SAND2008-4243P

REM 101

An Introduction to Reverse Engineering Malware

J. Larry Dishman
Senior Member of Technical Staff

LOCKHEED MARTIN

Sandia National Laboratories

Agenda

- **General Requirements**
- Overview of Malware Analysis
- Tools of the trade
- Analysis Fundamentals
- Setting up the Environment
- Time to give it a try
- Tips and Sources

Hardware & Software

- **The system used** MUST NOT CONNECT TO A PRODUCTION NETWORK WHILE DOING ANALYSIS WORK**. Never connecting is better**
- **A Windows XP laptop**
- **A system with a 1 GHz processor (faster is better)**
- **A system with a minimum of 1Gb RAM (more would be better)**
- **Lots of open space on the hard drive**

Myths about REM

- You need to be a great programmer
- You need an in-depth understanding of assembly code
- It's too hard to figure out what's going on
- You must be an uber-geek to understand this stuff
- It cost lots of money to do REM (Reverse Engineering Malware)

Facts about REM

- It's a learned process
- It's more of an art than a science
- It's like solving a big puzzle
- The more you do the better you get
- It's really FUN!

What won't be covered

- This is an introductory class
  - In-depth unpacking of packed executables
  - In-depth assembly code analysis
  - In-depth Wireshark usage
  - In-depth debugger usage

Why do REM?

- December 04, 2007 **(IDG News Service) – "Finnish security vendor F-Secure has collected twice as many malicious software samples this year as it has over the last 20 years, a trend that highlights the growing danger of malicious software on the Internet."**
- APRIL 22, 2008 **Sophos: "Infected Webpage Found Every 5 Seconds. One new infected Webpage found every five seconds, reveals latest Sophos security threat report**
- **Sooner or later we will get malware installed in our environment."**

Sandia National Laboratories

Agenda

- General Requirements
- **Overview of Malware Analysis**
- Tools of the trade
- Analysis Fundamentals
- Setting up the Environment
- Time to give it a try
- Tips and Sources

What to look for?

- Strange behavior from server or workstation that can't be fixed by normal processes
- Unusual inbound connections
- Unusual outbound connections, especially from known Trojans or services. (example port 12345 (hacker haven)
- Unusual or unknown processes running

Software Ports

- The ephemeral ports (0 through 1023), sometimes also known as trusted ports, can only be used by system (or root) processes or by programs executed by privileged users on most systems. The others include registered ports (1024 through 49151) and dynamic and/or private ports (49152 through 65535). Dynamically assigned ports are opened and closed by the server(s) as needed.
- Trojan port list http://www.glocksoft.com/trojan_port.htm
- Port information http://www.iana.org/assignments/port-numbers or http://insecure.org/nmap/data/nmap-services

When you find malware

- It's the same as incident handling, stop the bleeding first.
  1. Preparation
  2. Identification
  3. Containment
  4. Eradication
  5. Recovery
  6. Follow-Up

Safety

- Handle malware with care
- Use command line to copy/move
- Remove files from non-test systems
- Label storage media you save it to
- Password protect the folder so you don't accidentally infect yourself
- Don't multitask, your mind needs to be on what you are doing
- Don't put it on a live network

Agenda

- General Requirements
- Overview of Malware Analysis
- **Tools of the Trade**
- Analysis Fundamentals
- Setting up the Environment
- Time to give it a try
- Tips and Sources

Minimum Tool Set

- VMWare Player
- Md5sums
- Wireshark
- RegShot
- OllyDbg
- Netcat
- UPX
- WinRAR-Trial or PeaZip
- BinText
- Sysinternal tools

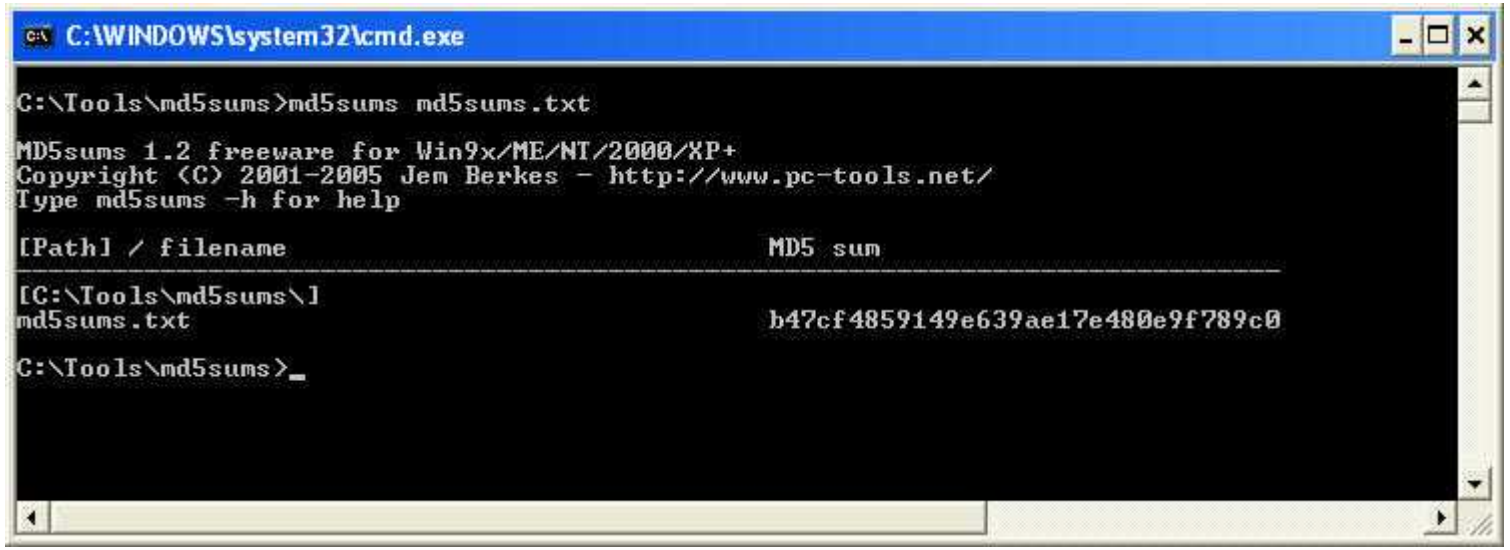
VMWare Player

- **Allows you to run virtual machines (more than 1 OS) on your system.**

Sandia National Laboratories

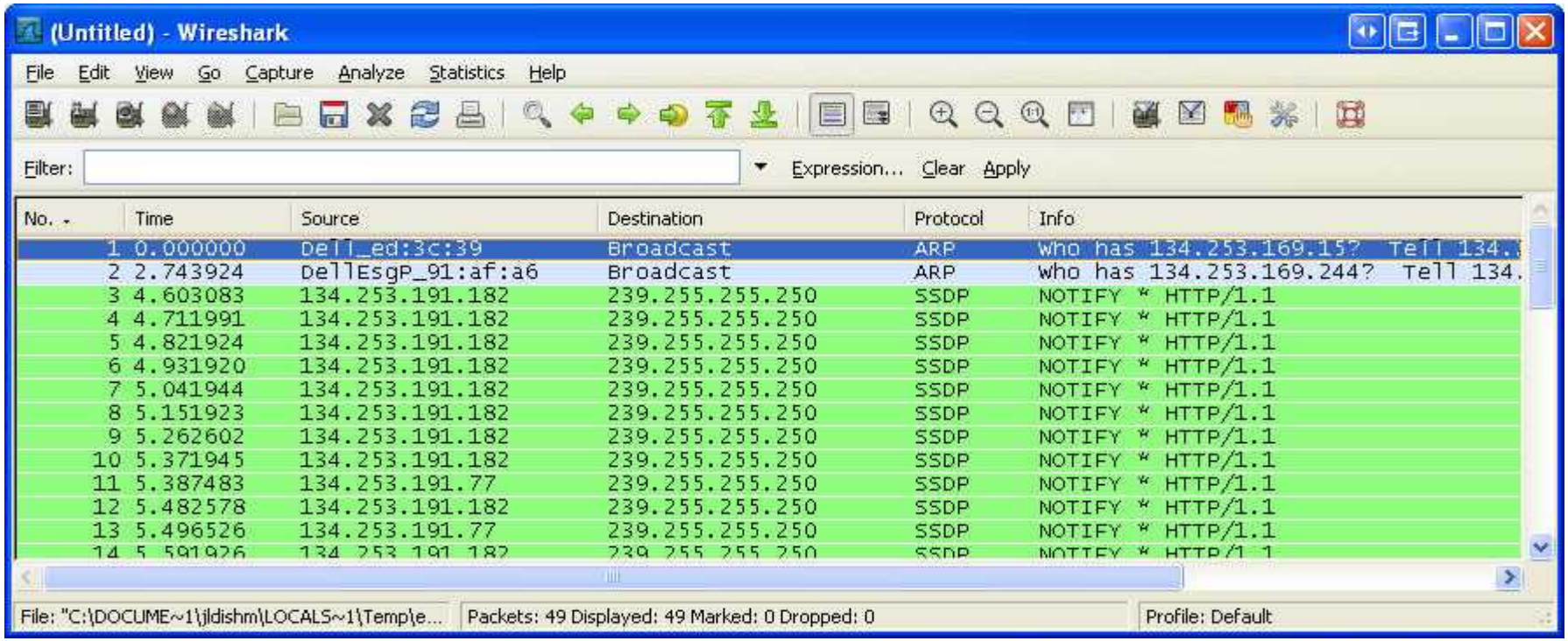
Md5sums

- Used to create a message digest (hash) of a file.
- If the files are the same the hash will be the same.



Wireshark

- **A protocol analyzer (sniffer) used to see the network activity of our sample.**



Sandia National Laboratories

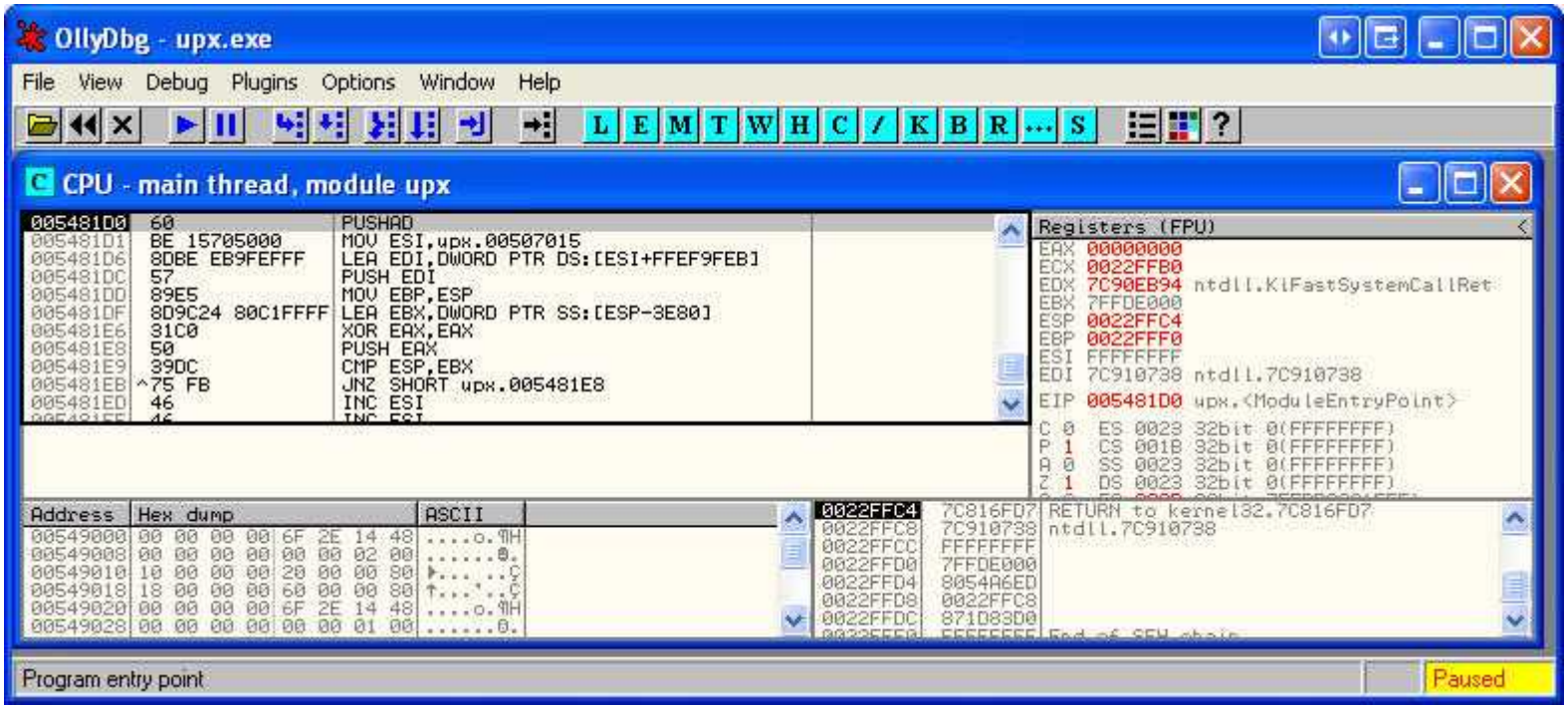
RegShot

- **A tool that takes a ‘before and after’ shot of your systems and tells you what has changed.**

Sandia National Laboratories

OllyDbg

- **Assembly level debugger for Windows.**
- **We will use it for viewing code and program flow.**



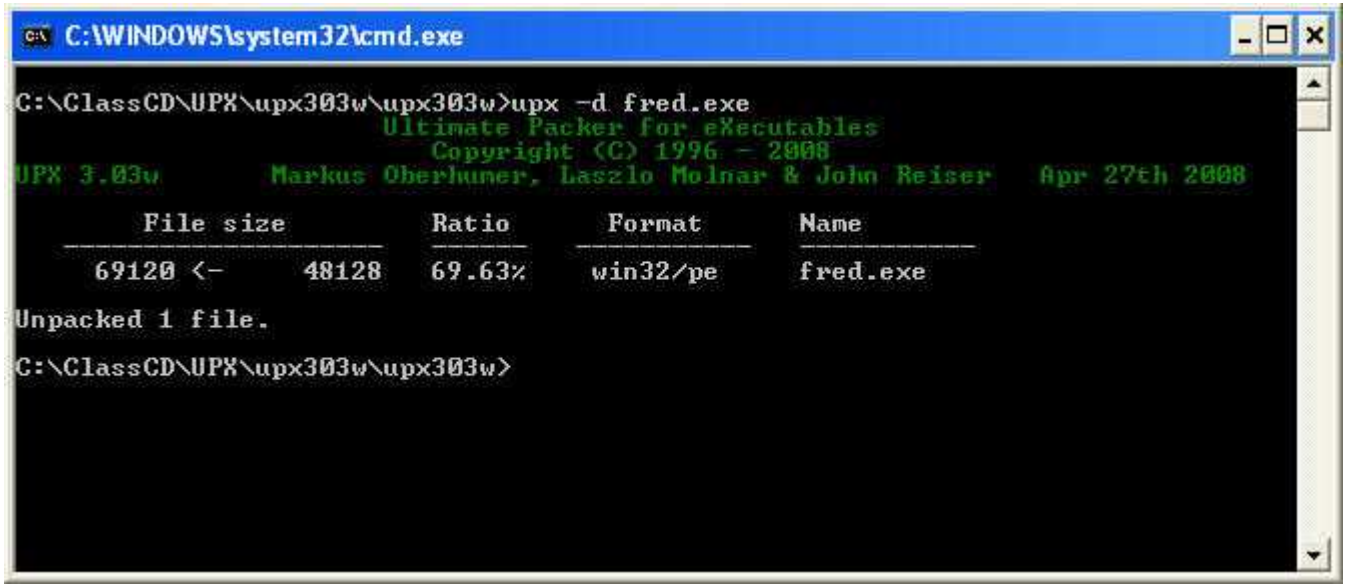
Sandia National Laboratories

Netcat

- It's known as the "Swiss army knife" of the network.
- We will use it when the malware needs something to connect to across the network.
- nc –L –p 80 will listen for incoming connections on port 80
- nc –L –p 80 –e cmd.exe for remote access to a command shell
- nc 192.168.10.100 80 to connect to remote system
- nc –l –p 5678 > file.txt type file.txt > nc 192.168.10.100 5678

UPX

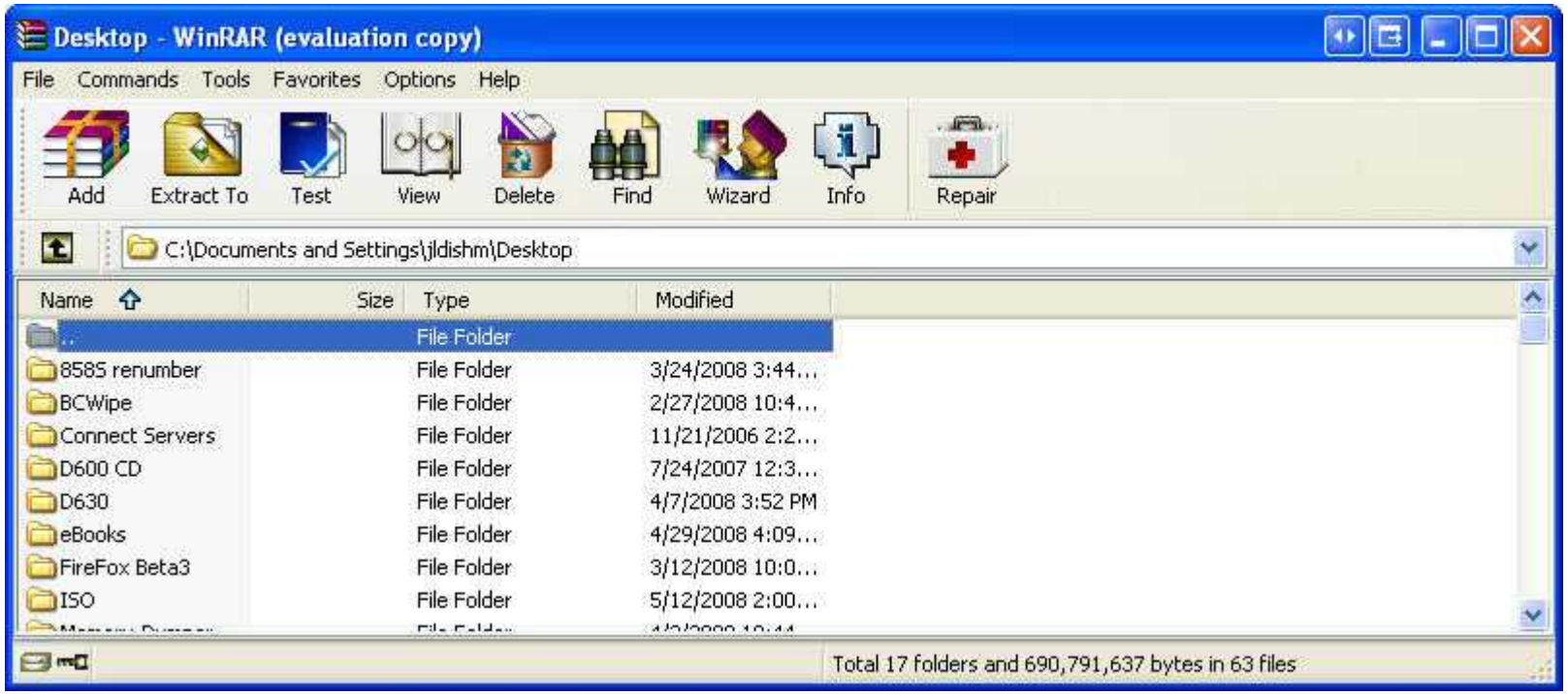
- A packer used to compress and obfuscate code.
- UPX –d file.exe to unpack the file.



