Malcode Analysis Techniques for Incident Handlers

Russ McRee holisticinfosec.org

20th Annual FIRST Conference

© Russ McRee

Bio / Disclaimer

- Security analyst / researcher for holisticinfosec.org
- I am also an incident response security analyst for Microsoft Online Services Security and Compliance, part of the Global Foundation Services group.
- The views, opinions, and methodologies discussed here do not reflect those of my employer, thus no content herein is to be attributed to Microsoft.
- Though I draw on resources from commercial vendors this does not imply that I promote or recommend said vendors.

Standard Forensic Methodology

- Verification
- System Description
- Evidence Collection
- Timeline Creation and Analysis
- OS-Specific Media Analysis
- Data Recovery
- String Search
- Reporting

Malware Investigative Methodology - Triage

- Incident Handlers rarely benefit from the same operating timelines as forensic investigators.
- “We need information and we need it now.”
- What is it, why or how did it get there, and how do we stop it?

Malware Investigative Methodology – Triage (2)

- Identify & Analyze
- Contain
- Eradicate
- Recover
- Prevent

- We’ll cover Identification and Analysis today.

Malcode Analysis Tools

- Monitored IDS or firewall logs have tipped you off to an infected host…

- Identify
  - **Mandiant Red Curtain**
  - **Process Explorer**
  - **Rapier 3.2**
  - **Online resources**
- Other helpful tools include SysInternals and Helix

Malcode Analysis Tools

- Analyze
  - **Process Monitor**
  - **Malcode Analysis Software Tools - iDefense Labs**
  - **Wireshark**
  - **Visualization**
  - **NSM-Console**
  - **IDS & Firewall logs**

IDENTIFICATION PHASE

Where’s Waldo?

Mandiant Red Curtain
http://mandiant.com/mrc

- An interesting tool that moves beyond expected norms.
- “MANDIANT Red Curtain is free software for Incident Responders that assists with the analysis of malware. MRC examines executables to determine how suspicious they are based on a set of criteria. It examines multiple aspects of an executable, looking at things such as the entropy, indications of packing, compiler and packing signatures, the presence of digital signatures, and other characteristics to generate a threat "score." This score can be used to identify whether a set of files is worthy of further investigation. ”

MRC – The Entropy of Evil

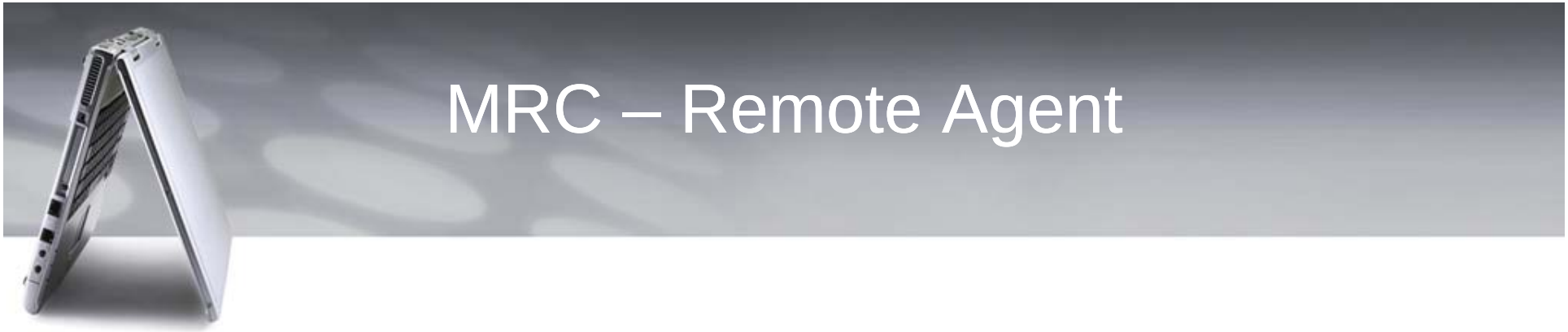
- Entropy - Measure of disorder and randomness.
- One of the fundamental properties of encrypted, compressed, or obfuscated (depending on the method of obfuscation) data is that its entropy (or "randomness") tends to be higher than that of "structured" data, such as user generated documents and computer programs.

MRC – The Entropy of Evil (2)

1. A file is opened and the bytes read in to calculate a global entropy value for the entire file.
2. MRC then divides the file into overlapping samples and calculates the entropy across them. For arguments sake, assume a file of size X is divided into n samples of size Y.
3. The mean and standard deviation of all entropy values from all samples is calculated. The overall entropy for the input file is derived by taking the mean and adding one standard deviation to it. This value is referred to as the Sample Source Entropy.
4. Sample Source Entropy and Global Entropy are compared to a threshold. This threshold is an empirically derived value between 0 and 1. If either entropy value is greater than the threshold, the data block is determined to be entropic, and therefore potentially interesting. - Mandiant Red Curtain User Guide
5. Blah, blah, blah…does it work?

MRC – Use & Deployment

- MRC can be run locally on the suspect host.
- .NET 2.0 framework dependent.
- Can also be run as a remote agent.
- Note: Engage only trusted tools as part of your analysis. Why?
- Here’s where Helix comes in handy.

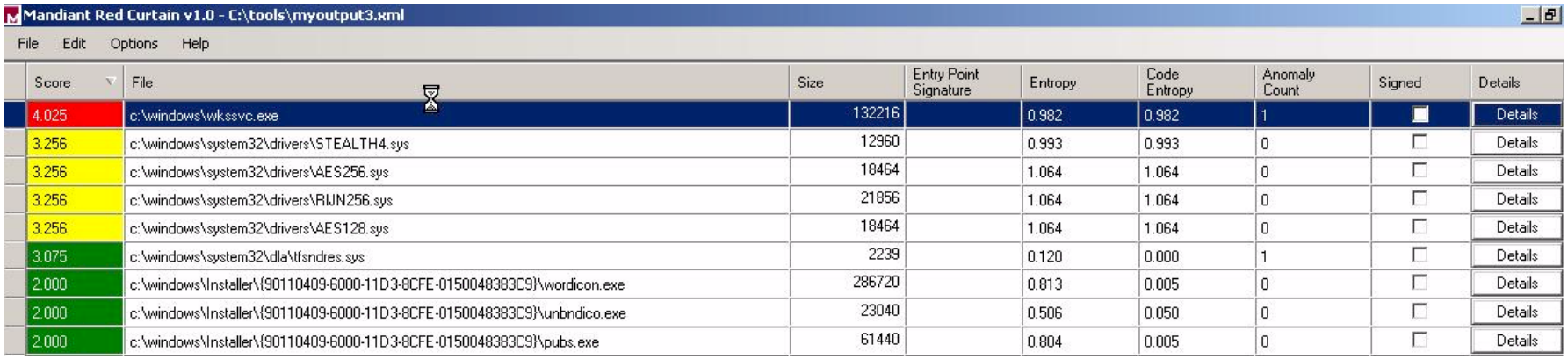


MRC – Remote Agent

- Create agent files with MRC.
- Copy to victim host.
- Share your local CD drive as cdrom.
- psexec -u <admin acct> -p <password> \\<victim host ip> net use x: \\ <localhost ip\cdrom>
- psexec –w x: \IR\xp -u <admin acct> -p <password> \\<victim host ip> x: \IR\xp\cmd.exe
- Now on victim host, issue MRCAgent.exe epcompilersigs.dat eppackersigs.dat roamingsigs -r c:\windows output.xml
- Open output.xml in MRC console.

Mandiant Red Curtain

Sometimes results are immediately conclusive:



Mandiant Red Curtain v1.0 - C:\tools\myoutput3.xml

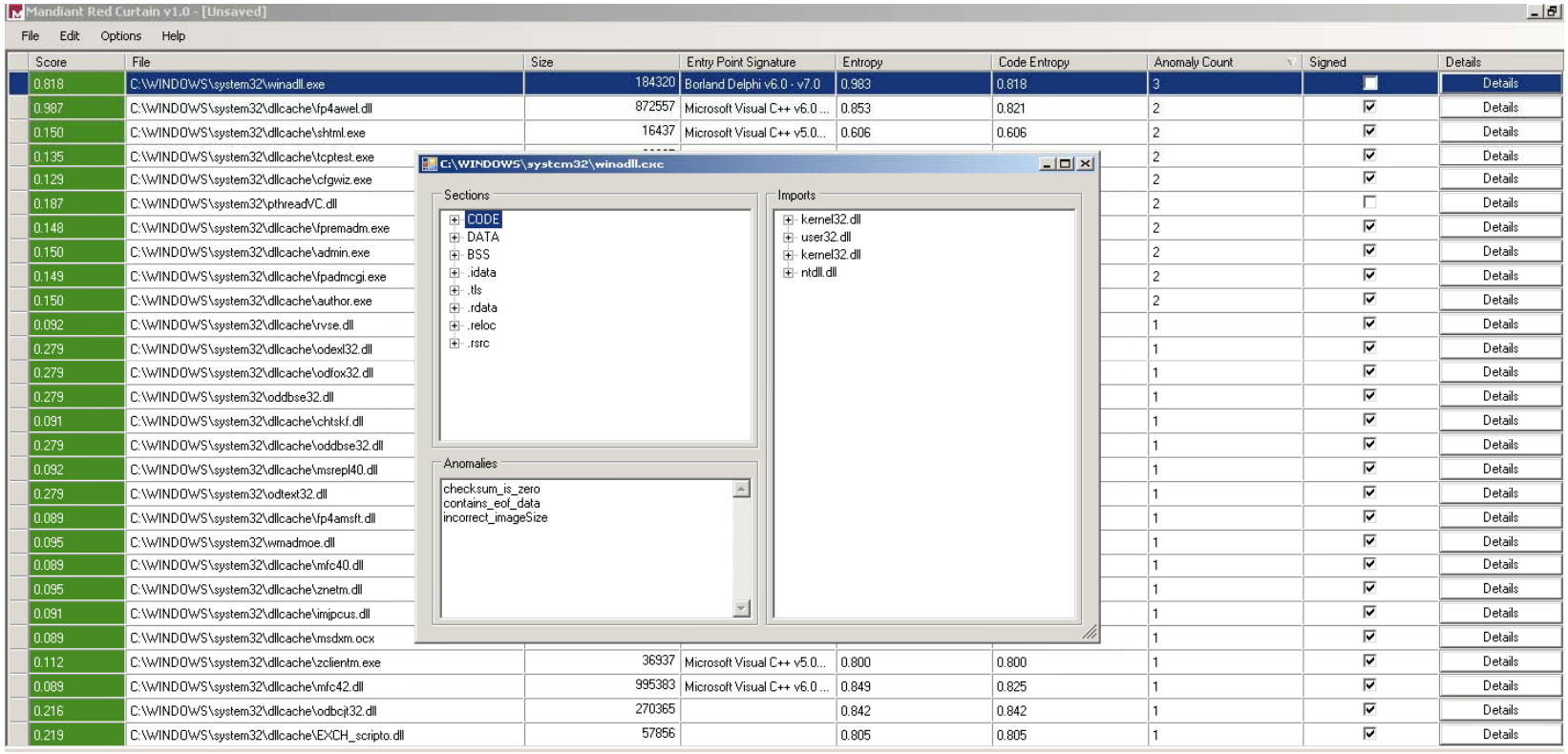
File Edit Options Help

Score	File	Size	Entry Point Signature	Entropy	Code Entropy	Anomaly Count	Signed	Details
4.025	c:\windows\wkssvc.exe	132216		0.982	0.982	1	☐	Details
3.256	c:\windows\system32\drivers\STEALTH4.sys	12960		0.993	0.993	0	☐	Details
3.256	c:\windows\system32\drivers\AES256.sys	18464		1.064	1.064	0	☐	Details
3.256	c:\windows\system32\drivers\RIJN256.sys	21856		1.064	1.064	0	☐	Details
3.256	c:\windows\system32\drivers\AES128.sys	18464		1.064	1.064	0	☐	Details
3.075	c:\windows\system32\dla\tfsndres.sys	2239		0.120	0.000	1	☐	Details
2.000	c:\windows\Installer\{90110409-6000-11D3-8CFE-0150048383C9}\wordicon.exe	286720		0.813	0.005	0	☐	Details
2.000	c:\windows\Installer\{90110409-6000-11D3-8CFE-0150048383C9}\unbndico.exe	23040		0.506	0.050	0	☐	Details
2.000	c:\windows\Installer\{90110409-6000-11D3-8CFE-0150048383C9}\pubs.exe	61440		0.804	0.005	0	☐	Details

- MRC doesn’t identify what the actual malware is (more later), but helps in sample gathering.

Mandiant Red Curtain (2)

Sometimes results aren't obvious:

