Malware Analysis & Prevention

Candid Wüest

Vice President Cyber Protection Research @ Acronis

@myLaocoon

Candid Wüest

- Vice president of Cyber Protection Research @ Acronis
- 17 years @ Symantec's global Security Response
- Prior to that IBM Research Lab Rüschlikon
- ETH Zürich, multiple patents, certificates, book, …
- Organizer AREA41 conference, BSidesZH, Defcon Switzerland,…
- Likes "breaking" things ;-)

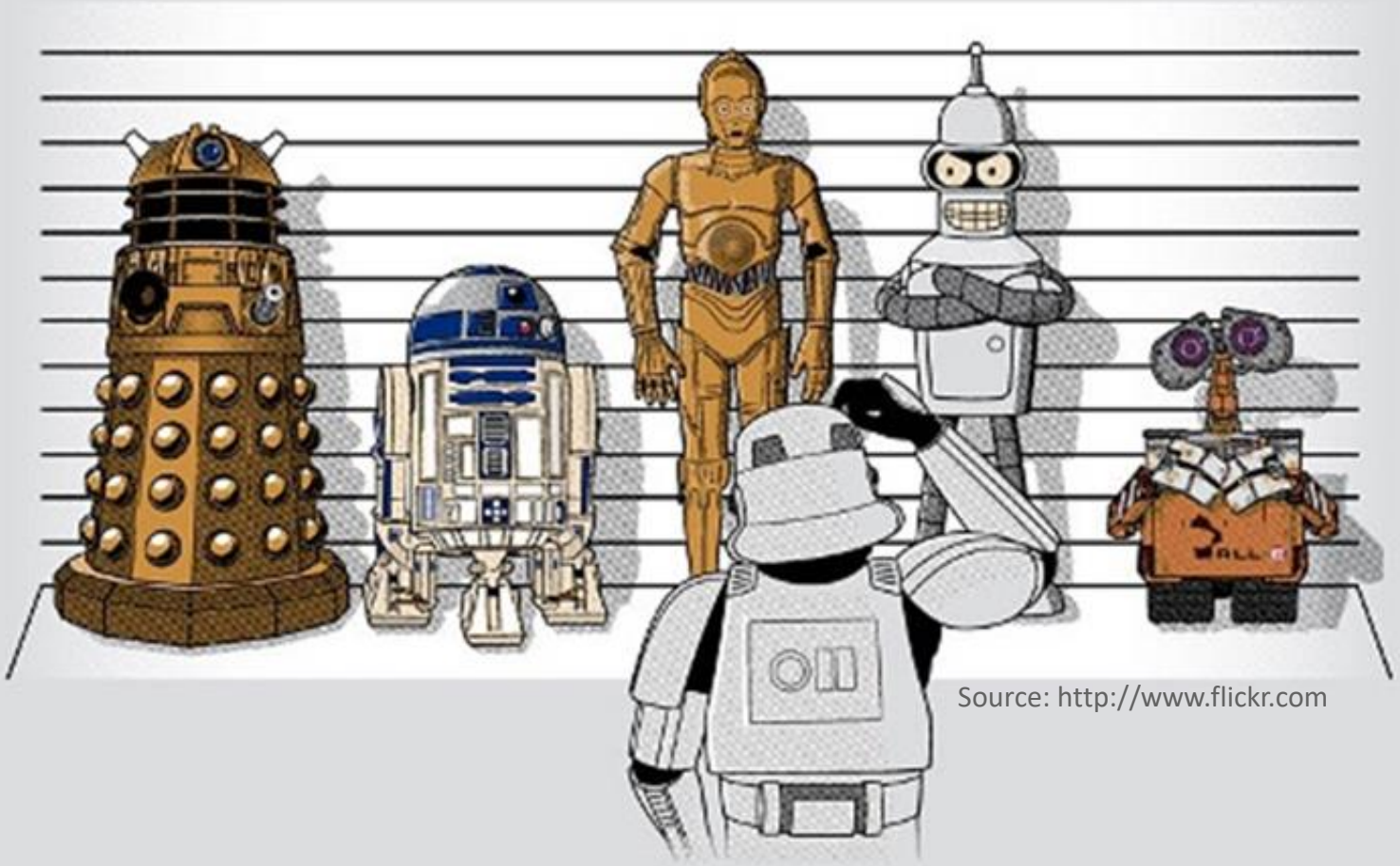
Agenda

- **Threat analysis**
  - Blackbox, whitebox, clustering
- **Prevention methods**
  - Signatures, behavior, hardening
- **Q&A**


CYBER
AI
BACKDOOR
ATTACK
TROJAN
APT
PHISHING
SOC
IOT
SSL
SECURITY
HACKER
EXPLOIT
INTRUDER
TRUST
DEFENSE
COMPUTER
PASSWORD
BUG
VPN
HEX
TLS
SSH
POWERSHELL
ZERO TRUST
XSS
MALWARE
VIRUS
STATE
LATERAL
TARGETED
BREACH
SQL INJECTION
WHITEHAT
CSRF
2FA
CODE
DDOS
VBS
DEEP
BINARY
NATION
SCAM
SPAM
MOBILE
INTERNET
CRACKER
ONLINE
CLOUD
CHAIN
IOC
ML
DAY
DNS
DATA
EDR
WEB
DLP
ICDX
PROXY
STEALING
INFECTION
CANDID METASPLOIT
MONITORING
ENCRYPTION
SOPHISTICATED
CRYPTOJACKING
FORMJACKING
VULNERABILITY
FIREWALL
ERROR
GATEWAY
ANALYSIS
LINUX
BLACKHAT
HONEYPOT
ALERT

Look for a sample that we can analyse

- Customers, collections, C&C servers, traps, crawlers, heuristics,…
- Memory dump, registry, BIOS, device firmware, encrypted?,...



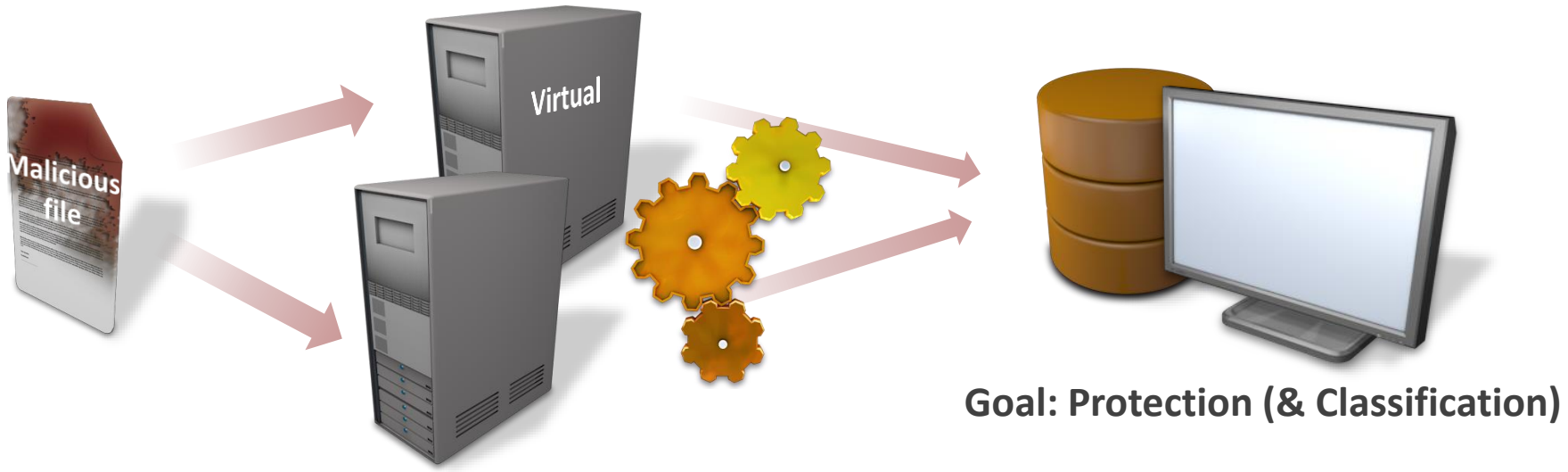
Source: http://www.flickr.com

☺ Is no the correct answer to this question?

Starting the analysis

Automated analysis done, to get first impression

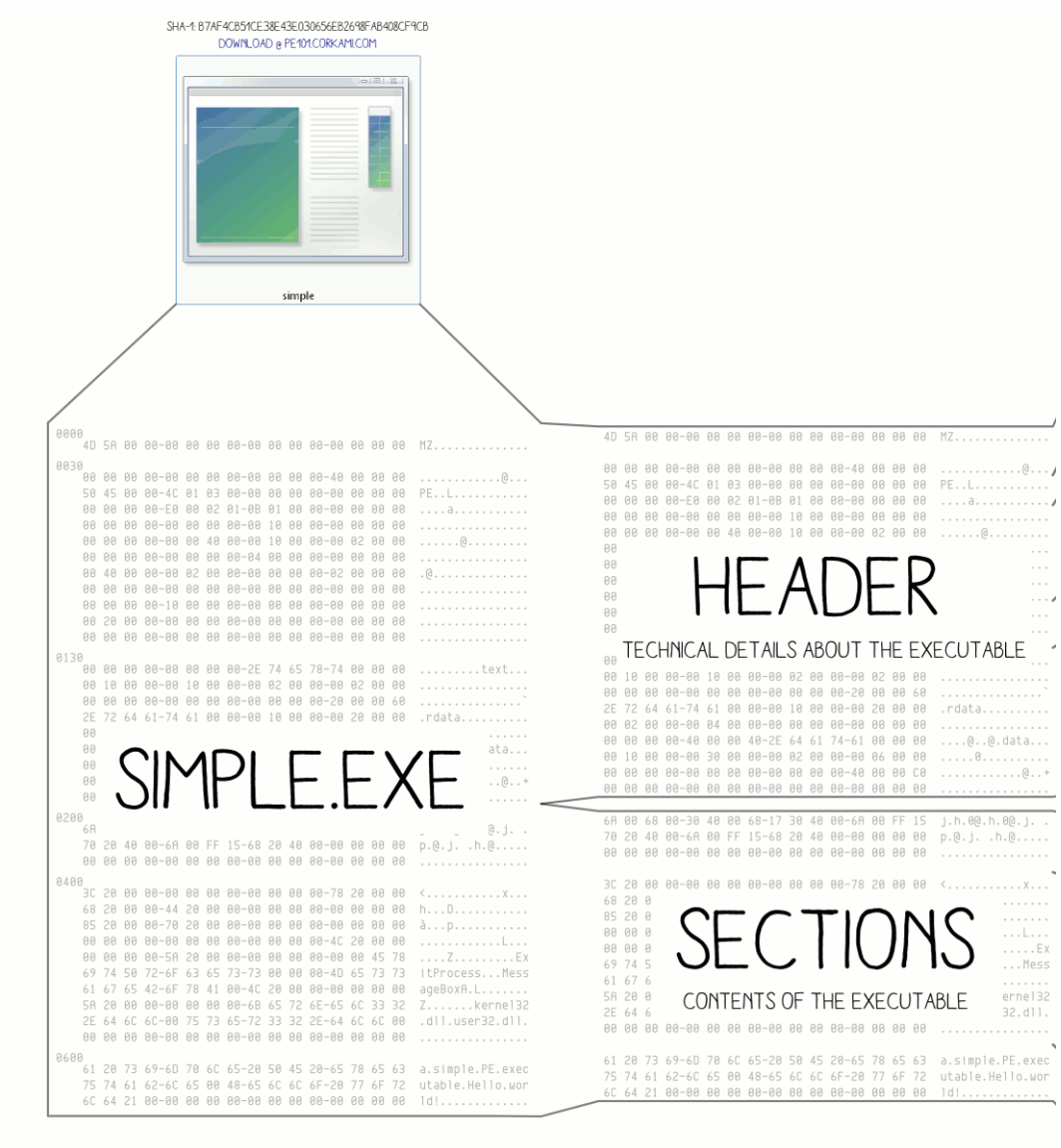
- Do we know or detect it already? (~400K new malware / day)
- Internal Sandboxes, clustering, etc.
- Impression from online scanners (VirusTotal.com, etc.)
  - But samples try to prevent automated analysis (~15% detect VM)



☺ A clear conscience is usually the sign of a bad memory.

Portable Executable Format

ANGE ALBERTINI
http://www.corkami.com

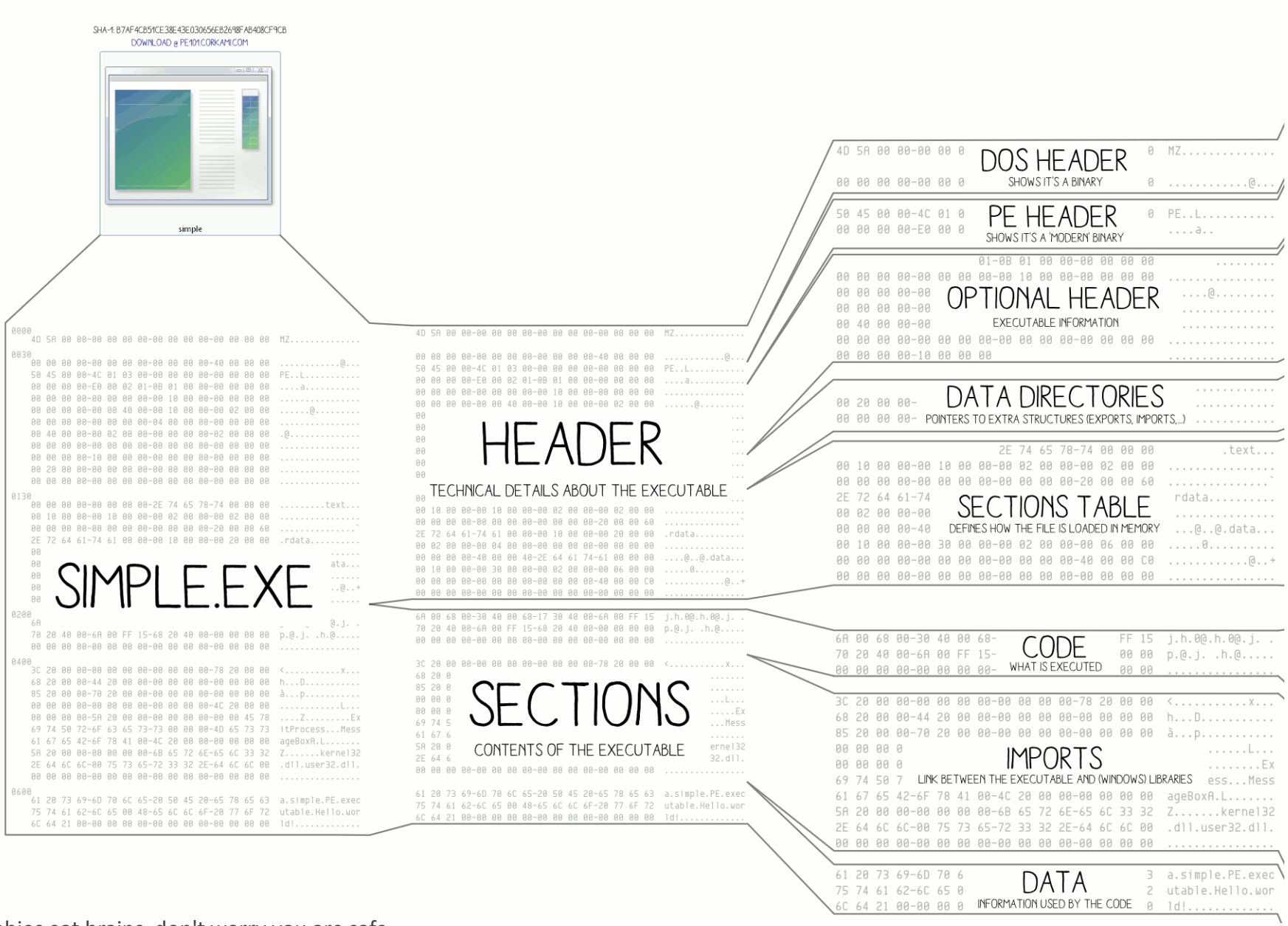


HexEditor - Example: cmd.exe

```
00000000: 4D5A9000 03000000 04000000 FFFF0000  MZ..........ÿÿ..
00000010: B8000000 00000000 40000000 00000000  ¸.......@.......
00000020: 00000000 00000000 00000000 00000000  ................
00000030: 00000000 00000000 00000000 E8000000  ............è...
00000040: 0E1FBA0E 00B409CD 21B8014C CD215468  ..º..´.Í!¸.LÍ!Th
00000050: 69732070 726F6772 616D2063 616E6E6F  is program canno
00000060: 74206265 2072756E 20696E20 444F5320  t be run in DOS
00000070: 6D6F6465 2E0D0D0A 24000000 00000000  mode....$.......
00000080: DE4E92B9 9A2FFCEA 9A2FFCEA 9A2FFCEA  ÞN'¹|/üê|/üê|/üê
00000090: 935778EA 982FFCEA 935769EA 9C2FFCEA  |Wxê|/üê|Wiê|/üê
000000A0: 9A2FFDEA 672FFCEA 93576FEA 932FFCEA  |/ýêg/üê|Woê|/üê
000000B0: 93577FEA A32FFCEA 935768EA 9B2FFCEA  |W.êf/üê|Whê|/üê
000000C0: 93576DEA 9B2FFCEA 52696368 9A2FFCEA  |Wmê|/üêRich|/üê
000000D0: 00000000 00000000 00000000 00000000  ................
000000E0: 00000000 00000000 50450000 4C010400  ........PE..L...
000000F0: 2B8EE74C 00000000 00000000 E0000201  +|çL........à...
00000100: 0B010900 002E0200 006C0200 00000000  ..........l.....
00000110: 9A820000 00100000 00200200 0000D04A  ||.......  ....ÐJ
00000120: 00100000 00020000 06000100 06000100  ................
00000130: 06000100 00000000 00C00400 00040000  ..........À.....
00000140: 3D7B0500 03004081 00001000 00D00F00  ={....@  .....Ð..
00000150: 00001000 00100000 00000000 10000000  ................
00000160: 00000000 00000000 D0270200 64000000  ........Ð'..d...
00000170: 00100400 50840000 00000000 00000000  ....P|..........
00000180: 00000000 00000000 00A00400 301B0000  ............0...
00000190: C43B0200 38000000 00000000 00000000  Ä;..8...........
000001A0: 00000000 00000000 00000000 00000000  ................
000001B0: A0BD0100 40000000 80020000 94000000   ½..@...|...|...
000001C0: 00100000 A4030000 FC240200 A0000000  ....¤...ü$......
000001D0: 00000000 00000000 00000000 00000000  ................
000001E0: 2E746578 74000000 202C0200 00100000  .text... ,......
000001F0: 002E0200 00040000 00000000 00000000  ................
00000200: 00000000 20000060 2E646174 61000000  .... ..`.data...
00000210: 30C90100 00400200 00CA0100 00320200  0É...@...Ê...2..
00000220: 00000000 00000000 00000000 400000C0  ............@..À
00000230: 2E727372 63000000 50840000 00100400  .rsrc...P|......
00000240: 00860000 00FC0300 00000000 00000000  .|...ü..........
00000250: 00000000 40000040 2E72656C 6F630000  ....@..@.reloc..
00000260: 301B0000 00A00400 001C0000 00820400  0.....  .....|..
00000270: 00000000 00000000 00000000 40000042  ............@..B
00000280: E0B8E74C 38000000 6EB9E74C 43000000  à¸çL8...n¹çLC...
00000290: EFB8E74C 4D000200 6EB9E74C 43000000  ï¸çLM...n¹çLC...
000002A0: 31B7E74C 5A000000 39BAE74C 84000000  1·çLZ...9ºçL|...
000002B0: 00000000 00000000 6D737663 72742E64  ........msvcrt.d
000002C0: 6C6C006E 74646C6C 2E646C6C 004B4552  ll.ntdll.dll.KER
```

☺ zombies eat brains, don't worry you are safe

Portable Executable Format



☺ zombies eat brains, don't worry you are safe

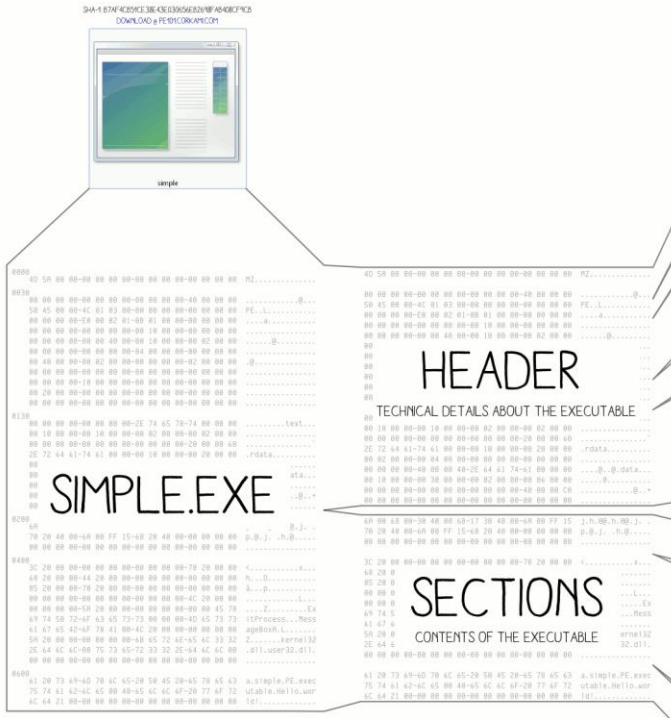
Portable Executable Format

ANGE ALBERTINI
http://www.corkami.com

PE 101 a windows executable walk-through

ANGE ALBERTINI
CORKAMI.COM

DISSECTED PE



HEXADECIMAL DUMP	ASCII DUMP	FIELDS	VALUES	EXPLANATION
4D 5A 00 00-00 00 00 00-00 00 00 00-00 00 00 00	MZ..............			
Offset:0x30 00 00 00 00-00 00 00 00-00 00 00 00-40 00 00 00	............@...	e_magic	'MZ'	CONSTANT SIGNATURE
		e_lfanew	0x40	OFFSET OF THE PE HEADER 1
Offset:0x40 50 45 00 00-4C 01 03 00-00 00 00 00-00 00 00 00	PE..L...........	Signature	'PE', 0, 0	CONSTANT SIGNATURE
00 00 00 00-E0 00 02 01...	....a...	Machine	0x14c [intel 386]	PROCESSOR: ARM/MIPS/INTEL/...
		NumberOfSections	3	NUMBER OF SECTIONS 2
		SizeOfOptionalHeader	0xe0	RELATIVE OFFSET OF THE SECTION TABLE 2
		Characteristics	0x102 [32b EXE]	EXE/DLL/...
Offset:0x58 ...0B 01 00 00-00 00 00 00	....	Magic	0x10b [32b]	32 BITS/64 BITS
00 00 00 00-00 00 00 00-00 10 00 00-00 00 00 00	....	AddressOfEntryPoint	0x1000	WHERE EXECUTION STARTS 5
00 00 00 00-00 00 40 00-00 10 00 00-00 02 00 00	......@.........	ImageBase	0x400000	ADDRESS WHERE THE FILE SHOULD BE MAPPED IN MEMORY 3
00 00 00 00-00 00 00 00-04 00 00 00-00 00 00 00	....	SectionAlignment	0x1000	WHERE SECTIONS SHOULD START IN MEMORY 2
00 40 00 00-00 02 00 00-00 00 00 00-02 00 00 00	.@..............	FileAlignment	0x200	WHERE SECTIONS SHOULD START ON FILE 2
00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00	....	MajorSubsystemVersion	4 [NT 4 or later]	REQUIRED VERSION OF WINDOWS
00 00 00 00-10 00 00 00...	....	SizeOfImage	0x4000	TOTAL MEMORY SPACE REQUIRED
		SizeOfHeaders	0x200	TOTAL SIZE OF THE HEADERS 3
		Subsystem	2 [GUI]	DRIVER/GRAPHICAL/COMMAND LINE/...
		NumberOfRvaAndSizes	16	NUMBER OF DATA DIRECTORIES 4
...00 00 00 00-00 00 00 00	....			
00 20 00 00-00 00 00 00-00 00 00 00-00 00 00 00	....	ImportsVA	0x2000	RVA* OF THE IMPORTS 4
00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00	....			

