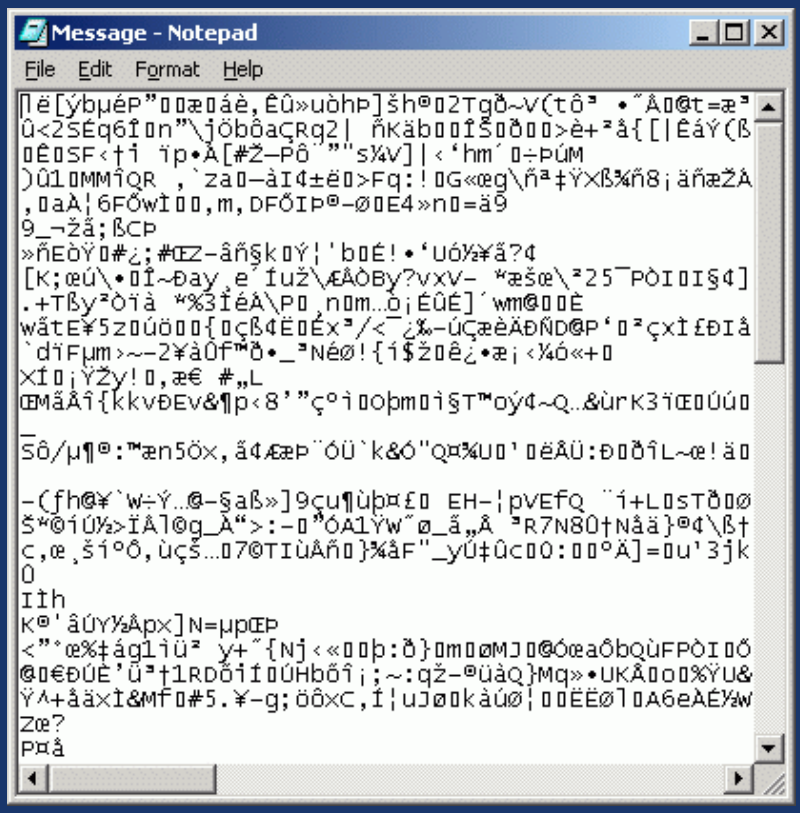
informační
bulletin
AEC DATA SECURITY COMPANY

(Připravuje AEC Data Security Company – jakékoliv připomínky, náměty či dotazy posílejte na e-mailové adresy tomas.pribyl@aec.cz nebo petr.nadenicek@aec.cz)

Počítačové viry, antivirové technologie, elektronický podpis, šifrování dat – prostě ochrana datových informací vůbec.

Dnes přinášíme:

- **MyDoom: bezprecedentní epidemie**
- **Program konference Security 2004**
- **Novinky mezi počítačovými viry: Bagle**
- **I antivirové programy stárnou**



Dosud největší virovou epidemii v historii způsobil e-mailový červ MyDoom na přelomu ledna a února 2004. Celosvětově mu „sedlo na lep“ několik miliónů uživatelů, kteří uvěřili, že se jedná o zprávu o nedoručení elektronické pošty či jiné hlášení poštovního serveru. Pokud na přílohu elektronické pošty poklikali, viděli jen takovouto změť znaků – a navíc si zavirovali počítač…

AEC DATA SECURITY COMPANY

MyDoom: bezprecedentní epidemie

Dotaz na Rádio Jerevan:
„Kdy bude líp?"
Odpověď:
„Už bylo."

Jako by počátek letošního roku chtěl prokázat smutnou pravdivost tohoto starého vtipu. Přestože je rok 2003 (právem) označovaný jako „nejhorší v historii počítačových virů", letošek už mu začal směle šlapat na paty. A to z něj čas ukrojil jen relativně malou část. Logicky tak vyvstává otázka: „Co dalšího nám ještě přinese?" Cílem tohoto materiálu ale není na ni odpovědět, nýbrž se ohlédnout nad útokem škodlivého kódu MyDoom, který se ostatně zapsal do historie jako největší epidemie v historii.

Na úvod několik statistických údajů, které názorně ukazují míru šíření červa Mydoom. Britská společnost Messagelabs, která se zabývá ochranou poštovních serverů některých velkých organizací a poskytovatelů internetového připojení, dává na svých stránkách k dispozici statistiky vytvořené pomocí takto získaných údajů. Díky velkému počtu chráněných e-mailových schránek můžeme tyto statistiky považovat za dostatečně odpovídající globální situaci. Za zhruba dva týdny společnost Messagelabs zachytila 38 miliónů kopií červa. Pro srovnání: do té doby největší epidemie (Sobig.F) představovala o pět miliónů zachycených kopií méně, a navíc za dobu celých tří týdnů!

