Mediálně známé kauzy uplynulého roku

Igor Glücksmann
ALWIL Software

Invex, říjen 2006

Mediálně známé kauzy uplynulého roku

- „Sony rootkit“
- „WMF exploit“

- Win32:Polip
- RFID virus

„Sony rootkit“

- **Rootkit**: program, který skrývá svou přítomnost před uživatelem, jinými programy, operačním systémem
  - DOS: „stealth“ viry
  - zachytávání systémových funkcí, modifikace systémových volání
  - hotové moduly/knihovny, které autor škodlivého kódu může použít pro skrytí svého výtvoru

„Sony rootkit“

- 31. října 2005, Mark Russinovich:

  Sony, Rootkits and Digital Rights Management Gone Too Far
- autor nástrojů File Monitor, Registry Monitor, Process Explorer, Rootkit Revealer…
- objevil na svém počítači:
  - skryté soubory *C:\Windows\system32\drivers\sys**
  - skryté soubory *C:\Windows\system32\$sys$filesystem**
  - skryté klíče *HKLM\System\ControlSet???\Services\sys**
  - …

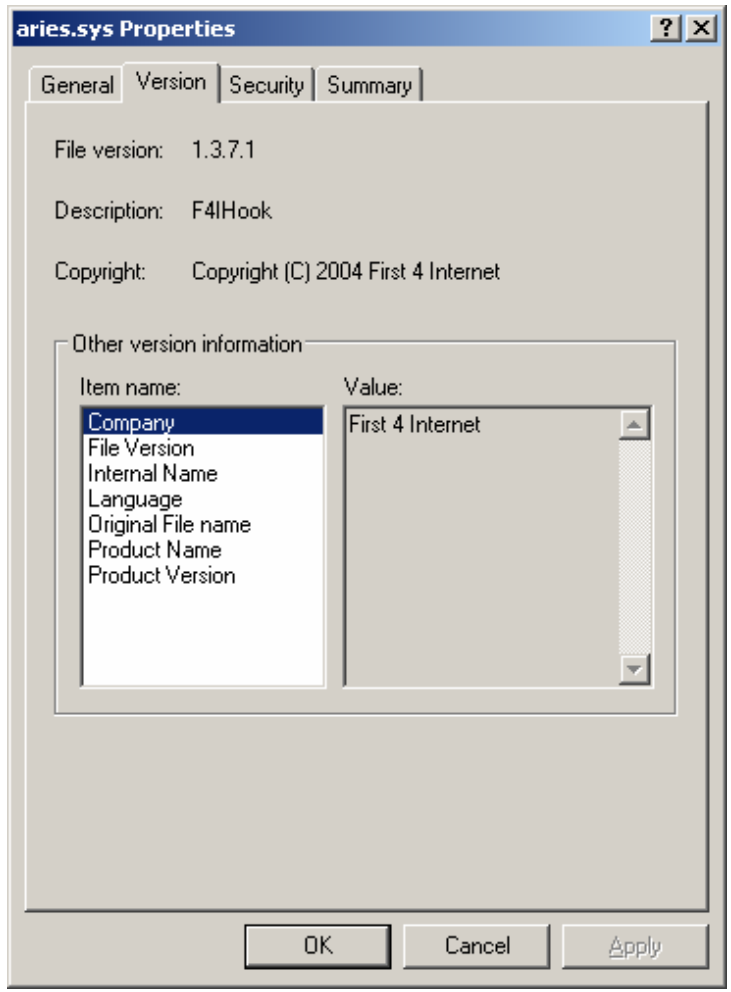
  ➔ *aries.sys* driver

  - skrývá všechny soubory, adresáře, procesy a klíče začínající na **sys**

„Sony rootkit“

- skryté soubory z adresáře *C:\Windows\system32\$sys$filesystem* – korektně vyplněné vlastnosti souboru (VersionInfo)
  - společnost: First 4 Internet
  - www.first4internet.com: vývoj DRM nástrojů, např. pro Sony

  ➔ Sony BMG: Van Zant brothers - Get Right with the Man
- automatická instalace při přehrání hudebního CD v počítači, „obtížná“ deinstalace
- brání „ripování“ CD



„Sony rootkit“

- následovaly více či méně použitelné odinstalační programy, výměna chráněných CD za nechráněná, soudní spory
- Thomas Hesse: "Většina lidí nechápe, co rootkit je, tak proč by se o ně měli starat?“
- http://en.wikipedia.org/wiki/2005_Sony_CD_copy_protection_controversy
- http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html

- 10. listopadu 2005 - první malware využívající tohoto rootkitu (%SysDir%\$sys$drv.exe): **Backdoor - Breplibot.C**