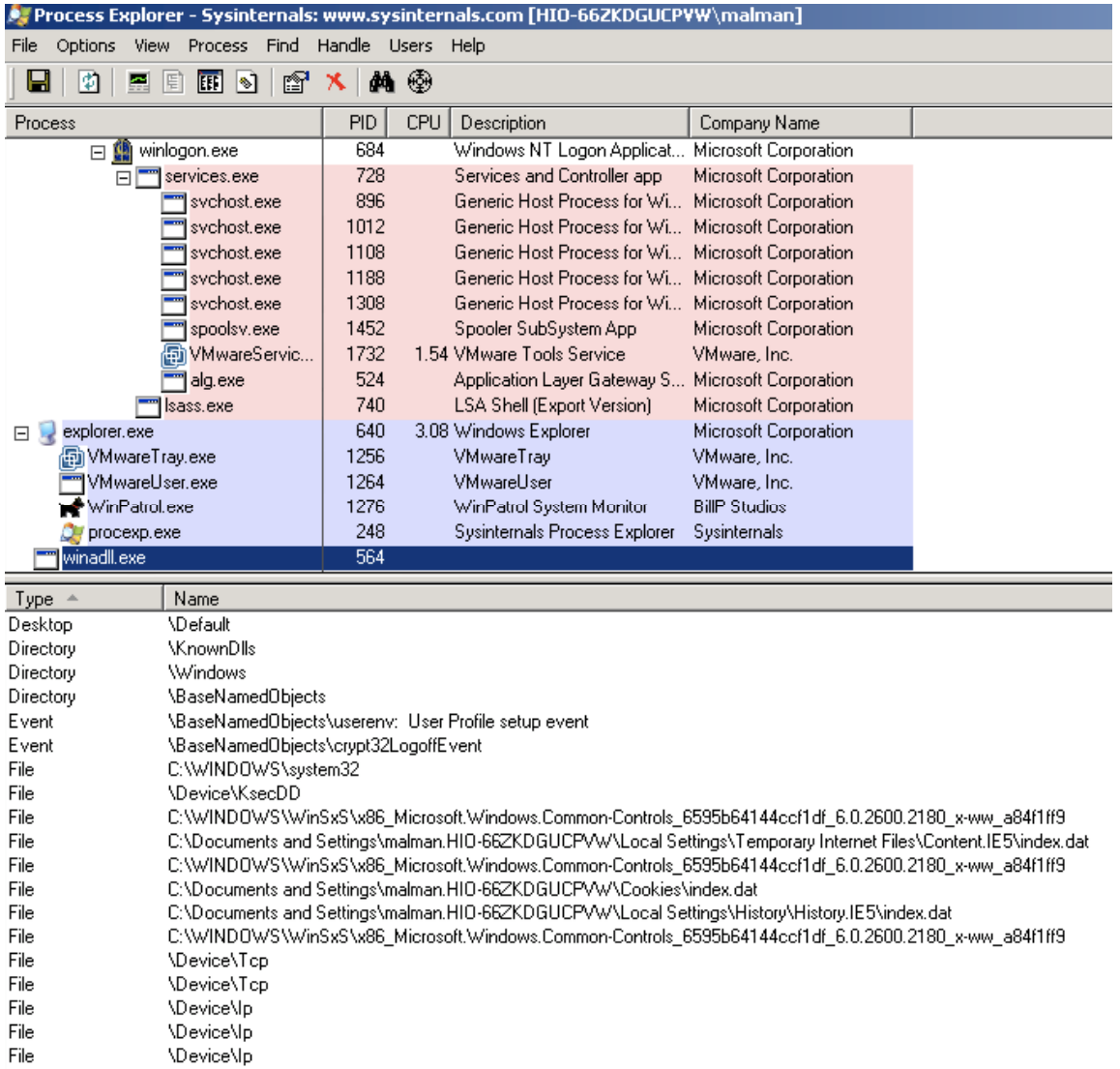


Score	File	Size	Entry Point Signature	Entropy	Code Entropy	Anomaly Count	Signed	Details
0.818	C:\WINDOWS\system32\winadll.exe	184320	Borland Delphi v6.0 - v7.0	0.983	0.818	3	☐	Details
0.987	C:\WINDOWS\system32\dllcache\fp4awel.dll	872557	Microsoft Visual C++ v6.0 ...	0.853	0.821	2	☑	Details
0.150	C:\WINDOWS\system32\dllcache\shtml.exe	16437	Microsoft Visual C++ v5.0...	0.606	0.606	2	☑	Details
0.135	C:\WINDOWS\system32\dllcache\tcptest.exe					2	☑	Details
0.129	C:\WINDOWS\system32\dllcache\cfgwiz.exe					2	☑	Details
0.187	C:\WINDOWS\system32\pthreadVC.dll					2	☐	Details
0.148	C:\WINDOWS\system32\dllcache\fpremadm.exe					2	☑	Details
0.150	C:\WINDOWS\system32\dllcache\admin.exe					2	☑	Details
0.149	C:\WINDOWS\system32\dllcache\fpadmcgi.exe					2	☑	Details
0.150	C:\WINDOWS\system32\dllcache\author.exe					2	☑	Details
0.092	C:\WINDOWS\system32\dllcache\rvse.dll					1	☑	Details
0.279	C:\WINDOWS\system32\dllcache\odexl32.dll					1	☑	Details
0.279	C:\WINDOWS\system32\dllcache\odfox32.dll					1	☑	Details
0.279	C:\WINDOWS\system32\oddbse32.dll					1	☑	Details
0.091	C:\WINDOWS\system32\dllcache\chtskf.dll					1	☑	Details
0.279	C:\WINDOWS\system32\dllcache\oddbse32.dll					1	☑	Details
0.092	C:\WINDOWS\system32\dllcache\msrepl40.dll					1	☑	Details
0.279	C:\WINDOWS\system32\odtext32.dll					1	☑	Details
0.089	C:\WINDOWS\system32\dllcache\fp4amsft.dll					1	☑	Details
0.095	C:\WINDOWS\system32\wmadmoe.dll					1	☑	Details
0.089	C:\WINDOWS\system32\dllcache\mfc40.dll					1	☑	Details
0.095	C:\WINDOWS\system32\dllcache\znetm.dll					1	☑	Details
0.091	C:\WINDOWS\system32\dllcache\imjpcus.dll					1	☑	Details
0.089	C:\WINDOWS\system32\dllcache\msdxm.ocx					1	☑	Details
0.112	C:\WINDOWS\system32\dllcache\zclientm.exe	36937	Microsoft Visual C++ v5.0...	0.800	0.800	1	☑	Details
0.089	C:\WINDOWS\system32\dllcache\mfc42.dll	995383	Microsoft Visual C++ v6.0 ...	0.849	0.825	1	☑	Details
0.216	C:\WINDOWS\system32\dllcache\odbcjt32.dll	270365		0.842	0.842	1	☑	Details
0.219	C:\WINDOWS\system32\dllcache\EXCH_scripto.dll	57856		0.805	0.805	1	☑	Details

Don't just look for the pretty red alert with a high score, look at entry point sigs and anomaly counts.

Process Explorer - Sysinternals

Running processes are noted via the Processes tab in Task Manager, but that won't provide unique feedback like file touches and device use.



RAPIER 3.2

- “RAPIER is a security tool built to facilitate first response procedures for incident handling. It is designed to acquire commonly requested information and samples during an information security event, incident, or investigation. RAPIER automates the entire process of data collection and delivers the results directly to the hands of a skilled security analyst.”
- Used by the authors at Intel, they wrote it to help them respond to incidents in the absence of a consolidated tool suite.

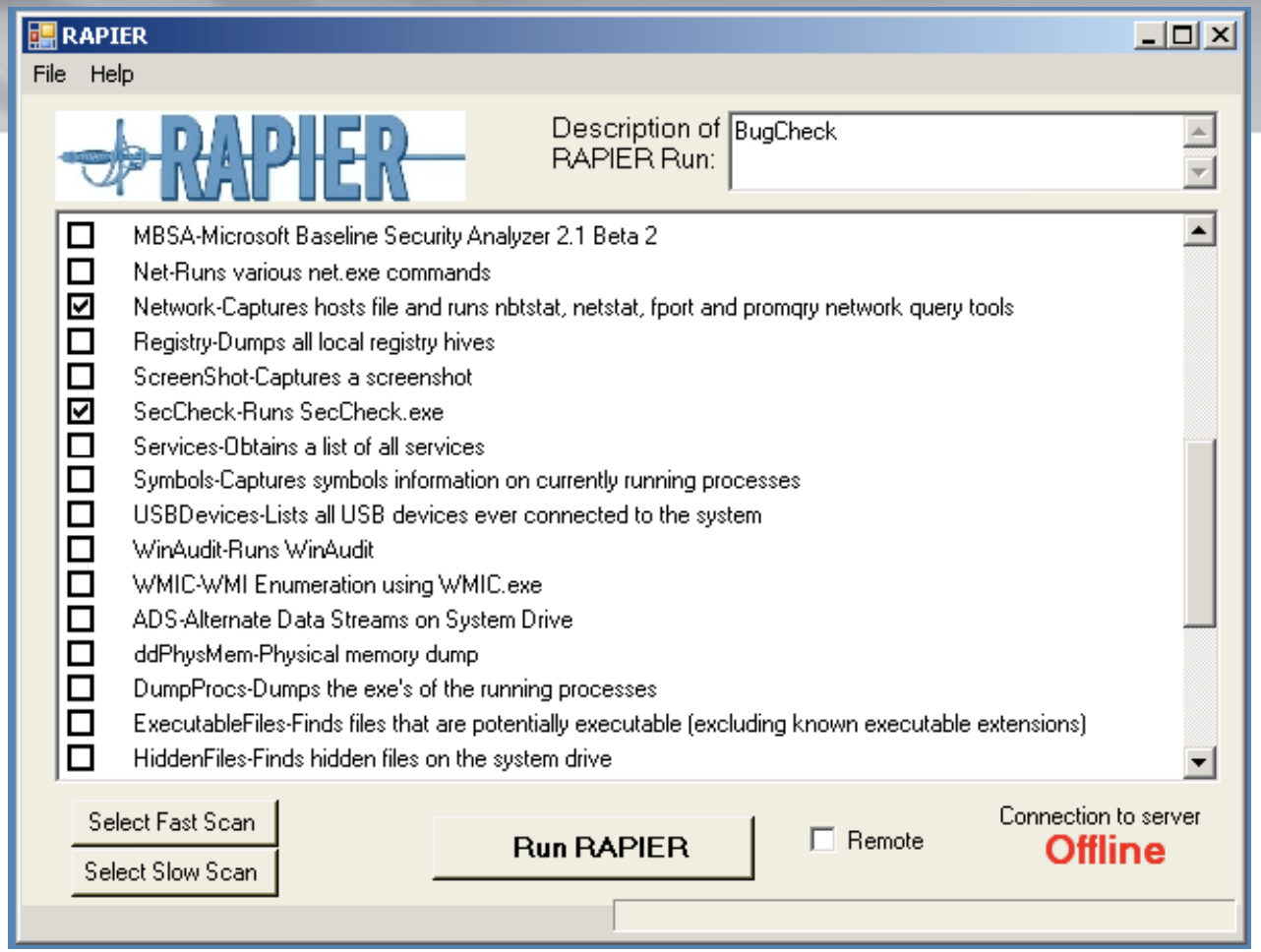
RAPIER 3.2 - Server

- Server acts as a central location for results to be uploaded to.
- When an analyst runs a RAPIER scan, an email is automatically sent out to the security analysts that look at the scans, with a list of included modules and other info, and a full path to the file just uploaded.
- Keeps the ClamAV, McAfee DAT and MBSA sigs up to date and in the current version.
- Acts as a central repository for everyone to download the tool from, can be setup as http://rapier.<your domain>.com on your Intranet.
- If any of the DAT files change, the download package is auto-updated on the site.

RAPIER 3.2 - Client

- RAPIER also works well as a standalone client.
- Can be run from a trusted resource (CD,USB) or run against a victim host remotely.
- Also .NET 2.0 framework dependent.

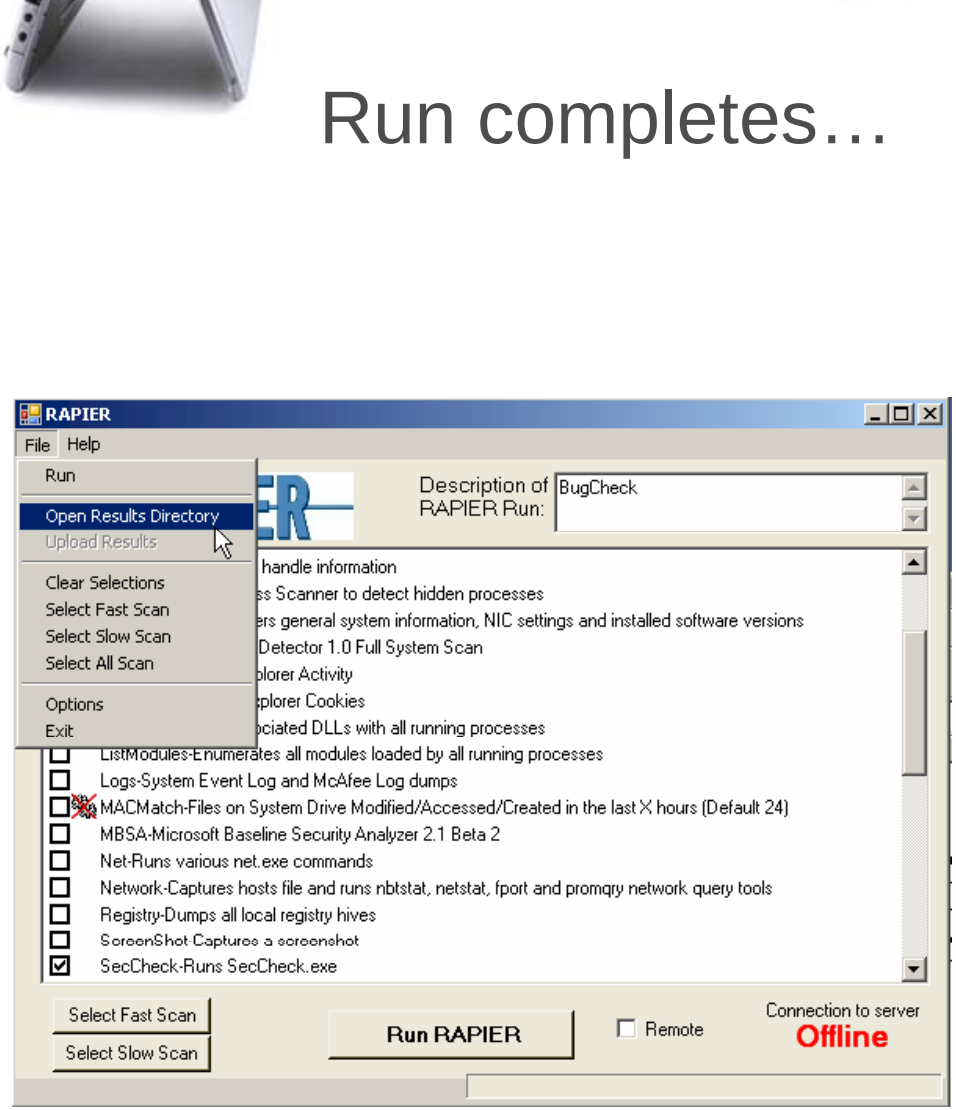
RAPIER 3.2 - Client

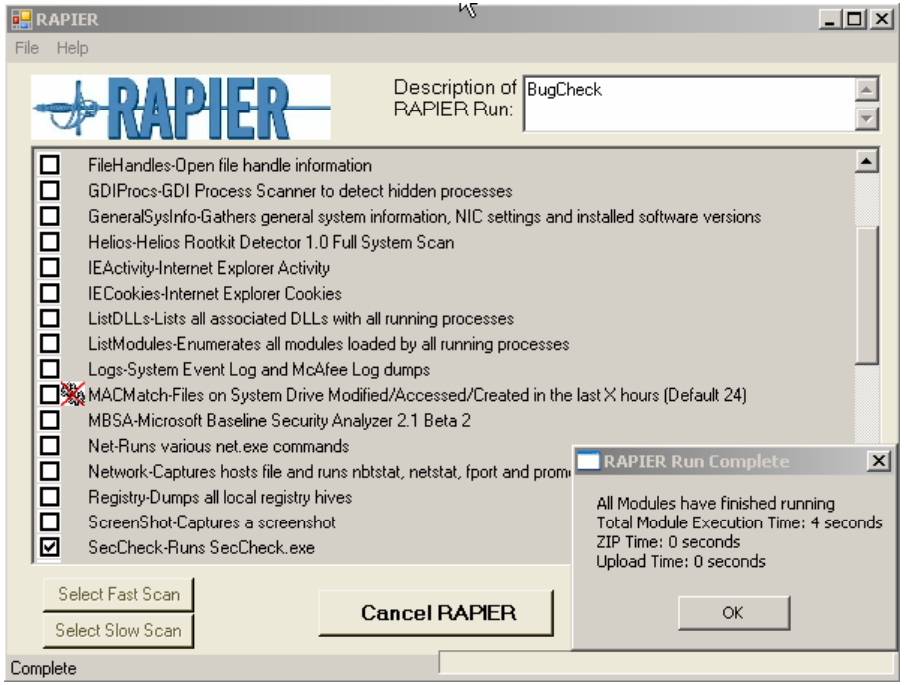


- Very simple interface, just select the modules you wish to run.
- If you only ever run two modules, be sure they are SecCheck from MyNetWatchman and the Network module.

RAPIER 3.2 - Client

Run completes…





…easy navigation to results.

