Malcode Analysis Techniques for Incident Handlers

Russ McRee holisticinfosec.org

20th Annual FIRST Conference

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

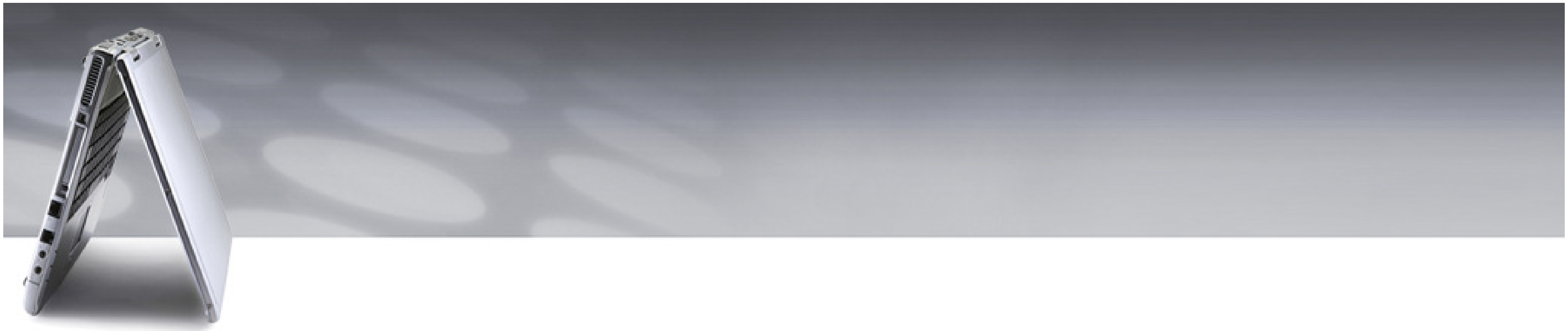
- We’ll cover Identification and Analysis today.

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

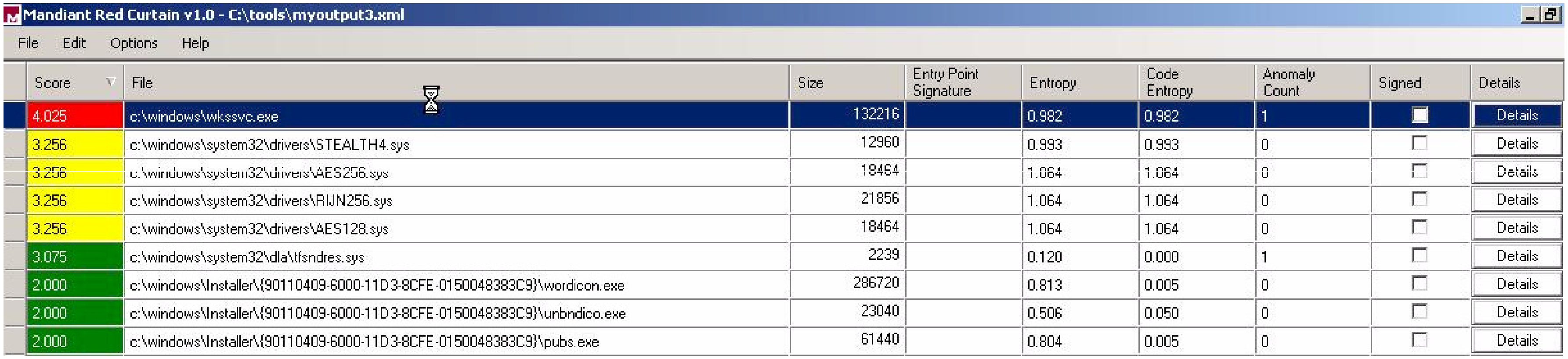
- MRC can be run locally on the suspect host.
- .NET 2.0 framework dependent.
- Can also be run as a remote agent.
- Note: Engage only trusted tools as part of your analysis. Why?
- Here’s where Helix comes in handy.

