Malware

Forensic & Analysis

21.09.2009

Oliver Karow

Security Consultant

Symantec Deutschland GmbH

Agenda

1. Introduction to Malware Forensic
2. Malware example
3. Forensics/Analysis by example
4. Time for questions

Forensic

Forensic

- From Latin adjective *forensis* = „of or before the forum“; In Roman times criminal charges were held on a public forum.
- Nowadays it means „*related to courts*“
- For us it means analysis of incidents usable in court of law

Malware

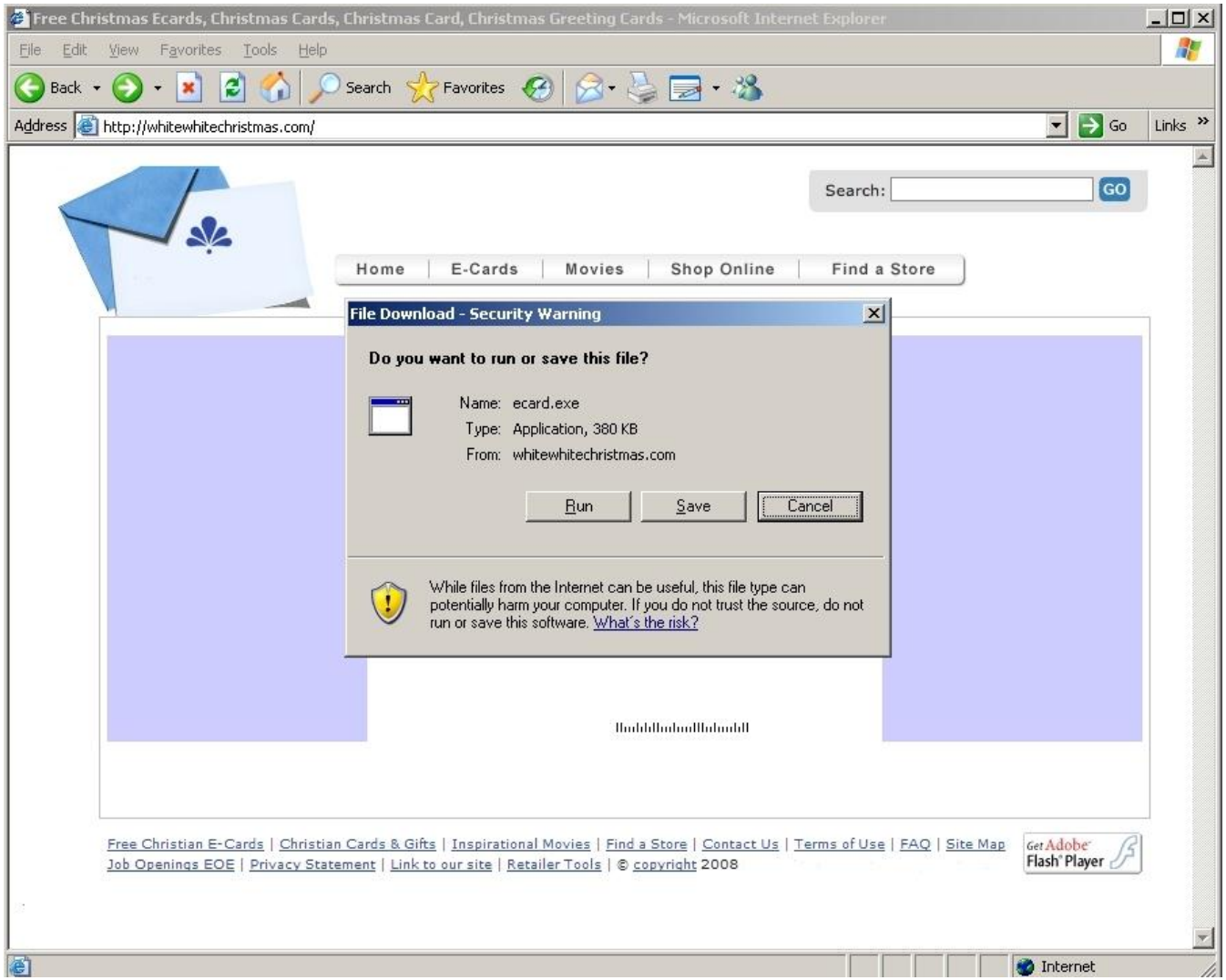
- **Malicious Software**
- **is software designed to infiltrate a computer without the owner's informed consent.**
- Includes **computer viruses, worms, trojan horses, rootkits, spyware, dishonest adware, crimeware and other malicious and unwanted software**

Objectives of Malware Analysis

- Understand the way the malware works
  - Changes on affected computer
  - Spreading techniques
  - Targets (OS‘es, Domains, etc.)
  - Command & Control Methods
- Understand the risk
  - Systems affected
  - Information manipulated/intercepted (Banking credentials, KeyLogger)
  - Bot-Net (Fishing, DoS, Spam, etc.)
- Develop mitigation strategies
  - Shutdown Drop-Zones, Mule-Accounts, etc.
  - Signatures

How does it get on your computer?

How does it get on your computer?



What does it do on your computer?

Well, thats what we want to figure out with our analysis ☺

But basically it does some of the following

- Sending Spam
- Stealing information
- Downloading other executables

What does it do on your computer?

Well, thats what we want to figure ou

But basically it does some of the foll

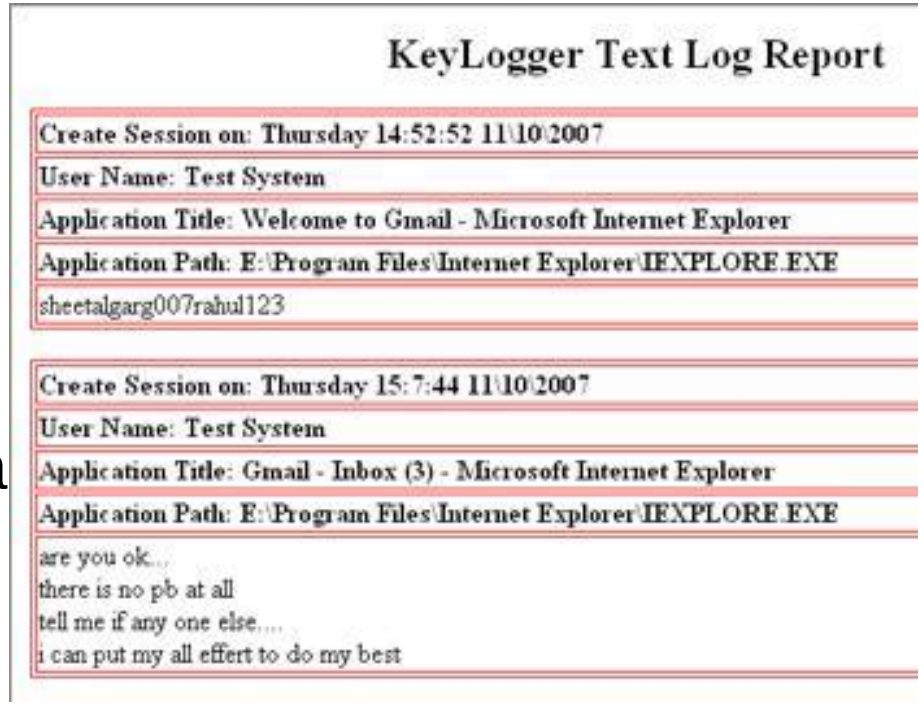
- Sending Spam
- Stealing information
- Downloading other executables

What does it do on your computer?

Well, thats what we want to figure out with our analysis ☺

But basically it does some of

- Sending Spam
- Stealing information
- Downloading other executa



KeyLogger Text Log Report

Create Session on: Thursday 14:52:52 11\10\2007
User Name: Test System
Application Title: Welcome to Gmail - Microsoft Internet Explorer
Application Path: E:\Program Files\Internet Explorer\IEXPLORE.EXE
sheetalgarg007rahul123

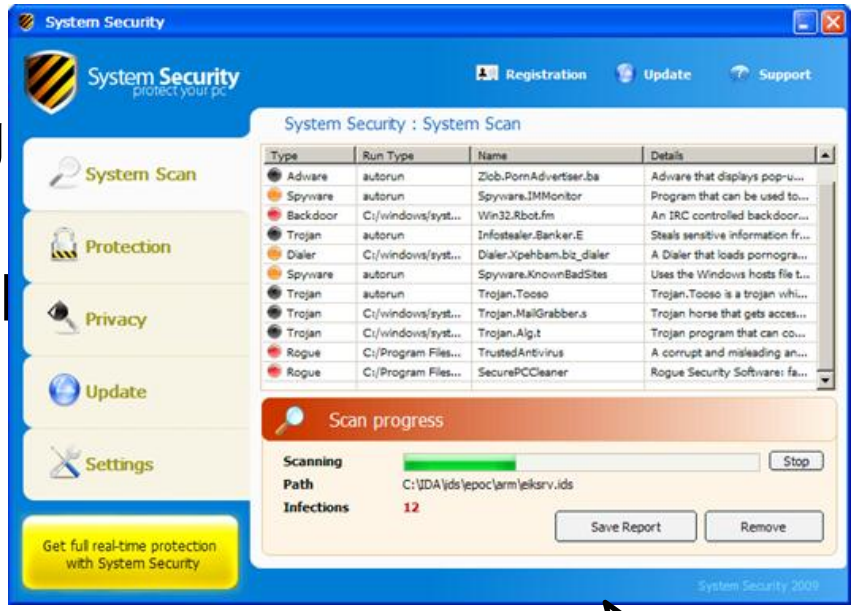
Create Session on: Thursday 15:7:44 11\10\2007
User Name: Test System
Application Title: Gmail - Inbox (3) - Microsoft Internet Explorer
Application Path: E:\Program Files\Internet Explorer\IEXPLORE.EXE
are you ok...
there is no pb at all
tell me if any one else....
i can put my all effert to do my best

What does it do on your computer?