RAPIER 3.2 - Client

Network module results - fport:

Network-fport.log - Notepad

File Edit Format View Help

```
================================================================================
LogFile Located at C:\tools\rapier\Results\HIO-66ZKDGUCPVW\2007-10-28\15-00\Network-fport.log
RAPIER Library Version=2005.06.06.01
System Name=HIO-66ZKDGUCPVW
Build Info=HIO SANDBOX
Processor(s) Quantity and Name=1xGenuine Intel(R) CPU           T2600  @ 2.16GHz
Module Name=Network
Description=Captures hosts file and runs nbtstat, netstat, fport and promqry network query tools
Execute Time=Sun 2007/10/28 15:02:04
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
908   svchost        ->  135   TCP   C:\WINDOWS\system32\svchost.exe
4     System         ->  139   TCP
4     System         ->  445   TCP
1056  svchost        ->  1025  TCP   C:\WINDOWS\System32\svchost.exe
4     System         ->  1030  TCP
1964  Explorer       ->  1798  TCP   C:\WINDOWS\Explorer.EXE
1964  Explorer       ->  1799  TCP   C:\WINDOWS\Explorer.EXE
820   winadll        ->  1813  TCP   C:\WINDOWS\System32\winadll.exe
1264                 ->  5000  TCP

0     System         ->  123   UDP
908   svchost        ->  135   UDP   C:\WINDOWS\system32\svchost.exe
0     System         ->  137   UDP
0     System         ->  138   UDP
4     System         ->  445   UDP
1056  svchost        ->  500   UDP   C:\WINDOWS\System32\svchost.exe
4     System         ->  1026  UDP
1964  Explorer       ->  1033  UDP   C:\WINDOWS\Explorer.EXE
1964  Explorer       ->  1397  UDP   C:\WINDOWS\Explorer.EXE
820   winadll        ->  1398  UDP   C:\WINDOWS\System32\winadll.exe
1264                 ->  1399  UDP
4     System         ->  1400  UDP
1964  Explorer       ->  1401  UDP   C:\WINDOWS\Explorer.EXE
1964  Explorer       ->  1417  UDP   C:\WINDOWS\Explorer.EXE
820   winadll        ->  1418  UDP   C:\WINDOWS\System32\winadll.exe
0     System         ->  1900  UDP


Execute Duration (in seconds)=1
```

RAPIER 3.2 - Client

SecCheck module results – Process List:

- Confirms what we saw in Process Explorer.

```
Process List:
        PID      4: System
        PID    176 [HIO-66ZKDGUCPVW\malman]: '"C:\WINDOWS\system32\cmd.exe" /c "start "" /D"C:\tools\rapier\Results\HIO-66ZKD
        PID    264 [HIO-66ZKDGUCPVW\malman]: '"C:\Program Files\VMware\VMware Tools\VMwareTray.exe" '
        PID    276 [HIO-66ZKDGUCPVW\malman]: '"C:\Program Files\VMware\VMware Tools\VMwareUser.exe" '
        PID    284 [HIO-66ZKDGUCPVW\malman]: '"C:\Program Files\BillP Studios\WinPatrol\winpatrol.exe" '
        PID    360 [HIO-66ZKDGUCPVW\malman]: 'cmd /c ""C:\tools\rapier\Modules\Fast\SecCheck\Module.cmd"  C:\tools\rapier\Res
        PID    532 [HIO-66ZKDGUCPVW\malman]: '"C:\tools\rapier\RAPIER.exe" '
        PID    544 [NT AUTHORITY\NETWORK SERVICE]: 'C:\WINDOWS\System32\wbem\wmiprvse.exe'
        PID    556 [NT AUTHORITY\SYSTEM]: '\SystemRoot\System32\smss.exe'
        PID    660 [NT AUTHORITY\SYSTEM]: 'C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512
        PID    684 [NT AUTHORITY\SYSTEM]: \??\C:\WINDOWS\system32\winlogon.exe
        PID    728 [NT AUTHORITY\SYSTEM]: 'C:\WINDOWS\system32\services.exe'
        PID    740 [NT AUTHORITY\SYSTEM]: 'C:\WINDOWS\system32\lsass.exe'
        PID    820 [HIO-66ZKDGUCPVW\malman]: 'C:\WINDOWS\System32\winadll.exe'
        PID    908 [NT AUTHORITY\SYSTEM]: 'C:\WINDOWS\system32\svchost -k rpcss'
        PID   1056 [NT AUTHORITY\SYSTEM]: 'C:\WINDOWS\System32\svchost.exe -k netsvcs'
        PID   1144 [HIO-66ZKDGUCPVW\malman]: 'cscript //nologo "C:\tools\rapier\Modules\Fast\SecCheck\Module.wsf" C:\tools\ra
        PID   1232 [NT AUTHORITY\NETWORK SERVICE]: 'C:\WINDOWS\System32\svchost.exe -k NetworkService'
        PID   1264 [NT AUTHORITY\LOCAL SERVICE]: 'C:\WINDOWS\System32\svchost.exe -k LocalService'
        PID   1364 [NT AUTHORITY\SYSTEM]: 'C:\WINDOWS\system32\spoolsv.exe'
        PID   1596 [NT AUTHORITY\SYSTEM]: '"C:\Program Files\VMware\VMware Tools\VMwareService.exe"'
        PID   1688 [BUILTIN\Administrators]: 'C:\WINDOWS\System32\wbem\wmiprvse.exe'
        PID   1900 [HIO-66ZKDGUCPVW\malman]: '"C:\tools\rapier\Modules\Fast\SecCheck\SecCheck.exe" '
        PID   1964 [HIO-66ZKDGUCPVW\malman]: 'C:\WINDOWS\Explorer.EXE'
        PID   1980 [HIO-66ZKDGUCPVW\malman]: '"C:\Program Files\Wisdom-soft AutoScreenRecorder\AutoScreenRecorder.exe" '
```

RAPIER 3.2 - Client

SecCheck module results – TCP/UDP and Run Entries:

SecCheck.log - Notepad

File Edit Format View Help

```
TCP table:
PID      908      0.0.0.0:135        LISTENING    (** Service **) C:\WINDOWS\system32\svchost.exe
PID        4      0.0.0.0:445        LISTENING    System
PID     1056      0.0.0.0:1025        LISTENING    (** Service **) C:\WINDOWS\System32\svchost.exe
PID        4      0.0.0.0:1030        LISTENING    System
PID     1964      0.0.0.0:1798        LISTENING    C:\WINDOWS\Explorer.EXE
PID     1964      0.0.0.0:1799        LISTENING    C:\WINDOWS\Explorer.EXE
PID      820      0.0.0.0:1813        LISTENING    C:\WINDOWS\System32\winadll.exe
PID     1264      0.0.0.0:5000        LISTENING    (** Service **) C:\WINDOWS\System32\svchost.exe
PID        4   192.168.101.129:139       LISTENING    System
PID     1964   192.168.101.129:1798   199.7.51.190:80    CLOSE_WAIT    C:\WINDOWS\Explorer.EXE
PID     1964   192.168.101.129:1799   199.7.51.190:80    CLOSE_WAIT    C:\WINDOWS\Explorer.EXE
PID      820   192.168.101.129:1813   121.22.36.74:65500    ESTABLISHED    C:\WINDOWS\System32\winadll.exe

UDP table:
PID      908      0.0.0.0:135    (** Service **) C:\WINDOWS\system32\svchost.exe
PID        4      0.0.0.0:445    System
PID      740      0.0.0.0:500    (** Service **) C:\WINDOWS\system32\lsass.exe
PID     1056      0.0.0.0:1026    (** Service **) C:\WINDOWS\System32\svchost.exe
PID     1232      0.0.0.0:1033    (** Service **) C:\WINDOWS\System32\svchost.exe
PID     1232      0.0.0.0:1397    (** Service **) C:\WINDOWS\System32\svchost.exe
PID     1232      0.0.0.0:1398    (** Service **) C:\WINDOWS\System32\svchost.exe
PID     1232      0.0.0.0:1399    (** Service **) C:\WINDOWS\System32\svchost.exe
PID     1232      0.0.0.0:1400    (** Service **) C:\WINDOWS\System32\svchost.exe
PID     1232      0.0.0.0:1401    (** Service **) C:\WINDOWS\System32\svchost.exe
PID     1232      0.0.0.0:1417    (** Service **) C:\WINDOWS\System32\svchost.exe
PID     1232      0.0.0.0:1418    (** Service **) C:\WINDOWS\System32\svchost.exe
PID     1056    127.0.0.1:123    (** Service **) C:\WINDOWS\System32\svchost.exe
PID     1264    127.0.0.1:1900    (** Service **) C:\WINDOWS\System32\svchost.exe
PID     1056   192.168.101.129:123    (** Service **) C:\WINDOWS\System32\svchost.exe
PID        4   192.168.101.129:137    System
PID        4   192.168.101.129:138    System
PID     1264   192.168.101.129:1900    (** Service **) C:\WINDOWS\System32\svchost.exe

Entries for HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run:
        'VMware Tools' = 'C:\Program Files\VMware\VMware Tools\VMwareTray.exe'
        'VMware User Process' = 'C:\Program Files\VMware\VMware Tools\VMwareUser.exe'
        'WinPatrol' = 'C:\Program Files\BillP Studios\WinPatrol\winpatrol.exe'
        'Display Device Driver' = 'winadll.exe'

Entries for HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce:

Entries for HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx:
```

Online Resources

- With our unwelcome visitor identified how can we quickly learn more?
- Online scanners are invaluable: Is it a new variant with little coverage, or is it easily identified, denoting a gap in the victim host's AV application.
- Be a good citizen, if coverage is light submit the sample directly to vendors.

Online Resources - Virustotal

VIRUS TOTAL

Virustotal is a **service that analyzes suspicious files** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

File **winadll.exe** received on **10.28.2007 22:05:31 (CET)**
Current status: **finished**
Result: **26/32 (81.25%)**

Compact | Print results

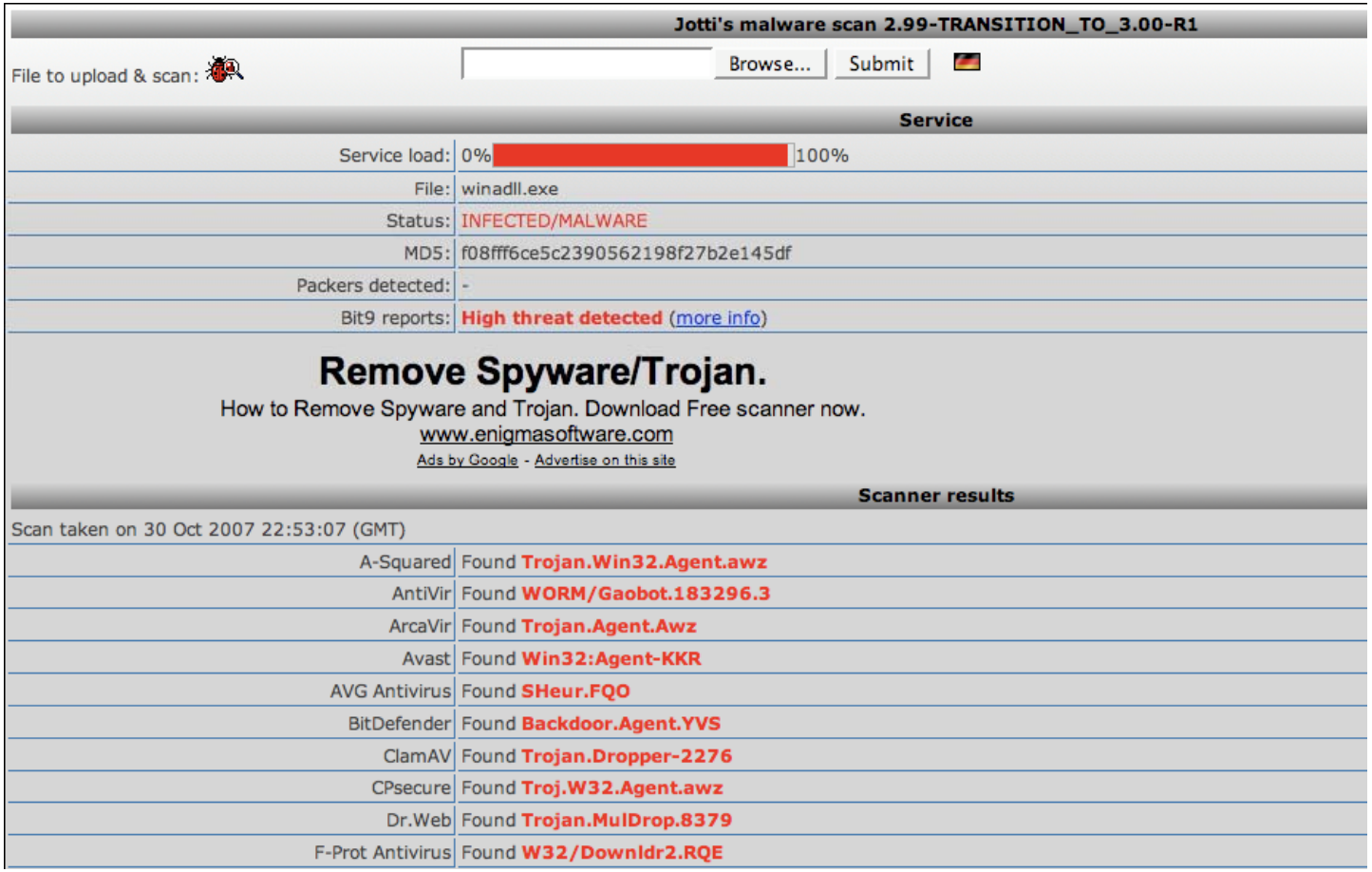
Antivirus	Version	Last Update	Result
AhnLab-V3	2007.10.27.0	2007.10.26	Win-Trojan/Agent.183296.F
AntiVir	7.6.0.30	2007.10.26	Worm/Gaobot.183296.3
Authentium	4.93.8	2007.10.28	W32/Trojan.BVZG
Avast	4.7.1074.0	2007.10.28	Win32:Agent-KKR
AVG	7.5.0.503	2007.10.28	SHeur.FQO
BitDefender	7.2	2007.10.28	Backdoor.Agent.YVS
CAT-QuickHeal	9.00	2007.10.26	Trojan.Agent.awz
ClamAV	0.91.2	2007.10.28	Trojan.Dropper-2276
DrWeb	4.44.0.09170	2007.10.28	Trojan.MulDrop.8379
eSafe	7.0.15.0	2007.10.28	-
eTrust-Vet	31.2.5244	2007.10.26	Win32/Rbot.HWL
Ewido	4.0	2007.10.28	-
FileAdvisor	1	2007.10.28	High threat detected
Fortinet	3.11.0.0	2007.10.19	W32/Agent.AWZ!tr
F-Prot	4.3.2.48	2007.10.26	W32/Trojan.BVZG

- Most analysts are likely familiar with this service. Samples submitted here are sent to vendors but often the feed is buried. Direct submittal to vendor is better.

http://www.virustotal.com

Online Resources - Jotti

- A good alternative to VirusTotal



Jotti's malware scan 2.99-TRANSITION_TO_3.00-R1

File to upload & scan: Browse... Submit

Service

Service load:	0% 100%
File:	winadll.exe
Status:	INFECTED/MALWARE
MD5:	f08fff6ce5c2390562198f27b2e145df
Packers detected:	-
Bit9 reports:	**High threat detected** (more info)

Remove Spyware/Trojan.
How to Remove Spyware and Trojan. Download Free scanner now.
www.enigmasoftware.com
Ads by Google - Advertise on this site

