Analýza malware v paměti počítače

Vašek Lorenc

Europen 2013

Doporučený software

- Oracle VirtualBox
  - plus dostatek místa na disku (cca 12 GB)
- Volatility Framework
- Mandiant Redline
- Unixové utility
  - strings, foremost
- Textový editor na poznámky
- Nástroje na analýzu dokumentů, JS, ...

Průběh tutoriálu

- Úvod do problematiky, zprovoznění VM
  - Nebude to o assembleru
  - Ani o (de)obfuskaci malware
- Hledání „podivností“ v systému
  - Malware, rootkity, Windows
- Jednoduchá forenzní analýza
  - Nácvik hledání zdroje infekce
- **To vše na příkladech (funkční malware)!**

A jedna otázka...

- Jak dlouho zhruba trvá, než denně aktualizovaný antivirus najde virus/exploit, kterým byl počítač infikován?
  - okamžitá detekce, žádné čekání!
  - 1 den
  - 2 dny
  - týden
  - měsíc

Malý kvíz na úvod/1

- Který z následujících virů/malware používal sociální sítě pro své další šíření?
  - Torpig
  - Code Red
  - TwitterNET
  - Koobface

Malý kvíz na úvod/2

- Který z následujících programů využívají autoři APT malware pro přístup do napadených systémů?
  - Back Orifice
  - Poison Ivy
  - SpyEye
  - Phoenix

Malý kvíz na úvod/3

- V roce 2012 se objevil virus zaměřený na OS X a využívající zranitelností v Javě. Který?
  - SMSSend
  - Battery Doctor
  - JFake
  - Flashback

Malý kvíz na úvod/4

- Které z následujících systémových volání by pro svoji činnost mohl nejlépe využít *keylogger*?
  - POP
  - GetProcAddress
  - GetAsyncState
  - VirtualAllocEx

Malý kvíz na úvod/5

- Pokud by si chtěl malware zajistit spuštění i po restartu systému, pravděpodobně by využil:
  - HKCU\System\CurrentControlSet\Control\MediaProperties
  - %UserProfile%\ntuser.dat
  - HKLM\Software\Microsoft\Windows\CurrentVersion\Run
  - HKLM\SECURITY

Proč analyzovat paměť?

- **Je to zábava!**
- Součást zajištění důkazů při vyšetřování
  - Změna proti dřívějším doporučením a postupům
- Incident Response
  - Možnost sledovat chování útočníků, jejich nástroje, ...
- Technické zjednodušení problému reverzní analýzy
  - Není třeba umět assembler a chápat anti-RE triky
  - Často mnohem rychlejší nalazení důležitých indikátorů

Jak získat obraz paměti?

- Přímý přístup k HW
  - windd, fastdump, memoryze, ...
  - obraz hybernovaného systému (hiberfil.sys)
- Vzdálený přístup
  - Encase, Mandiant Intelligent Response, Access Data FTK, ...
- VMWare, VirtualBox, ...
  - často jednoduchá možnost získání paměti
  - `VirtualBox --dbg --startvm "MalwareVM"` (*a následně* `.pgmphystofile`)
- Komplikace
  - nepodporovaný OS (Linux, MacOS; 32bit/64bit)
  - swap

Volatility Framework

- Open Source nástroj
  - GPL licence
- Psaný v Pythonu
  - dostupný pro všechny možné platformy
  - možnosti automatizace, pluginy, ...
- Umožňuje analyzovat paměť mnoha systémů
  - Windows, Linux, MacOS, Android
  - 32/64-bitové varianty
- Příkazová řádka
- Spousta příkladů, oficiální školení, velmi populární, ...

Mandiant Redline

- Volně dostupný
  - Nikoliv open source
  - Pouze pod Windows (.NET)
- Sympatické uživatelské rozhraní
  - Dobře použitelné workflow
  - Snadné vyhledávání, timeline, řetězce
  - Hodnotící systém procesů (míra podezřelosti)
- Nevýhody
  - Analýza pouze Windows OS, horší detekce datových struktur

HBGary Responder Pro

- Velmi obtížná dostupnost
  - placená verze + „community-edition“ s obtížnou aktivací
  - Pouze pro Windows (.NET)
  - Horší stabilita
- Výborný nástroj pro analytiky
  - vizuální debugger, „Canvas“
  - „Digital DNA“ – výborný systém hodnocení rizik
- Možnost analyzovat i přímo binárky
- **Není součástí dnešního tutoriálu :(**

