



Malware Analysis – Lessons Learned

Pedro Bueno, SANS GCIA

SANS Internet Storm Center

pbueno@isc.sans.org



- First...keep in mind that...

"Malware development is accelerating due to efficient and open collaboration, moving from months and years to weeks and days"

--Johannes Ullrich, CTO do SANS Internet Storm Center (ISC)

Agenda

- Introduction
- Part I – Packers...
- Part II – “The meaning of life...”
- Part III – “But I just went to winupdates...”
- Part IV – “What a nice postcard!”
- Part V – “My computer is just slow...”
- Part VI – “The Empire Strikes Back”
- Conclusion

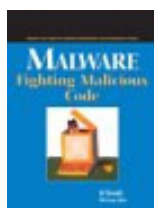
Introduction

- Malware Analysis...but what is a Malware ?

“Malware is a set of instructions that run on your computer and make your system do something that an attacker want it to do.”

--Ed Skoudis

ISC Handler and “Malware: Fighting Malicious Code” book author



Introduction

*Try to learn something about everything and
everything about something.*

Thomas H. Huxley



Introduction

- What you will NOT see in this presentation:
 - This is not about teach REM!:-)
- What you WILL see in this presentation:
 - We will see example of categories of REM used on the Malware Analysis Quizes:
 - Visual Analysis
 - Behavioral Analysis
 - Code Analysis
 - You will be presented to a non completed list of tools used to do Malware Analysis!

Part I – Malware Analysis Quiz 1

Packers...



.Analyze the output of the Linux strings command on real malwares and answer 3 questions!

Part I - Malware Analysis Quiz I

- **Category: Visual Analysis**
- The Questions:
 1. What is a PE file?
 2. What is a PE packer?
 3. Looking just at the strings files from real malwares, do you think that they were packed with some packer? If so, which one?

Part I - Malware Analysis Quiz I

- **Answers:**

- 1) Anton Chuvakin, one of the authors of Securit Warrior book, defines it as:
"The native file format of Windows is the **Portable Executable (PE)**. "Portable" means that **all Windows platforms and processors recognize the program**. In order to under-stand the process of unpacking a compressed application, it is first necessary to under-stand the structure of the Win32 PE file format (Figure 2-8). This format has remained relatively constant over the years, even with newer 64-bit Windows platforms."
- 2) Dr. Neal says that "The goal for most packers is to obscure opcodes and functions:
 - Limits unauthorized code theft.
 - **Obscures network addresses, URLs, IRC channels, etc.**
 - Hinders code modification (like cracking tools that remove licensing requirements)
 - **Makes code smaller.** (Why download a 100Meg file when you can download a 20Meg file that self-uncompresses?)"

Part I - Malware Analysis Quiz I

3. File 1: Strings of visualize.scr-ebd92f1bff47ed100d49a555f3c03c3e

This program must be run
under Win32

UPX0

UPX1

.rsrc

-> Packer UPX

1.25

UPX!

File 2: Strings of voxcard.exe-01a1d472a9bd3702ebe7a5ad8f4d5e16

This program must be run
under Win32

CODE

DATA

.idata

.tls

.rdata

.reloc

.rsrc

.aspack

.adata

-> Packer ASPACK

SANSFire 2006

<http://isc.sans.org>

Notes:

-> File 1: visualize.scr-ebd92f1bff47ed100d49a555f3c03c3e.strings.txt - The strings bellow are right on the beginning of the file:

This program must be run under Win32

UPX0

UPX1

.rsrc

1.25

UPX!

These UPX0, UPX1 and UPX! are typical from files packed with the UPX packer (upx.sourceforge.net). The 1.25 is the UPX version. Dr. Neal also pointed something that I didnt know, that when you have a registered version of UPX, the string UPX2 will also appear there.

-> File 2: voxcard.exe-01a1d472a9bd3702ebe7a5ad8f4d5e16.strings.txt - The strings bellow are right on the beginning of the file:

This program must be run under Win32

CODE

DATA

.idata

.tls

.rdata

.reloc

.rsrc

.aspack

.adata

Basically in all files packed with the ASPACK packer will include the section .aspack. Another section included by ASPACK can have its name configurable. The default is .adata, as in our example above. :)

Part I – (cont.)

File 3: wwlink.exe-da57aa6eea6ff3ea3166f53da11aec74

File 4: wyvisualizar.exe-f04cb834ac843ad08a1a5c17e4f67ba3

-> Packer PECompact2

!This program cannot be run in DOS mode.

RichA

[AspackDie!]