Well, thats what we want to fig

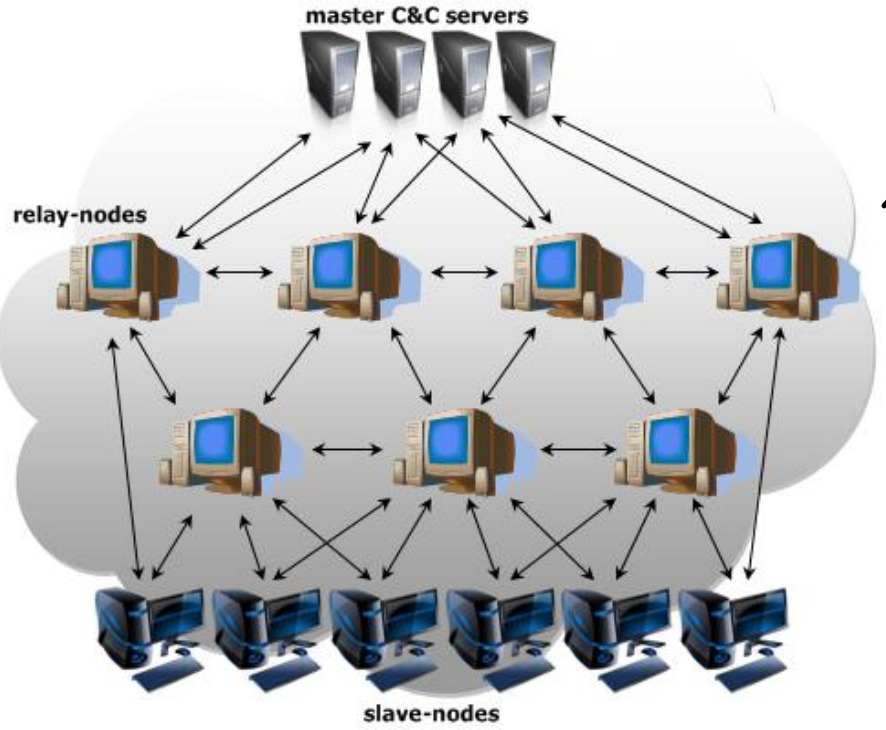
But basically it does some of t

- Sending Spam
- Stealing information
- Downloading other executables



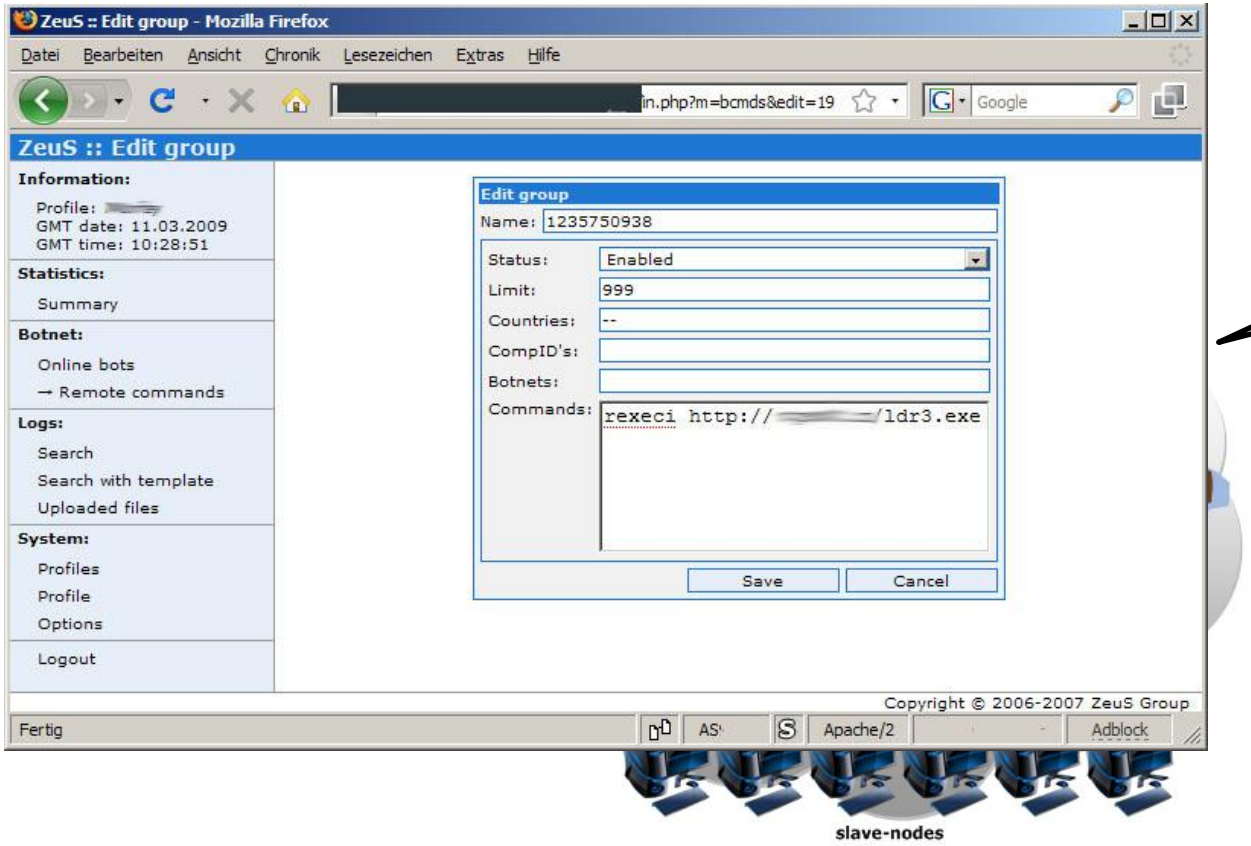
Fake AV Software

How does it get controlled



Command & Control Servers communication scheme

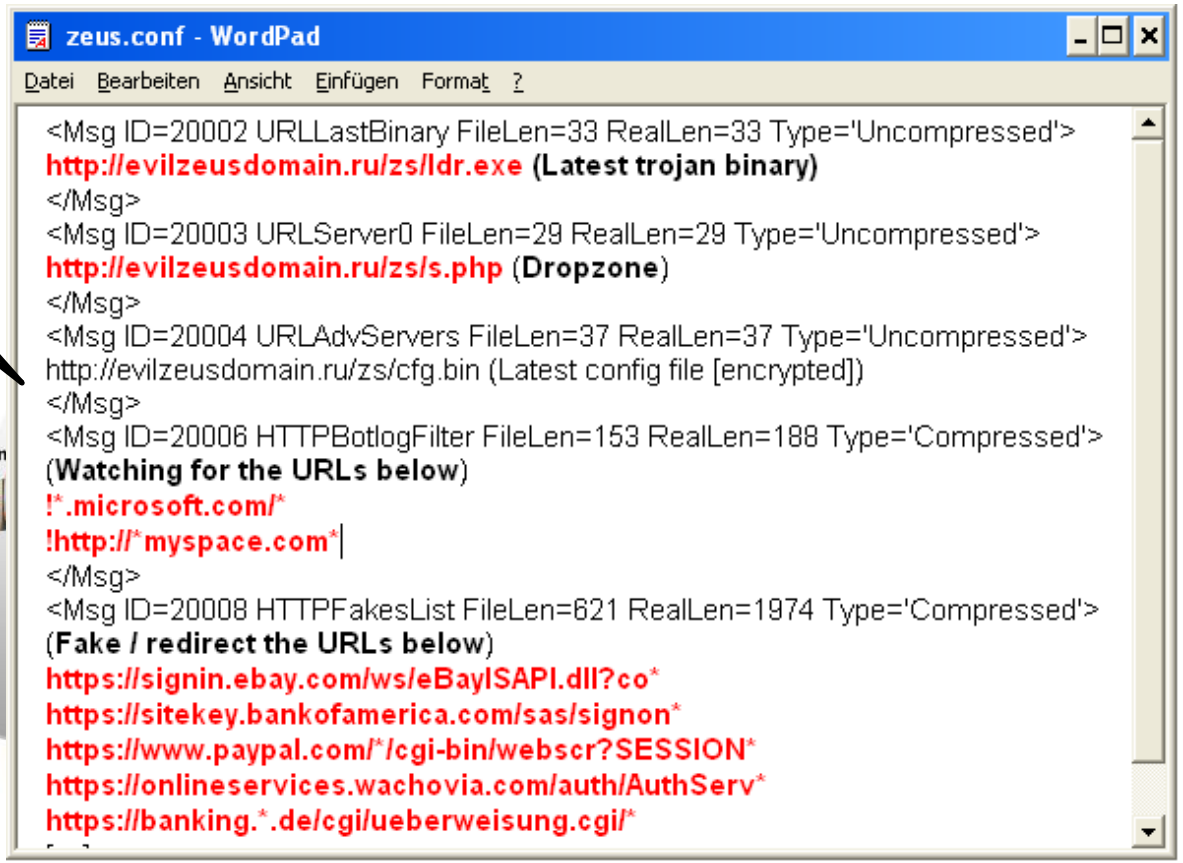
How does it get controlled



C&C Server Admin Interface

How does it get controlled

Zombie configuration file



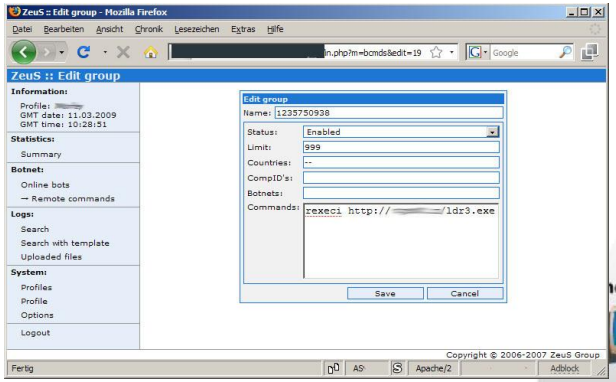
How does it get controlled

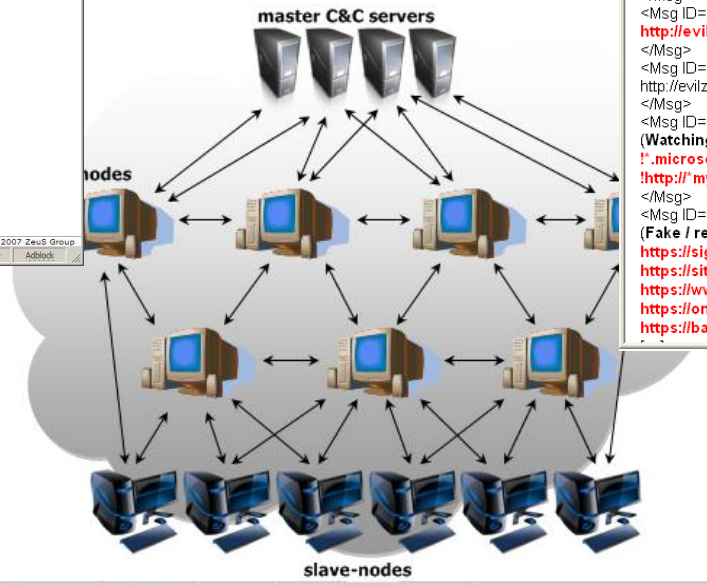
Master-Slave communication via HTTP

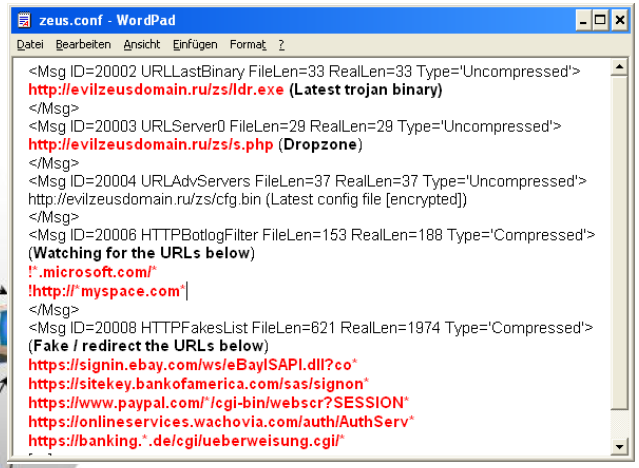
```
POST /wrax.png HTTP/1.1
Referer: Mozilla
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla
Host:
Content-Length: 978
Pragma: no-cache

a=_wAAA5W-
vwQEB5lgwY2mxP1WkBQ2d1k5xgXt4bREnc9mg7pE148JdLvX7yYYUe5wBKuuSbMccayUg2i1lhwMYh6jh_mrz
7m-
DCAfCJPc_fu6ViARKujjlnzHxEd2ujw4rsxMT_xVZGCmaHW6kTG8GmrM70X295B4Kyra9MvQ6hDF9m6xe6ybo
oCPoqLly5KeeFJ5Pmn8UGtxRnFzqhT7mD2NksLK2CdHZTwq6_
17QRkPQuxAaRkQUnqc3gWP9W2SQIn6UoHy5jDWFF_xU5HDQRafFIhA4eGbR0nR8nQUXU7UqAnXDi3udsgHod3
b7Hd1n3LuWozcJ8HUXhIcxydqOYFUo978oKcxCspaoEv_EKUtocriBEnO9OiO_jFdpHGMuukCqk38i8t41c_A
c809ImONeNEUHKMxhSWFyCrQVqEKYc__NT_bRrTeobM8s9gac6PpBM5xJ22Q3jlO_
9o_uvOK5nvmiismio6hAAosq5sjHKQZFDhTnkIBNSOJJdRDf8h6oxCtxN8ng4SxXuyt_FIOCtO8V3WuAa1yxT
DT60r92QZVXNTy29wrQH-5xfcEkHHaPSHpthGxTTUzETUl4AF1NqqEze4frSVV35h020-5KanG9id7n-
kW4xaeP2zwz6Cv2415FLaAPAP5g2QQTMmC3YGG_OyKZpHRh7ZUw-Tk9HxfTxnwW2LmefaZkRrgv-
es1w1KGOjmqjdblWhtcob4ekvAeFjnQu-8AV-ljTEtXhG9QKbqoYaiy_jF2pP2jOS4NPB-
4GzxnFEeuqlHcBNs16TjbVleE8rLa_WAcQYUik9ooCl0uBYcKH3yUKbLQ9KrCmTCBamXICPOCFeG60-
flGAElQR9lyRZk6-dNOy6J-
Xev345ASPHBHa4hQOH_ZiQwdffu2ZSjQLiAVJrcMwfwhaKaZkra2MUueOP5iak24JF1sZaBp8QQwOGoNMx3yS
MC2A&b=AAAAAA
```

