
REM 101

An Introduction to Reverse Engineering Malware

J. Larry Dishman
Senior Member of Technical Staff



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.”



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**

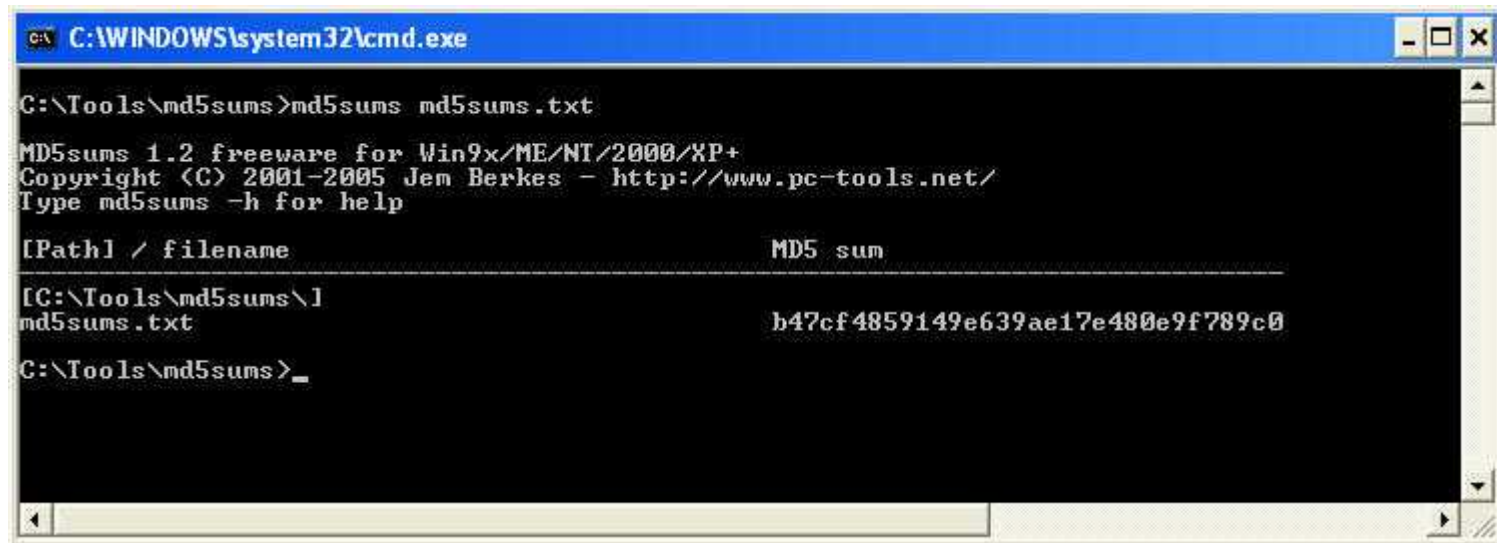
VMWare Player

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



Md5sums

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



```
C:\WINDOWS\system32\cmd.exe

C:\Tools\md5sums>md5sums md5sums.txt

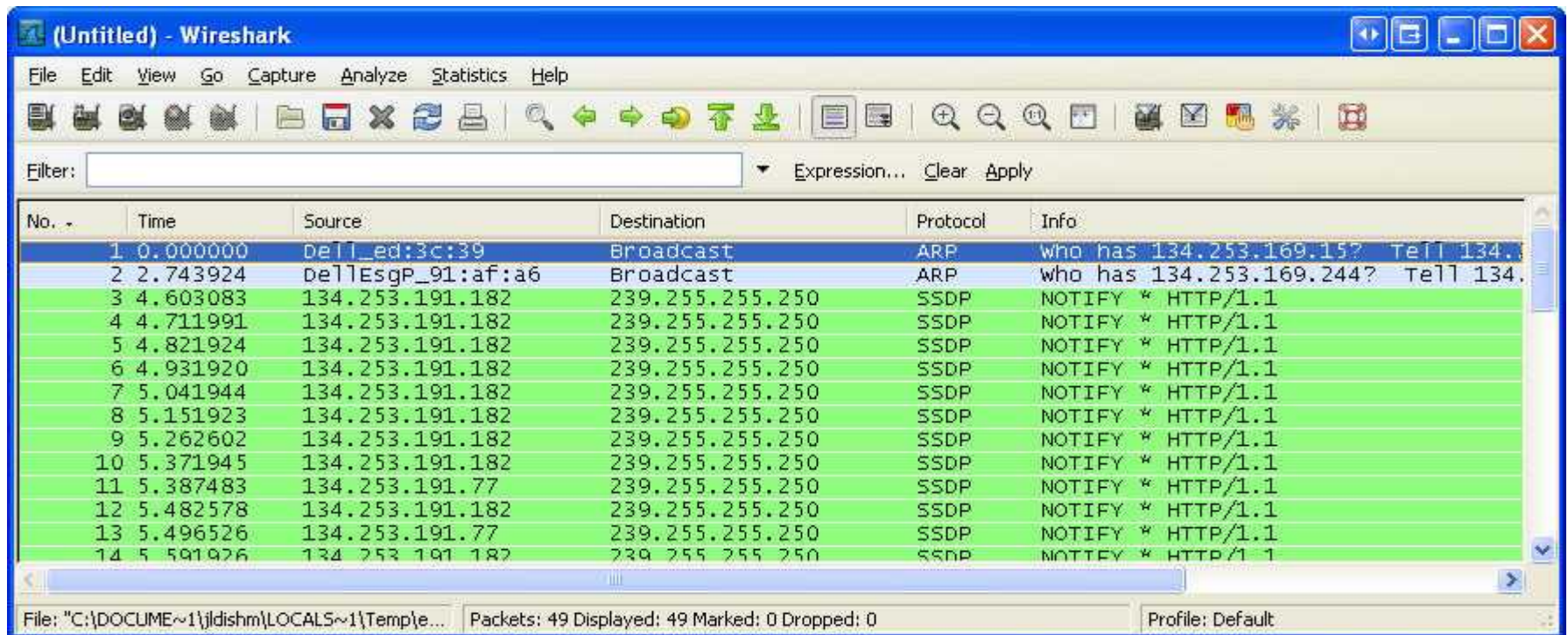
MD5sums 1.2 freeware for Win9x/ME/NT/2000/XP+
Copyright (C) 2001-2005 Jem Berkes - http://www.pc-tools.net/
Type md5sums -h for help

[Path] / filename                MD5 sum
-----
[C:\Tools\md5sums\]
md5sums.txt                      b47cf4859149e639ae17e480e9f789c0
C:\Tools\md5sums>_
```



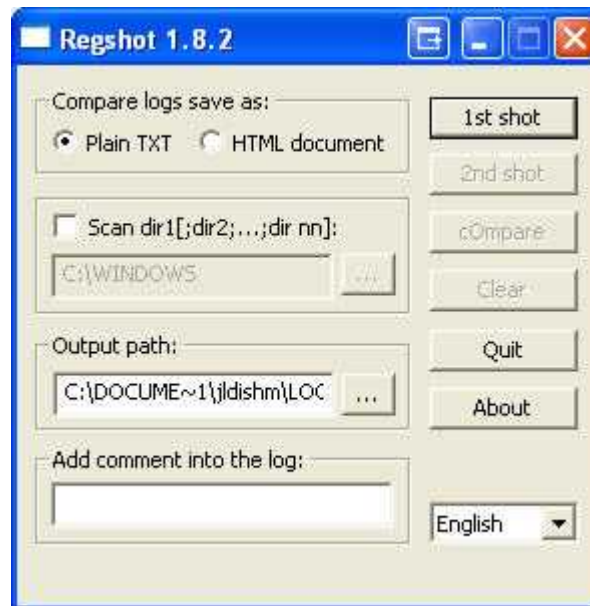

Wireshark

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



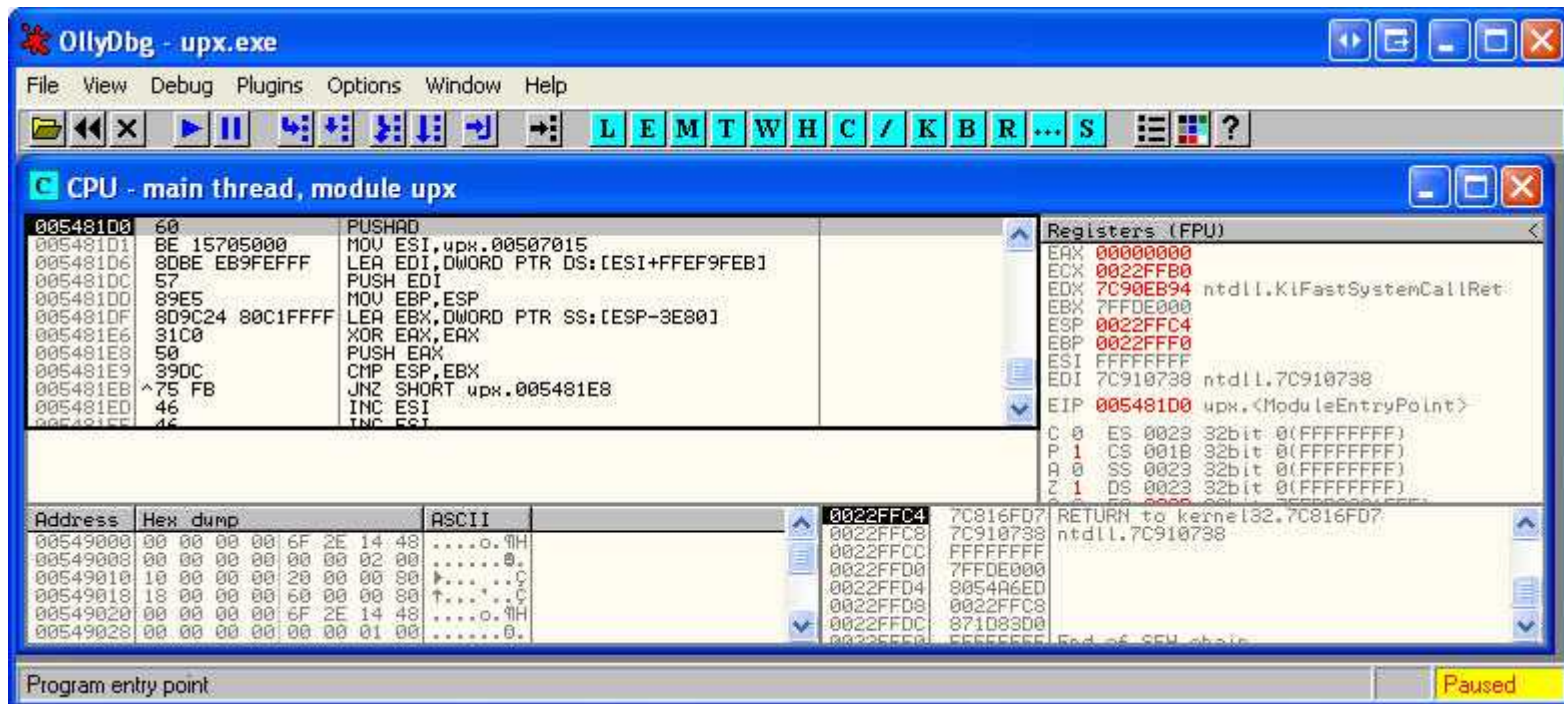
RegShot

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



OllyDbg

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



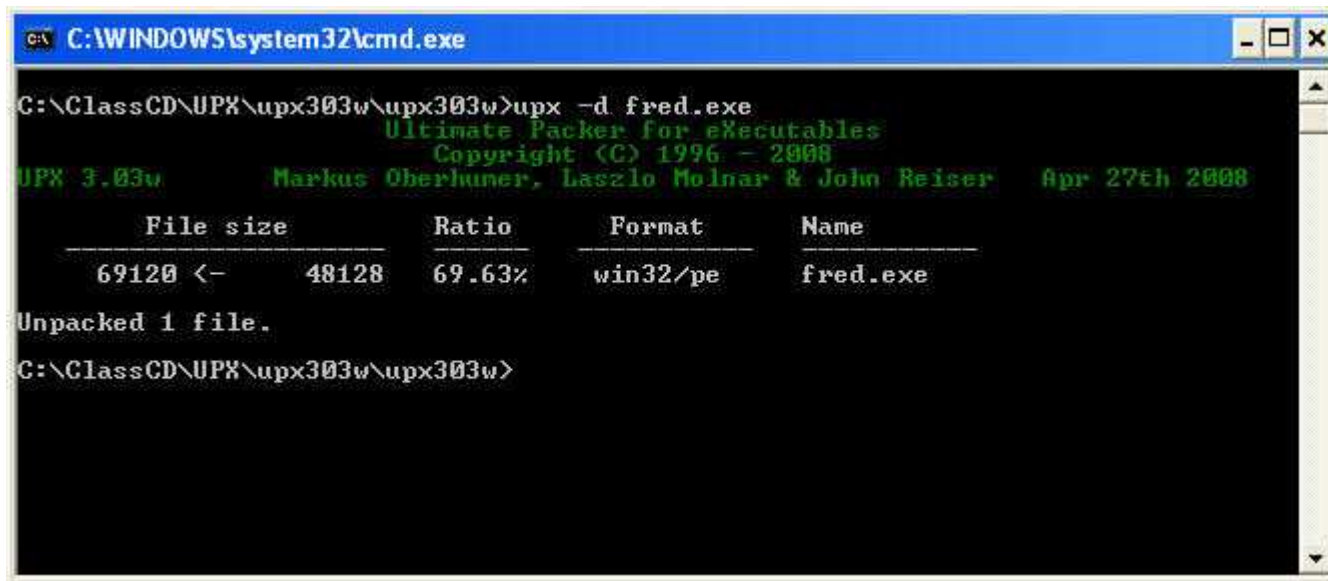


Netcat

- 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.



```
C:\WINDOWS\system32\cmd.exe

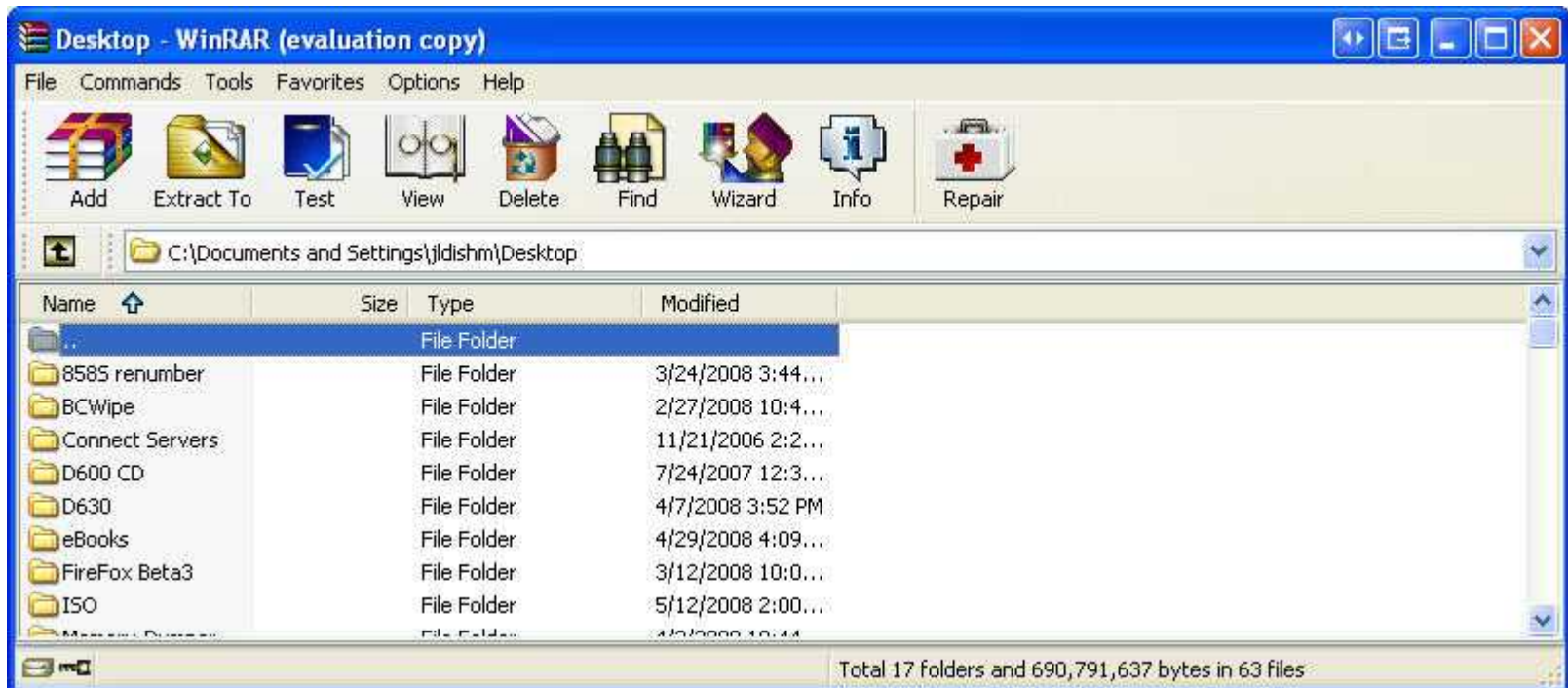
C:\ClassCD\UPX\upx303w\upx303w>upx -d fred.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2008
UPX 3.03w Markus Oberhumer, Laszlo Molnar & John Reiser Apr 27th 2008

  File size      Ratio      Format      Name
  -----
  69120 <-    48128    69.63%    win32/pe    fred.exe

Unpacked 1 file.
C:\ClassCD\UPX\upx303w\upx303w>
```