.text

PEC2

.rsrc

File 4: x1.exe-0c7ec6408547fcd0647a2a4790987935

-> Packer RAR

```
#####
<?xml version="1.0" encoding="UTF-8" standalone="
yes"?> <assembly xmlns="urn:schemas-microsoft-com
:asm.v1" manifestVersion="1.0"> <assemblyIdentity
version="1.0.0.0" processorArchitecture="X86" na
me="Roshal.WinRAR.WinRAR" type="win32" /> <descri
ptions>WinRAR archiver.</description> <dependency>
<dependentAssembly> <assemblyIdentity type="win3
2" name="Microsoft.Windows.Common-Controls" versi
on="6.0.0.0" processorArchitecture="X86" publicKe
yToken="6595b64144ccf1df" language="*" /> </depen
dentAssembly> </dependency> </assembly>
KERNEL32.DLL
```

SANSFire 2006

<http://isc.sans.org>

Notes:

-> File 3: wwlink.exe-da57aa6eea6ff3ea3166f53da11aec74.strings.txt

-> File 4: wyvisualizar.exe-f04cb834ac843ad08a1a5c17e4f67ba3.strings.txt

Both File 3 and File 4 have the same packer...which one??? I got almost the same amount of answers for ASPACKDie! and PECompact2 ...

The answer is....

PECompact2!

Why??!

Well...the question is quite simple...Lets look at the first 6 lines of the strings:

!This program cannot be run in DOS mode.

RichA

[AspackDie!]

.text

PEC2

.rsrc

-> File 5: x1.exe-0c7ec6408547fcd0647a2a4790987935.strings.txt

Look at the strings bellow:

%sRarSFX%d

.lnk

.inf

Install

.exe

Software\WinRAR SFX

RarHtmlClassName

Part I – Malware Analysis

Quiz 1



This program must be run
under Win32

UPX0

UPX1

.rsrc

1.25

UPX!

!This program cannot be run
in DOS mode.

RichA

[AspackDie!]

.text

PEC2

.rsrc

GGGGGGGGG

GGGGG

#####

```
<?xml version="1.0" encoding="UTF-8" standalone="
yes"?> <assembly xmlns="urn:schemas-microsoft-com
:asm.v1" manifestVersion="1.0"> <assemblyIdentity
version="1.0.0.0" processorArchitecture="X86" na
me="Roshal.WinRAR.WinRAR" type="win32" /> <descri
ption>WinRAR archiver.</description> <dependency>
<dependentAssembly> <assemblyIdentity type="win3
2" name="Microsoft.Windows.Common-Controls" versi
on="6.0.0.0" processorArchitecture="X86" publicKe
yToken="6595b64144cfd1df" language="*" /> </depen
dentAssembly> </dependency> </assembly>
KERNEL32.DLL
```

This program must be run
under Win32

CODE

DATA

.idata

.tls

.rdata

.reloc

.rsrc

.aspack

.adata



Part II - Malware Analysis



Quiz 2

- **Category: Visual and Behavioral Analysis**
- "The meaning of Life..."
- The Mission:
 - Analyze an inoffensive piece of software...☺

SANSFire 2006

<http://isc.sans.org>

Notes:

This file was created by myself, so people could test the lessons learned on the first quiz!

Quiz 2

- Objective:

- Get basic info from a piece of inoffensive software...

- Specific Questions:

- 1) Is this file Packed? If so, which packer was used?
- 2) Which command did you use to identify it?
- 3) Do you believe that is there any other way to identify the packer?
- 6) And finally, as a bonus question: What is the meaning of life?

Quiz 3

- New lessons learned here:
 - 1) Multiple ways to identify if a file is packed:
 - Use Linux/Sysinternals command 'Strings' to get the strings...☺
 - Open it on notepad and see the strings
 - Use the right-click properties and check the Archive tab!
 - Use BinText
 - Use PEiD
 - Use Linux command 'File'

SANSFire 2006

<http://isc.sans.org>

Notes:

Sysinternals Tool Strings can be found here:

- Strings: <http://www.sysinternals.com/Utilities/Strings.html>

Foundstone's BinText is a tool that finds Ascii, Unicode and Resource strings in a file. It can be found here:

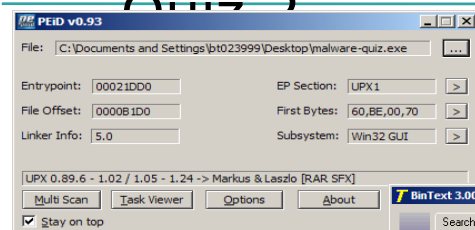
- BinText:

<http://www.foundstone.com/resources/termsofuse.htm?file=bintext.zip>

PEiD is a tool that detects most common packers, cryptors and compilers for PE files. It can currently detect more than 600 different signatures in PE files. Version 0.94 can be found here: <http://www.secretashell.com/codomain/peid/files/PEiD-0.94-20060510.zip>

Unix FILE application can identify some packers as well, as UPX/RAR/PECompact2...