Scanner results

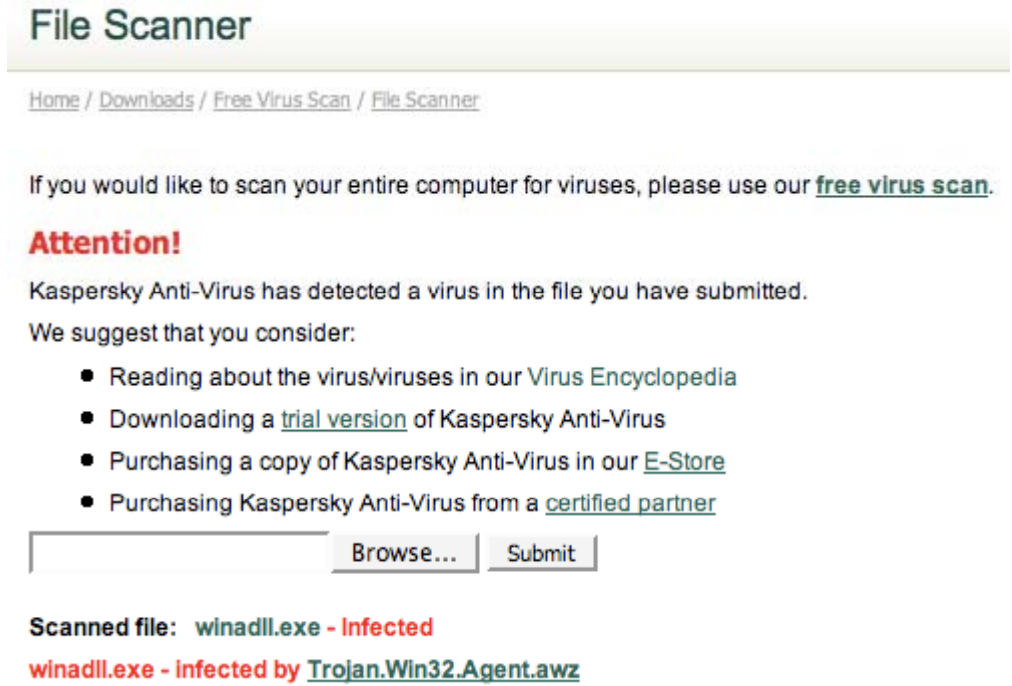
Scan taken on 30 Oct 2007 22:53:07 (GMT)

A-Squared	Found **Trojan.Win32.Agent.awz**
AntiVir	Found **WORM/Gaobot.183296.3**
ArcaVir	Found **Trojan.Agent.Awz**
Avast	Found **Win32:Agent-KKR**
AVG Antivirus	Found **SHeur.FQO**
BitDefender	Found **Backdoor.Agent.YVS**
ClamAV	Found **Trojan.Dropper-2276**
CPsecure	Found **Troj.W32.Agent.awz**
Dr.Web	Found **Trojan.MulDrop.8379**
F-Prot Antivirus	Found **W32/Downldr2.RQE**

http://virusscan.jotti.org/

Online Resources - Kaspersky

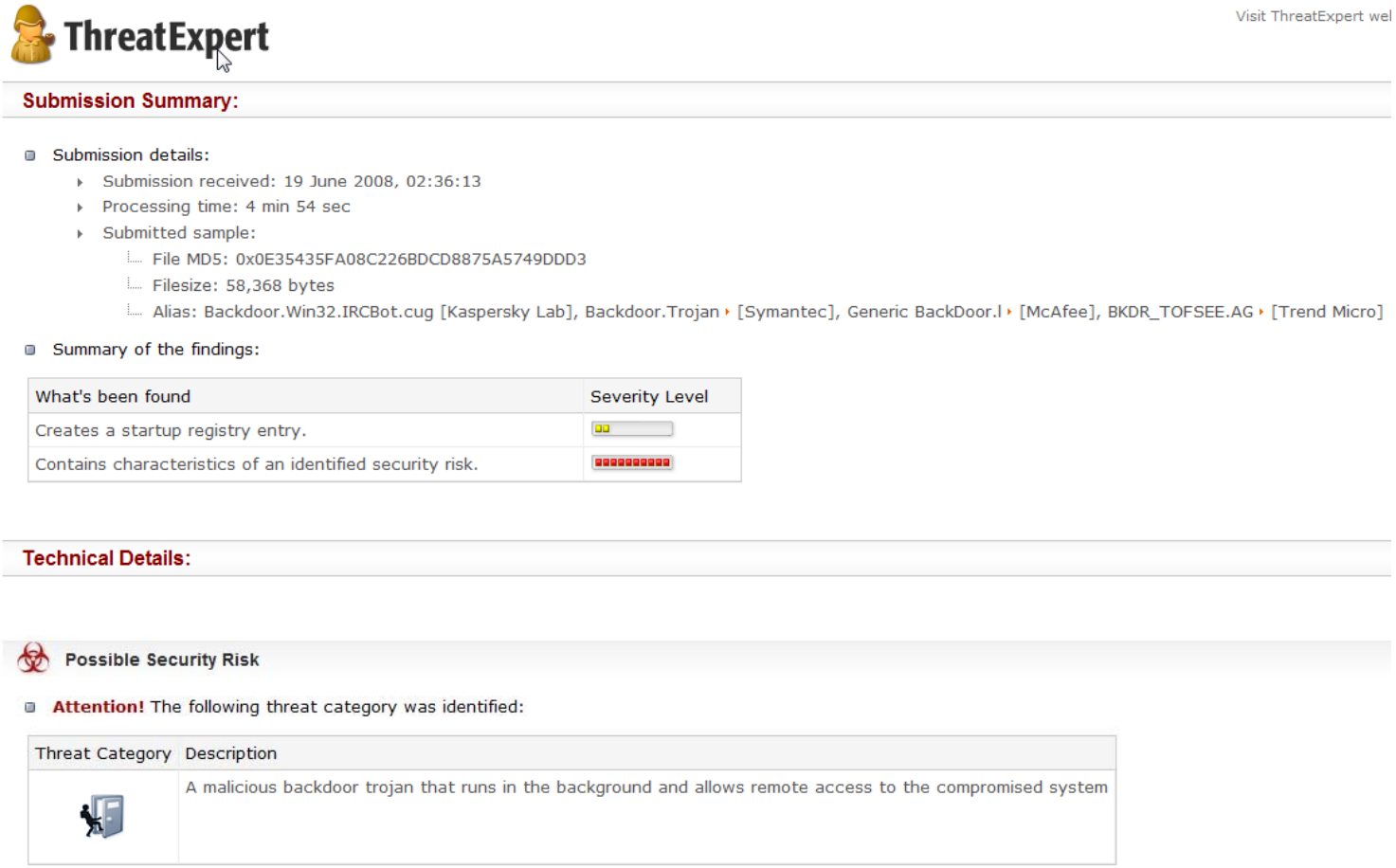
- If you just want a quick, single source ID, try Kaspersky.



http://www.kaspersky.com/scanforvirus

Online Resources - ThreatExpert

- Does a lot of the analysis work for you.



http://www.threatexpert.com

Online Resources - ThreatExpert

- File system mods, process changes.

File System Modifications

The following files were created in the system:

#	Filename(s)	File Size	File MD5	Alias
1	%UserProfile%\emtprx.exe %UserProfile%\jrjd.exe %System%\anhml.exe %System%\mvscv.exe	58,368 bytes	0x0E35435FA08C226BDCD8875A5749DDD3	Backdoor.Win32.IRCBot.cug [Kaspersky Lab]Backdoor.Trojan ‣ [Symantec]Generic BackDoor.l ‣ [McAfee]BKDR_TOFSEE.AG ‣ [Trend Micro]
2	%Temp%\removeMe8753.bat	143 bytes	0x03F371BF38AFBFC67ECE3E884314B869	(not available)

Notes:

- %UserProfile% is a variable that specifies the current user's profile folder. By default, this is C:\Documents and Settings\[UserName] (Windows NT/2000/XP).
- %System% is a variable that refers to the System folder. By default, this is C:\Windows\System (Windows 95/98/Me), C:\Winnt\System32 (Windows NT/2000), or C:\Windows\System32 (Windows XP).
- %Temp% is a variable that refers to the temporary folder in the short path form. By default, this is C:\Documents and Settings\[UserName]\Local Settings\Temp\ (Windows NT/2000/XP).

Memory Modifications

There were new processes created in the system:

Process Name	Process Filename	Main Module Size
anhml.exe	%System%\anhml.exe	184,320 bytes
mvscv.exe	%System%\mvscv.exe	184,320 bytes
[filename of the sample #1]	[file and pathname of the sample #1]	184,320 bytes

http://www.threatexpert.com

Online Resources - ThreatExpert

- Registry changes, Mutex, & ports

Registry Modifications

- The following Registry Keys were created:
  - HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\InformationBar
  - HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms
- The newly created Registry Values are:
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\BitBucket]
    - Inner = 0x00000016
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
    - mvscv = "%System%\mvscv.exe \u"

    so that mvscv.exe runs every time Windows starts
  - [HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\InformationBar]
    - FirstTime = 0x00000000
  - [HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms]
    - AskUser = 0x00000000
  - [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings]
    - WarnOnZoneCrossing = 0x00000000
    - WarnOnPostRedirect = 0x00000000
    - WarnonBadCertRecving = 0x00000000
- The following Registry Values were modified:
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
    - Userinit = "%System%\userinit.exe,%UserProfile%\jrjd.exe \s"

    so that jrjd.exe runs every time Windows starts
  - [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings]
    - WarnOnPost = 00 00 00 00
  - [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2]
    - MinLevel = 0x00000000
    - RecommendedLevel = 0x00000000
    - 1004 = 0x00000000
    - 1201 = 0x00000000
    - 1609 = 0x00000000

Other details

- To mark the presence in the system, the following Mutex object was created:
  - ghegdjf
- The following ports were open in the system:

Port	Protocol	Process
1040	UDP	mvscv.exe (%System%\mvscv.exe)
1042	UDP	anhml.exe (%System%\anhml.exe)

http://www.threatexpert.com

ANALYSIS PHASE

Who’s Waldo?

Analysis cautions

- Sandbox the analysis phase!
- Obviously, avoid your corporate network.
- VMWare is great only if the malware isn’t virtualization-aware (becoming a prevalent issue).
- My host OS in typically Linux or Mac OS X, and I run Windows as a guest OS.

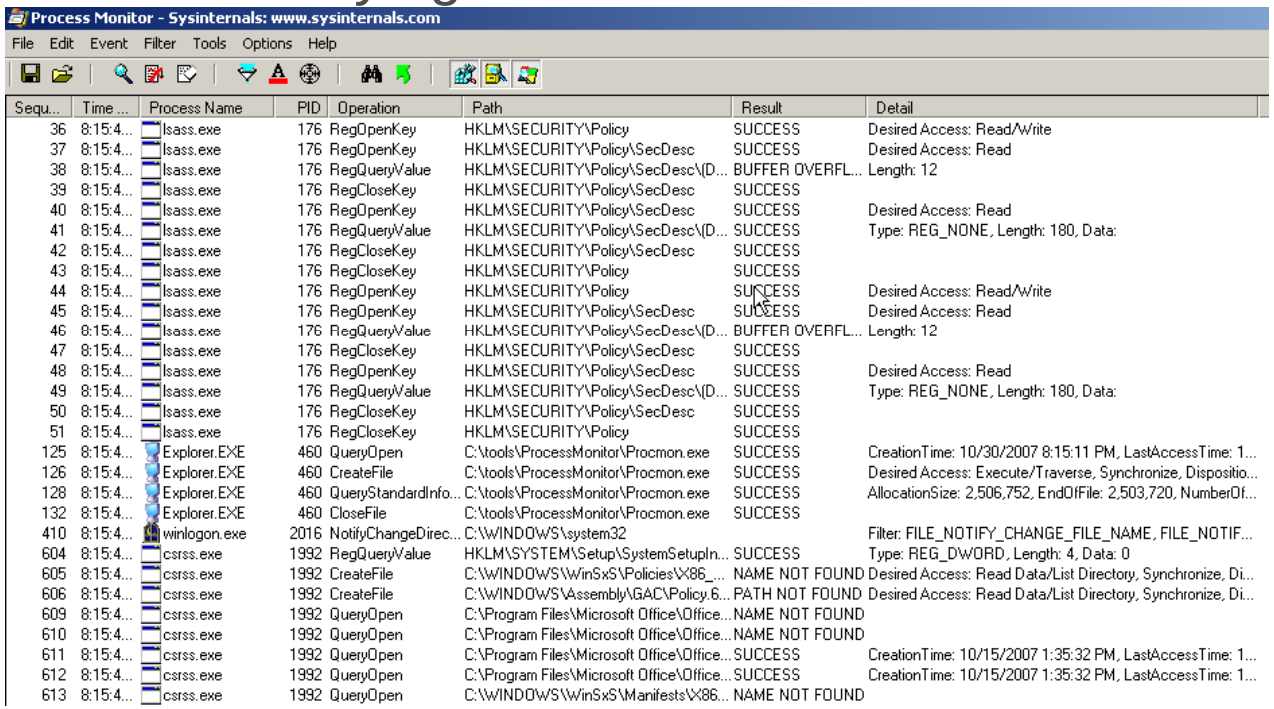
Analysis virtualization alternatives

- Options other than VMWare, et al, to avoid virtualization-detecting malware issues:
  - Joe Stewart's Truman (free, not for the timid or easily deterred as it unsupported and version 0.1)
  - Faronics Deep Freeze (commercial)
  - Windows SteadyState (free, XP & Vista)
  - Returnil Virtual System 2008 Personal Edition v2.0 (free)
  - CoreRestore (hardware) – very interesting project: "redirects system changes to a "temporary working area," allowing the administrator to revert to a pristine state via a reboot.

http://isc.sans.org/diary.html?storyid=4147&rss

Process Monitor - Sysinternals

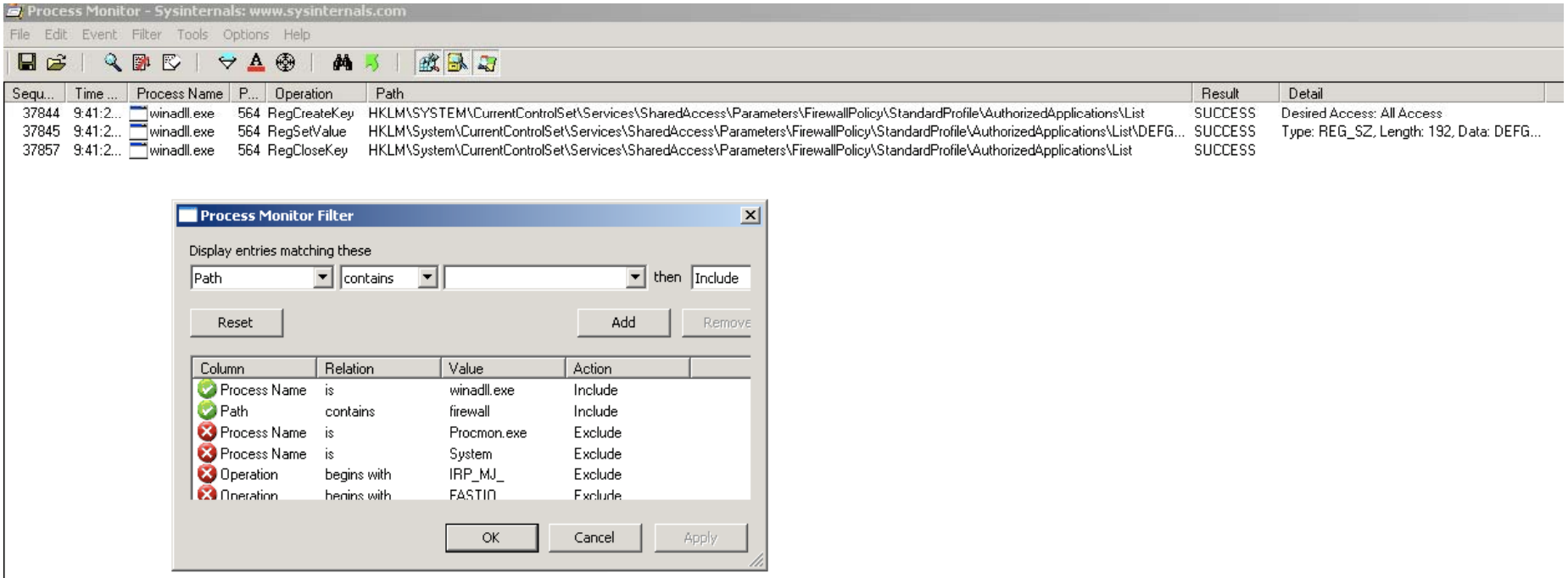
- Process Monitor makes use of Filemon and Regmon functionality, but adds major feature enhancements such as filtering, search, logging, and capture.
- Can be somewhat daunting without filtering…TMI (every process).
- Great for identifying behavioral attributes.