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:



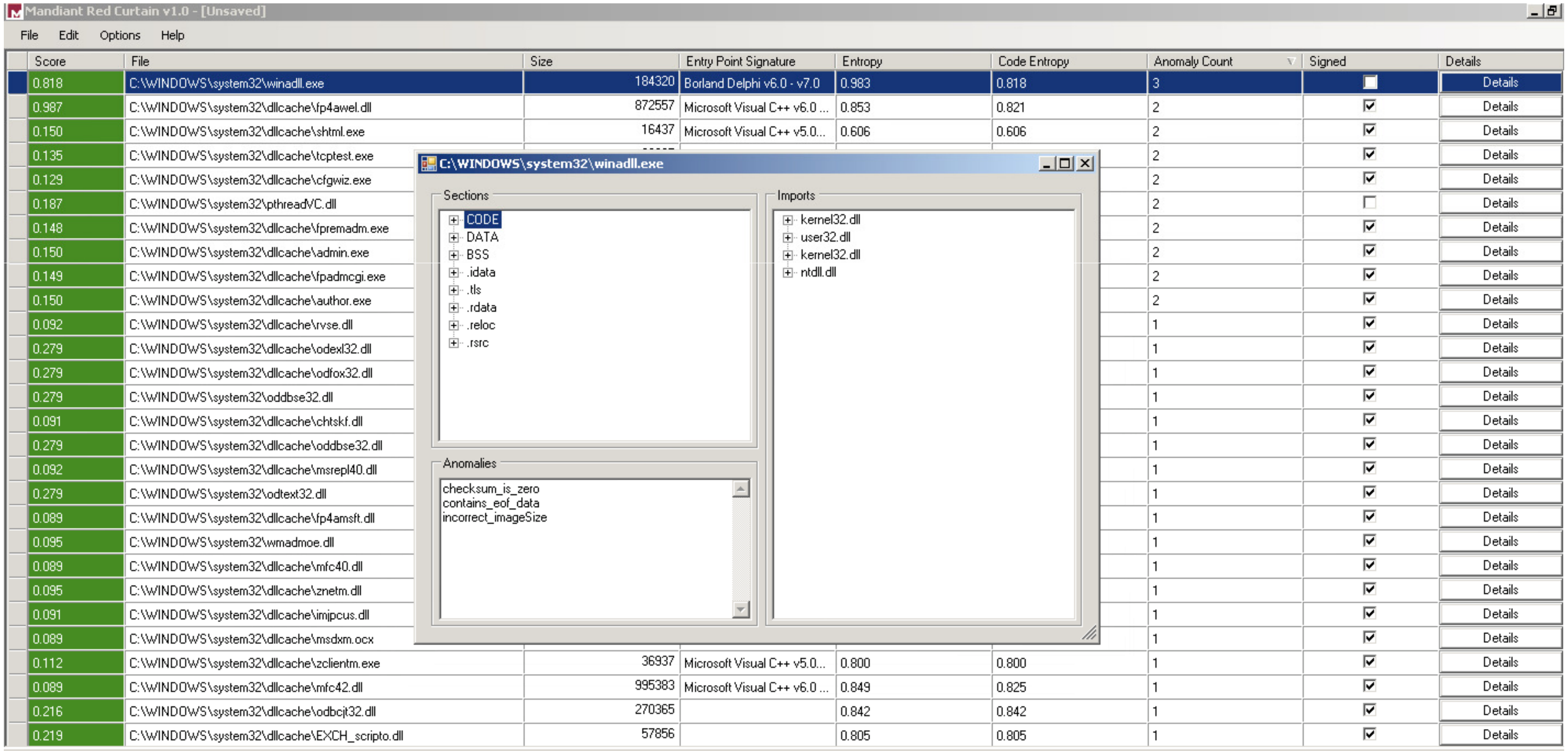
Mandiant Red Curtain v1.0 - C:\tools\myoutput3.xml