Offset:0x130

2E 74 65 78-74 00 00 00	.text...
00 10 00 00-00 10 00 00-00 02 00 00-00 02 00 00	....
00 00 00 00-00 00 00 00-00 00 00 00-20 00 00 60	....`
2E 72 64 61-74 61 00 00-00 10 00 00-00 20 00 00	.rdata..... ....
00 02 00 00-00 04 00 00-00 00 00 00-00 00 00 00	....
00 00 00 00-40 00 00 40-2E 64 61 74-61 00 00 00	....@..@.data...
00 10 00 00-00 30 00 00-00 02 00 00-00 06 00 00	.....0..........
00 00 00 00-00 00 00 00-00 00 00 00-40 00 00 C0	............@..*

SECTIONS TABLE

NAME	VIRTUALSIZE (RVA*)	VIRTUALADDRESS (RVA*)	SIZEOFRAWDATA (PHYSICAL SIZE)	POINTERTORAWDATA (PHYSICAL OFFSET)	CHARACTERISTICS
.text	0x1000	0x1000	0x200	0x200	CODE EXECUTE READ
.rdata	0x1000	0x2000	0x200	0x400	INITIALIZED READ
.data	0x1000	0x3000	0x200	0x600	DATA READ WRITE

FOR EACH SECTION, A SIZEOFRAWDATA SIZED BLOCK IS READ FROM THE FILE AT POINTERTORAWDATA OFFSET.
IT WILL BE LOADED IN MEMORY AT ADDRESS IMAGEBASE + VIRTUALADDRESS IN A VIRTUALSIZE SIZED BLOCK, WITH SPECIFIC CHARACTERISTICS.

Offset:0x200/RVA:0x401000

6A 00 68 00-30 40 00 68-17 30 40 00-6A 00 FF 15	j.h.0@.h.0@.j. .
70 20 40 00-6A 00 FF 15-68 20 40 00	p.@.j. .h.@.

X86 ASSEMBLY

```
push 0
push 0x403000
push 0x403017
push 0
call [0x402070]      ->MessageBox(0, "Hello World!","a simple PE executable", 0);
push 0
call [0x402068]      ->ExitProcess(0);
```

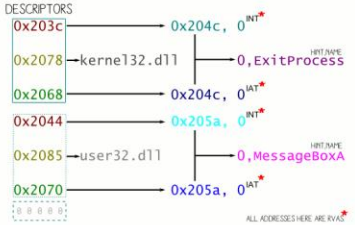
EQUIVALENT C CODE

Offset:0x400/RVA:0x402000

3C 20 00 00-00 00 00 00-00 00 00 00-78 20 00 00	<...........x...
68 20 00 00-44 20 00 00-00 00 00 00-00 00 00 00	h...D...........
85 20 00 00-70 20 00 00-00 00 00 00-00 00 00 00	à...p...........
00 00 00 00-00 00 00 00-00 00 00 00-4C 20 00 00	............L...
00 00 00 00-5A 20 00 00-00 00 00 00-00 00 45 78	....Z.........Ex
69 74 50 72-6F 63 65 73-73 00 00 00-4D 65 73 73	itProcess...Mess
61 67 65 42-6F 78 41 00-4C 20 00 00-00 00 00 00	ageBoxA.L.......
5A 20 00 00-00 00 00 00-6B 65 72 6E-65 6C 33 32	Z.......kernel32
2E 64 6C 6C-00 75 73 65-72 33 32 2E-64 6C 6C 00	.dll.user32.dll.

IMPORTS STRUCTURES

DESCRIPTORS



CONSEQUENCES

AFTER LOADING,
0X402068 WILL POINT TO KERNEL32.DLL'S EXITPROCESS
0X402070 WILL POINT TO USER32.DLL'S MESSAGEBOXA

Offset:0x600/RVA:0x403000

61 20 73 69-6D 70 6C 65-20 50 45 20-65 78 65 63	a.simple.PE.exec
75 74 61 62-6C 65 00 48-65 6C 6C 6F-20 77 6F 72	utable.Hello.wor
6C 64 21 00	ld!.

STRINGS

```
a simple PE executable\0
Hello world!\0
```

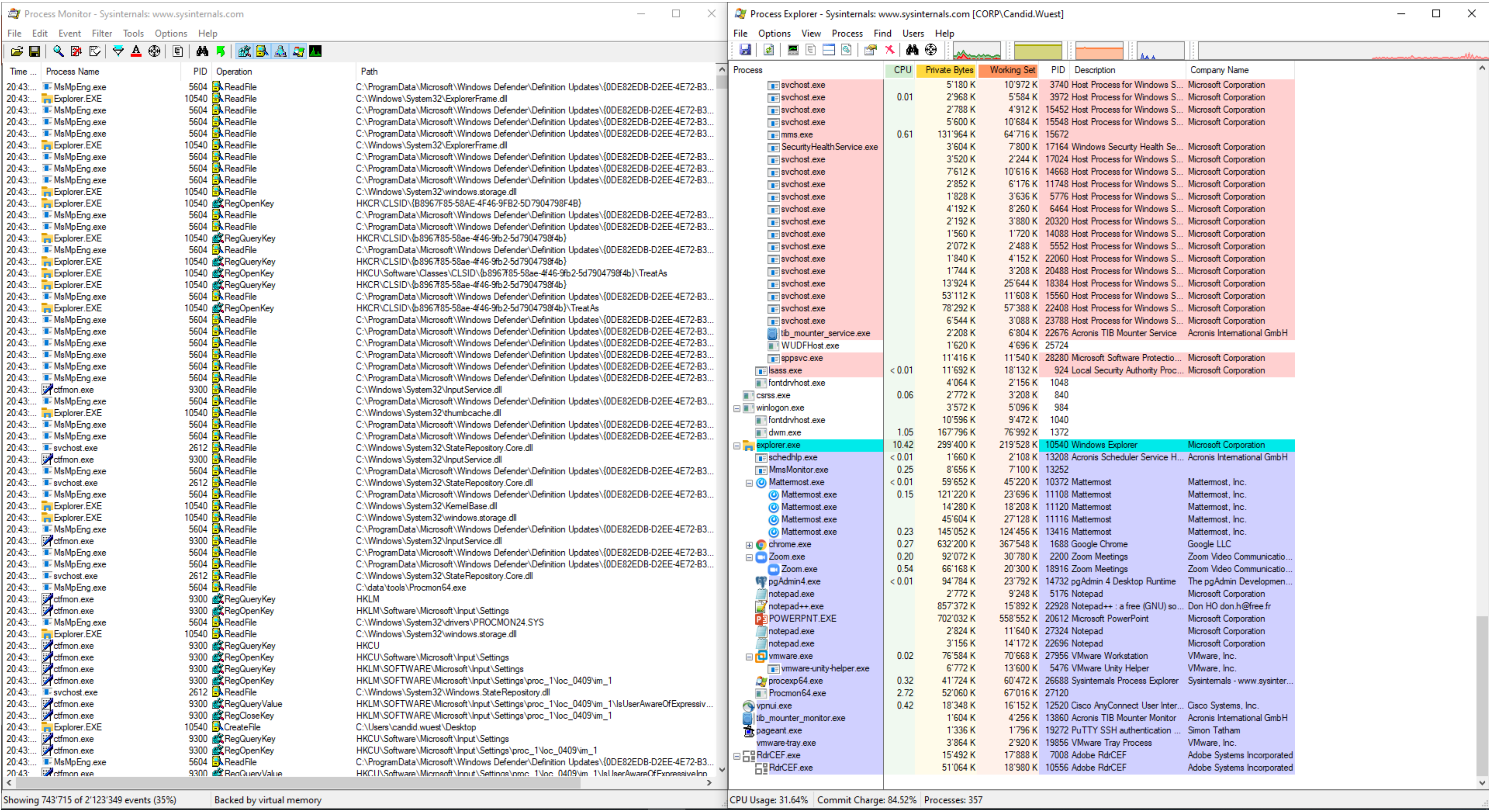
THIS IS THE WHOLE FILE, HOWEVER, MOST PE FILES CONTAIN MORE ELEMENTS.
EXPLANATIONS ARE SIMPLIFIED FOR CONCISENESS.

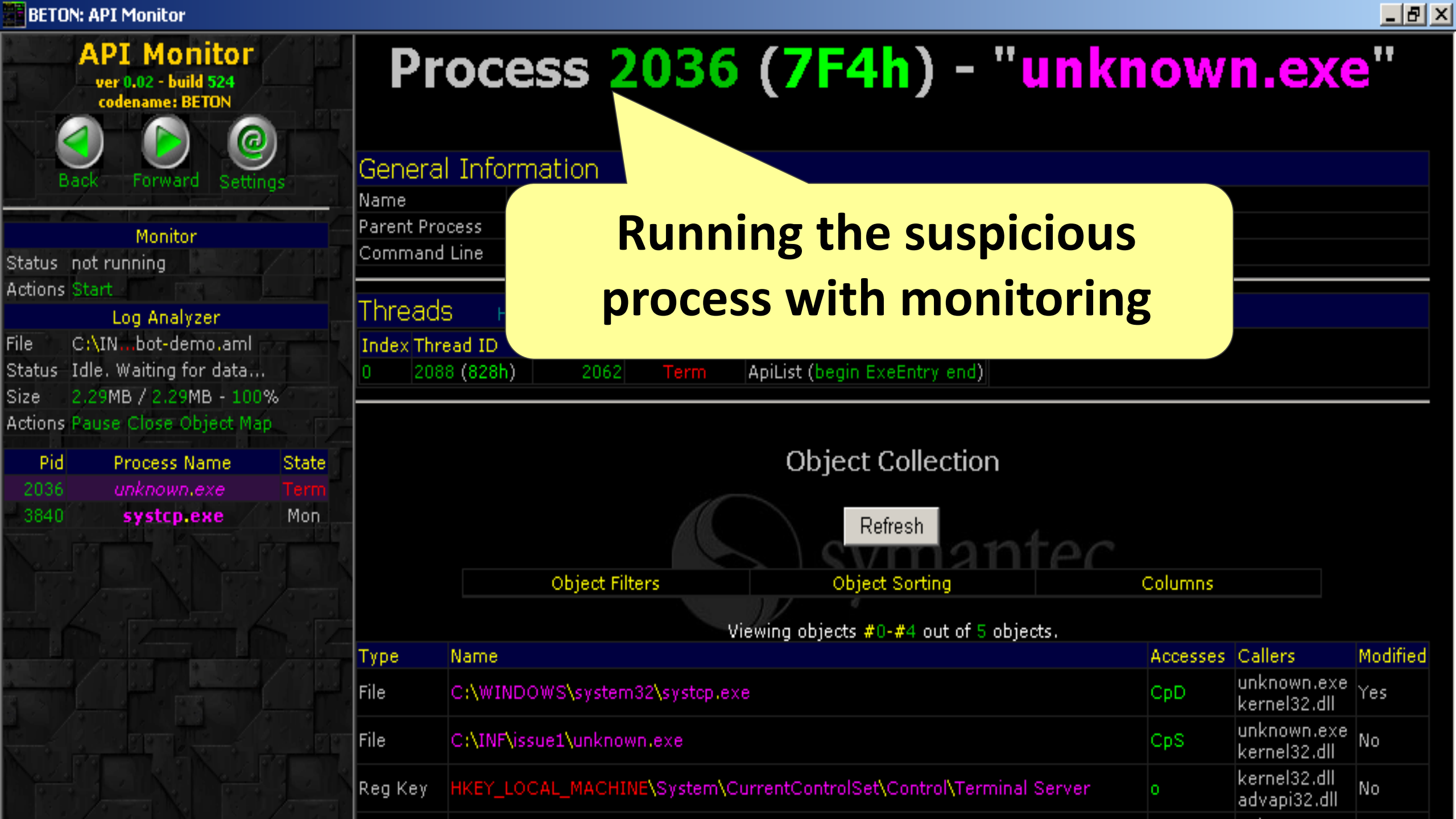
Blackboxing (Dynamic Analysis)

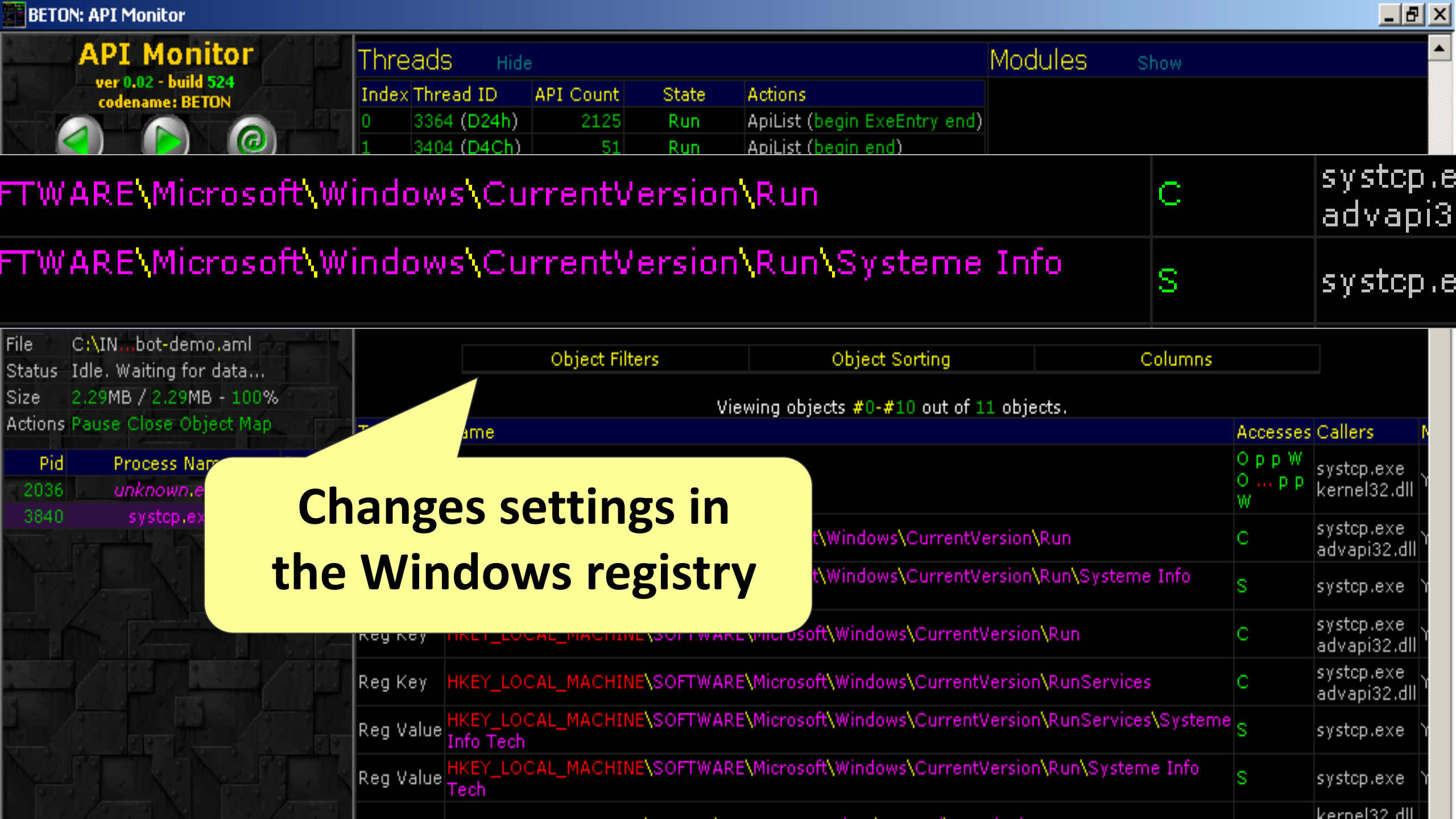
- Execute the sample on a dedicated system (virtual or real)
  - It is about the “what” does it do and not the “how”
- Monitor all operating system API calls
- Analyze logged information and compare
  - E.g. free Sysinternals tools (Regmon, Filemon, TCPView etc.)
- Dump decrypted content from memory
- Done automatically on internal systems → clustering

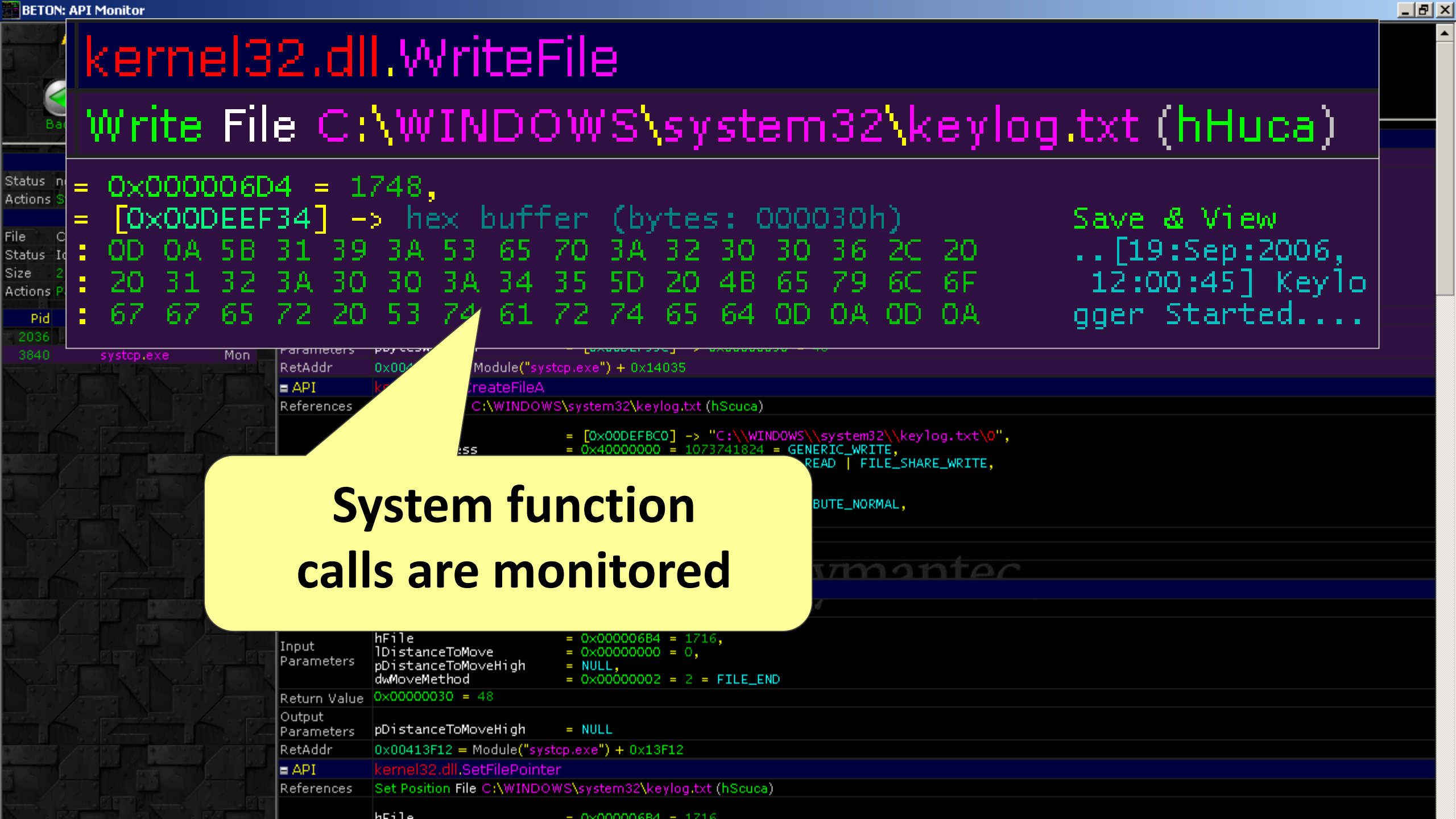
Example: API Monitor

☺ The voices in my head may not be real, but they have some good ideas!