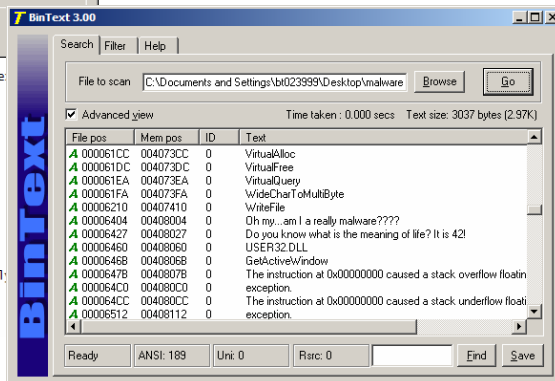
Quiz 2



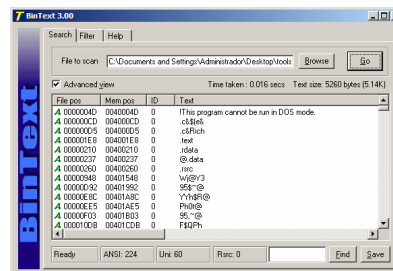
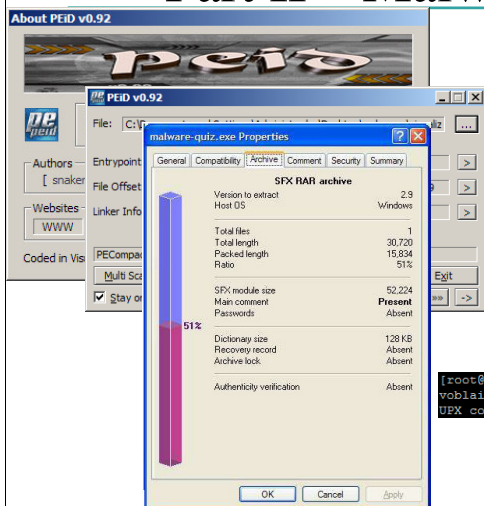
Ultimate Packer for eXecutables
Copyright (C) 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004
UPX 1.25w Markus F.X.J. Oberhumer & Laszlo Molnar Jun 29th :
File size Ratio Format Name
114991 <- 68399 59.48% win32/pe malware-quiz.exe
Unpacked 1 file.

UNRAR 3.50 freeware Copyright (c) 1993-2005 Alexander Liska

```
Extracting from malware-quiz.exe
;The comment below contains SFX script commands
Path=c:\windows\temp
SavePath
Silent=1
Overwrite=1
Title=^w3d^
Text
{
just kidding...
}
License=Malware License
{
This malware was created for educational purpose only.
check handlers.dshield.org/pbueno
}
Extracting malware.exe
```



Part II – Malware Analysis Quiz



```
[root@catyph root]# file voblaizdupla.exe
voblaizdupla.exe: PE executable for MS Windows (GUI) Intel 80386 32-bit,
UPX compressed
```



Part III - Malware Analysis



Quiz 3

- **Category: Visual and Behavioral Analysis**

- "But I just went to Winupdates.com"

- The Mission:

"A machine was presenting a strange behavior on the corporate. The Incident Response Team was called to check the machine. The user said that the only thing that he remembers was that he was checking a Windows Update website..."

<http://handlers.sans.org/pbueno/ma3.html>

SANSFire 2006

<http://isc.sans.org>

Notes:

This one was regarding a Spyware. Lots of fun on this analysis...lot of things to follow...!☺

Quiz 3

- Objectives:

- Analyze a Spyware!

- Specific Questions:

1. What is a .cmd extension? In which systems that this file extension would work?
3. Is it packed? If yes, which packed was used?
5. Please describe the process which this malware will try to get installed on the system.
7. In the same machine, was observed that some registry entries were messed up...Again, does this malware have something to do with it? If so, why?
8. Please, describe how this malware tries to install softwares (and which ones) in the machine...