Sandia National Laboratories

WinRAR-Trial

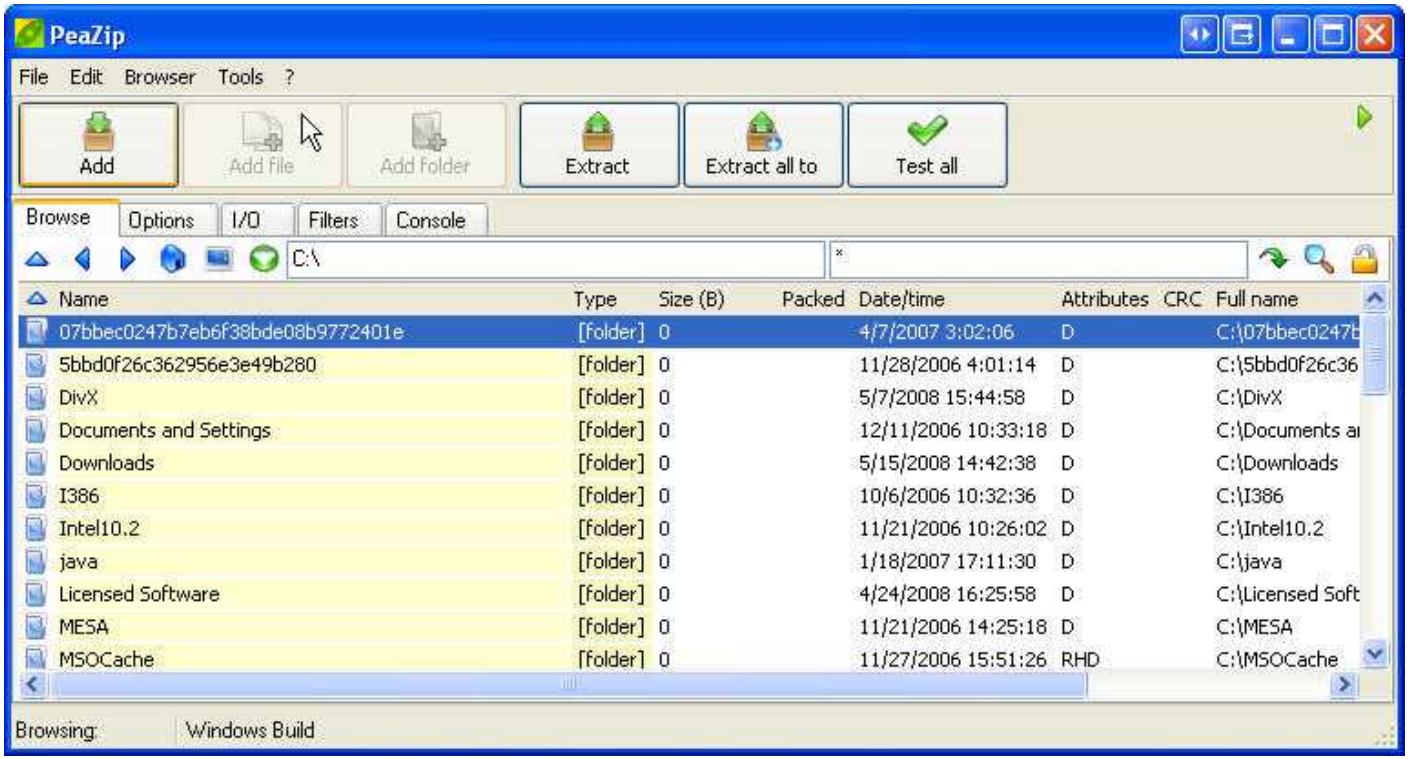
- **A tools to compress/decompress files and folders in various formats.**



Sandia National Laboratories

PeaZip

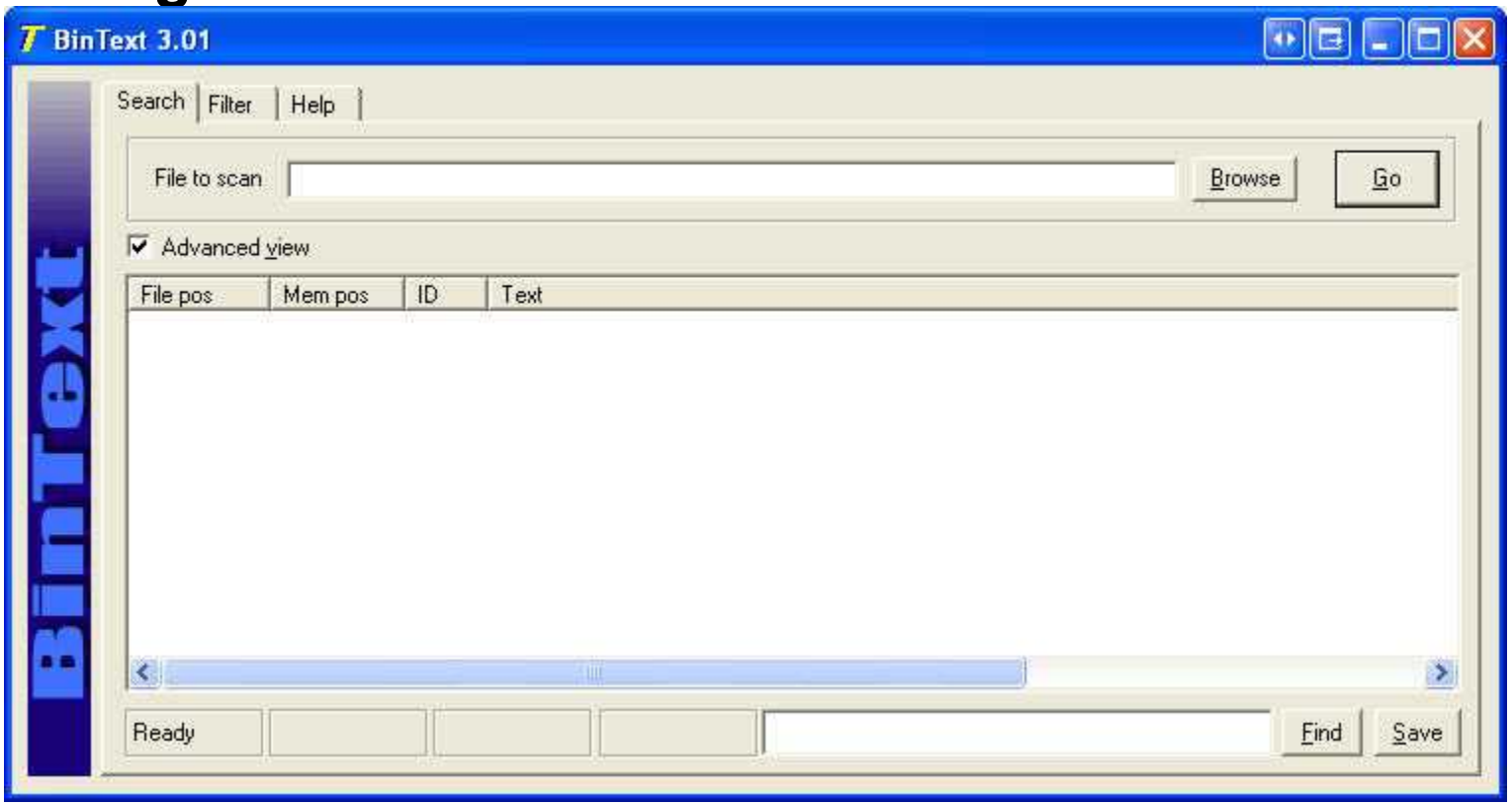
- **A tools to compress/decompress files and folders in various formats.**



Sandia National Laboratories

BinText

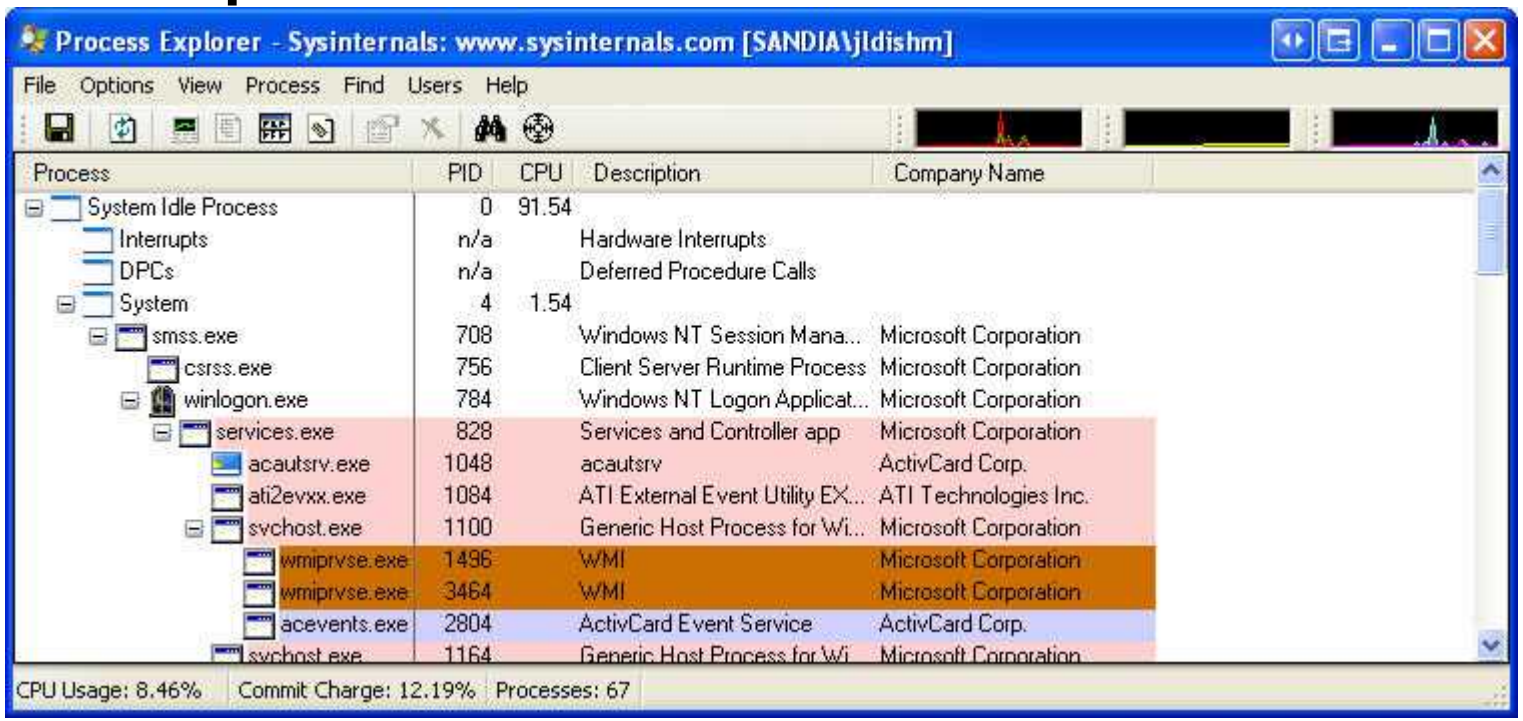
- A GUI utility for Windows that extracts ASCII strings from executable files.



Sandia National Laboratories

Process Explorer

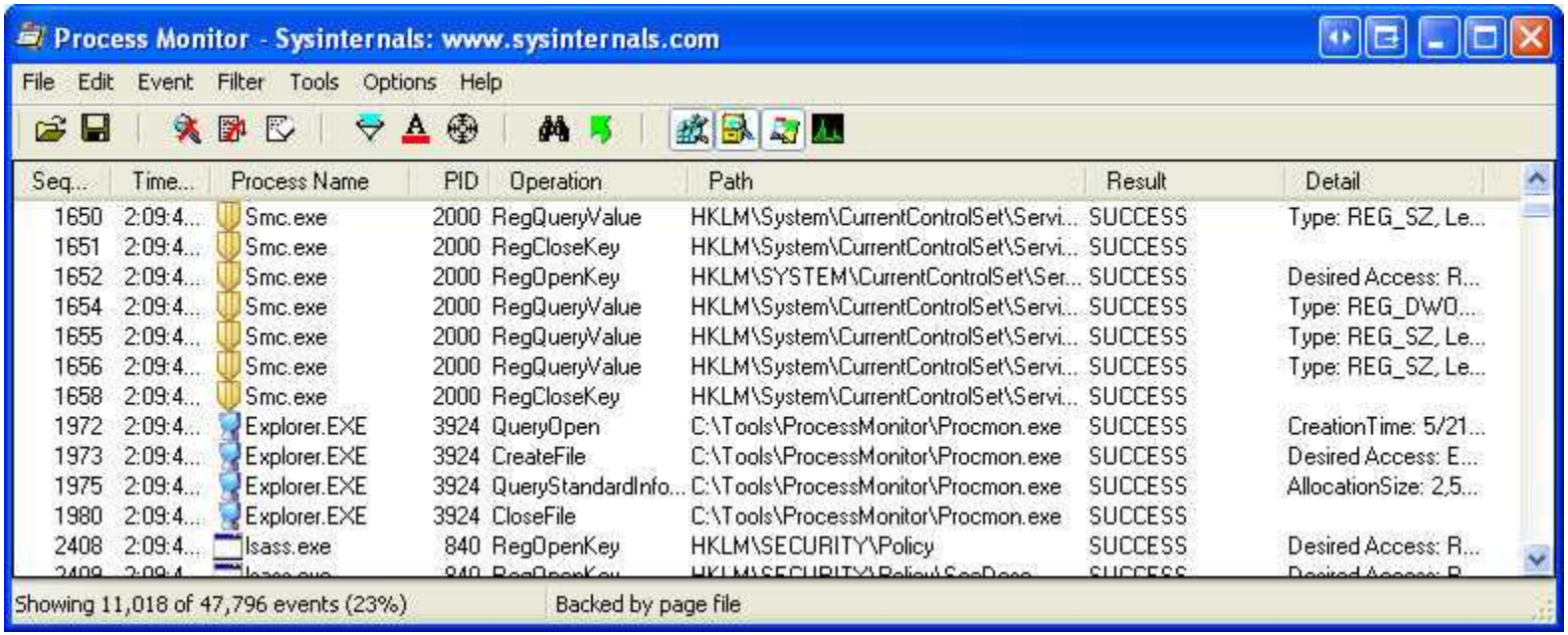
- **Process Explorer – allows you to see what processes, files and DLLs are running or have been opened.**



Sandia National Laboratories

Process Monitor

- **Process Monitor – monitors file system, registry, process, thread and DLL activity in real-time.**