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... Explorer.EXE 10540 ReadFile C:\Windows\System32\ExplorerFrame.dll
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... Explorer.EXE 10540 ReadFile C:\Windows\System32\ExplorerFrame.dll
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... Explorer.EXE 10540 ReadFile C:\Windows\System32\windows.storage.dll
20:43:... Explorer.EXE 10540 RegOpenKey HKCR\CLSID\{B8967F85-58AE-4F46-9FB2-5D7904798F4B}
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... Explorer.EXE 10540 RegQueryKey HKCR\CLSID\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... Explorer.EXE 10540 RegQueryKey HKCR\CLSID\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}
20:43:... Explorer.EXE 10540 RegOpenKey HKCU\Software\Classes\CLSID\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}\TreatAs
20:43:... Explorer.EXE 10540 RegQueryKey HKCR\CLSID\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... Explorer.EXE 10540 RegOpenKey HKCR\CLSID\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}\TreatAs
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... ctfmon.exe 9300 ReadFile C:\Windows\System32\InputService.dll
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... Explorer.EXE 10540 ReadFile C:\Windows\System32\thumbcache.dll
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... svchost.exe 2612 ReadFile C:\Windows\System32\StateRepository.Core.dll
20:43:... ctfmon.exe 9300 ReadFile C:\Windows\System32\InputService.dll
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... svchost.exe 2612 ReadFile C:\Windows\System32\StateRepository.Core.dll
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... Explorer.EXE 10540 ReadFile C:\Windows\System32\KernelBase.dll
20:43:... Explorer.EXE 10540 ReadFile C:\Windows\System32\windows.storage.dll
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... ctfmon.exe 9300 ReadFile C:\Windows\System32\InputService.dll
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
20:43:... svchost.exe 2612 ReadFile C:\Windows\System32\StateRepository.Core.dll
20:43:... MsMpEng.exe 5604 ReadFile C:\data\tools\Procmon64.exe
20:43:... ctfmon.exe 9300 RegQueryKey HKLM
20:43:... ctfmon.exe 9300 RegOpenKey HKLM\Software\Microsoft\Input\Settings
20:43:... MsMpEng.exe 5604 ReadFile C:\Windows\System32\drivers\PROCMON24.SYS
20:43:... Explorer.EXE 10540 ReadFile C:\Windows\System32\windows.storage.dll
20:43:... ctfmon.exe 9300 RegQueryKey HKCU
20:43:... ctfmon.exe 9300 RegOpenKey HKCU\Software\Microsoft\Input\Settings
20:43:... ctfmon.exe 9300 RegQueryKey HKLM\SOFTWARE\Microsoft\Input\Settings
20:43:... ctfmon.exe 9300 RegOpenKey HKLM\SOFTWARE\Microsoft\Input\Settings\proc_1\loc_0409\im_1
20:43:... svchost.exe 2612 ReadFile C:\Windows\System32\Windows.StateRepository.dll
20:43:... ctfmon.exe 9300 RegQueryValue HKLM\SOFTWARE\Microsoft\Input\Settings\proc_1\loc_0409\im_1\IsUserAwareOfExpressiv...
20:43:... ctfmon.exe 9300 RegCloseKey HKLM\SOFTWARE\Microsoft\Input\Settings\proc_1\loc_0409\im_1
20:43:... Explorer.EXE 10540 CreateFile C:\Users\candid.wuest\Desktop
20:43:... ctfmon.exe 9300 RegQueryKey HKCU\Software\Microsoft\Input\Settings
20:43:... ctfmon.exe 9300 RegOpenKey HKCU\Software\Microsoft\Input\Settings\proc_1\loc_0409\im_1
20:43:... MsMpEng.exe 5604 ReadFile C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{0DE82EDB-D2EE-4E72-B3...
Showing 743'715 of 2'123'349 events (35%)
Backed by virtual memory
Process Explorer - Sysinternals: www.sysinternals.com [CORP\Candid.Wuest]
File Options View Process Find Users Help
Process CPU Private Bytes Working Set PID Description Company Name
svchost.exe 5'180 K 10'972 K 3740 Host Process for Windows S... Microsoft Corporation
svchost.exe 0.01 2'968 K 5'584 K 3972 Host Process for Windows S... Microsoft Corporation
svchost.exe 2'788 K 4'912 K 15452 Host Process for Windows S... Microsoft Corporation
svchost.exe 5'600 K 10'684 K 15548 Host Process for Windows S... Microsoft Corporation
mms.exe 0.61 131'964 K 64'716 K 15672
SecurityHealthService.exe 3'604 K 7'800 K 17164 Windows Security Health Se... Microsoft Corporation
svchost.exe 3'520 K 2'244 K 17024 Host Process for Windows S... Microsoft Corporation
svchost.exe 7'612 K 10'616 K 14668 Host Process for Windows S... Microsoft Corporation
svchost.exe 2'852 K 6'176 K 11748 Host Process for Windows S... Microsoft Corporation
svchost.exe 1'828 K 3'636 K 5776 Host Process for Windows S... Microsoft Corporation
svchost.exe 4'192 K 8'260 K 6464 Host Process for Windows S... Microsoft Corporation
svchost.exe 2'192 K 3'880 K 20320 Host Process for Windows S... Microsoft Corporation
svchost.exe 1'560 K 1'720 K 14088 Host Process for Windows S... Microsoft Corporation
svchost.exe 2'072 K 2'488 K 5552 Host Process for Windows S... Microsoft Corporation
svchost.exe 1'840 K 4'152 K 22060 Host Process for Windows S... Microsoft Corporation
svchost.exe 1'744 K 3'208 K 20488 Host Process for Windows S... Microsoft Corporation
svchost.exe 13'924 K 25'644 K 18384 Host Process for Windows S... Microsoft Corporation
svchost.exe 53'112 K 11'608 K 15560 Host Process for Windows S... Microsoft Corporation
svchost.exe 78'292 K 57'388 K 22408 Host Process for Windows S... Microsoft Corporation
svchost.exe 6'544 K 3'088 K 23788 Host Process for Windows S... Microsoft Corporation
tib_mounter_service.exe 2'208 K 6'804 K 22676 Acronis TIB Mounter Service Acronis International GmbH
WUDFHost.exe 1'620 K 4'696 K 25724
sppsvc.exe 11'416 K 11'540 K 28280 Microsoft Software Protectio... Microsoft Corporation
lsass.exe < 0.01 11'692 K 18'132 K 924 Local Security Authority Proc... Microsoft Corporation
fontdrvhost.exe 4'064 K 2'156 K 1048
csrss.exe 0.06 2'772 K 3'208 K 840
winlogon.exe 3'572 K 5'096 K 984
fontdrvhost.exe 10'596 K 9'472 K 1040
dwm.exe 1.05 167'796 K 76'992 K 1372
explorer.exe 10.42 299'400 K 219'528 K 10540 Windows Explorer Microsoft Corporation
schedhlp.exe < 0.01 1'660 K 2'108 K 13208 Acronis Scheduler Service H... Acronis International GmbH
MmsMonitor.exe 0.25 8'656 K 7'100 K 13252
Mattermost.exe < 0.01 59'652 K 45'220 K 10372 Mattermost Mattermost, Inc.
Mattermost.exe 0.15 121'220 K 23'696 K 11108 Mattermost Mattermost, Inc.
Mattermost.exe 14'280 K 18'208 K 11120 Mattermost Mattermost, Inc.
Mattermost.exe 45'604 K 27'128 K 11116 Mattermost Mattermost, Inc.
Mattermost.exe 0.23 145'052 K 124'456 K 13416 Mattermost Mattermost, Inc.
chrome.exe 0.27 632'200 K 367'548 K 1688 Google Chrome Google LLC
Zoom.exe 0.20 92'072 K 30'780 K 2200 Zoom Meetings Zoom Video Communicatio...
Zoom.exe 0.54 66'168 K 20'300 K 18916 Zoom Meetings Zoom Video Communicatio...
pgAdmin4.exe < 0.01 94'784 K 23'792 K 14732 pgAdmin 4 Desktop Runtime The pgAdmin Developmen...
notepad.exe 2'772 K 9'248 K 5176 Notepad Microsoft Corporation
notepad++.exe 857'372 K 15'892 K 22928 Notepad++ : a free (GNU) so... Don HO don.h@free.fr
POWERPNT.EXE 702'032 K 558'552 K 20612 Microsoft PowerPoint Microsoft Corporation
notepad.exe 2'824 K 11'640 K 27324 Notepad Microsoft Corporation
notepad.exe 3'156 K 14'172 K 22696 Notepad Microsoft Corporation
vmware.exe 0.02 76'584 K 70'668 K 27956 VMware Workstation VMware, Inc.
vmware-unity-helper.exe 6'772 K 13'600 K 5476 VMware Unity Helper VMware, Inc.
procexp64.exe 0.32 41'724 K 60'472 K 26688 Sysinternals Process Explorer Sysinternals - www.sysinter...
Procmon64.exe 2.72 52'060 K 67'016 K 27120
vpnui.exe 0.42 18'348 K 16'152 K 12520 Cisco AnyConnect User Inter... Cisco Systems, Inc.
tib_mounter_monitor.exe 1'604 K 4'256 K 13860 Acronis TIB Mounter Monitor Acronis International GmbH
pageant.exe 1'336 K 1'796 K 19272 PuTTY SSH authentication ... Simon Tatham
vmware-tray.exe 3'864 K 2'920 K 19856 VMware Tray Process VMware, Inc.
RdrCEF.exe 15'492 K 17'888 K 7008 Adobe RdrCEF Adobe Systems Incorporated
RdrCEF.exe 51'064 K 18'980 K 10556 Adobe RdrCEF Adobe Systems Incorporated
CPU Usage: 31.64% Commit Charge: 84.52% Processes: 357

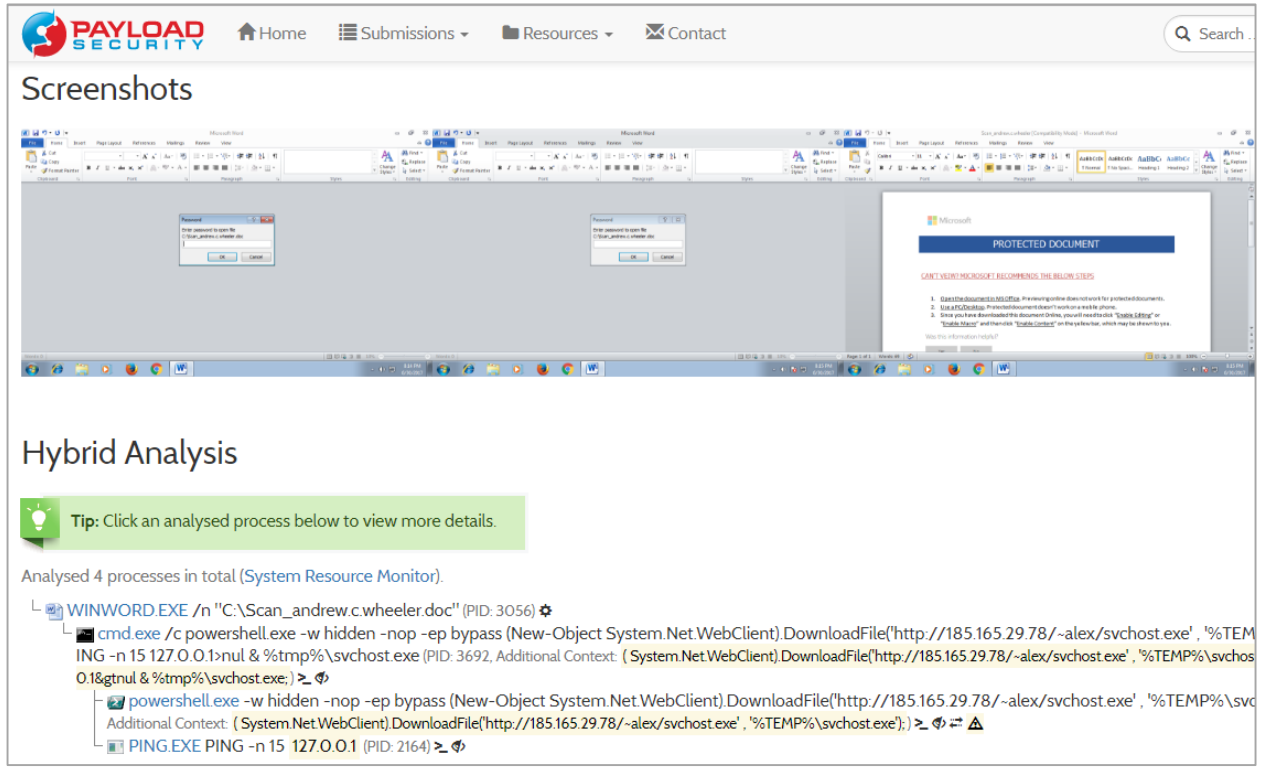

BETON: API Monitor
API Monitor
ver 0.02 - build 524
codename: BETON
Back
Forward
Settings
Monitor
Status not running
Actions Start
Log Analyzer
File C:\IN...bot-demo.aml
Status Idle. Waiting for data...
Size 2.29MB / 2.29MB - 100%
Actions Pause Close Object Map
Pid Process Name State
2036 unknown.exe Term
3840 systcp.exe Mon
Process 2036 (7F4h) - "unknown.exe"
General Information
Name
Parent Process
Command Line
Threads
Index Thread ID
0 2088 (828h) 2062 Term ApiList (begin ExeEntry end)
Running the suspicious process with monitoring
Object Collection
Refresh
Object Filters
Object Sorting
Columns
Viewing objects #0-#4 out of 5 objects.
Type Name Accesses Callers Modified
File C:\WINDOWS\system32\systcp.exe CpD unknown.exe kernel32.dll Yes
File C:\INF\issue1\unknown.exe CpS unknown.exe kernel32.dll No
Reg Key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server o kernel32.dll advapi32.dll No


BETON: API Monitor
API Monitor
ver 0.02 - build 524
codename: BETON
Threads Hide
Modules Show
Index Thread ID API Count State Actions
0 3364 (D24h) 2125 Run ApiList (begin ExeEntry end)
1 3404 (D4Ch) 51 Run ApiList (begin end)
FTWARE\Microsoft\Windows\CurrentVersion\Run
C
systcp.e
advapi3
FTWARE\Microsoft\Windows\CurrentVersion\Run\Systeme Info
S
systcp.e
File C:\IN...bot-demo.aml
Status Idle. Waiting for data...
Size 2.29MB / 2.29MB - 100%
Actions Pause Close Object Map
Pid
2036
3840
Object Filters
Object Sorting
Columns
Viewing objects #0-#10 out of 11 objects.
Accesses
Callers
O p p W
O ... p p
W
systcp.exe
kernel32.dll
t\Windows\CurrentVersion\Run
C
systcp.exe
advapi32.dll
t\Windows\CurrentVersion\Run\Systeme Info
S
systcp.exe
Changes settings in the Windows registry
Reg Key
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
C
systcp.exe
advapi32.dll
Reg Key
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
C
systcp.exe
advapi32.dll
Reg Value
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Systeme Info Tech
S
systcp.exe
Reg Value
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Systeme Info Tech
S
systcp.exe


BETON: API Monitor
kernel32.dll.WriteFile
Write File C:\WINDOWS\system32\keylog.txt (hHuca)
= 0x000006D4 = 1748,
= [0x00DEEF34] -> hex buffer (bytes: 000030h)
: 0D 0A 5B 31 39 3A 53 65 70 3A 32 30 30 36 2C 20
: 20 31 32 3A 30 30 3A 34 35 5D 20 4B 65 79 6C 6F
: 67 67 65 72 20 53 74 61 72 74 65 64 0D 0A 0D 0A
Save & View
..[19:Sep:2006,
12:00:45] Keylo
gger Started....
System function
calls are monitored
RetAddr
Module("systcp.exe") + 0x14035
API
References
C:\WINDOWS\system32\keylog.txt (hScuca)
= [0x00DEFBC0] -> "C:\\WINDOWS\\system32\\keylog.txt\0",
= 0x40000000 = 1073741824 = GENERIC_WRITE,
READ | FILE_SHARE_WRITE,
BUTE_NORMAL,
Input Parameters
hFile = 0x000006B4 = 1716,
lDistanceToMove = 0x00000000 = 0,
pDistanceToMoveHigh = NULL,
dwMoveMethod = 0x00000002 = 2 = FILE_END
Return Value
0x00000030 = 48
Output Parameters
pDistanceToMoveHigh = NULL
RetAddr
0x00413F12 = Module("systcp.exe") + 0x13F12
API
kernel32.dll.SetFilePointer
References
Set Position File C:\WINDOWS\system32\keylog.txt (hScuca)
hFile = 0x000006B4 = 1716,

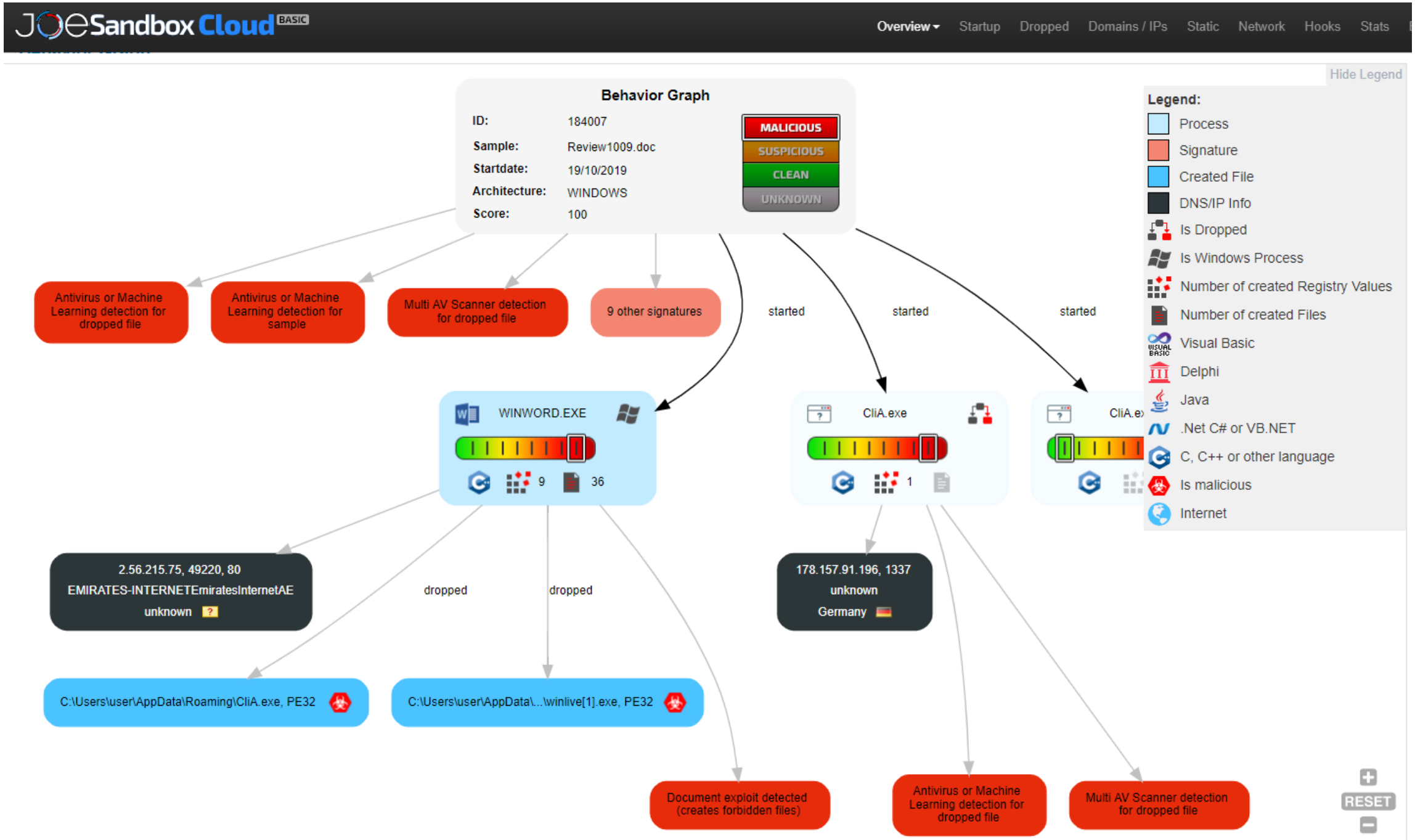
Many solutions to execute and monitor behavior

Sandbox: hybrid-analysis.com



JoeSandbox (joeSecurity.org) in CH

☺ It's bad luck to be superstitious.



☺ It's bad luck to be superstitious.

VMRay Analyzer Report

Dashboard » Samples » #55543 » Analyses » #403825

Activity flow with screenshots etc.