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

C:\WINDOWS\system32\winadll.exe

Sections

- CODE
- DATA
- BSS
- .idata
- .tls
- .rdata
- .reloc
- .rsrc

Imports

- kernel32.dll
- user32.dll
- kernel32.dll
- ntdll.dll

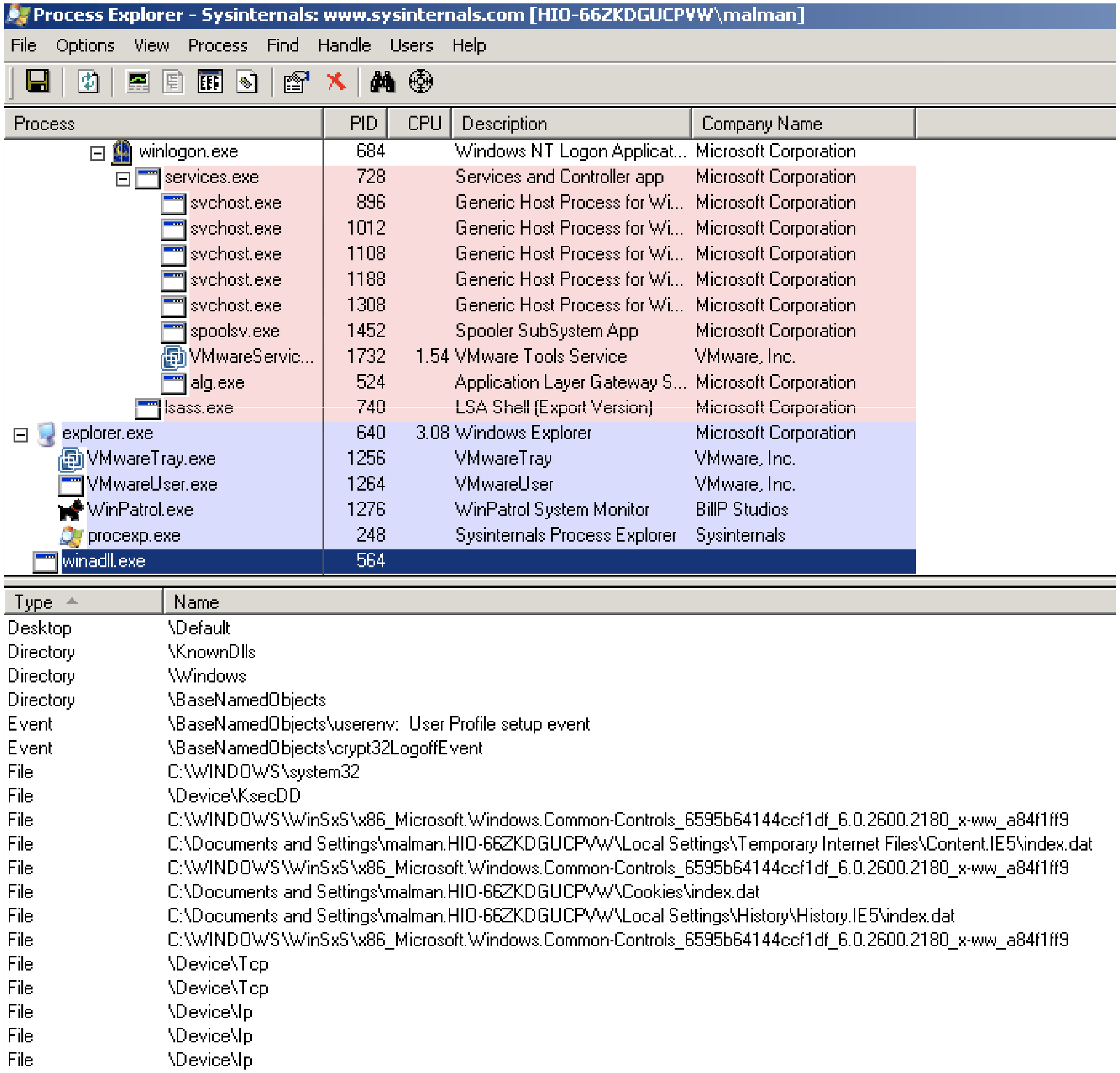
Anomalies

```
checksum_is_zero
contains_eof_data
incorrect_imageSize
```

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.