Sequ...	Time ...	Process Name	PID	Operation	Path	Result	Detail
36	8:15:4...	lsass.exe	176	RegOpenKey	HKLM\SECURITY\Policy	SUCCESS	Desired Access: Read/Write
37	8:15:4...	lsass.exe	176	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: Read
38	8:15:4...	lsass.exe	176	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\(D...	BUFFER OVERFL...	Length: 12
39	8:15:4...	lsass.exe	176	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
40	8:15:4...	lsass.exe	176	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: Read
41	8:15:4...	lsass.exe	176	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\(D...	SUCCESS	Type: REG_NONE, Length: 180, Data:
42	8:15:4...	lsass.exe	176	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
43	8:15:4...	lsass.exe	176	RegCloseKey	HKLM\SECURITY\Policy	SUCCESS	
44	8:15:4...	lsass.exe	176	RegOpenKey	HKLM\SECURITY\Policy	SUCCESS	Desired Access: Read/Write
45	8:15:4...	lsass.exe	176	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: Read
46	8:15:4...	lsass.exe	176	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\(D...	BUFFER OVERFL...	Length: 12
47	8:15:4...	lsass.exe	176	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
48	8:15:4...	lsass.exe	176	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: Read
49	8:15:4...	lsass.exe	176	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\(D...	SUCCESS	Type: REG_NONE, Length: 180, Data:
50	8:15:4...	lsass.exe	176	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
51	8:15:4...	lsass.exe	176	RegCloseKey	HKLM\SECURITY\Policy	SUCCESS	
125	8:15:4...	Explorer.EXE	460	QueryOpen	C:\tools\ProcessMonitor\Procmon.exe	SUCCESS	CreationTime: 10/30/2007 8:15:11 PM, LastAccessTime: 1...
126	8:15:4...	Explorer.EXE	460	CreateFile	C:\tools\ProcessMonitor\Procmon.exe	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Dispositio...
128	8:15:4...	Explorer.EXE	460	QueryStandardInfo...	C:\tools\ProcessMonitor\Procmon.exe	SUCCESS	AllocationSize: 2,506,752, EndOfFile: 2,503,720, NumberOf...
132	8:15:4...	Explorer.EXE	460	CloseFile	C:\tools\ProcessMonitor\Procmon.exe	SUCCESS	
410	8:15:4...	winlogon.exe	2016	NotifyChangeDirec...	C:\WINDOWS\system32		Filter: FILE_NOTIFY_CHANGE_FILE_NAME, FILE_NOTIF...
604	8:15:4...	csrss.exe	1992	RegQueryValue	HKLM\SYSTEM\Setup\SystemSetupIn...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
605	8:15:4...	csrss.exe	1992	CreateFile	C:\WINDOWS\WinSxS\Policies\X86_...	NAME NOT FOUND	Desired Access: Read Data/List Directory, Synchronize, Di...
606	8:15:4...	csrss.exe	1992	CreateFile	C:\WINDOWS\Assembly\GAC\Policy.6...	PATH NOT FOUND	Desired Access: Read Data/List Directory, Synchronize, Di...
609	8:15:4...	csrss.exe	1992	QueryOpen	C:\Program Files\Microsoft Office\Office...	NAME NOT FOUND	
610	8:15:4...	csrss.exe	1992	QueryOpen	C:\Program Files\Microsoft Office\Office...	NAME NOT FOUND	
611	8:15:4...	csrss.exe	1992	QueryOpen	C:\Program Files\Microsoft Office\Office...	SUCCESS	CreationTime: 10/15/2007 1:35:32 PM, LastAccessTime: 1...
612	8:15:4...	csrss.exe	1992	QueryOpen	C:\Program Files\Microsoft Office\Office...	SUCCESS	CreationTime: 10/15/2007 1:35:32 PM, LastAccessTime: 1...
613	8:15:4...	csrss.exe	1992	QueryOpen	C:\WINDOWS\WinSxS\Manifests\X86...	NAME NOT FOUND	

Process Monitor - Sysinternals

- Add a bit of filtering and zero in on the information you seek.



Malcode Analysis Software Tools – iDefense Labs

- iDefense Labs offers some excellent tools for use in your sandbox.
  - **SysAnalyzer**
    - Apilogger
  - **Malcode Analysis Pack**
    - Shell extensions
    - Mailpot – mail server capture port
    - fakeDNS – Spoofs responses
    - Sniff Hit – HTTP, IRC, DNS sniffer

Malcode Analysis Software Tools – iDefense Labs

- SysAnalyzer – very straightforward usage.
- The resulting reports are very comprehensive.

Malcode Analysis Software Tools – iDefense Labs

```
Monitored RegKeys
Registry Key    Value
-------------------------------------------------
File: winadll.exe
Size: 184320 Bytes
MD5: F08FFF6CE5C2390562198F27B2E145DF
Packer: File not found C:\iDEFENSE\SysAnalyzer\peid.exe

File Properties: CompanyName
FileDescription
FileVersion
InternalName
LegalCopyright
OriginalFilename
ProductName
ProductVersion

Exploit Signatures:
-------------------------------------------------------------------------------
Scanning for 19 signatures
*** Found: RPC DCOM Exploit MS03-026
*** Found: LSASS exploit - MS04-011
*** Found: Spreads Via Weak Passwords in MSSQL Server
*** Found: CA License Client Overflow v1.61
Scan Complete: 1196Kb in 0.062 seconds
Urls
-------------------------------------------------
http:/
iroffer v1.3b10 [D&P 23874155], http://iroffer.org/

RegKeys
-------------------------------------------------
Software\BioWare\NWN\Neverwinter
Software\Activision\Soldier of Fortune II - Double Helix
Software\Illusion Softworks\Hidden & Dangerous 2
Software\Techland\Chrome
Software\Westwood\NOX
Software\Westwood\Red Alert 2
Software\Westwood\Red Alert
Software\Westwood\Tiberian Sun
Software\Red Storm Entertainment\RAVENSHIELD
Software\Electronic Arts\EA Sports\Nascar Racing 2003\ergc
Software\Electronic Arts\EA Sports\Nascar Racing 2002\ergc
Software\Electronic Arts\EA Sports\NHL 2003\ergc
Software\Electronic Arts\EA Sports\NHL 2002\ergc
Software\Electronic Arts\EA Sports\FIFA 2003\ergc
Software\Electronic Arts\EA Sports\FIFA 2002\ergc
Software\Electronic Arts\EA GAMES\Shogun Total War - Warlord Edition\ergc
Software\Electronic Arts\EA GAMES\Need For Speed Underground\ergc
Software\Electronic Arts\EA GAMES\Need For Speed Hot Pursuit 2
Software\Electronic Arts\EA GAMES\Medal of Honor Allied Assault Spearhead\ergc
Software\Electronic Arts\EA GAMES\Medal of Honor Allied Assault Breakthrough\ergc
Software\Electronic Arts\EA GAMES\Medal of Honor Allied Assault\ergc
Software\Electronic Arts\EA GAMES\Global Operations\ergc
```

- Report findings
- Multiple exploit payload
- Send me your game keys!

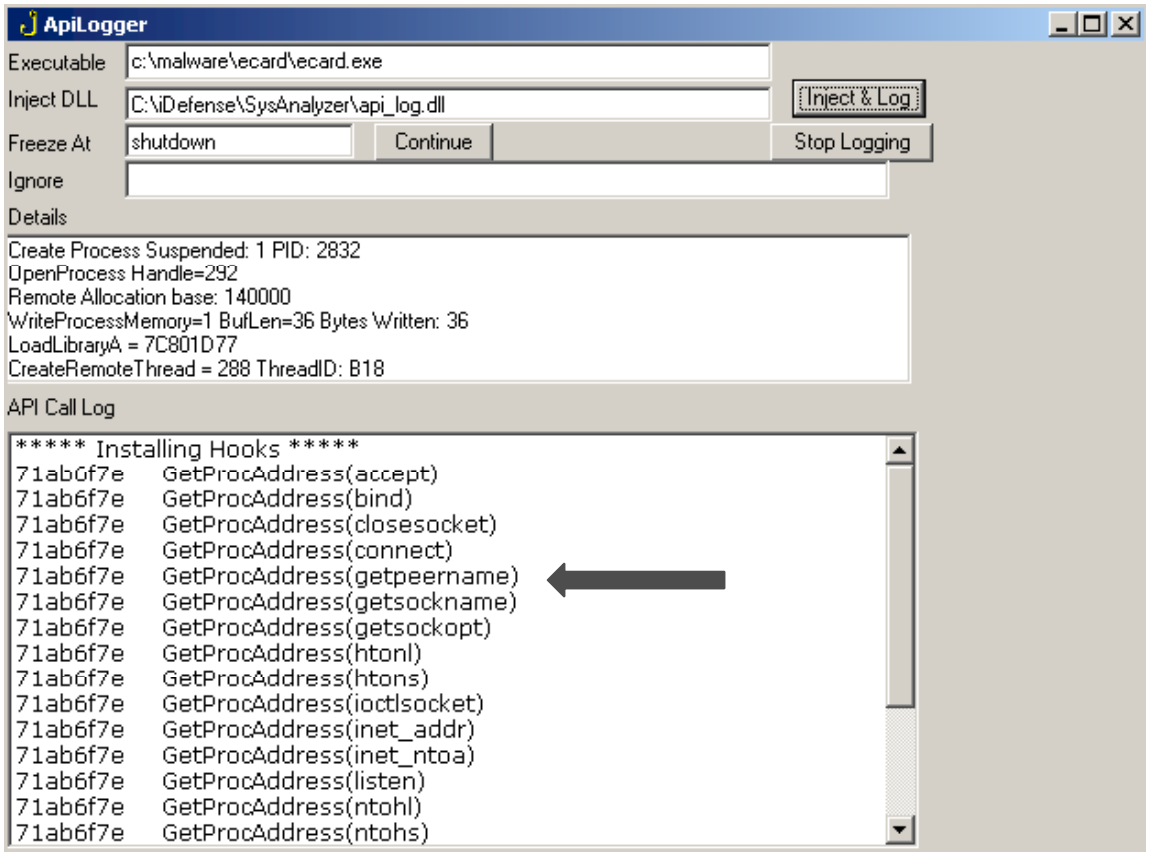
Malcode Analysis Software Tools – iDefense Labs

```
ExeRefs
-------------------------------------------------
File: winadll_dmp.exe_
WinXP Professional    [universal] lsass.exe
SOFTWARE\Clients\StartMenuInternet\firefox.exe\shell\open\command
explorer.exe
cmd.exe
winadll.exe
winadll.exe
ftp.exe
com.execute
%s%s.exe
i11r54n4.exe
irun4.exe
d3dupdate.exe
rate.exe
ssate.exe
winsys.exe
winupd.exe
SysMonXP.exe
bbeagle.exe
Penis32.exe
mscvb32.exe
sysinfo.exe
PandaAVEngine.exe
F-AGOBOT.EXE
HIJACKTHIS.EXE
_AVPM.EXE
_AVPCC.EXE
_AVP32.EXE
ZONEALARM.EXE
ZONALM2601.EXE
ZATUTOR.EXE
ZAPSETUP3001.EXE
ZAPRO.EXE
XPF202EN.EXE
WYVERNWORKSFIREWALL.EXE
WUPDT.EXE
WUPDATER.EXE
WSBGATE.EXE
WRCTRL.EXE
WRADMIN.EXE
WNT.EXE
WNAD.EXE
```

- Report findings (2)

Hook, line, and sinker…

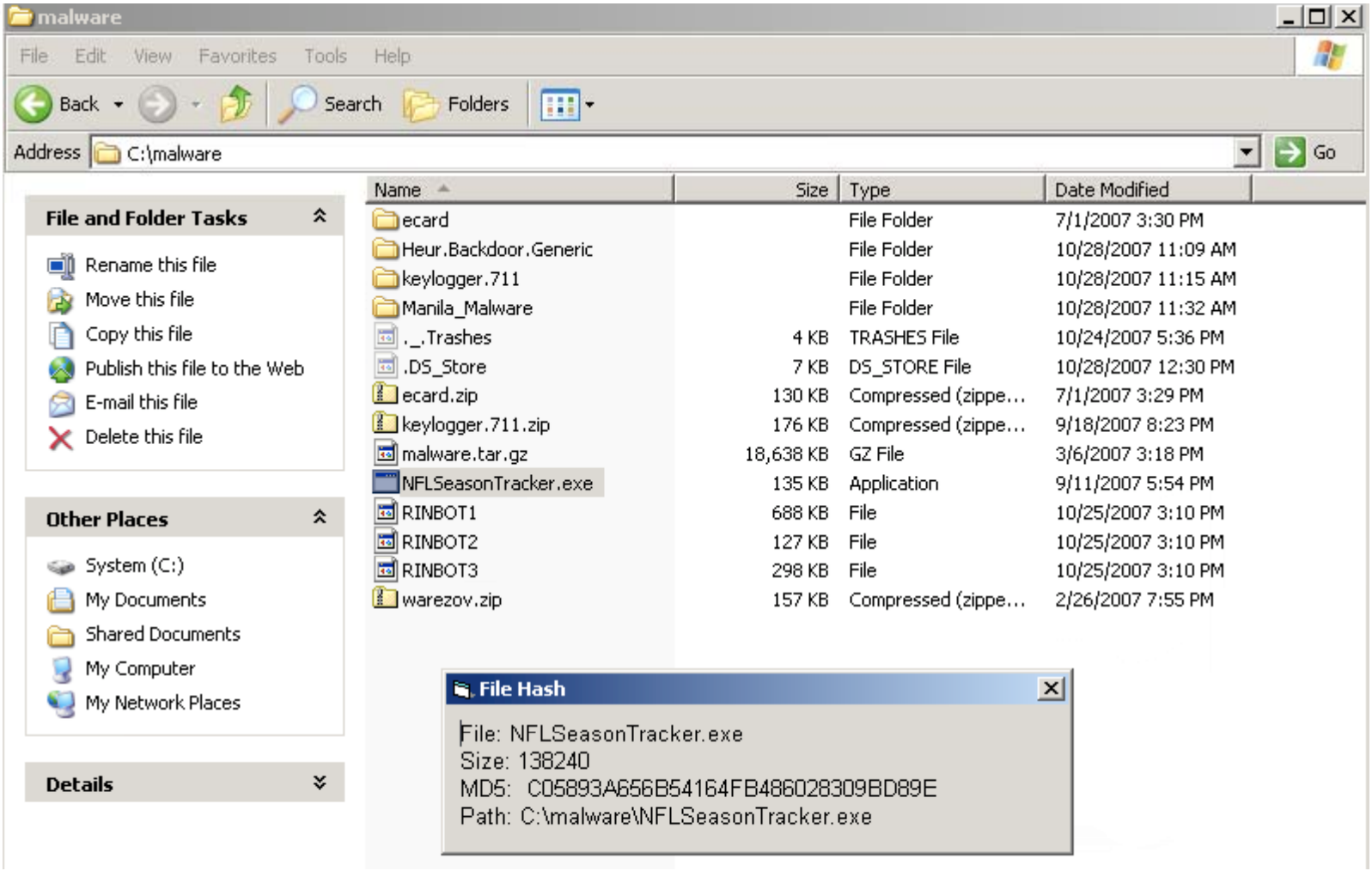
- Apilogger injects a dll into the target process & inserts a series of detour-style hooks into specific api calls. When these APIs are accessed by any code in the process, they will trigger a notification message which is sent to the SysAnalyzer interface.