slave-nodes

How does it get controlled



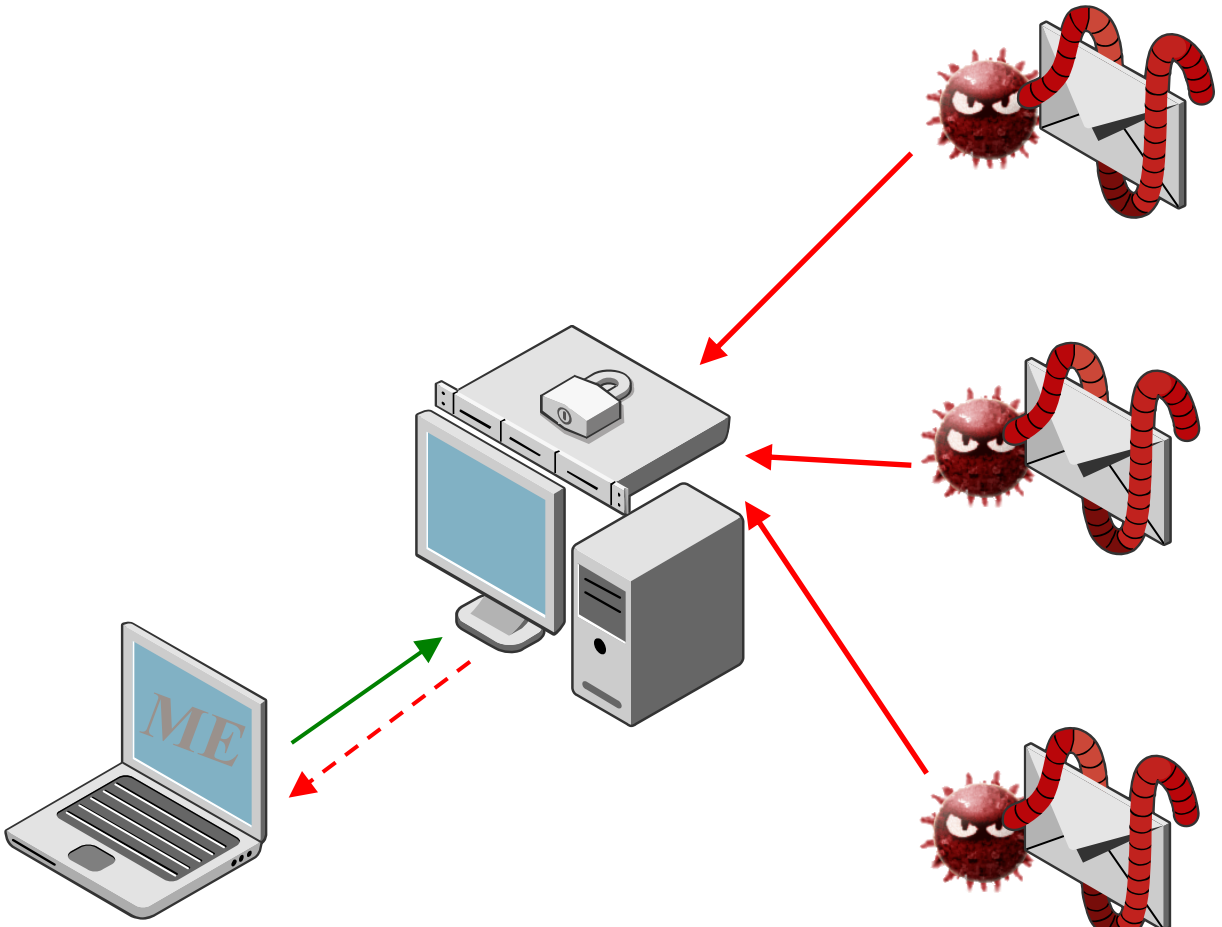





```
POST /wrax.png HTTP/1.1
Referer: Mozilla
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla
Host: [redacted]
Content-Length: 978
Pragma: no-cache

a=_wAAASW-
vwQEB5lgWYXmxP1WkBQ2d1k5xgXt4bREnc9mg7pE148JdLvX7yYYUe5wBKuuSbMccayUg2i1lhwMYh6jh_mrz
7m-
DCAfCJPc_fu6ViARKujjlnzHxEd2ujw4rsxMT_xVZGCmaHW6kTG8GmrM70X295B4Kyra9MvQ6hDF9m6xe6ybo
oCPoqLly5KeeFJ5Pmn8UGtxRnFzqhT7mD2NksLK2CdHZTwq6_
17QRkPQuxAaRkQUnqc3gWP9W2SQIn6UoHy5jDWFF_xU5HDQRafFIhA4eGbROnR8nQUXU7UqAnXDi3udsgHod3
b7Hd1n3LuWozcJ8HUXhIcxydqOYFUo978oKCxCspaoEv_EkUtocriBEnO9OiQ_jFdpHGMuukCqk38i8t41c_A
c809ImONeNEUHKMxhSWFyCrQVqEKYc__NT_bRrTeobM8s9gac6PpBM5xJ22Q3jlO_
9o_uvOK5nvmiismio6hAAosq55jHKQZFDhTnkIBNSOJJdRDf8h6oxCtxN8ng4SxXuyt_FIOCtO8V3WuAa1yxT
DT6Or92QZvXNTy29wrQH-SxfcEkHHaPSHpthGxTTUzETUl4AF1NqqEze4fr5VV35h020-5KanG9id7n-
kW4xaePzZwz6Cv241SFLaAPAP5g2QQTMmC3YGG_OyKZpHRh7ZUw-Tk9HxfTxnwW2LmefaZkRrgv-
es1w1KGOjmqjdblWhtcob4ekvAeFjnQu-8AV-ljTEtXhG9QKbqoYaiy_jF2pP2jOS4NPB-
4GzxnFEeuqlHcBNs16TjbVleE8rLa_WAcQYUik9ooCl0uBYcKH3yUkbLQ9KrCmTCBamXICPOCFeG60-
flGAElQR9lyRZk6-dN0y6J-
Xev345ASPHBHa4hQ0H_ZiQwdffu2ZSjQLiAVJrcMwfwhaKaZkra2MUue0P5iak24JF1sZaBp8QQwDGoNMx3yS
MC2A&b=AAAAAA
```

Malware Sample Analysis

- We need a sample to analyse



Isolated binary

Forensic HDD-Image

Honeypots Web Crawler

VirusTotal & Co

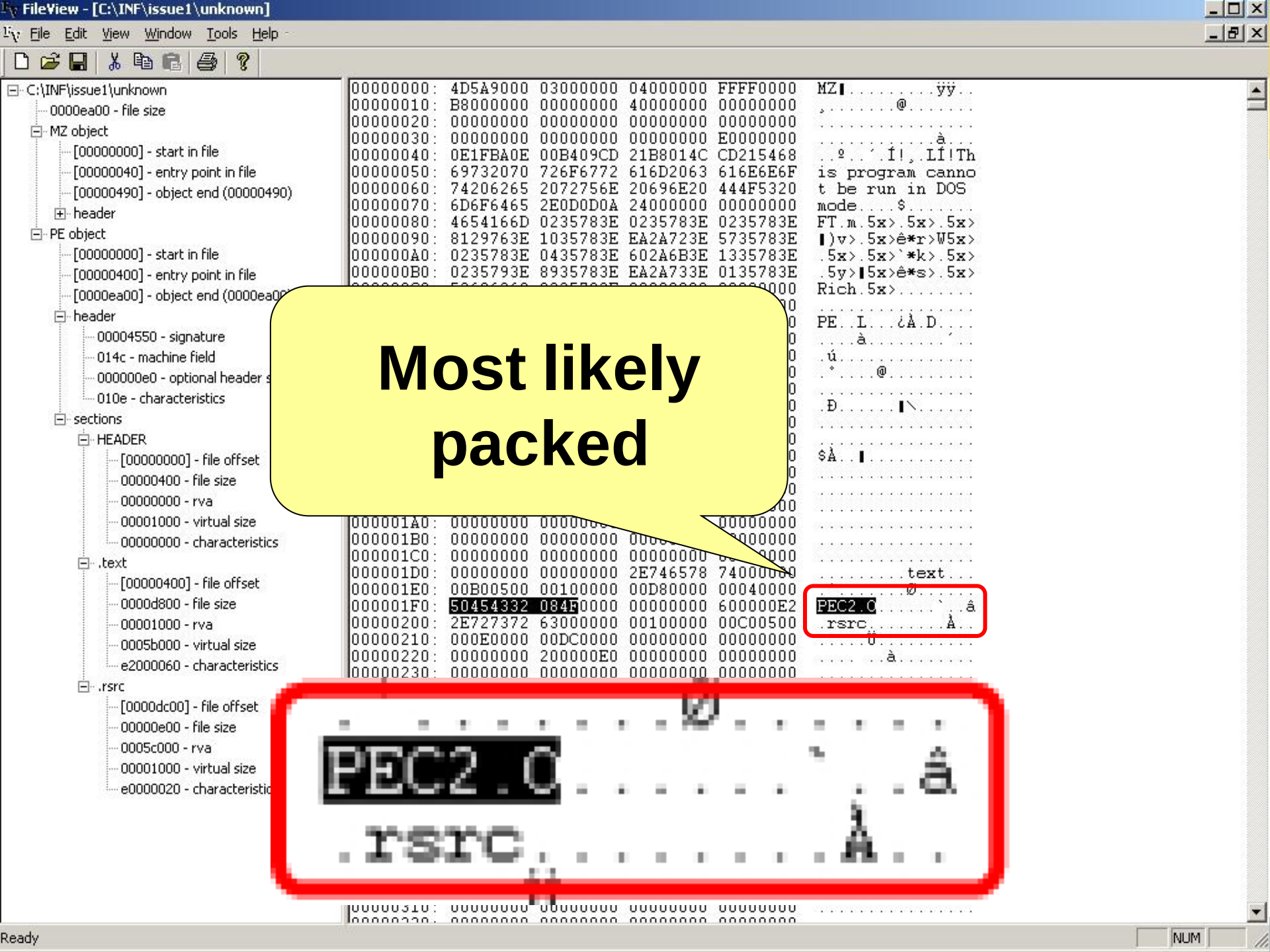
- Good indication if something is malicious
- But only signature are tested! No real behavior test!
- No detection does NOT mean product does not detect it
- Better use online sandboxes like http://threatexpert.com/

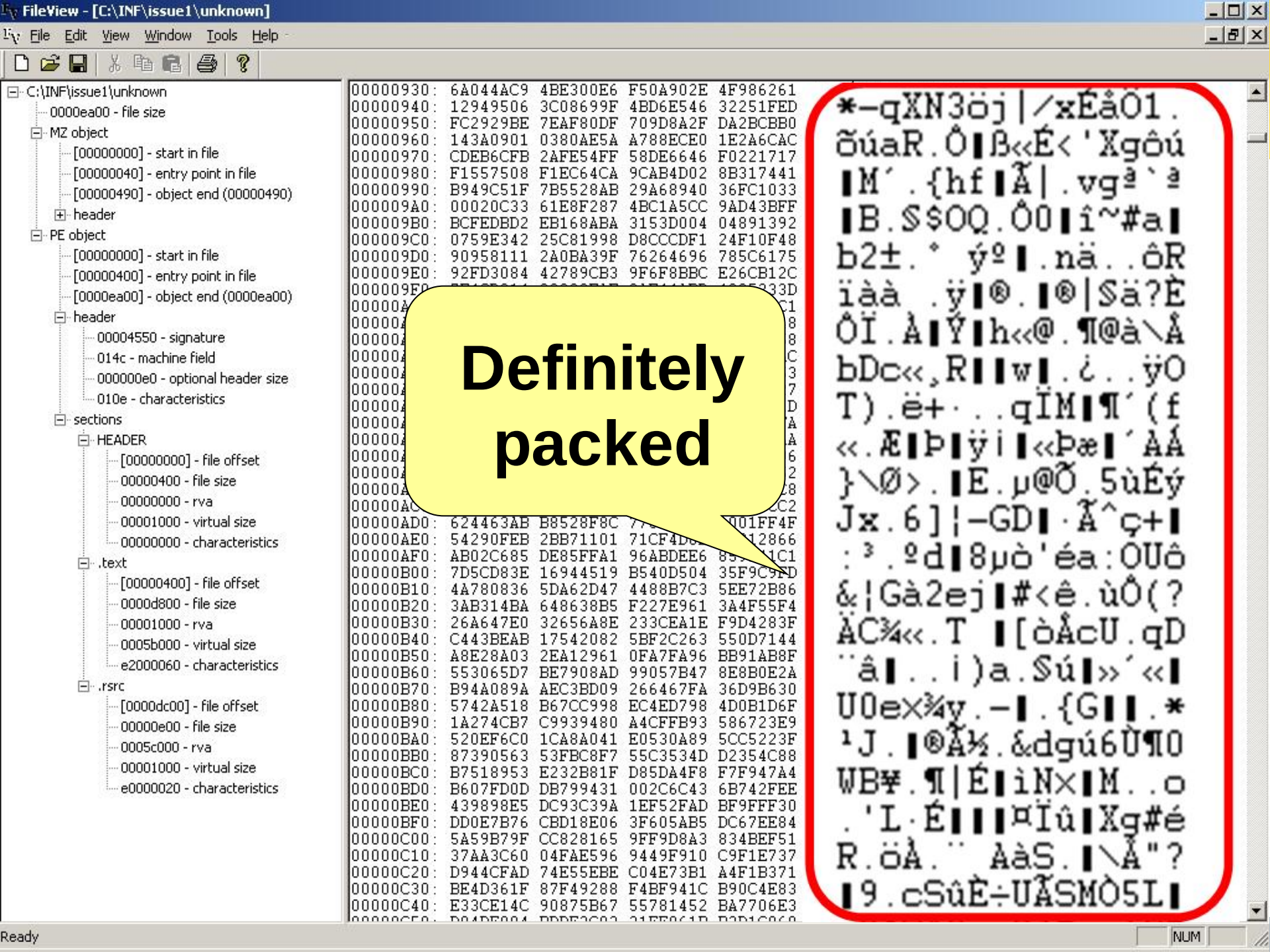
Antivirus	Version	Last Update	Result
Ikarus	T3.1.1.8	2007.07.30	Trojan-Spy.Win32.Bancos.aam
Kaspersky	4.0.2.24	2007.07.30	-
McAfee	5085	2007.07.27	-
Microsoft	1.2704	2007.07.30	-
NOD32v2	2428	2007.07.30	-
Norman	5.80.02	2007.07.30	-
Panda	9.0.0.4	2007.07.29	Suspicious file
Rising	19.34.02.00	2007.07.30	-
Sophos	4.19.0	2007.07.26	-
Sunbelt	2.2.907.0	2007.07.28	VIPRE.Suspicious
Symantec	10	2007.07.30	Trojan.Gpcoder.E
TheHacker	6.1.7.158	2007.07.30	-