Sandia National Laboratories

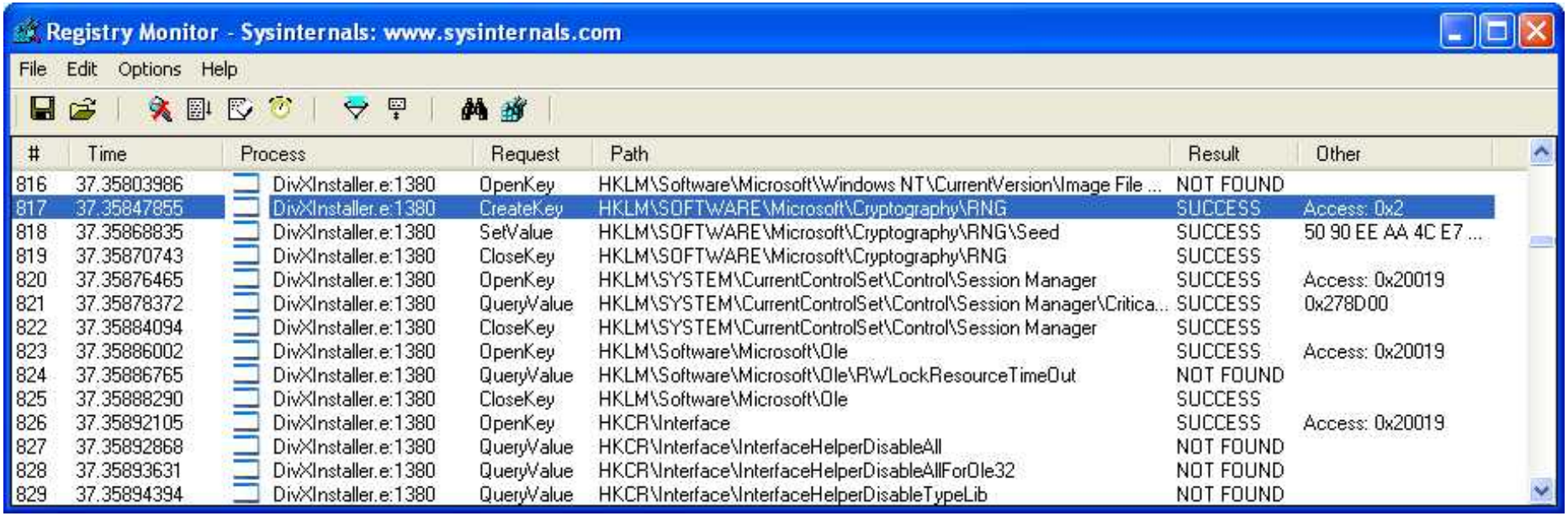
TCPview

- **TCPview – Views all open ports and tells you what process owns them.**

Sandia National Laboratories

Regmon

- **Monitors the system registry for read, access and write changes in real time.**

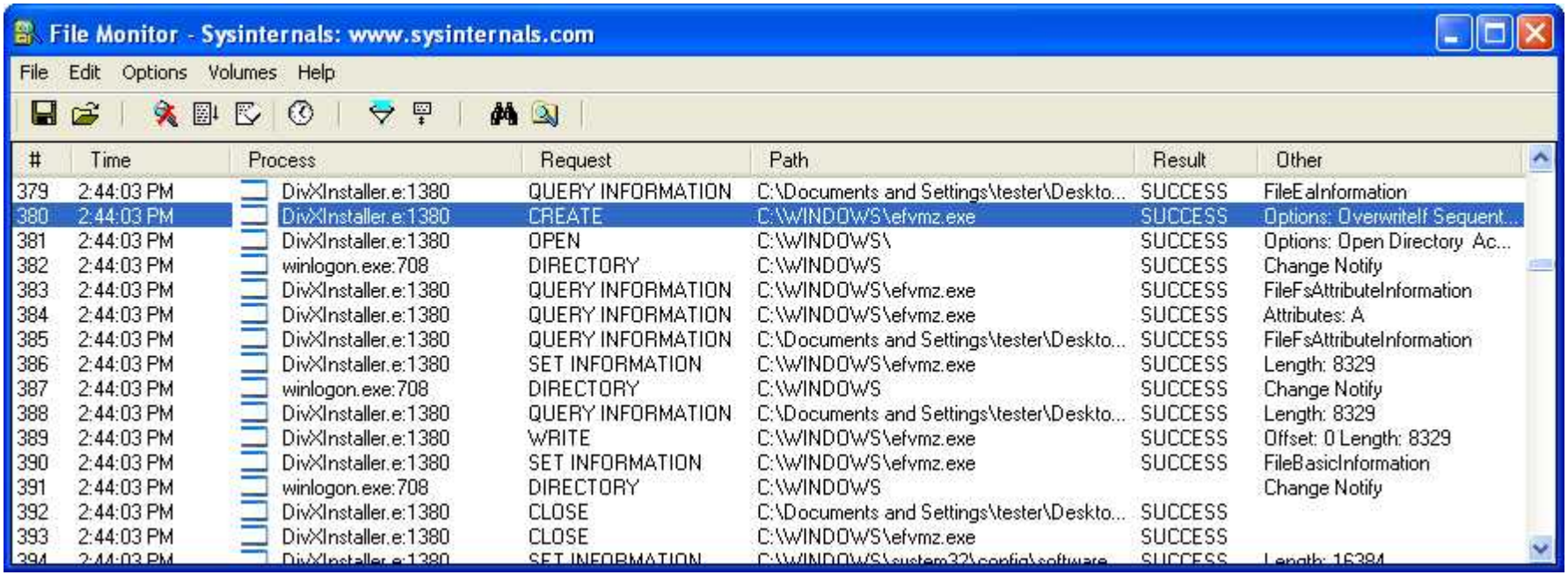


#	Time	Process	Request	Path	Result	Other
816	37.35803986	DivXInstaller.e:1380	OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File ...	NOT FOUND	
817	37.35847855	DivXInstaller.e:1380	CreateKey	HKLM\SOFTWARE\Microsoft\Cryptography\RNG	SUCCESS	Access: 0x2
818	37.35868835	DivXInstaller.e:1380	SetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS	50 90 EE AA 4C E7 ...
819	37.35870743	DivXInstaller.e:1380	CloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\RNG	SUCCESS	
820	37.35876465	DivXInstaller.e:1380	OpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	SUCCESS	Access: 0x20019
821	37.35878372	DivXInstaller.e:1380	QueryValue	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Critica...	SUCCESS	0x278D00
822	37.35884094	DivXInstaller.e:1380	CloseKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	SUCCESS	
823	37.35886002	DivXInstaller.e:1380	OpenKey	HKLM\Software\Microsoft\Ole	SUCCESS	Access: 0x20019
824	37.35886765	DivXInstaller.e:1380	QueryValue	HKLM\Software\Microsoft\Ole\RWLockResourceTimeOut	NOT FOUND	
825	37.35888290	DivXInstaller.e:1380	CloseKey	HKLM\Software\Microsoft\Ole	SUCCESS	
826	37.35892105	DivXInstaller.e:1380	OpenKey	HKCR\Interface	SUCCESS	Access: 0x20019
827	37.35892868	DivXInstaller.e:1380	QueryValue	HKCR\Interface\InterfaceHelperDisableAll	NOT FOUND	
828	37.35893631	DivXInstaller.e:1380	QueryValue	HKCR\Interface\InterfaceHelperDisableAllForOle32	NOT FOUND	
829	37.35894394	DivXInstaller.e:1380	QueryValue	HKCR\Interface\InterfaceHelperDisableTypeLib	NOT FOUND	

Sandia National Laboratories

Filemon

- **Monitors and displays file system activity on a system in real time.**



#	Time	Process	Request	Path	Result	Other
379	2:44:03 PM	DivXInstaller.e:1380	QUERY INFORMATION	C:\Documents and Settings\tester\Deskto...	SUCCESS	FileEaInformation
380	2:44:03 PM	DivXInstaller.e:1380	CREATE	C:\WINDOWS\efvmz.exe	SUCCESS	Options: OverwriteIf Sequent...
381	2:44:03 PM	DivXInstaller.e:1380	OPEN	C:\WINDOWS\	SUCCESS	Options: Open Directory Ac...
382	2:44:03 PM	winlogon.exe:708	DIRECTORY	C:\WINDOWS	SUCCESS	Change Notify
383	2:44:03 PM	DivXInstaller.e:1380	QUERY INFORMATION	C:\WINDOWS\efvmz.exe	SUCCESS	FileFsAttributeInformation
384	2:44:03 PM	DivXInstaller.e:1380	QUERY INFORMATION	C:\WINDOWS\efvmz.exe	SUCCESS	Attributes: A
385	2:44:03 PM	DivXInstaller.e:1380	QUERY INFORMATION	C:\Documents and Settings\tester\Deskto...	SUCCESS	FileFsAttributeInformation
386	2:44:03 PM	DivXInstaller.e:1380	SET INFORMATION	C:\WINDOWS\efvmz.exe	SUCCESS	Length: 8329
387	2:44:03 PM	winlogon.exe:708	DIRECTORY	C:\WINDOWS	SUCCESS	Change Notify
388	2:44:03 PM	DivXInstaller.e:1380	QUERY INFORMATION	C:\Documents and Settings\tester\Deskto...	SUCCESS	Length: 8329
389	2:44:03 PM	DivXInstaller.e:1380	WRITE	C:\WINDOWS\efvmz.exe	SUCCESS	Offset: 0 Length: 8329
390	2:44:03 PM	DivXInstaller.e:1380	SET INFORMATION	C:\WINDOWS\efvmz.exe	SUCCESS	FileBasicInformation
391	2:44:03 PM	winlogon.exe:708	DIRECTORY	C:\WINDOWS		Change Notify
392	2:44:03 PM	DivXInstaller.e:1380	CLOSE	C:\Documents and Settings\tester\Deskto...	SUCCESS	
393	2:44:03 PM	DivXInstaller.e:1380	CLOSE	C:\WINDOWS\efvmz.exe	SUCCESS	
394	2:44:03 PM	DivXInstaller.e:1380	SET INFORMATION	C:\WINDOWS\system32\config\software	SUCCESS	Length: 16384

Sandia National Laboratories

Other Tools

- These tools are not free, but worth the money if you get into REM.
- Ida Pro Full Version– A dis-assembler and debugger all rolled into one http://www.hex-rays.com/idapro/ Free version is included on the CD.
- VMWare workstation – used to create virtual environments
- WinRAR – Full version used to create password protected archive files

Agenda

- General Requirements
- Overview of Malware Analysis
- Tools of the Trade
- **Analysis Fundamentals**
- Setting up the Environment
- Time to give it a try
- Tips and Sources

Analysis Fundamentals

- The analysis is divided into three parts.
  - Visual Analysis – what can you tell from just looking around?
  - Behavioral Analysis – what happens when the malware is executed?
  - Code Analysis – view the actual code to understand what the malware is doing.

Visual Analysis

- What's the file type? exe, bat, xls, zip, etc.
- What size is the file? Large or small
- Where did it come from? Email, website, file download, etc.
- Can you see any ASCII strings in it?
- What's the MD5 hash and has it been seen before?

Behavioral Analysis

- How was it launched?
- What traffic is being generated?
- What protocol is being used?
- What files were installed or modified and where?
- Were any entries made in the registry?
- Does it restart after a reboot?
- Are there any listening ports?

Code Analysis

- If the code is compressed, what was used to compress it?
- After it's uncompressed can you see additional strings?
- If it's being remotely controlled, is authentication required?
- Look for key pieces of code.

Code Analysis

- A few of the key structures to look for
  - stricmp or strcmp (string compare)
  - retn (returns to calling program)
  - call (calls a subroutine)
- These are all usually good places to set breakpoints in your debugger.

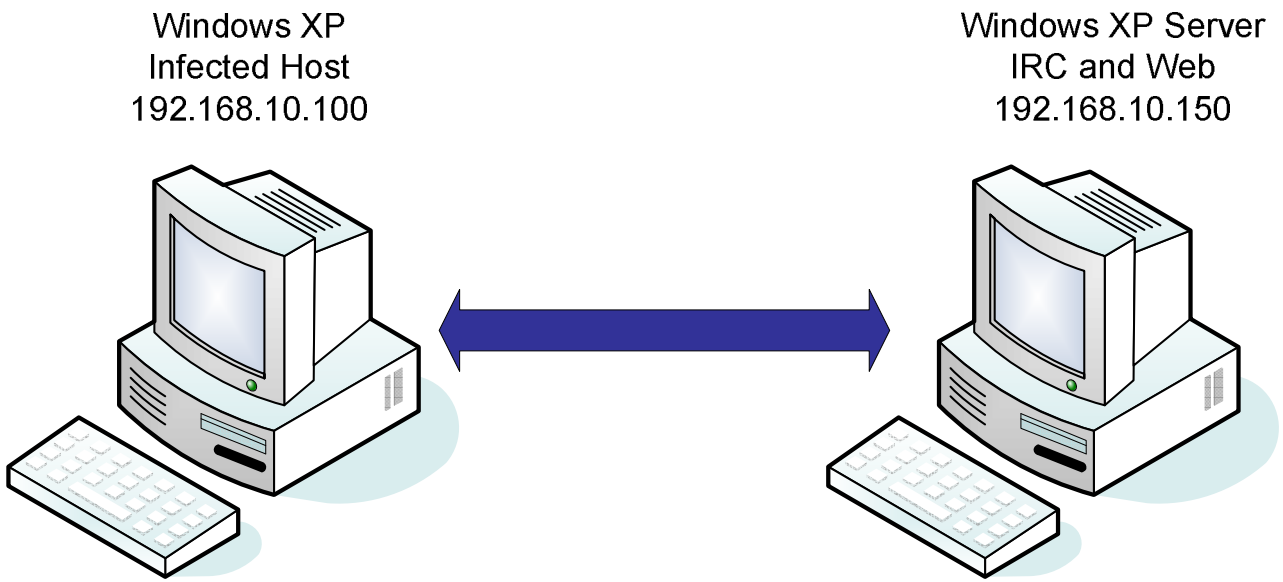
Agenda

- General Requirements
- Overview of Malware Analysis
- Tools of the Trade
- Analysis Fundamentals
- **Setting up the Environment**
- Time to give it a try
- Tips and Sources

Software Setup

- From the CD provided:
- Copy the VMWare-Player folder to your desktop and install it.
- After you install the player you can delete the install folder from your desktop.
- Copy the My Virtual Machines directory to your my documents folder.

The Virtual Environment Setup



Agenda

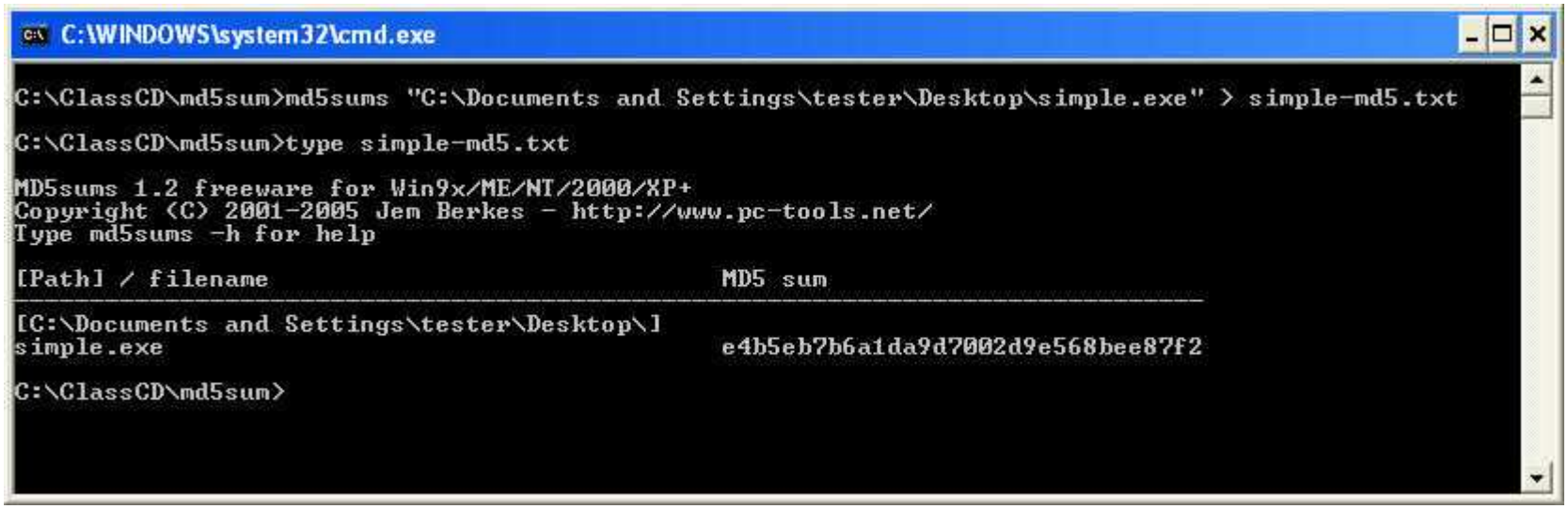
- General Requirements
- Overview of Malware Analysis
- Tools of the Trade
- Analysis Fundamentals
- Setting up the Environment
- **Time to give it a try**
- Tips and Sources

Simple.exe analysis

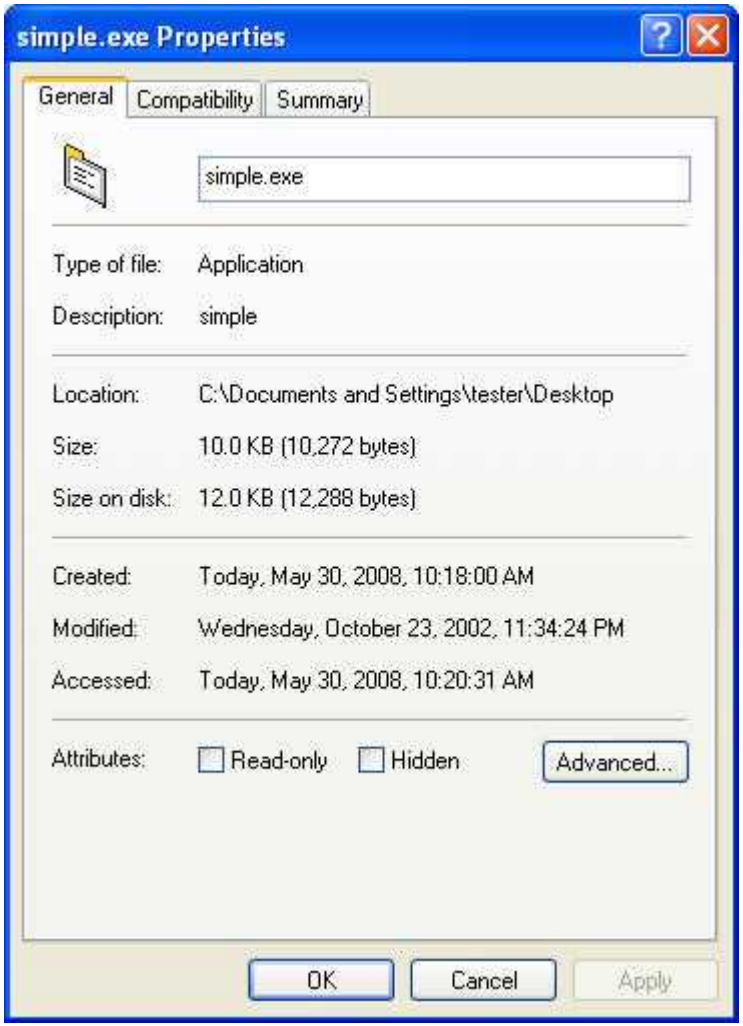
- First – Get the sample into your test environment.
- Second – Create an md5 hash for future reference.
- Third – Look for visual clues, file type and strings.
- Fourth – Run in test environment and monitor system and network activity.
- Repeat until you understand what it's doing.
- Fifth – Use code analysis if required.