- Hmm…am I a P2P Storm bot variant? I do believe…

Malcode Analysis Software Tools
iDefense Labs

- The value of hashing



Malcode Analysis Software Tools
iDefense Labs

- Take the resulting MD5 output and search for it.

Google C05893A656B54164FB486028309BD89E Search Advanced Search Preferences

Web

DISOG
They are sticking with the static MD5 sum of **c05893a656b54164fb486028309bd89e**. Most of the major Antivirus vendors are aware of the file: ...
www.disog.org/labels/CME-711.html - 77k - Cached - Similar pages

Known CME-711/STORMWORM Malware MD5's. For more information, visit ...
Known CME-711/STORMWORM Malware MD5's. For more information, visit the Digital Intelligence and Strategic Operations Group at http://www.disog.org ...
www.disog.org/text/stormworm-md5.txt - 250k - Cached - Similar pages
[More results from www.disog.org]

CastleCops® eCard Malware
MD5 Fingerprint: **c05893a656b54164fb486028309bd89e** SHA1 Fingerprint: 8ad506547710d61a6ac0613fdb1d290911f8e600. HTTP/1.1 200 OK Date: Sun, ...
www.castlecops.com/eCard_malware2641.html - Similar pages

Malcode Analysis Software Tools
iDefense Labs

Malcode Analysis Pack - Strings

- **Strings – can offer a ton of information.**
- **What functionality do we see here?**

```
Ascii Strings:
--------------------------------------------------------------------------------
!This program cannot be run in DOS mode.
Rich\
.text
`.rdata
@.data

KERNEL32.dll
t (ddos.m
  Done with flood (%iKB/sec).
t (ddos.m
  Send error: <%d>.
ddos.random
ddos.ack
ddos.syn
t (icmp.m
  Done with %s flood to IP: %s. Sent: %d packet(s) @ %dKB/sec (%dMB).
t (icmp.m
  Error sending packets to IP: %s. Packets sent: %d. Returned: <%d>.
t (icmp.m
  Invalid target IP.
t (icmp.m
  Error: setsockopt() failed, returned: <%d>.
t (icmp.m
  Error: socket() failed, returned: <%d>.
[SUPERSYN]: Done with flood (%iKB/sec)
t (syn.m
  Done with flood (%iKB/sec).
t (syn.m
  Send error: <%d>.
t (tcp.m
  Done with %s flood to IP: %s. Sent: %d packet(s) @ %dKB/sec (%dMB).
t (tcp.m
  Error sending packets to IP: %s. Packets sent: %d. Returned: <%d>.
random
t (tcp.m
  Invalid target IP.
t (tcp.m
  Error: setsockopt() failed, returned: <%d>.
t (tcp.m
  Error: socket() failed, returned: <%d>.
e-gold
PayPal
StormPay
Vodafone
Poste Italiane
eBay
Yahoo!
Banca Sella
Email
Bank Of America
exploit
Benvenuto a gmail
```

Malcode Analysis Software Tools – iDefense Labs

Malcode Analysis Pack – Strings (2)

- **What functionality do we see here?**

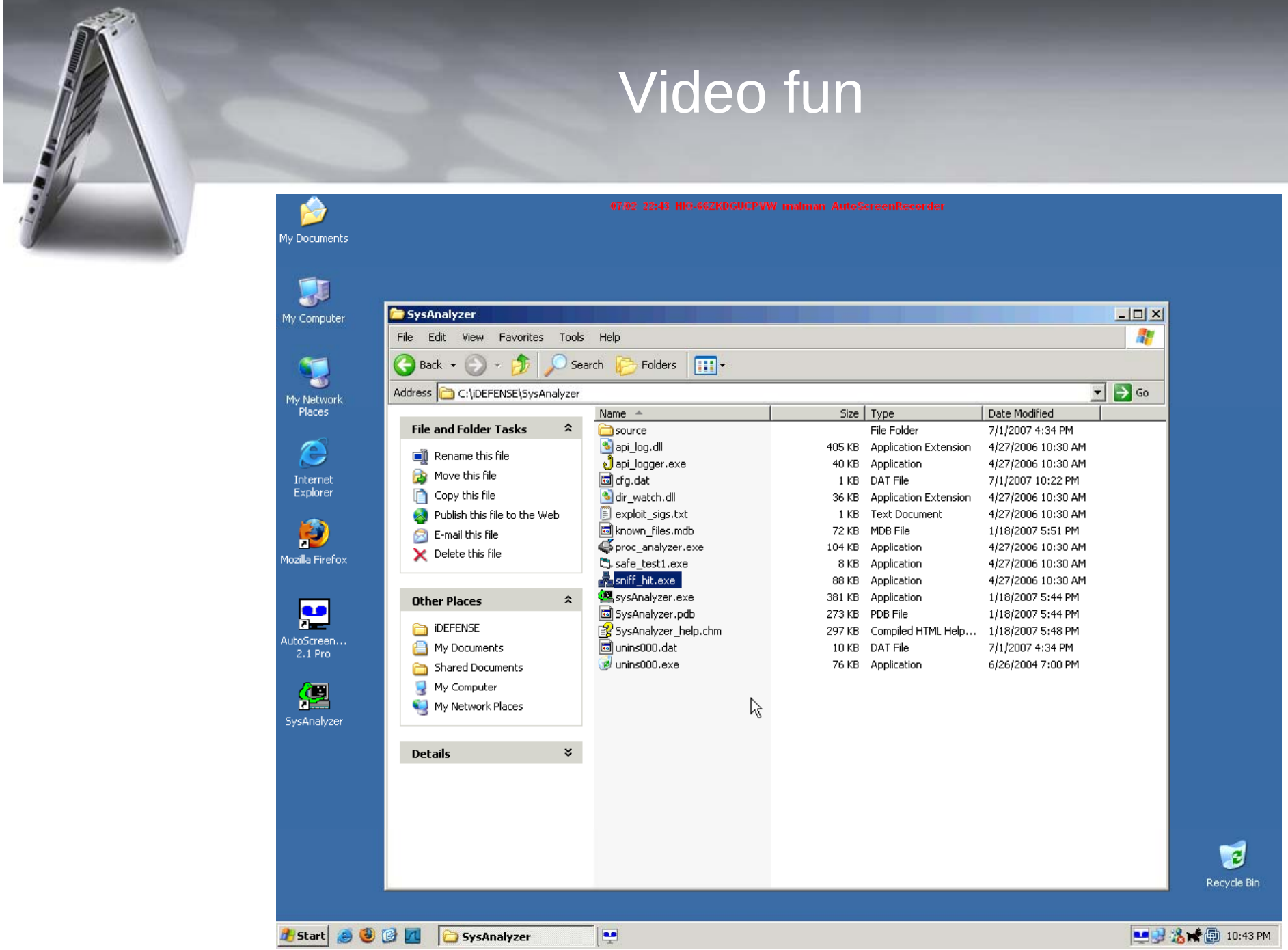
```
VNC%d.%d %s: %s - [AuthBypass]
RFB %03d.%03d
exit
tftp -i %s GET %s
RFB 003.008
221 Goodbye happy r00ting.
QUIT
425 Can't open data connection.
t (ftpd.m
  %s, port:%d now executing %s on remote machine.
226 Transfer complete.
150 Opening BINARY mode data connection
RETR
200 PORT command successful.
%s.%s.%s.%s
%x%x
%*s %[^,],%[^,],%[^,],%[^,],%[^,],%[^
PORT
226 Transfer complete
LIST
425 Passive not supported on this server
PASV
200 Type set to I.
200 Type set to A.
TYPE
257 "/" is current directory.
350 Restarting.
REST
215 NzmxFtpd
SYST
230 User logged in.
PASS
331 Password required
USER
%s %s
220 NzmxFtpd 0wns j0
t (httpd.m
  Error: server failed, returned: <%d>.
GET
HTTP/1.0 200 OK
Server: myBot
Cache-Control: no-cache,no-store,max-age=0
pragma: no-cache
Content-Type: %s
Content-Length: %i
Accept-Ranges: bytes
Date: %s %s GMT
Last-Modified: %s %s GMT
Expires: %s %s GMT
Connection: close
HTTP/1.0 200 OK
Server: myBot
```

Malcode Analysis Software Tools
iDefense Labs

Malcode Analysis Pack – Sniff Hit

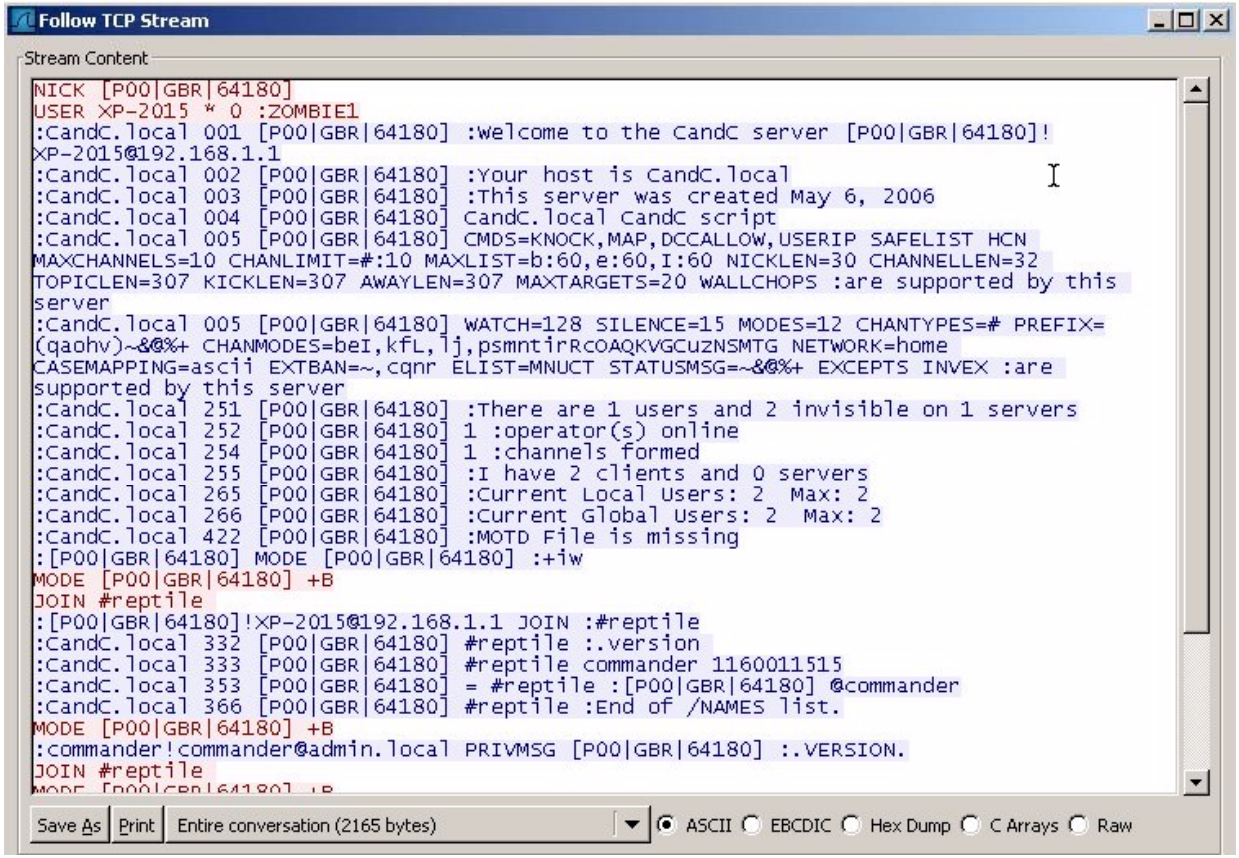
- HTTP, IRC, DNS sniffer
- Grabs unique IP addresses
- Designed to sniff target communication data and present it in an easily viewable interface. Includes basic methods to pick up on target traffic that is not on a known or predefined port.

Video fun

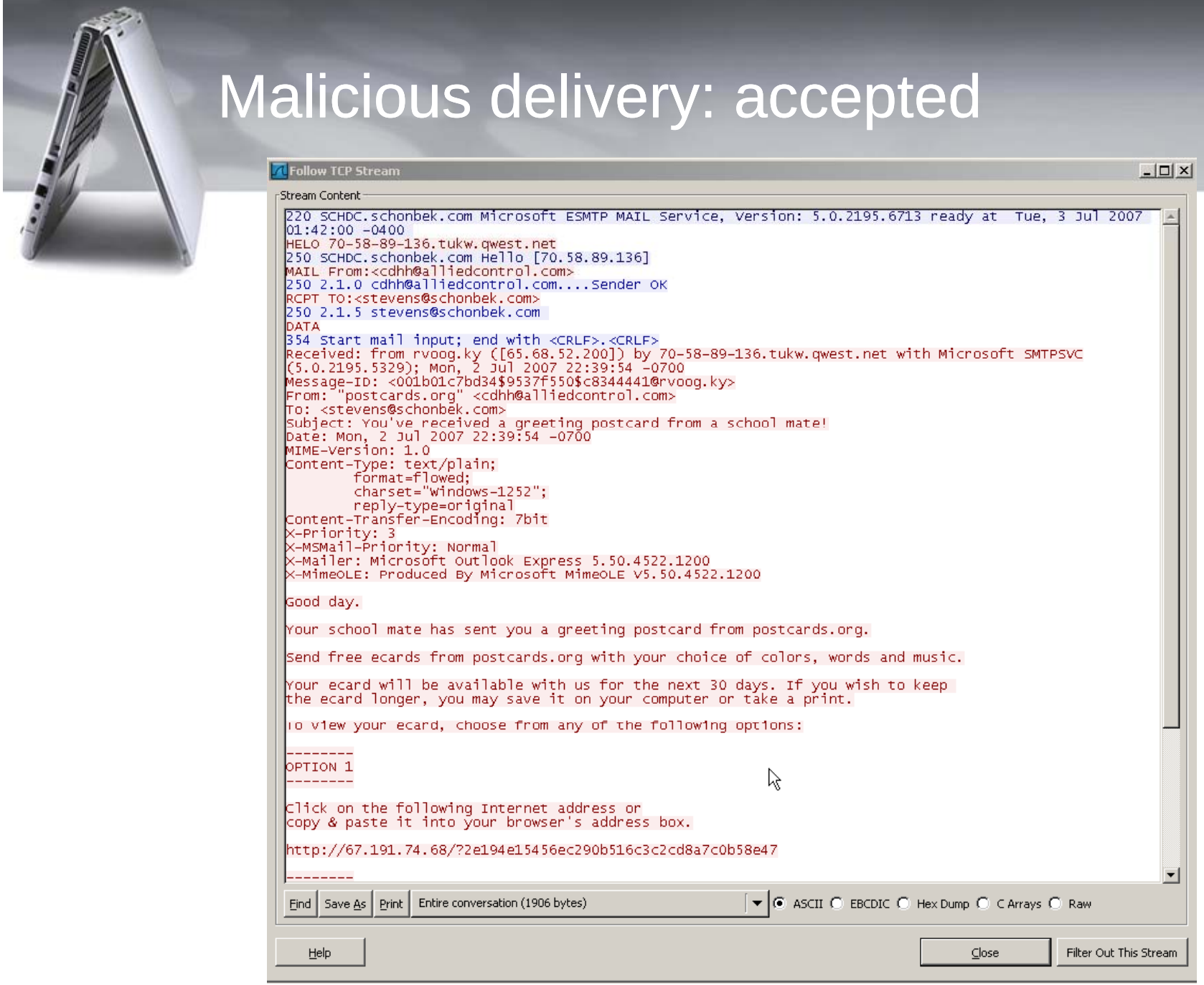

My Documents
My Computer
My Network Places
Internet Explorer
Mozilla Firefox
AutoScreen... 2.1 Pro
SysAnalyzer
SysAnalyzer
File Edit View Favorites Tools Help
Back Search Folders
Address C:\iDEFENSE\SysAnalyzer
Go
File and Folder Tasks
Rename this file
Move this file
Copy this file
Publish this file to the Web
E-mail this file
Delete this file
Other Places
iDEFENSE
My Documents
Shared Documents
My Computer
My Network Places
Details
Name Size Type Date Modified
source File Folder 7/1/2007 4:34 PM
api_log.dll 405 KB Application Extension 4/27/2006 10:30 AM
api_logger.exe 40 KB Application 4/27/2006 10:30 AM
cfg.dat 1 KB DAT File 7/1/2007 10:22 PM
dir_watch.dll 36 KB Application Extension 4/27/2006 10:30 AM
exploit_sigs.txt 1 KB Text Document 4/27/2006 10:30 AM
known_files.mdb 72 KB MDB File 1/18/2007 5:51 PM
proc_analyzer.exe 104 KB Application 4/27/2006 10:30 AM
safe_test1.exe 8 KB Application 4/27/2006 10:30 AM
sniff_hit.exe 88 KB Application 4/27/2006 10:30 AM
sysAnalyzer.exe 381 KB Application 1/18/2007 5:44 PM
SysAnalyzer.pdb 273 KB PDB File 1/18/2007 5:44 PM
SysAnalyzer_help.chm 297 KB Compiled HTML Help... 1/18/2007 5:48 PM
unins000.dat 10 KB DAT File 7/1/2007 4:34 PM
unins000.exe 76 KB Application 6/26/2004 7:00 PM
Recycle Bin
Start
SysAnalyzer
10:43 PM