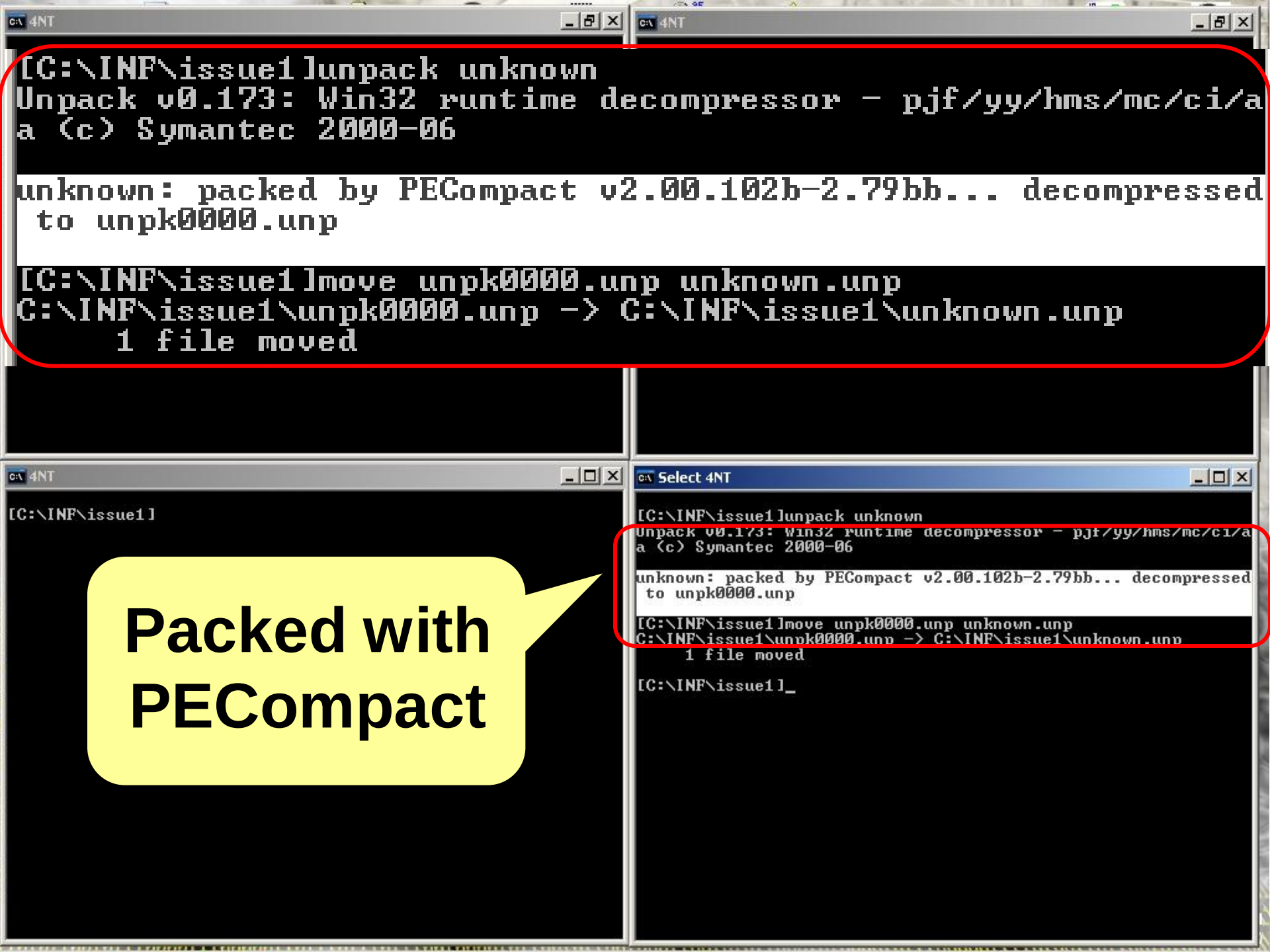
symantec

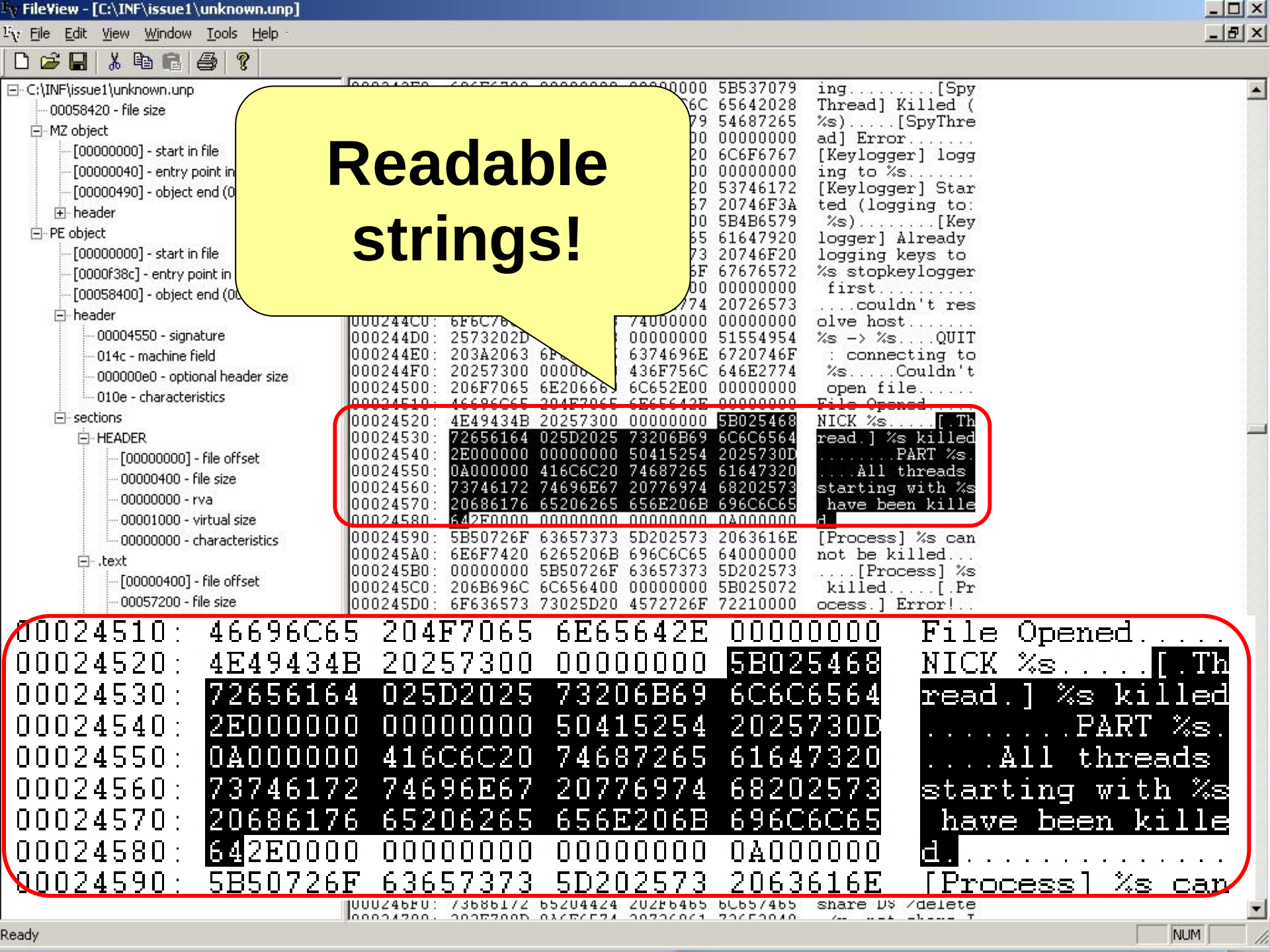
Confidence in a connected world.

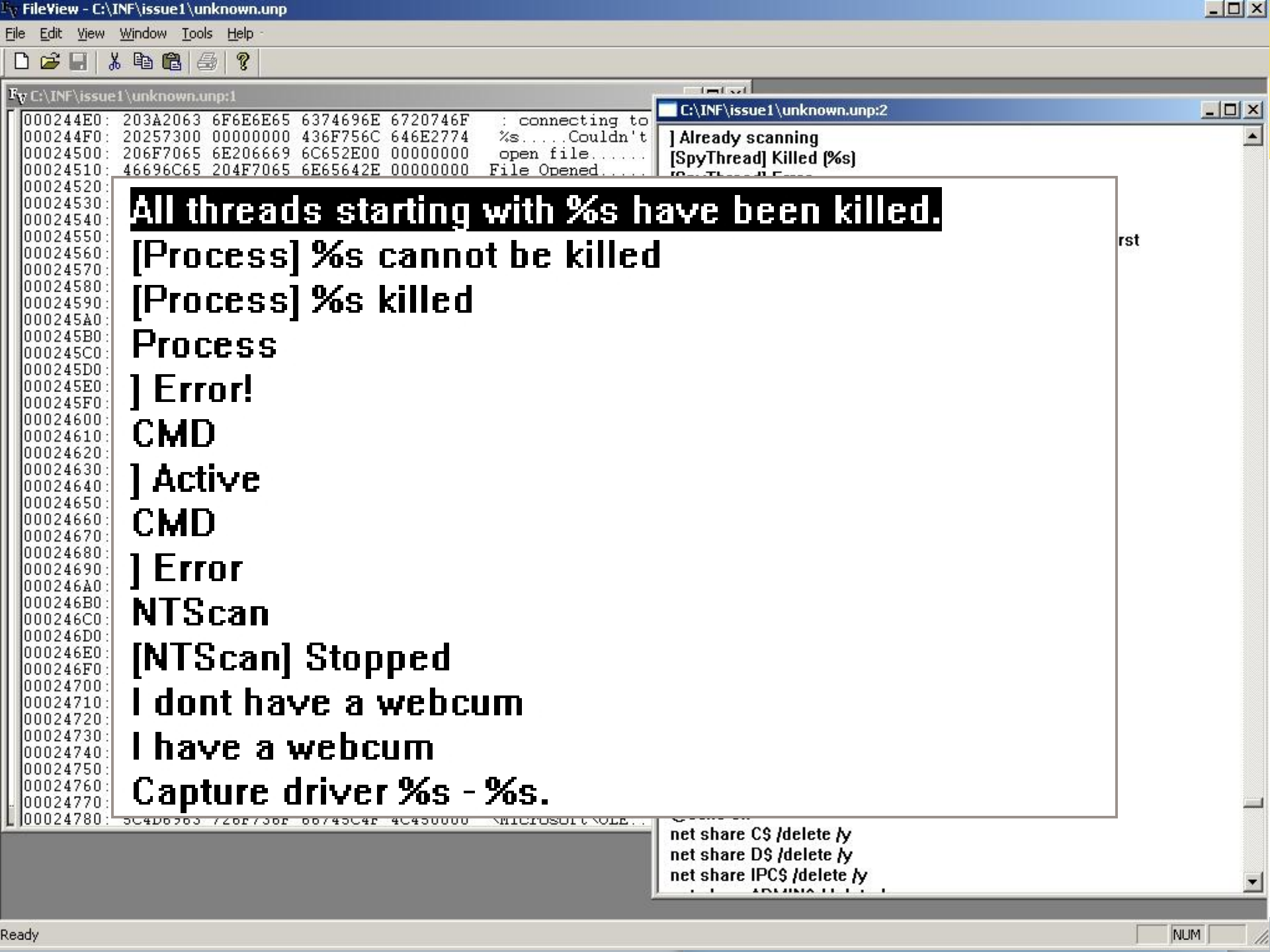
Peeking with a Hex-Editor


FileView - [C:\INF\issue1\unknown]
File Edit View Window Tools Help
C:\INF\issue1\unknown
0000ea00 - file size
MZ object
[00000000] - start in file
[00000040] - entry point in file
[00000490] - object end (00000490)
header
PE object
[00000000] - start in file
[00000400] - entry point in file
[0000ea00] - object end (0000ea00
header
00004550 - signature
014c - machine field
000000e0 - optional header s
010e - characteristics
sections
HEADER
[00000000] - file offset
00000400 - file size
00000000 - rva
00001000 - virtual size
00000000 - characteristics
.text
[00000400] - file offset
0000d800 - file size
00001000 - rva
0005b000 - virtual size
e2000060 - characteristics
.rsrc
[0000dc00] - file offset
00000e00 - file size
0005c000 - rva
00001000 - virtual size
e0000020 - characteristic
Most likely packed
00000000: 4D5A9000 03000000 04000000 FFFF0000 MZ▌.....ÿÿ..
00000010: B8000000 00000000 40000000 00000000 ¸.......@.......
00000020: 00000000 00000000 00000000 00000000 ....
00000030: 00000000 00000000 00000000 E0000000 ....à...
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: 4654166D 0235783E 0235783E 0235783E FT.m.5x>.5x>.5x>
00000090: 8129763E 1035783E EA2A723E 5735783E ▌)v>.5x>ê*r>W5x>
000000A0: 0235783E 0435783E 602A6B3E 1335783E .5x>.5x>`*k>.5x>
000000B0: 0235793E 8935783E EA2A733E 0135783E .5y>▌5x>ê*s>.5x>
Rich.5x>........
PE..L...¿À.D....
....à.........´..
.ú..............
.°....@.........
Ð.....▌\.....
$À..▌...........
000001D0: 00000000 00000000 2E746578 74000000 ....text...
000001E0: 00B00500 00100000 00D80000 00040000 ....°...Ø.....
000001F0: 50454332 2E430000 00000000 600000E2 PEC2.C......`..â
00000200: 2E727372 63000000 00100000 00C00500 .rsrc.........À..
00000210: 000E0000 00DC0000 00000000 00000000 .....Ü..........
00000220: 00000000 200000E0 00000000 00000000 .... ..à.........
00000230: 00000000 00000000 00000000 00000000 ....
PEC2.C
rsrc