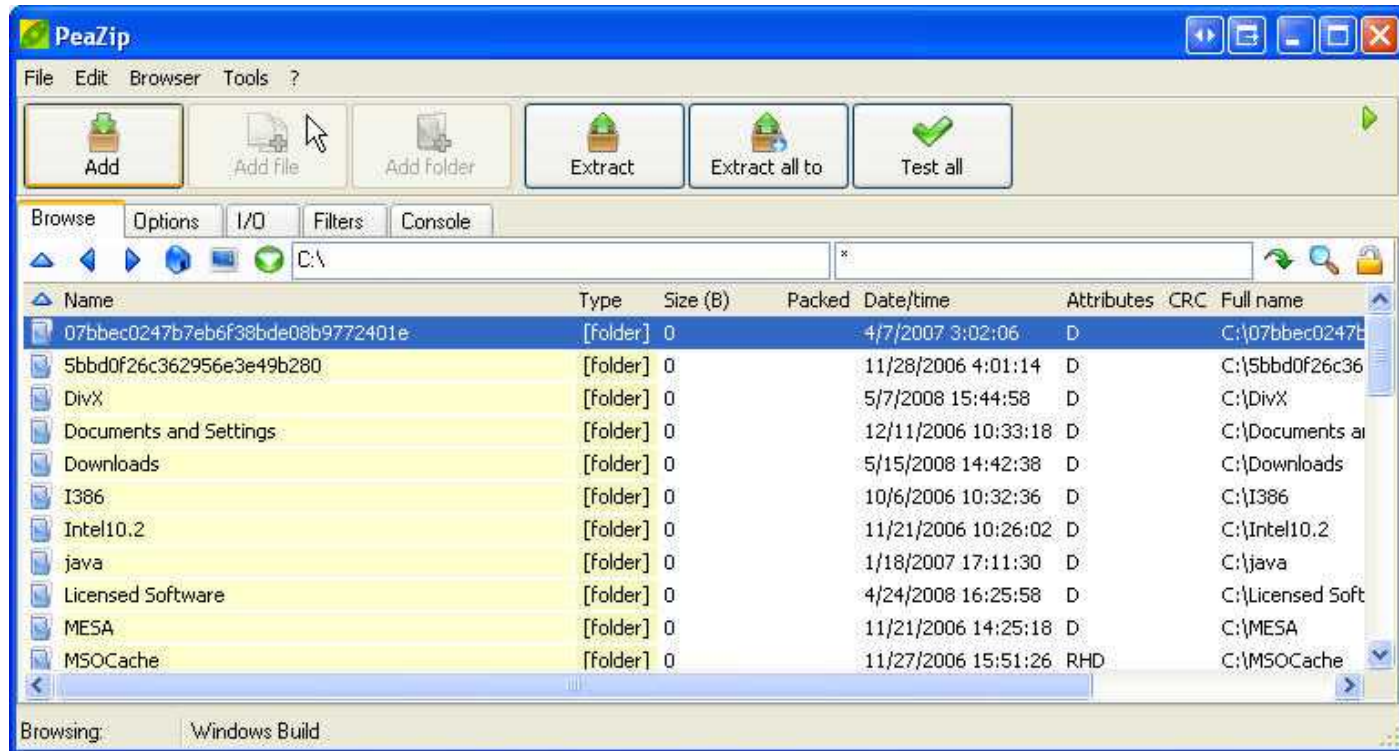

WinRAR-Trial

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



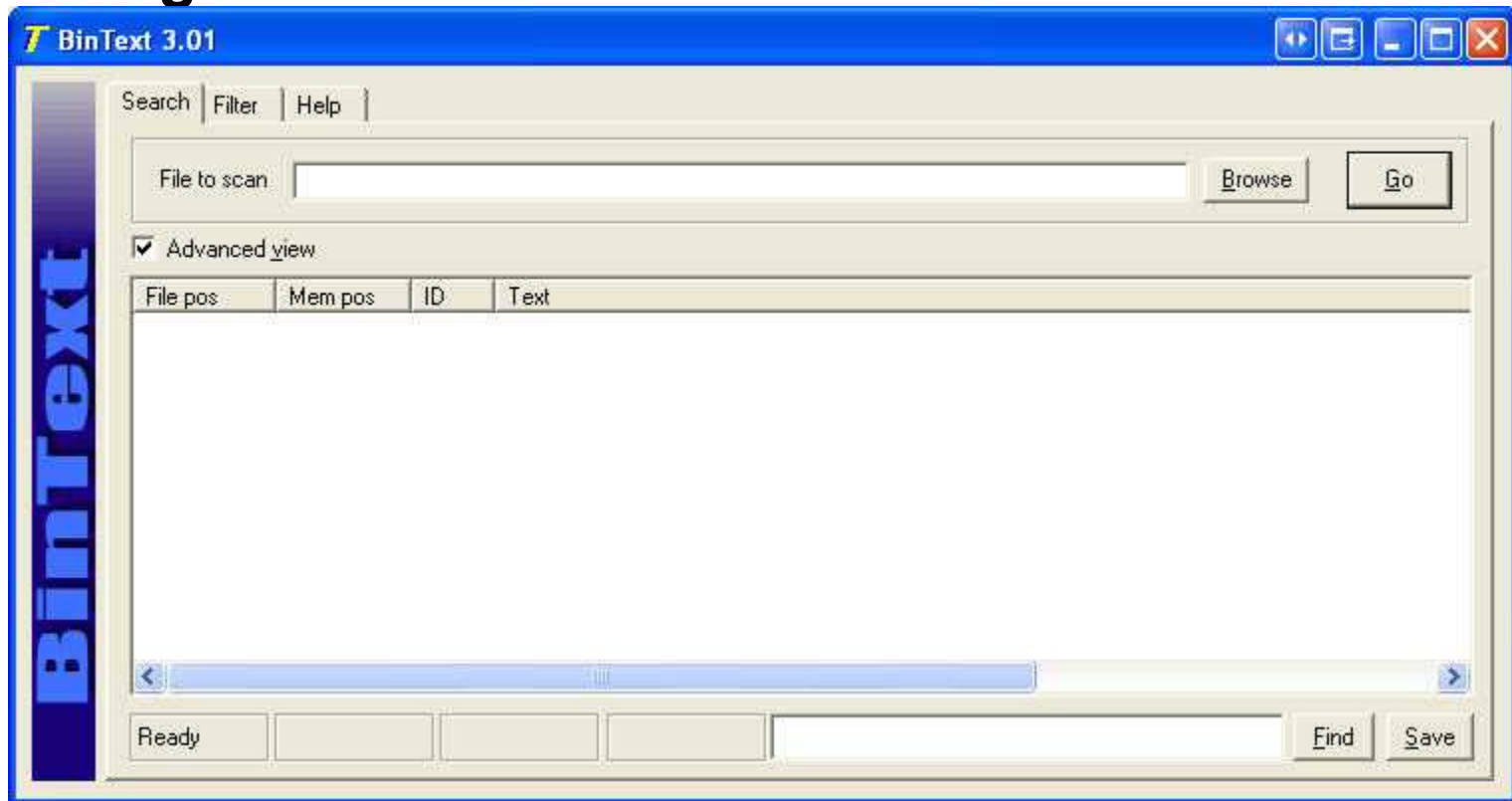
PeaZip

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



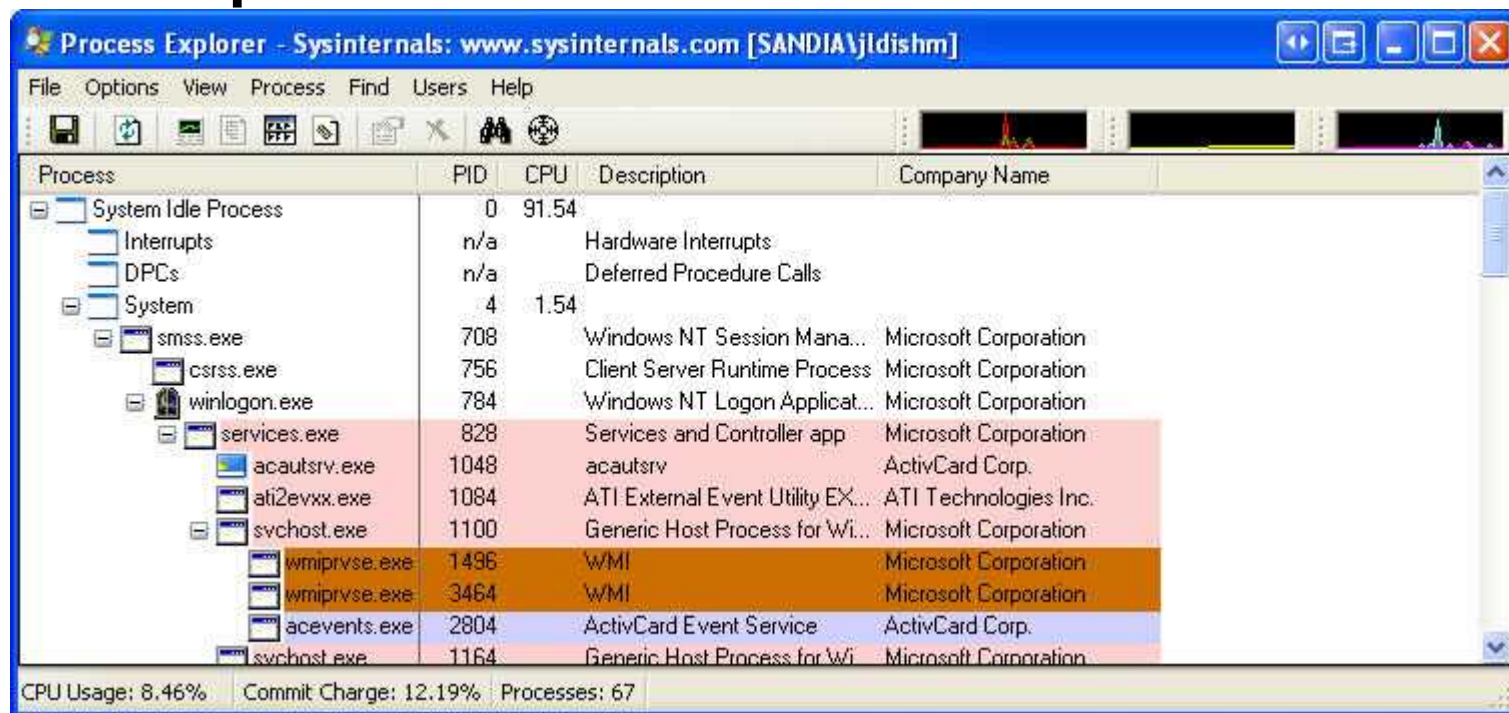
BinText

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



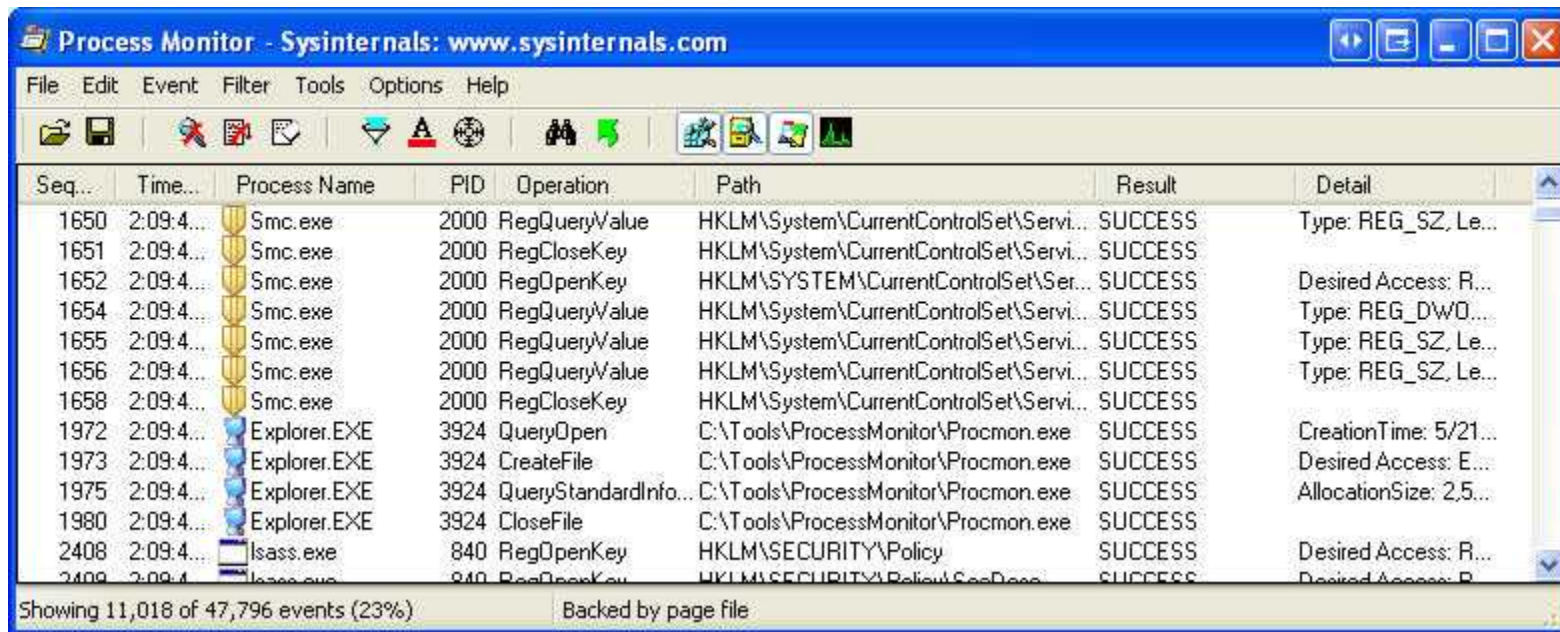
Process Explorer

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



Process Monitor

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



The screenshot shows the Process Monitor application window with the title bar 'Process Monitor - Sysinternals: www.sysinternals.com'. The menu bar includes File, Edit, Event, Filter, Tools, Options, and Help. The toolbar contains icons for file operations, event filtering, and viewing options. The main window displays a table of system events with columns for Sequence Number, Time, Process Name, PID, Operation, Path, Result, and Detail.