MD5 Hash

- **Md5sums simple.exe > simple-md5.txt**

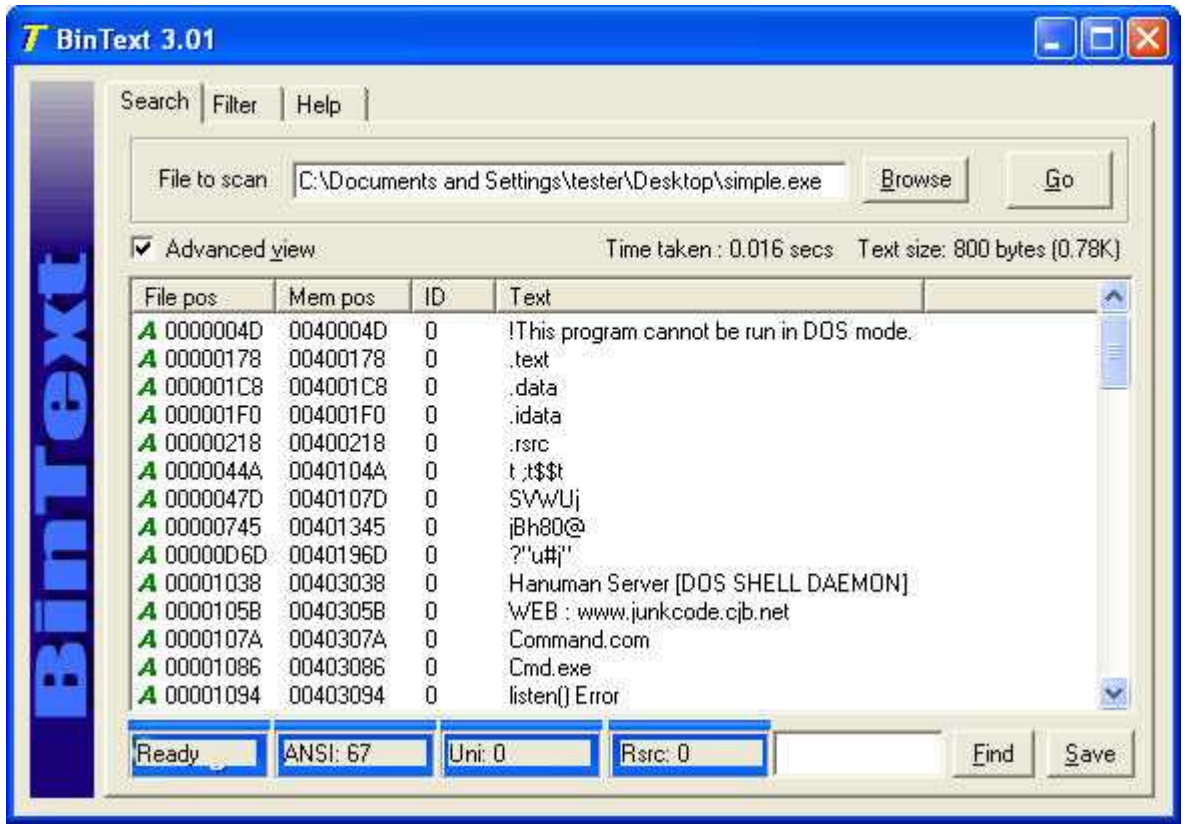


Visual Clues



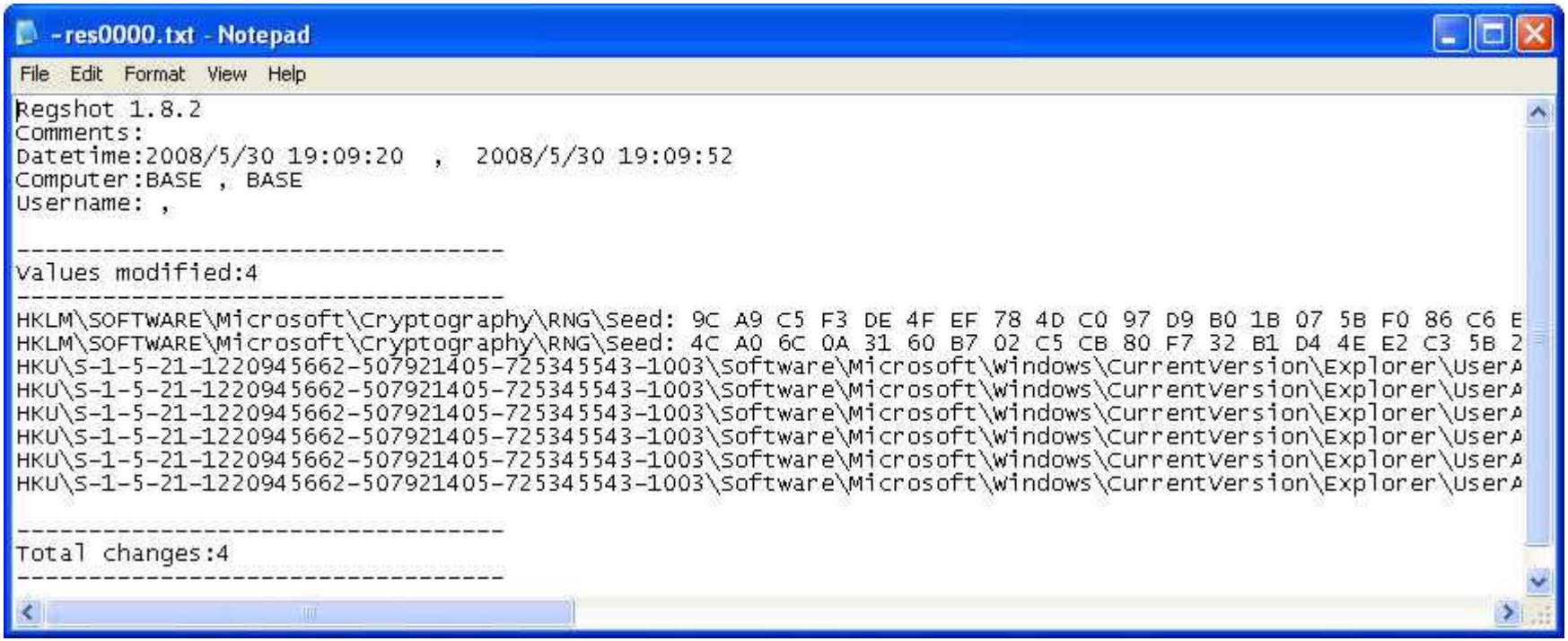
Sandia National Laboratories

Simple.exe Strings



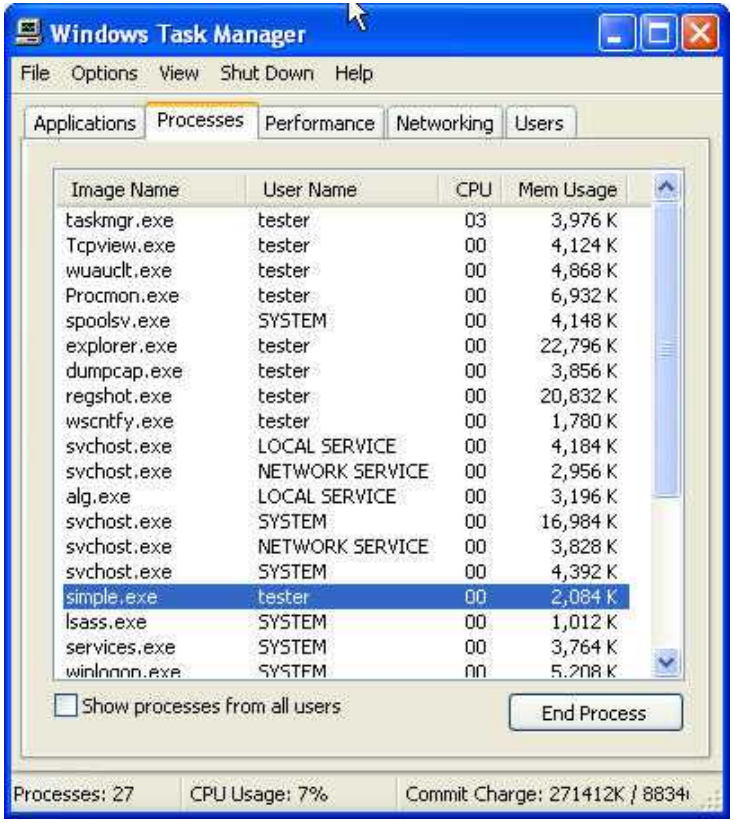
Sandia National Laboratories

Simple.exe RegShot



Simple.exe

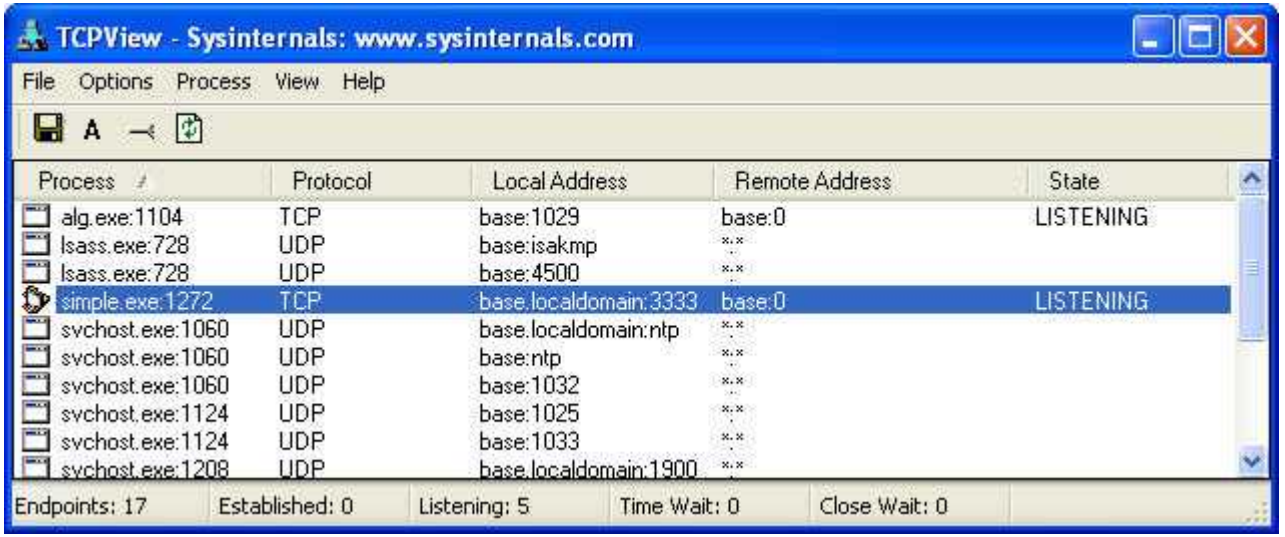
- Does it show up in Task Manager?



Sandia National Laboratories

Simple.exe TCPview

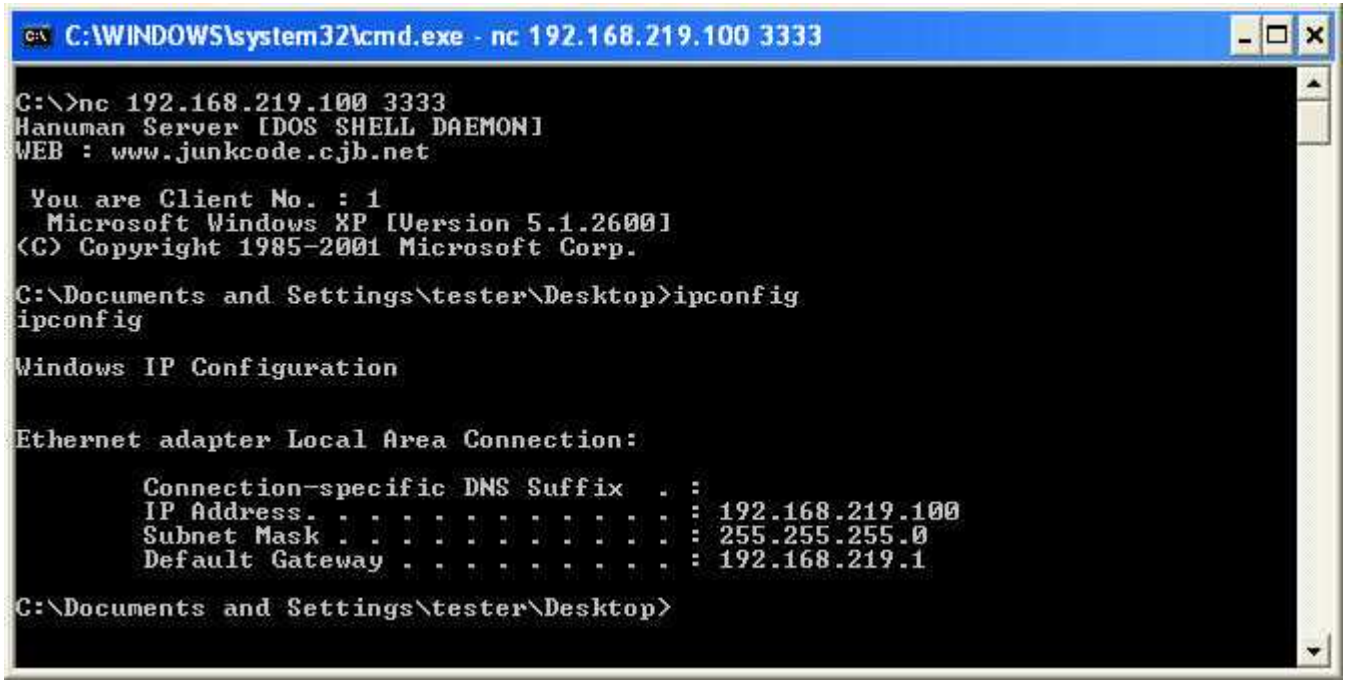
- It sets up a listening port on port 3333.



Sandia National Laboratories

Network Activity

- Let's try and connect to the "listening" port. Time to use netcat.



What can we say about simple.exe

- It is a relatively simple backdoor Trojan.
- It allows remote unauthenticated connections on software port 3333.
- It shows up in task manager and the process can be killed.
- It doesn't have a restart mechanism.

Manager calls at 2 AM

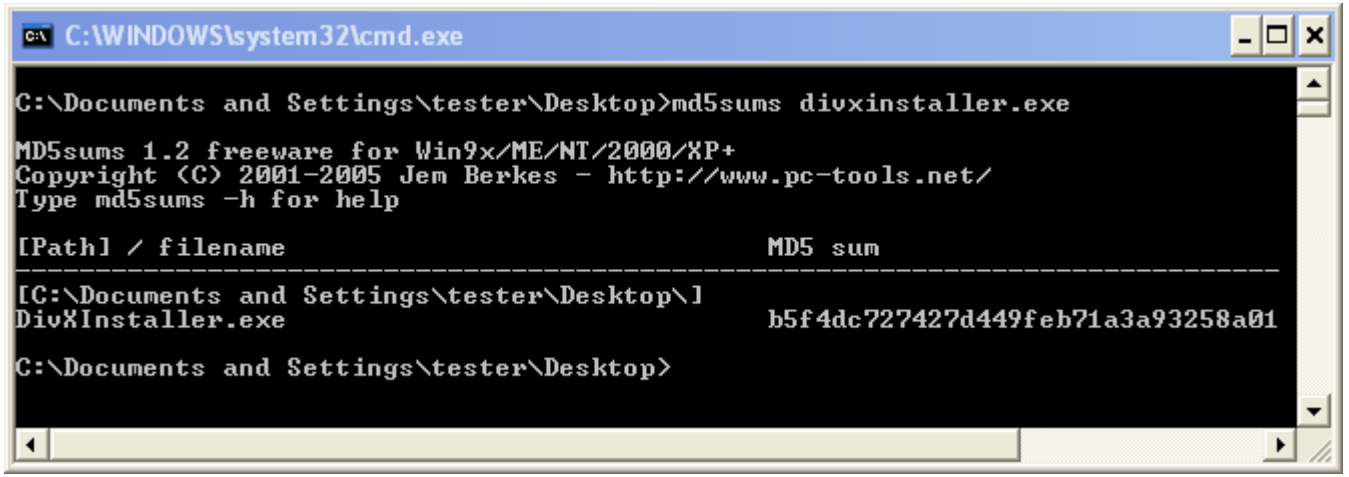
- Manager: “Strange things are happening with my laptop. It’s very slow, reboots for no reason and sometimes programs just start and stop by themselves.”
- Me: “Call me when you get into work and I’ll look at it.”
- Me: When I start to look at the laptop it is indeed having problems and I tell the manager I need to take the laptop back to my office. Knowing the manager would require a laptop to operate, I brought one for him. After getting him setup I was off to my office.