Overview

PE Info

Behavior

Kernel

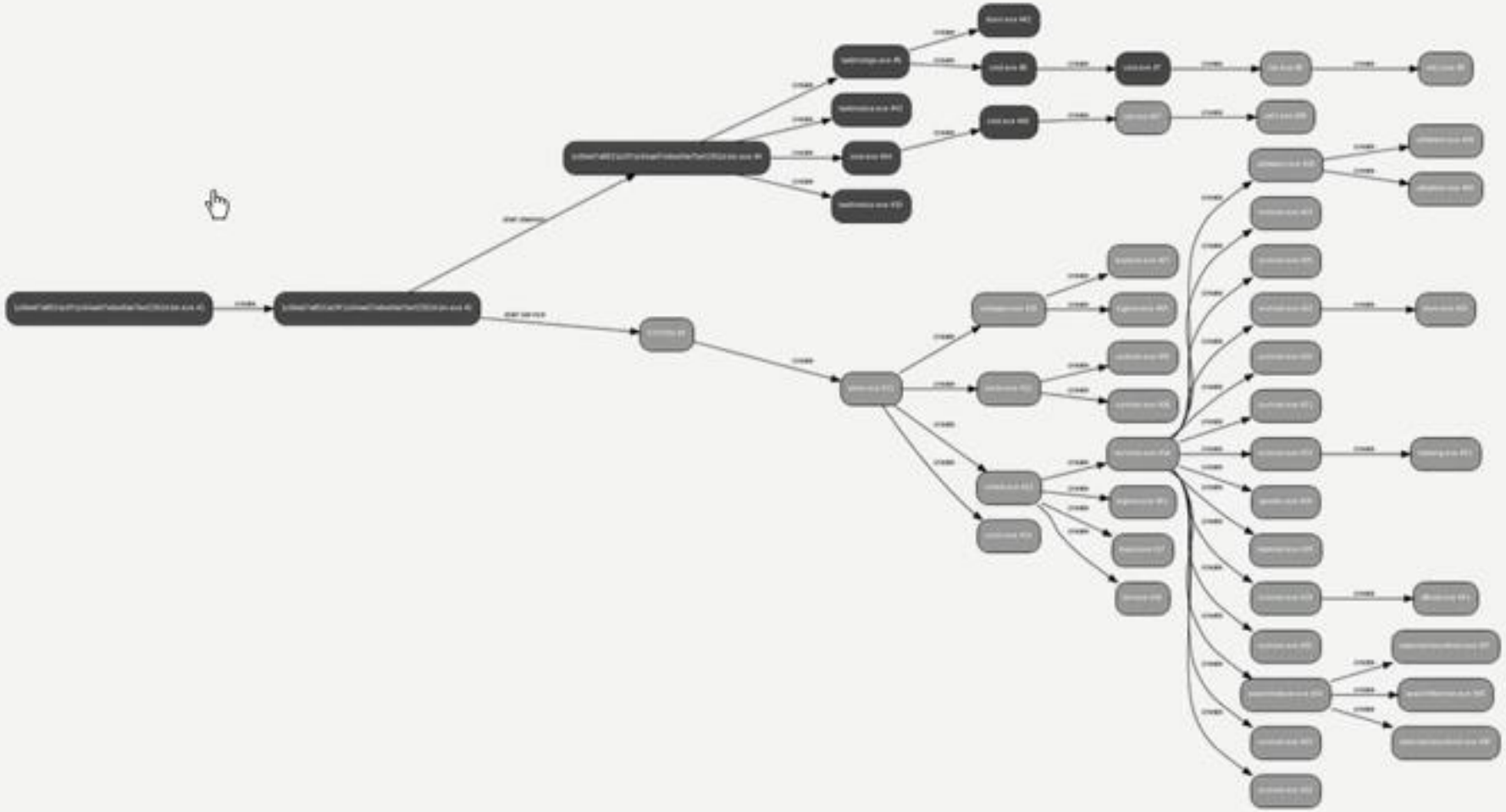
Statistics

Severity

Expand All

Collapse All

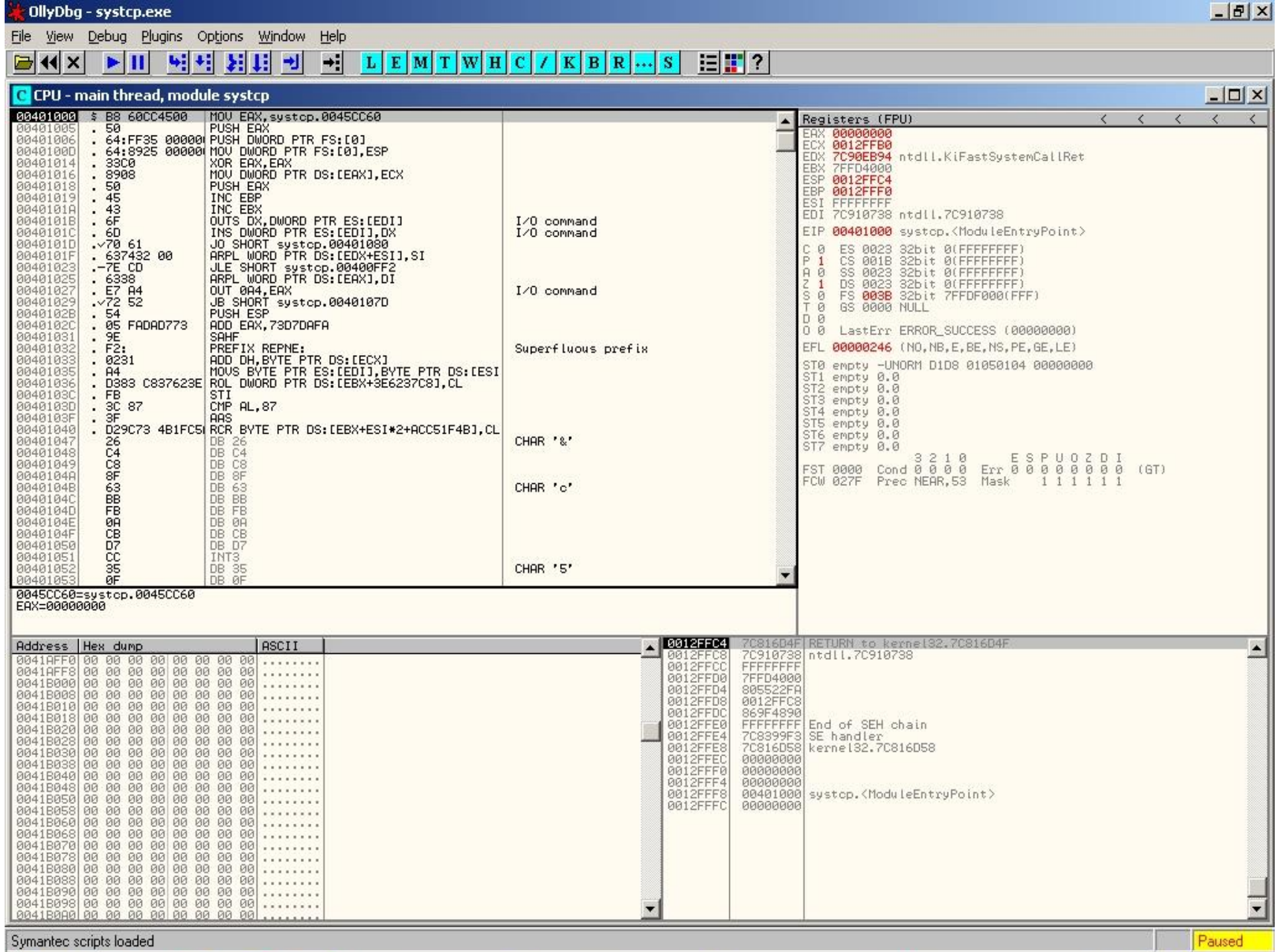
Monitored Processes

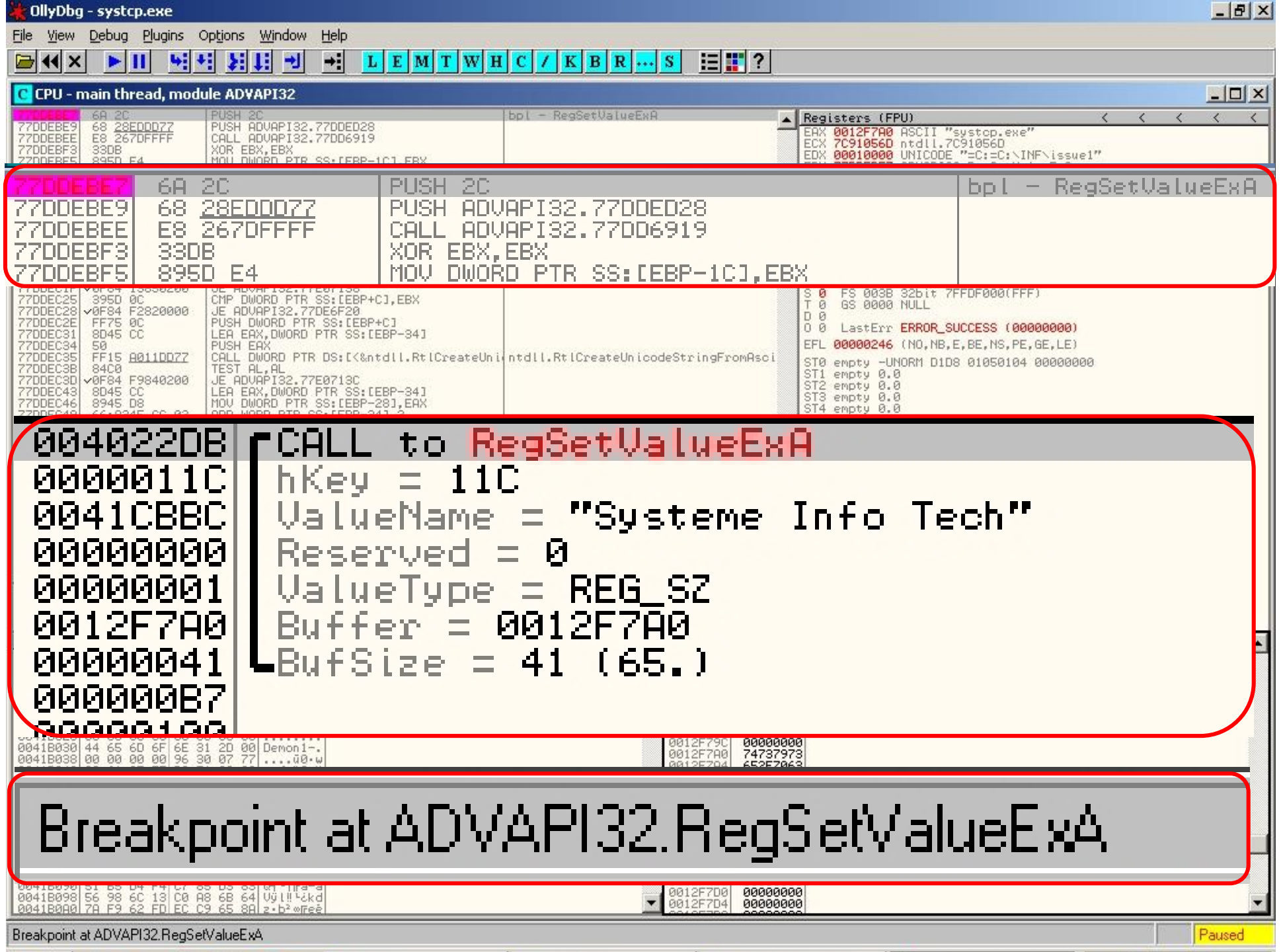


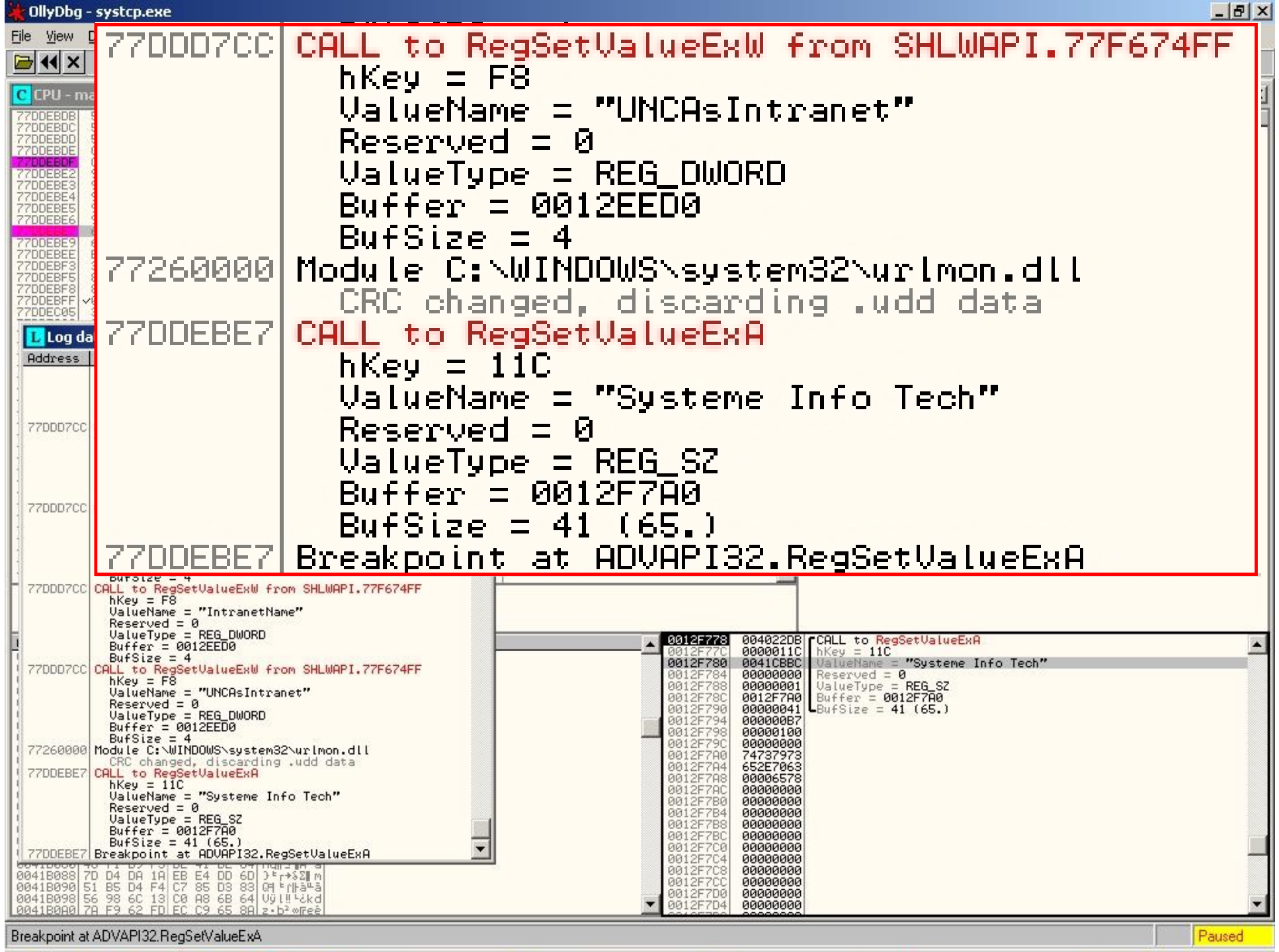
Whiteboxing

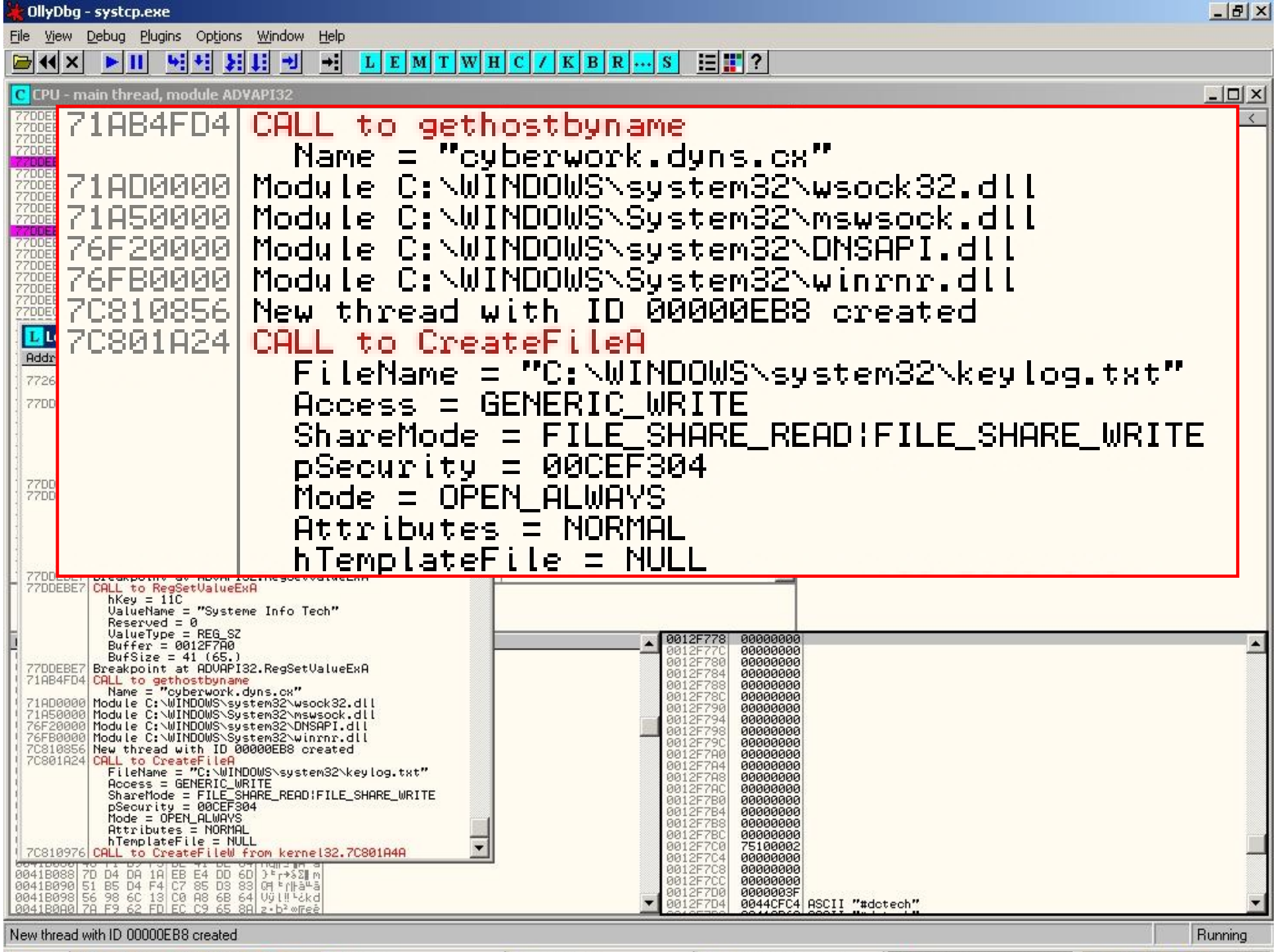
- Blackboxing alone can never tell you everything!
- Use a debugger or disassembler to see & read the code (static analysis)
- See “hidden” functions (time bombs – e.g. Friday 13th ;-)
  - Analyze & copy decryption routines
  - Patch routines if needed (anti-debugging tricks)
  - Find interesting code (e.g. payload)