| Seq... | Time... | Process Name | PID | Operation | Path | Result | Detail |
|--------|-----------|--------------|------|----------------------|--|---------|------------------------|
| 1650 | 2:09:4... | Smc.exe | 2000 | RegQueryValue | HKLM\System\CurrentControlSet\Servi... | SUCCESS | Type: REG_SZ, Le... |
| 1651 | 2:09:4... | Smc.exe | 2000 | RegCloseKey | HKLM\System\CurrentControlSet\Servi... | SUCCESS | |
| 1652 | 2:09:4... | Smc.exe | 2000 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Ser... | SUCCESS | Desired Access: R... |
| 1654 | 2:09:4... | Smc.exe | 2000 | RegQueryValue | HKLM\System\CurrentControlSet\Servi... | SUCCESS | Type: REG_DW0... |
| 1655 | 2:09:4... | Smc.exe | 2000 | RegQueryValue | HKLM\System\CurrentControlSet\Servi... | SUCCESS | Type: REG_SZ, Le... |
| 1656 | 2:09:4... | Smc.exe | 2000 | RegQueryValue | HKLM\System\CurrentControlSet\Servi... | SUCCESS | Type: REG_SZ, Le... |
| 1658 | 2:09:4... | Smc.exe | 2000 | RegCloseKey | HKLM\System\CurrentControlSet\Servi... | SUCCESS | |
| 1972 | 2:09:4... | Explorer.EXE | 3924 | QueryOpen | C:\Tools\ProcessMonitor\Procmon.exe | SUCCESS | CreationTime: 5/21... |
| 1973 | 2:09:4... | Explorer.EXE | 3924 | CreateFile | C:\Tools\ProcessMonitor\Procmon.exe | SUCCESS | Desired Access: E... |
| 1975 | 2:09:4... | Explorer.EXE | 3924 | QueryStandardInfo... | C:\Tools\ProcessMonitor\Procmon.exe | SUCCESS | AllocationSize: 2,5... |
| 1980 | 2:09:4... | Explorer.EXE | 3924 | CloseFile | C:\Tools\ProcessMonitor\Procmon.exe | SUCCESS | |
| 2408 | 2:09:4... | lsass.exe | 840 | RegOpenKey | HKLM\SECURITY\Policy | SUCCESS | Desired Access: R... |
| 2409 | 2:09:4... | lsass.exe | 840 | RegOpenKey | HKLM\SECURITY\Policy\SecDepe... | SUCCESS | Desired Access: R... |

Showing 11,018 of 47,796 events (23%) Backed by page file

TCPview

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



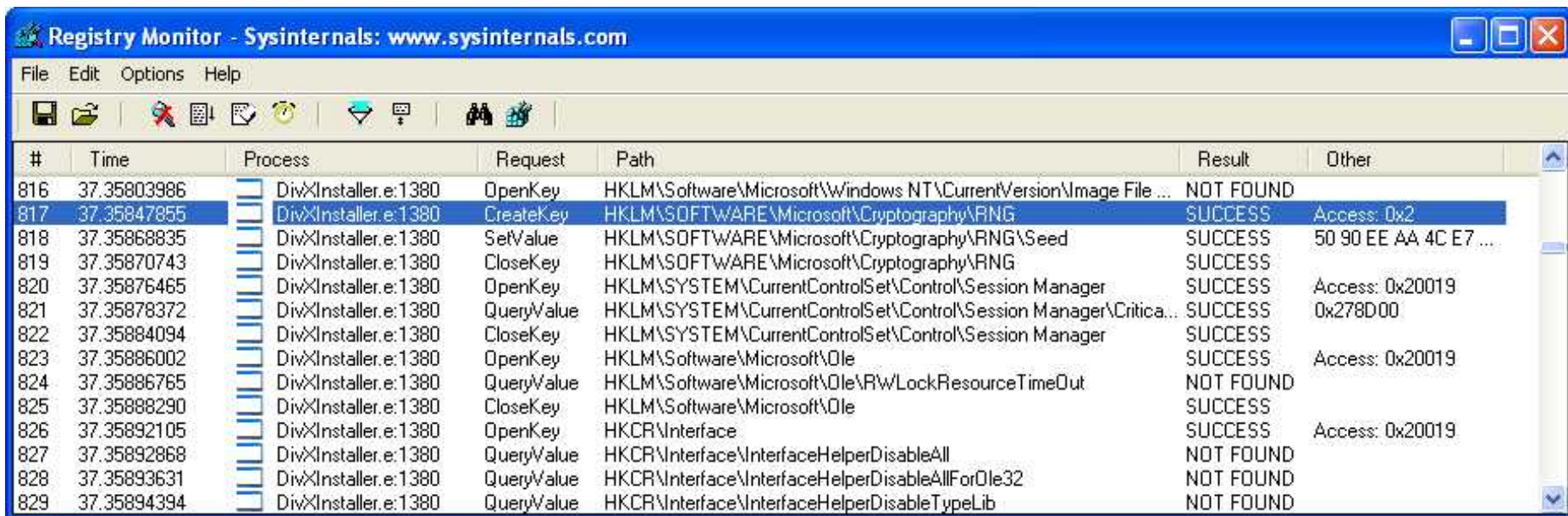
The screenshot shows the TCPView application window with the title bar "TCPView - Sysinternals: www.sysinternals.com". The menu bar includes "File", "Options", "Process", "View", and "Help". The toolbar contains icons for saving, undo, and redo. The main table displays network connections with columns for Process, Protocol, Local Address, Remote Address, and State. The status bar at the bottom shows summary statistics: Endpoints: 82, Established: 20, Listening: 22, Time Wait: 4, and Close Wait: 1.

| Proc... | # | Protocol | Local Address | Remote Address | State |
|-----------------|---|----------|-----------------------------|------------------------------------|-------------|
| [System Proc... | | TCP | s883738.srn.sandia.gov:4690 | ds07snlnt.sandia.gov:microsoft-ds | TIME_WAIT |
| [System Proc... | | TCP | s883738.srn.sandia.gov:4688 | fs02mesant.sandia.gov:microsoft-ds | TIME_WAIT |
| [System Proc... | | TCP | s883738.srn.sandia.gov:4699 | ds07snlnt.sandia.gov:netbios-ssn | TIME_WAIT |
| [System Proc... | | TCP | s883738.srn.sandia.gov:4696 | fs02mesant.sandia.gov:microsoft-ds | TIME_WAIT |
| Alert.exe:1724 | | TCP | S883738:4445 | S883738:0 | LISTENING |
| alg.exe:3144 | | TCP | S883738:1080 | S883738:0 | LISTENING |
| AppleMobileD... | | TCP | S883738:27015 | S883738:0 | LISTENING |
| ccApp.exe:24... | | TCP | S883738:1208 | S883738:0 | LISTENING |
| CcmExec.exe... | | UDP | S883738:1104 | ... | ... |
| communicator... | | TCP | s883738.srn.sandia.gov:3993 | dc12snlnt.srn.sandia.gov:1026 | ESTABLISHED |
| communicator... | | TCP | s883738.srn.sandia.gov:3985 | ls01snlnt.sandia.gov:5061 | ESTABLISHED |
| communicator... | | TCP | s883738.srn.sandia.gov:3997 | es01snlnt.sandia.gov:2171 | ESTABLISHED |
| communicator... | | TCP | s883738.srn.sandia.gov:3991 | es04snlnt.sandia.gov:2138 | ESTABLISHED |
| communicator... | | UDP | S883738:3982 | ... | ... |
| DkService.ex... | | TCP | S883738:31038 | S883738:0 | LISTENING |

Endpoints: 82 Established: 20 Listening: 22 Time Wait: 4 Close Wait: 1

Regmon

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

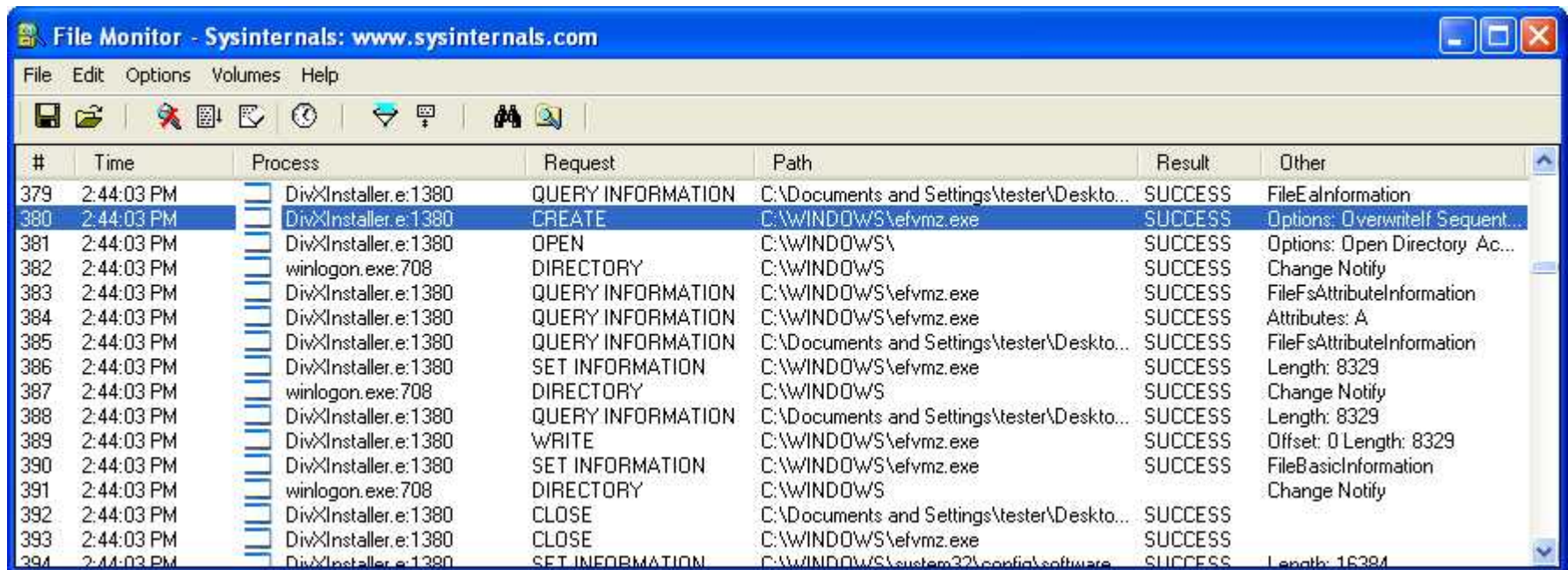


The image shows a screenshot of the Registry Monitor application window. The title bar reads "Registry Monitor - Sysinternals: www.sysinternals.com". The menu bar includes "File", "Edit", "Options", and "Help". The toolbar contains icons for file operations and monitoring. The main display area is a table with the following columns: #, Time, Process, Request, Path, Result, and Other. The table lists a series of registry operations performed by "DivX\Installer.e:1380".

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

Filemon

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



The screenshot shows the File Monitor application window with a blue title bar and a menu bar (File, Edit, Options, Volumes, Help). The main area displays a table of file system activity. The table has columns for #, Time, Process, Request, Path, Result, and Other. The data shows a sequence of operations performed by DivXInstaller.e:1380 and winlogon.exe:708, including queries, creates, opens, writes, and closes of files and directories.

| # | Time | Process | Request | Path | Result | Other |
|-----|------------|----------------------|-------------------|---|---------|---------------------------------|
| 379 | 2:44:03 PM | DivXInstaller.e:1380 | QUERY INFORMATION | C:\Documents and Settings\tester\Desktop... | 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\Desktop... | 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\Desktop... | 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 | SUCCESS | Change Notify |
| 392 | 2:44:03 PM | DivXInstaller.e:1380 | CLOSE | C:\Documents and Settings\tester\Desktop... | 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 |



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**
 - **strcmp or stricmp (string compare)**
 - **ret (returns to calling program)**
 - **call (calls a subroutine)**
- **These are all usually good places to set breakpoints in your debugger.**



Agenda

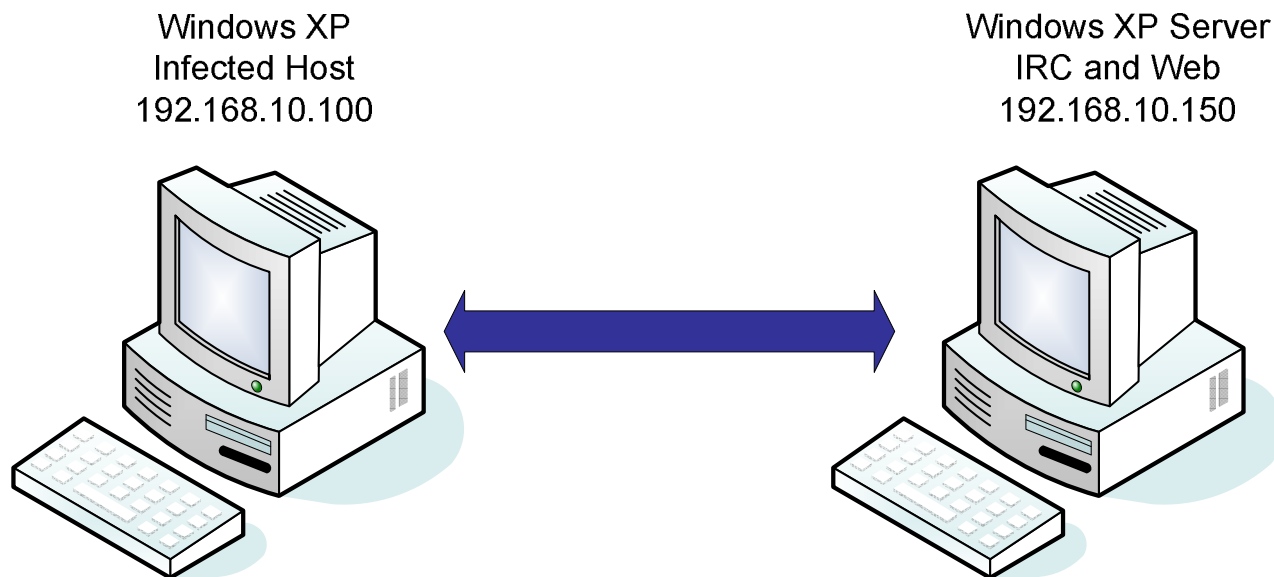
- General Requirements
- Overview of Malware Analysis
- Tools of the Trade
- Analysis Fundamentals
- **Setting up the Environment**
- Time to give it a try
- Tips and Sources