Quiz 3

New Lessons Learned:

1. Learned about .cmd extension
2. RegShot tool – before and after system changes
3. Unrar x /UPX -d to unpack
4. Some Windows batch-fu (regedit /S)

Notes:

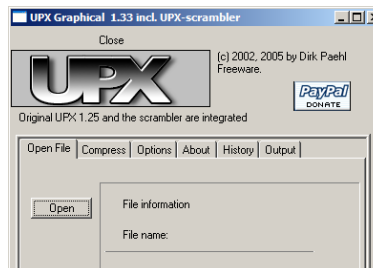
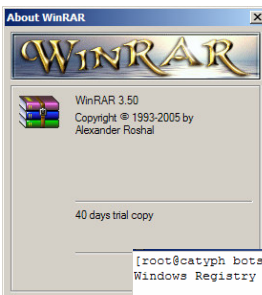
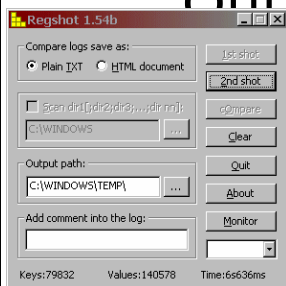
1) A .cmd extension is a Windows NT Command file script extension. It is only supported in WinNT and above. WinNT and above recognize .cmd files as executables and will run them. Win9x doesn't recognize .cmd as an executable file type. If you attempt to run a .cmd file under Win9x it will return a Bad command or file name error message. Its usage is similar to that of a batch file (.bat) in Win9x.

2) **Regshot** is a small, free and open-sourced registry compare utility that allows you to quickly take a snapshot of your registry and then compare it with a second one - done after doing system changes or installing a new software product. The changes report can be produced in text or HTML format and contains a list of all modifications that have taken place between snapshot1 and snapshot2. In addition, you can also specify folders (with sub folders) to be scanned for changes as well. It can be found here: <http://regshot.blog.googlepages.com/regshot.html>

3) If you identified a file to be packed with UPX/RAR, you could use the Linux applications UPX (<http://upx.sourceforge.com>) or unrar to unpack it.

4) If you attempt to open a .reg file using Regedit.exe the application will prompt you to add the entries to the registry. By using the /S flag a silent install occurs requiring no user intervention.

Quiz 3



```
[root@catyph bots]# more msnupdater.cmd
@echo off
echo Updating Windows Shell Files
REGEDIT.EXE /S 2377.reg
REGEDIT.EXE /S 5577.reg
echo Updating Windows Shell Files....
msnhomepage.html
echo Updating Windows Shell Files.....
yahoohomepage.html
echo Updating Windows Shell Files.....
echo Updating Windows Shell Files.....
echo Updating Windows Shell Files is now Complete.
exit
```

```
[root@catyph bots]# more 2377.reg
Windows Registry Editor Version 5.00
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Intern
et Settings\Zones\0]
"1004"=dword:00000000
"1201"=dword:00000000
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Intern
et Settings\Zones\1]
"1004"=dword:00000000
"1201"=dword:00000000
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Intern
et Settings\Zones\2]
"1004"=dword:00000000
"1201"=dword:00000000
```

4

- **Category: Visual and Behavioral Analysis**

- "What a Nice Postcard!"

- **The Mission:**

"One user in the organization received a phone call from his bank manager, telling that his account was empty and if something wrong happened. Our little Joe was completely astonished!! What did happen, he knew that he had some money in that bank account! So, he decided to take a look at his account and saw a lot a strange transfers from his account to a lot of different accounts...

As he doesn't have computer at home, he only uses his online bank at work and though that someone had stolen his passwords. The Incident Response Team was called to check his computer and found the following file in his computer, called *credito.scr*."

<http://handlers.sans.org/pbueno/ma4.html>



Part IV - Malware Analysis



Quiz 4

- Objectives:

- Analyze a piece of a Modified Password Stealer Trojan

- Specific questions:

1. Is this file packed? If so, which packer?
2. Without running the file, what do you think that this malware can and will do?
3. Now, using any methods available to you, which changes, if any, will this malware do in the system, among new files and registry entries...?
4. Now, what is the purpose of this malware?
6. Could you show any example of this malware behavior?

SANSFire 2006

<http://isc.sans.org>

Notes:

This was a real malware that I modified to include fake email address instead of the real ones.



Part IV - Malware Analysis

Quiz 4



</div>

Hello friend !

You have just received a postcard from someone who cares about you!

This is a part of the message:

"Hy there! It has been a long time since I haven't heard about you!

I've just found out about this service from Claire, a friend of mine who also told me that..."

If you'd like to see the rest of the message click here to

receive your animated postcard!

=====

Thank you for using www.yourpostcard.com 's services !!!

Please take this opportunity to let your friends hear about us by sending them a postcard from our collection !

=====

</div>

SANSFire 2006

<http://isc.sans.org>

Notes:

This is an example of the email received with the link to download the real malware.

