Detection & Eradication
About RedIRIS

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

1. By Traps
   1. Honeypots
   2. Spamtrap
   3. ...

2. By traffic analysis
   1. Netflow
   2. Darknet

3. By our users
How can we detect malware?

- Unfortunately malware are quite easy to obtain:
  - Spamtrap
  - From honeypots
  - Received from another CSIRT or group
  - From our customer, when handling an incident.
• 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
Getting binaries from outside

- Instead of blocking malicious traffic (ex 445/TCP), redirect it to a nepenthes box.
- Redirect all your dark space to your nepenthes box.
- Use DNAT in your nepenthes box to accept and simulate the victims.
- ~10,000 file /day
From our custumer

• 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
Malware identification tool:
SecCheck

• 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.merijin.org/index.php
  • Sysinternal tools
  • http://www.microsoft.com/technet/sysinternal/default.mspx
  • Foundstone tools
  • http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/freetools.htm

  • That allow us to recover the malware to analyze
Practical:

- Connect to the hands-on wireless network.

- Download the file
  - [http://192.168.1.31/exercises/SecCheck.log](http://192.168.1.31/exercises/SecCheck.log)

  (seccheck report)

Do you find the binary?
Eradication

Same as Obliteration

- Complete destruction of every trace of something

From www.wordreference.com
We want to

- Analyze the malware
  - Malware lab creation session in this conference.
  - Remote tools to analyze the files

- Eradicate the bot
  - Contact with the owners of the IP address & domains
  - Connect to the botnet and shutdown it
- 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
Complete scanning result of "example.exe", received in VirusTotal at 06.06.2007, 20:52:57 (CET).