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

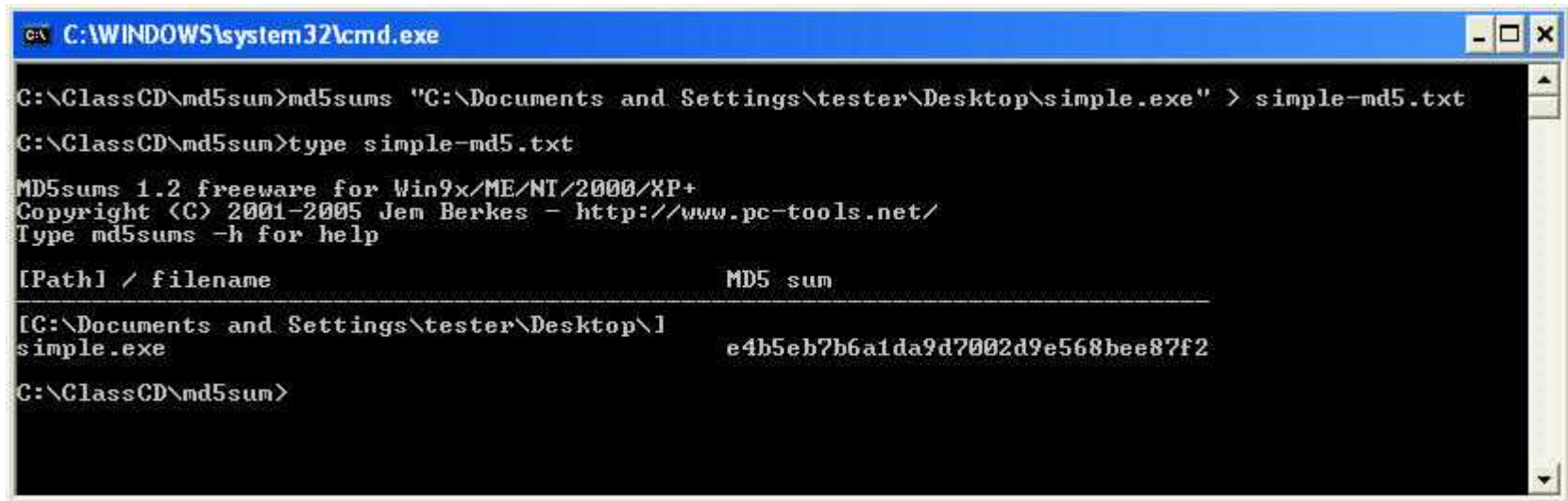


Simple.exe analysis

- **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**

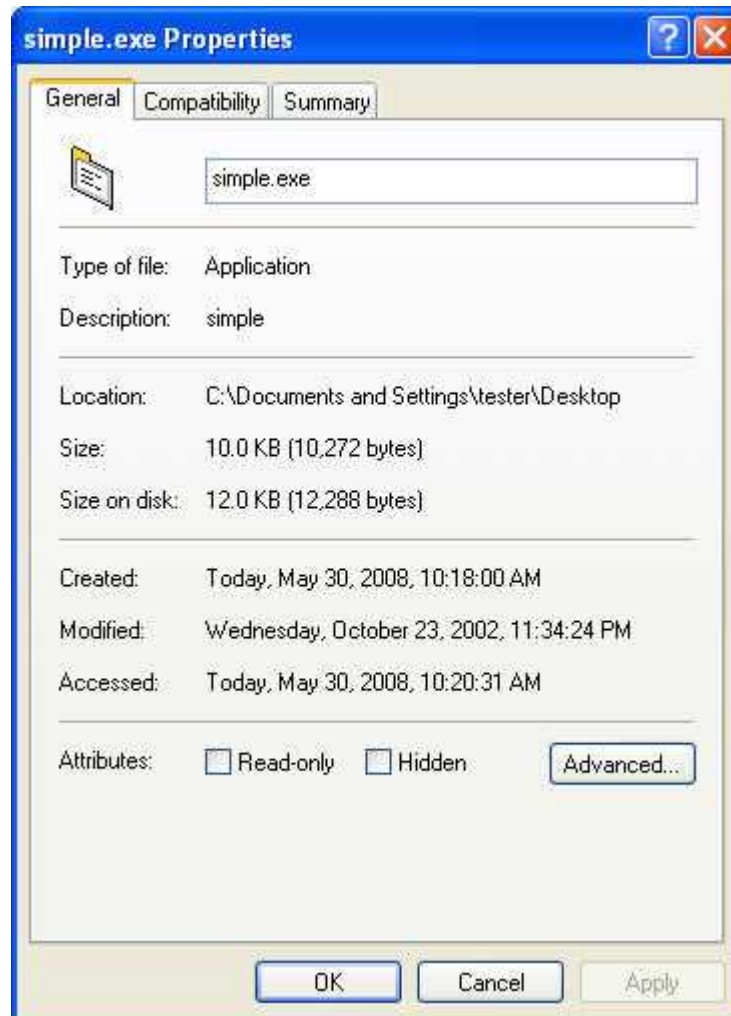


```
C:\WINDOWS\system32\cmd.exe

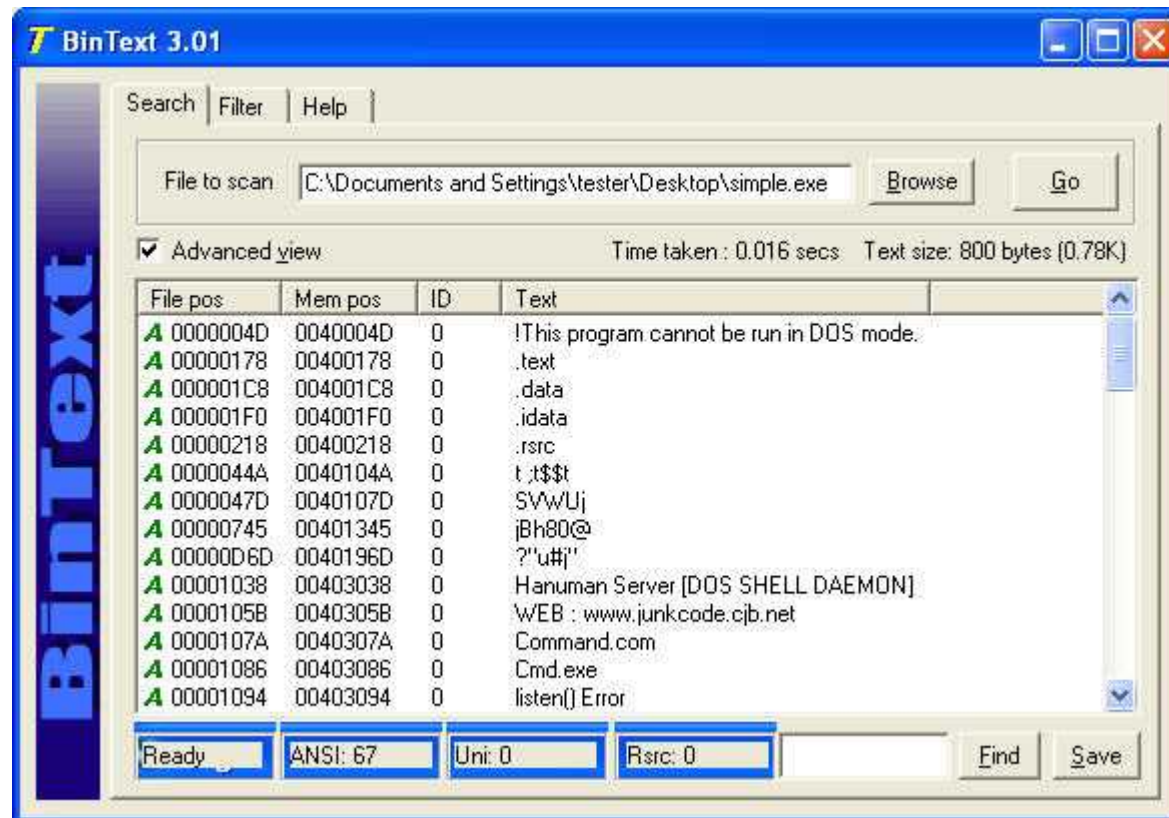
C:\ClassCD\md5sum>md5sums "C:\Documents and Settings\tester\Desktop\simple.exe" > simple-md5.txt
C:\ClassCD\md5sum>type simple-md5.txt
MD5sums 1.2 freeware for Win9x/ME/NT/2000/XP+
Copyright (C) 2001-2005 Jem Berkes - http://www.pc-tools.net/
Type md5sums -h for help

[Path] / filename                                MD5 sum
-----
[C:\Documents and Settings\tester\Desktop\]
simple.exe                                         e4b5eb7b6a1da9d7002d9e568bee87f2
C:\ClassCD\md5sum>
```

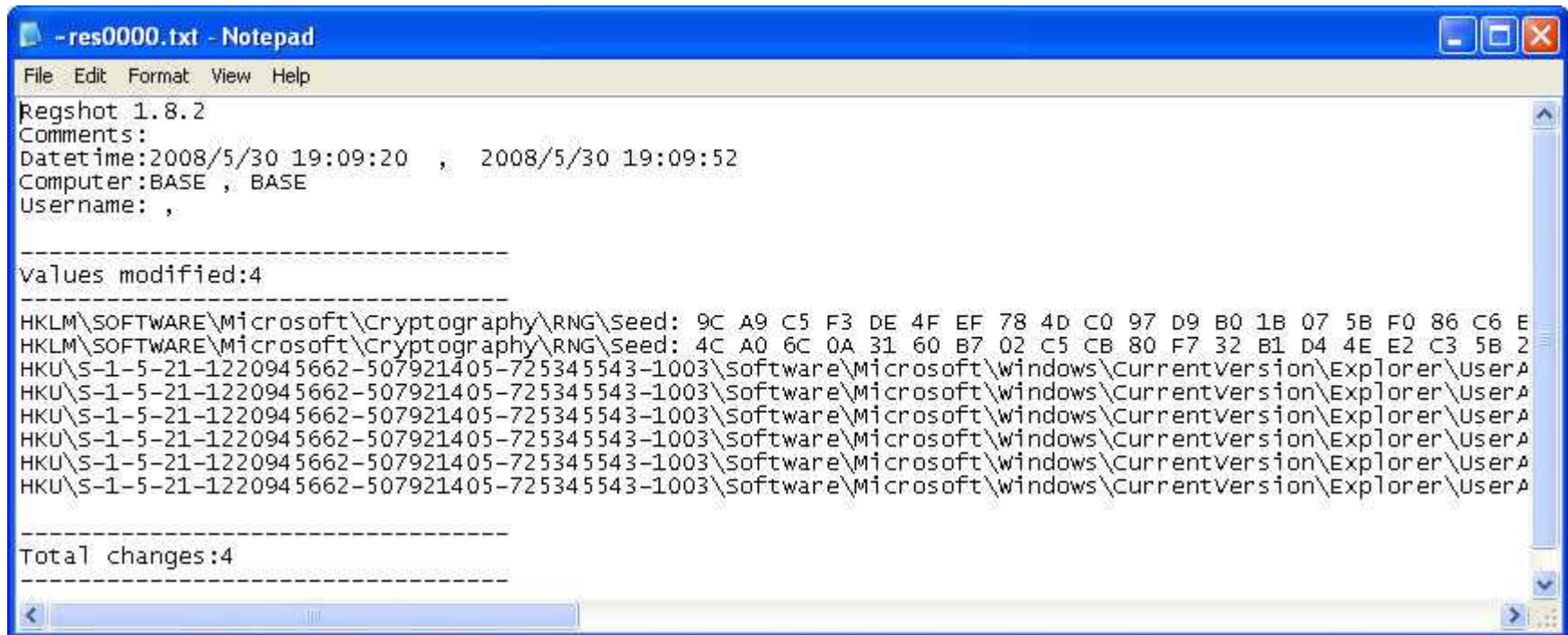
Visual Clues



Simple.exe Strings



Simple.exe RegShot



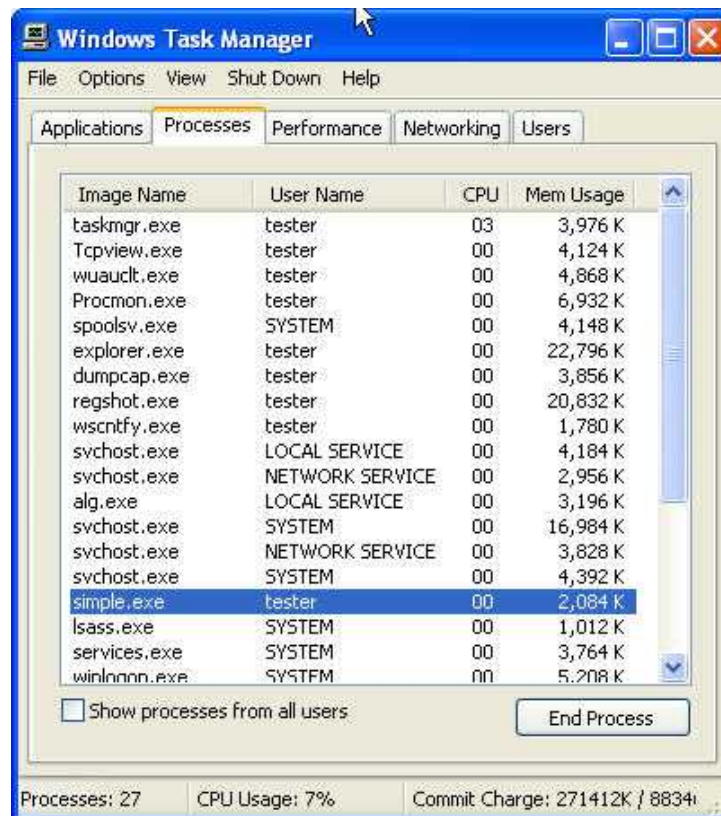
```
-res0000.txt - Notepad
File Edit Format View Help
Regshot 1.8.2
Comments:
Datetime:2008/5/30 19:09:20 , 2008/5/30 19:09:52
Computer:BASE , BASE
Username: ,

-----
Values modified:4
-----
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 9C A9 C5 F3 DE 4F EF 78 4D C0 97 D9 B0 1B 07 5B F0 86 C6 E
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 4C A0 6C 0A 31 60 B7 02 C5 CB 80 F7 32 B1 D4 4E E2 C3 5B 2
HKU\S-1-5-21-1220945662-507921405-725345543-1003\Software\Microsoft\windows\CurrentVersion\Explorer\UserA
HKU\S-1-5-21-1220945662-507921405-725345543-1003\Software\Microsoft\windows\CurrentVersion\Explorer\UserA
HKU\S-1-5-21-1220945662-507921405-725345543-1003\Software\Microsoft\windows\CurrentVersion\Explorer\UserA
HKU\S-1-5-21-1220945662-507921405-725345543-1003\Software\Microsoft\windows\CurrentVersion\Explorer\UserA
HKU\S-1-5-21-1220945662-507921405-725345543-1003\Software\Microsoft\windows\CurrentVersion\Explorer\UserA
HKU\S-1-5-21-1220945662-507921405-725345543-1003\Software\Microsoft\windows\CurrentVersion\Explorer\UserA

-----
Total changes:4
-----
```

Simple.exe

- Does it show up in Task Manager?



Simple.exe TCPview

- It sets up a listening port on port 3333.



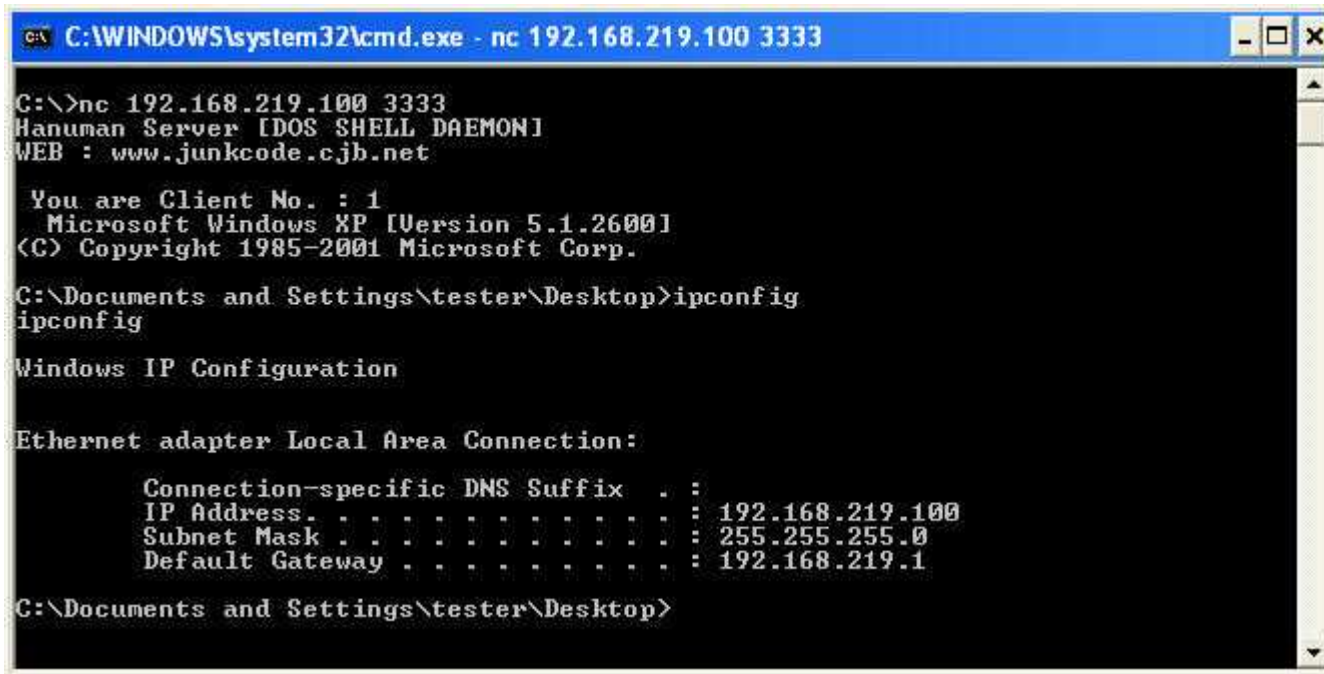
The screenshot shows the TCPView application window from Sysinternals. The title bar reads 'TCPView - Sysinternals: www.sysinternals.com'. The menu bar includes 'File', 'Options', 'Process', 'View', and 'Help'. Below the menu is a toolbar with icons for saving, refreshing, and other functions. The main area is a table with columns: Process #, Protocol, Local Address, Remote Address, and State. The table lists several processes, with 'simple.exe:1272' highlighted in blue, showing it is listening on 'base.localdomain:3333' to 'base:0' via TCP. Other processes like 'alg.exe:1104', 'lsass.exe:728', and 'svchost.exe' are also listed with their respective protocols and addresses. At the bottom, a status bar shows summary statistics: Endpoints: 17, Established: 0, Listening: 5, Time Wait: 0, and Close Wait: 0.