Process Explorer - Sysinternals: www.sysinternals.com [HIO-66ZKDGUCPVW\malman]
File Options View Process Find Handle Users Help

Process	PID	CPU	Description	Company Name
winlogon.exe	684		Windows NT Logon Applicat...	Microsoft Corporation
services.exe	728		Services and Controller app	Microsoft Corporation
svchost.exe	896		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1012		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1108		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1188		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1308		Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe	1452		Spooler SubSystem App	Microsoft Corporation
VMwareServic...	1732	1.54	VMware Tools Service	VMware, Inc.
alg.exe	524		Application Layer Gateway S...	Microsoft Corporation
lsass.exe	740		LSA Shell (Export Version)	Microsoft Corporation
explorer.exe	640	3.08	Windows Explorer	Microsoft Corporation
VMwareTray.exe	1256		VMwareTray	VMware, Inc.
VMwareUser.exe	1264		VMwareUser	VMware, Inc.
WinPatrol.exe	1276		WinPatrol System Monitor	BillP Studios
procexp.exe	248		Sysinternals Process Explorer	Sysinternals
winadll.exe	564			

Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\Windows
Directory	\BaseNamedObjects
Event	\BaseNamedObjects\userenv: User Profile setup event
Event	\BaseNamedObjects\crypt32LogoffEvent
File	C:\WINDOWS\system32
File	\Device\KsecDD
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.2180_x-ww_a84f1ff9
File	C:\Documents and Settings\malman.HIO-66ZKDGUCPVW\Local Settings\Temporary Internet Files\Content.IE5\index.dat
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.2180_x-ww_a84f1ff9
File	C:\Documents and Settings\malman.HIO-66ZKDGUCPVW\Cookies\index.dat
File	C:\Documents and Settings\malman.HIO-66ZKDGUCPVW\Local Settings\History\History.IE5\index.dat
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.2180_x-ww_a84f1ff9
File	\Device\Tcp
File	\Device\Tcp
File	\Device\Ip
File	\Device\Ip
File	\Device\Ip

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.