Quiz 4

- New Lessons Learned:
 1. How to unpack Aspack:
 - AspackDIE!
 - pmak 2
 - On this quiz, it was used to unpack the malware, so information could be extract from it.
 2. Use of the Foremost to data carving
 - On this quiz, foremost was used to extract bank figures, like virtual keyboards, logos...all used on the banker trojan.

Notes:

1- AspackDie! – this one is an unpacker for files packed with Aspack. It can be found here: <http://www.exetools.com/unpackers.htm>. Another way to unpack aspack is the usage of pmak2 that can be found here: <http://www.pmode.net/USERS/117/Files/Pmak2.rar>

2- Foremost is a console program to recover files based on their headers, footers, and internal data structures. This process is commonly referred to as data carving. Foremost can work on image files, such as those generated by dd, Safeback, Encase, etc, or directly on a drive. The headers and footers can be specified by a configuration file or you can use command line switches to specify built-in file types. These built-in types look at the data structures of a given file format allowing for a more reliable and faster recovery. It can be found here: <http://foremost.sourceforge.net/>

Quiz 4

[AspackDie 1.41] by yoda - Select the target file...

Examinar: aspackdie



SRC



AspackDie.exe

Nome do arquivo:

Arquivos do tipo: EXE/DLL/OCX files

```

root@catyph output]# more audit.txt
Foremost version 1.2 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Thu May 18 10:21:44 2006
Invocation: /usr/local/bin/foremost -i Cartao.scr
Output directory: /home/malwares/output
Configuration file: /usr/local/etc/foremost.conf
-----
File: Cartao.scr
Start: Thu May 18 10:21:44 2006
Length: 3 MB (3799040 bytes)

Num  Name (bs=512)      Size  File Offset  Comment
---  -
0:    1486.jpg          74 KB    761247
1:    1650.jpg          20 KB    845162
2:    2002.jpg          22 KB   1025199
3:    2054.jpg          16 KB   1051804
4:    3306.jpg          64 KB   1692730
5:    3439.jpg           5 KB   1760899
6:    3450.jpg           3 KB   1766697
7:    3459.jpg          656 B   1771092
8:    3460.jpg          656 B   1771930
9:    3462.jpg          656 B   1772568
10:   3463.jpg          656 B   1773306
11:   3466.jpg          10 KB   1774638
12:                   1787709
13:                   1806563
14:                   1809790
15:                   1814526
16:                   1817834
17:                   1822510

```

```

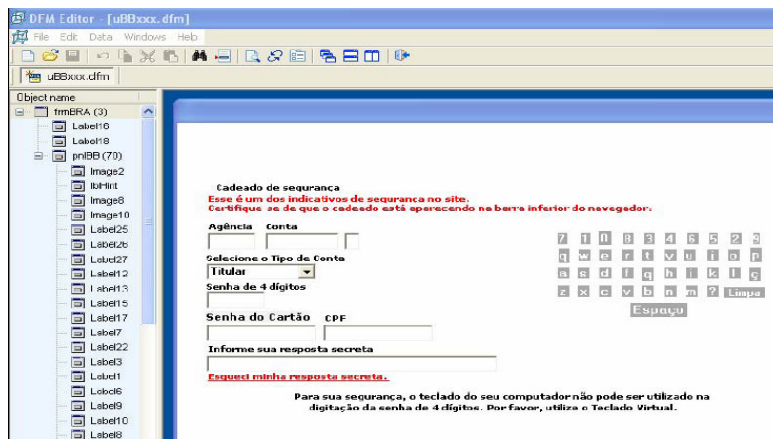
[root@catyph malwares]# file Cartao.scr
Cartao.scr: PE executable for MS Windows (GUI) Intel 80386 32-bit
[root@catyph malwares]# /usr/local/bin/foremost -i Cartao.scr
Processing: Cartao.scr
[*]
[root@catyph malwares]# cd output/
[root@catyph output]# ls
audit.txt  bmp  exe  jpg

```

Quiz 4

- New Lessons Learned: (cont.)