| Process # | Protocol | Local Address | Remote Address | State |
|------------------|----------|-----------------------|----------------|-----------|
| alg.exe:1104 | TCP | base:1029 | base:0 | LISTENING |
| lsass.exe:728 | UDP | base:isakmp | ... | |
| lsass.exe:728 | UDP | base:4500 | ... | |
| simple.exe:1272 | TCP | base.localdomain:3333 | base:0 | LISTENING |
| svchost.exe:1060 | UDP | base.localdomain:ntp | ... | |
| svchost.exe:1060 | UDP | base:ntp | ... | |
| svchost.exe:1060 | UDP | base:1032 | ... | |
| svchost.exe:1124 | UDP | base:1025 | ... | |
| svchost.exe:1124 | UDP | base:1033 | ... | |
| svchost.exe:1208 | UDP | base.localdomain:1900 | ... | |

Endpoints: 17 Established: 0 Listening: 5 Time Wait: 0 Close Wait: 0

Network Activity

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



```
C:\WINDOWS\system32\cmd.exe - nc 192.168.219.100 3333

C:\>nc 192.168.219.100 3333
Hanuman Server [DOS SHELL DAEMON]
WEB : www.junkcode.cjb.net

You are Client No. : 1
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\tester\Desktop>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.219.100
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.219.1

C:\Documents and Settings\tester\Desktop>
```




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.**



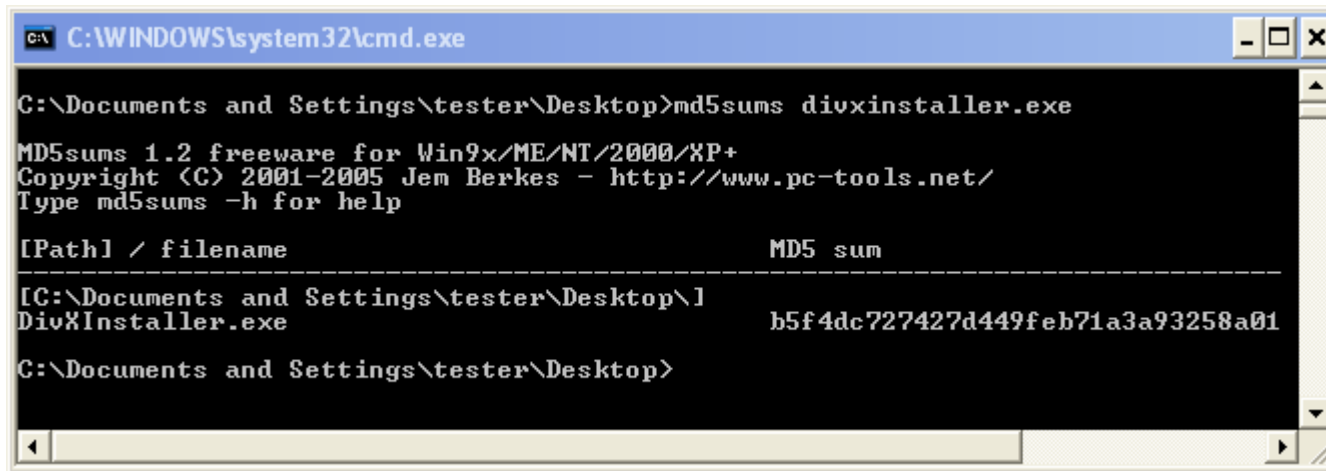
First Look

- **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.



```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\tester\Desktop>md5sums divxinstaller.exe

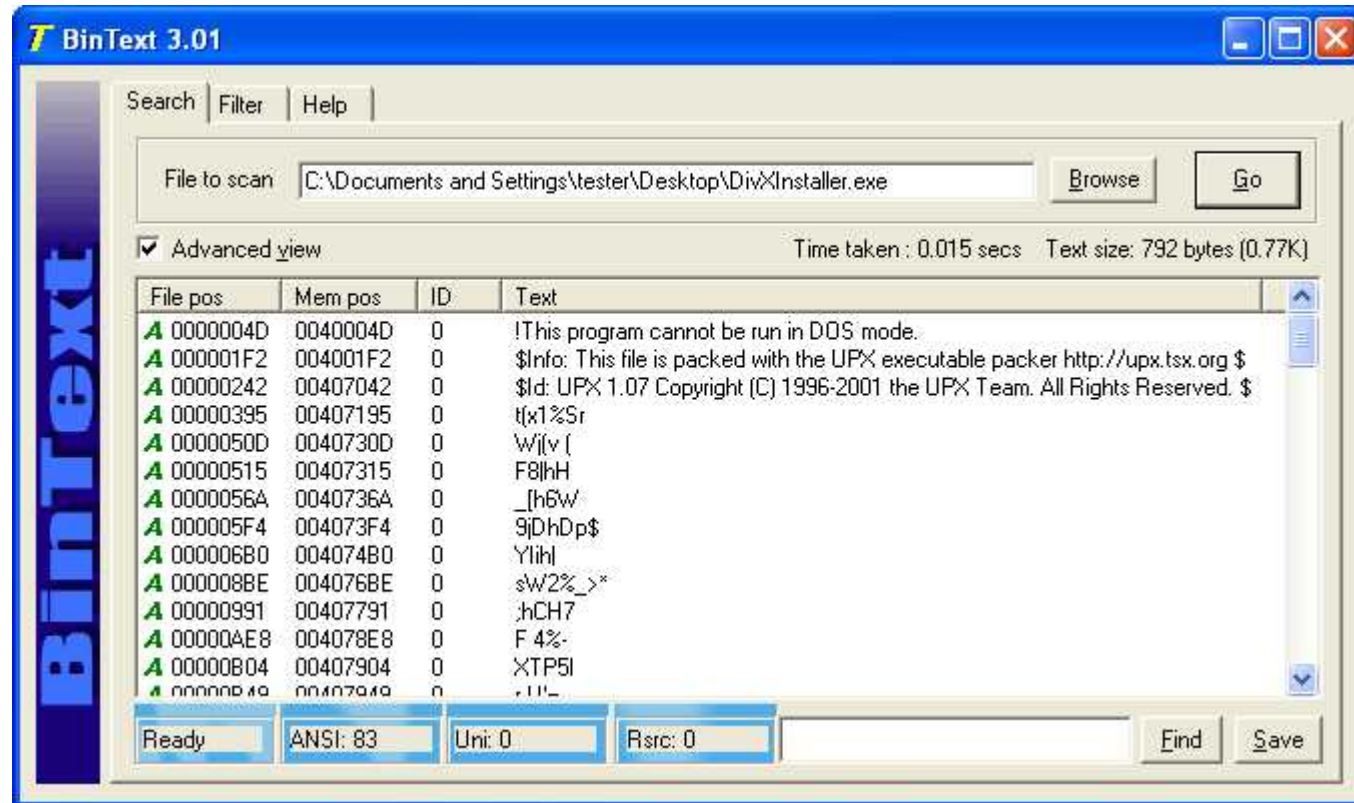
MD5sums 1.2 freeware for Win9x/ME/NT/2000/XP+
Copyright (C) 2001-2005 Jem Berkes - http://www.pc-tools.net/
Type md5sums -h for help

[Path] / filename                                MD5 sum
-----
[C:\Documents and Settings\tester\Desktop\]
DivXInstaller.exe                                b5f4dc727427d449feb71a3a93258a01

C:\Documents and Settings\tester\Desktop>
```

Look For Strings

- Open the file in BinText.



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.





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.



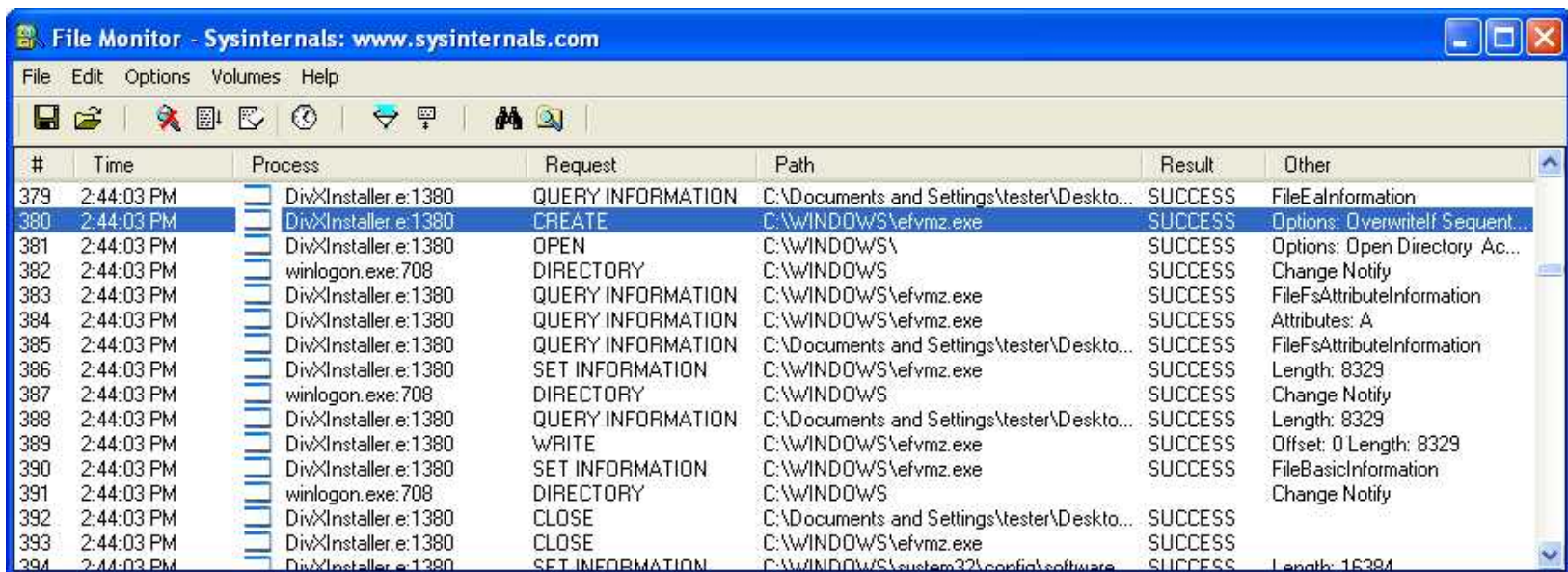
What has changed?

- **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.



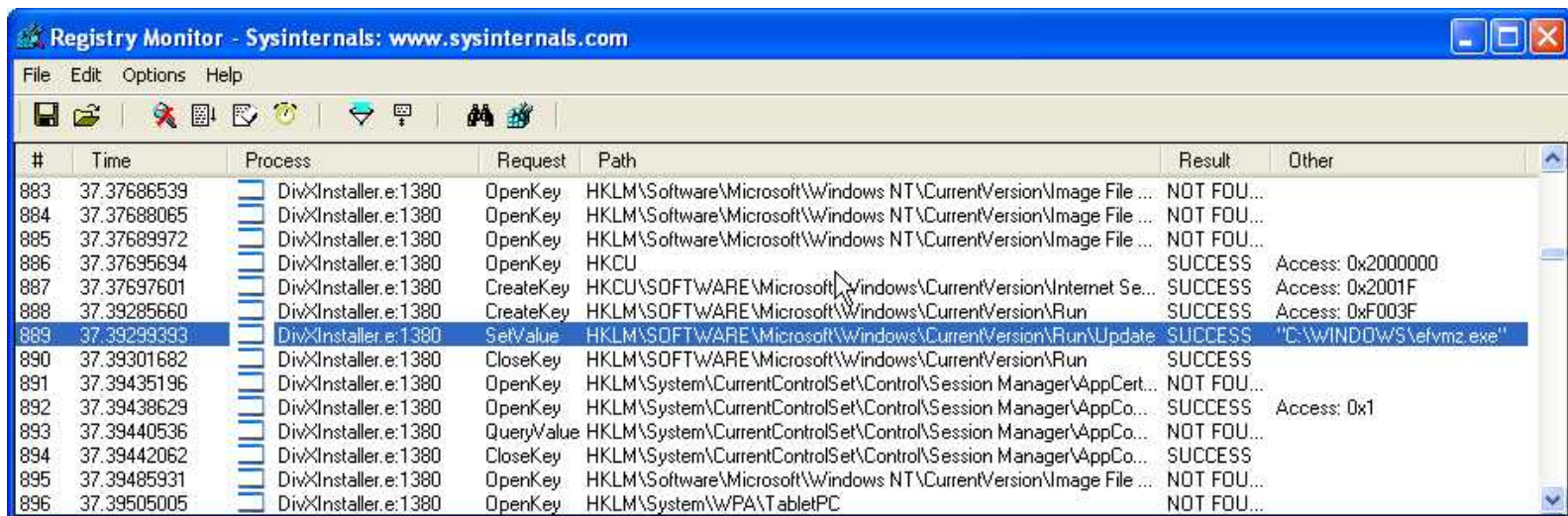
The screenshot shows the File Monitor application window with the title bar "File Monitor - Sysinternals: www.sysinternals.com". The window contains a table of file system operations. The table has columns for #, Time, Process, Request, Path, Result, and Other. The operations are listed from 379 to 394. The process involved is DivXInstaller.e:1380. The requests include QUERY INFORMATION, CREATE, OPEN, DIRECTORY, SET INFORMATION, WRITE, and CLOSE. The paths involve C:\Documents and Settings\tester\Desktop, C:\WINDOWS\efvmz.exe, and C:\WINDOWS. The results are all SUCCESS. The 'Other' column contains additional details such as FileEaInformation, Options: OverwriteIf Sequent..., Change Notify, FileFsAttributeInformation, Attributes: A, FileFsAttributeInformation, Length: 8329, Offset: 0 Length: 8329, FileBasicInformation, and Length: 16384.

| # | Time | Process | Request | Path | Result | Other |
|-----|------------|----------------------|-------------------|---|---------|---------------------------------|
| 379 | 2:44:03 PM | DivXInstaller.e:1380 | QUERY INFORMATION | C:\Documents and Settings\tester\Desktop... | 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\Desktop... | 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\Desktop... | 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 | SUCCESS | Change Notify |
| 392 | 2:44:03 PM | DivXInstaller.e:1380 | CLOSE | C:\Documents and Settings\tester\Desktop... | 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 |

What has changed?