Example: OllyDbg Debugger

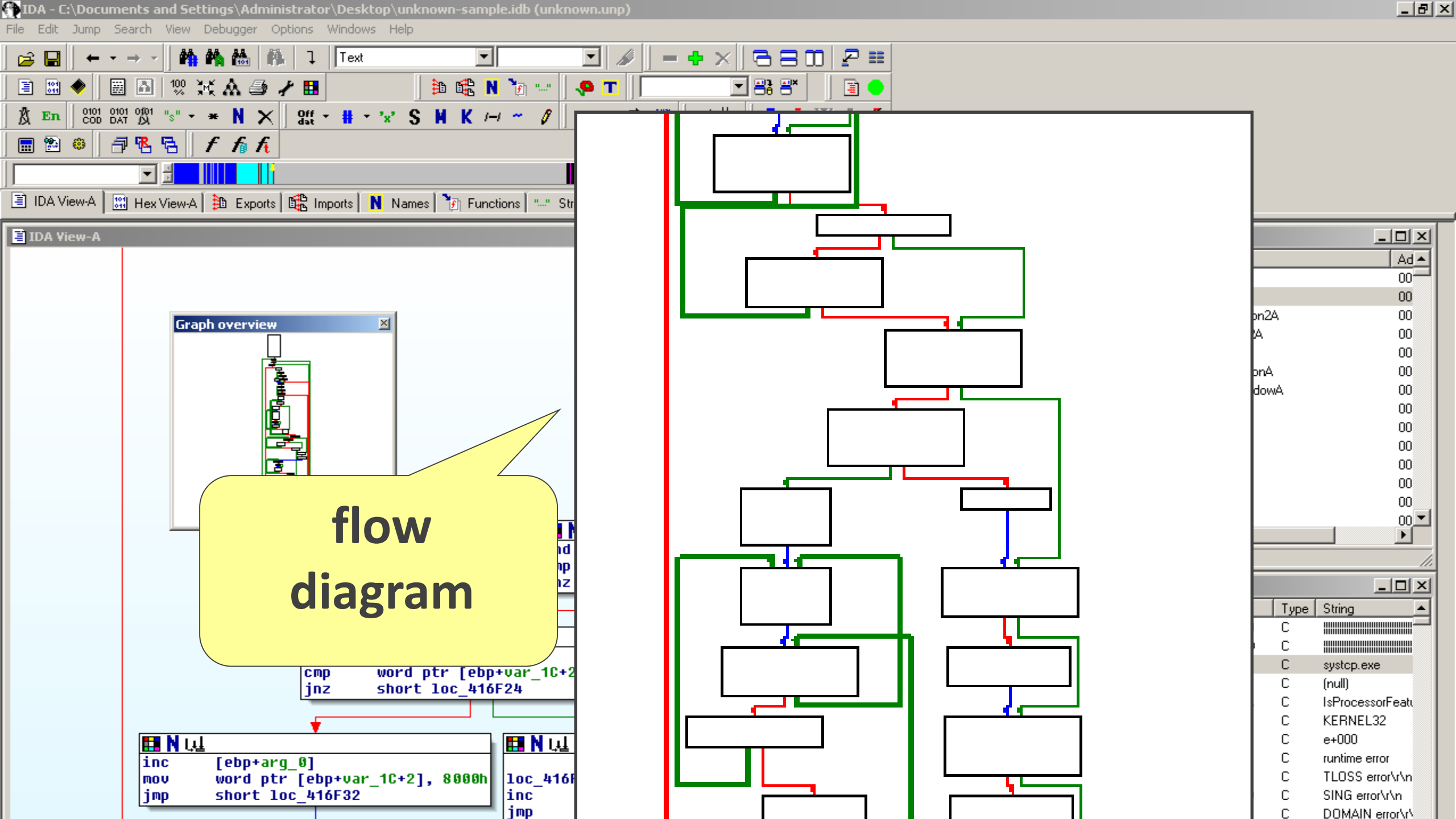

OllyDbg - systcp.exe
File View Debug Plugins Options Window Help
CPU - main thread, module systcp
00401000 $ B8 60CC4500 MOV EAX,systcp.0045CC60
00401005 . 50 PUSH EAX
00401006 . 64:FF35 00000(PUSH DWORD PTR FS:[0]
0040100D . 64:8925 00000(MOV DWORD PTR FS:[0],ESP
00401014 . 33C0 XOR EAX,EAX
00401016 . 8908 MOV DWORD PTR DS:[EAX],ECX
00401018 . 50 PUSH EAX
00401019 . 45 INC EBP
0040101A . 43 INC EBX
0040101B . 6F OUTS DX,DWORD PTR ES:[EDI] I/O command
0040101C . 6D INS DWORD PTR ES:[EDI],DX I/O command
0040101D .v70 61 JO SHORT systcp.00401080
0040101F . 637432 00 ARPL WORD PTR DS:[EDX+ESI],SI
00401023 .-7E CD JLE SHORT systcp.00400FF2
00401025 . 6338 ARPL WORD PTR DS:[EAX],DI
00401027 . E7 A4 OUT 0A4,EAX I/O command
00401029 .v72 52 JB SHORT systcp.0040107D
0040102B . 54 PUSH ESP
0040102C . 05 FADAD773 ADD EAX,73D7DAFA
00401031 . 9E SAHF
00401032 . F2: PREFIX REPNE: Superfluous prefix
00401033 . 0231 ADD DH,BYTE PTR DS:[ECX]
00401035 . A4 MOVS BYTE PTR ES:[EDI],BYTE PTR DS:[ESI
00401036 . D383 C837623E ROL DWORD PTR DS:[EBX+3E6237C8],CL
0040103C . FB STI
0040103D . 3C 87 CMP AL,87
0040103F . 3F AAS
00401040 . D29C73 4B1FC5(RCR BYTE PTR DS:[EBX+ESI*2+ACC51F4B],CL
00401047 26 DB 26 CHAR '&'
00401048 C4 DB C4
00401049 C8 DB C8
0040104A 8F DB 8F
0040104B 63 DB 63 CHAR 'c'
0040104C BB DB BB
0040104D FB DB FB
0040104E 0A DB 0A
0040104F CB DB CB
00401050 D7 DB D7
00401051 CC INT3
00401052 35 DB 35 CHAR '5'
00401053 0F DB 0F
0045CC60=systcp.0045CC60
EAX=00000000
Registers (FPU)
EAX 00000000
ECX 0012FFB0
EDX 7C90EB94 ntdll.KiFastSystemCallRet
EBX 7FFD4000
ESP 0012FFC4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C910738 ntdll.7C910738
EIP 00401000 systcp.<ModuleEntryPoint>
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 1 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDF000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty -UNORM D1D8 01050104 00000000
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
3 2 1 0 E S P U O Z D I
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
Address Hex dump ASCII
0041AFF0 00 00 00 00 00 00 00 00 ....
0041AFF8 00 00 00 00 00 00 00 00 ....
0041B000 00 00 00 00 00 00 00 00 ....
0041B008 00 00 00 00 00 00 00 00 ....
0041B010 00 00 00 00 00 00 00 00 ....
0041B018 00 00 00 00 00 00 00 00 ....
0041B020 00 00 00 00 00 00 00 00 ....
0041B028 00 00 00 00 00 00 00 00 ....
0041B030 00 00 00 00 00 00 00 00 ....
0041B038 00 00 00 00 00 00 00 00 ....
0041B040 00 00 00 00 00 00 00 00 ....
0041B048 00 00 00 00 00 00 00 00 ....
0041B050 00 00 00 00 00 00 00 00 ....
0041B058 00 00 00 00 00 00 00 00 ....
0041B060 00 00 00 00 00 00 00 00 ....
0041B068 00 00 00 00 00 00 00 00 ....
0041B070 00 00 00 00 00 00 00 00 ....
0041B078 00 00 00 00 00 00 00 00 ....
0041B080 00 00 00 00 00 00 00 00 ....
0041B088 00 00 00 00 00 00 00 00 ....
0041B090 00 00 00 00 00 00 00 00 ....
0041B098 00 00 00 00 00 00 00 00 ....
0041B0A0 00 00 00 00 00 00 00 00 ....
0012FFC4 7C816D4F RETURN to kernel32.7C816D4F
0012FFC8 7C910738 ntdll.7C910738
0012FFCC FFFFFFFF
0012FFD0 7FFD4000
0012FFD4 805522FA
0012FFD8 0012FFC8
0012FFDC 869F4890
0012FFE0 FFFFFFFF End of SEH chain
0012FFE4 7C8399F3 SE handler
0012FFE8 7C816D58 kernel32.7C816D58
0012FFEC 00000000
0012FFF0 00000000
0012FFF4 00000000
0012FFF8 00401000 systcp.<ModuleEntryPoint>
0012FFFC 00000000
Symantec scripts loaded
Paused

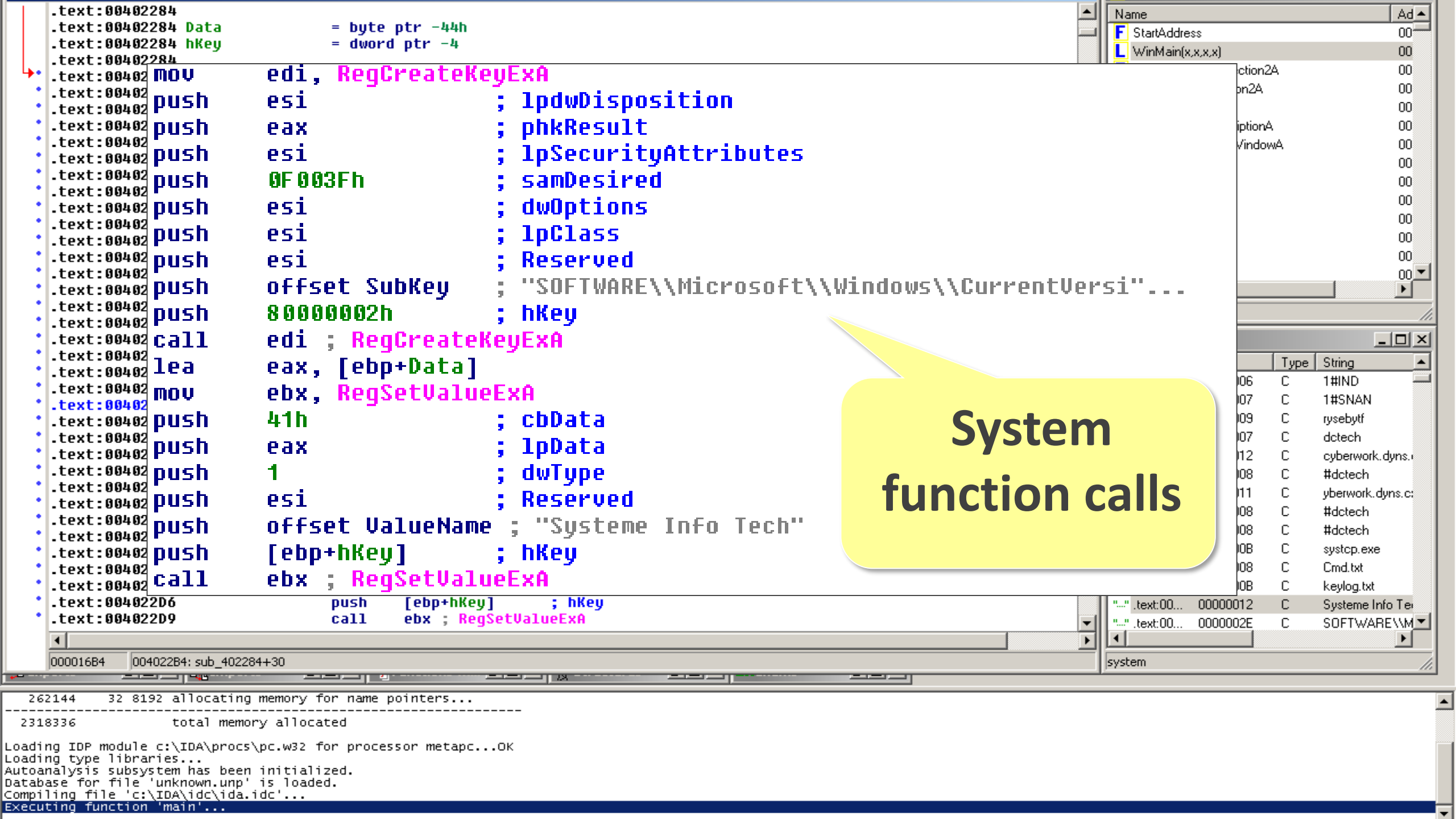

OllyDbg - systcp.exe
File View Debug Plugins Options Window Help
CPU - main thread, module ADVAPI32
77DDEBE7 6A 2C PUSH 2C bpl - RegSetValueExA
77DDEBE9 68 28EDDD77 PUSH ADVAPI32.77DDED28
77DDEBEE E8 267DFFFF CALL ADVAPI32.77DD6919
77DDEBF3 33DB XOR EBX,EBX
77DDEBF5 895D E4 MOV DWORD PTR SS:[EBP-1C],EBX
Registers (FPU)
EAX 0012F7A0 ASCII "systcp.exe"
ECX 7C91056D ntdll.7C91056D
EDX 00010000 UNICODE "=C:=C:\INF\issue1"
004022DB CALL to RegSetValueExA
0000011C hKey = 11C
0041CBBC ValueName = "Systeme Info Tech"
00000000 Reserved = 0
00000001 ValueType = REG_SZ
0012F7A0 Buffer = 0012F7A0
00000041 BufSize = 41 (65.)
000000B7
Breakpoint at ADVAPI32.RegSetValueExA
Breakpoint at ADVAPI32.RegSetValueExA
Paused


OllyDbg - systcp.exe
77DDD7CC CALL to RegSetValueExW from SHLWAPI.77F674FF
hKey = F8
ValueName = "UNCAsIntranet"
Reserved = 0
ValueType = REG_DWORD
Buffer = 0012EED0
BufSize = 4
77260000 Module C:\WINDOWS\system32\urlmon.dll
CRC changed, discarding .udd data
77DDEBE7 CALL to RegSetValueExA
hKey = 11C
ValueName = "Systeme Info Tech"
Reserved = 0
ValueType = REG_SZ
Buffer = 0012F7A0
BufSize = 41 (65.)
77DDEBE7 Breakpoint at ADVAPI32.RegSetValueExA
77DDD7CC CALL to RegSetValueExW from SHLWAPI.77F674FF
hKey = F8
ValueName = "IntranetName"
Reserved = 0
ValueType = REG_DWORD
Buffer = 0012EED0
BufSize = 4
77DDD7CC CALL to RegSetValueExW from SHLWAPI.77F674FF
hKey = F8
ValueName = "UNCAsIntranet"
Reserved = 0
ValueType = REG_DWORD
Buffer = 0012EED0
BufSize = 4
77260000 Module C:\WINDOWS\system32\urlmon.dll
CRC changed, discarding .udd data
77DDEBE7 CALL to RegSetValueExA
hKey = 11C
ValueName = "Systeme Info Tech"
Reserved = 0
ValueType = REG_SZ
Buffer = 0012F7A0
BufSize = 41 (65.)
77DDEBE7 Breakpoint at ADVAPI32.RegSetValueExA
0012F778 004022DB CALL to RegSetValueExA
0012F77C 0000011C hKey = 11C
0012F780 0041CBBC ValueName = "Systeme Info Tech"
0012F784 00000000 Reserved = 0
0012F788 00000001 ValueType = REG_SZ
0012F78C 0012F7A0 Buffer = 0012F7A0
0012F790 00000041 BufSize = 41 (65.)
Breakpoint at ADVAPI32.RegSetValueExA
Paused


OllyDbg - systcp.exe
File View Debug Plugins Options Window Help
CPU - main thread, module ADVAPI32
71AB4FD4 CALL to gethostbyname
Name = "cyberwork.dyns.cx"
71AD0000 Module C:\WINDOWS\system32\wsock32.dll
71A50000 Module C:\WINDOWS\System32\mswsock.dll
76F20000 Module C:\WINDOWS\system32\DNSAPI.dll
76FB0000 Module C:\WINDOWS\System32\winrnr.dll
7C810856 New thread with ID 00000EB8 created
7C801A24 CALL to CreateFileA
FileName = "C:\WINDOWS\system32\keylog.txt"
Access = GENERIC_WRITE
ShareMode = FILE_SHARE_READ|FILE_SHARE_WRITE
pSecurity = 00CEF304
Mode = OPEN_ALWAYS
Attributes = NORMAL
hTemplateFile = NULL
77DDEBE7 CALL to RegSetValueExA
hKey = 11C
ValueName = "Systeme Info Tech"
Reserved = 0
ValueType = REG_SZ
Buffer = 0012F7A0
BufSize = 41 (65.)
77DDEBE7 Breakpoint at ADVAPI32.RegSetValueExA
71AB4FD4 CALL to gethostbyname
Name = "cyberwork.dyns.cx"
71AD0000 Module C:\WINDOWS\system32\wsock32.dll
71A50000 Module C:\WINDOWS\System32\mswsock.dll
76F20000 Module C:\WINDOWS\system32\DNSAPI.dll
76FB0000 Module C:\WINDOWS\System32\winrnr.dll
7C810856 New thread with ID 00000EB8 created
7C801A24 CALL to CreateFileA
FileName = "C:\WINDOWS\system32\keylog.txt"
Access = GENERIC_WRITE
ShareMode = FILE_SHARE_READ|FILE_SHARE_WRITE
pSecurity = 00CEF304
Mode = OPEN_ALWAYS
Attributes = NORMAL
hTemplateFile = NULL
7C810976 CALL to CreateFileW from kernel32.7C801A4A
0012F778 00000000
0012F77C 00000000
0012F780 00000000
0012F784 00000000
0012F788 00000000
0012F78C 00000000
0012F790 00000000
0012F794 00000000
0012F798 00000000
0012F79C 00000000
0012F7A0 00000000
0012F7A4 00000000
0012F7A8 00000000
0012F7AC 00000000
0012F7B0 00000000
0012F7B4 00000000
0012F7B8 00000000
0012F7BC 00000000
0012F7C0 75100002
0012F7C4 00000000
0012F7C8 00000000
0012F7CC 00000000
0012F7D0 0000003F
0012F7D4 0044CFC4 ASCII "#dctech"
New thread with ID 00000EB8 created
Running

Example: IDA pro


IDA - C:\Documents and Settings\Administrator\Desktop\unknown-sample.idb (unknown.unp)
File Edit Jump Search View Debugger Options Windows Help
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Graph overview
flow diagram
cmp word ptr [ebp+var_1C+2
jnz short loc_416F24
inc [ebp+arg_0]
mov word ptr [ebp+var_1C+2], 8000h
jmp short loc_416F32
loc_416F
inc
jmp
Type
String
systcp.exe
(null)
KERNEL32
runtime error
TLOSS error\r\n
SING error\r\n
DOMAIN error\r\


.text:00402284
.text:00402284 Data = byte ptr -44h
.text:00402284 hKey = dword ptr -4
.text:00402284
mov edi, RegCreateKeyExA
push esi ; lpdwDisposition
push eax ; phkResult
push esi ; lpSecurityAttributes
push 0F003Fh ; samDesired
push esi ; dwOptions
push esi ; lpClass
push esi ; Reserved
push offset SubKey ; "SOFTWARE\\Microsoft\\Windows\\CurrentVersi"...
push 80000002h ; hKey
call edi ; RegCreateKeyExA
lea eax, [ebp+Data]
mov ebx, RegSetValueExA
push 41h ; cbData
push eax ; lpData
push 1 ; dwType
push esi ; Reserved
push offset ValueName ; "Systeme Info Tech"
push [ebp+hKey] ; hKey
call ebx ; RegSetValueExA
.text:004022D6 push [ebp+hKey] ; hKey
.text:004022D9 call ebx ; RegSetValueExA
000016B4
004022B4: sub_402284+30
Name
StartAddress
WinMain(x,x,x,x)
Type
String
1#IND
1#SNAN
rysebytf
dctech
cyberwork.dyns.
#dctech
yberwork.dyns.c
#dctech
#dctech
systcp.exe
Cmd.txt
keylog.txt
.text:00... 00000012 C Systeme Info Te
.text:00... 0000002E C SOFTWARE\\M
system
System function calls
262144 32 8192 allocating memory for name pointers...
2318336 total memory allocated
Loading IDP module c:\IDA\procs\pc.w32 for processor metapc...OK
Loading type libraries...
Autoanalysis subsystem has been initialized.
Database for file 'unknown.unp' is loaded.
Compiling file 'c:\IDA\idc\ida.idc'...
Executing function 'main'...

```
rep stosd
lea     eax, [ebp+Buffer]
push    104h            ; uSize
push    eax             ; lpBuffer
mov     [ebp+var_C], ebx
call    GetSystemDirectoryA
lea     eax, [ebp+Buffer]
push    offset aKeylog_txt ; "keylog.txt"
push    eax
lea     eax, [ebp+var_3F4]
push    offset aSS_2    ; "%s\\%s"
push    eax             ; char *
call    _sprintf
lea     eax, [ebp+var_3F4]
push    offset aAw      ; "aw"
push    eax             ; char *
call    _fopen
mov     edi, eax
add     esp, 18h
cmp     edi, ebx
jz      short loc_40D7E0
lea     eax, [ebp+TimeStr]
push    46h             ; cchDate
push    eax             ; lpDateStr
push    offset aDdMmmYyyy ; "\n[dd:MMM:yyyy, "
push    ebx             ; lpDate
mov     esi, 409h
push    ebx             ; dwFlags
push    esi             ; Locale
call    GetDateFormatA
lea     eax, [ebp+TimeStr]
push    edi             ; FILE *
push    eax             ; char *
call    _fputs
push    46h             ; size_t
```

Follow the code flow

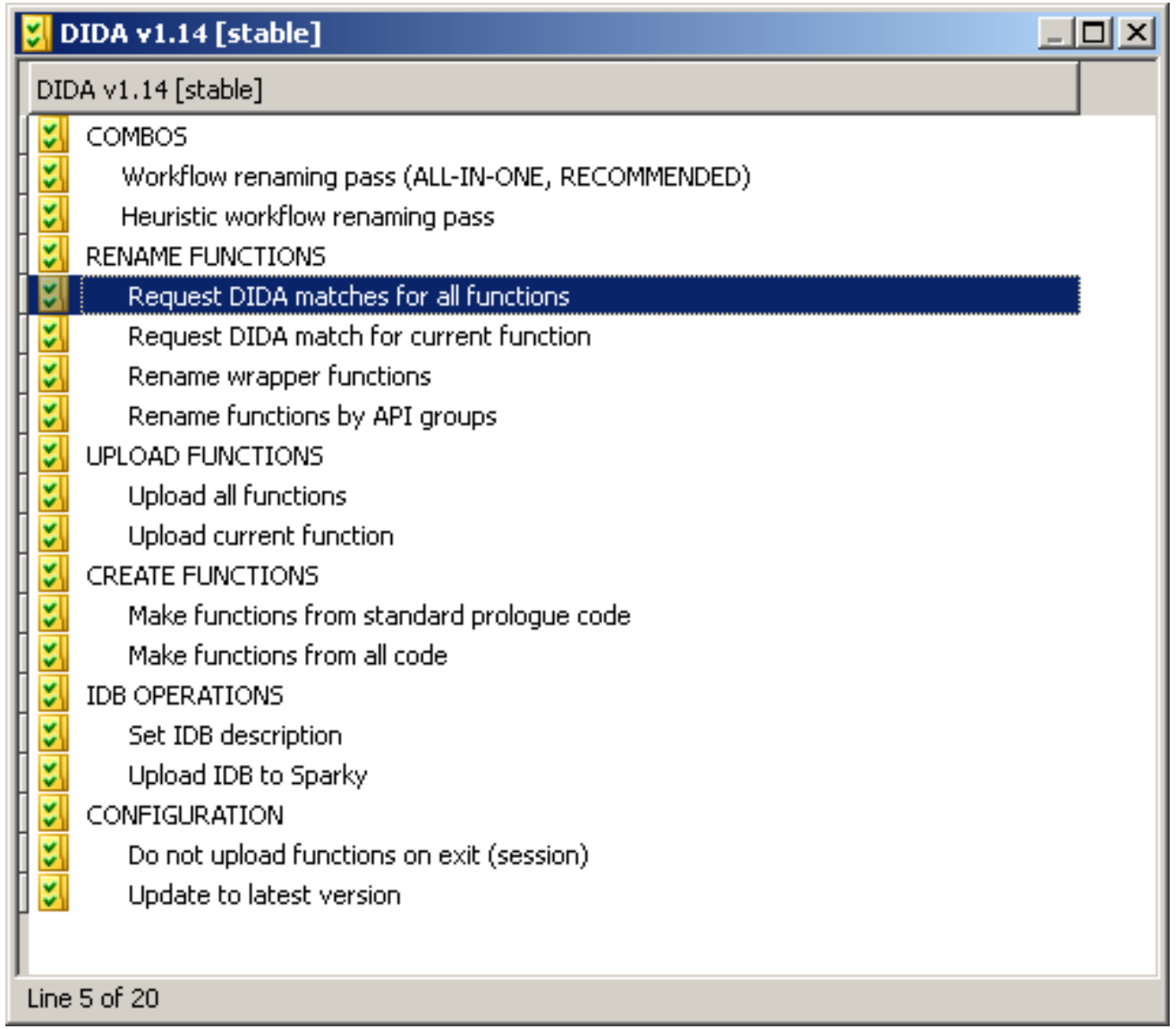
F StartAddress
L WinMain(x,x,x,x
F WNetCancelCo
F WNetAddConn
F __WSAFDIsSet
F capGetDriverDe
F capCreateCaptu
L __cinit
L _exit
L __exit
L __cexit
L __c_exit
L _doexit
L initterm