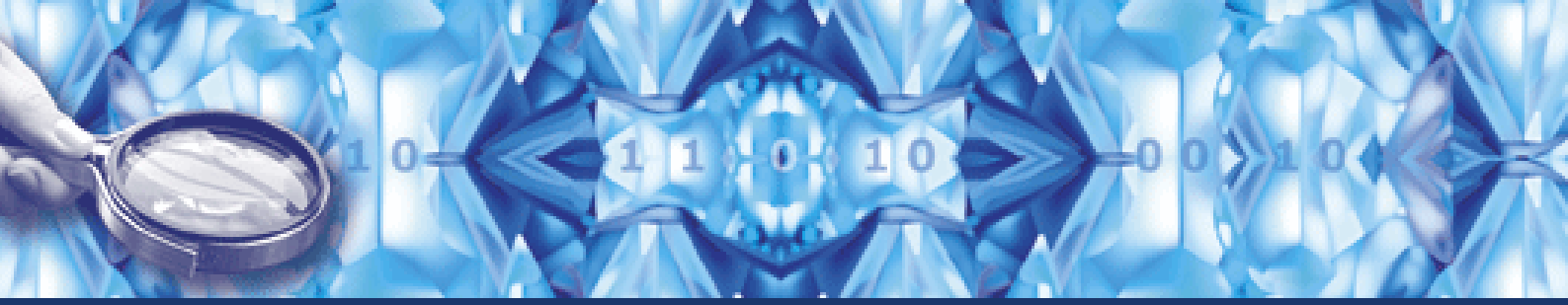
Z technického či technologického hlediska musíme konstatovat, že MyDoom nepředstavuje prakticky nic nového. Skoro bychom jej mohli zařadit na úroveň jiných e-mailových červů starých dva až tři roky. V čem tedy tkví tajemství jeho úspěchu? Odpovědí je několik, přičemž základní je: v obratném využití sociálního inženýrství. MyDoom se totiž maskoval do zprávy s následujícími předměty: test, hi, hello, Mail Delivery System, Mail Transaction Failed, Server Report, Status nebo Error. Jak vidno, některé z nich se tváří jako chybová hlášení o neúspěšném odeslání/doručení e-mailu nebo chybové hlášení. Takovéto informace člověka i v obrovské záplavě elektronické pošty zajímají. Který e-mail nebyl odeslaný? Kde je chyba? Co mám napravit? Uživatelé si uvědomují, že neodeslání elektronické pošty může v mnoha případech představovat ekonomickou ztrátu (nezískání zakázky apod.).

V okamžiku, kdy MyDoom přijde do počítače, je k jeho aktivaci nutná spolupráce uživatele. Ta představuje nutnost poklikat na přílohu e-mailu: na rozdíl od jiných škodlivých kódů nemá tento červ možnost se díky bezpečnostním chybám (např. I-Frame) samočinně aktivovat. Po poklikání na přílohu se aktivuje nejen červ, ale dojde také k zobrazení změti znaků v okně Poznámkového bloku (Notepadu). To slouží ke zmatení uživatelů, kteří očekávají nějakou akci.

MyDoom se následně instaluje do systémového adresáře Windows jako soubor TASKMON.EXE a přidává pro něj záznam do systémového registru, který zajišťuje jeho spuštění při každém startu operačního systému. Dále na pevný disk infikovaného počítače kopíruje soubor SHIMGAPI.DLL, který představuje zadní vrátka otevíraná na TCP portu v intervalu 3127 až 3198. Zadní vrátka mohou být útočníkem zneužita pro neoprávněnou manipulaci s počítačem na dálku.

Počínaje 1. únorem má každá aktivní kopie červa úkol začít posílat v intervalu 1024 milisekund požadavky (GET / HTTP/1.1) na webový server sco.com. Cílem tohoto snažení je server přetížit, a tím vyřadit z provozu (DDoS útok).

Kromě výše popsané varianty e-mailového červa se později objevila ještě verze MyDoom.B, jejíž největší odlišností je směrování DDoS útoku proti doméně microsoft.com. Tento útok ale nebyl příliš úspěšný. Zatímco první verze MyDoomu má naprogramováno ukončení činnost k 12. únoru, „béčko" až k 1. březnu. Přesto se s nimi lze setkat i po těchto datech: zásluhou uživatelů a jejich počítač se špatně nastavenými systémovými daty.