First Look

- During the initial look I found a file on the desktop, DivXInstaller.exe
- I called the manager and asked he has installed any software recently. He said “no”, after asking further questions he said he did install something to watch a movie.
- I copied the file to my thumb drive and moved it into my analysis setup.

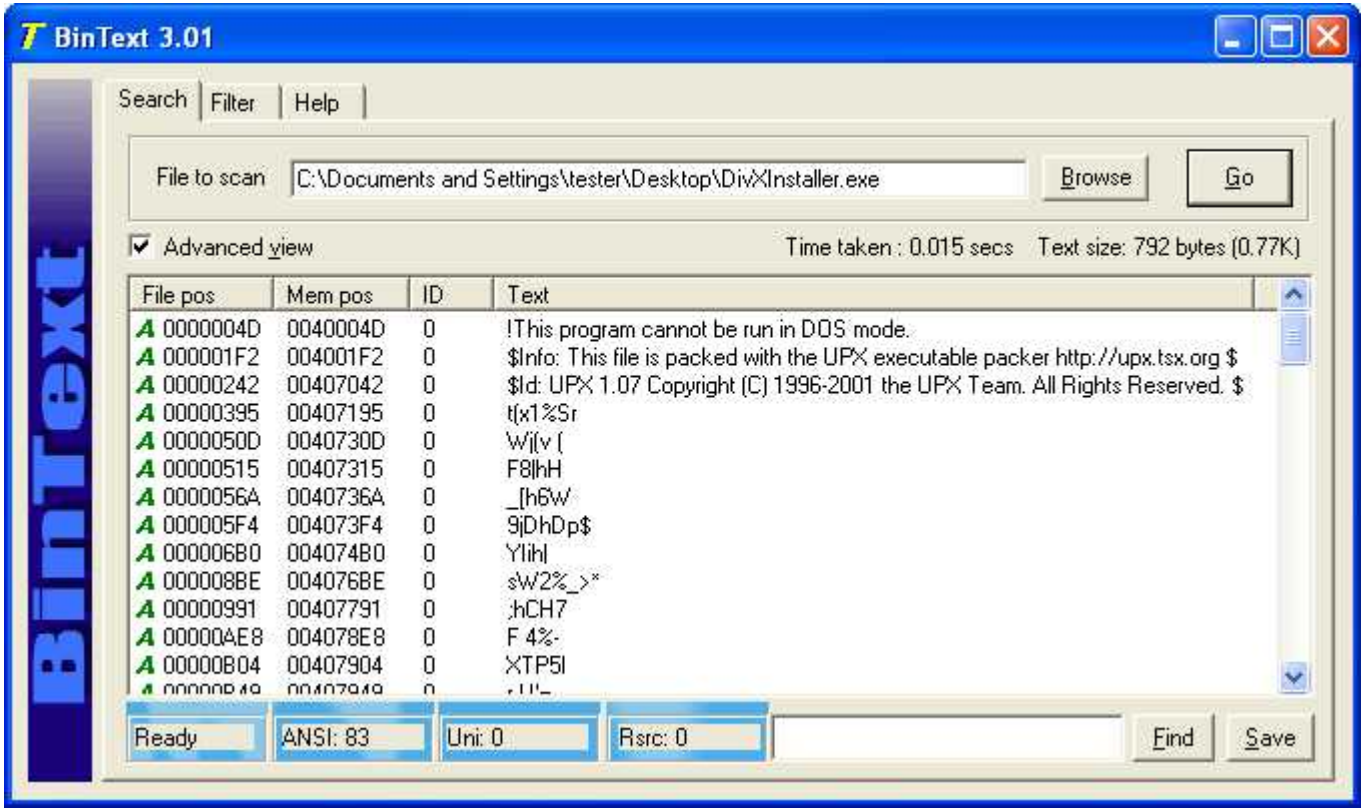
Lets See What It Does

- Copy the file to analysis desktop.
- Look at file properties and calculate MD5 hash.



Look For Strings

- **Open the file in BinText.**



Sandia National Laboratories

DivXInstall.exe Behavior Analysis

- Launch filemon, regmon and tcpview.
- Pause, capture and clear all the logs.
- On the XP-server launch wireshark and start the network capture.
- Launch regshot and take your first snapshot.

Sandia National Laboratories

DivXInstall.exe Behavior Analysis

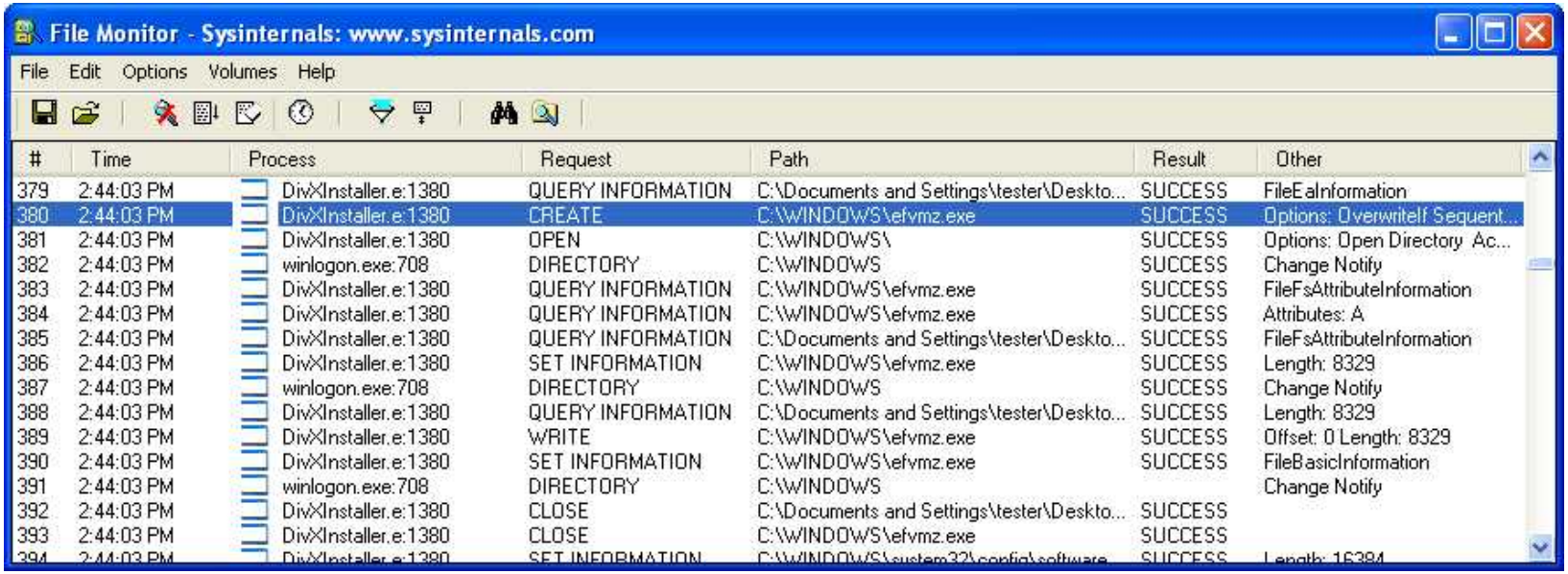
- Run DivXInstall.exe for 30 seconds then stop all data captures.
- Take your second regshot and click the *cOmpare* button.
- Create a folder on the desktop and save all the log files.
- Don’t forget the network capture on the XP-server.

What has changed?

- Regshot
  - File added C:\windows\efvmz.exe
  - Run key modified to launch efvmz.exe at boot, HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Update: "C:\WINDOWS\efvmz.exe"

What has changed?

- TCPView – Nothing interesting.
- Filemon – Shows file created in the windows directory.

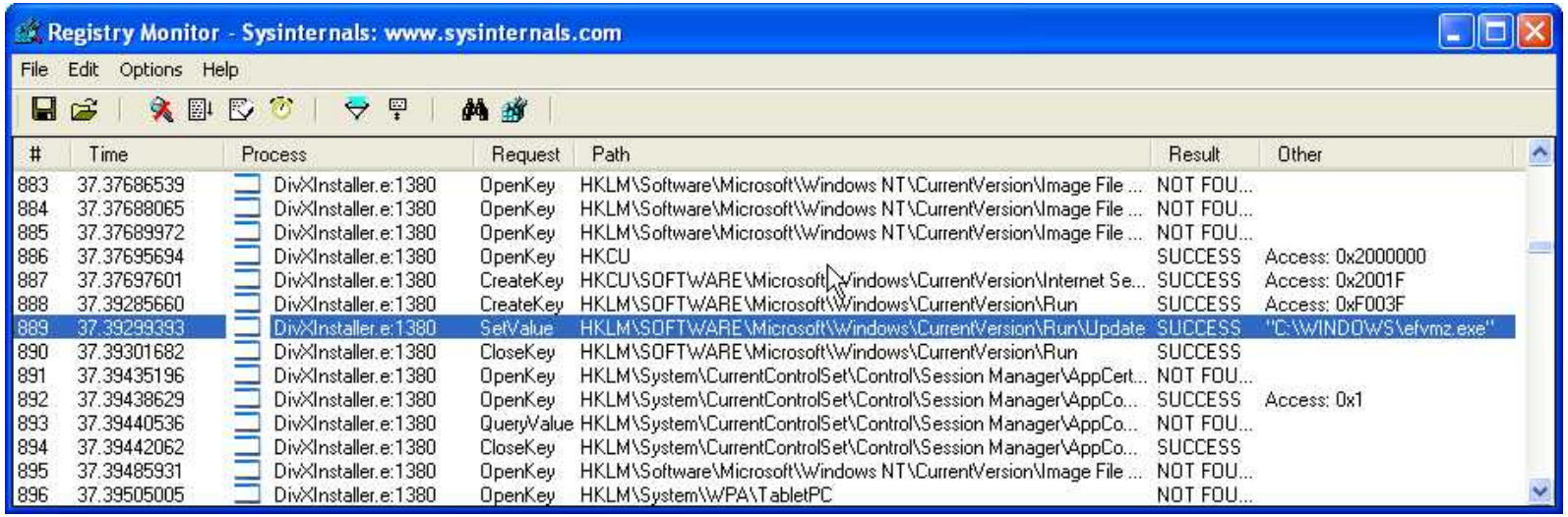


#	Time	Process	Request	Path	Result	Other
379	2:44:03 PM	DivXInstaller.e:1380	QUERY INFORMATION	C:\Documents and Settings\tester\Deskto...	SUCCESS	FileEaInformation
380	2:44:03 PM	DivXInstaller.e:1380	CREATE	C:\WINDOWS\efvmz.exe	SUCCESS	Options: OverwriteIf Sequent...
381	2:44:03 PM	DivXInstaller.e:1380	OPEN	C:\WINDOWS\	SUCCESS	Options: Open Directory Ac...
382	2:44:03 PM	winlogon.exe:708	DIRECTORY	C:\WINDOWS	SUCCESS	Change Notify
383	2:44:03 PM	DivXInstaller.e:1380	QUERY INFORMATION	C:\WINDOWS\efvmz.exe	SUCCESS	FileFsAttributeInformation
384	2:44:03 PM	DivXInstaller.e:1380	QUERY INFORMATION	C:\WINDOWS\efvmz.exe	SUCCESS	Attributes: A
385	2:44:03 PM	DivXInstaller.e:1380	QUERY INFORMATION	C:\Documents and Settings\tester\Deskto...	SUCCESS	FileFsAttributeInformation
386	2:44:03 PM	DivXInstaller.e:1380	SET INFORMATION	C:\WINDOWS\efvmz.exe	SUCCESS	Length: 8329
387	2:44:03 PM	winlogon.exe:708	DIRECTORY	C:\WINDOWS	SUCCESS	Change Notify
388	2:44:03 PM	DivXInstaller.e:1380	QUERY INFORMATION	C:\Documents and Settings\tester\Deskto...	SUCCESS	Length: 8329
389	2:44:03 PM	DivXInstaller.e:1380	WRITE	C:\WINDOWS\efvmz.exe	SUCCESS	Offset: 0 Length: 8329
390	2:44:03 PM	DivXInstaller.e:1380	SET INFORMATION	C:\WINDOWS\efvmz.exe	SUCCESS	FileBasicInformation
391	2:44:03 PM	winlogon.exe:708	DIRECTORY	C:\WINDOWS		Change Notify
392	2:44:03 PM	DivXInstaller.e:1380	CLOSE	C:\Documents and Settings\tester\Deskto...	SUCCESS	
393	2:44:03 PM	DivXInstaller.e:1380	CLOSE	C:\WINDOWS\efvmz.exe	SUCCESS	
394	2:44:03 PM	DivXInstaller.e:1380	SET INFORMATION	C:\WINDOWS\system32\config\software	SUCCESS	Length: 16384

Sandia National Laboratories

What has changed?

- **Regmon**
  - **Shows a SetValue request to the run key.**
  - **Will launch efvmz.exe at boot.**

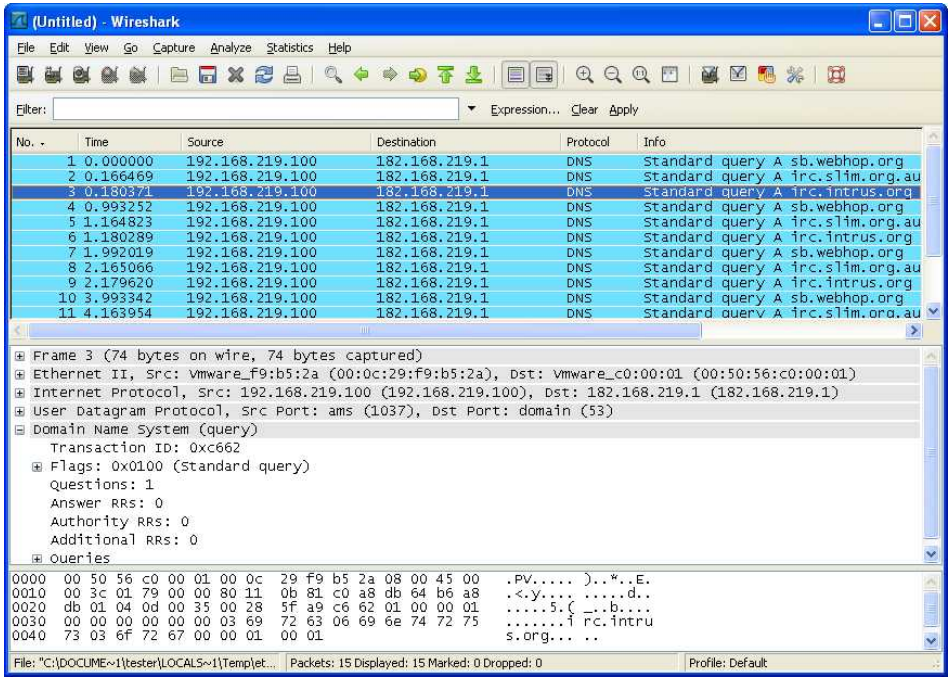


#	Time	Process	Request	Path	Result	Other
883	37.37686539	DivXInstaller.e:1380	OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File ...	NOT FOU...	
884	37.37688065	DivXInstaller.e:1380	OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File ...	NOT FOU...	
885	37.37689972	DivXInstaller.e:1380	OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File ...	NOT FOU...	
886	37.37695694	DivXInstaller.e:1380	OpenKey	HKCU	SUCCESS	Access: 0x2000000
887	37.37697601	DivXInstaller.e:1380	CreateKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Se...	SUCCESS	Access: 0x2001F
888	37.39285660	DivXInstaller.e:1380	CreateKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Access: 0xF003F
889	37.39299393	DivXInstaller.e:1380	SetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Update	SUCCESS	"C:\WINDOWS\efvmz.exe"
890	37.39301682	DivXInstaller.e:1380	CloseKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	SUCCESS	
891	37.39435196	DivXInstaller.e:1380	OpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCert...	NOT FOU...	
892	37.39438629	DivXInstaller.e:1380	OpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCo...	SUCCESS	Access: 0x1
893	37.39440536	DivXInstaller.e:1380	QueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\AppCo...	NOT FOU...	
894	37.39442062	DivXInstaller.e:1380	CloseKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCo...	SUCCESS	
895	37.39485931	DivXInstaller.e:1380	OpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File ...	NOT FOU...	
896	37.39505005	DivXInstaller.e:1380	OpenKey	HKLM\System\WPA\TabletPC	NOT FOU...	