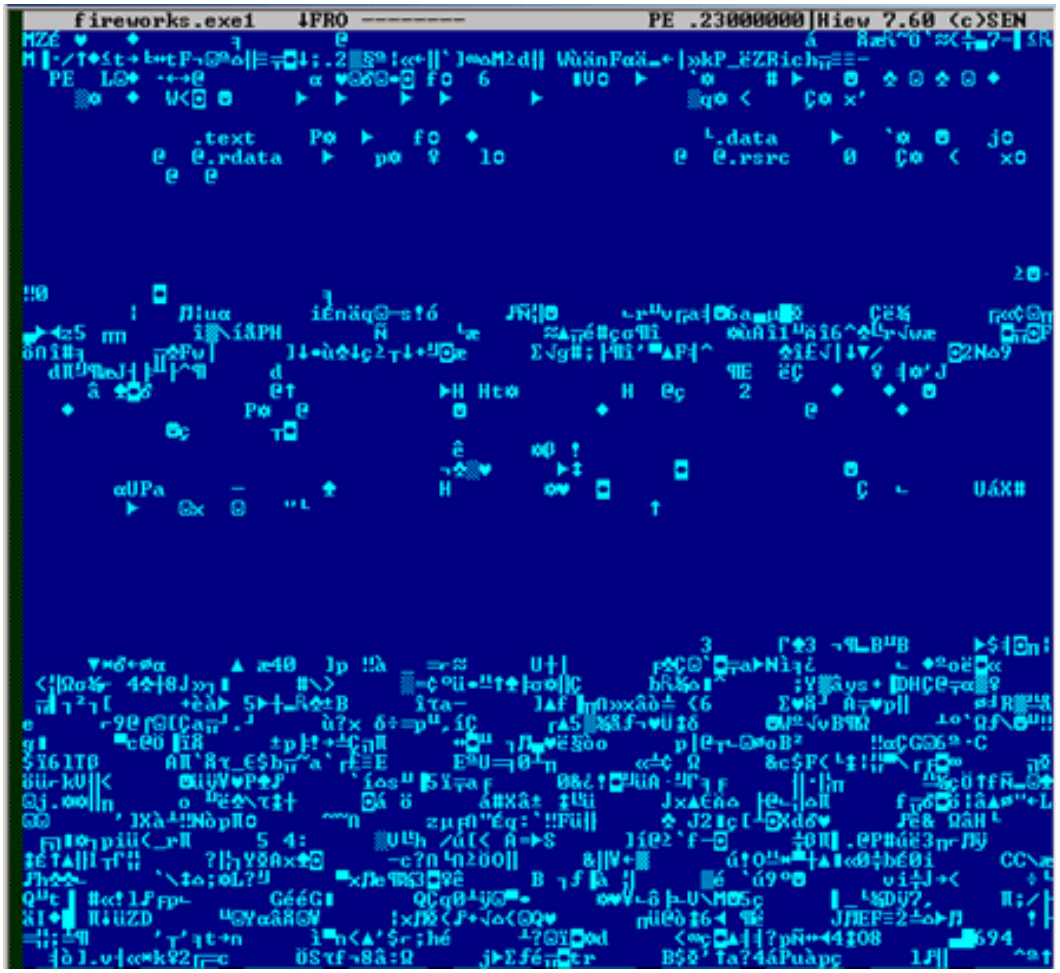

FileView - [C:\INF\issue1\unknown]
File Edit View Window Tools Help
C:\INF\issue1\unknown
0000ea00 - file size
MZ object
[00000000] - start in file
[00000040] - entry point in file
[00000490] - object end (00000490)
header
PE object
[00000000] - start in file
[00000400] - entry point in file
[0000ea00] - object end (0000ea00)
header
00004550 - signature
014c - machine field
000000e0 - optional header size
010e - characteristics
sections
HEADER
[00000000] - file offset
00000400 - file size
00000000 - rva
00001000 - virtual size
00000000 - characteristics
.text
[00000400] - file offset
0000d800 - file size
00001000 - rva
0005b000 - virtual size
e2000060 - characteristics
.rsrc
[0000dc00] - file offset
00000e00 - file size
0005c000 - rva
00001000 - virtual size
e0000020 - characteristics
00000930: 6A044AC9 4BE300E6 F50A902E 4F986261
00000940: 12949506 3C08699F 4BD6E546 32251FED
00000950: FC2929BE 7EAF80DF 709D8A2F DA2BCBB0
00000960: 143A0901 0380AE5A A788ECE0 1E2A6CAC
00000970: CDEB6CFB 2AFE54FF 58DE6646 F0221717
00000980: F1557508 F1EC64CA 9CAB4D02 8B317441
00000990: B949C51F 7B5528AB 29A68940 36FC1033
000009A0: 00020C33 61E8F287 4BC1A5CC 9AD43BFF
000009B0: BCFEDBD2 EB168ABA 3153D004 04891392
000009C0: 0759E342 25C81998 D8CCCDF1 24F10F48
000009D0: 90958111 2A0BA39F 76264696 785C6175
000009E0: 92FD3084 42789CB3 9F6F8BBC E26CB12C
00000AD0: 624463AB B8528F8C
00000AE0: 54290FEB 2BB71101 71CF4D
00000AF0: AB02C685 DE85FFA1 96ABDEE6
00000B00: 7D5CD83E 16944519 B540D504 35F9C9
00000B10: 4A780836 5DA62D47 4488B7C3 5EE72B86
00000B20: 3AB314BA 648638B5 F227E961 3A4F55F4
00000B30: 26A647E0 32656A8E 233CEA1E F9D4283F
00000B40: C443BEAB 17542082 5BF2C263 550D7144
00000B50: A8E28A03 2EA12961 0FA7FA96 BB91AB8F
00000B60: 553065D7 BE7908AD 99057B47 8E8B0E2A
00000B70: B94A089A AEC3BD09 266467FA 36D9B630
00000B80: 5742A518 B67CC998 EC4ED798 4D0B1D6F
00000B90: 1A274CB7 C9939480 A4CFFB93 586723E9
00000BA0: 520EF6C0 1CA8A041 E0530A89 5CC5223F
00000BB0: 87390563 53FBC8F7 55C3534D D2354C88
00000BC0: B7518953 E232B81F D85DA4F8 F7F947A4
00000BD0: B607FD0D DB799431 002C6C43 6B742FEE
00000BE0: 439898E5 DC93C39A 1EF52FAD BF9FFF30
00000BF0: DD0E7B76 CBD18E06 3F605AB5 DC67EE84
00000C00: 5A59B79F CC828165 9FF9D8A3 834BEF51
00000C10: 37AA3C60 04FAE596 9449F910 C9F1E737
00000C20: D944CFAD 74E55EBE C04E73B1 A4F1B371
00000C30: BE4D361F 87F49288 F4BF941C B90C4E83
00000C40: E33CE14C 90875B67 55781452 BA7706E3
Definitely packed
Ready
NUM


4NT
[C:\INF\issue1]unpack unknown
Unpack v0.173: Win32 runtime decompressor - pjf/yy/hms/mc/ci/a
a (c) Symantec 2000-06
unknown: packed by PECompact v2.00.102b-2.79bb... decompressed
to unpk0000.unp
[C:\INF\issue1]move unpk0000.unp unknown.unp
C:\INF\issue1\unpk0000.unp -> C:\INF\issue1\unknown.unp
1 file moved
4NT
[C:\INF\issue1]
Packed with PECompact
Select 4NT
[C:\INF\issue1]unpack unknown
Unpack v0.173: Win32 runtime decompressor - pjf/yy/hms/mc/ci/a
a (c) Symantec 2000-06
unknown: packed by PECompact v2.00.102b-2.79bb... decompressed
to unpk0000.unp
[C:\INF\issue1]move unpk0000.unp unknown.unp
C:\INF\issue1\unpk0000.unp -> C:\INF\issue1\unknown.unp
1 file moved
[C:\INF\issue1]_


FileView - [C:\INF\issue1\unknown.unp]
File Edit View Window Tools Help
C:\INF\issue1\unknown.unp
00058420 - file size
MZ object
[00000000] - start in file
[00000040] - entry point in
[00000490] - object end (0
header
PE object
[00000000] - start in file
[0000f38c] - entry point in
[00058400] - object end (0
header
00004550 - signature
014c - machine field
000000e0 - optional header size
010e - characteristics
sections
HEADER
[00000000] - file offset
00000400 - file size
00000000 - rva
00001000 - virtual size
00000000 - characteristics
.text
[00000400] - file offset
00057200 - file size
Readable strings!
00024510: 46696C65 204F7065 6E65642E 00000000 File Opened.....
00024520: 4E49434B 20257300 00000000 5B025468 NICK %s.....[.Th
00024530: 72656164 025D2025 73206B69 6C6C6564 read.] %s killed
00024540: 2E000000 00000000 50415254 2025730D ....PART %s.
00024550: 0A000000 416C6C20 74687265 61647320 ....All threads
00024560: 73746172 74696E67 20776974 68202573 starting with %s
00024570: 20686176 65206265 656E206B 696C6C65 have been kille
00024580: 642E0000 00000000 00000000 0A000000 d.............
00024590: 5B50726F 63657373 5D202573 2063616E [Process] %s can
Ready
NUM


FileView - C:\INF\issue1\unknown.unp
File Edit View Window Tools Help
C:\INF\issue1\unknown.unp:1
000244E0: 203A2063 6F6E6E65 6374696E 6720746F : connecting to
000244F0: 20257300 00000000 436F756C 646E2774 %s.....Couldn't
00024500: 206F7065 6E206669 6C652E00 00000000 open file.....
00024510: 46696C65 204F7065 6E65642E 00000000 File Opened.....
C:\INF\issue1\unknown.unp:2
] Already scanning
[SpyThread] Killed (%s)
All threads starting with %s have been killed.
[Process] %s cannot be killed
[Process] %s killed
Process
] Error!
CMD
] Active
CMD
] Error
NTScan
[NTScan] Stopped
I dont have a webcum
I have a webcum
Capture driver %s - %s.
net share C$ /delete /y
net share D$ /delete /y
net share IPC$ /delete /y
Ready
NUM

ASCII vs. Polymorphism



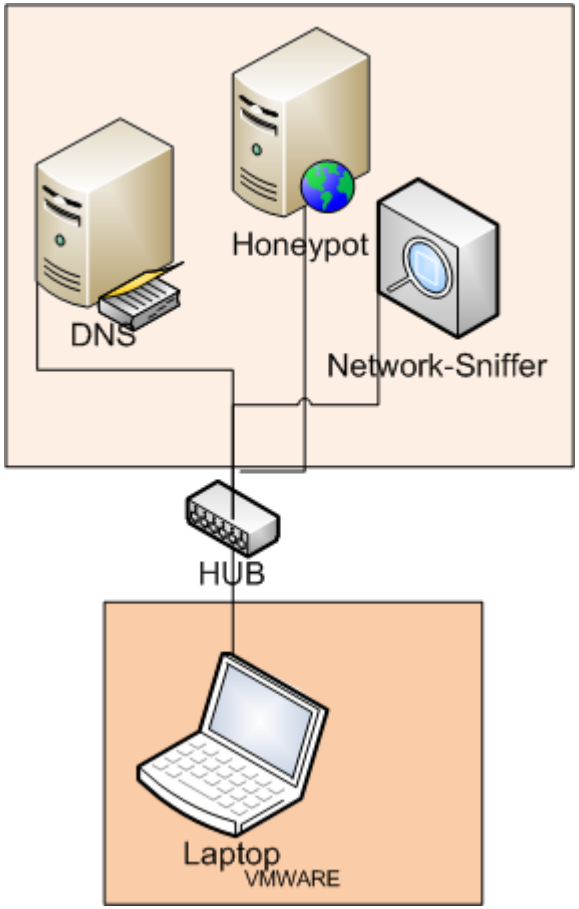
symantec™

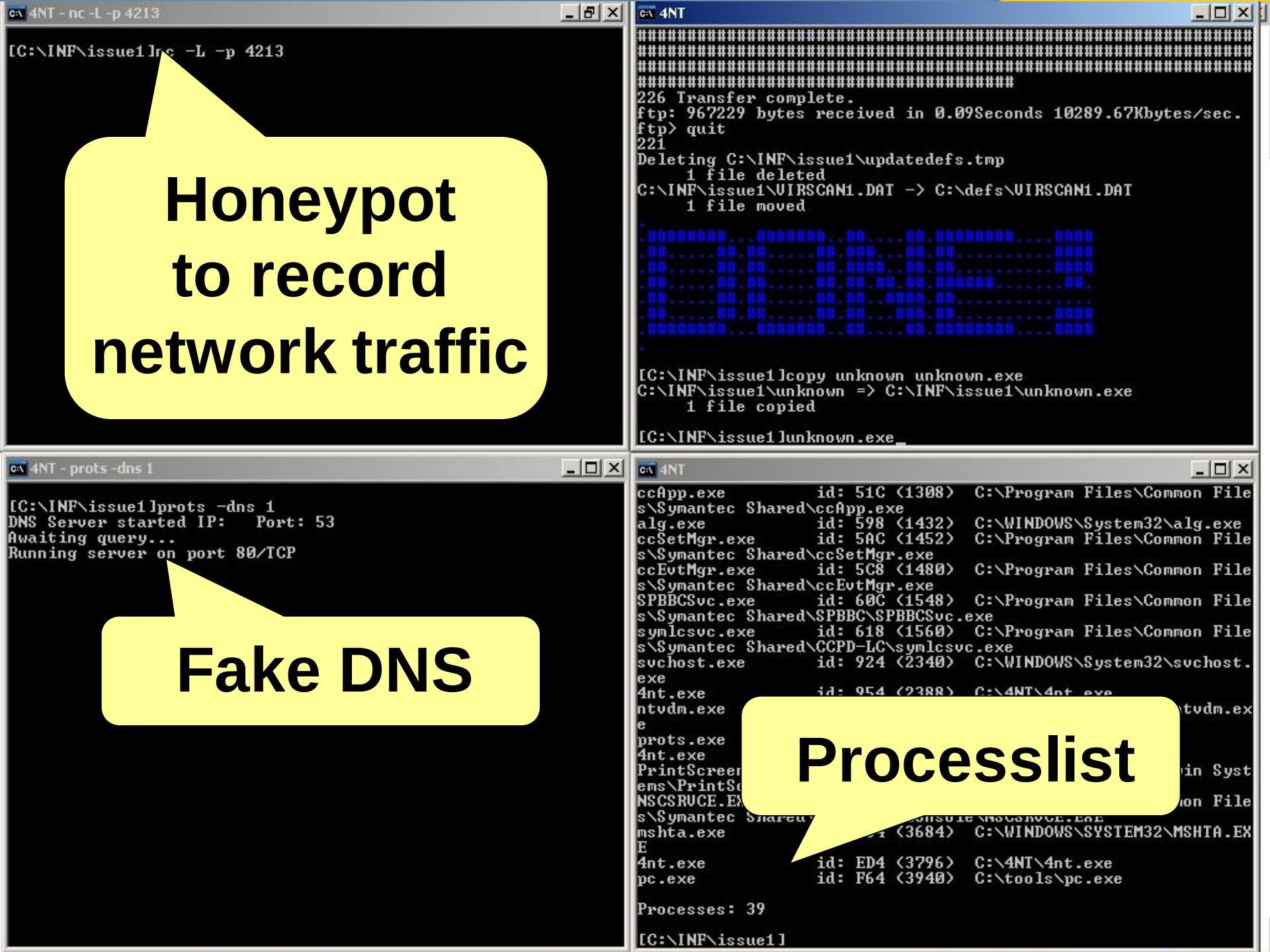
Confidence in a connected world.