- **Regmon**

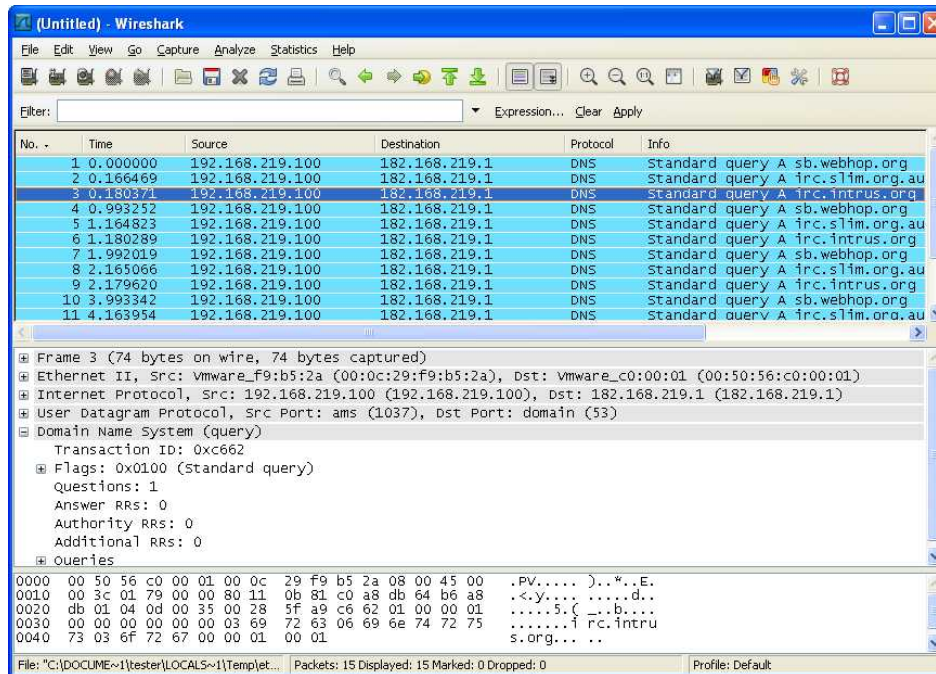
- Shows a SetValue request to the run key.
- Will launch efvmz.exe at boot.



| # | 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\TTablePC | NOT FOU... | |

Network Traffic

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



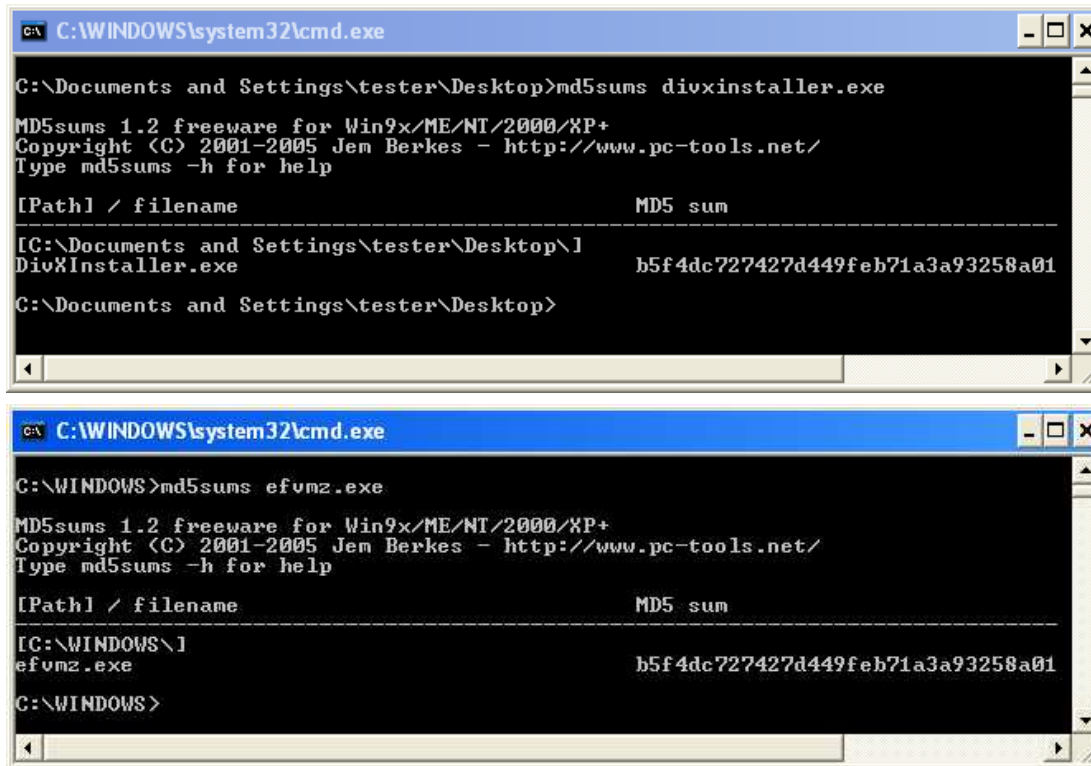


What we know so far?

- 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 DivXInstaller.exe?



The image shows two screenshots of a Windows command prompt window. The top screenshot shows the command 'md5sums divxinstaller.exe' being executed, resulting in the MD5 sum 'b5f4dc727427d449feb71a3a93258a01'. The bottom screenshot shows the command 'md5sums efvmz.exe' being executed, resulting in the same MD5 sum 'b5f4dc727427d449feb71a3a93258a01'.

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\tester\Desktop>md5sums divxinstaller.exe

MD5sums 1.2 freeware for Win9x/ME/NT/2000/KP+
Copyright (C) 2001-2005 Jem Berkes - http://www.pc-tools.net/
Type md5sums -h for help

[Path] / filename                                MD5 sum
-----
[C:\Documents and Settings\tester\Desktop\]
DivXInstaller.exe                                b5f4dc727427d449feb71a3a93258a01

C:\Documents and Settings\tester\Desktop>

C:\WINDOWS\system32\cmd.exe

C:\WINDOWS>md5sums efvmz.exe

MD5sums 1.2 freeware for Win9x/ME/NT/2000/KP+
Copyright (C) 2001-2005 Jem Berkes - http://www.pc-tools.net/
Type md5sums -h for help

[Path] / filename                                MD5 sum
-----
[C:\WINDOWS\]
efvmz.exe                                         b5f4dc727427d449feb71a3a93258a01

C:\WINDOWS>
```




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.



```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com   # source server
#       38.25.63.10      x.acme.com       # x client host
127.0.0.1        localhost
192.168.219.200  irc.intrus.org
```

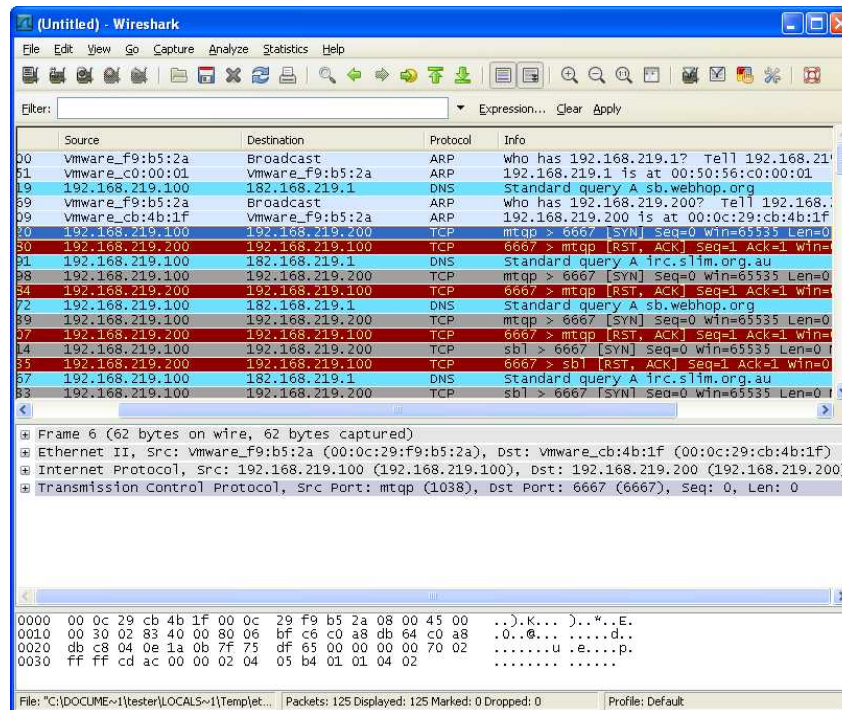


Network Activity

- **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.



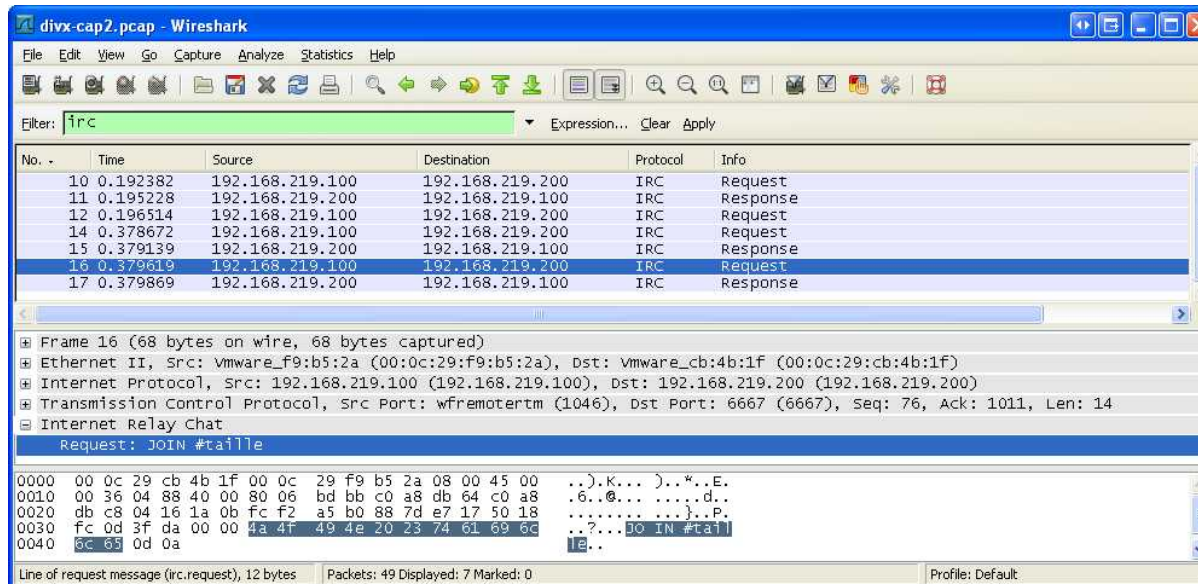


More Resources

- **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.**

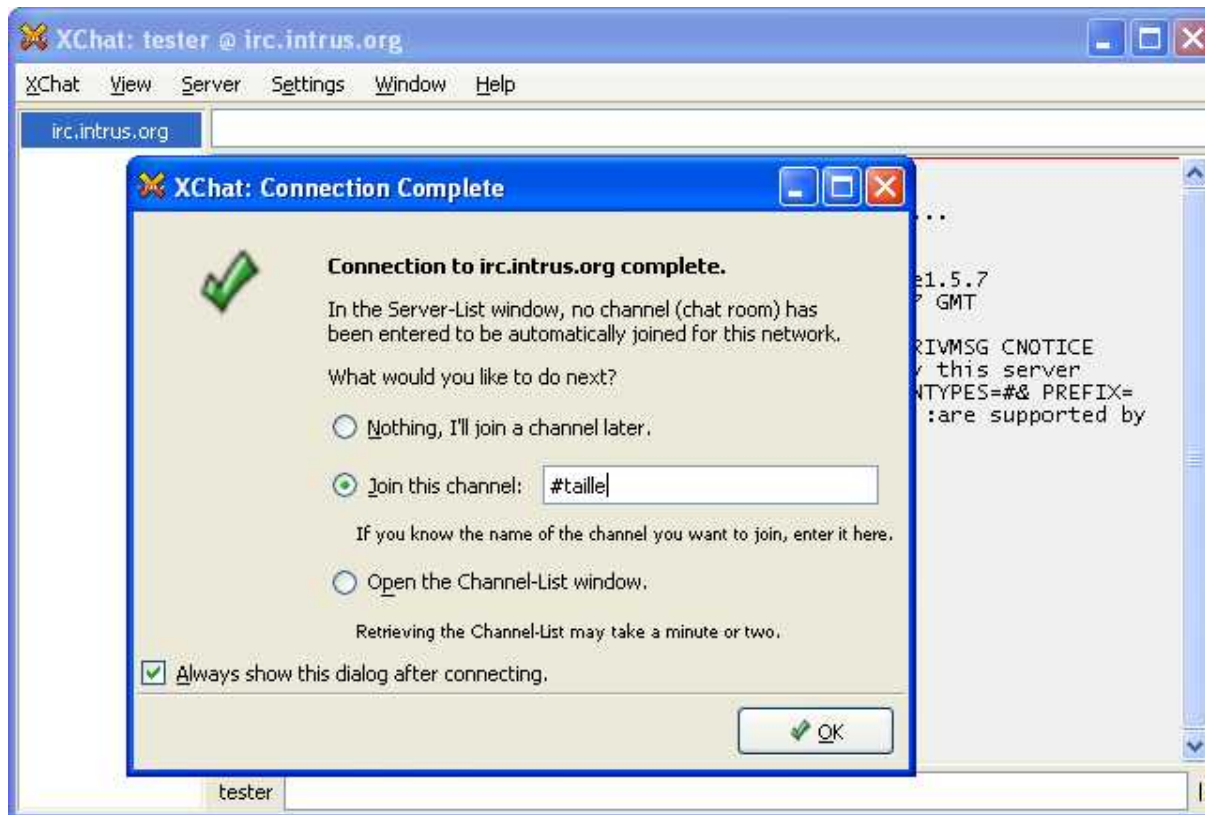
Network Activity

- It joins a channel called “taille”.



IRC Activity

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



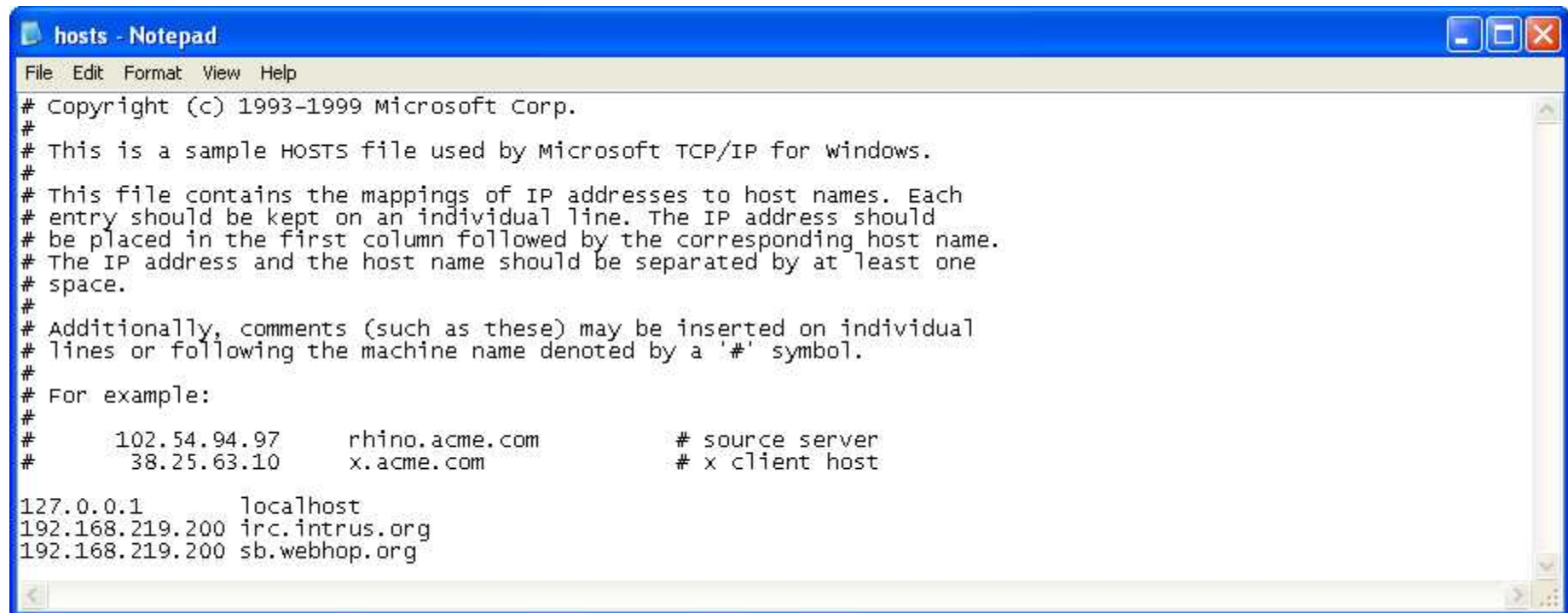
IRC Activity

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



Webhop Analysis

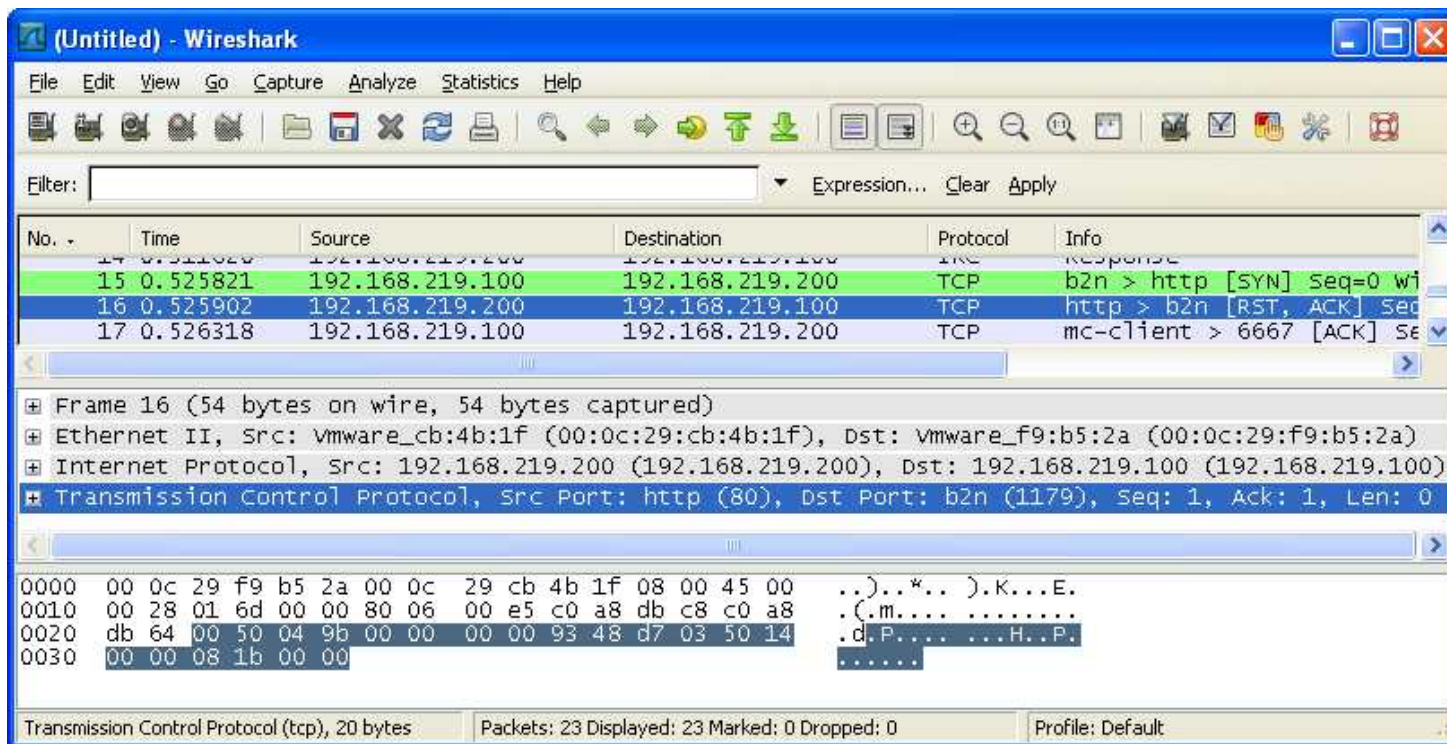
- Edit the host file to add sb.webhop.org