3. DFM Editor



SANSFire 2006

<http://isc.sans.org>

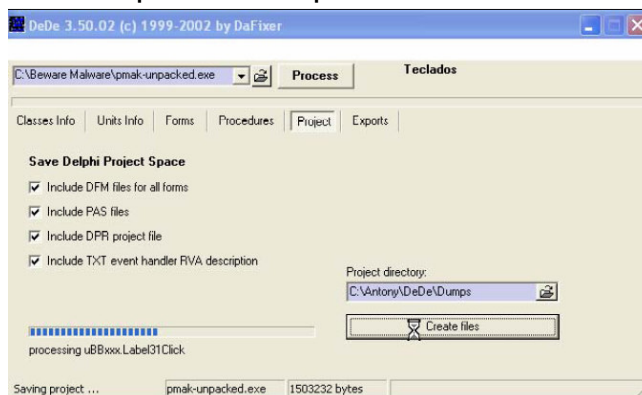
Notes:

3. DFM Editor – “Standalone editor for Delphi Form files (*.dfm) in both binary and text format. It has object tree, object inspector and syntax highlighted editor and form previewing capability. It can be extended with external packages (bpl files) to know more classes. Forms can also be extracted from executables or libraries. Supports D1-D7 forms. Free to use for both private and commercial users. “ It can be found here: <http://www.mitec.cz/Downloads/DFMEdit.zip>

Quiz 4

- New Lessons Learned: (cont.)

4. DeDe – Delphi Decompiler



SANSFire 2006

<http://isc.sans.org>

Notes:

4- DeDe – This is a delphi decompiler . It can be found here:
<http://download.softpedia.ro/software/PROGRAMMING/DeDe.3.50.02.1619.bin.rar>
 According the webpage:

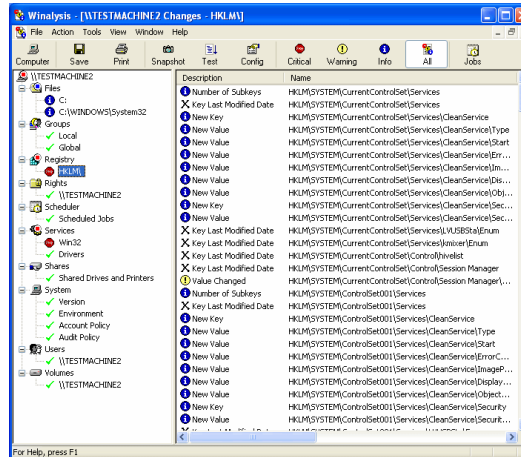
“DeDe is a very fast [program](#) that can analyze executables compiled with [Delphi](#) 2,3,4,5,6 Builder,Kylix and Kol and give you the following:

- All dfm files of the target. You will be able to open and edit them with Delphi.
- All published methods in well commented ASM code with references to strings, imported function calls, classes methods calls, components in the unit, Try-Except and Try-Finally blocks.
- (By default DeDe retrieves only the published methods sources, but you may also process another procedure in a executable if you know the RVA offset using the Tools\Disassemble Proc menu.)
- A lot of additional information.
- You can create a Delphi project folder with all dfm,pas, dpr files. Note: pas files contains the mentioned above well commented ASM code. They can not be recompiled !
- View the PE Header of all PE Files and change/edit the sections flags.
- Use the opcode-to-asm tool for translating [intel](#) opcode to assembler.
- Use RVA-to-PhysOffset tool for fast converting physical and RVA addresses.
- Use the DCU Dumper (view dcu2int.txt for more details) to retrieve near to pascal code of your DCU files.
- Use BPL(DPL) Dumper to see BPL exports and create symbol files to use with DeDe disassembler.
- Disassemble a target EXE directly from memory in case of a packed exe.”

Quiz 4

- New Lessons Learned: (cont.)

5. Winalysis



SANSFire 2006

<http://isc.sans.org>

Note:

5. Winalysis: “Winalysis is a program to detect changes on your computer caused by software installs or unauthorized access and optionally restore the Windows registry and selected files from snapshots. It allows you to save a snapshot of a computer's configuration and then monitor for changes to files, the registry, users, local and global groups, rights policy, services, the scheduler, volumes, shares. “

It can be found here: <http://www.winalysis.com/wnaly310.exe>

Quiz 5

- "My computer is just slow..."

- The Mission:

"A user called the help desk complaining that his computer was too slow, after following the basic IR procedures, the Incident Response Team was called."

