ANALÝZA MALWARE V PAMĚTI POČÍTAČE

Vašek Lorenc

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 LABÁKU

- Úvod do problematiky
  - 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)!**

ANKETA!

- Setkali jste se někdy s napadeným počítačem/serverem?
- Zdrojem nákazy byl:
  - Obecný malware
  - Malware/kód cílený na vaši organizaci
  - Phishing/dokument
  - Zranitelnost serveru/aplikace
  - USB virus...

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

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
- **Není součástí dnešního labáku :(**

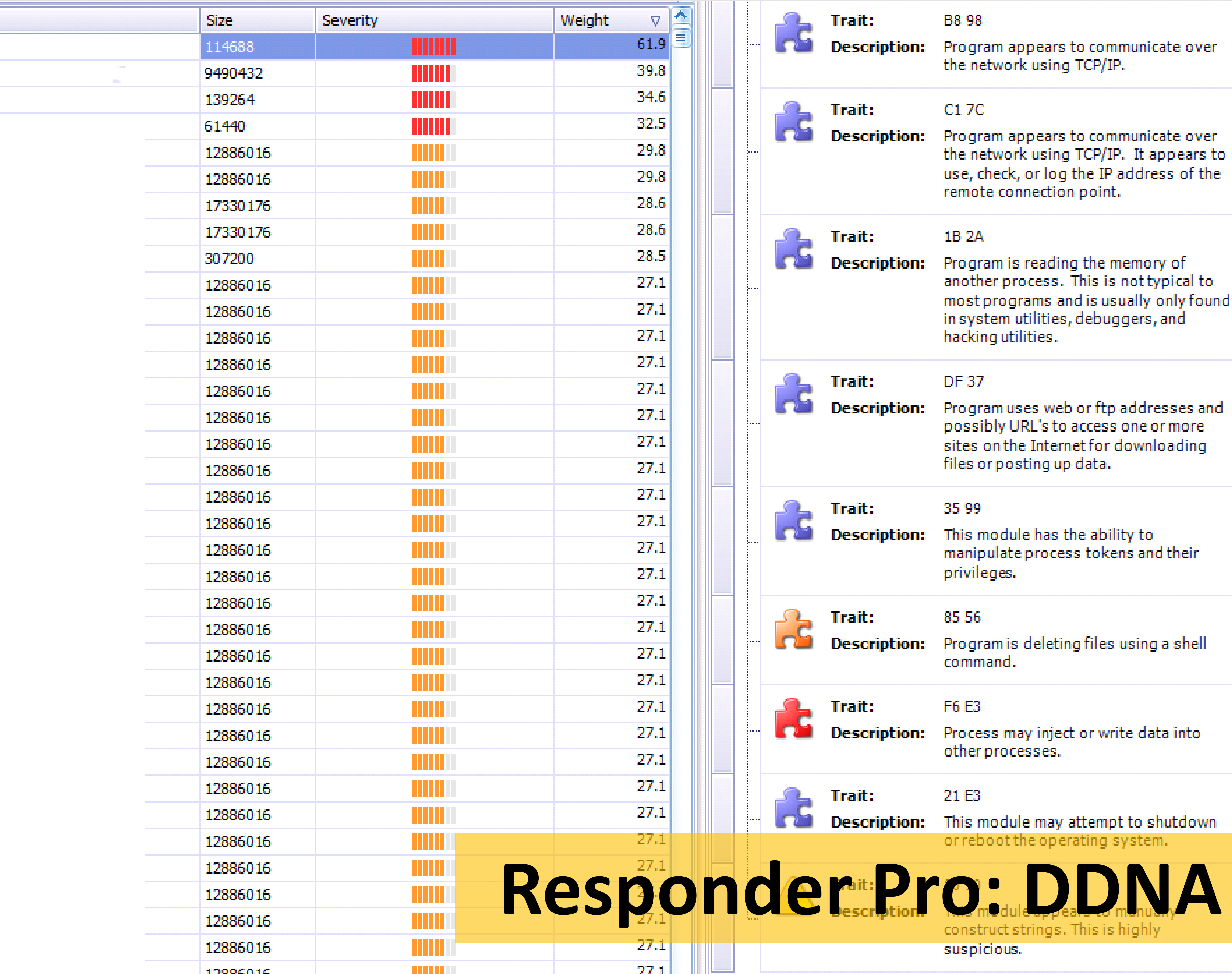
HBGARY RESPONDER PRO