Wireshark

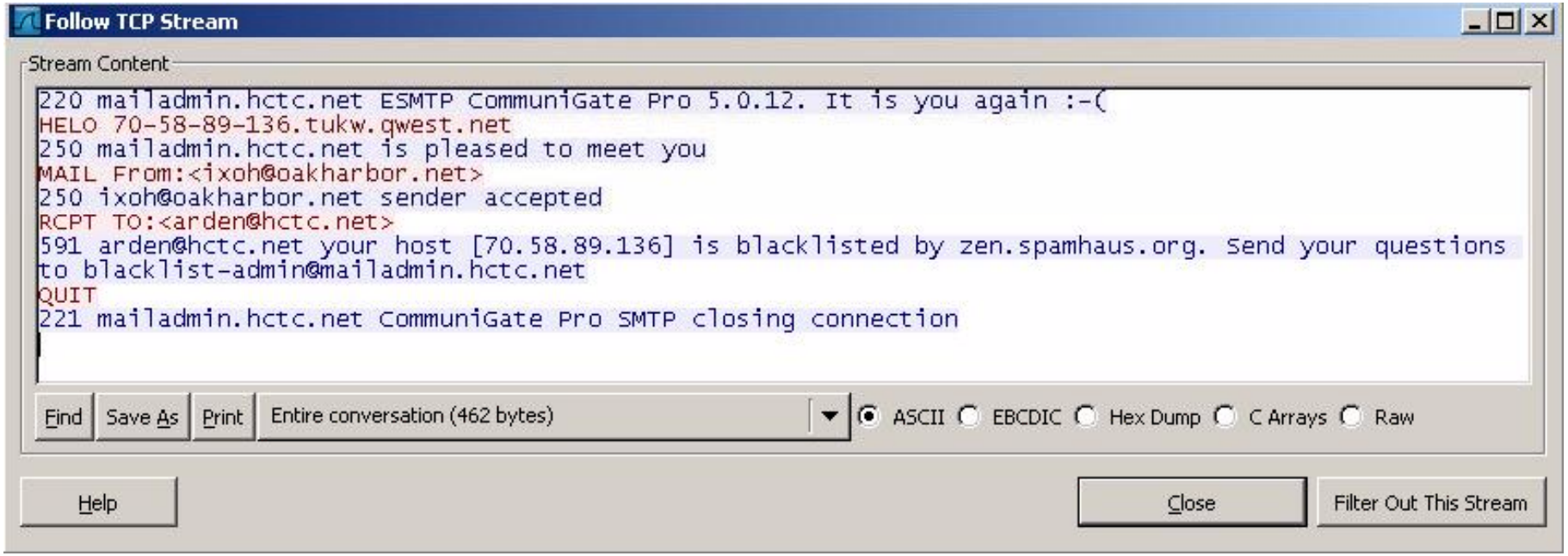
- Don’t forget **the** standby!
- Tons of information in ye olde packet capture
- *Follow TCP Stream* is your friend.



Malicious delivery: accepted

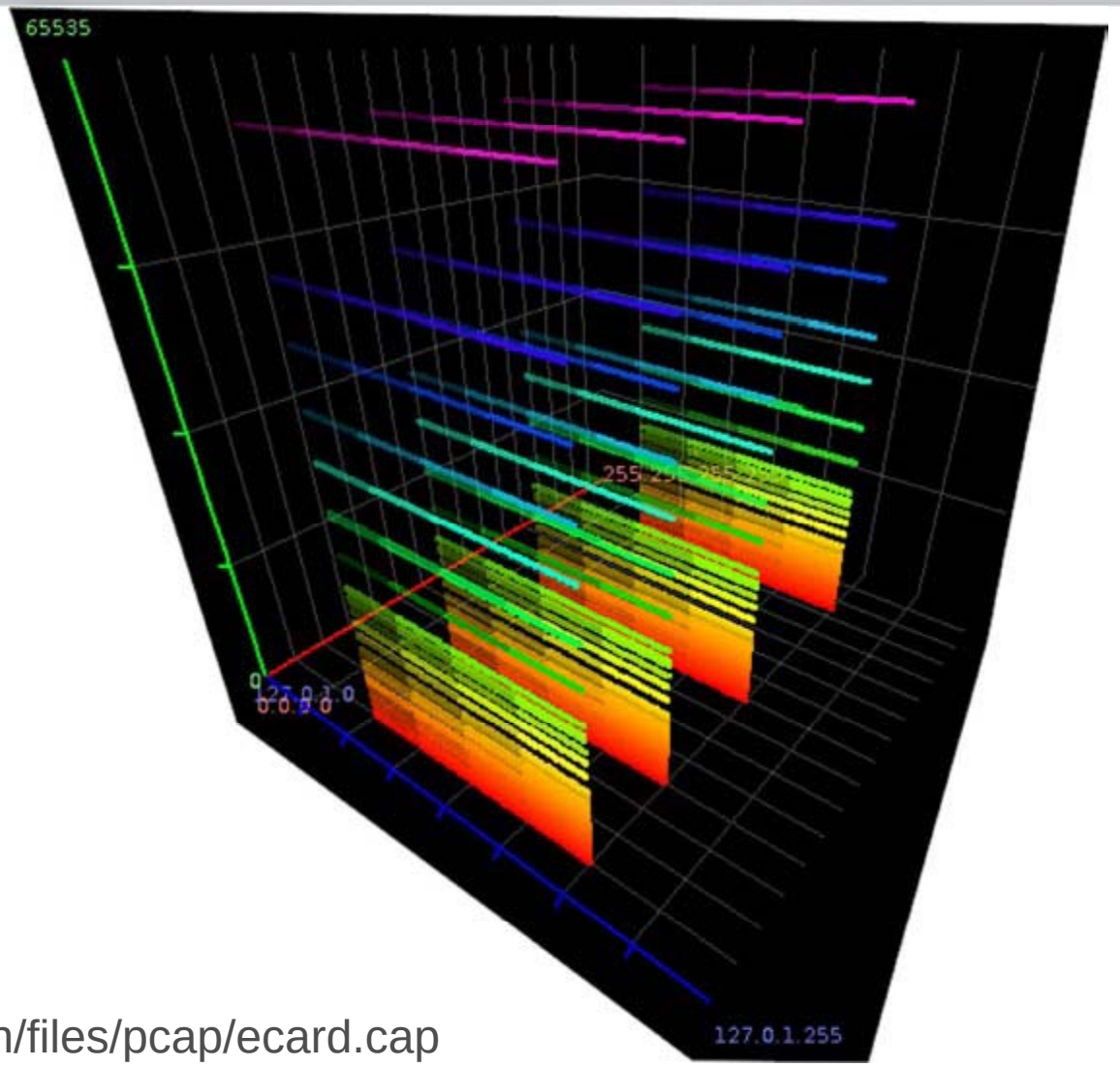


Malicious delivery: rejected ☹



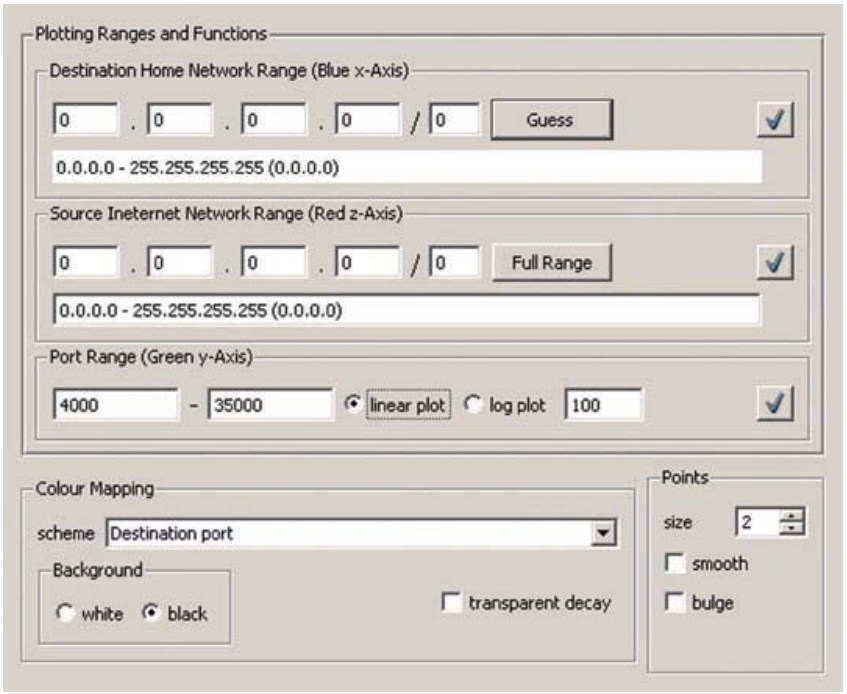
Security Data Visualization - InetVis

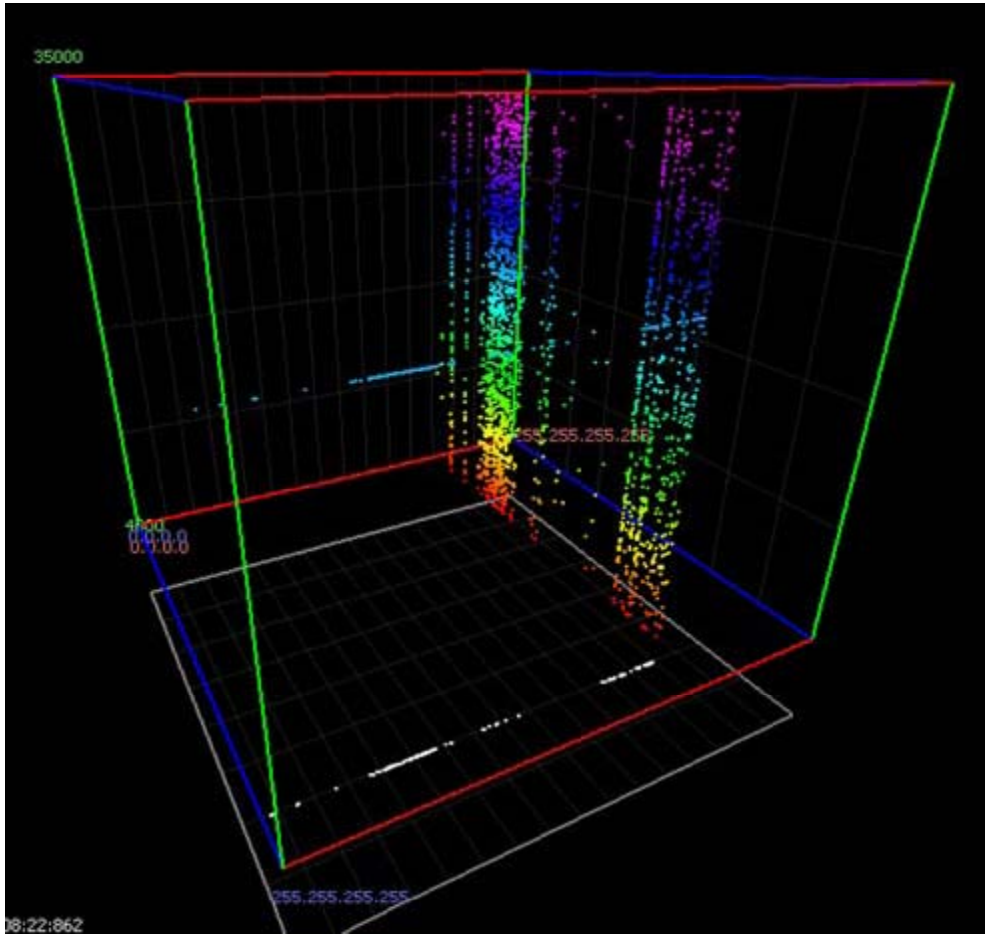
- I’ve found that visualization helps spot behavior not easily picked out of raw logs.