```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com   # source server
#       38.25.63.10       x.acme.com      # x client host
127.0.0.1       localhost
192.168.219.200 irc.intrus.org
192.168.219.200 sb.webhop.org
```

Webhop Analysis

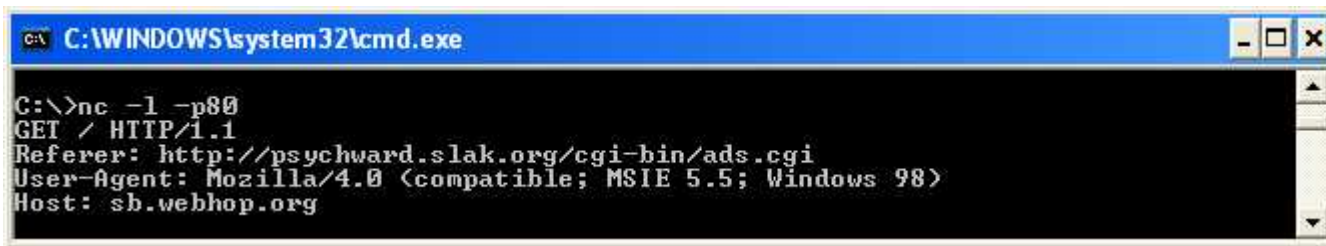
- Start Wireshark on the server and start the capture.





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?



```
C:\WINDOWS\system32\cmd.exe

C:\>nc -l -p80
GET / HTTP/1.1
Referer: http://psychward.slak.org/cgi-bin/ads.cgi
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows 98)
Host: sb.webhop.org
```




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.

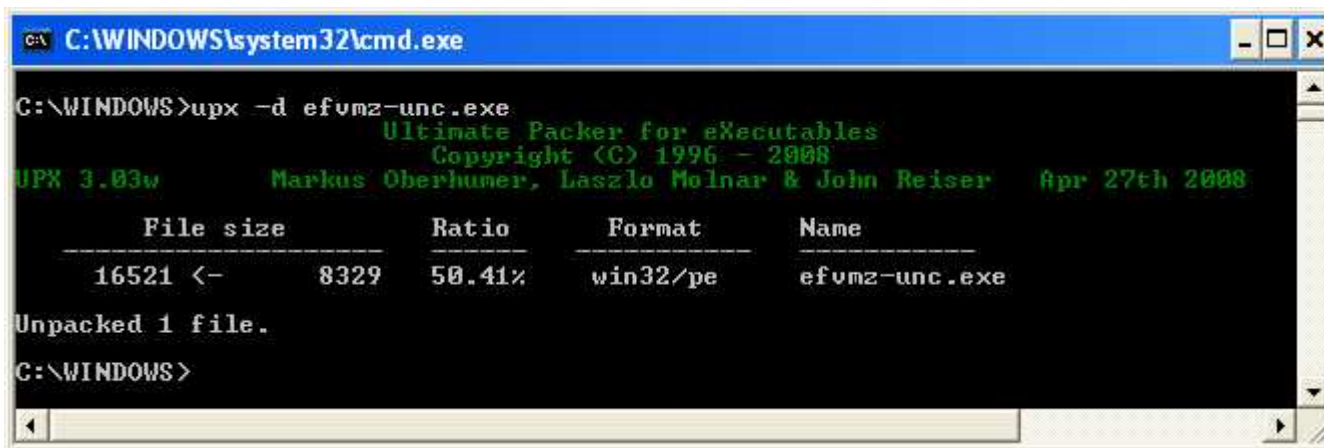


Code Analysis

- **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`



The screenshot shows a Windows command prompt window titled "C:\WINDOWS\system32\cmd.exe". The command `C:\WINDOWS>upx -d efvmz-unc.exe` has been entered. The output of the command is displayed in green text, showing the UPX version (3.03w), copyright information (1996-2008), and authors (Markus Oberhumer, Laszlo Molnar & John Reiser). Below this, a table provides details about the unpacked file:

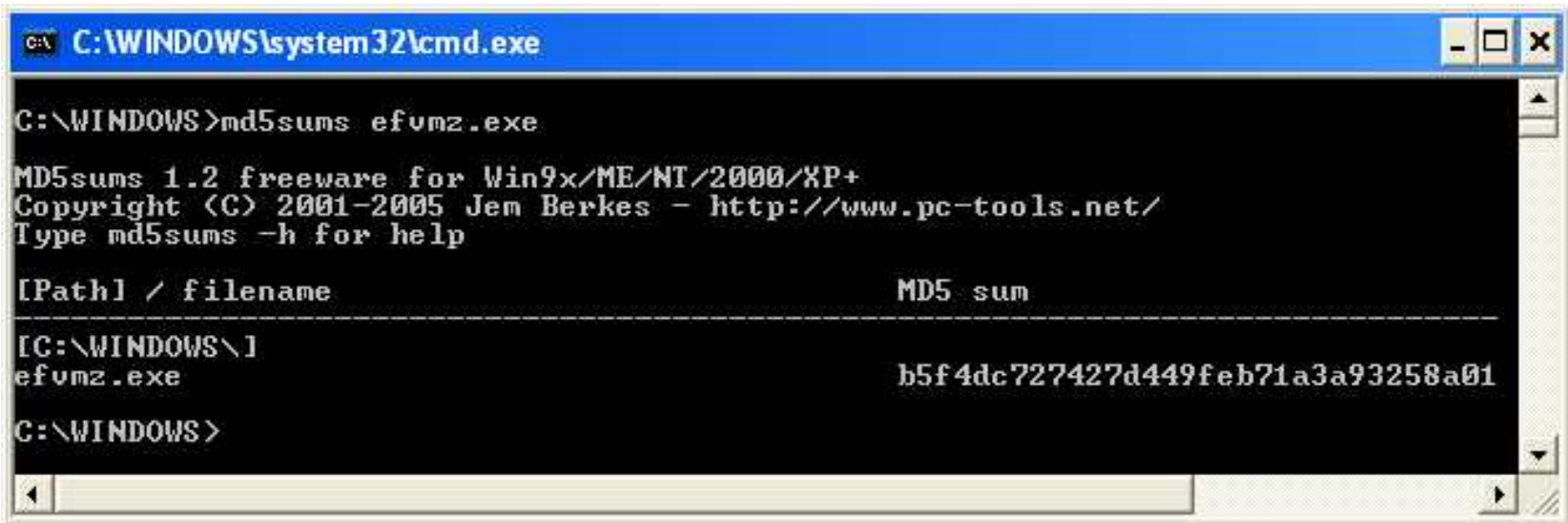
| File size | Ratio | Format | Name |
|---------------|--------|----------|---------------|
| 16521 <- 8329 | 50.41% | win32/pe | efvmz-unc.exe |

The output concludes with "Unpacked 1 file." and the prompt returns to `C:\WINDOWS>`.



Code Analysis

- Like always we do an MD5 hash.



```
C:\WINDOWS\system32\cmd.exe

C:\WINDOWS>md5sums efumz.exe

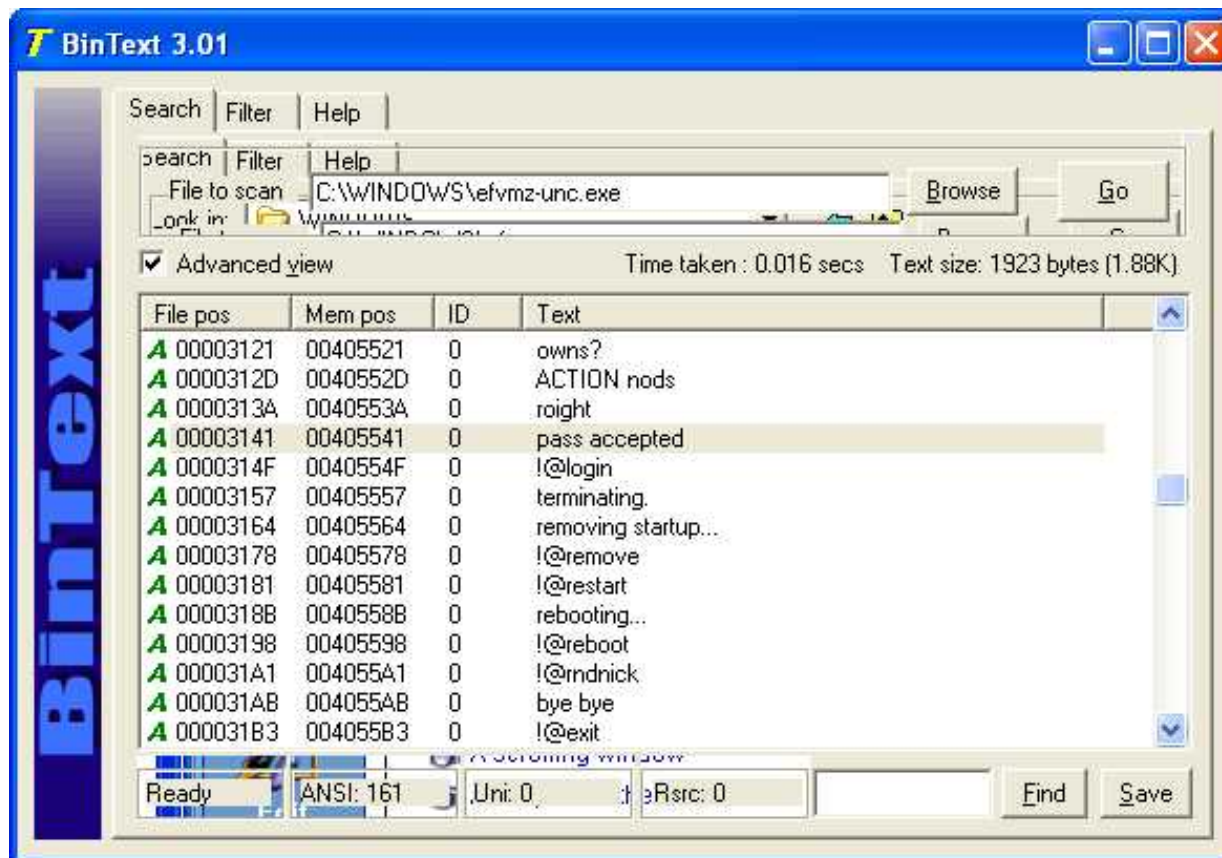
MD5sums 1.2 freeware for Win9x/ME/NT/2000/XP+
Copyright (C) 2001-2005 Jem Berkes - http://www.pc-tools.net/
Type md5sums -h for help

[Path] / filename                                MD5 sum
-----
[C:\WINDOWS\]
efumz.exe                                         b5f4dc727427d449feb71a3a93258a01

C:\WINDOWS>
```

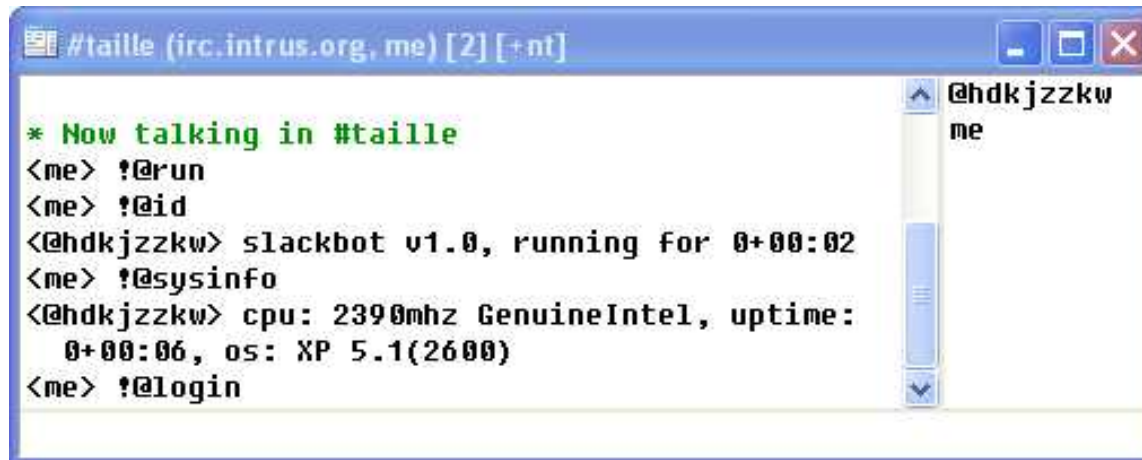
Code Analysis

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



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.



The screenshot shows an IRC chat window with a blue title bar. The chat history includes a green system message, several user commands starting with '!@', and responses from a user named '@hdkjzzkw'.