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Version</th>
<th>Update</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>AhnLab-V3</td>
<td>2007.5.31.2</td>
<td>06.05.2007</td>
<td>Win32/IRCBot.worm.Gen</td>
</tr>
<tr>
<td>AntiVir</td>
<td>7.4.0.32</td>
<td>06.06.2007</td>
<td>Worm/Rbot.90668</td>
</tr>
<tr>
<td>Authentium</td>
<td>4.93.8</td>
<td>05.23.2007</td>
<td>W32/SdBot.LZA</td>
</tr>
<tr>
<td>Avast</td>
<td>4.7.997.0</td>
<td>06.06.2007</td>
<td>Win32:SdBot-gen44</td>
</tr>
<tr>
<td>AVG</td>
<td>7.5.0.467</td>
<td>06.06.2007</td>
<td>IRC/BackDoor.SdBot.ILM</td>
</tr>
<tr>
<td>BitDefender</td>
<td>7.2</td>
<td>06.06.2007</td>
<td>Generic.Sdbot.9856E601</td>
</tr>
<tr>
<td>CAT-QuickHeal</td>
<td>9.00</td>
<td>06.06.2007</td>
<td>Backdoor.Rbot.gen</td>
</tr>
<tr>
<td>ClamAV</td>
<td>devel-20070416</td>
<td>06.06.2007</td>
<td>Trojan.Mybot-2924</td>
</tr>
<tr>
<td>DrWeb</td>
<td>4.33</td>
<td>06.06.2007</td>
<td>Win32.HLLW.MyBot.based</td>
</tr>
<tr>
<td>eSafe</td>
<td>7.0.15.0</td>
<td>06.06.2007</td>
<td>Win32.Rbot.aeu</td>
</tr>
<tr>
<td>eTrust-Vet</td>
<td>30.7.3696</td>
<td>06.06.2007</td>
<td>Win32/Rbot.EUH</td>
</tr>
<tr>
<td>Ewido</td>
<td>4.0</td>
<td>06.06.2007</td>
<td>Backdoor.Rbot.aeu</td>
</tr>
<tr>
<td>FileAdvisor</td>
<td>1</td>
<td>06.06.2007</td>
<td>High threat detected</td>
</tr>
<tr>
<td>Fortinet</td>
<td>2.85.0.0</td>
<td>06.06.2007</td>
<td>W32/RBotlr.bdr</td>
</tr>
<tr>
<td>F-Prot</td>
<td>4.3.2.48</td>
<td>06.05.2007</td>
<td>W32/Sdbot.LZA</td>
</tr>
<tr>
<td>F-Secure</td>
<td>6.70.130.300</td>
<td>06.06.2007</td>
<td>Backdoor.Win32.Rbot.aeu</td>
</tr>
<tr>
<td>Ikarus</td>
<td>T3.1.1.8</td>
<td>06.06.2007</td>
<td>Backdoor.Win32.Wootbot</td>
</tr>
<tr>
<td>Kaspersky</td>
<td>4.0.2.24</td>
<td>06.06.2007</td>
<td>Backdoor.Win32.Rbot.aeu</td>
</tr>
<tr>
<td>McAfee</td>
<td>5047</td>
<td>06.06.2007</td>
<td>Generic Packed</td>
</tr>
<tr>
<td>Microsoft</td>
<td>1.2503</td>
<td>06.06.2007</td>
<td>Backdoor:Win32/Rbot18FF3</td>
</tr>
<tr>
<td>NOD32v2</td>
<td>2313</td>
<td>06.06.2007</td>
<td>probably a variant of Win32/Rbot</td>
</tr>
<tr>
<td>Norman</td>
<td>5.80.02</td>
<td>06.05.2007</td>
<td>W32/Spybot.SVH</td>
</tr>
<tr>
<td>Panda</td>
<td>9.0.0.4</td>
<td>06.06.2007</td>
<td>W32/Gaobot.gen.worm</td>
</tr>
<tr>
<td>Prevx1</td>
<td>V2</td>
<td>06.06.2007</td>
<td>Covert.Sys.Exec</td>
</tr>
<tr>
<td>Sophos</td>
<td>4.16.0</td>
<td>06.01.2007</td>
<td>W32/Rbot-Gen</td>
</tr>
<tr>
<td>Sunbelt</td>
<td>2.2.907.0</td>
<td>06.04.2007</td>
<td>Backdoor:Win32.Rbot.aeu</td>
</tr>
<tr>
<td>Symantec</td>
<td>10.3</td>
<td>06.06.2007</td>
<td>W32/Spybot.Worm</td>
</tr>
<tr>
<td>TheHacker</td>
<td>6.1.6.130</td>
<td>06.06.2007</td>
<td>Backdoor/Rbot.gen</td>
</tr>
<tr>
<td>VBA32</td>
<td>3.12.0</td>
<td>06.06.2007</td>
<td>Backdoor:Win32.Rbot.gen</td>
</tr>
<tr>
<td>VirusBuster</td>
<td>4.3.23.9</td>
<td>06.06.2007</td>
<td>Worm.Rbot.JCW</td>
</tr>
<tr>
<td>Webwasher-Gateway</td>
<td>6.0.1</td>
<td>06.06.2007</td>
<td>Worm.Rbot.90668</td>
</tr>
</tbody>
</table>
Remote: Norman Sandbox

- First remote malware analysis tool

- Two level model.
  - Free, small report by email.
  - Paid service: detailed information
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\nmupdate32.exe.
  * Deletes file 256.
[ Changes to registry ]
  * Creates value "microsoft windows updates"="nmupdate32.exe" in key "HKLM\Software\Microsoft\Windows\CurrentVersion\Run".
  * Creates value "microsoft windows updates"="nmupdate32.exe" in key "HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices".
  * Sets value "restrictanonymouse"="" in key "HKLM\System\CurrentControlSet\Control\Lsa".
  * Sets value "restrictanonymousem"="" 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 NeTxx803400.
  * IRC: Uses username ezkleyac.
  * IRC: Joins channel "#NeTxx## with password wayne.
  * IRC: Sets the usemode for user NeTxx803400 to +x+1.
  * 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\nmupdate32.exe (90668 bytes) : W32/Spybot.SVH.
Remote: cwsandbox