http://holisticinfosec.org/toolsmith/files/pcap/ecard.cap

Security Data Visualization - InetVis

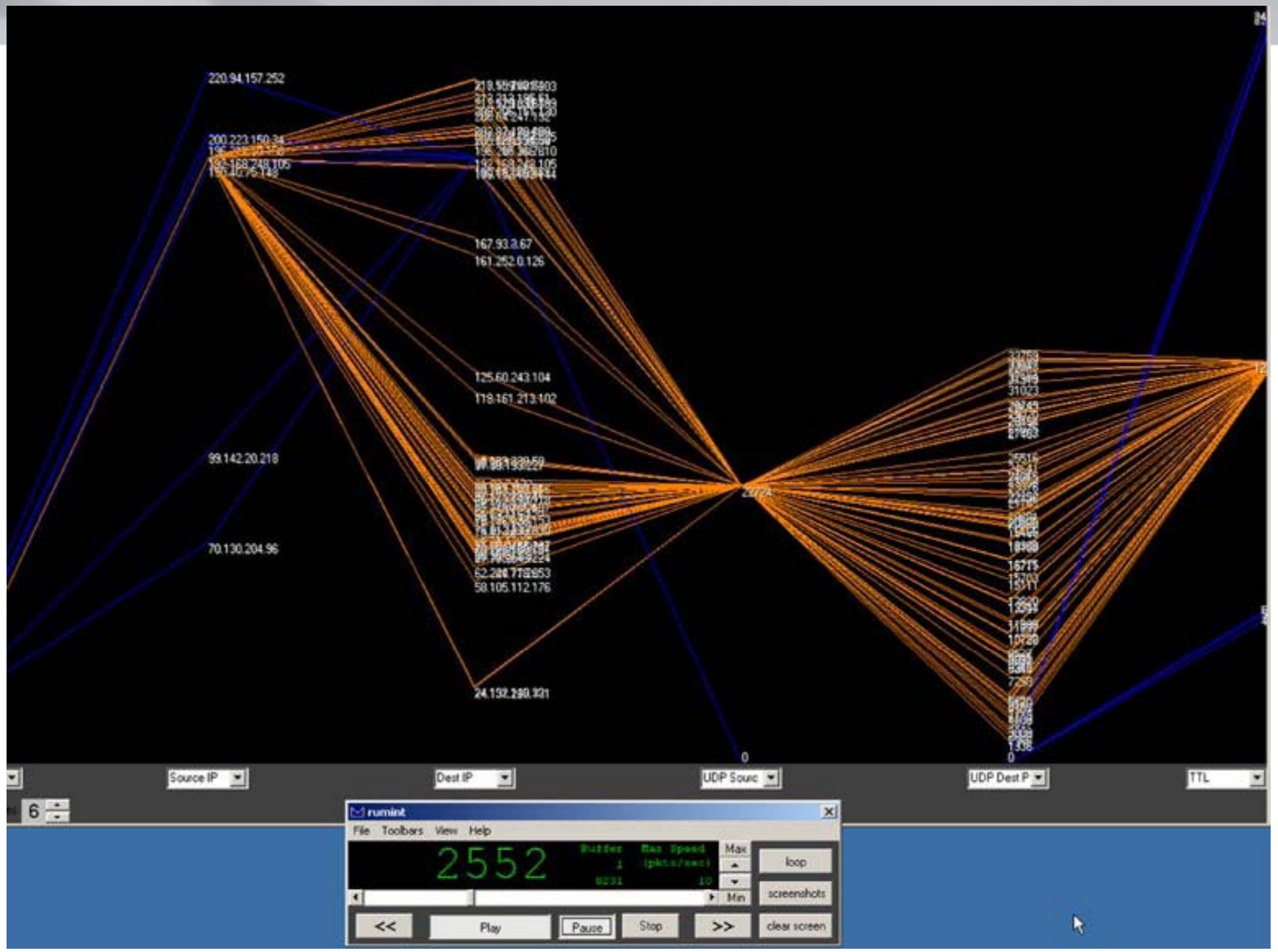




A single Storm infection as visualized with InetVis

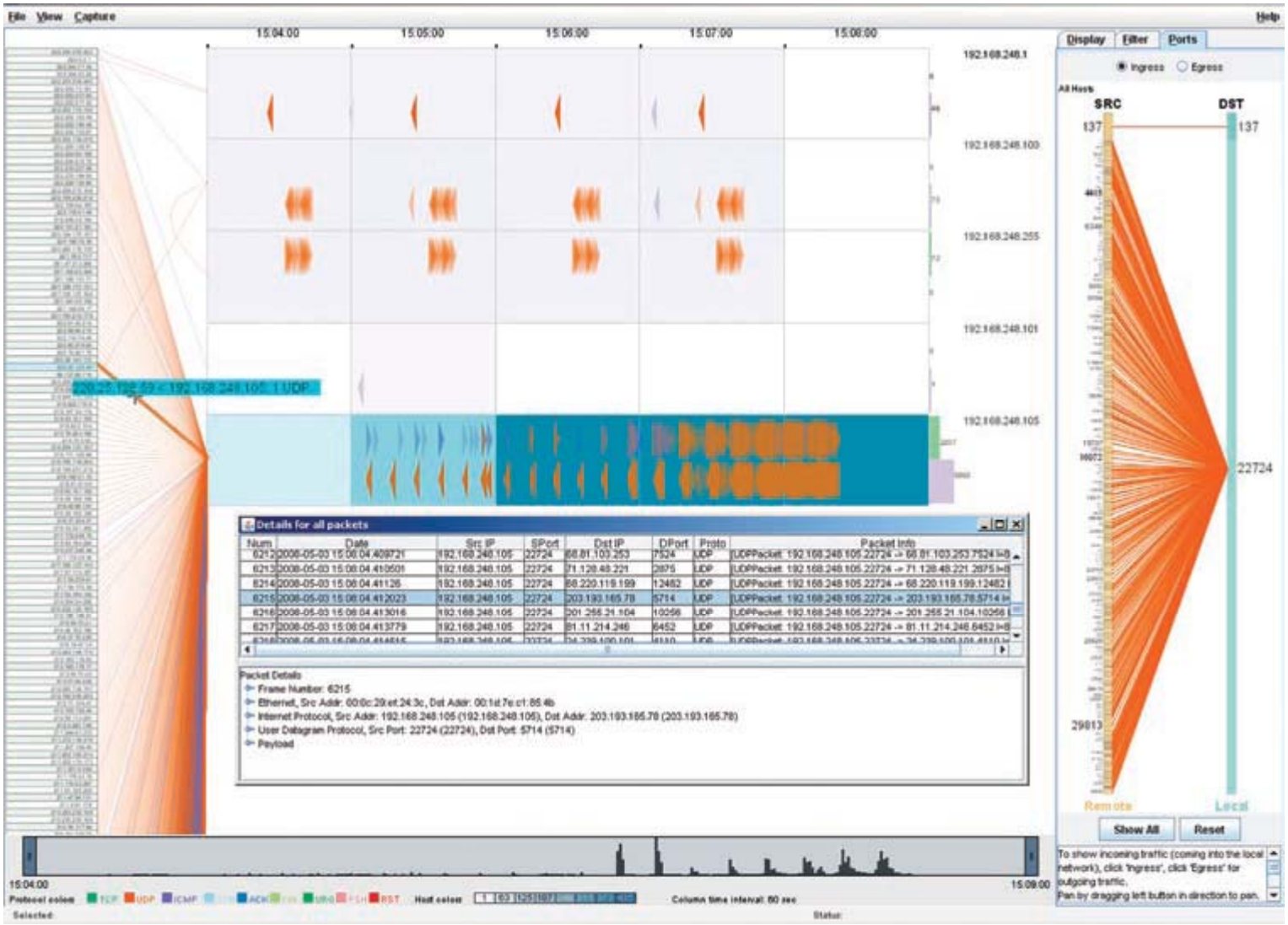
Visualization - Rumint

- Visualized by Source IP, Dest IP, UDP Source, UDP Dest, and TTL using the same ecard.cap sample.
- Greg Conti's excellent offering.



Visualization – TNV

Notice all the connections from hundreds of IPs to a single infected host and egress to a single external destination port.



NSM-Console & HeX System

- NSM-Console is developed by Matthew Lee Hinman, and is included in the HeX System
- Easiest to use from LiveCD or LiveUSB
- Run NSM-Console against single pcaps, or a directory with many files in one fell swoop.
- After setting the file option, you will need to choose modules; you can return all available modules and categories by passing *list*. You can also learn more about modules at any time by passing *nsm> info <module>* for more details. Change global options by passing *nsm> options* or change options on a specific module via *nsm> options <module>*.

NSM-Console & HeX System
Modules, modules, modules

- aimsnarf
- ngrep (gif/jpg/pdf/exe/pe/ne/elf/3pg/torrent)
- tcpxtract
- tcpflow
- chaosreader
- bro-IDS
- snort
- tcpdstat
- capinfos
- tshark
- Argus
- honeysnap
- p0f
- pads
- fl0p
- Iploc
- foremost
- flowgrep
- tcptrace
- tcpick
- flowtime
- flowtag
- harimau
- clamscan

NSM-Console & HeX System

nsm> file /home/analyzt/toolsmith.pcap **(specify the source file)**

nsm> options **(set global options)**

nsm> output /home/analyzt **(define output directory)**

nsm> toggle tcpdstat **(extract tcp statistics about a pcap)**

nsm> toggle capinfos **(print information about a pcap)**

nsm>toggle hash **(hash a pcap)**

nsm> run **(you get the point)**

NSM-Console & HeX System - hash

/home/analyzt/hash

MD5 (/home/analyzt/toolsmith.pcap) =

bfd6c78a0b6d9f41d4496ea1ed2d5d52

SHA256 (/home/analyzt/toolsmith.pcap) =
e619ba3d83471b0e

3bf4878a7219bf3237c48cf4f29d6634e30b3b07d4b83e6f

NSM-Console & HeX System - tcpdstat

/home/analyzt/tcpdtstat

toolsmith.pcap.tcpdstat (abbreviated output)

DumpFile: /home/analyzt/toolsmith.pcap

FileSize: 1.15MB

Id: 200801072234

StartTime: Mon Jan 7 22:34:59 2008

EndTime: Mon Jan 7 22:36:55 2008

TotalTime: 115.45 seconds

TotalCapSize: 1.12MB CapLen: 1514 bytes

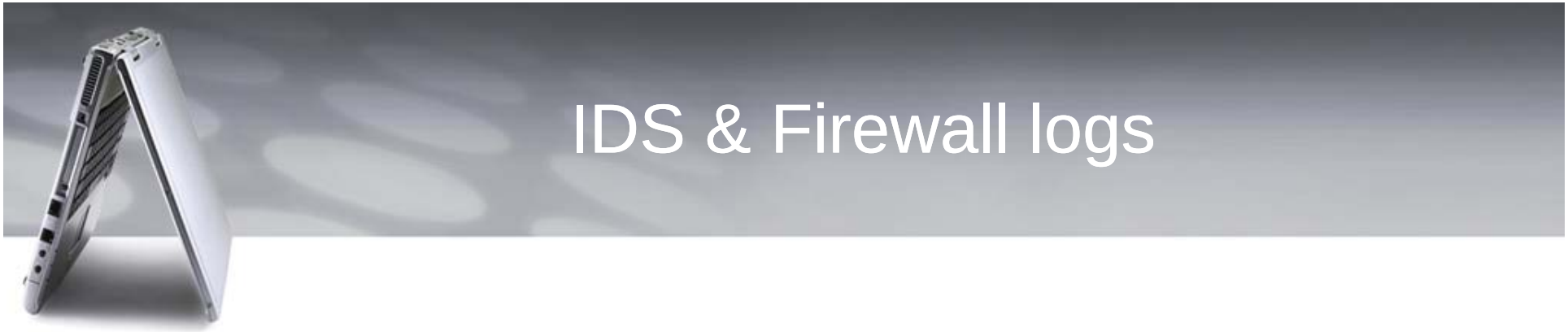
# of packets: 2143 (1.12MB)

AvgRate: 108.84Kbps stddev:197.69K

Protocol Breakdown
<<<<
protocol packets bytes bytes/pkt
----
[0] total 2143 (100.00%) 1173519 (100.00%) 547.61
[1] ip 2143 (100.00%) 1173519 (100.00%) 547.61
[2] tcp 2007 (93.65%) 1153160 (98.27%) 574.57
[3] http(s) 1036 (48.34%) 1000215 (85.23%) 965.46
[3] http(c) 971 (45.31%) 152945 (13.03%) 157.51
[2] udp 135 (6.30%) 20299 (1.73%) 150.36
[3] dns 130 (6.07%) 18889 (1.61%) 145.30
[3] mcast 1 (0.05%) 82 (0.01%) 82.00
[3] other 4 (0.19%) 1328 (0.11%) 332.00
[2] igmp 1 (0.05%) 60 (0.01%) 60.00
>>>>

NSM-Console & HeX System - capinfos

/home/analyzt/capinfos
toolsmith.pcap.capinfos
File name: /home/analyzt/toolsmith.pcap
File type: Wireshark/tcpdump/... - libpcap
Number of packets: 2143
File size: 1207831 bytes
Data size: 1173519 bytes
Capture duration: 115.445612 seconds
Start time: Mon Jan 7 22:34:59 2008
End time: Mon Jan 7 22:36:55 2008
Data rate: 10165.12 bytes/s
Data rate: 81320.99 bits/s
Average packet size: 547.61 bytes
File name: /home/analyzt/toolsmith.pcap
File type: Wireshark/tcpdump/... - libpcap
Number of packets: 2143
File size: 1207831 bytes
Data size: 1173519 bytes
Capture duration: 115.445612 seconds
Start time: Mon Jan 7 22:34:59 2008
End time: Mon Jan 7 22:36:55 2008
Data rate: 10165.12 bytes/s
Data rate: 81320.99 bits/s
Average packet size: 547.61 bytes



IDS & Firewall logs

- …monitored IDS or firewall logs have tipped you off to an infected host.
- Remember one of our first slides?
- Good reason for egress filtering…

Export to csv

Less | More Previous Page | Next Page

Date	Time	Severity	Device	Device Description	Event ID	Event Summary	Incident	Helpdesk ID	Source	Destination	Count
05 Jul 2007	16:55:17	Low	BEL-EF-	PIX HA Primary - Pair	38877663	probe for 10487/udp	-	-	172.30.91.2	85.76.252.138	1
05 Jul 2007	16:55:16	Low	BEL-EF-	PIX HA Primary - Pair	38877656	probe for 10629/udp	-	-	172.30.91.2	68.42.150.171	1
05 Jul 2007	16:55:11	Low	BEL-EF-	PIX HA Primary - Pair	38877628	probe for 4183/udp	-	-	172.30.91.2	61.228.201.222	1
05 Jul 2007	16:55:10	Low	BEL-EF-	PIX HA Primary - Pair	38877620	probe for 54695/udp	-	-	172.30.91.2	82.55.220.212	1
05 Jul 2007	16:55:04	Low	BEL-EF-	PIX HA Primary - Pair	38877592	probe for dyna-lm/udp	-	-	172.30.91.2	84.74.226.207	1
05 Jul 2007	16:55:02	Low	BEL-EF-	PIX HA Primary - Pair	38877577	probe for vinainstall/udp	-	-	172.30.91.2	84.123.166.106	1
05 Jul 2007	16:55:00	Low	BEL-EF-	PIX HA Primary - Pair	38877568	Possible StormWorm Activity	-	-	172.30.91.2	154.37.66.209	2
05 Jul 2007	16:54:52	High	BEL-EF-	PIX HA Primary - Pair	38877529	probe for 7871/udp	-	-	172.30.91.2	69.26.191.34	2
05 Jul 2007	16:54:52	Low	BEL-EF-	PIX HA Primary - Pair	38877531	probe for 3714/udp	-	-	172.30.91.2	82.64.169.85	1
05 Jul 2007	16:54:51	Low	BEL-EF-	PIX HA Primary - Pair	38877524	probe for 4533/udp	-	-	172.30.91.2	81.83.232.171	1
05 Jul 2007	16:54:51	Low	BEL-EF-	PIX HA Primary - Pair	38877525	Possible StormWorm Activity	-	-	172.30.91.2	81.2.209.136	2
05 Jul 2007	16:54:08	Low	BEL-EF-	PIX HA Primary - Pair	38877341	probe for 16464/udp	-	-	172.30.91.2	83.97.181.149	2
05 Jul 2007	16:54:08	Low	BEL-EF-	PIX HA Primary - Pair	38877342	Possible StormWorm Activity	-	-	172.30.91.2	72.36.146.114	3
05 Jul 2007	16:54:07	Low	BEL-EF-	PIX HA Primary - Pair	38877339	probe for 13327/udp	-	-	172.30.91.2	213.112.20.102	2
05 Jul 2007	16:54:06	Low	BEL-EF-	PIX HA Primary - Pair	38877335	probe for 33333/udp	-	-	172.30.91.2	85.125.224.183	2

Summary

- You don’t need expensive, commercial tools.
- Don’t be afraid to experiment (in a controlled environment).
- No one way is right, and it is certain there are a plethora of tools available that we didn’t cover.
- Some of these tools will also aid you during other types of incidents and investigations.

Questions?

holisticinfosec@gmail.com
Holisticinfosec.org

Thank you!

© Russ McRee

References

- Mandiant Red Curtain http://mandiant.com/mrc
- RAPIER http://code.google.com/p/rapier/
- SysInternals http://www.microsoft.com/technet/sysinternals/default.mspx
- iDefense Labs http://labs.idefense.com/software/malcode.php
- Virustotal http://www.virustotal.com/
- Jotti http://virusscan.jotti.org/
- Process Monitor http://www.microsoft.com/technet/sysinternals/utilities/processmonitor.mspx
- Helix http://www.e-fense.com/helix/
- Wireshark – http://www.wireshark.org
- NSM-Console - http://writequit.org/projects/nsm-console/
- Visualization - http://secviz.org/