Sandia National Laboratories

Network Traffic

- **Wireshark**
  - **DNS request for irc.intrus.org, sb.webhop.org and irc.slim.org.au.**



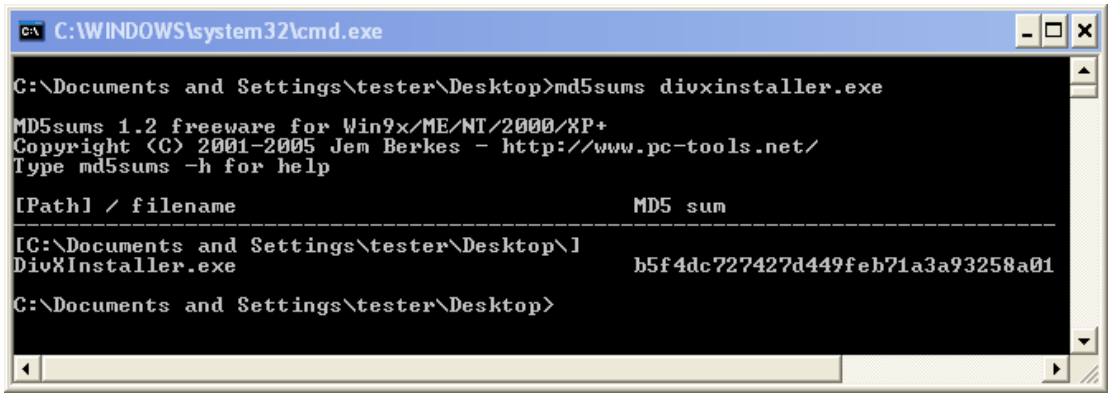
Sandia National Laboratories

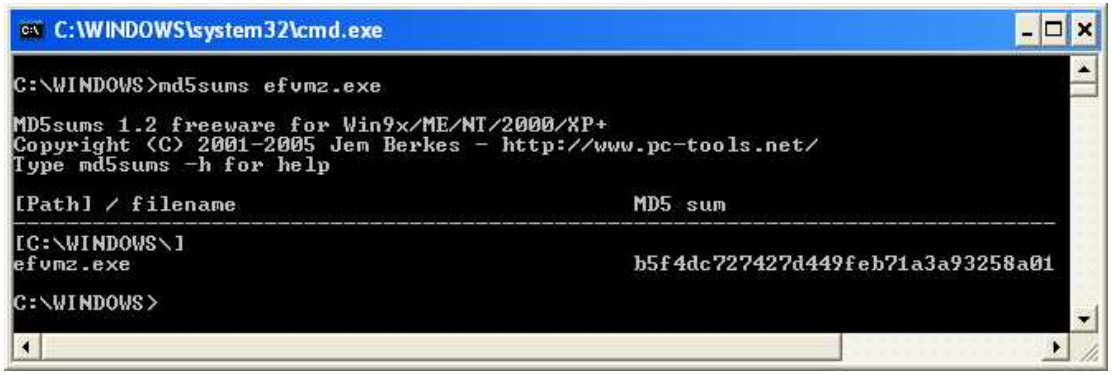
What we know so far?

- Copies a file to C:\WINDOWS\efvmz.exe.
- Creates run key to keep it alive after a reboot.
- Runs a process by the name of “efvmz”.
- Attempts to make a DNS request to three places.
- It’s probably a packed executable.

Check copied program

- Is C:\WINDOWS\efvmz.exe the same as DivXInstall.exe?

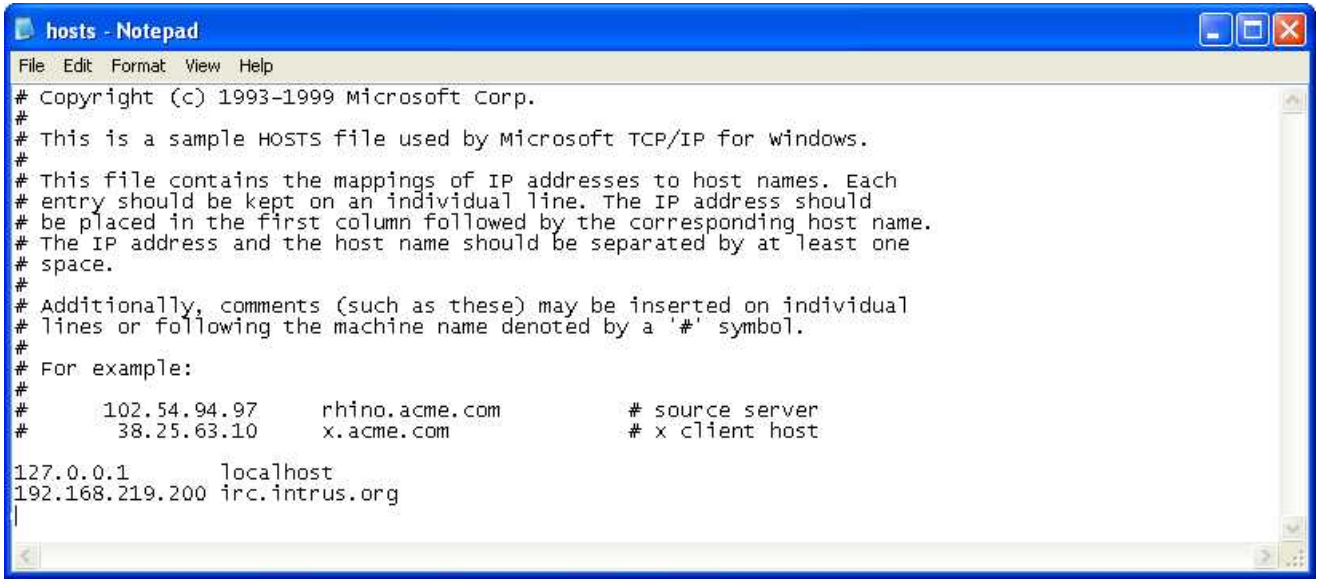




Sandia National Laboratories

Resolve the DNS issue

- We always want to control our environment, so only change one thing at a time.
- First we point irc.intrus.org to our XP-server and see what happens.



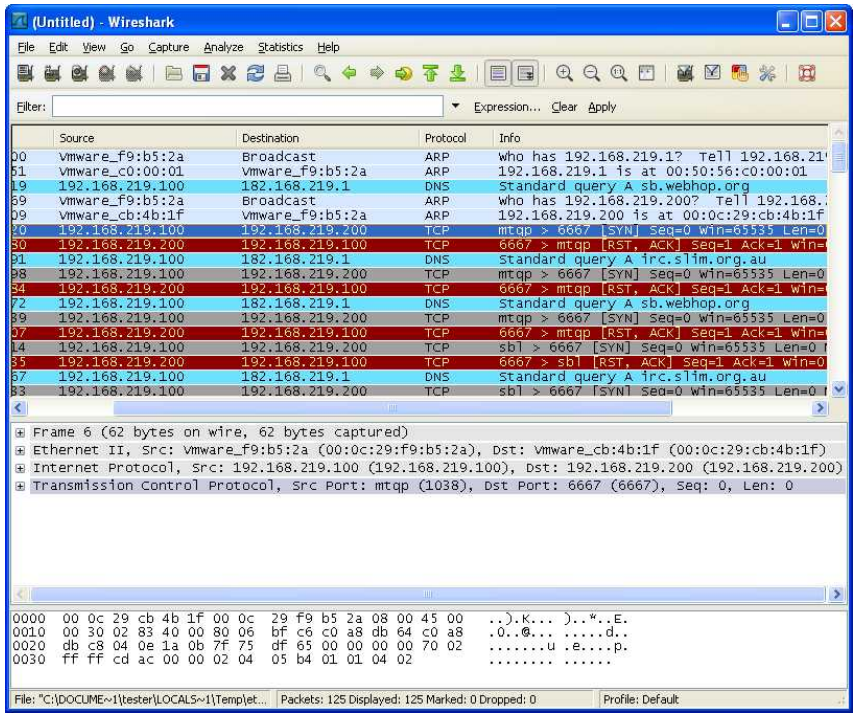
Sandia National Laboratories

Network Activity

- Clear the capture in Wireshark.
- Run malware for 30 seconds and terminate it.
- Stop Wireshark capture.
- Look at the packets captured going to our XP-server.

Network Activity

- It's attempting to connect to TCP port 6667.
- TCP port 6667 is officially listing is Internet Relay Chat TCP 6665-6669.



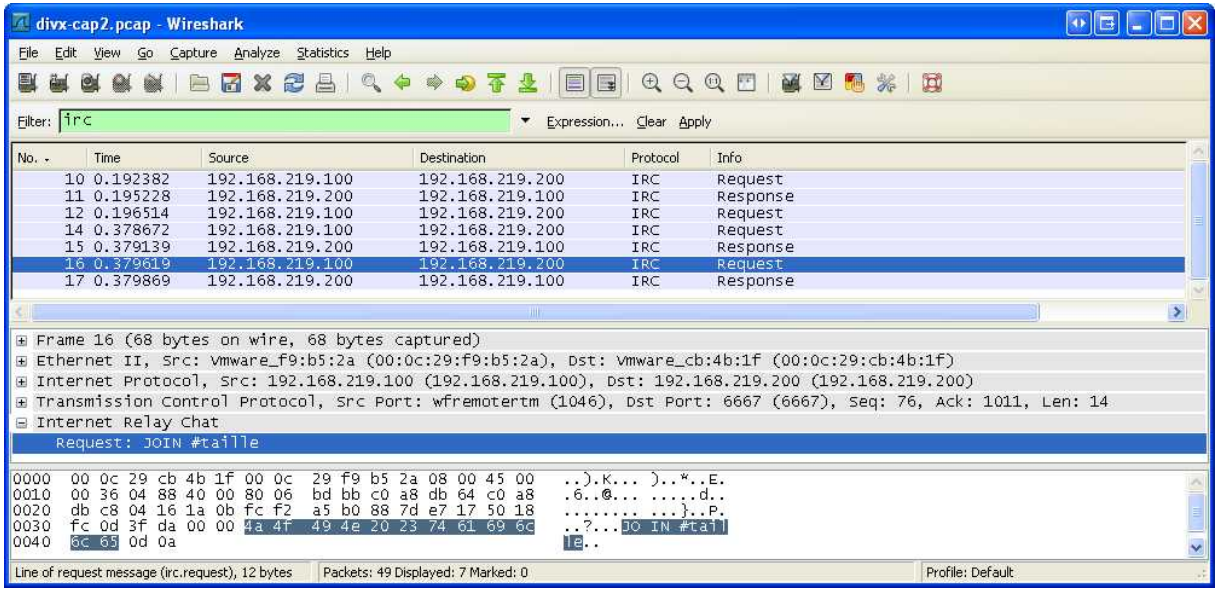
Sandia National Laboratories

More Resources

- Stop the malware.
- Go to the XP-server and start the IRC server. To launch the IRC service go to C:\IRC\ and launch bircd.exe.
- Check task manager to make sure the server is running.
- Start a new network capture in Wireshark.
- Launch the malware and see what it does next.

Network Activity

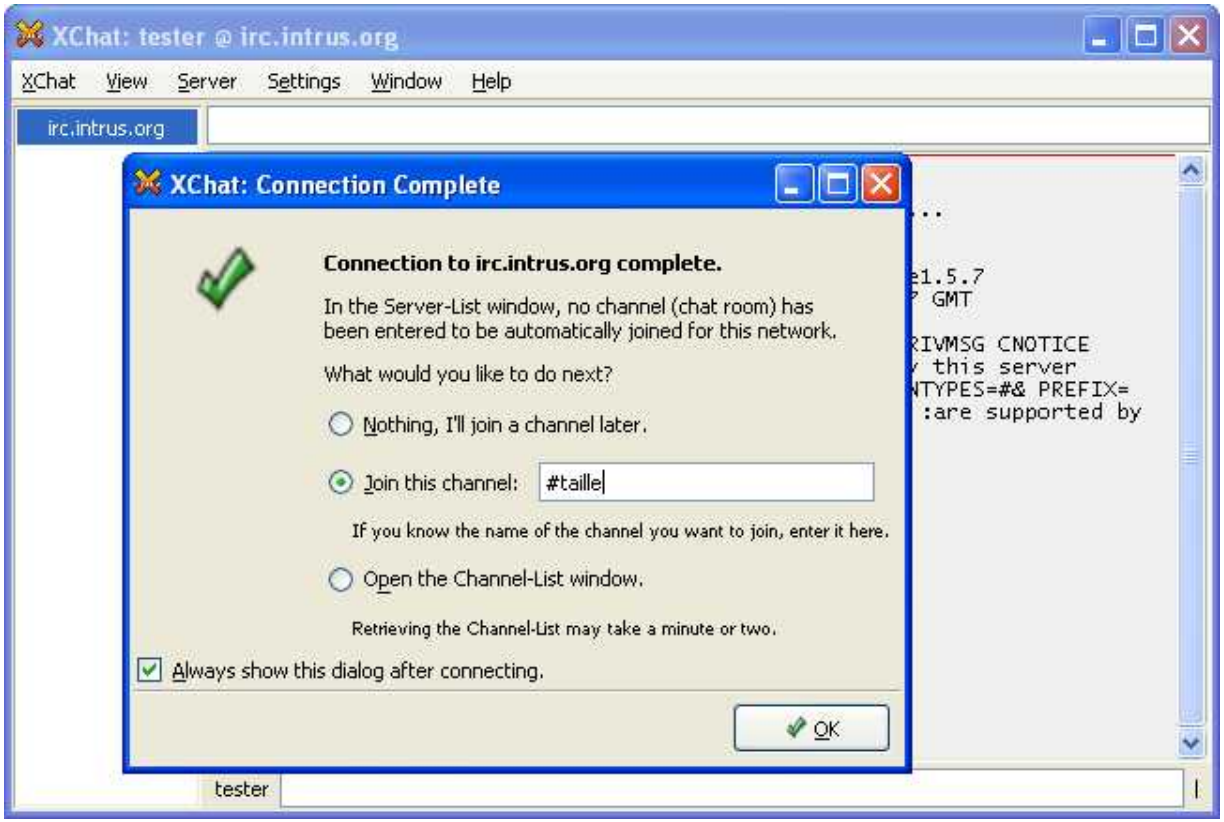
- It joins a channel called “taille”.



Sandia National Laboratories

IRC Activity

- **Go to the server and join the channel “taille” and see if you can talk to the malware.**



Sandia National Laboratories

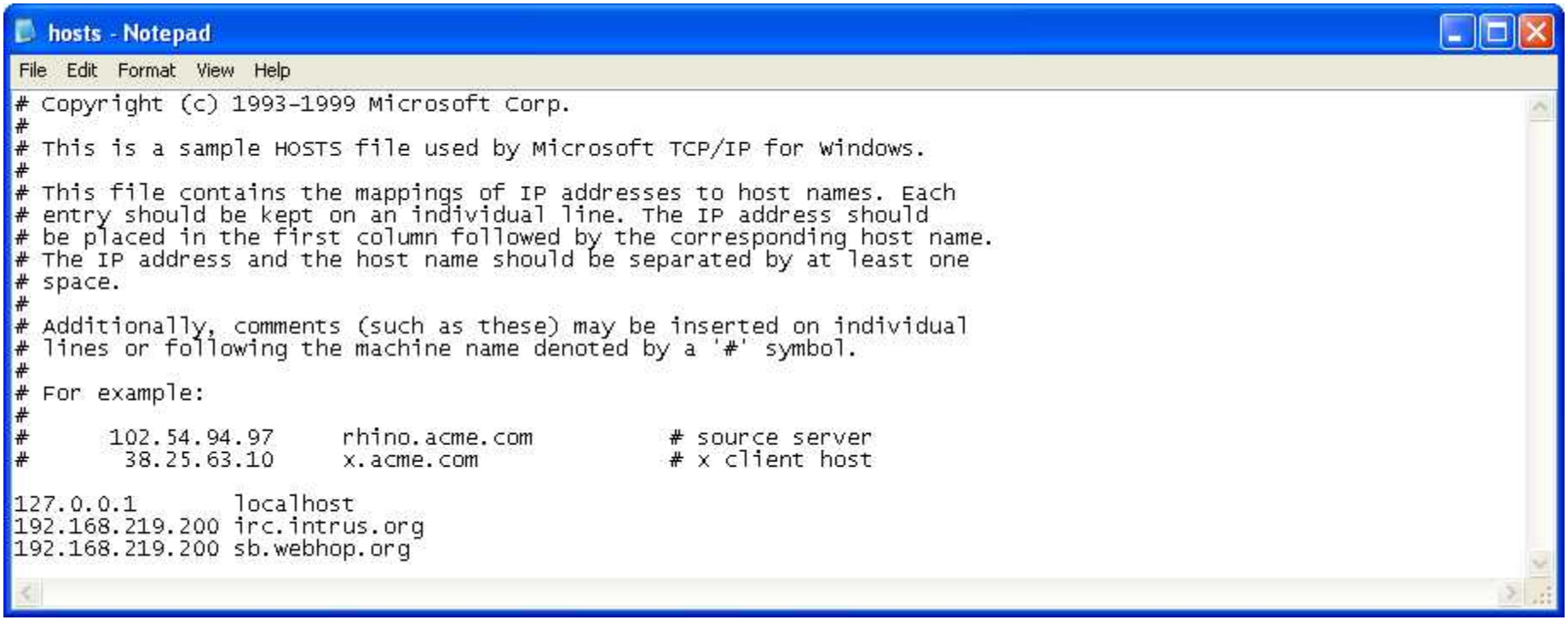
IRC Activity

- Try to communicate with it.
- The name the malware joins with is always random.