<http://handlers.sans.org/pbueno/ma5.html>

Quiz 5

- **Category: Visual, Behavioral and Code Analysis**

- Objectives:

- Study a Bot for Windows

- Especific questions:

2. Without running the file, is it possible to identify what this malware can and will do?
3. Now, using any methods available to you, which changes, if any, will this malware do in the system, among new files and registry entries...?
5. When will this malware be triggered/start?
6. Can you explain the netstat output?
7. What about the TaskManager screenshot? What useful information can you get?
8. About the creztu file, please explain each of the files that it contain! :)

Quiz 5

New Lessons Learned:

1. Meaning of configuration files of mIRC, used by some bots!
2. Use of Stud_PE to analyze the malware on Windows (headers, packers...)
3. Sysinternal Kit:
 - RegMon - registry monitoring
 - Filemon - file monitoring
 - TDImon - monitor monitor TCP and UDP activity
 - Process explorer - monitor the process activity

Notes:

1) Files:

aliases.ini Aliasing commands for mIRC

Control.ini As if mIRC version 6.01 "The control dialog lists, ie. ignore, voice, protect, op, are now stored in acontrol.ini file"

Mirc.ico A blank icon to hide mIRC from showing in the taskbar

Moo.dll DLL for getting OS and hardware information

Nicks.txt Random names used to generate a NICK

Perform.ini Used to set commands to perform automatically on connect.

Popups.ini Sets the popups which are like alias but require mouse intervention rather than typing
/<command>

Radmin.txt Header for scan results of port 4899 "Radmin"

Remote.ini By default the remote users list, variables and scripts are saved in the remote.ini file.

Run.exe Looks like left over from another variant of this BOT/ Backdoor / Trojan

Script.ini Scripts for this BOT such as a SCANNER, file find, random name gen....etc

Servers.ini List of IRC servers in the Undernet range

Sup.bat Install script file run by the winrar SFX

Sup.reg Reg file containing the registry entries added start the mIRC BOT up

Svchost.exe mIRC application with a name change

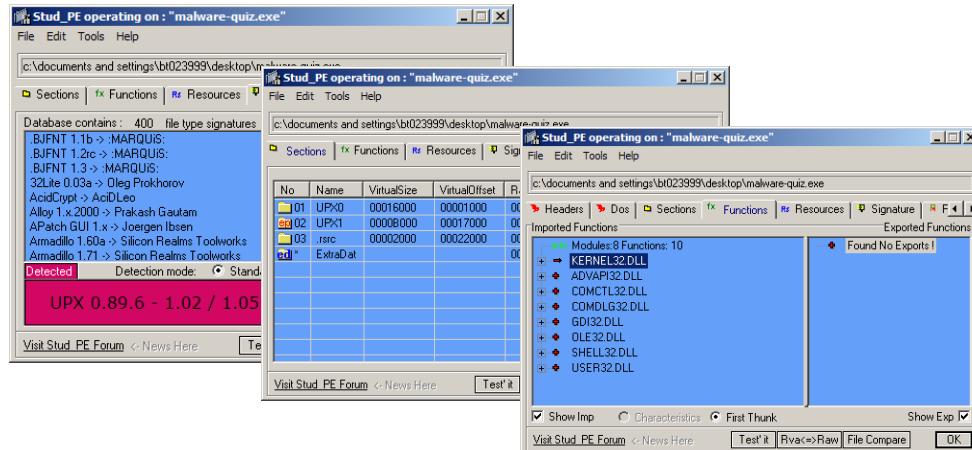
Users.ini Sets the users which can talk to the bot

2) Stud_PE - Stud_PE is a Portable Executable Viewer/Editor. It can be found here
<http://www.cgsoftlabs.ro/studpe.html>

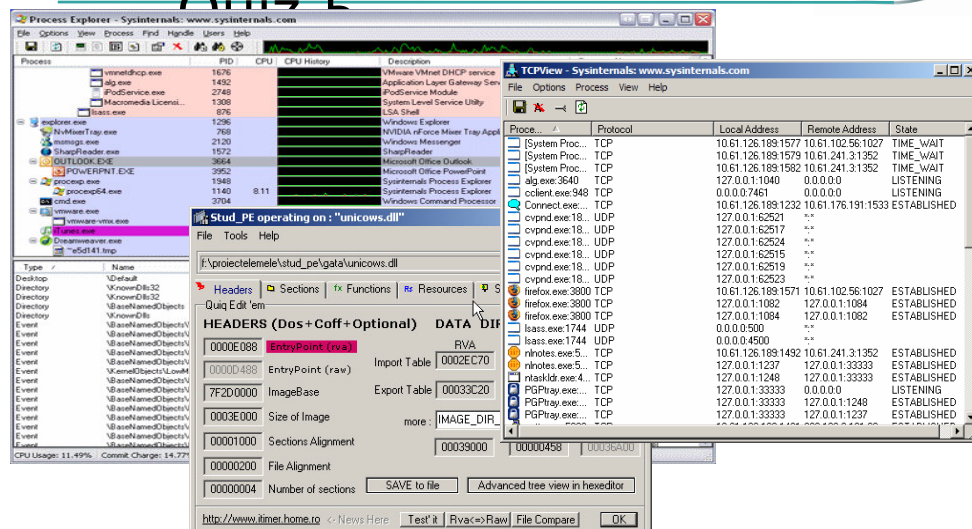
3) Sysinternal tools can be found at <http://www.sysinternals.com>

Quiz 5

- Stud_pe is almost a swiss knife!