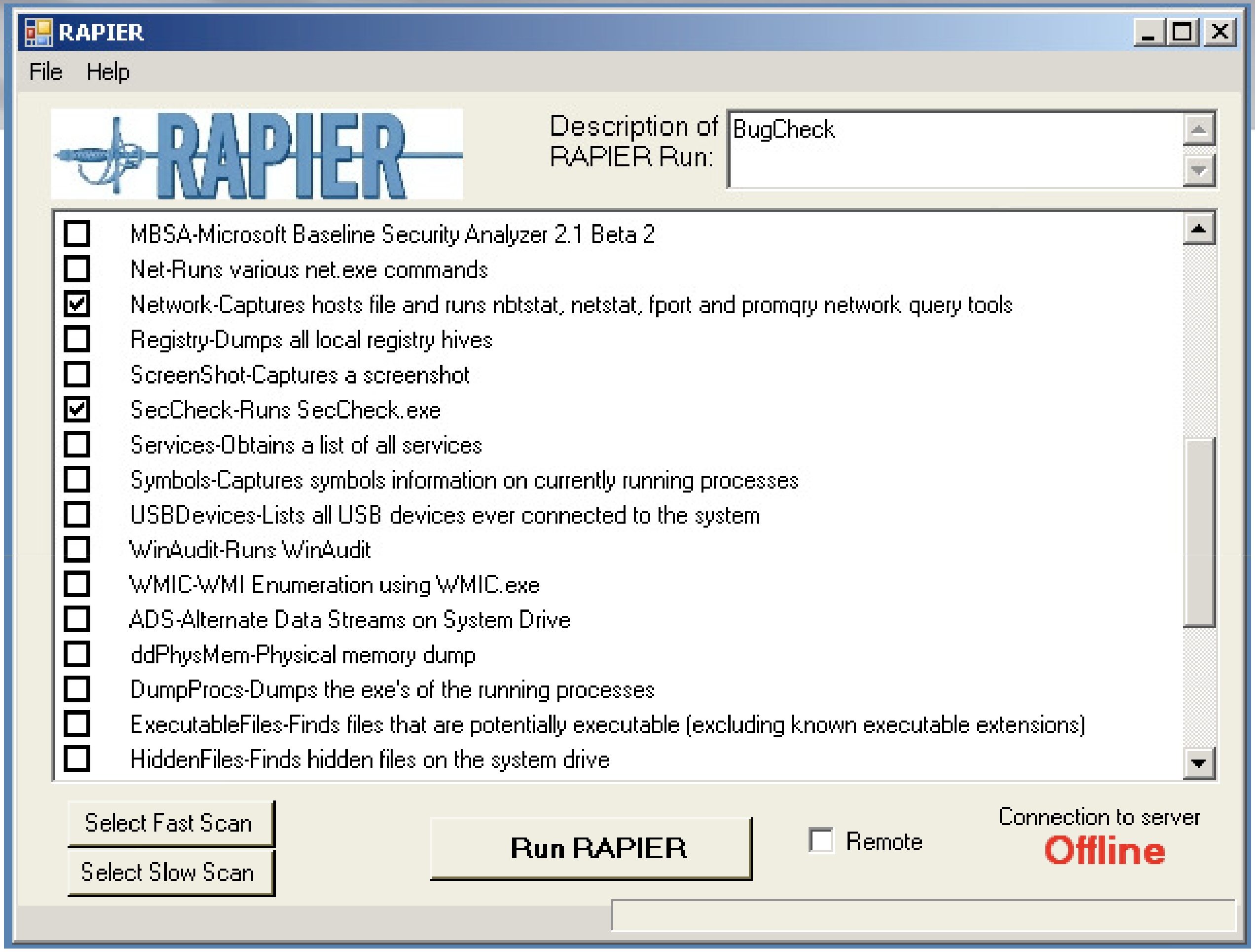
RAPIER 3.2 - Server

- 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



Description of RAPIER Run: BugCheck

- □ MBSA-Microsoft Baseline Security Analyzer 2.1 Beta 2
- □ Net-Runs various net.exe commands
- ☑ Network-Captures hosts file and runs nbtstat, netstat, fport and promqry network query tools
- □ Registry-Dumps all local registry hives
- □ ScreenShot-Captures a screenshot
- ☑ SecCheck-Runs SecCheck.exe
- □ Services-Obtains a list of all services
- □ Symbols-Captures symbols information on currently running processes
- □ USBDevices-Lists all USB devices ever connected to the system
- □ WinAudit-Runs WinAudit
- □ WMIC-WMI Enumeration using WMIC.exe
- □ ADS-Alternate Data Streams on System Drive
- □ ddPhysMem-Physical memory dump
- □ DumpProcs-Dumps the exe's of the running processes
- □ ExecutableFiles-Finds files that are potentially executable (excluding known executable extensions)
- □ HiddenFiles-Finds hidden files on the system drive