Sandia National Laboratories

Webhop Analysis

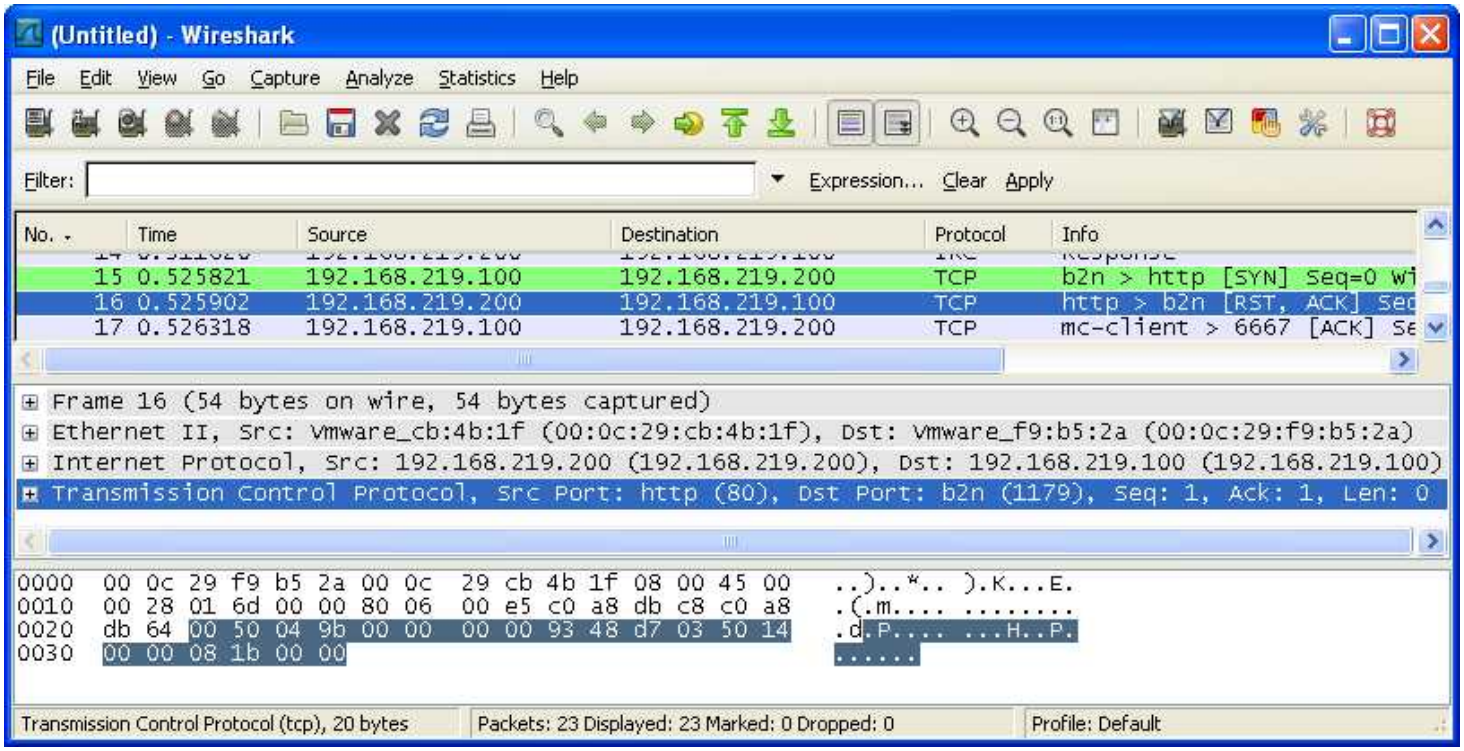
- **Edit the host file to add sb.webhop.org**



Sandia National Laboratories

Webhop Analysis

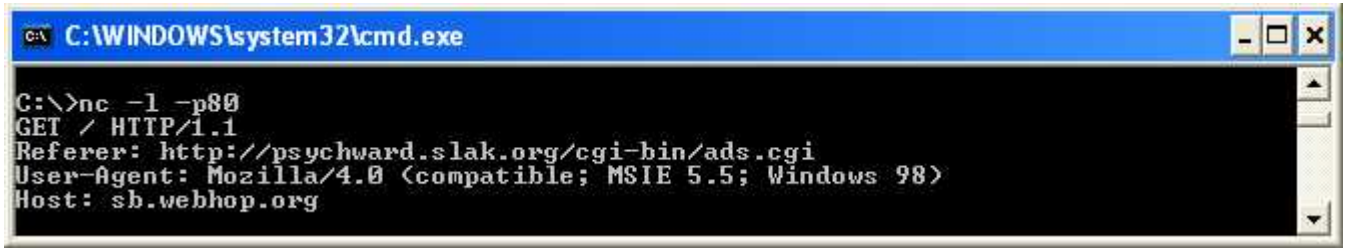
- **Start Wireshark on the server and start the capture.**



Sandia National Laboratories

Webhop Analysis

- Now it's time to give it something to connect to. If you don't want to install a webserver use Netcat.
- On the server, open a dos window and type "nc –l –p80".
- Why do you think it visits this site?



Sandia National Laboratories

What we know so far?

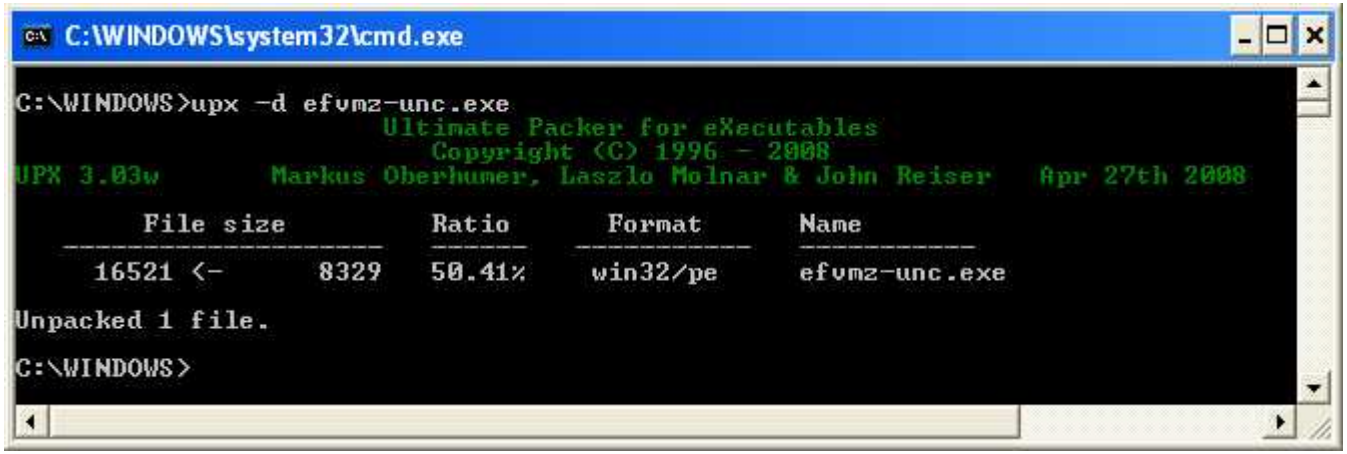
- Copies a file to C:\WINDOWS\efvmz.exe.
- Creates run key to keep it alive after a reboot.
- Runs a process by the name of “efvmz”.
- Attempts to make a DNS request to three places.
- It’s probably a packed executable.
- Uses IRC to communicate to irc.intrus.org.
- Uses a command structure we don’t know about yet.
- Connects to sb.webhop.org on port 80.

Code Analysis

- What do we want to find out?
  - Find out how to get a response out of the malware.
    - Find the IRC communication structure.
    - Find the authentication mechanism if one is used.
  - Find out what we can do with the backdoor.

Code Analysis

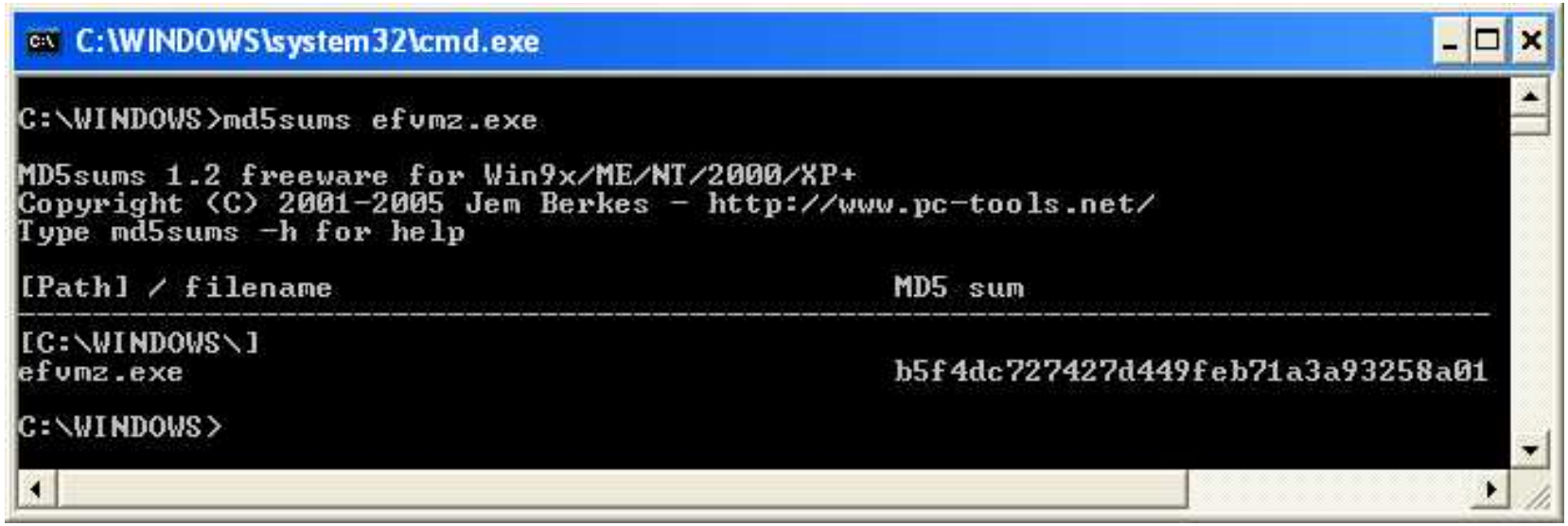
- As we saw before the malware is packed. Looking at the strings, it's probably packed using UPX.
- Let's try and unpack it.
- Make a copy of the original executable and change the file name efvmz–unp.exe to it.
- upx –d efvmz-unp.exe



Sandia National Laboratories

Code Analysis

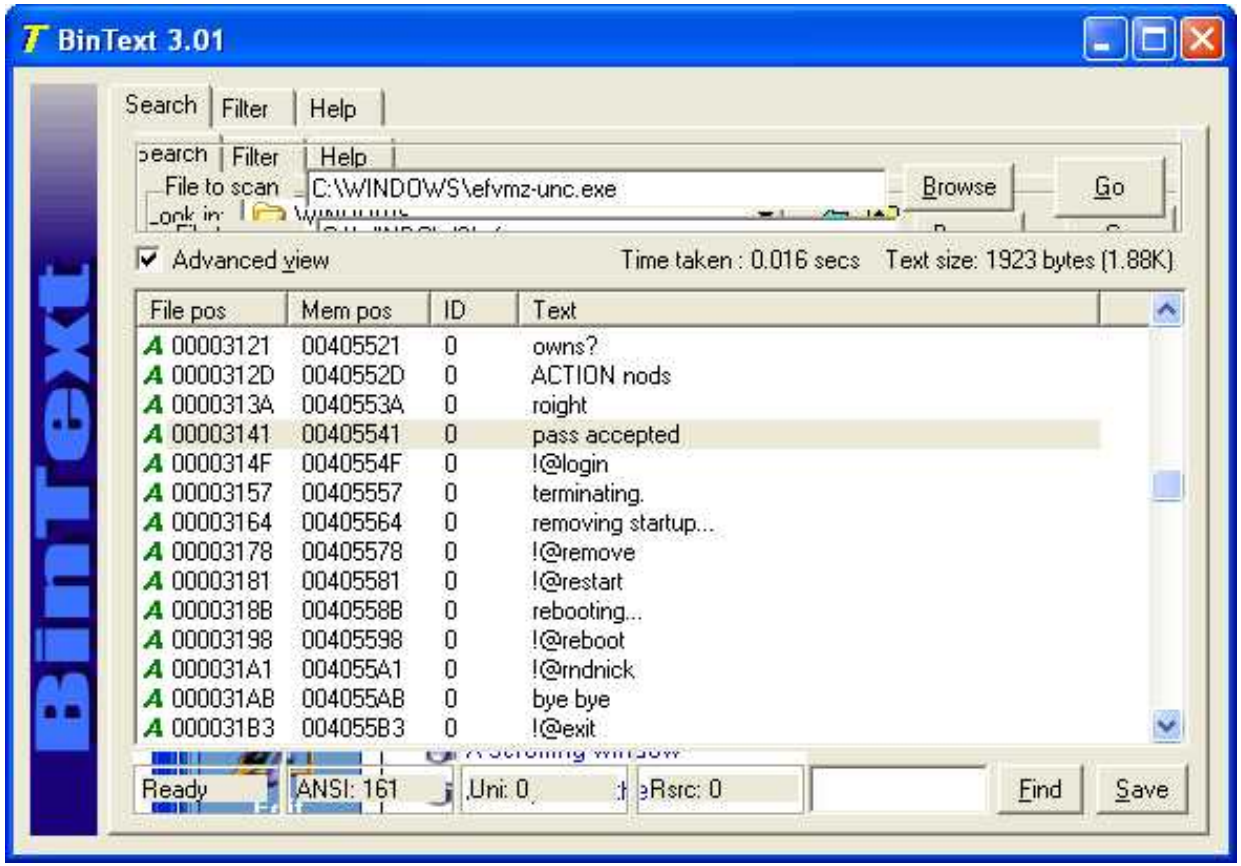
- Like always we do an MD5 hash.



Sandia National Laboratories

Code Analysis

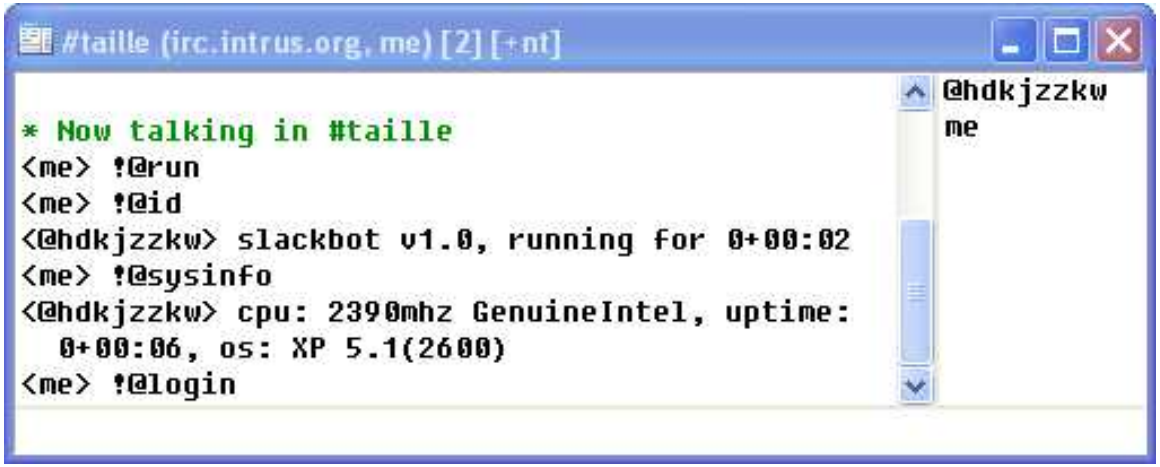
- **Next we look at the ASCII strings in the new file.**



Sandia National Laboratories

Code Analysis

- Now we are getting somewhere, we can see several items that look like commands that all start with “!@”.
- A few that look interesting to me are, !@sysinfo, !@login, !@run, !@id.
- Lets try them.



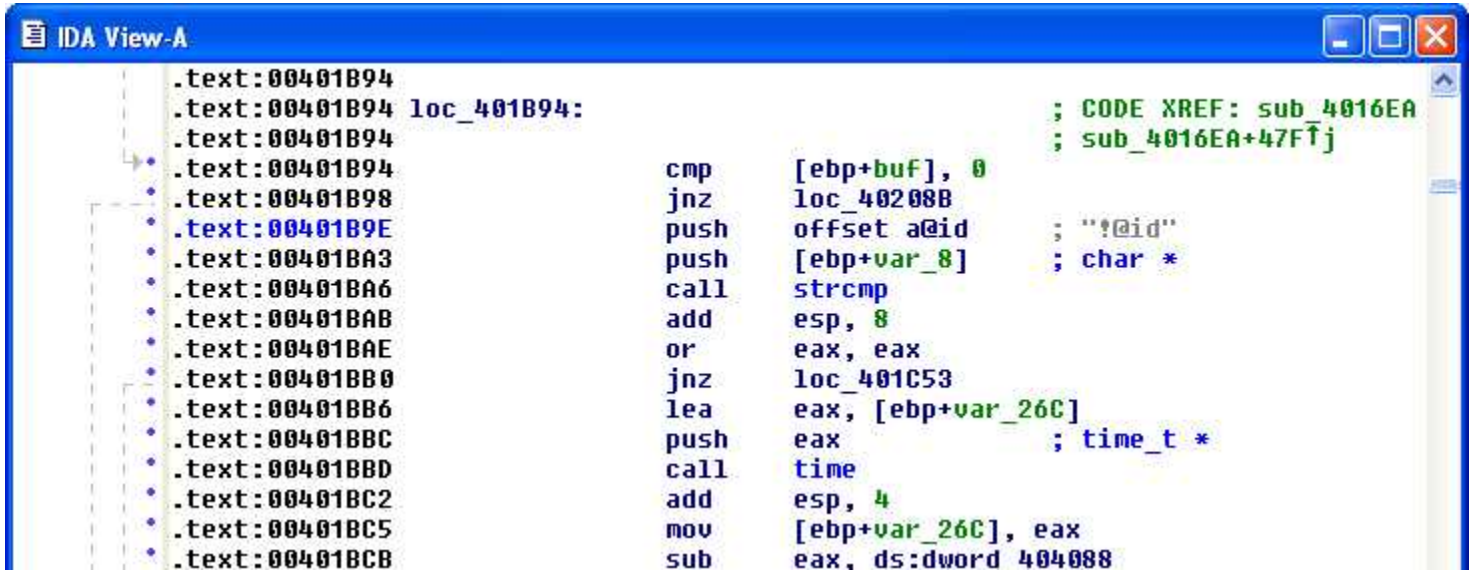
Sandia National Laboratories

Code Analysis

- It looks like some of the commands work and some don’t. It looks like the fun ones require some kind of authentication.
- Time to use Ida Pro.