- firma F-Secure kontaktovala Sony ohledně rookitu již o několik týdnů dříve

„Sony rootkit“

- Skrývání / rootkity v dalších aplikacích
  - Symantec SystemWorks - Recycle Bin
  - Kaspersky AV - NTFS streams
  - Daemon Tools / Alcohol (DRM vs anti-DRM)

„WMF Exploit“

- 27. prosince 2005 - objeven bezpečnostní problém ve zpracování WMF souborů

- týkající se všech verzí Windows od 3.1, plně záplatovaných
- „0day exploit“ – instalace různých škodlivých programů

„WMF Exploit“

- WMF soubor
  - Windows Metafile: grafický formát
  - posloupnost příkazů (volání funkcí) Windows GDI
  - funkce „SetAbortProc“ umožňuje nastavit „callback“ funkci (AbortProc), kterou systém periodicky volá a dává tím rodičovské aplikaci možnost přerušit zpracování obrázku (původně jako možnost zrušení naplánovaného tisku)
  - tuto funkci může ovšem zaregistrovat i speciálně upravený soubor – sám do sebe – a tím vyvolat připravený kód
  - v nejnovějších verzích Windows jsou WMF soubory asociovány na nějaký prohlížeč (Windows Picture and Fax Viewer)

„WMF Exploit“

- nejedná se o klasickou chybu (jako byla např. MS04-028 – zpracování JPEG souborů), ale o chybu návrhu API
  - API z Windows 2.x/3.x
- problém přítomen na všech verzích Windows, dokonce snad i na Wine

- objevily se i konspirační teorie (Steve Gibson) 

„WMF Exploit“

- Microsoft oznámil, že záplata bude uvolněna 10. ledna
- 31.12. uvolnil Ilfak Guilfanov vlastní záplatu
  - včetně zdrojových kódů, doporučena bezpečnostními organizacemi
  - potlačení možnosti volat funkci SetAbortProc při zpracování WMF souboru (změna ve funkci Escape, volané z PlayMetaFileRecord)
  - tj. znemožnění registrace AbortProc z WMF souboru
- Microsoft nakonec vydal záplatu 5. ledna 2006

- http://en.wikipedia.org/wiki/Windows_Metafile_vulnerability

Win32:Polip

- 19. dubna 2006 - společnost Dr.Web oznámila, že již více než měsíc se po P2P sítích šíří nový nebezpečný polymorfní virus, který nikdo jiný není schopen detekovat
- infikuje soubory, šíří se po P2P sítích

- Win32:Polipos
- později přejmenován na Win32:Polip

Win32:Polip

- skutečně se objevil nový polymorfní virus
- poměrně silný polymorfismus (náhodné přiřazení registrů, cykly, operace s pamětí, volání procedur s různými volacími konvencemi a operacemi na předaných parametrech, …)
- pozoruhodně dobře napsaný (důkladná kontrola operačního systému a použití specifických částí kódu pro daný systém, kontrola CPU, podporuje import forwarding, terminal services, synchronizace vláken, …)
- při infekci instalačních programů spouštění přesné původní kopie
- silný šifrovací algoritmus – (významně) modifikovaný XTEA
- kompresní algoritmus JCALG1

- šíření po Gnutella sítích

Win32:Polip

- detekce ve skutečnosti není příliš komplikovaná

- jiné antivirové společnosti o tomto viru vůbec nevěděly
- po oznámení byla většina antivirů schopna tento virus detekovat do několika málo dnů

- žádná velká epidemie se nekonala

RFID virus

- Březen 2006: M. Rieback, P. Simpson, B. Crispo, A. Tanenbaum (Vrije Universiteit Amsterdam):

  Is Your Cat Infected with a Computer Virus?

- RFID: Radio Frequency Identification
- “RFID tags” – malé počítače, napájené indukčně pomocí čtečky
- některé umožňují pouze čtení, jiné i zápis
- označení zboží v obchodech, čipy pro domácí zvířata, bezkontaktní „klíče“, pasy
- diskutabilní z hlediska bezpečnosti a ochrany soukromí

RFID virus

- „čtečka“ RFID je připojena k počítači, který zpracovává přijatá data
  - obslužný software
  - připojení k databázi
  - připojení k lokální síti

- software obsahuje chyby; potencionálně zneužitelné pomocí speciálně upravených vstupních dat (= RFID tagu)
  - přetečení bufferu
  - neošetřené databázové dotazy
  - odkaz na připravený (škodlivý) objekt / URL

RFID virus

- speciálně upravený RFID tag tady může na obslužném počítači spustit připravený kód nebo modifikovat obsah připojené databáze
- může pak také upravit program/databázi tak, aby se stejný „exploit“ zapisoval do dalších RFID tagů, se kterými přijde do kontaktu

  ➔ replikující se virus

- velikost paměti tagů, možnost zápisu i rozšíření RFID technologie do budoucna poroste
- http://www.rfidvirus.org

  - příklad replikujícího se viru