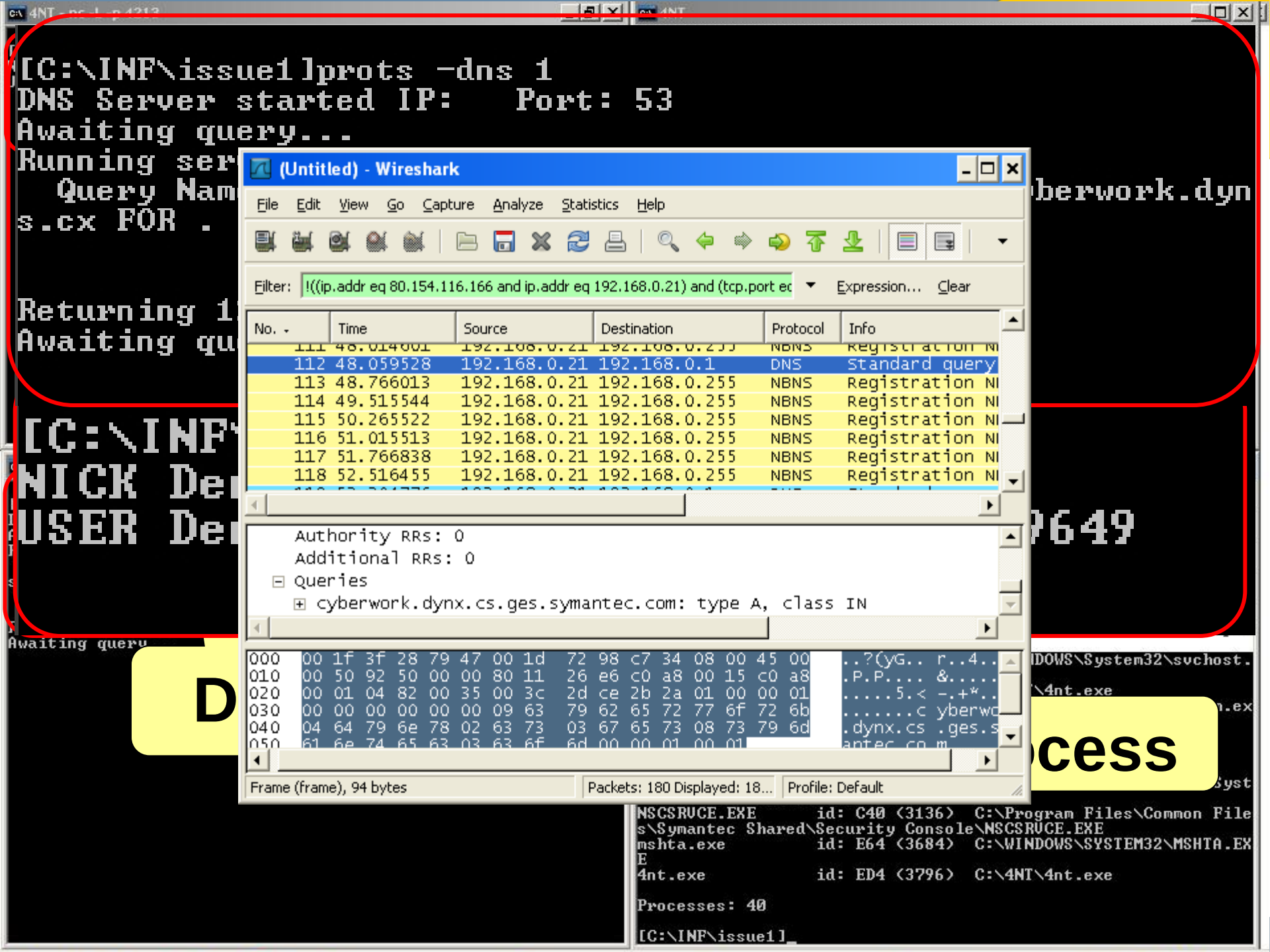
Let‘s Double-Click it

…on a special system

..the special system




4NT - nc -L -p 4213
[C:\INF\issue1]nc -L -p 4213
Honeypot to record network traffic
4NT
226 Transfer complete.
ftp: 967229 bytes received in 0.09Seconds 10289.67Kbytes/sec.
ftp> quit
221
Deleting C:\INF\issue1\updatedefs.tmp
1 file deleted
C:\INF\issue1\VIRSCAN1.DAT -> C:\defs\VIRSCAN1.DAT
1 file moved
[C:\INF\issue1]copy unknown unknown.exe
C:\INF\issue1\unknown => C:\INF\issue1\unknown.exe
1 file copied
[C:\INF\issue1]unknown.exe
4NT - prots -dns 1
[C:\INF\issue1]prots -dns 1
DNS Server started IP: Port: 53
Awaiting query...
Running server on port 80/TCP
Fake DNS
4NT
ccApp.exe id: 51C (1308) C:\Program Files\Common Files\Symantec Shared\ccApp.exe
alg.exe id: 598 (1432) C:\WINDOWS\System32\alg.exe
ccSetMgr.exe id: 5AC (1452) C:\Program Files\Common Files\Symantec Shared\ccSetMgr.exe
ccEvtMgr.exe id: 5C8 (1480) C:\Program Files\Common Files\Symantec Shared\ccEvtMgr.exe
SPBBCSvc.exe id: 60C (1548) C:\Program Files\Common Files\Symantec Shared\SPBBC\SPBBCSvc.exe
symlcsvc.exe id: 618 (1560) C:\Program Files\Common Files\Symantec Shared\CCPD-LC\symlcsvc.exe
svchost.exe id: 924 (2340) C:\WINDOWS\System32\svchost.exe
prots.exe
4nt.exe
mshta.exe (3684) C:\WINDOWS\SYSTEM32\MSHTA.EXE
4nt.exe id: ED4 (3796) C:\4NT\4nt.exe
pc.exe id: F64 (3940) C:\tools\pc.exe
Processes: 39
[C:\INF\issue1]
Processlist

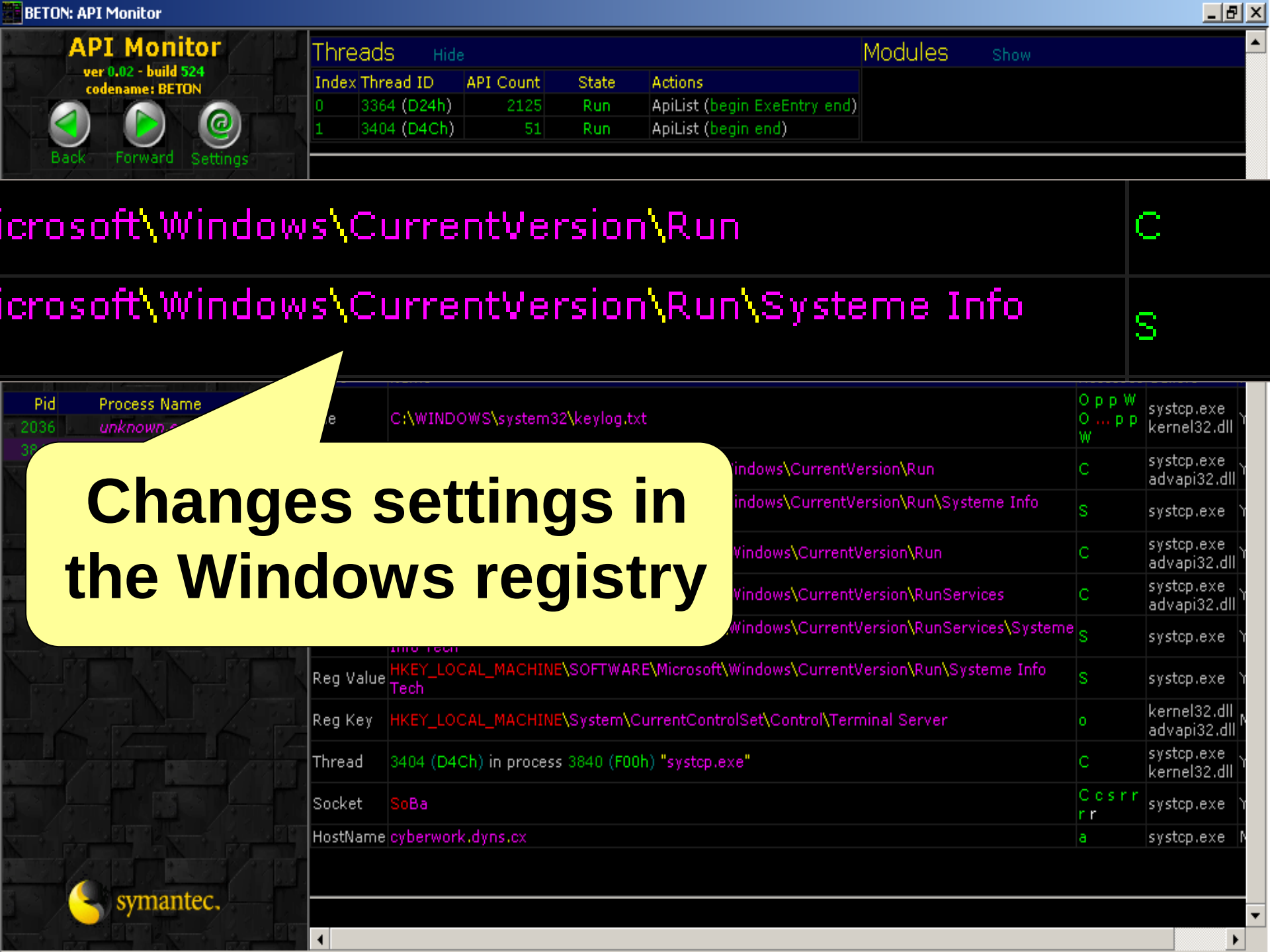

[C:\INF\issue1]prots -dns 1
DNS Server started IP: Port: 53
Awaiting query...
Running ser
Query Nam
s.cx FOR .
Returning 1
Awaiting qu
[C:\INF
NICK De
USER De
(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: !((ip.addr eq 80.154.116.166 and ip.addr eq 192.168.0.21) and (tcp.port eq
Expression... Clear
No. Time Source Destination Protocol Info
112 48.059528 192.168.0.21 192.168.0.1 DNS Standard query
113 48.766013 192.168.0.21 192.168.0.255 NBNS Registration NI
114 49.515544 192.168.0.21 192.168.0.255 NBNS Registration NI
115 50.265522 192.168.0.21 192.168.0.255 NBNS Registration NI
116 51.015513 192.168.0.21 192.168.0.255 NBNS Registration NI
117 51.766838 192.168.0.21 192.168.0.255 NBNS Registration NI
118 52.516455 192.168.0.21 192.168.0.255 NBNS Registration NI
Authority RRs: 0
Additional RRs: 0
Queries
cyberwork.dynx.cs.ges.symantec.com: type A, class IN
000 00 1f 3f 28 79 47 00 1d 72 98 c7 34 08 00 45 00 ..?(yG.. r..4..
010 00 50 92 50 00 00 80 11 26 e6 c0 a8 00 15 c0 a8 .P.P.... &.....
020 00 01 04 82 00 35 00 3c 2d ce 2b 2a 01 00 00 01 .....5.< -.+*..
030 00 00 00 00 00 00 09 63 79 62 65 72 77 6f 72 6b .....c yberwo
040 04 64 79 6e 78 02 63 73 03 67 65 73 08 73 79 6d .dynx.cs .ges.s
050 61 6e 74 65 63 03 63 6f 6d 00 00 01 00 01 antec.co m.....
Frame (frame), 94 bytes
Packets: 180 Displayed: 18...
Profile: Default
berwork.dyn
9649
DOWS\System32\svchost.
\4nt.exe
ocess
NSCSRVCE.EXE id: C40 (3136) C:\Program Files\Common File
s\Symantec Shared\Security Console\NSCSRVCE.EXE
mshta.exe id: E64 (3684) C:\WINDOWS\SYSTEM32\MSHTA.EX
E
4nt.exe id: ED4 (3796) C:\4NT\4nt.exe
Processes: 40
[C:\INF\issue1]_

