29. 1. 2004

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Červ MyDoom – 22 kB zkázy v příloze

Masivně se šířící červ MyDoom opět ukázal, že školení o nebezpečnosti pošty je málo a jedno navíc nikdy neuškodí. Následující popis je tedy napsán tak, aby tohoto červa dokázal identifikovat i neodborný uživatel a v případě nákazy se dokázal ubránit.

V současné době je červ MyDoom (označovaný také jako Novarg či SCO) nejvíce se šířícím virem na planetě a úspěšně atakuje žebříčky nejaktivnějších virů všech dob. Ač obsahuje určité nové techniky vlastního rozesílání, stále spoléhá na nejslabší článek bezpečnosti - člověka, který ho sám z e-mailu spustí.

Jak ho poznám

Viry, které používají náhodné předměty zpráv, náhodné názvy souborů pro přípony a různý text v těle zpráv se upřímně dost špatně rozpoznávají. Tento červ má také docela velkou variabilitu a mění názvy dle potřeby. Záměrem jeho autora především bylo, aby vypadal jako obyčejné chybové hlášení o špatném e-mailu.

Základní rozpoznávací znaky jsou:

Velikost zprávy je mezi 22 a 23 kB. Velikost souboru v příloze je vždy 22528 bajtů. Příloha má často lákavě obyčejnou ikonku textového souboru, na kterou skočí i zkušenější uživatel. Soubor v příloze se například jmenuje *message.scr* a nese ikonku textového dokumentu. Opatrnost velí vždy kontrolovat celý název souboru, a pokud končí na .exe, .bat, .pif, .scr, .com, .cmd, rozhodně jej nespouštět. Tento červ využívá také jinak bezpečnou příponu .zip. Soubory mají obvykle jméno:

- document
- readme
- doc
- text
- file
- data
- test
- message
- body

Obsahem těla zprávy je buď nic nebo jeden z textů:

```
test

Mail transaction failed. Partial message is available.

The message contains Unicode characters and has been sent as a binary
attachment.

The message cannot be represented in 7-bit ASCII encoding and has been sent
```

`as a binary attachment.`

Poznámka: poslední tři texty jsou smysluplné chybové hlášky a najdete je občas i v normálních, jen špatně poslaných e-mailech. Pro tentokrát je ale můžete automaticky pokládat za podezřelé.

Objevují se ale také varianty, kdy přijde v těle zprávy spousta nesmyslných znaků.

V případě, že spustíte soubor z přílohy e-mailu, poznáte tento konkrétní virus jednoduše. Otevře se vám Poznámkový blok, ve kterém uvidíte nesmyslný text souboru:

Kam se zavrtá

Po spuštění se virus usídlí na řadě míst systému:

- Nakopíruje se do systémové složky Windows (třeba c:Windowssystem) jako taskmon.exe
- Do stejné složky uloží i vlastní DLL knihovnu shimgapi.dll (4096 bajtů)
- Nastaví se v registrech pro spouštění při startu systému
  HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionRun "TaskMon" = %SysDir%taskmon.exe
  nebo
  HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun "TaskMon" = %SysDir%taskmon.exe
- Začlení DLL do základního programu Explorer.exe pro obsluhu pracovní plochy a práci se složkami:
  HKEY_CLASSES_ROOTCLSID{E6FB5E20-DE35-11CF-9C87-00AA005127ED}InProcServer32 "(Default)" = %SysDir%shimgapi.dll
- Nakopíruje se do sdílené složky programu Kazaa (c:Program FilesKaZaAMy Shared Folder) jako následující soubory se spustitelnou příponou (pif, scr, bat nebo exe):
  - nuke2004
  - office_crack
  - rootkitXP
  - strip-girl-2.0bdcom_patches
  - activation_crack
  - icq2004-final
  - winamp

Čím škodí

Červ obsahuje dvě varianty zákeřného kódu. Jednou je útok na webovou stránku www.sco.com, kterou chce od 1. února zahltit požadavky na titulní stranu.

Druhá část, o kterou se stará DLL knihovna, je otevření TCP portů 3127 až 3198. Na těchto portech pak červ poslouchá požadavkům s různým využitím, může například přeposílat poštu pro spammery nebo krýt připojení útočníka k jinému serveru. Jednou z variant je také stažení připojeného souboru a jeho spuštění. Možnosti jsou tedy skutečně bohaté.

Veškerou činnost červ ukončí k 12. únoru, neodinstaluje se ale a stále zůstane otevřený pro útočníka.

Jak se šíří

Virus obsahuje vestavěné SMTP a DNS jádro. Není tedy závislý na poštovním serveru a nevyžaduje ani nastavené DNS servery v počítači.

E-mailové adresy získává ze všech souborů s příponami: wab, adb, tbb, dbx, asp, php, sht, htm a txt. Záběr je tedy úctyhodný a vyrovnávací paměť internetového prohlížeče na disku je pro něj vítaným soustem. Vir navíc ještě vygeneruje další e-mailové adresy na základě pár desítek křestních jmen a domény z nalezené adresy. Následně se pokusí odhadnout mailový server přidáním mx., mail., smtp., mx1., mxs., mail1., relay., nebo ns. před doménu odesílatele.

Jak se ho zbavím

Pokud si netroufáte na ruční odstranění, můžete využít automatické odstraňovače od Network Associates, F-Secure nebo Pandy (odstraňovačů je dnes již více, ale předpokládám, že chcete červa odstranit, ne sbírat všechny varianty téhož) .

- Ruční postup odstraňování je protikladem infekce. Tedy musíte v registrech smazat klíče:
  HKEY_CLASSES_ROOTCLSID{E6FB5E20-DE35-11CF-9C87-00AA005127ED}InProcServer32 "(Default)" = %SysDir%shimgapi.dll
  a
  HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionRun "TaskMon" = %SysDir%taskmon.exe
  případně
  HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun "TaskMon" = %SysDir%taskmon.exe
- Restartujte počítač, aby se soubory přestaly používat.
- Smažte v systémové složce soubor taskmon.exe a shimgapi.dll.
- Smažte vygenerované soubory ve sdílené složce Kazaa

Poslední bod je pak preventivní – napište na tabuli padesátkrát *„nebudu spouštět podezřelé přílohy z e-mailů!“*.

Zdroj: www.zive.cz