<table>
<thead>
<tr>
<th>ID</th>
<th>591651</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>None</td>
</tr>
<tr>
<td>Flag</td>
<td>1</td>
</tr>
</tbody>
</table>

**Analysis Summary:**
- Analysis Date: 5/16/2007 1:20:30 PM
- Sandbox Version: 3.315
- Filename: 3e7da8308f3c5cf4d1f0d0239af60d4.exe

**Technical Details:**
- Analysis Number: 1
- Parent ID: 0
- Process ID: 554
- Filename: c:\temp\3e7da8308f3c5cf4d1f0d0239af60d4.exe
- Filesize: 90662 bytes
- MD5: 3e7da8308f3c5cf4d1f0d0239af60d4
- Start Reason: AnalysisTarget
- Termination Reason: NormalTermination
- Start Time: 00:00:188
- End Time: 00:00:188
Remote: Anubis

http://analysis.seclab.tuwien.ac.at/result.php?taskid=5e787c8b81e57f74d9501c966734d74d&refresh=1&embedde
How those tools works?

- 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 it
Setting up our lab: Linux server (I)

- 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
Setting up our lab:
Linux server (II)

- 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.
Configuring a DNS root server:

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

// 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 "/var/named/fake-master"

Set up the corresponding fake DNS zone

All queries will reply the same IP address

```plaintext
$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
```
Network traffic

- 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
  ▪ ...
Capturing the traffic:

- 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*
• Live analysis
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
Behaviour-based tools:
RegShot example

----------------------------------
Values added: 4
----------------------------------
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\microsoft windows updates: "mwupdate32.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\microsoft 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\fcrpvzragf\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\speciments\example.exe: "example"
01:25:42.120500 IP 192.168.150.254.1029 > 192.168.150.2.domain: 24256+ A?
dad.darksensi.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 02d 9d6e 5ec0 0100 0001 ....5.-.n^.....
  0x0030:  0000 0000 0000 0364 6164 0a64 6172 6b73 ........dad.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 96fe 5ec0 .]..@.@........
  0x0020:  9702 0405 0035 0049 87c5 5ec0 8580 0001 ...5...I..^.....
  0x0030:  0001 0001 0000 0364 6164 0a64 6172 6b73 .........dad.darks
  0x0040:  656e 7375 6904 696e 666f 0000 0100 01 ensui.info.....
  0x0050:  0c00 0100 0100 0151 8000 04c0 a897 0200 ......Q........
  0x0060:  0002 0001 0001 5180 0001 00 .....Q....
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 282c 0000 8006 2349 c0a8 96fe c0a8 .]..@...#I......
  0x0020:  9702 0453 23b0 efba ad46 0000 0000 7002 ...S#....F....p.
  0x0030:  faf0 13d8 0000 0204 05b4 0101 0402 ...............
example malware:
IRC information (I)

0x0040:  6554 787c 3836 3032 3434 0d0a          eTx|860244..
• 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 OIN.##NeTx##.way
• 0x00a0:  6e65 0d0a                                   ne..
• 01:54:25.624956 IP 192.168.150.2.9136 > 192.168.150.254.1077: P 1864:1939(75) ack 181 win 5840
• 0x0000:  000c 29d5 7e15 0050 5601 0203 0800 4500 ..)~..PV.....E.
• 0x0010:  0073 86bc 4000 4006 0577 c0a8 9602 c0a8 .s..@.@.w......
• 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”? 
Two approach