Quiz 5



Quiz 6

- “The Empire Strikes Back”
...or “Arghhh...there ARE bots for Linux!”



- The Mission:

“This system is a Linux box...everything was calm until the ISP received a report about this machine being scanning other machines...”

Our great guys from the Incident Response Team was called again...”

<http://handlers.sans.org/pbueno/ma6.html>



6 • Objectives:

- Bots and remote control application

• Specific Questions:

2 (a & b). (a) Without running the applications, identify what the malware can/will do, then (b) run the applications and identify additional details evident when the applications are run.

4. Now, what are the purpose of the malware? Are they related?

7. About the 'shell' and cmd.gif file, what useful information could you get?

6 New Lessons Learned:

1. Linux Toolkit:
 - Strings!
 - Objdump -d and Objdump -x
 - Strace -f -o out ./shell &
 - Nm
2. A password cracker: John the ripper
3. A Ircd server: Ng-ircd
4. Use of a Disassembler! Did you hear IDA?

Notes:

1) Linux Toolkit

- Our old and good strings!
- Objdump -d, --disassemble Display assembler contents of executable sections
- x, --all-headers Display the contents of all headers
- nm - list symbols from object files
- strace - trace system calls and signals

2) John the ripper is a famous password cracker. It can be found here:
<http://www.openwall.com/john/>

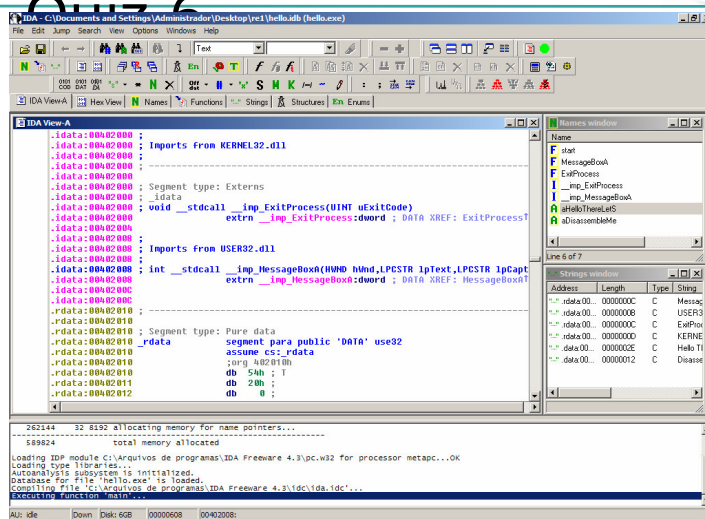
3) ng-ircd is a ircd server that can be used to simulate a botnet. It can be found here: ng-ircd; see <http://ngircd.barton.de/>

4) *“IDA Pro combines an interactive, programmable, multi-processor disassembler coupled to a local and remote debugger and augmented by a complete plugin programming environment.”* It can be found here:
<http://www.datarescue.com/idabase/>

<http://isc.sans.org>

-“Kaiten wa goraku”

Quiz 6



Conclusion

- Different approaches can lead to the same results!
- Different tools can lead to the same results!
- Choose your tools of confidence and let the game begin!
- Remember that if you have a problem, probably there is a specific tool for your need!
- Did you miss Ollydbg?? Yes...me too...☺
Learn how to use it!!
 - ps: take a look at ollyscript and ollydump...;)
- Do you know Lenny's class? Reverse Engineering Malware? ☺

SANSFire 2006

<http://isc.sans.org>

Conclusion

And remember...

- *A wise man gets more use from his enemies than a fool from his friends.*

– Baltasar Gracian

Questions?



Do you have any questions ? ? ?

- I would like to thank all the persons below who spent lots of time to complete the Quizes!



Dr.Neal, Tyler Hudak, Ivan Macalintal, Jack McCarthy, Anthony Thompson, Cory Dodds, Jeremy Scott, Fixer, Thomas Prokosch, Nicholas Albright , Lenny C, Patrick Kennedy, Kevin Johnston, Joao Azevedo ,Rudolph Pereira, Dean de Beer, Randy Armknecht, Michel Jordon, Jeremy Scott, Michel Ligh, Justin Acquaro, Jacomo Piccolini, Zach Jansen, Neil Desai, Steve Caligo, Anthony Martinez, Jim Halfpenny.