```
#taille (irc.intrus.org, me) [2] [+nt]

* Now talking in #taille
<me> !@run
<me> !@id
<@hdkjzzkw> slackbot v1.0, running for 0+00:02
<me> !@sysinfo
<@hdkjzzkw> cpu: 2390mhz GenuineIntel, uptime:
0+00:06, os: XP 5.1(2600)
<me> !@login
```

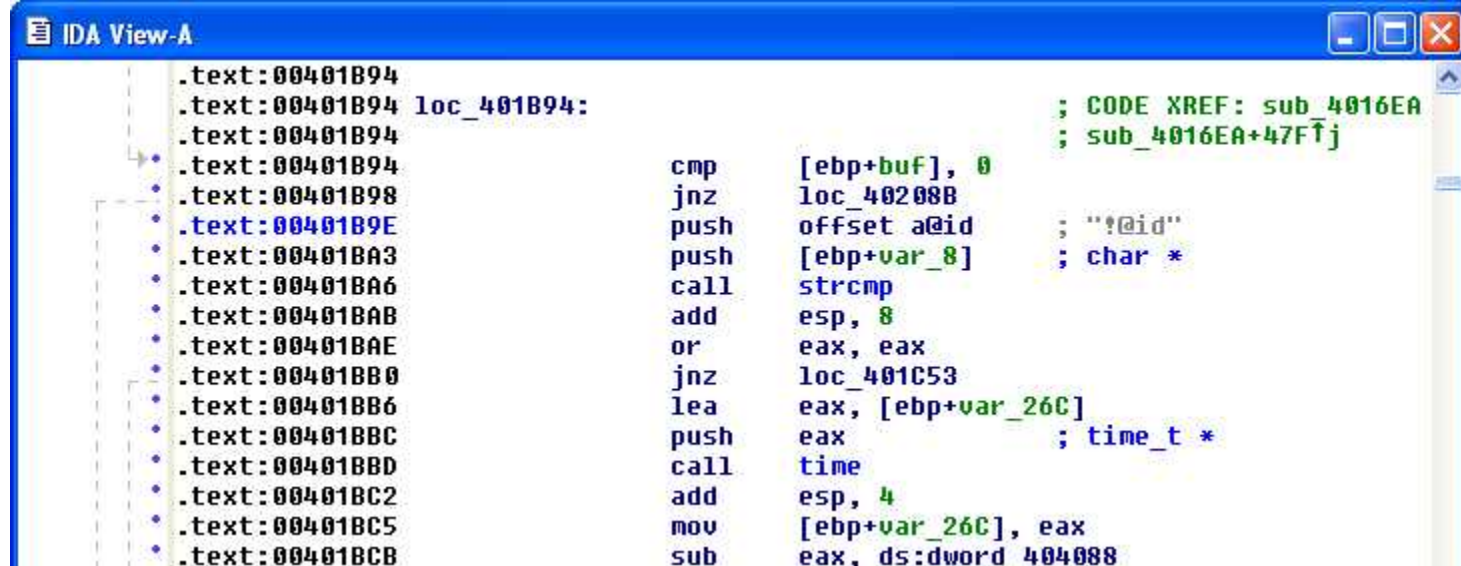


Code Analysis

- **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.



The screenshot shows the IDA View-A window with the assembly code for function loc_401B94. The code is as follows:

```
.text:00401B94
.text:00401B94 loc_401B94:
.text:00401B94
.text:00401B94
.text:00401B98
.text:00401B9E
.text:00401BA3
.text:00401BA6
.text:00401BAB
.text:00401BAE
.text:00401BB0
.text:00401BB6
.text:00401BBC
.text:00401BBD
.text:00401BC2
.text:00401BC5
.text:00401BCB

cmp     [ebp+buf], 0
jnz     loc_40208B
push    offset a@id      ; "!@id"
push    [ebp+var_8]       ; char *
call     strcmp
add     esp, 8
or      eax, eax
jnz     loc_401C53
lea     eax, [ebp+var_26C]
push    eax               ; time_t *
call     time
add     esp, 4
mov     [ebp+var_26C], eax
sub     eax, ds:dword 404088
```

Comments on the right side of the code include:
; CODE XREF: sub_4016EA
; sub_4016EA+47F↑j



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.**

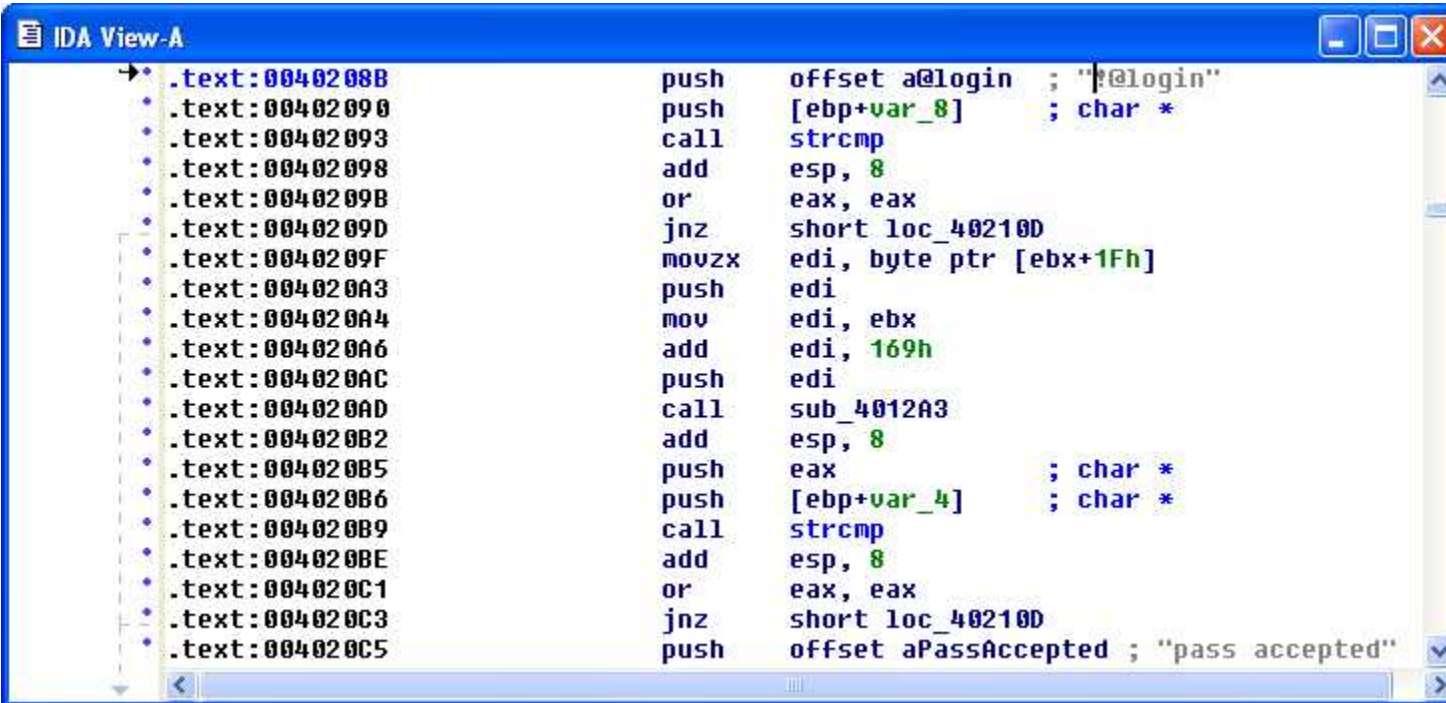


Code Analysis

- 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.



```
IDA View-A
.text:0040208B      push     offset a@login ; "!@login"
.text:00402090      push     [ebp+var_8]    ; char *
.text:00402093      call     strcmp
.text:00402098      add      esp, 8
.text:0040209B      or       eax, eax
.text:0040209D      jnz      short loc_40210D
.text:0040209F      movzx    edi, byte ptr [ebx+1Fh]
.text:004020A3      push     edi
.text:004020A4      mov      edi, ebx
.text:004020A6      add      edi, 169h
.text:004020AC      push     edi
.text:004020AD      call     sub_4012A3
.text:004020B2      add      esp, 8
.text:004020B5      push     eax             ; char *
.text:004020B6      push     [ebp+var_4]     ; char *
.text:004020B9      call     strcmp
.text:004020BE      add      esp, 8
.text:004020C1      or       eax, eax
.text:004020C3      jnz      short loc_40210D
.text:004020C5      push     offset aPassAccepted ; "pass accepted"
```



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.

| | | | |
|----------|------------------|-------------------------------|-----------------------|
| 004020AC | . 57 | PUSH EDI | [Arg1 |
| 004020AD | . E8 F1F1FFFF | CALL efvmz.004012A3 | efvmz.004012A3 |
| 004020B2 | . 83C4 08 | ADD ESP,8 | |
| 004020B5 | . 50 | PUSH EAX | [s2 |
| 004020B6 | . FF75 FC | PUSH DWORD PTR SS:[EBP-4] | s1 |
| 004020B9 | . E8 56150000 | CALL <JMP.&CRTDLL.strcmp> | strcmp |
| 004020BE | . 83C4 08 | ADD ESP,8 | |
| 004020C1 | . 09C0 | OR EAX,EAX | |
| 004020C3 | . 75 48 | JNZ SHORT efvmz.0040210D | |
| 004020C5 | . 68 41554000 | PUSH efvmz.00405541 | ASCII "pass accepted" |
| 004020CA | . FF75 A0 | PUSH DWORD PTR SS:[EBP-60] | |
| 004020CD | . FF75 E4 | PUSH DWORD PTR SS:[EBP-1C] | |
| 004020D0 | . E8 C90C0000 | CALL efvmz.00402D9E | |
| 004020D5 | . 83C4 0C | ADD ESP,0C | |
| 004020D8 | . 8B45 DC | MOV EAX,DWORD PTR SS:[EBP-24] | |
| 004020DB | . 89C1 | MOV ECX,EAX | |
| 004020DD | . 83C8 FF | OR EAX,FFFFFFFF | |
| 004020E0 | . 40 | INC EAX | |
| 004020E1 | . 803C01 00 | CMP BYTE PTR DS:[ECX+EAX],0 | |
| 004020E5 | . 75 F9 | JNZ SHORT efvmz.004020E0 | |
| 004020E7 | . 83C0 01 | ADD EAX,1 | |
| 004020EA | . 50 | PUSH EAX | [size |
| 004020EB | . E8 B8140000 | CALL <JMP.&CRTDLL.malloc> | malloc |
| 004020F0 | . 83C4 04 | ADD ESP,4 | |
| 004020F3 | . 8945 D0 | MOV DWORD PTR SS:[EBP-30],EAX | |
| 004020F6 | . FF75 DC | PUSH DWORD PTR SS:[EBP-24] | |
| 004020F9 | . FF75 D0 | PUSH DWORD PTR SS:[EBP-30] | |
| 004020FC | . E8 9B120000 | CALL efvmz.0040339C | |
| 00402101 | . C745 CC 010001 | MOV DWORD PTR SS:[EBP-34],1 | |
| 00402108 | . F9 04090000 | IMP efvmz.00402A11 | |

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).



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.7C901 |
| 0012F814 | 00000001 | |
| 0012F818 | FFFFFFFF | |
| 0012F81C | 00000000 | |
| 0012F820 | 00000000 | |
| 0012F824 | 7FFDF000 | |
| 0012F828 | 0012F900 | |
| 0012F82C | 00001000 | |

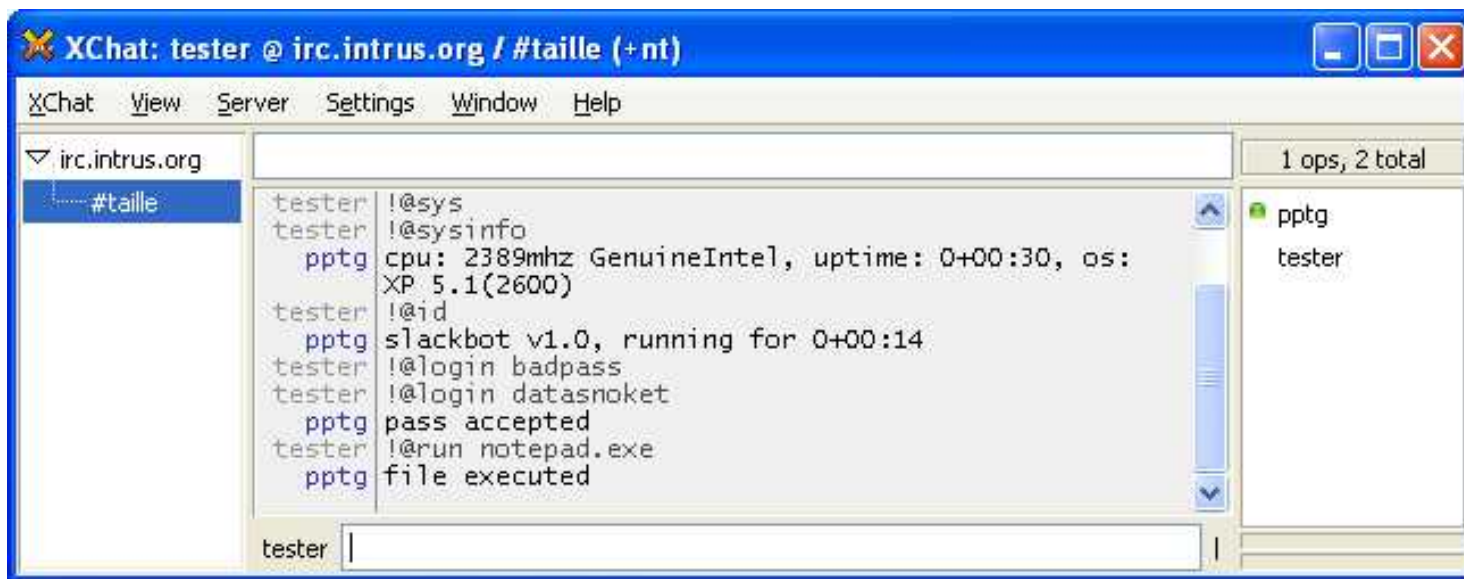


Code Analysis

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

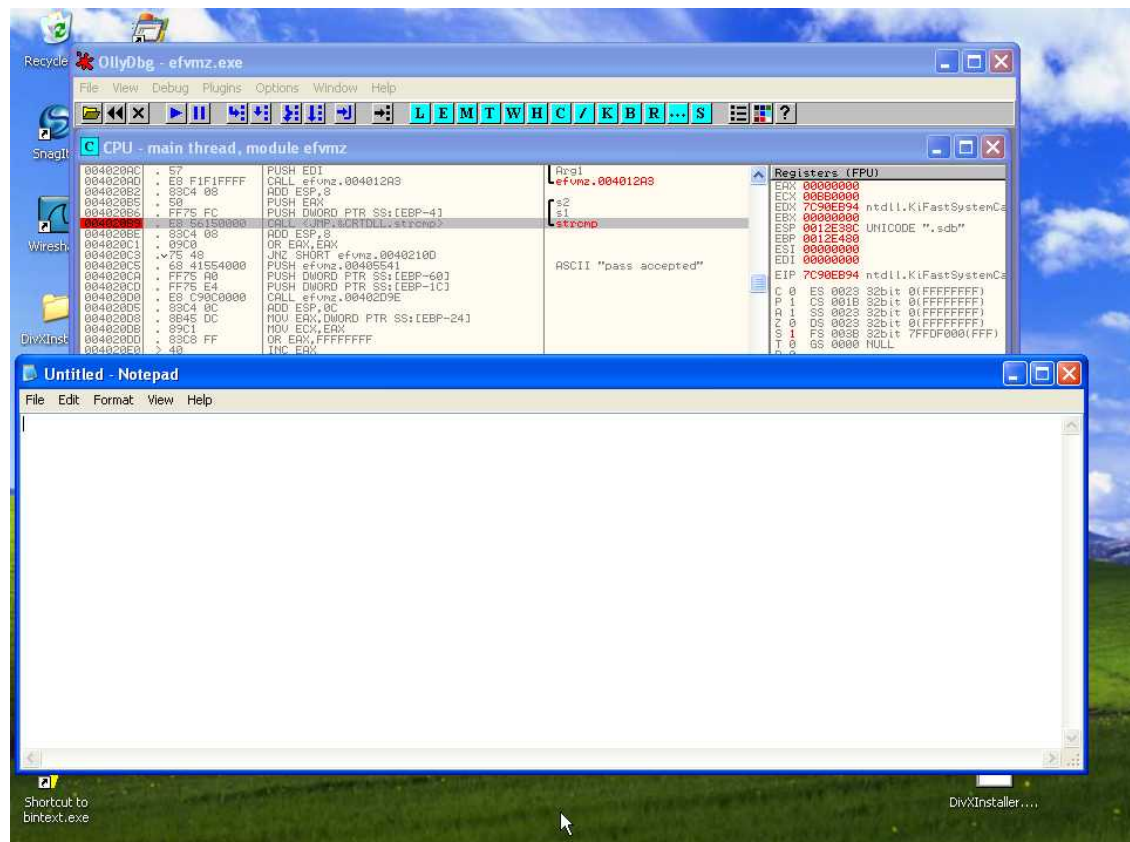
Code Analysis

- 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.





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 “datasnokit”.
- 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**



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/>