát obrázků JPG (resp. JPEG). Je tomu ale skutečně tak?

Ve chvíli, kdy je virus Perrun spuštěn, vyhledá v počítači všechny soubory s koncovkou JPG a na konec každého z nich připojí svůj kód (aby zabránil vícenásobné infikaci, přidává do napadených souborů svou „značku"). Navíc Perrun vytvoří EXE soubor, který uloží do počítače. Poté provede zápis do registrů v operačním systému tak, že kdykoliv je otevíraný nějaký obrázek JPG, je nejprve spuštěný výše uvedený EXE soubor. Ten se vzápětí „podívá" do těla volaného JPG souboru, z nějž si vyextrahuje data, uloží je do nového souboru X.EXE a vykoná je. Výsledkem tedy je, že JPG soubory mohou nést škodlivý kód, ale tento nemůže být z nich samovolně aktivován. Obrázky formátu JPG jsou tak samy o sobě bezpečné. Jsou pouze nosiči dat – primárně obrazových, sekundárně je ale možné je zneužít i k nekalým činnostem. V praxi se běžně obrázky JPG používají třeba k předávání šifrovaných dat: na první pohled uživatel dokáže zobrazit jen obrázek, ale s pomocí specializovaného software je možné z něj „vytěžit další informace. Něco podobného dokáží využít i počítačové viry.

Tady virus nemůže být!

Škodlivý kód (ať již virus či síťový červ) se do počítače ve zhruba devadesáti procentech případů dostává prostřednictvím elektronické pošty. Jedná se o různé programy ve formátu EXE, PIF, SCR (či jiné „exotické" koncovky jako CPH) nebo třeba o skripty vložené v HTML kódu. Proto se někdy doporučuje při posílání dokumentů tyto zabalit (třeba do archívu ZIP, ARJ, RAR nebo CAR) – donedávna platilo, že počítačové viry putují světem v „otevřené" podobě.

Jenomže změnu přinesl škodlivý kód Cervivec. Ten putoval světem ve zprávách elektronické pošty, přičemž vlastní EXE soubor byl zabalený do archívu ZIP. V tomto formátu pak vesele procházel přes antivirové brány – ne že by antivirové programy nedokázaly nahlédnout do archívů, ale většinou něco podobného v rámci zvýšení rychlosti kontroly neměly nastavené. Vždyť „takhle se přece virus nechová"!

Omyl, choval. Cervivec vyžadoval velkou míru spolupráce uživatele (rozbalení archívu a následné spuštění extrahovaného souboru), nicméně přesto fungoval a celkem úspěšně se šířil světem. K tomu mu jistě napomohla i skutečnost, že využíval textu e-mailové zprávy v několika jazykových mutacích (česky, slovensky, německy, polsky, rusky…), což zvyšovalo jeho důvěryhodnost u příjemců.

Nejsem virus, jsem antivirus

Sociální inženýrství. Tímto termínem je označováno snížení lidské pozornost způsobem, který by se v reálném světě dal označit za „ránu pod pás". Jak vlastně funguje? Pokud elektronickou poštou přijde soubor „znicim_data.exe", asi jej spustí jen málokterý šílenec. Ale soubor „Kurnikovova.exe" nebo „girls.exe" spustí prakticky kdekdo. Přitom obsah obou souborů může být stejný, neboť jejich název o skutečném obsahu absolutně nic nevypovídá.

Přímo čítankovým příkladem sociálního inženýrství může být jedna z variant viru Iloveyou. Uživateli přišla e-mailová zpráva, v níž stálo, že jím objednané květiny budou doručeny na stanovenou adresu a že z jeho bankovního účtu bude strženo 329 dolarů 50 centů. Bližší informace o celé transakci naleznete v příloze e-mailové zprávy. Samozřejmě, že se uživatel, který nic neobjednával, vyděsil, zapomněl na veškerou opatrnost (obava o 329 dolarů 50 centů zvítězila) a poklikal na přiložený soubor. Žádné informace o nákupu květin v něm ovšem nebyly, neboť šlo o virus – a ten právě "napálený" uživatel aktivoval.

V rámci sociálního inženýrství se škodlivé kódy vydávají za soubory s erotickým obsahem, za vtipy (těch si lidé elektronickou poštou posílají mraky) a v neposlední řadě třeba také za aktualizace antivirových programů. Lidé se z principu bojí počítačových virů, a tak vítají každou pomocnou ruku, která je jim podána. A když někomu přijde soubor tvrdící o sobě, že je to univerzální aktualizační soubor proti supernebezpečnému viru ABCD, mnoho uživatelů jej v bláhové naději spustí. Že se nejedná o univerzální aktualizační soubor (což je sám o sobě technický nesmysl, protože každý antivirový program používá jiný formát a strukturu dat), ale o vlastní virus, jistě netřeba zdůrazňovat.

V BOJI PROTI SPYWARE

Společnost Norman, známý výrobce software pro antivirovou ochranu a bezpečnost dat, spojil svoje síly s firmou Lavasoft. Výsledkem je produkt Norman Ad-Aware SE, který je dostupný ve verzi pro jednotlivé uživatele i v síti.

Problémy spojené s nežádoucím software – spywarem v poslední době narůstají. Uživatelé s přístupem na internet se s ním setkávají stále častěji. Podle některých statistik je spywarem infikováno až 90 % počítačů. Pod tímto pojmem si přitom můžeme představit například různé programy sloužící k monitorování aktivit uživatele na internetu nebo také přímo škodlivé kódy zaznamenávající stisknuté klávesy (keylogger). Můžeme se setkat dokonce i s aktivní destrukcí dat.