Je zajímavé, že případ MyDoom měl pokračování v podobě internetového červa (ten pro své šíření nevyužíval elektronickou poštu, ale pouze síťové prostředí). Jeho jméno bylo Doomjuice. Napadal počítače infikované červem MyDoom.A, podnikal DdoD útok na microsoft.com a především kopíroval na disky napadených počítačů zdrojových kód první verze MyDoomu.

Proč to dělal? Do té doby totiž měli zdrojový kód červa k dispozici pouze autoři. Pokud by se je podařilo vypátrat, mohl by být použit coby důkaz proti nim. Jenomže takto se během krátké doby dostal zdrojový kód na desetitisíce počítačů – což samozřejmě snížilo důkazní hodnotu zdrojového kódu v případě, že by se pachatele útoku podařilo dopadnout. (Za jejich hlavu mimochodem vypsaly firmy SCO a Microsoft odměnu po čtvrt miliónu dolarů.)

Podtrženo, sečteno: přestože z technického hlediska MyDoom a jeho následovník nepředstavovaly nic nového, dokázaly způsobit obrovskou epidemii. Důvodem byla neopatrnost nebo nedůslednost uživatelů, protože každý, kdo dodržel základní bezpečnostní pravidla, byl přímých důsledků této epidemie ušetřen.

Program konference SECURITY 2004

V úterý 6. dubna 2004 se bude v prostorách hotelu Andel´s (Stroupežnického 21, Praha) konat další ročník konference Security (konference.aec.cz). Odborným garantem je již tradičně společnost AEC Data Security Company, záštitu letos převzalo Ministerstvo informatiky ČR. Mediálním partnerem je už tradičně vydavatelství Vogel Burda Communications (Chip, Level, Počítač pro každého aj.). Na konferenci zazní následující příspěvky/přednášky:

- Úvodní slovo (Ing. Alena Řezníčková, AEC)
- Informační bezpečnost na prahu 21. století (Ing. Lubomír Moravčík, Ministerstvo informatiky ČR)
- Outsoursing bezpečnosti a použití IT ve státní správě (Ing. Jiří Mrnuštík, AEC)
- Systém řízení IT bezpečnosti a možnosti jeho certifikace (Luděk Novák, BDO IT)
- Případová studie ke zpracování a prosazování bezpečnostní politiky ve veřejné správě (Olga Přikrylová, AEC)
- Smart PKI – nejenom bezpečnostní aspekty distribuce osobní elektronické identity (Ing. Vladimír Král, Monet+)
- WiTness projekt (EU) – Wireless Trust for mobile businesses (Ing. Roman Garba, T-Mobile CZ)
- Data Security and the Real World (Mikko Hypponen, F-Secure Corp.)
- Organised Crime in the Internet: Future Reality? (Alexej Kalgin, Kaspersky Lab)
- Spam a vírusy – bratia v zbrani (Ing. Miroslav Trnka, ESET)
- Firewally: bojovníci první linie (Tomáš Vobruba, AEC)
- Tajemství IDS a IPS (Oldřich Válka, AEC)
- Stručný průvodce světem a podsvětím testů antivirových systémů (Ing. Petr Odehnal, Grisoft)
- Havět 2003 (Igor Hák, www.viry.cz)
- Virové události za poslední rok v kostce (Ing. Pavel Baudiš, Alwil Software)

AEC
DATA SECURITY COMPANY

Novinky mezi počítačovými viry: Bagle

Bagle je e-mailový červ, který na infikovanou stanici instaluje komponentu umožňující její zneužití na dálku prostřednictvím TCP portu 6777. Šíří se e-mailem, jehož přiložený soubor má náhodné jméno (např. frjujs.exe) s ikonou kalkulačky Windows.

Pokud dojde ke spuštění přílohy uživatelem, červ nejdříve ověřuje, zda je systémové datum rovno 28. lednu 2004 nebo pozdější. Pokud ano, ukončuje svoji činnost a systém neinfikuje. V opačném případě spouští standardní Kalkulátor (program calc.exe) obsažený v systému Windows, čímž kryje vlastní instalaci. Svůj soubor bbeagle.exe kopíruje do systémového adresáře Windows a vytváří pro něj klíč v registru, který zajišťuje jeho spuštění při startu systému.

E-mailové adresy pro další šíření čerpá ze souborů s příponou .wab, .txt, .htm a .html. Rozesílání infikovaných e-mailů provádí pomocí vlastního SMTP motoru. Falšuje přitom adresu odesílatele, místo které dosazuje některou z nalezených v infikovaném systému.