Line 2 of 2996

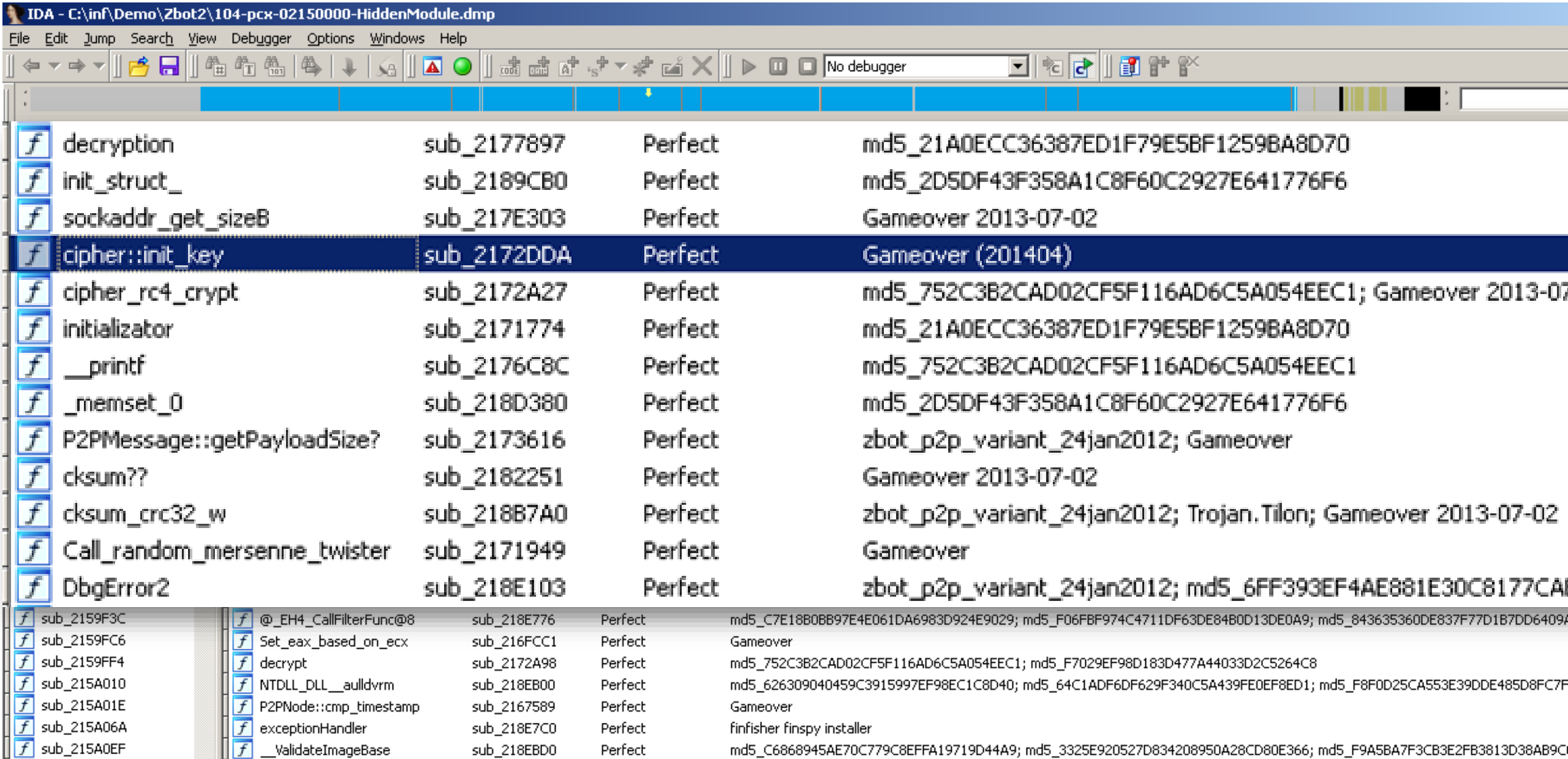
Strings windo

Address	Len
.text:00...	000
.text:00...	000
.text:00...	000
.text:00...	000
.text:00...	000
.text:00...	000
.text:00...	000
.text:00...	000
.text:00...	000
.text:00...	000
.text:00...	000
.text:00...	000
.text:00...	000

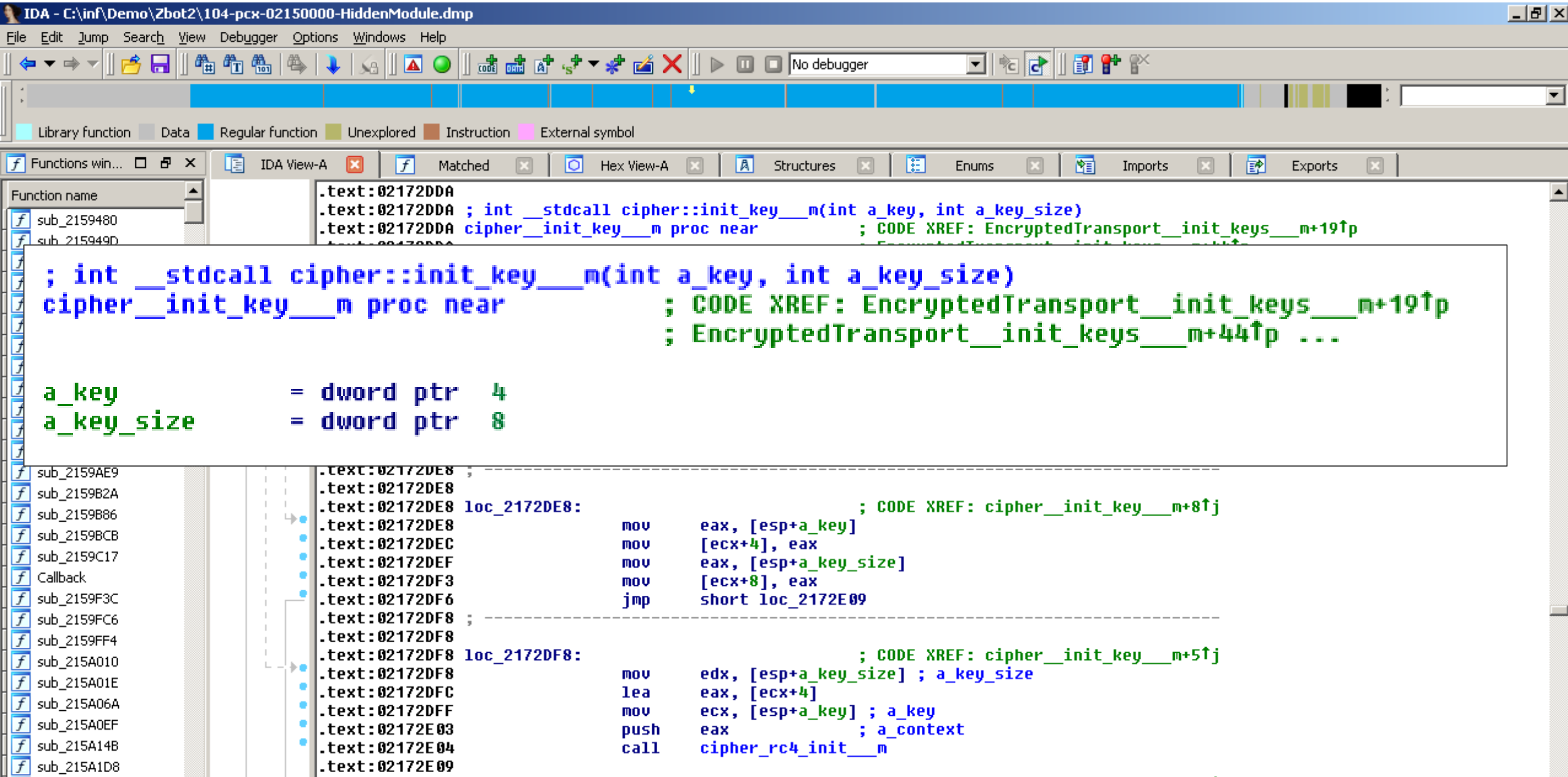
To speed things up: match known functions

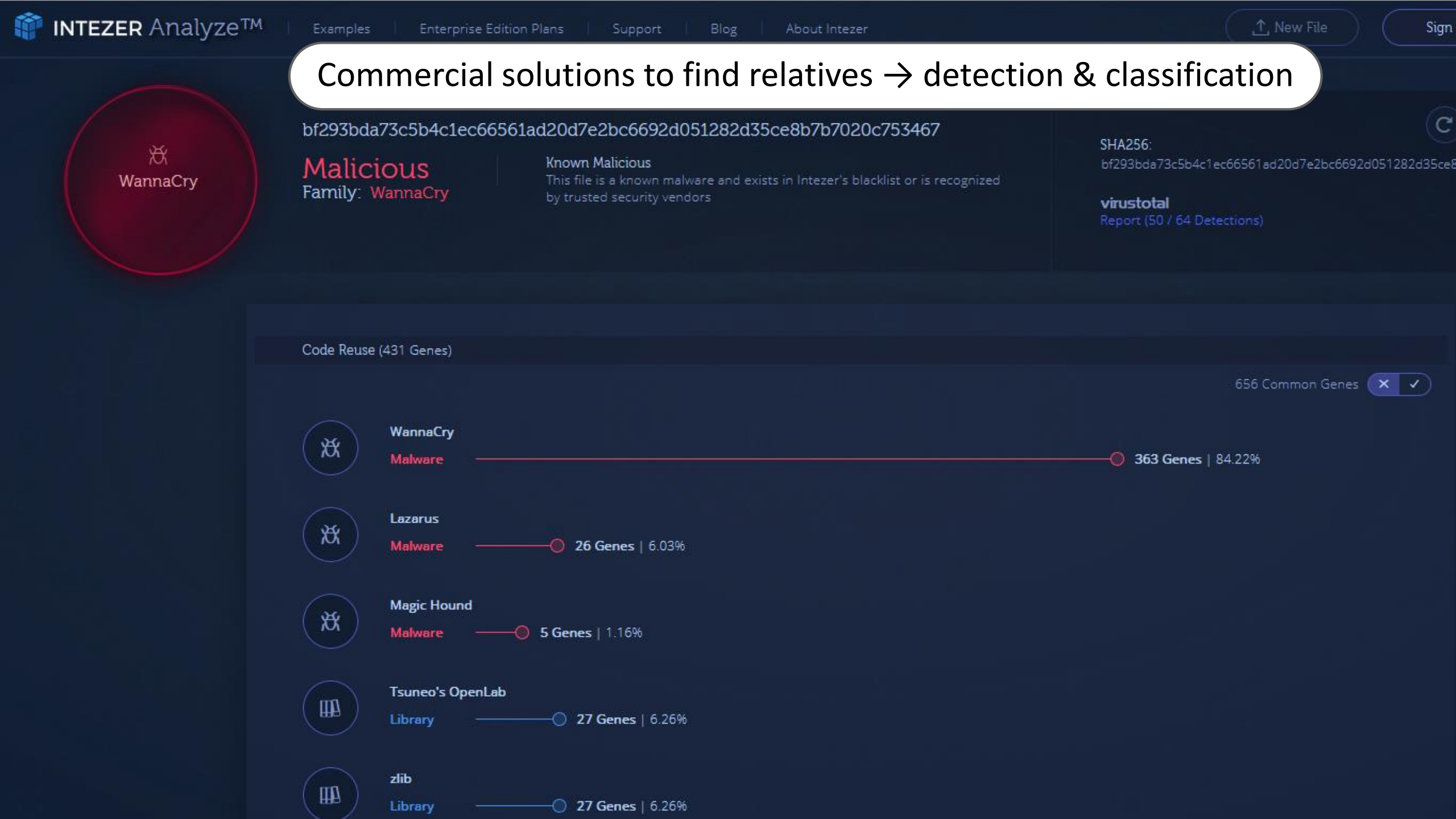


Match known functions



Match known functions in IDA

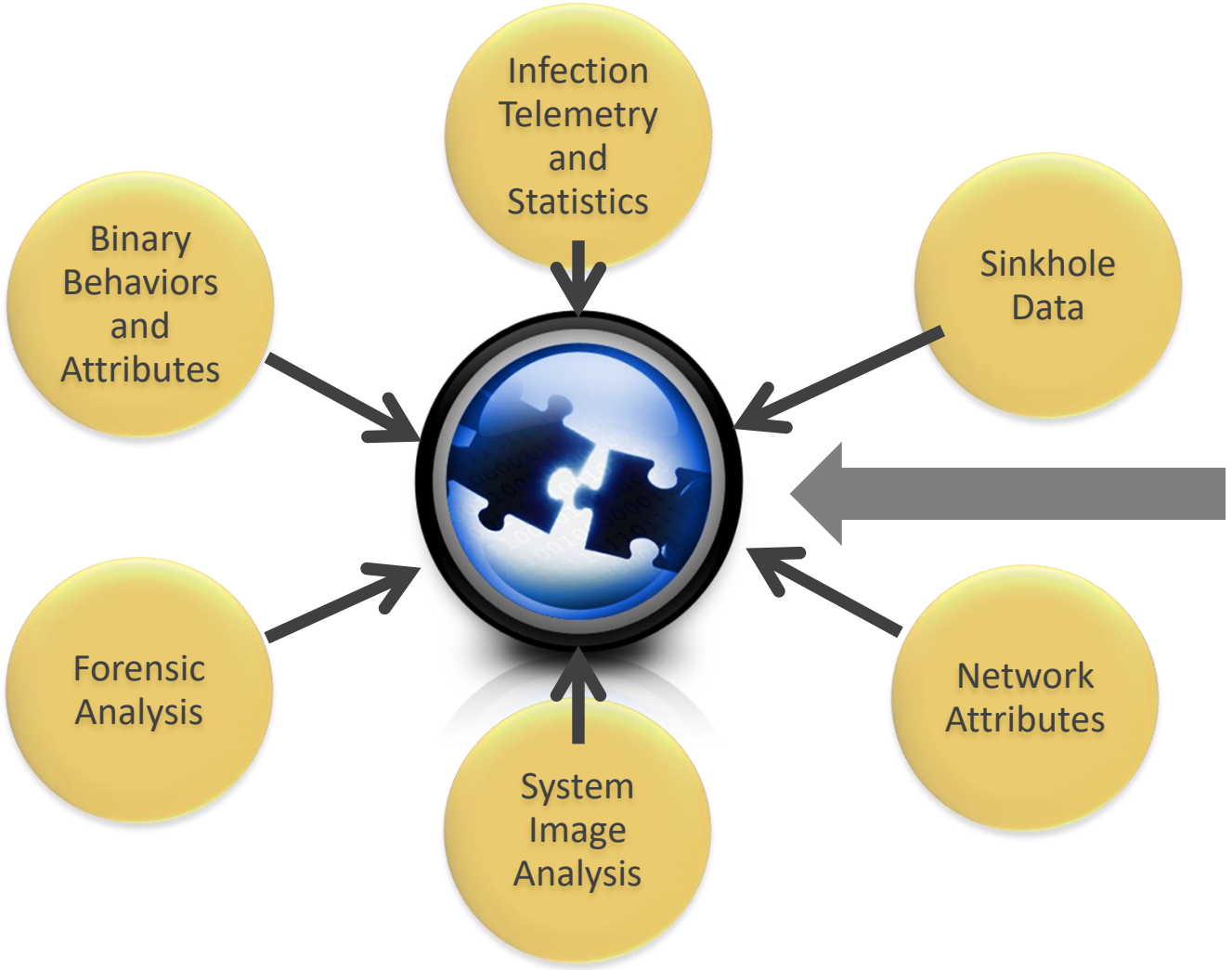



INTEZER Analyze™
Examples
Enterprise Edition Plans
Support
Blog
About Intezer
New File
Sign
Commercial solutions to find relatives → detection & classification
WannaCry
bf293bda73c5b4c1ec66561ad20d7e2bc6692d051282d35ce8b7b7020c753467
Malicious
Family: WannaCry
Known Malicious
This file is a known malware and exists in Intezer's blacklist or is recognized by trusted security vendors
SHA256:
bf293bda73c5b4c1ec66561ad20d7e2bc6692d051282d35ce8
virustotal
Report (50 / 64 Detections)
Code Reuse (431 Genes)
656 Common Genes
WannaCry
Malware
363 Genes | 84.22%
Lazarus
Malware
26 Genes | 6.03%
Magic Hound
Malware
5 Genes | 1.16%
Tsuneo's OpenLab
Library
27 Genes | 6.26%
zlib
Library
27 Genes | 6.26%

The Analysis generates Metadata

- **URLs** (=more to analyse & visit)
  - Command & Control servers, drop zones, updates, …
- **Files**
  - Names, hashes, dropper name, …
- **Registry Data**
  - Clustering, removal instructions, …
- **Network traffic**
  - IPS signatures, Data Loss Prevention (DLP) checks, take downs, …
- **Memory dumps**
  - Binary strings, further analysis, protection updates, …

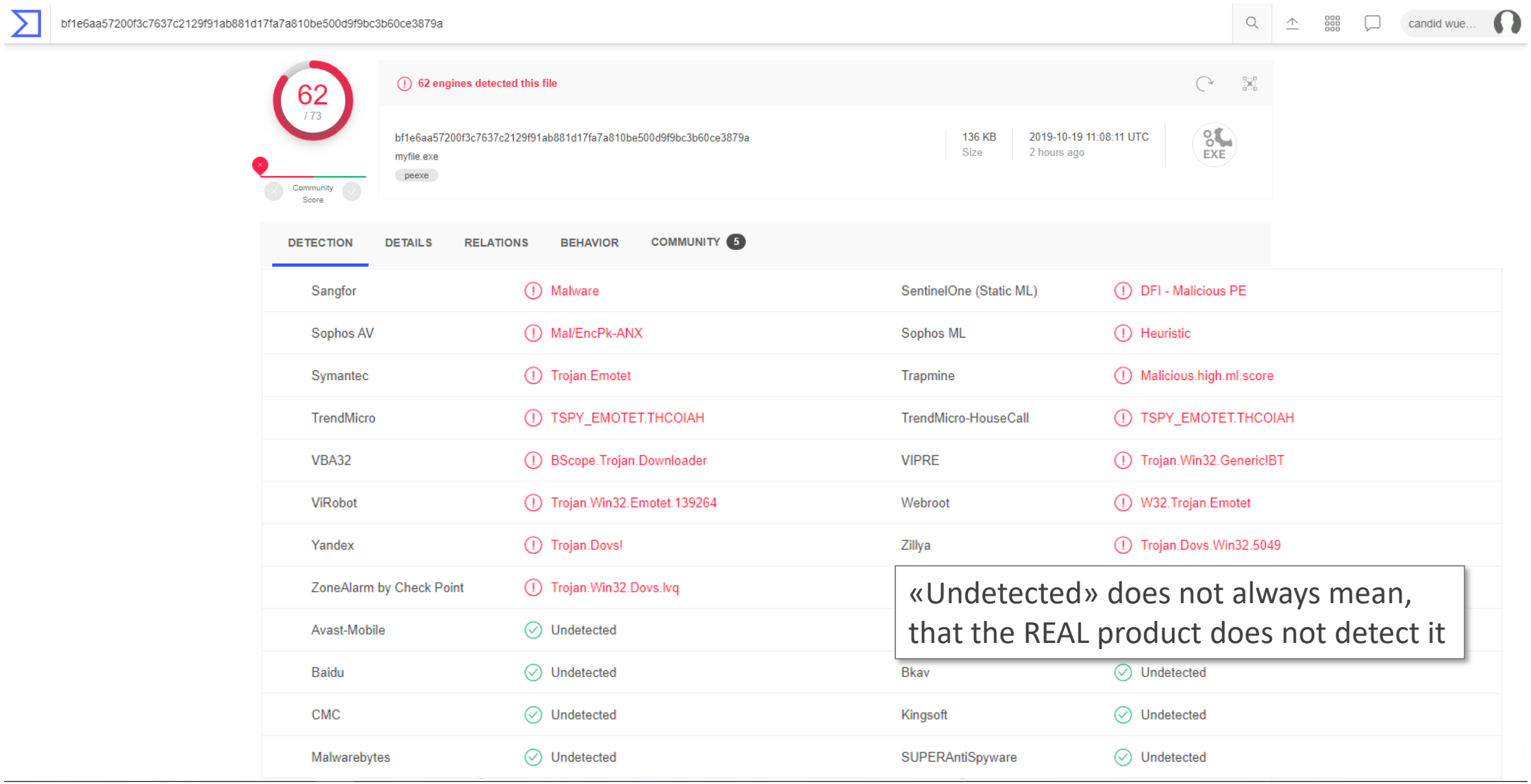
Cluster data for the big intelligence picture



Big data cloud cluster
350 TB hot-data
7 PB data
25 TB RAM
5000 vCores
150K queries/day

☺ I always learn from mistake of others who take my advice.

VirusTotal.com



☺ Nostalgia isn’t what it used to be.

Search for one or more entities here

candid wue...

ef50b6f32132114fed376859fe9c2bad4
3b45beca6d1cef144ddd141dda3e44c

Untitled Graph

Basic Properties

Type	Win32 EXE
Size	7.35 MB
First Seen	2015-10-07 01:56:47
Last Seen	2015-10-07 01:56:47
Submissions	1

Relations

It doesn't have relations.

Detections 55 / 71

ALYac
Win32.Sality.3

AVG
Win32:Kukacka

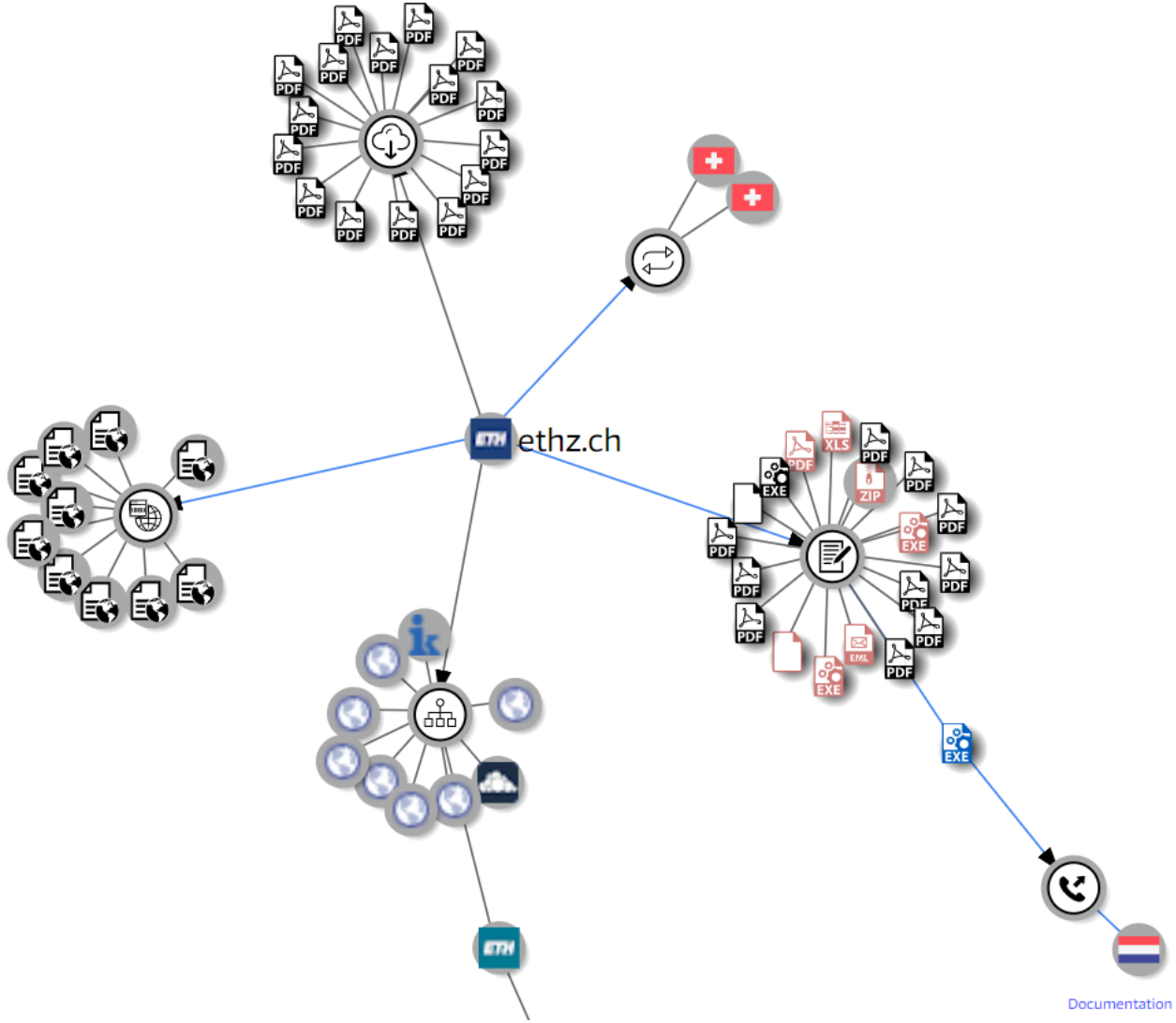
Ad-Aware
Win32.Sality.3

AegisLab
Virus.Win32.Generic.n!c

AhnLab-V3
Win32/Kashu.E

Antiy-AVL
Virus/Win32.Sality.gen

Arcabit
Win32.Sality.3



API requests: 91

Documentation | Send feedback | Premium Services & Private Keys

☺ Parachute for sale, used once, never opened!!