Norman Ad-Aware poskytuje neustálou ochranu proti tomuto nechtěnému software. Uživatel je při každé činnosti na internetu dokonale chráněn. Program kolem počítače vytváří imaginární ochranné pásmo, ve kterém vyhledává a likviduje veškeré škodlivé činnosti a pokusy o narušení bezpečnosti systému.

Norman Ad-Aware uživateli umožňuje pomocí řady nastavení určit vlastní úroveň bezpečnosti podle individuálních potřeb.

Norman uvolňuje tyto dva produkty:

- **Norman Ad-Aware SE Plus Edition** – určen pro použití jednotlivými uživateli, které chrání při surfování na internetu.
- **Norman Ad-Aware SE Professional Edition for Networks** – určen pro použití ve firemním síťovém prostředí.

BAGLE: NEKONEČNÝ PŘÍBĚH

Podle zpráv světových antivirových společností se šíří vyskytuje další z dlouhé řady variant e-mailového červa Bagle, tentokrát s označením AS. Kromě rutin pro šíření prostřednictvím P2P (Peer-To-Peer) sítí červ disponuje také kódem zadních vrátek.

Zmatek v označování jednotlivých verzí červů Bagle se projevuje různým indexováním u různých antivirových firem. Kromě „AS" je tento červ označován také jako Beagle.AR, Bagle.az nebo Bagle.AM.

Bagle.AS se šíří prostřednictvím infikovaných e-mailů, které jsou složeny z řady možných komponent. Přiložený soubor může mít název „Price", „price" nebo „Joke" s příponou .exe, .scr, .com nebo .cpl. Adresy čerpá „klasicky" ze souborů určitých typů nalezených na discích infikovaného počítače. Některým adresám se vyhýbá. Rozesílání provádí pomocí vlastního SMTP motoru. Adresa odesílatele je samozřejmě falešná.

Pokud je červ uživatelem spuštěn (možno pouze manuálně, tzn. poklikáním na soubor červa), vytváří v systému vlastní mutex a do systémového adresáře Windows umisťuje soubory: cjector.exe, bawindo.exe, bawindo.exeopen a bawindo.exeopenopen.

Červ také vytváří vlastní klíč v systémovém registru a některé položky z něj naopak maže. Ty patří různým jiným červům a bezpečnostním programům. Kromě toho se snaží přerušovat také procesy patřící různým bezpečnostním aplikacím.

K šíření se snaží zneužít také P2P sítě. NA všech lokálních pevných discích vyhledává složky, které obsahují ve svém názvu text „shar". Pokud takovou najde, umístí do ní spoustu svých kopií s lákavými názvy (např. Microsoft Office XP working Crack, Keygen.exe, Serials.txt.exe apod.).

Červ navíc instaluje do systému zadní vrátka, která komunikují na TCP portu 81 a náhodně zvoleném UDP portu. Umožňují vzdálenému útočníkovi ovládnutí infikovaného počítače. Kromě toho červ obsahuje ještě funkci pro stažení souboru WS.JPG z některého z mnoha webů z vnitřního seznamu. Obrázek se ale dosud na žádném z webů neobjevil.

NOVÉ PRODUKTY F-SECURE V ČEŠTINĚ

Brány finské společnosti F-Secure opouští nové verze programů F-Secure Internet Security 2005 a F-Secure Client Security. Kromě mnoha vylepšení, která obsahují, je důležité i to, že jsou v češtině.

F-Secure uvolňuje nové verze svých programů určených k ochraně domácích uživatelů a malých firem, které nemají vlastní IT oddělení. F-Secure Internet Security 2005 a F-Secure Anti-Virus 2005 nově obsahují nástroje na likvidaci spyware a záchranné CD. F-Secure Internet Security 2005 navíc přináší ochranu před hrozbami přicházejícími z internetu. Kromě anti-spyware obsahuje také funkce pro kontrolu přístupu, likvidaci spamu, přesměrování vytáčeného internetového připojení a ochranu proti dalším zranitelnostem.

F-Secure Internet Security 2005 obsahuje oproti předchozí verzi množství nových funkcí a vylepšení. Anti-spyware chrání uživatele před nežádoucími aplikacemi, které mohou být instalovány s některým software (např. klienty P2P sítí). Další nové funkce zabraňují úniku citlivých informací, které mohou být odeslány z chráněného počítače do internetu některými škodlivými kódy. Nejmladší uživatelé jsou chráněni před nežádoucím obsahem přicházejícím z internetu pomocí modulu „Parental Control". Program dokáže blokovat internetové stránky obsahující odkaz na nežádoucí materiály.

Anti-Spam filtruje nevyžádané e-mailové zprávy a redukuje útoky typu „phishing". Anti dialer zabraňuje nežádoucímu podvodnému přesměrování vytáčeného připojení k internetu na drahé linky bez vědomí uživatele. Nový systém automatické aktualizace udržuje denně všechny součásti programu (virové definiční databáze, parental control a anti-spam) v maximální pohotovosti tak, aby dokázaly reagovat na každou novou hrozbu. Uživatel má taktéž k dispozici bezpečnostní zpravodajství informující ho o nových hrozbách.

F-Secure Internet Security 2005 je kompatibilní s Windows XP SP 2 a podporuje také Microsoft Security Center, do kterého je integrován.

Nově v českém jazyce je k dispozici také F-Secure Anti-Virus Client Security - řešení pro komplexní ochranu pracovních stanic. V poslední verzi uživatel najde kromě některých drobných vylepšení např. také podporu protokolu IMAP. Výhodou tohoto řešení je při nasazení ve firemní síti zejména jeho centrální správa prostřednictvím F-Secure Policy Manageru.

[KONEC magazínu AEC VIRUS EYE]