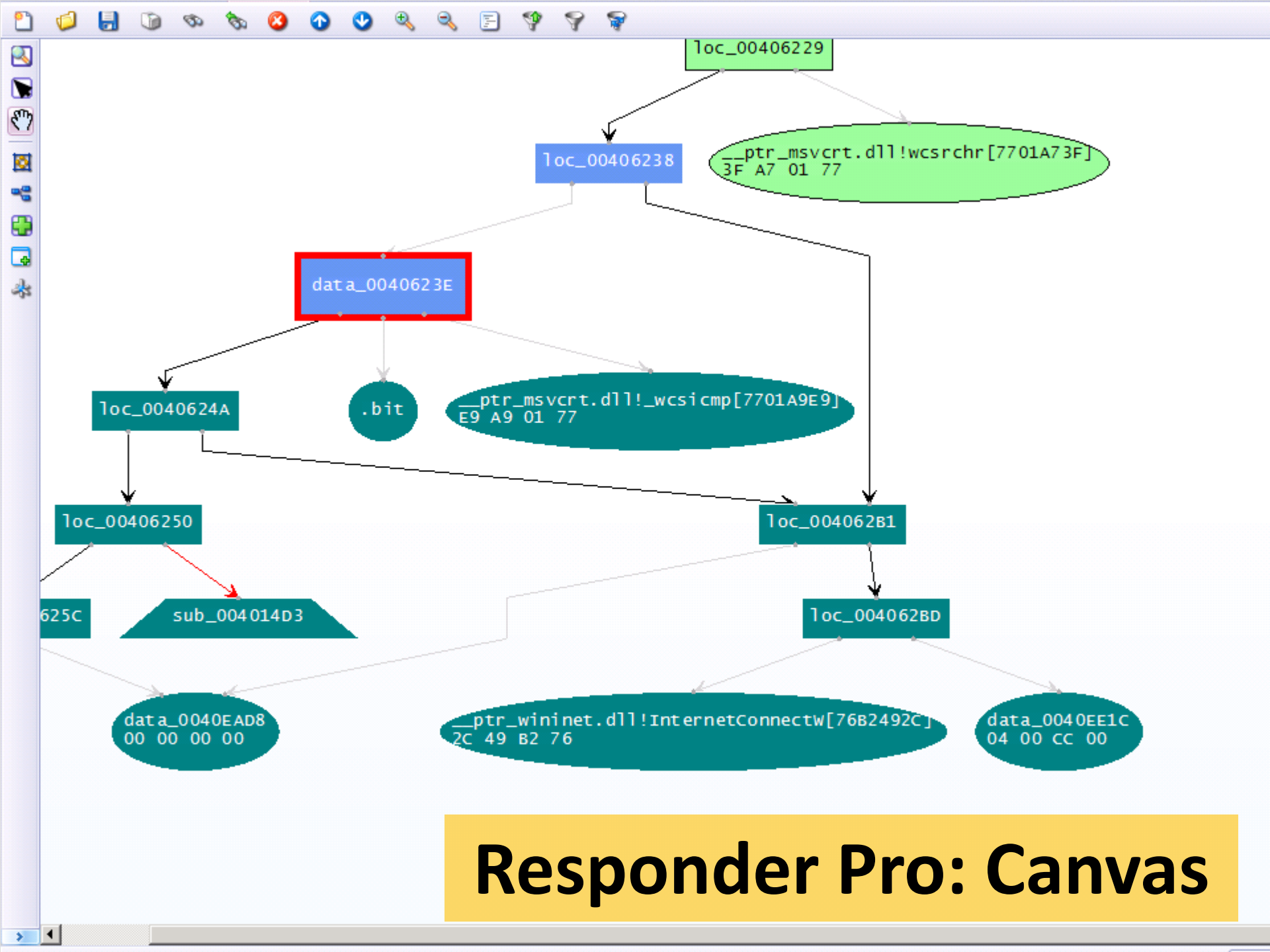
- Velmi obtížná dostupnost
  - placená verze + „community-edition“ s obtížnou aktivací
  - Pouze pro Windows (.NET)
  - Horší stabilita
- Výborný nástroj pro analytiky
  - vizuální debugger, „Canvas“
  - „Digital DNA“ – výborný systém hodnocení rizik
- Možnost analyzovat i přímo binárky
- **Není součástí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

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		

Responder Pro: DDNA





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
- 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 – PŘÍKAZY

- 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