Každá kopie červa poté naslouchá na TCP portu 6777 příkazům zvenčí. Svoji existenci a připravenost poslouchat rozkazy dává najevo kontaktováním některých webových serverů (resp. se pokouší volat určitý PHP skript, který je/byl na nich umístěn).

V polovině února 2004 se objevila v pořadí druhá varianta tohoto „úspěšného“ e-mailového červa. Bagle.B se rozesílá ve zprávách s přiloženým EXE souborem, který má ikonu zvukového souboru. Svoje šíření ukončil 25. února.

Svoje spuštění se snaží zamaskovat současným otevřením aplikace Záznam zvuku (soubor sndrec32.exe), která je součástí systému Windows. Fyzicky se do počítače instaluje jako soubor AU.EXE do systémového adresáře Windows. Modifikuje také registr systému tak, aby byl spuštěn při každém startu Windows. Pokud je červ aktivní, pokouší se přistupovat na určité webové stránky na serverech www.47df.de, www.strato.de a intern.games-ring.de

E-mailové adresy vybírá ze souborů s příponou html, htm, wab a txt nacházejících se na disku infikovaného počítače. Svoje další kopie rozesílá pomocí vlastního SMTP motoru. Vyhýbá se přitom adresám, které obsahují textové řetězce: .r1u, @hotmail.com, @msn.com, @microsoft a @avp. Bagle.B instaluje do systému také zadní vrátka komunikující na portu 8866. Jejich prostřednictvím může být na infikovaný počítač stažen a následně i spuštěn další cizí soubor.

AEC
DATA SECURITY COMPANY

I antivirové programy stárnou

Je to scénka, kterou snad každý specialista na problematiku počítačových virů už někdy zažil. „Jak se mi mohl do počítače dostat virus, vždyť mám antivirový program," volá pan Zoufalec a zpravidla následuje ne příliš lichotivé hodnocení práce antivirových firem. Jenomže při bližším ohledání místa činu je zjištěno, že počítač střežil program „Zabiják virů" z roku 1996. Přestože šlo ve své době o špičkový program, dnes je už beznadějně zastaralý. Stejně jako po čase měníme staré za nové oblečení, nábytek, automobily apod. Problém ve světě počítačových technologií je jednak v tom, že stárnou velmi rychle, a jednak jejich „opotřebování" nemusí být na první pohled patrné.

Je tedy skutečně nutné antivirový program měnit? (Nemáme teď na mysli přechod od produktů jednoho výrobce k jinému, ale o prostou obměnu stávajícího programu verzí vyšší.) Odpověď je poměrně jednoduchá a z hlediska uživatele neradostná: Ano, je to nutné. Dokonce nezbytně nutné. Není to vedeno snahou antivirových firem zajistit si trvalý odbyt, ale skutečností, že počítačové viry se stejně jako celý svět informačních technologií vyvíjejí. „Tvůrci" virů přicházejí s různými novinkami, využívají nové technologie, napadají programy či soubory donedávna považované za nedotknutelné… A aby s nimi antivirové systémy dokázaly držet krok a plnily svou funkci, je celkem pochopitelné, že čas od času morálně zastarají a je třeba je vyměnit.

Krásným příkladem může být situace v polovině devadesátých let. Ještě v roce 1994 neexistoval ani jeden makrovirus (speciální případ počítačového viru, který je schopen infikovat dokumenty programů, jako je např. Word, Excel, Powerpoint). A o dva roky později už připadalo devadesát procent celosvětových infekcí počítačů právě na makroviry. Uživatelé proto museli vyměnit své antivirové programy za nové, protože jejich starší typy kategorii „makrovirus" prostě neznaly. Mimochodem, tato situace byla velmi nepříjemná i pro antivirový průmysl, protože mnohem firem, které nedokázaly dostatečně pružně zareagovat, zkrachovalo.

Na předchozích řádcích jsme hovořili o nutnosti výměny antivirového programu za novější verzi (upgrade). Ovšem při jeho používání je nutné myslet také na aktualizace (update). Každý měsíc se totiž objevuje zhruba 800 až 1000 nových škodlivých kódů a právě prostřednictvím aktualizací je zapotřebí s nimi antivirový program „seznámit" (dalo by se i říci „doplnit databázi podezřelých programů").

Jinými slovy – antivirový program není možné pouze MÍT, ale je zapotřebí se o něj i STARAT. Jinak dává pouze falešný pocit bezpečí a takto „chráněný" počítač má pro viry náruč otevřenou.

AEC
DATA SECURITY COMPANY