Responder Pro: DDNA

Digital DNA Sequence	Name	Process Name	Size	Severity	Weig
04 D3 C5 00 B4 EE 00 5A ...	syshost.exe	syshost.exe	114688		
00 5D 09 01 4D F2 00 B4 ...			9490432		
05 0E 3A 05 DD 33 05 73 ...	firetdi.sys	System	139264		
0F 20 22 00 66 09 03 1B ...	hippssa.dll		61440		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5D 09 00 5A 6A 01 1E ...	mso.dll		17330176		
00 5D 09 00 5A 6A 01 1E ...	mso.dll		17330176		
2A 80 AC 00 67 6C 00 66 ...	memorymod-pe-0x75350000-0x7539b000		307200		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		
00 5A 6A 00 67 6C 00 66 ...	shell32.dll		12886016		

Responder Pro: DDNA

Size	Severity	Weight
114688		61.9
9490432		39.8
139264		34.6
61440		32.5
12886016		29.8
12886016		29.8
17330176		28.6
17330176		28.6
307200		28.5
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1
12886016		27.1

Trait: B8 98
Description: Program appears to communicate over the network using TCP/IP.

Trait: C1 7C
Description: Program appears to communicate over the network using TCP/IP. It appears to use, check, or log the IP address of the remote connection point.

Trait: 1B 2A
Description: Program is reading the memory of another process. This is not typical to most programs and is usually only found in system utilities, debuggers, and hacking utilities.

Trait: DF 37
Description: Program uses web or ftp addresses and possibly URL's to access one or more sites on the Internet for downloading files or posting up data.

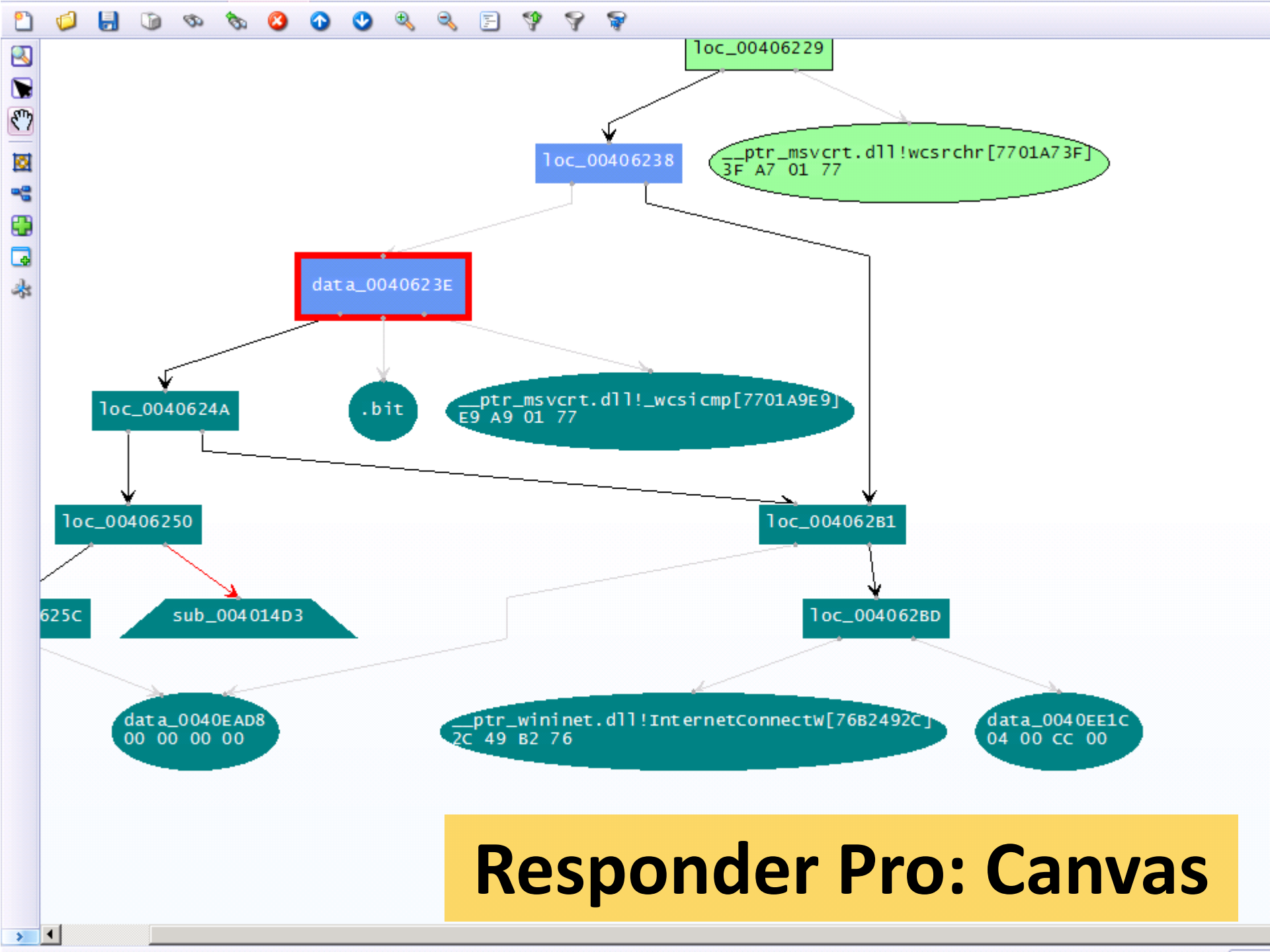
Trait: 35 99
Description: This module has the ability to manipulate process tokens and their privileges.