- 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
Encrypted files

- 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

<table>
<thead>
<tr>
<th>File pos</th>
<th>Mem pos</th>
<th>ID</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>A0001040</td>
<td>00406E40</td>
<td>7B_0F</td>
<td></td>
</tr>
<tr>
<td>A0001063</td>
<td>00406E63</td>
<td>43_0F</td>
<td></td>
</tr>
<tr>
<td>A00010BC</td>
<td>00406FBC</td>
<td>43_0F</td>
<td></td>
</tr>
<tr>
<td>A00010E0</td>
<td>00406F08</td>
<td>03_0F</td>
<td></td>
</tr>
<tr>
<td>A0001220</td>
<td>0040720A</td>
<td>04_0F</td>
<td></td>
</tr>
<tr>
<td>A0001300</td>
<td>00407180</td>
<td>03_0F</td>
<td></td>
</tr>
<tr>
<td>A0001318</td>
<td>00407236</td>
<td>02_0F</td>
<td></td>
</tr>
<tr>
<td>A000134A</td>
<td>004074D3</td>
<td>04_0F</td>
<td>Yop3F</td>
</tr>
<tr>
<td>A0001370</td>
<td>00407520</td>
<td>03_0F</td>
<td>Yifm</td>
</tr>
<tr>
<td>A0001390</td>
<td>00407629</td>
<td>03_0F</td>
<td>NPeM</td>
</tr>
<tr>
<td>A00013C7</td>
<td>00407573</td>
<td>03_0F</td>
<td>30_0F</td>
</tr>
<tr>
<td>A00013CE</td>
<td>004076CE</td>
<td>04_0F</td>
<td></td>
</tr>
<tr>
<td>A00013F1</td>
<td>00407840</td>
<td>04_0F</td>
<td>w&gt; |</td>
</tr>
<tr>
<td>A00013F7</td>
<td>00407848</td>
<td>04_0F</td>
<td>w&gt; |</td>
</tr>
<tr>
<td>A00013F9</td>
<td>0040784E</td>
<td>04_0F</td>
<td></td>
</tr>
<tr>
<td>A00013FC</td>
<td>00407850</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A00013FD</td>
<td>00407852</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A00013F7</td>
<td>00407854</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A00013F9</td>
<td>00407856</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A000140D</td>
<td>00407858</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A000141D</td>
<td>0040785A</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A000142D</td>
<td>00407862</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001458</td>
<td>00407870</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001468</td>
<td>00407872</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001478</td>
<td>00407874</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001488</td>
<td>00407876</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001498</td>
<td>00407878</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A00014A8</td>
<td>00407880</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A00014B8</td>
<td>00407882</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A00014C8</td>
<td>00407884</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A00014D8</td>
<td>00407886</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A00014E8</td>
<td>00407888</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A00014F8</td>
<td>00407890</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001508</td>
<td>00407892</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001518</td>
<td>00407894</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001528</td>
<td>00407896</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001538</td>
<td>00407898</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001548</td>
<td>004078A0</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001558</td>
<td>004078A2</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001568</td>
<td>004078A4</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001578</td>
<td>004078A6</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001588</td>
<td>004078A8</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001598</td>
<td>004078AA</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A00015A8</td>
<td>004078AC</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A00015B8</td>
<td>004078AE</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A00015C8</td>
<td>004078B0</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A00015D8</td>
<td>004078B2</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A00015E8</td>
<td>004078B4</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A00015F8</td>
<td>004078B6</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001608</td>
<td>004078B8</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001618</td>
<td>004078BA</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001628</td>
<td>004078BC</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001638</td>
<td>004078BD</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001648</td>
<td>004078BE</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001658</td>
<td>004078BF</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001668</td>
<td>004078C0</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001678</td>
<td>004078C2</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001688</td>
<td>004078C4</td>
<td>05_0F</td>
<td></td>
</tr>
<tr>
<td>A0001698</td>
<td>004078C6</td>
<td>05_0F</td>
<td></td>
</tr>
</tbody>
</table>
• 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

- Attach to the process.
- Launch Ollydump plugin
- Save the file ..
• 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 disassemble the malware and analyze it.
Typical C function call:
- `printf ("hello %s\n", somename);`

Somename is a `*char` ;-) Subtitute %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?
Where the malware comes from? (II)
Finding the password
Finding the password
Yourself exercise

• Never execute any file in your real environment
  - Kids don’t do that ....
  - Check three times that you are in a virtual environment

• Try to analyze the file
  - /malware contains binary files from a nephenthes box
  - /exercises contains the sample.exe & gilherme bot