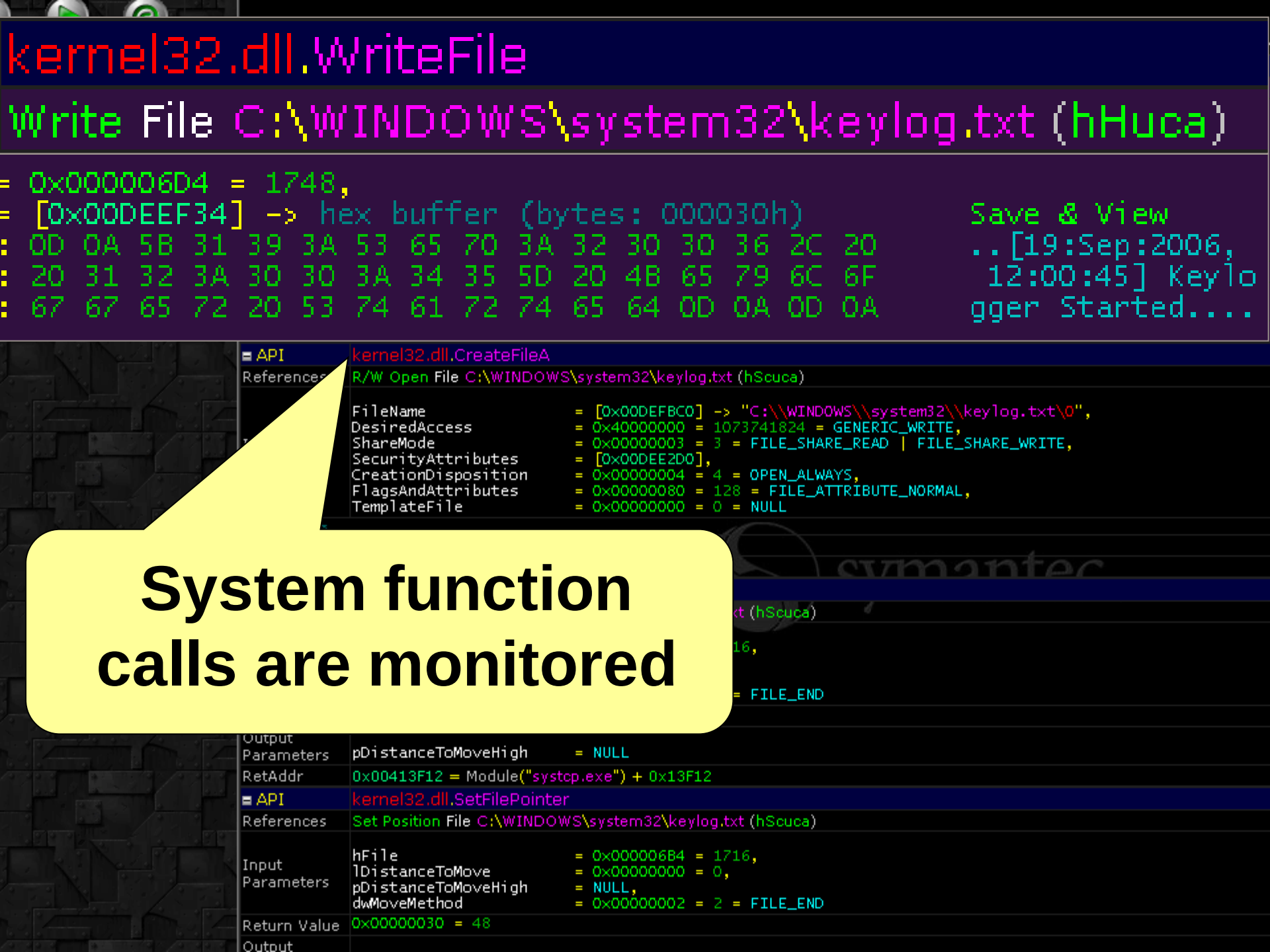
Blackboxing

- Execute the sample on an isolated system
- Monitor all operating system API calls
- Analyse logged information
- E.g. free Sysinternal tools (Regmon, Filemon, TCPView etc)

Example: API Monitor

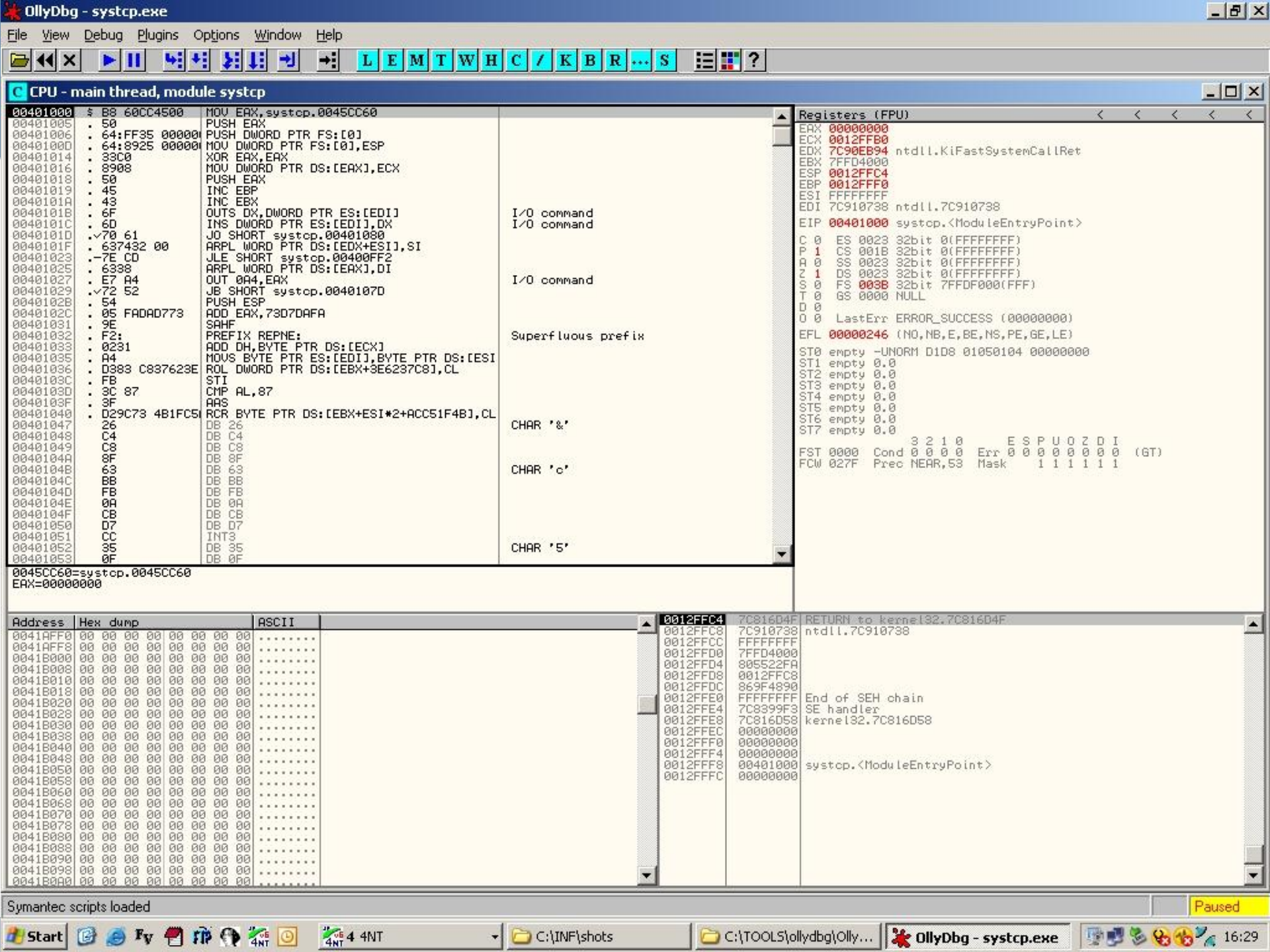

BETON: API Monitor
API Monitor
ver 0.02 - build 524
codename: BETON
Back
Forward
Settings
Monitor
Status not running
Actions Start
Log Analyzer
File C:\IN...bot-demo.aml
Status Idle. Waiting for data...
Size 2.29MB / 2.29MB - 100%
Actions Pause Close Object Map
Pid Process Name State
2036 unknown.exe Term
3840 systcp.exe Mon
symantec.
Process 2036 (7F4h) - "unknown.exe"
General Information
Name unknown.exe
Parent Process 3040 (BE0h)
Command Line
Threads
Index Thread ID
0 2088 (828
The suspicious process is now running
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
Process 3840 (F00h) "systcp.exe" C unknown.exe kernel32.dll Yes
Thread 3364 (D24h) in process 3840 (F00h) "systcp.exe" C unknown.exe kernel32.dll Yes

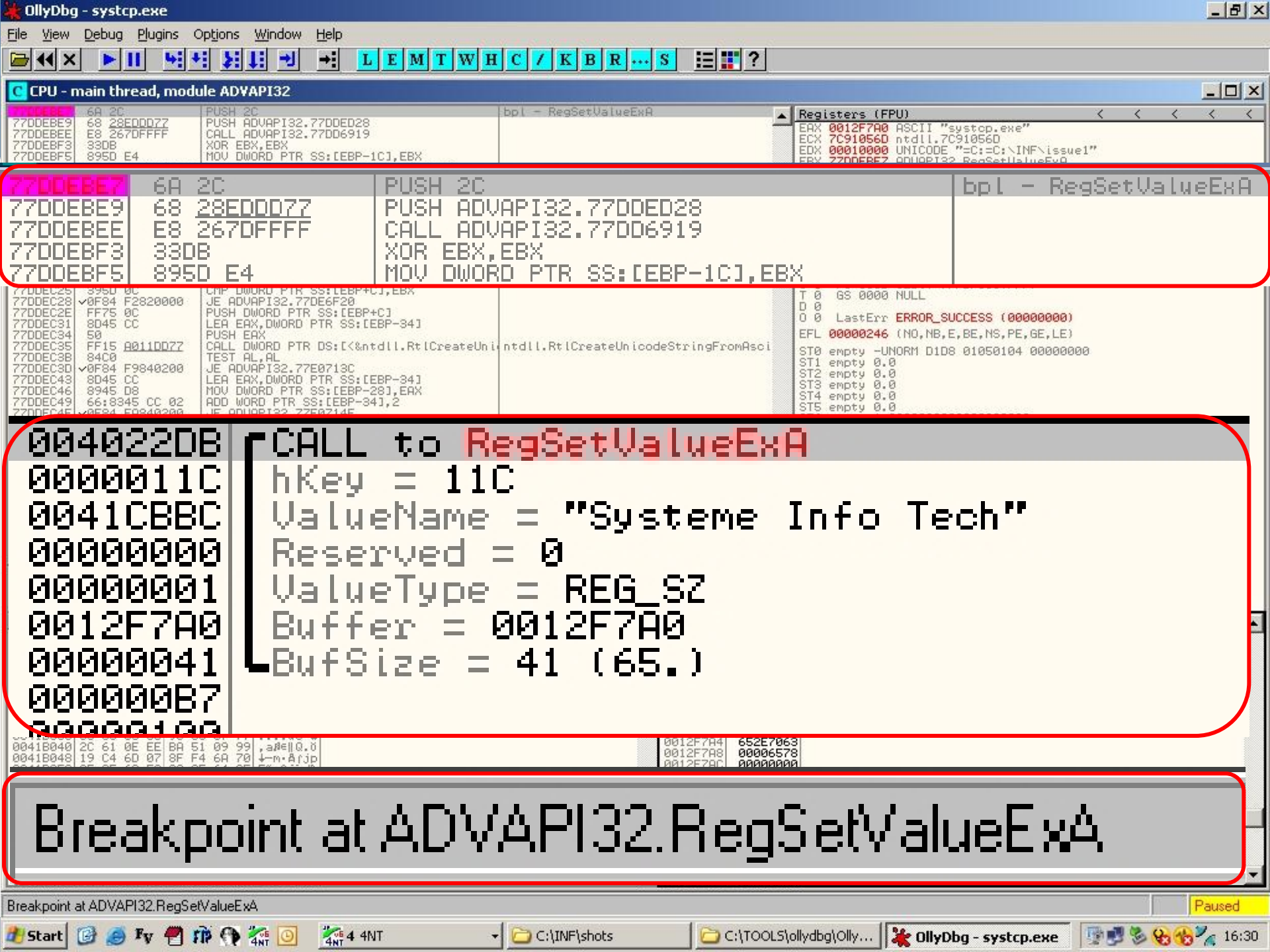

BETON: API Monitor
API Monitor
ver 0.02 - build 524
codename: BETON
Back
Forward
Settings
Threads
Hide
Modules
Show
Index
Thread ID
API Count
State
Actions
0
3364 (D24h)
2125
Run
ApiList (begin ExeEntry end)
1
3404 (D4Ch)
51
Run
ApiList (begin end)
icrosoft\Windows\CurrentVersion\Run
C
icrosoft\Windows\CurrentVersion\Run\Systeme Info
S
Changes settings in the Windows registry
Pid
Process Name
2036
C:\WINDOWS\system32\keylog.txt
systcp.exe
kernel32.dll
indows\CurrentVersion\Run
C
systcp.exe
advapi32.dll
indows\CurrentVersion\Run\Systeme Info
S
systcp.exe
Windows\CurrentVersion\Run
C
systcp.exe
advapi32.dll
Windows\CurrentVersion\RunServices
C
systcp.exe
advapi32.dll
Windows\CurrentVersion\RunServices\Systeme
S
systcp.exe
Reg Value
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Systeme Info Tech
S
systcp.exe
Reg Key
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server
o
kernel32.dll
advapi32.dll
Thread
3404 (D4Ch) in process 3840 (F00h) "systcp.exe"
C
systcp.exe
kernel32.dll
Socket
SoBa
systcp.exe
HostName
cyberwork.dyns.cx
a
systcp.exe
symantec.