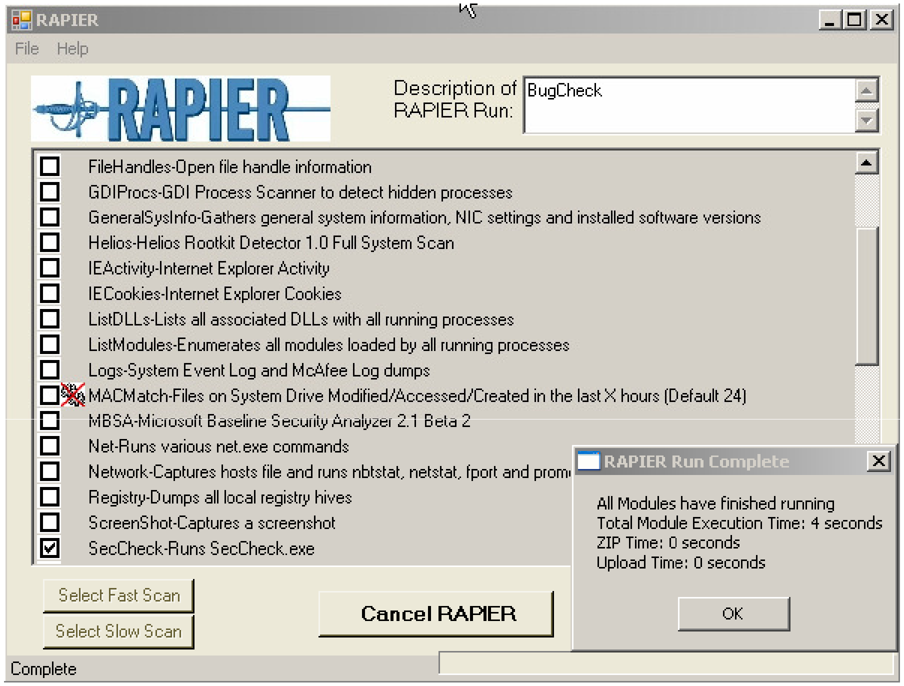
□ Remote

Connection to server **Offline**

- 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…



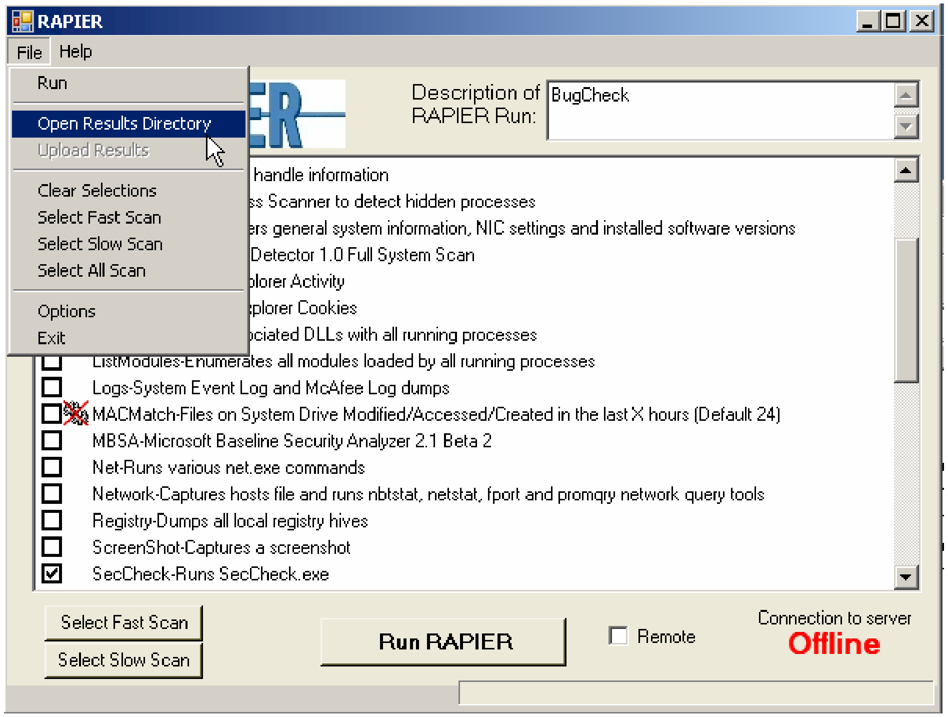
Description of RAPIER Run: BugCheck

□ FileHandles-Open file handle information
□ GDIProcs-GDI Process Scanner to detect hidden processes
□ GeneralSysInfo-Gathers general system information, NIC settings and installed software versions
□ Helios-Helios Rootkit Detector 1.0 Full System Scan
□ IEActivity-Internet Explorer Activity
□ IECookies-Internet Explorer Cookies
□ ListDLLs-Lists all associated DLLs with all running processes
□ ListModules-Enumerates all modules loaded by all running processes
□ Logs-System Event Log and McAfee Log dumps
□ MACMatch-Files on System Drive Modified/Accessed/Created in the last X hours (Default 24)
□ MBSA-Microsoft Baseline Security Analyzer 2.1 Beta 2
□ Net-Runs various net.exe commands
□ Network-Captures hosts file and runs nbtstat, netstat, fport and prom
□ Registry-Dumps all local registry hives
□ ScreenShot-Captures a screenshot
☑ SecCheck-Runs SecCheck.exe