Failblog.org

ordom

DETECTION/PROTECTION?

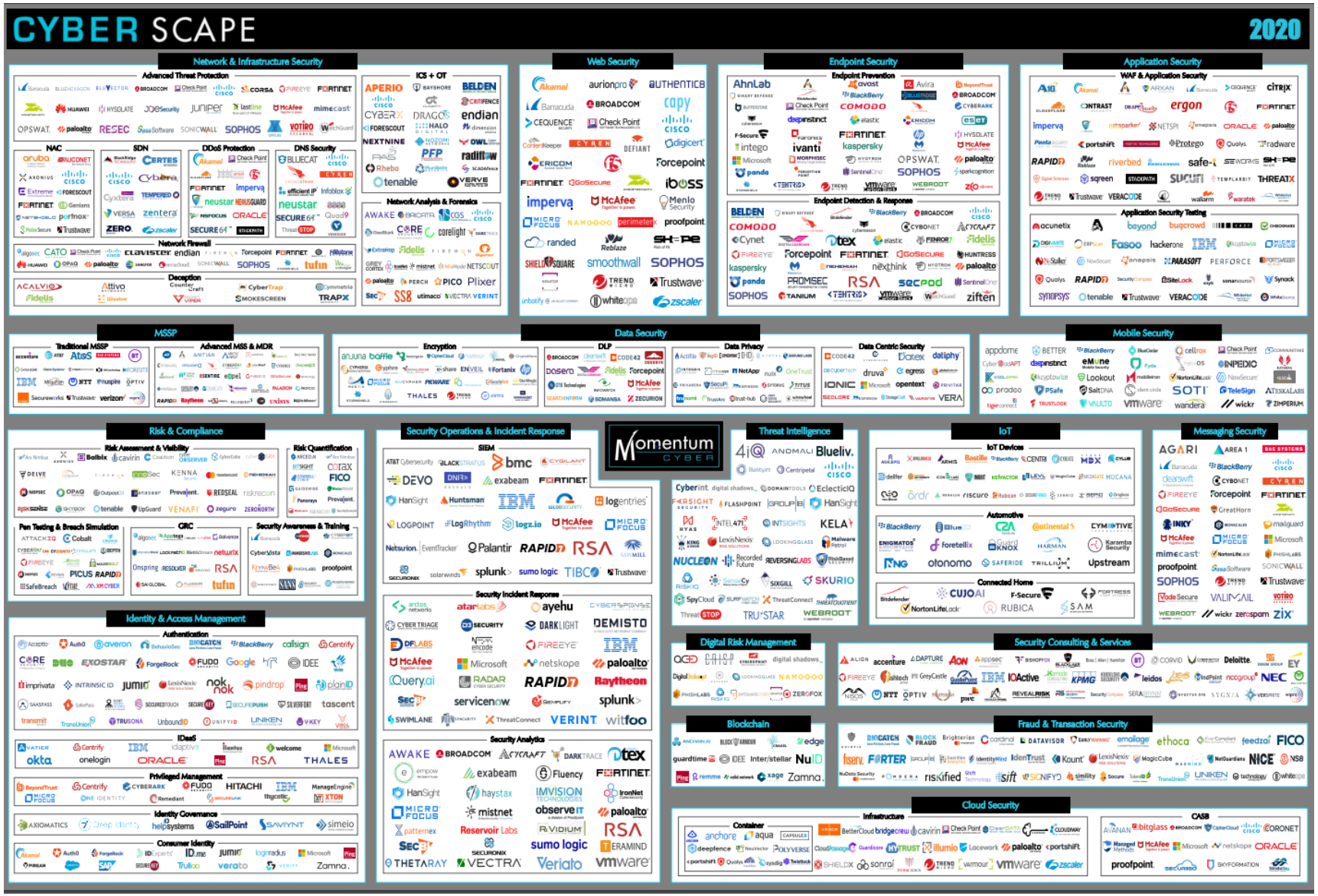
Failblog.org

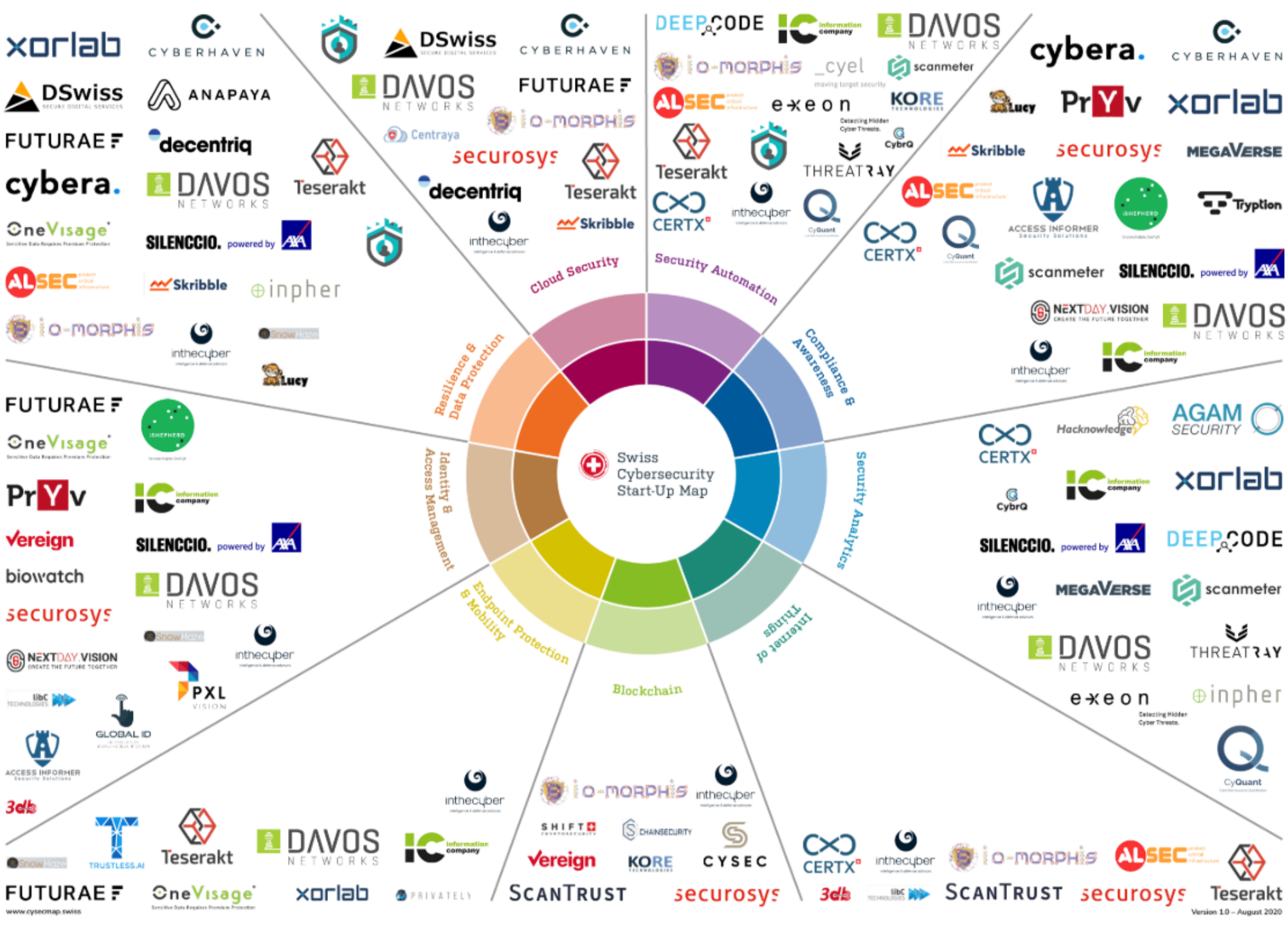
Taringa.net

A Lot of InfoSec Companies out there

What is a good solution?

- Artificial Intelligence (AI)
- Machine Learning (ML)
- Blockchain
- Military Grade
- Cloud Aware
- Big Data
- Post Quantum
- Moving target defense
- Darkweb crawling
- IoC intelligence loop
- …




Swiss Cybersecurity Start-Up Map
Cloud Security
Security Automation
Compliance & Awareness
Security Analytics
Internet of Things
Blockchain
Endpoint Protection & Mobility
Identity & Access Management
Resilience & Data Protection
www.cysecmap.swiss
Version 1.0 – August 2020

Main types of protection methods

Three main protection types – already highlighted by Fred Cohen in 1984

Pattern matching

Signatures
Static ML
Data Loss Prevention

Analysing Behavior

Anomalie detection
Post-execution ML
Web Application Firewall

Prevent unwanted access/changes

Hardening
Firewall
App isolation

Some new sub-classes have been introduced: reputation, UEBA, deception,…

How would you describe a …

Ferrari

True Positive ☑

False Positive ☒

Quick Quiz

Yes, it is possible!

Unfortunately this method

has a high false positive rate ;-)

Report ALL files as infected!

Example code:
print «This file is infected!»

☺ My software never has bugs. It just develops random features.


A detection rate WITHOUT the
false positive rate is MEANINGLESS!

GEEK.COM

alone

APPS AND SOFTWARE

Symantec says antivirus is dead and isn't a moneymaker

BY LEE MATHEWS 05.07.2014 :: 1:16PM EDT

Your car's safety features are more then just the airbag

☺ Relax, its only ONES and ZEROS!

Static File Signatures (are not dead!)

- Find unique part of a threat, generic enough to catch variants (not MD5 hash)
- 8 Million signatures in Symantec's set (many from automation)
  - Signature updates every ~7 minutes
  - Applied to files on disk, memory and network traffic
- Engine can use the context (dropper process, URL, reputation, heuristics …)
- Signatures can be stored/queried in the cloud
- Whitelisting works similar

Disadvantage:

- Reactive
- Bad with mutation or polymorphism
- Bad with dual-use tools and Living off the land

☺ Brains are wonderful, I wish everyone had one.

Different signature methods possible

- Simple group of checksums or byte arrays
- Complex ones of up to a few hundred lines of proprietary coding language. Used for example to repair file infectors.
- Indicators of Compromise **(IoC)** sharing is popular (mostly IPs & file hashes)

Example: Yara rule (malware classificator) or **Snort** for IPS or **Sigma** for logs

```
rule BadTrojan
{
    strings:
        $a = {4E 45 54 53 45 43 32 30 31 34}
        $b = {41 52 45 41 34 31}
        $c = "X:\\Projects\\ZeusFork\\Release\\ZeusFork.pdb"

    condition: ($a or $b) and $c
}
```

YARA rules

rule ransomware_exPetr {

meta:

copyright = “Kaspersky Lab”
description = “Rule to detect PetrWrap ransomware samples”
last_modified = “2017-06-27”
author = “Kaspersky Lab”
hash = “71B6A493388E7D0B40C83CE903BC6B04”
version = “1.0”

strings:

- $a1 = “MIIBCgKCAQEAxP/VqKc0yLe9JhVqFMQGwUITO6WpXWnKSNQAYT0O65Cr8PjIQInTeHkXEjfO2n2JmURWV/uHB0ZrlQ/wcYJBwLhQ9EqJ3iDqmN19Oo7NtyEUmbYmopcq+YLIBZzQ2ZTK0A2DtX4GRKxEEFLCy7vP12EYOPXknVy/+mf0JFWixz29QiTf5oLu15wVLONCuEibGaNNpgq+CXsPwfITDbDDmdrRIiUEUw6o3pt5pNOskfOJbMan2TZu” fullword wide
- $a2 = “.3ds.7z.accdb.ai.asp.aspx.avhd.back.bak.c.cfg.conf.cpp.cs.ctl.dbf.disk.djvu.doc.docx.dwg.eml.fdb.gz.h.hdd.kdbx.mail.mdb.msg.nrg.ora.ost.ova.ovf.pdf.php.pmf.ppt.pptx.pst.pvi.py.pyc.rar.rtf.sln.sql.tar.vbox.vbs.vcb.vdi.vfd.vmc.vmdk.vmsd.vmx.vsdx.vsv.work.xls” fullword wide
- $a3 = “DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED” fullword asci
- $a4 = “1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX” fullword asci
- $a5 = “wowsmith123456@posteo.net.” fullword wide

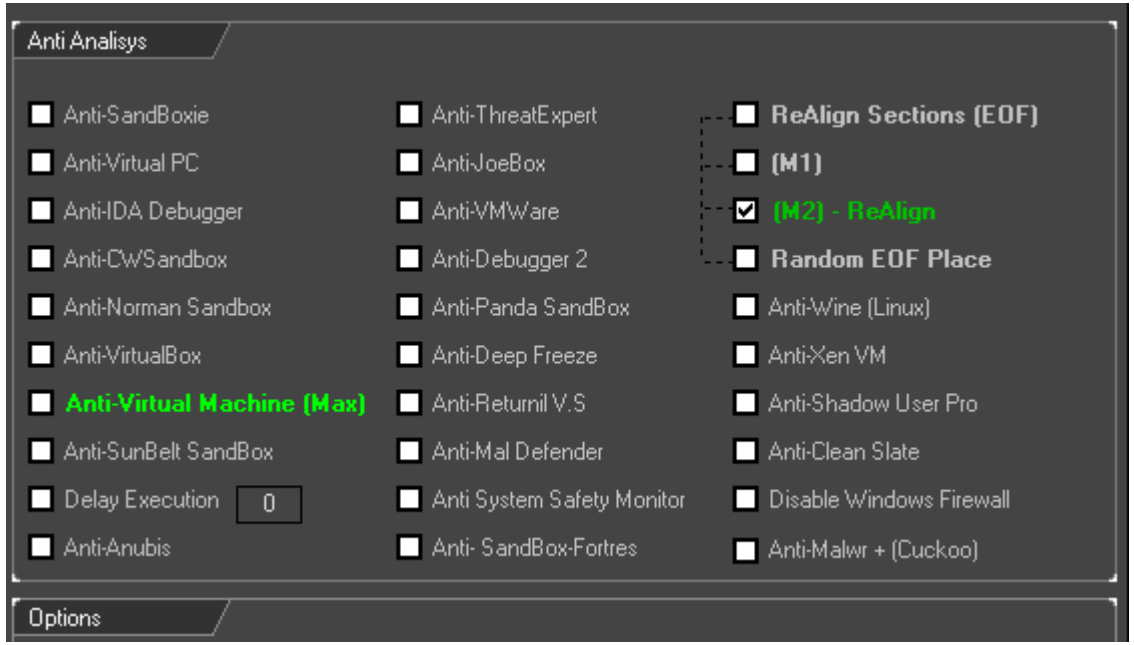
condition:

(uint16(0) == 0x5A4D) and
(filesize<1000000) and
(any of them)
}

Anti-Virus bypass tools

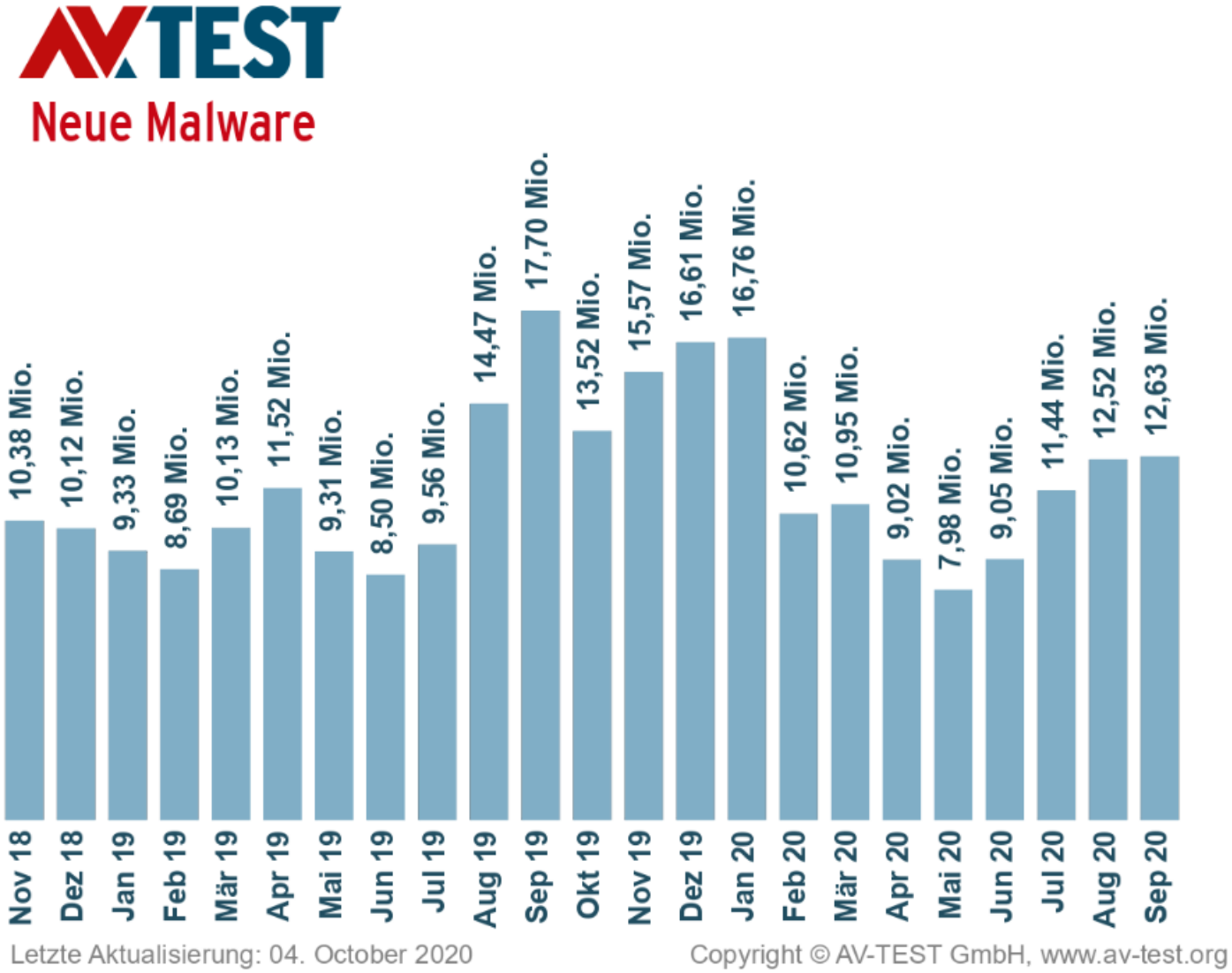
Work well against «common» signatures
But not against all methods ;-)

Similar tools for Network IDS/IPS e.g. Chiron
Working with fragmentation, flags, TTL, …



☺ He who smiles in a crisis has found someone to blame.

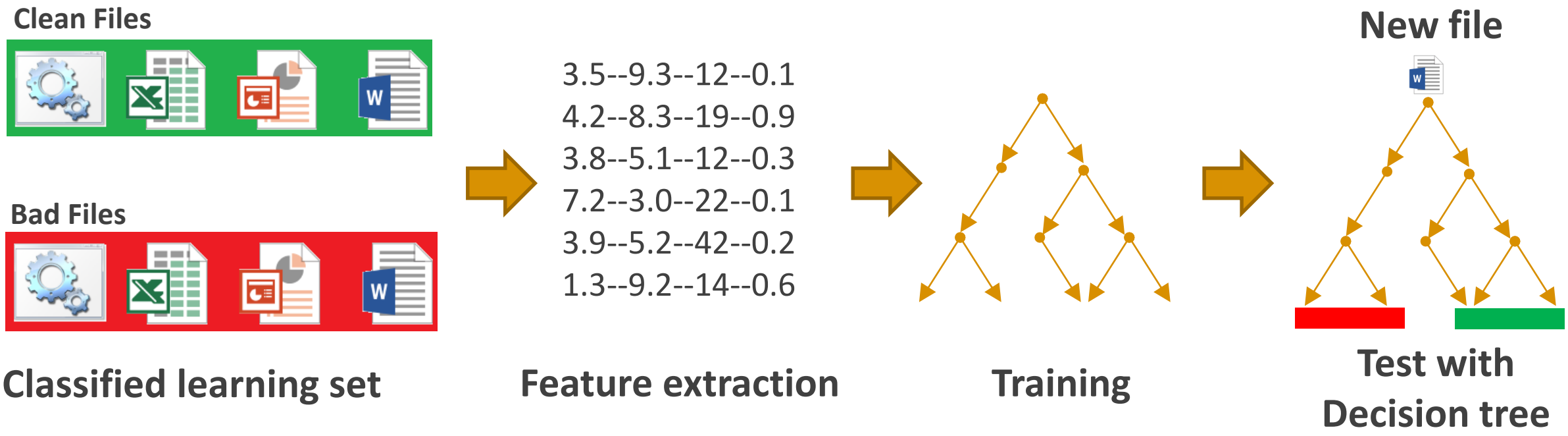
A flood of new threats every day



☺ If I wanted a warm fuzzy feeling, I'd antialias my graphics

Static analysis with Machine Learning (ML)

- Bayesian classifier tree a.k.a. Machine Learning (ML) on different file attributes
- Pre-execution (the file does not run yet)
- Does not need to be updated daily in contrast to file signatures

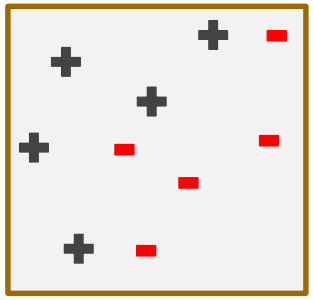


☺ I need a six month vacation, twice a year.