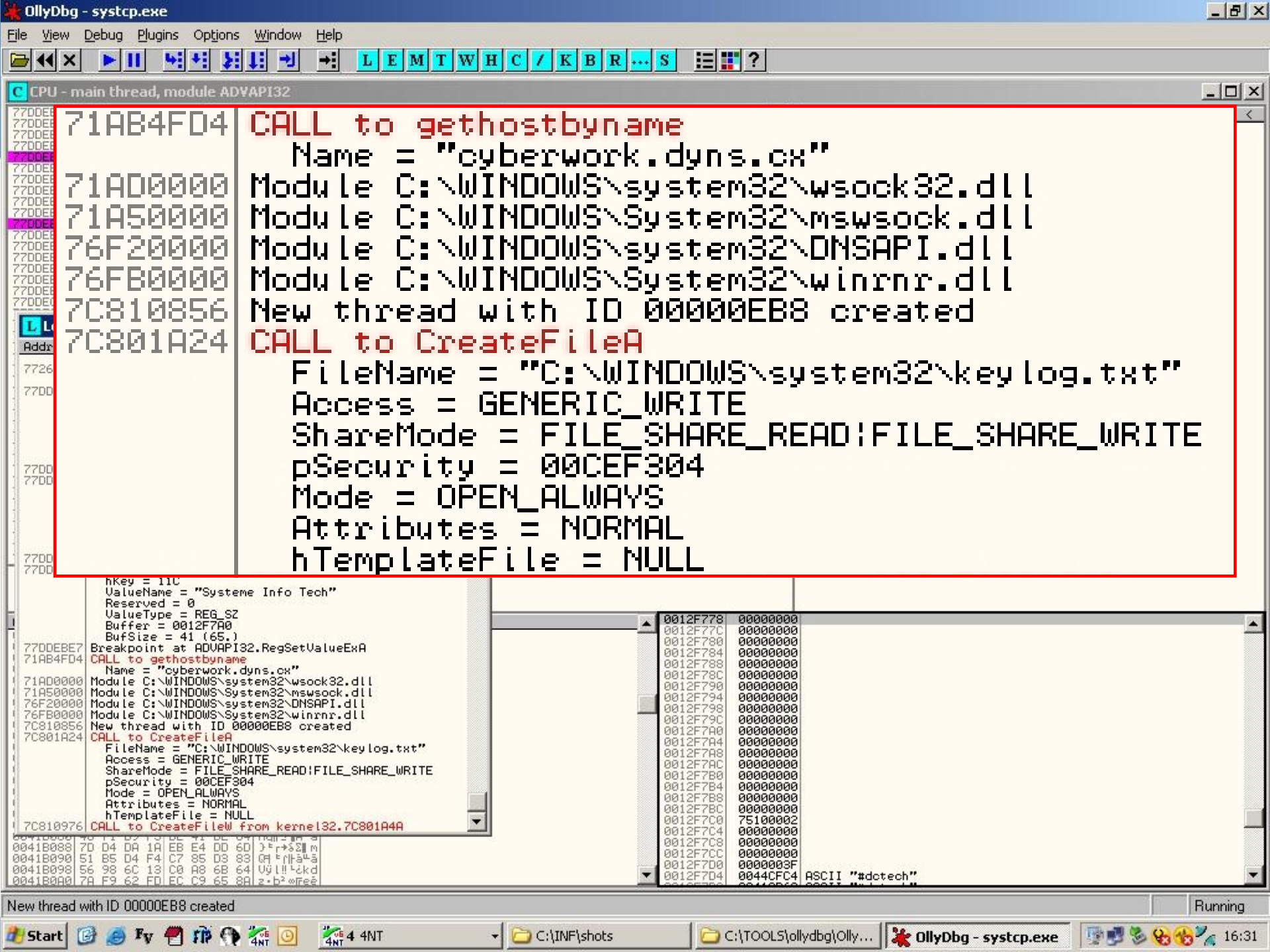

kernel32.dll.WriteFile
Write File C:\WINDOWS\system32\keylog.txt (hHuca)
= 0x000006D4 = 1748,
= [0x00DEEF34] -> hex buffer (bytes: 000030h)
: 0D 0A 5B 31 39 3A 53 65 70 3A 32 30 30 36 2C 20
: 20 31 32 3A 30 30 3A 34 35 5D 20 4B 65 79 6C 6F
: 67 67 65 72 20 53 74 61 72 74 65 64 0D 0A 0D 0A
Save & View
..[19:Sep:2006,
12:00:45] Keylo
gger Started....
API
kernel32.dll.CreateFileA
References
R/W Open File C:\WINDOWS\system32\keylog.txt (hScuca)
FileName = [0x00DEFBC0] -> "C:\\WINDOWS\\system32\\keylog.txt\0",
DesiredAccess = 0x40000000 = 1073741824 = GENERIC_WRITE,
ShareMode = 0x00000003 = 3 = FILE_SHARE_READ | FILE_SHARE_WRITE,
SecurityAttributes = [0x00DEE2D0],
CreationDisposition = 0x00000004 = 4 = OPEN_ALWAYS,
FlagsAndAttributes = 0x00000080 = 128 = FILE_ATTRIBUTE_NORMAL,
TemplateFile = 0x00000000 = 0 = NULL
System function calls are monitored
Output Parameters
pDistanceToMoveHigh = NULL
RetAddr
0x00413F12 = Module("systcp.exe") + 0x13F12
API
kernel32.dll.SetFilePointer
References
Set Position File C:\WINDOWS\system32\keylog.txt (hScuca)
Input Parameters
hFile = 0x000006B4 = 1716,
lDistanceToMove = 0x00000000 = 0,
pDistanceToMoveHigh = NULL,
dwMoveMethod = 0x00000002 = 2 = FILE_END
Return Value
0x00000030 = 48
Output

If you need more insight

- Use a debugger like OllyDbg
- Possible to interact with the binary
- Possible to change the execution flow
- Might need to use anti anti-debugging tricks


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
Start
4 4NT
C:\INF\shots
C:\TOOLS\ollydbg\Olly...
OllyDbg - systcp.exe
16:29


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
Paused
Start
C:\INF\shots
C:\TOOLS\ollydbg\Olly...
OllyDbg - systcp.exe
16:30


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
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
Start
4 4NT
C:\INF\shots
C:\TOOLS\ollydbg\Olly...
OllyDbg - systcp.exe
16:31

symantec™

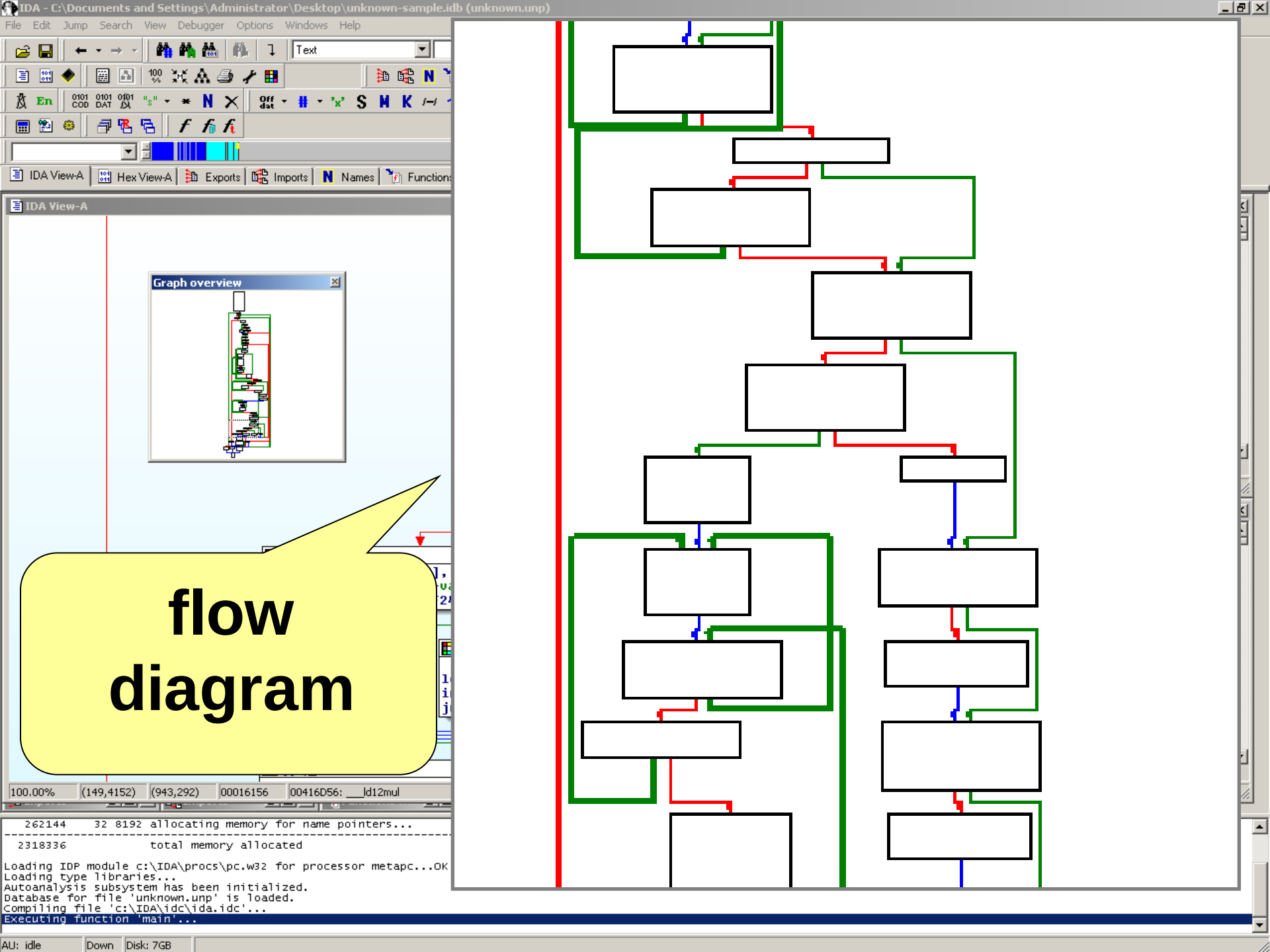
Confidence in a connected world.

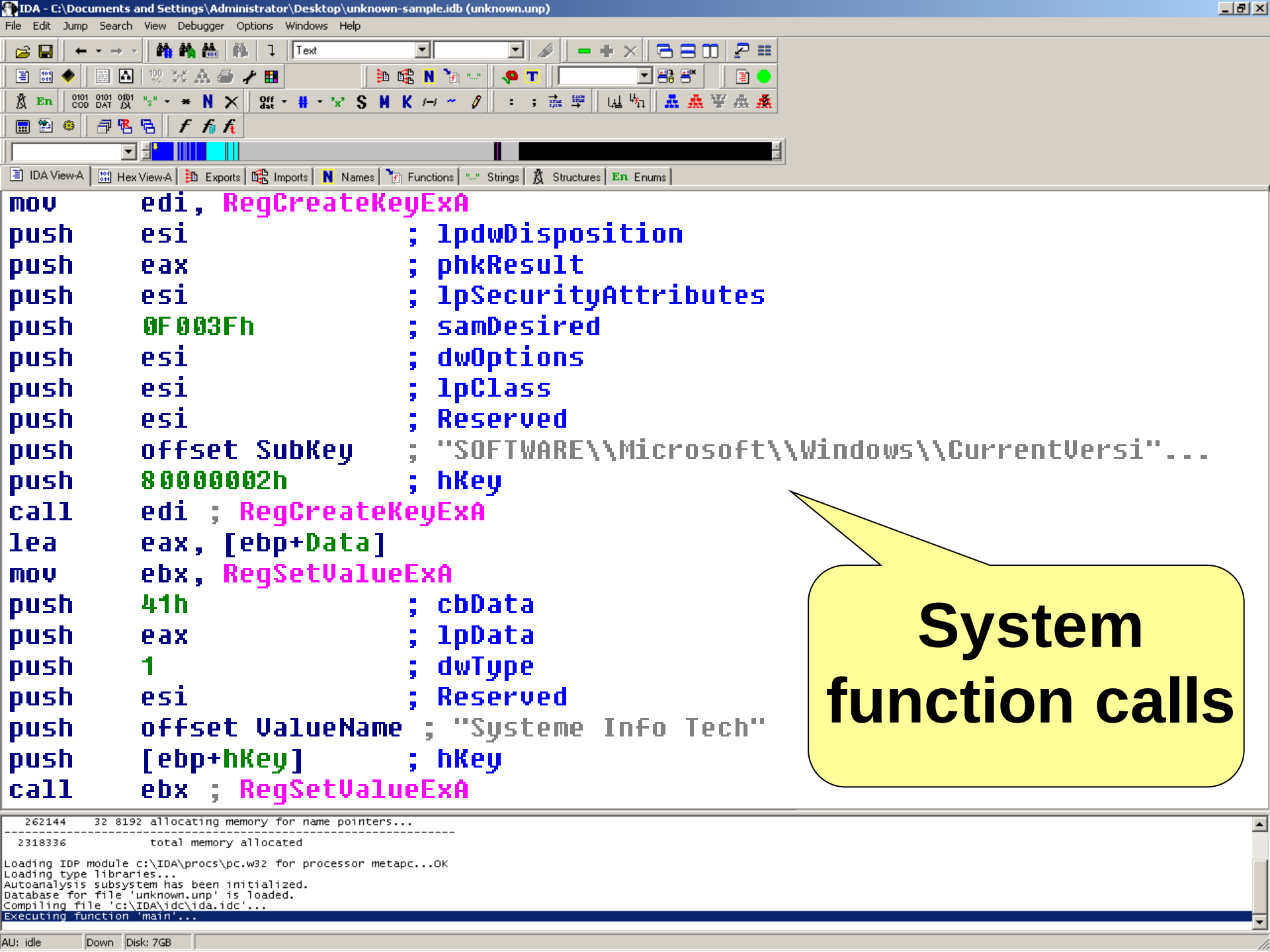
Reading the code

Whiteboxing

- Use a disassembler like IDA to see & read the code
- See “hidden” functions (time bombs)
- Analyze decryption routines

Example: IDA pro


IDA - C:\Documents and Settings\Administrator\Desktop\unknown-sample.idb (unknown.unp)
File Edit Jump Search View Debugger Options Windows Help
Text
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
IDA View-A
Graph overview
flow diagram
100.00%
(149,4152)
(943,292)
00016156
00416D56: __ld12mul
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'...
AU: idle
Down
Disk: 7GB


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 Strings Structures Enums
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
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'...
AU: idle Down Disk: 7GB

```
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
```

Questions ?

Oliver Karow
Security Consultant
Symantec Deutschland GmbH

Thank you
for your attention!