Code Analysis

- Load the malware into IDA Pro.
- Find “!@id” use Alt+T for text search.
- “!@id” doesn’t require additional parameters.



Sandia National Laboratories

Code Analysis

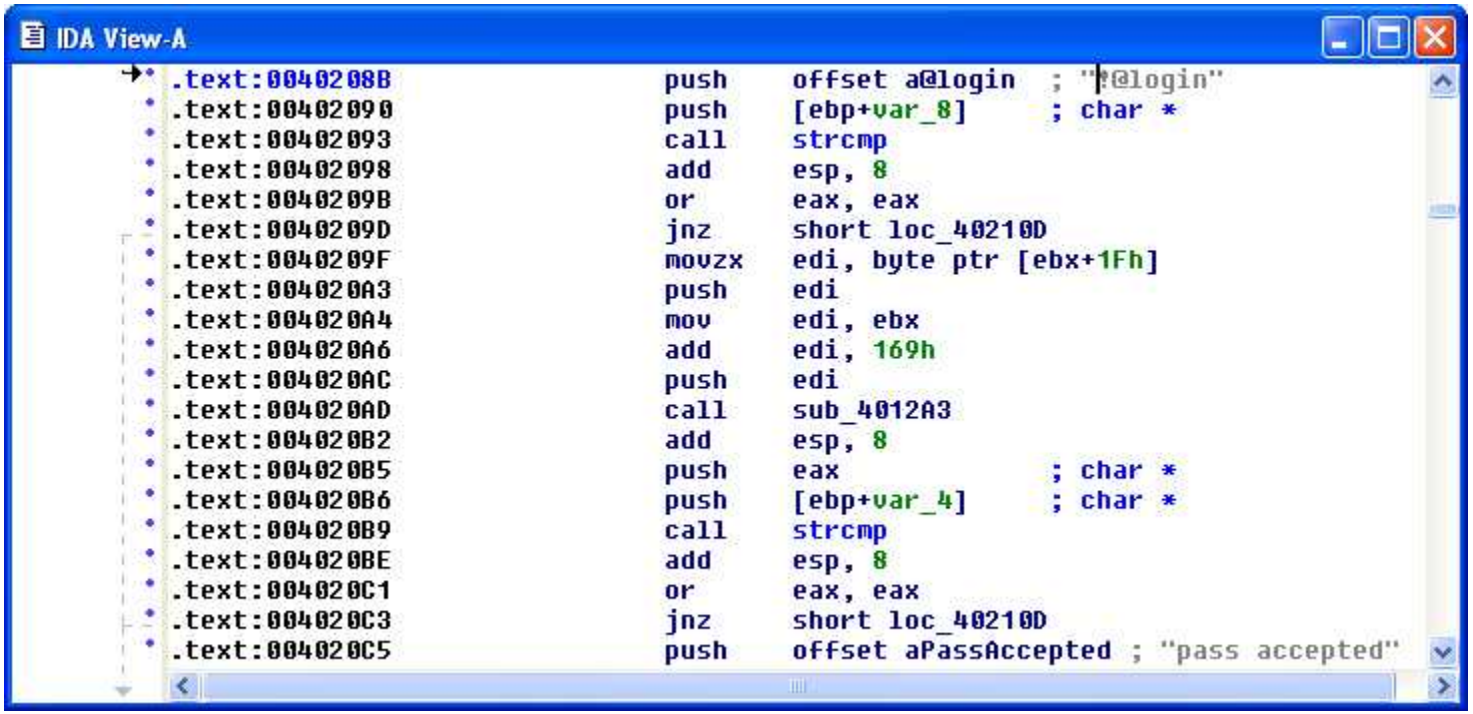
- Look for calls.
- It's calling strcmp.
- If will compare the data from the last two push statements, returns 0 if the compare is true.
- Look at the next call.
- It's calling time.
- Remember the command returned the uptime of the bot.

Code Analysis

- If it doesn't compare the "jnz" command takes it to another subroutine.
- Probably to some sort of case structure for command processing.

Code Analysis

- Next lets look for “!@login”.
- Locate “!@login” in the code.



Sandia National Laboratories

Code Analysis

- As you can see the structure looks similar to the “!@id” code.
- The first just compares the “!@login” with the string it gets from the IRC.
- If it does it proceeds.
- Let’s look at the second call to strcmp at offset 4020B9.
- This should be the password verification section.
- You should see the “pass accepted”.

Code Analysis

- How do we get to “password accepted”?
- Will we get there if the jnz isn’t taken?
- jnz is a conditional jump in this case the jump is not taken if the value is 0.
- When do we have the condition where the value is 0?
- When the two strings that are being compared by strcmp are the same.

Now it's time for a debugger, OllyDbg

- Common commands you need to know.
- F7 to step through the code execution one step at a time.
- F8 is the same as F7 except it doesn't step into the function calls.
- F9 executes code until it hits a breakpoint.
- Ctrl+F9 executes to end of procedure
- Right click instruction to set break point.

Code Analysis

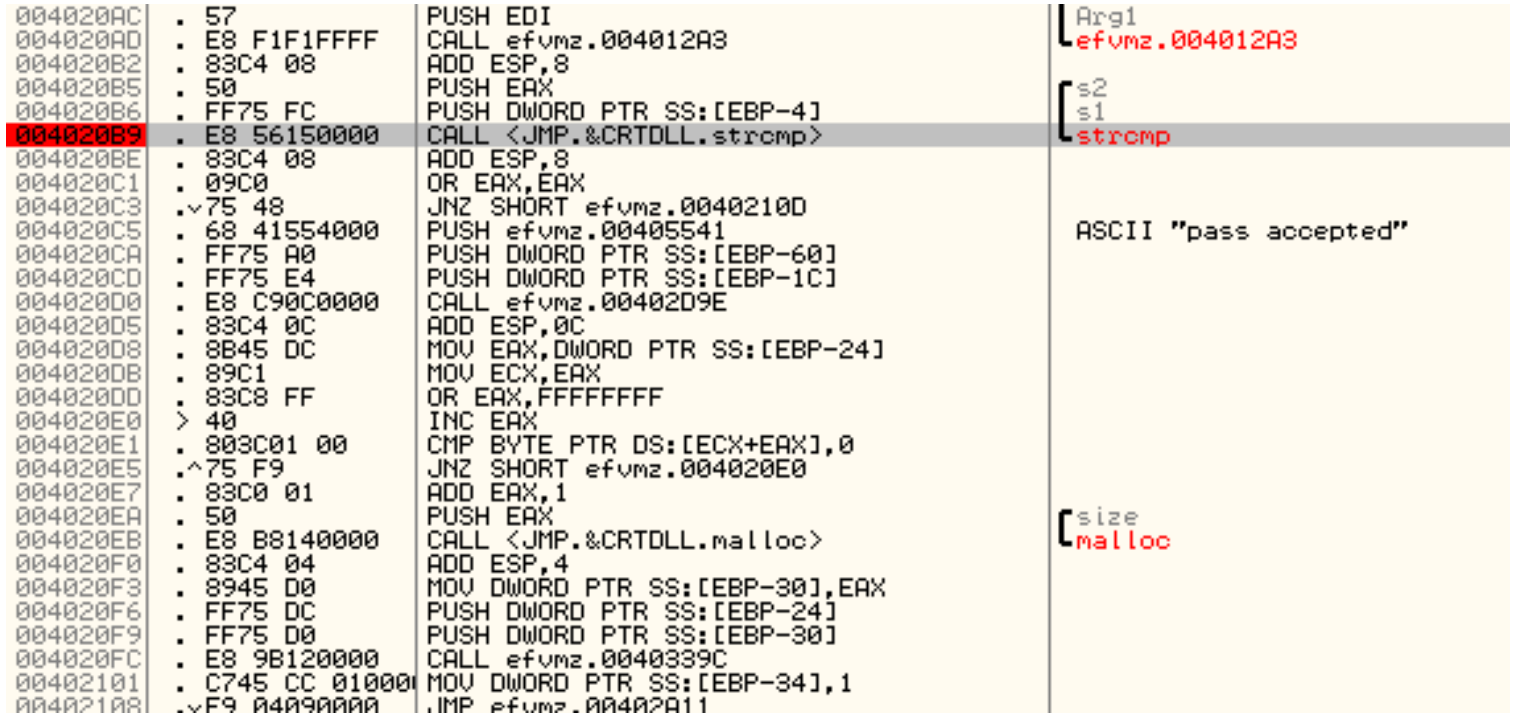
- Let's get the password.
- Kill the existing process.
- Launch OllyDbg.
- Use file open to connect to the malware in the windows directory.
- Set a breakpoint at the strcmp we are interested in (offset 4020B9).
- Use F2 to set the breakpoint.
- It should now be highlighted in red.

Code Analysis

- OllyDgb should pause when it hits the breakpoint.
- The disassemble pane shows where the execution paused.
- The stack pane shows the parameters passed to srtcmp.
- One of them is the real password and the other is the password we provided.

Code Analysis

- Select run from the debug menu, you should see “Running” in the bottom right corner of OllyDbg.



Sandia National Laboratories

Code Analysis

- Go to your IRC server and try the !@id command and make sure it works.
- Try to login via the IRC channel using a known bad password (badpass).

Sandia National Laboratories

Code Analysis

- The “s1” parameter is the password we provided “badpass”.
- The “s2” parameter is the real password “datasnoket”.

```
0012F7E8  00162C92  s1 = "badpass"
0012F7EC  0016AEB0  s2 = "datasnoket"
0012F7F0  0000004C
0012F7F4  00003E20
0012F7F8  7FFD8000
0012F7FC  00000000
0012F800  7C91030C  ASCII "Actx "
0012F804  00000000
0012F808  0012F8F8
0012F80C  00000008
0012F810  7C9102ED  RETURN to ntdll.7C9102ED from ntdll.7C90
0012F814  00000001
0012F818  FFFFFFFF
0012F81C  00000000
0012F820  00000000
0012F824  7FFDF000
0012F828  0012F900
0012F82C  00001000
```

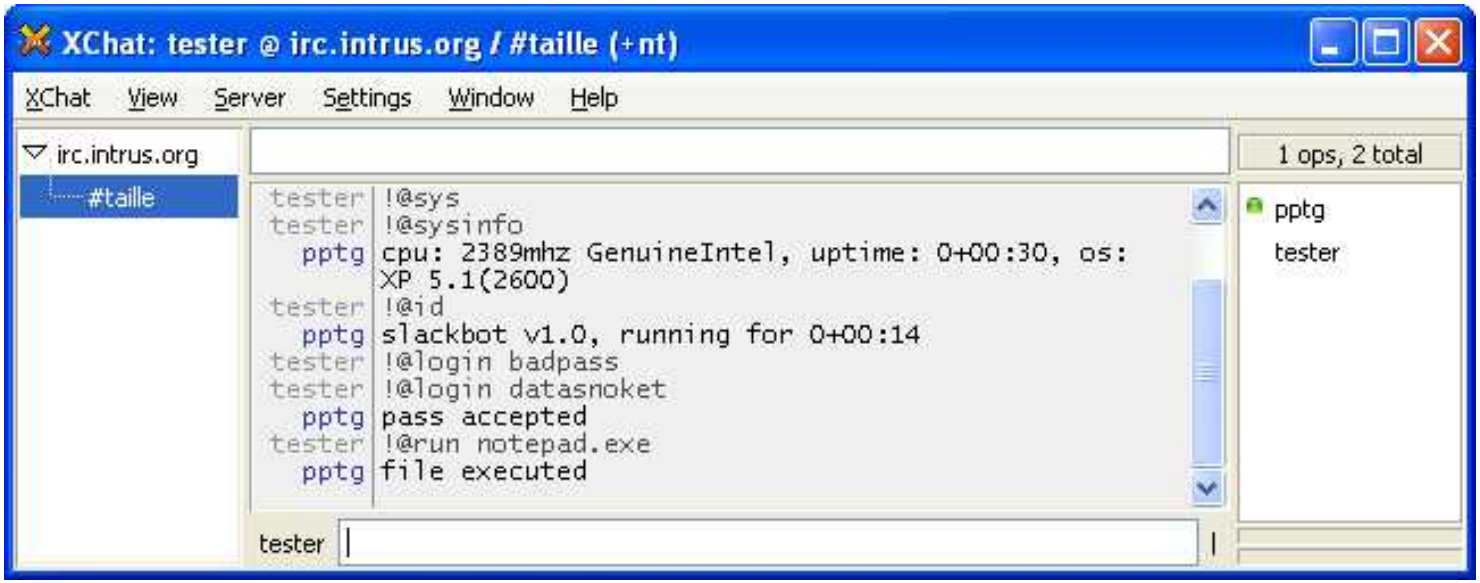
Sandia National Laboratories

Code Analysis

- Let's give it a try.
- The real password is "datasnoket"
- Press F9 to continue execution in OllyDbg
- Login giving the correct password "!@login datasnoket"
- Press F9 in OllyDbg to continue.
- Sometimes you need to do this quickly before some other process times out.

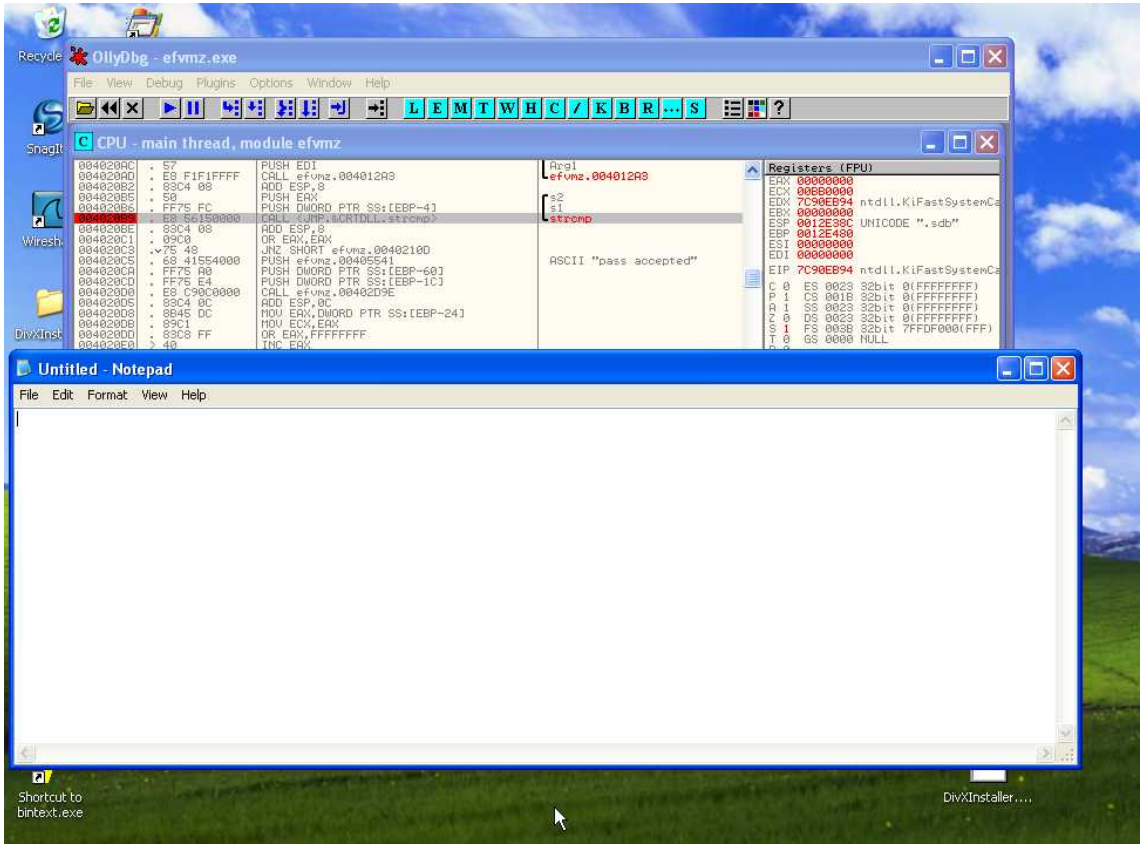
Code Analysis

- We can now try some of the other commands.
- Lets try one of the other commands “!@ run notepad.exe”.



Code Analysis

- **Looks like it works.**



Sandia National Laboratories

What Did We Learn About the Malware?

- Pretends to be a DivX codec.
- Copies a file to C:\WINDOWS\efvmz.exe.
- Creates run key to keep it alive after a reboot.
- Runs a process by the name of “efvmz”.
- Makes connections to three places.
- Uses IRC to communicate to irc.intrus.org.
- Uses a command structure we didn’t know.
- Connects to sb.webhop.org on port 80.
- Compressed with generic UPX.
- Some commands don’t require authentication.
- Password for authentication is “datasnoket”.
- With the malware installed, we own the system.

Agenda

- General Requirements
- Overview of Malware Analysis
- Tools of the Trade
- Analysis Fundamentals
- Setting up the Environment
- Time to give it a try
- **Sources**

Sandia National Laboratories

Useful Sources

- Sysinternals - http://technet.microsoft.com/en-us/sysinternals/default.aspx
- UPX - http://upx.sourceforge.net/
- AspackDIE -http://www.exetools.com/unpackers.htm
- Assembly code tutorial - http://hem.passagen.se/danma/asmprog.htm
- Offensive Computing it check hash of known malware. http://www.offensivecomputing.net/
- OpneRCE http://www.openrce.org/articles/
- Stud_PE http://cgsoftlabs.ro/studpe.html
- LordPE - http://www.exetools.com/