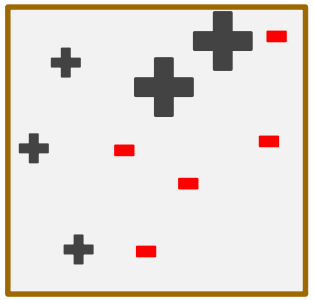
Machine Learning – Logic Regression

Goal: separate + and - with a line

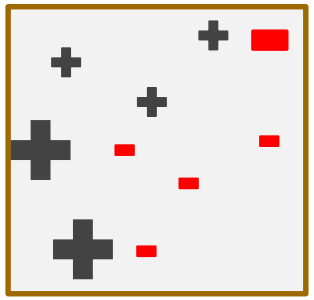
1. Iteration

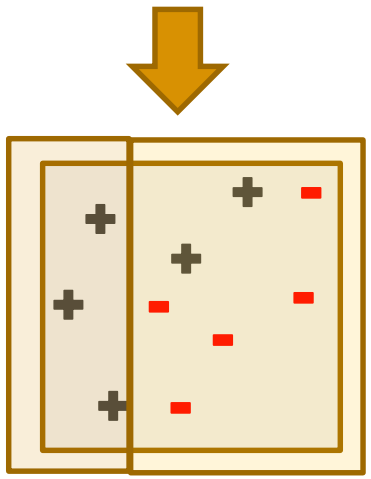


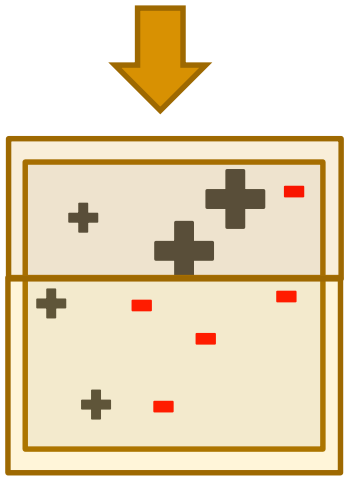
2. Iteration

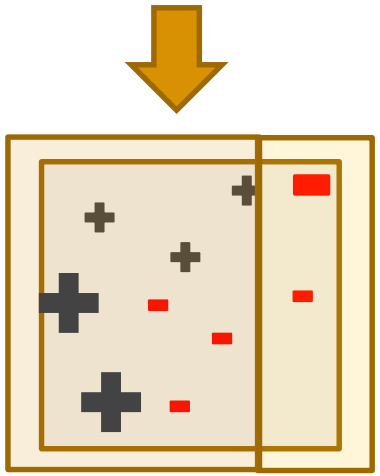


3. Iteration





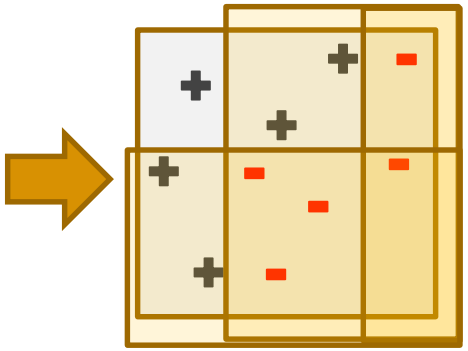




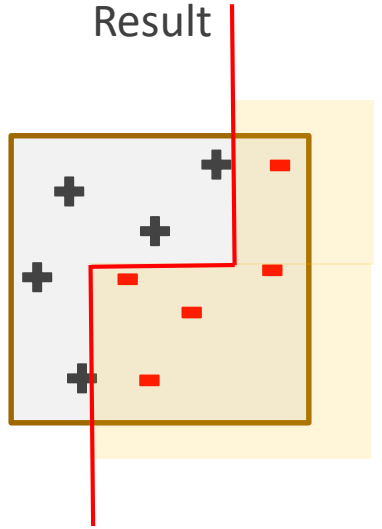
Random divider

Add weigth for false classificaton

Kombination

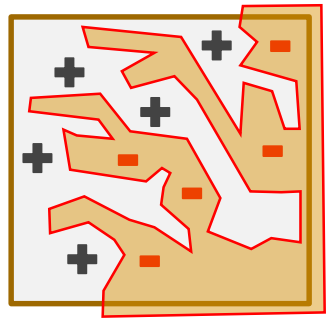


Result



Correct result, but still bad

Overfitting



Machine Learning

- Pre-execution and/or post-execution e.g. on behavior
- Machine Learning (oversimplified: prediction based on attributes)
  - Supervised learning (input attribute and test-sets are given)
  - Unsupervised learning (data mining on data with no idea about structure)
  - Neural networks (non-linear statistical data modeling tool)
  - Deep Learning (multiple layers of neural networks)
  - Artificial intelligence (behaves and reasons)

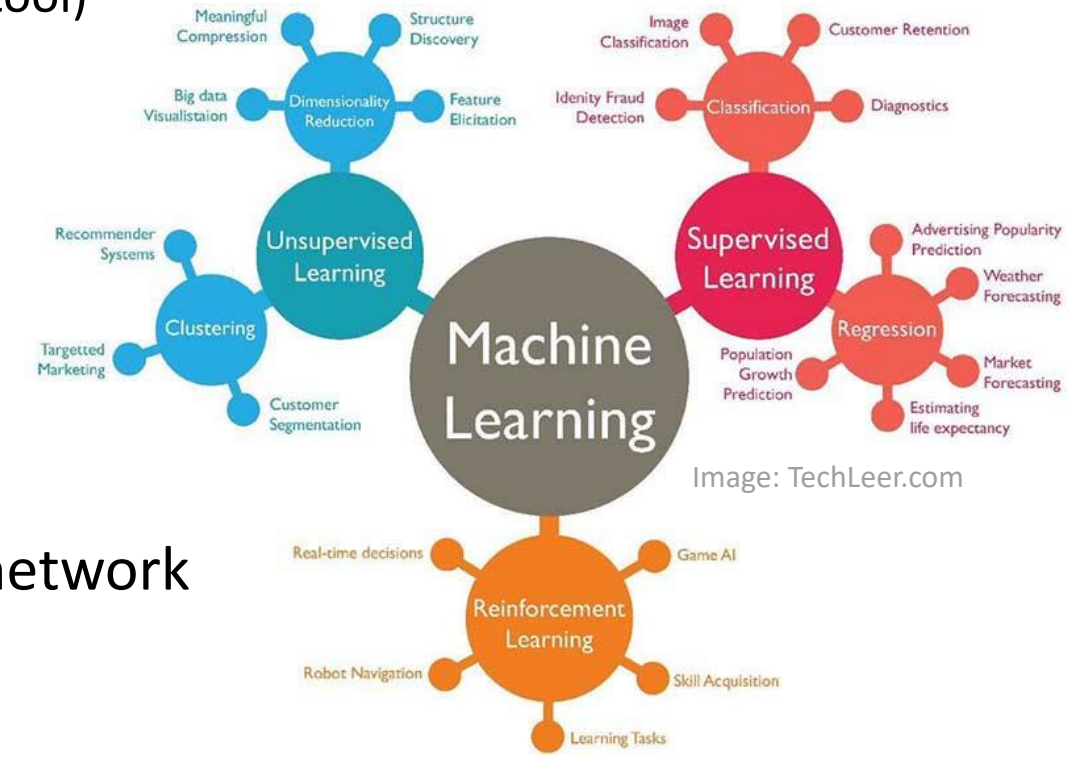


Image: TechLeer.com

Application area:

- Classification e.g. bad or good
- Clustering e.g. all ransomware variants
- Anomaly detection e.g. data exfiltration in the network

☺ Latest survey shows that 3 out of 4 people make up 75% of the world's population.

Artificial Intelligence (AI)

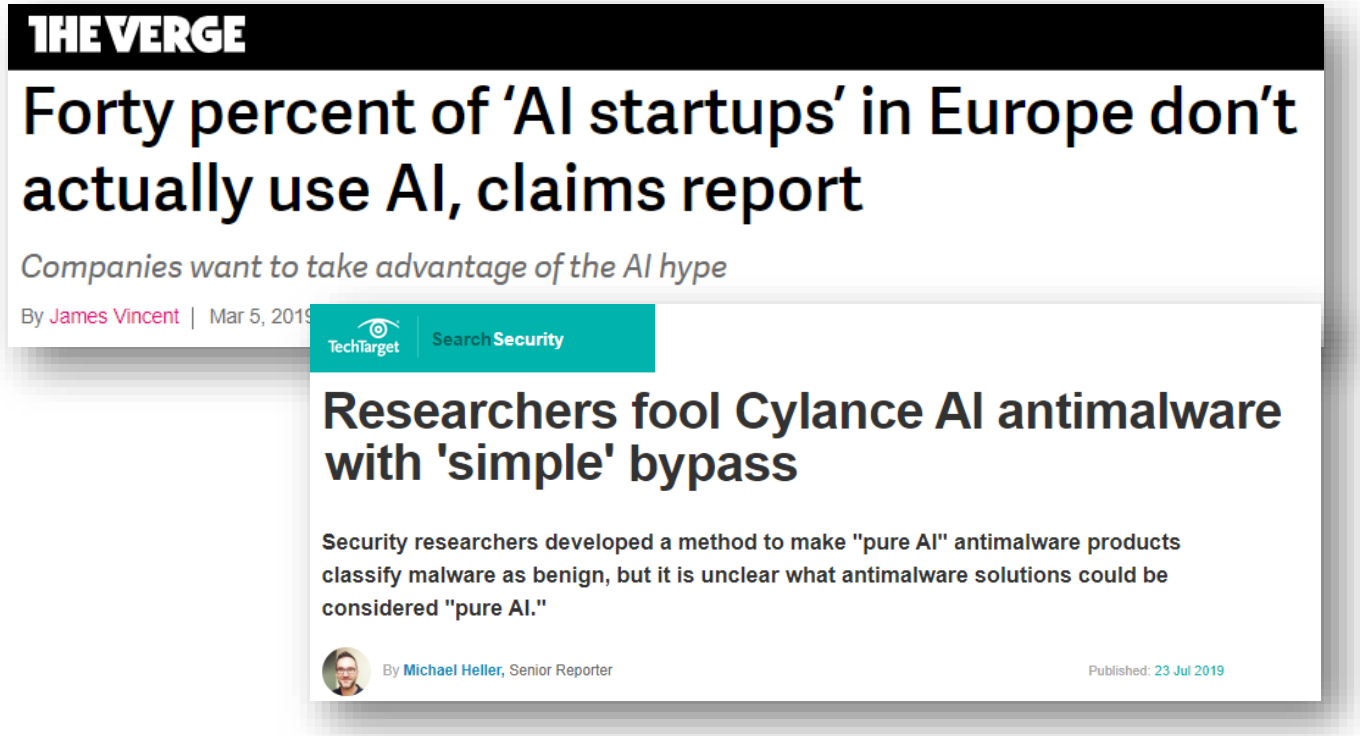
AI is next evolution step after Machine Learning (ML)

Not just learning how to solve a specific task very good (=ML),
learn how to improve itself to solve new previously unknown task (=AI)

- The aim of AI is to increase chance of success and not accuracy

Often used in protection:

- Anomaly detection
- New threat detection
- Logfile analysis / SOC

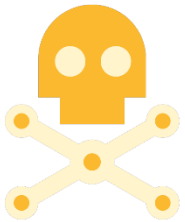


☺ I'm on a whiskey diet. I've lost three days already.

Machine Learning (ML)
Artificial Intelligence (AI/KI)

Defense

- Logfile analysis / SOC
- Anomalie detection
- APT detection with ML
- …



Offense

- ML for phishing email
- AI to modify Malware
- Deep Fake voice BEC
- …

In both groups the data quality is crutial

☺ Computers are not intelligent. They only think they are

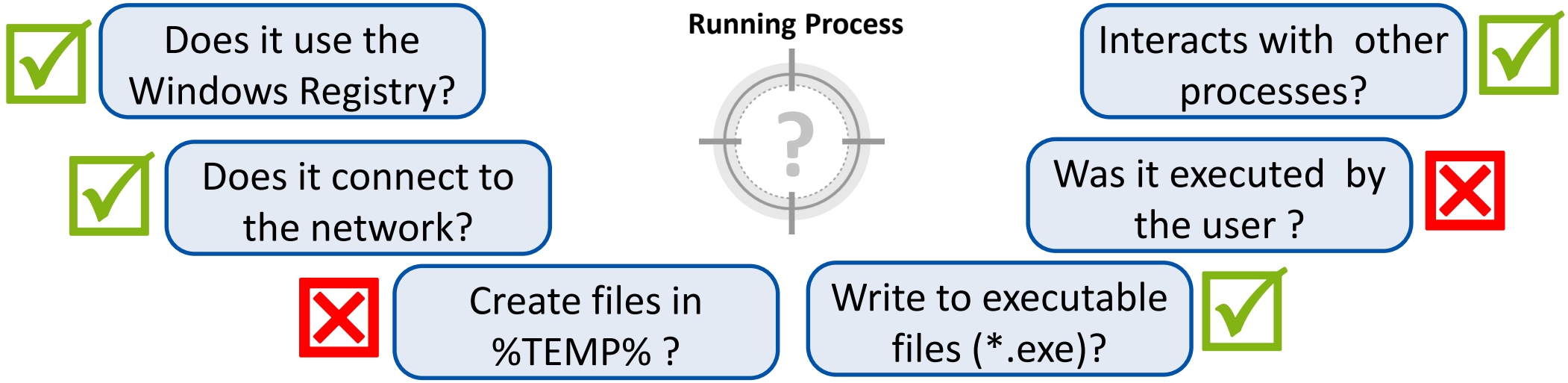
Behaviour Based Detections

Monitor WHAT a process is doing and block bad behaviour pattern

Pro 👍**:** Detect never before seen malware

Con 👎**:** Malware is already executed

Prone to False Positives (FPs)



Behavior Based Detection

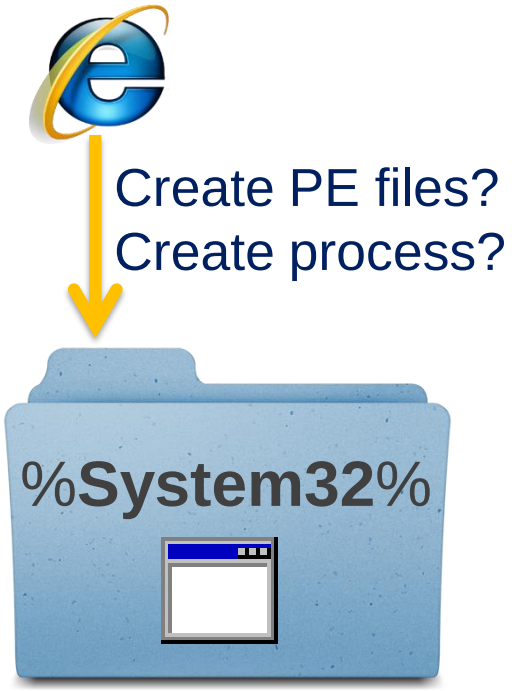
- Realtime analysis of process behavior or blackboxing in a sandbox
- Suspicious threats can be terminated or isolated
- This is a true proactive method
  = detecting previously unknown threats
- **Similar things can be applied to network attributes**

Disadvantage:
- Malware must be executed
- More prone to false positives

Behavioral Policy Lockdown / Anomaly Detection

- Define normal behavior of standard processes or network
  - Block anything that is not „normal“
  - API based, control flow graph based, network based, …
- Can protect from unknown exploits
- What is normal behavior? Difficult to know, even with ML

Disadvantage:
- Not trivial to generate policies
- False positive prone
- Might not catch standalone Trojans



File or URL Reputation

- What do we know about the file (prevalence, age, origin, …) from telemetry data
  - 80+ Billion files in the database (2019)
  - 13 Trillion lookups per day
- Each malware variant is usually only on a few systems world wide
- **Dilemma for attacker:**
  - Mutate more → bad reputation/bad prevalence → suspicious
  - Mutate less → easy detection by signatures

Disadvantage:
- Needs online connection / privacy?
- Dynamic
- Bad with custom software packages

How do you see what you do not see?

«Survivorship Bias»

How can you count, what you did not detect?

Most solutions focus on known behavior

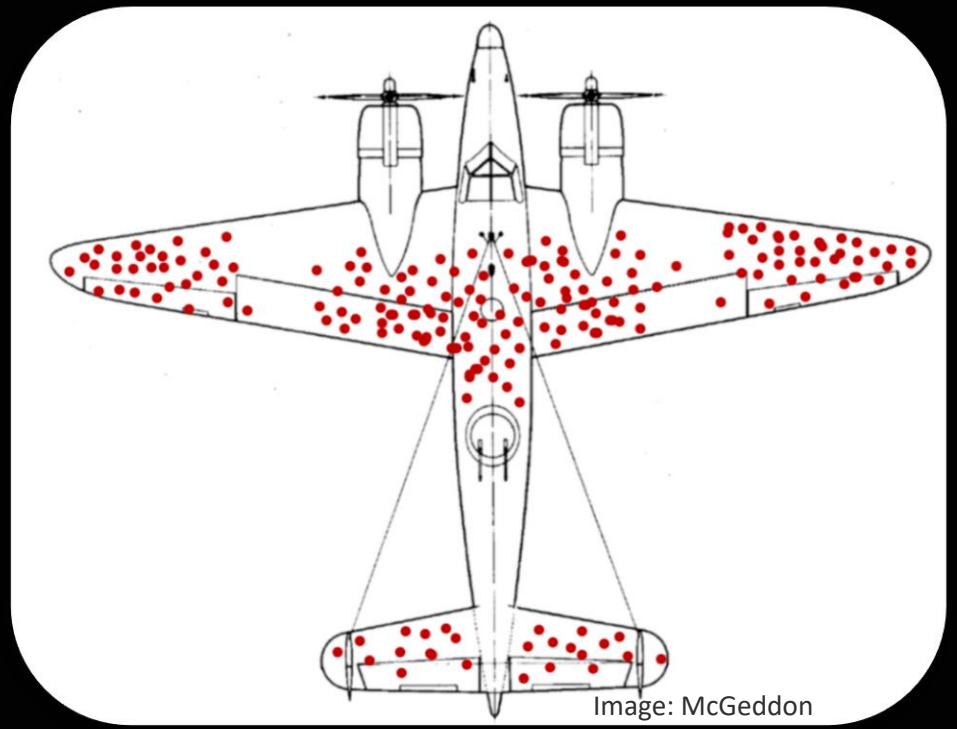


Image: McGeddon

☺ E-mail returned to sender -- insufficient voltage.

Some other protection concepts

- **Deception**
  - Honeypot like, place artifacts on system and wait till someone uses them
  - Next steps are moving target defense, obfuscation, tar pits, …
- **User Entity Behavior Analytics → Zero Trust**
  - What did the user normaly do? Is this an interaction that we can trust?
- **Endpoint Detect & Response (EDR, XDR)**
  - Forget about the blocking, just make sure that you detect it later and can remove it
- **Networkbased detection & IPS**
  - **Anomaly detections in the network** e.g. lateral movement or data exfiltration
  - **Extracting files and submitting them to sandboxes**
  - Increasingly difficult as more and more traffic is encrypted TLS/SSL and DoH/DoT


taringa.net
YOU NEED TO KNOW
WHERE TO LOOK
funny-picturess.us
ViralHog

One method alone is not enough
combine multiple methods

Network Threat Protection

Application Lockdown

Advanced Scanning

Static analyis Machine learning

File und URL Reputation

Whitelisting

Behavior Analysis

Signatures Heuristics

Sandboxing Emulator

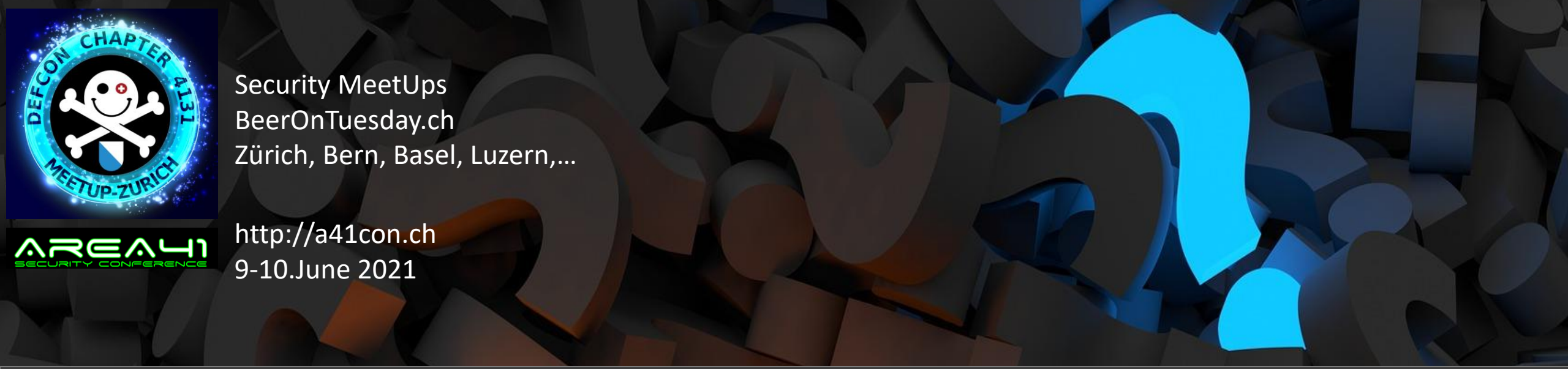
Exploit protection

☺ I didn't say it was your fault, I said I was blaming you.

Summary

- There is no “100% security”,
  but protection is still possible & needed
- If the malware executes, it can be analyzed
- Automated analysis can often be circumvented
- Artificial intelligence is not the solution to everything
- Combine multiple detection technologies
- Mixture of signatures, behavior and prevention

Snake oil? Useless? No!



Security MeetUps
BeerOnTuesday.ch
Zürich, Bern, Basel, Luzern,…

http://a41con.ch
9-10.June 2021

WHICH QUESTIONS ARE STILL OPEN?

https://bsideszh.ch/

https://www.blackalps.ch

https://insomnihack.ch

https://hacking-lab.com

THANK YOU!

Candid West
@MyLaocoon