Trait: 85 56
Description: Program is deleting files using a shell command.

Trait: F6 E3
Description: Process may inject or write data into other processes.

Trait: 21 E3
Description: This module may attempt to shutdown or reboot the operating system.

Trait:
Description: This module appears to manually construct strings. This is highly suspicious.


loc_00406229
loc_00406238
__ptr_msvcrt.dll!wcsrchr[7701A73F]
3F A7 01 77
data_0040623E
loc_0040624A
.bit
__ptr_msvcrt.dll!_wcsicmp[7701A9E9]
E9 A9 01 77
loc_00406250
loc_004062B1
625C
sub_004014D3
loc_004062BD
data_0040EAD8
00 00 00 00
__ptr_wininet.dll!InternetConnectW[76B2492C]
2C 49 B2 76
data_0040EE1C
04 00 CC 00
Responder Pro: Canvas

Co budeme hledat?

- Komunikaci s C&C/RAT
- Skryté procesy
- „Process/DLL injection“
- Nestandardní/známé umístění binárek
- Nestandardní/známé mutexy
- Otevřené soubory/sockety
- Záznamy v registrech
- Historii příkazového řádku
- Alternate Data Streams
- Klíče, ...

Doporučený postup analýzy

- **Používejte Internet** (Google, VirusTotal, ...)
- **Nezapomeňte si dělat poznámky!**
- Co analyzujeme za systém (OS, verze, bitness)
- Síťová spojení (+ whois, atd.)
- Procesy (skryté, viditelné, podivné názvy, časy spuštění a ukončení, ...)
- Mutexy (+ soubory)
- Řetězce (URI, %s, %d, domény, jména procesů, user-agent, …)
- ...
- **Závěrečný report**

Volatility Framework

Nápověda

```
vol.py –h / vol.py plugin –h / vol.py příkaz --info
```

Informace o souboru s pamětí počítače

```
vol.py –f image.file imageinfo
```

Příklad volání jednotlivých modulů Volatility

```
vol.py -f image.file --profile=profile příkaz
   export VOLATILITY_LOCATION=image.file
   export VOLATILITY_PROFILE=WinXPSP3x86
```

Volatility Framework – stručný přehled

- psxview (vyhledávání skrytých procesů)
- apihooks
- driverscan
- ssdt / driverirp / idt
- connections / connscan (WinXP, seznam otevřených spojení)
- netscan (Win7, vyhledávání otevřených síťových spojení/socketů)
- pslist / psscan (výpis procesů získaných přes WinAPI vs. přes EPROCESS bloky)
- malfind / ldrmodules (hledání vloženého kódu + dump / detekce DLL)
- hivelist (nalezení a vypsání složek s registry) / hashdump
- handles / dlllist / filescan (seznam souborů / DLL files / FILE_OBJECT handles)
- cmdscan / consoles (historie cmd.exe / console buffer)
- shimcache (application compatibility info)
- memdump / procmemdump / procexedump

Analýza: xp-infected.vmem

- Doporučené nástroje
  - Redline, Volatility

Analýza: zeus.vmem

- Doporučené nástroje
  - Redline, Volatility

Analýza: zeus2x4.vmem

- Doporučené nástroje
  - Redline, Volatility

Forenzní analýza operační paměti?

- Foremost
  - Nástroj na získávání souborů známých typů z obrazů disku/paměti
- Strings
  - Řetězce v paměti mohou být uloženy v různých kódováních (UTF-8, UTF-16)

Analýza: bob.vmem

- Doporučené nástroje
  - Redline, Volatility, Foremost, Strings

Analýza: homework.vmem

- Doporučené nástroje
  - Redline, Volatility, Foremost, Strings

Odkazy, otázky, odpovědi...

- Zajímavé zdroje čtení kolem (analýzy) malware
  - http://www.kernelmode.info/forum/viewtopic.php?f=16&t=2680
  - http://contagiodump.blogspot.com/
- Twitter!

Děkuji za účast i za vaši pozornost!

email: vaclav.lorenc@gmail.com

twitter: @valorcz