RAPIER Run Complete

All Modules have finished running
Total Module Execution Time: 4 seconds
ZIP Time: 0 seconds
Upload Time: 0 seconds

Complete



Description of RAPIER Run: BugCheck

handle information
ss Scanner to detect hidden processes
ers general system information, NIC settings and installed software versions
Detector 1.0 Full System Scan
plorer Activity
xplorer Cookies
ociated DLLs with all running processes
□ ListModules-Enumerates all modules loaded by all running processes
□ Logs-System Event Log and McAfee Log dumps
□ MACMatch-Files on System Drive Modified/Accessed/Created in the last X hours (Default 24)
□ MBSA-Microsoft Baseline Security Analyzer 2.1 Beta 2
□ Net-Runs various net.exe commands
□ Network-Captures hosts file and runs nbtstat, netstat, fport and promqry network query tools
□ Registry-Dumps all local registry hives
□ ScreenShot-Captures a screenshot
☑ SecCheck-Runs SecCheck.exe

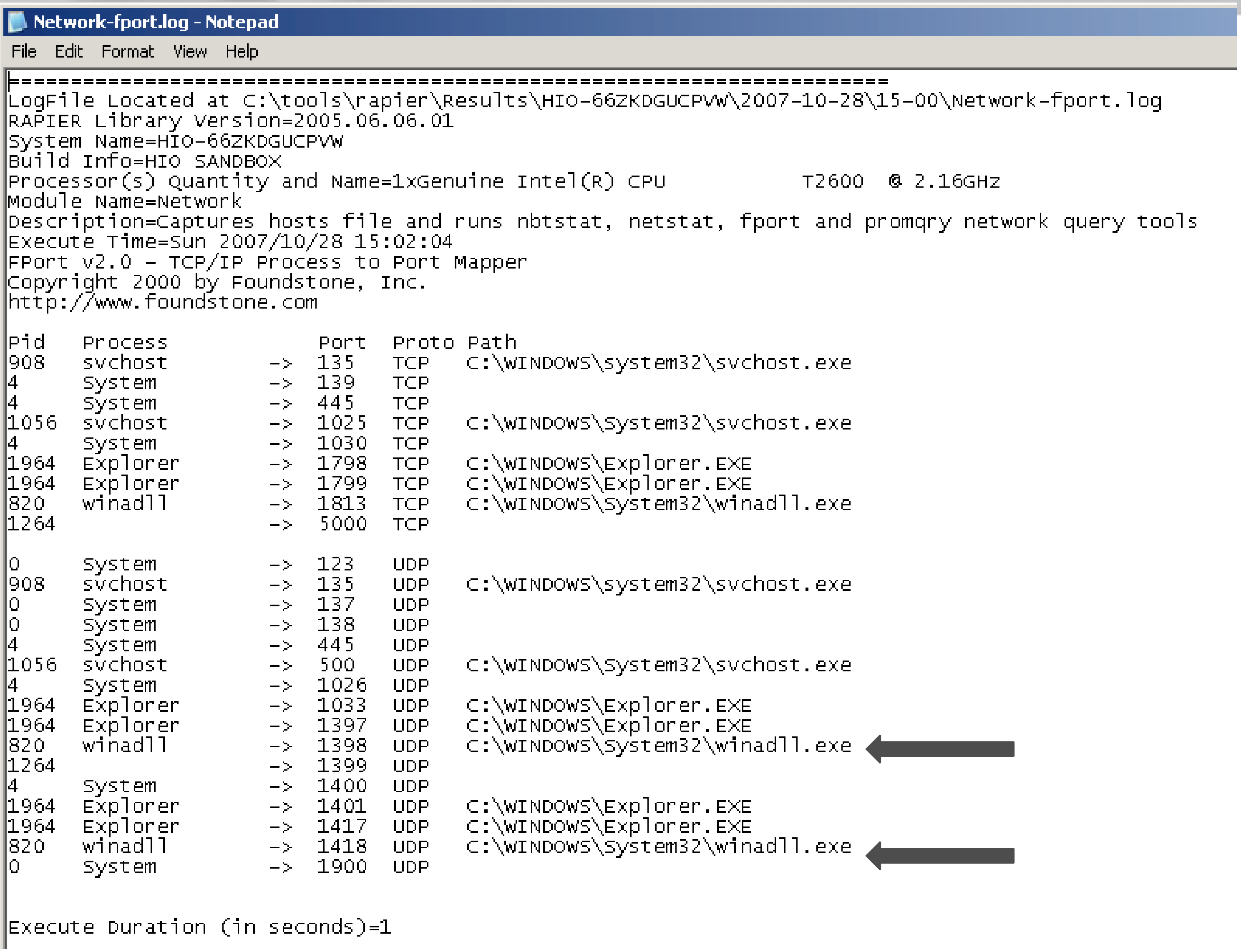
□ Remote

Connection to server **Offline**

…easy navigation to results.

RAPIER 3.2 - Client

Network module results - fport:

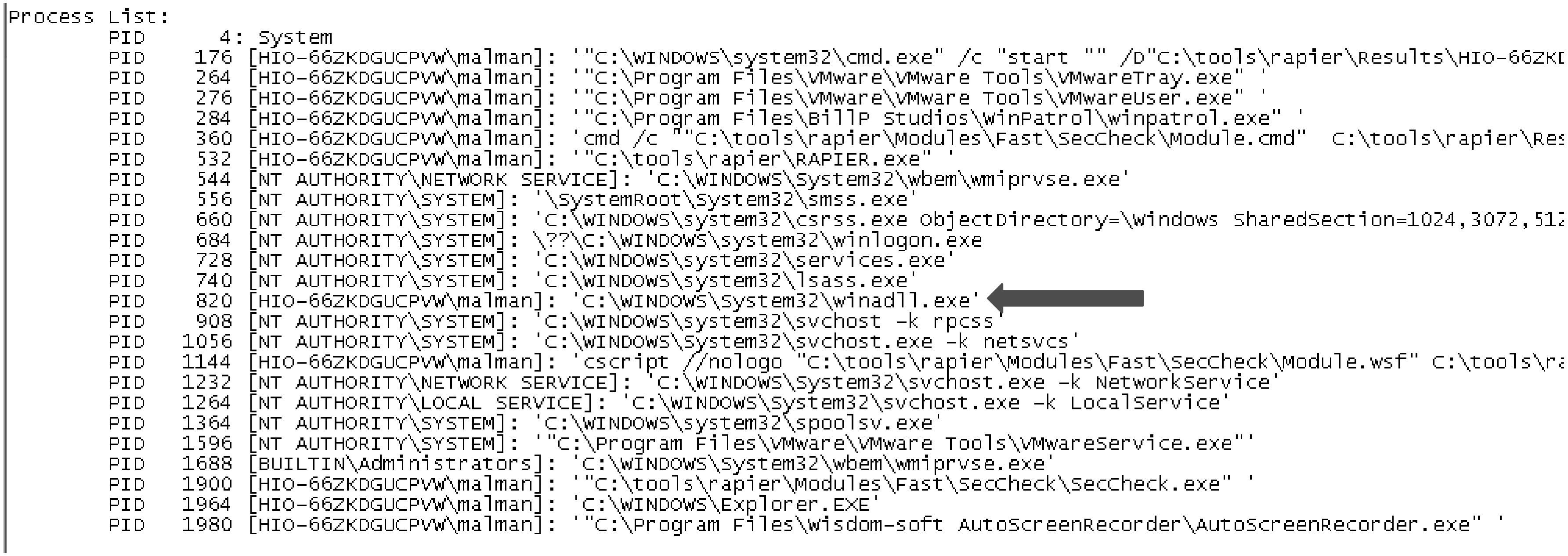


```
=======================================================================
LogFile Located at C:\tools\rapier\Results\HIO-66ZKDGUCPVW\2007-10-28\15-00\Network-fport.log
RAPIER Library Version=2005.06.06.01
System Name=HIO-66ZKDGUCPVW
Build Info=HIO SANDBOX
Processor(s) Quantity and Name=1xGenuine Intel(R) 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:

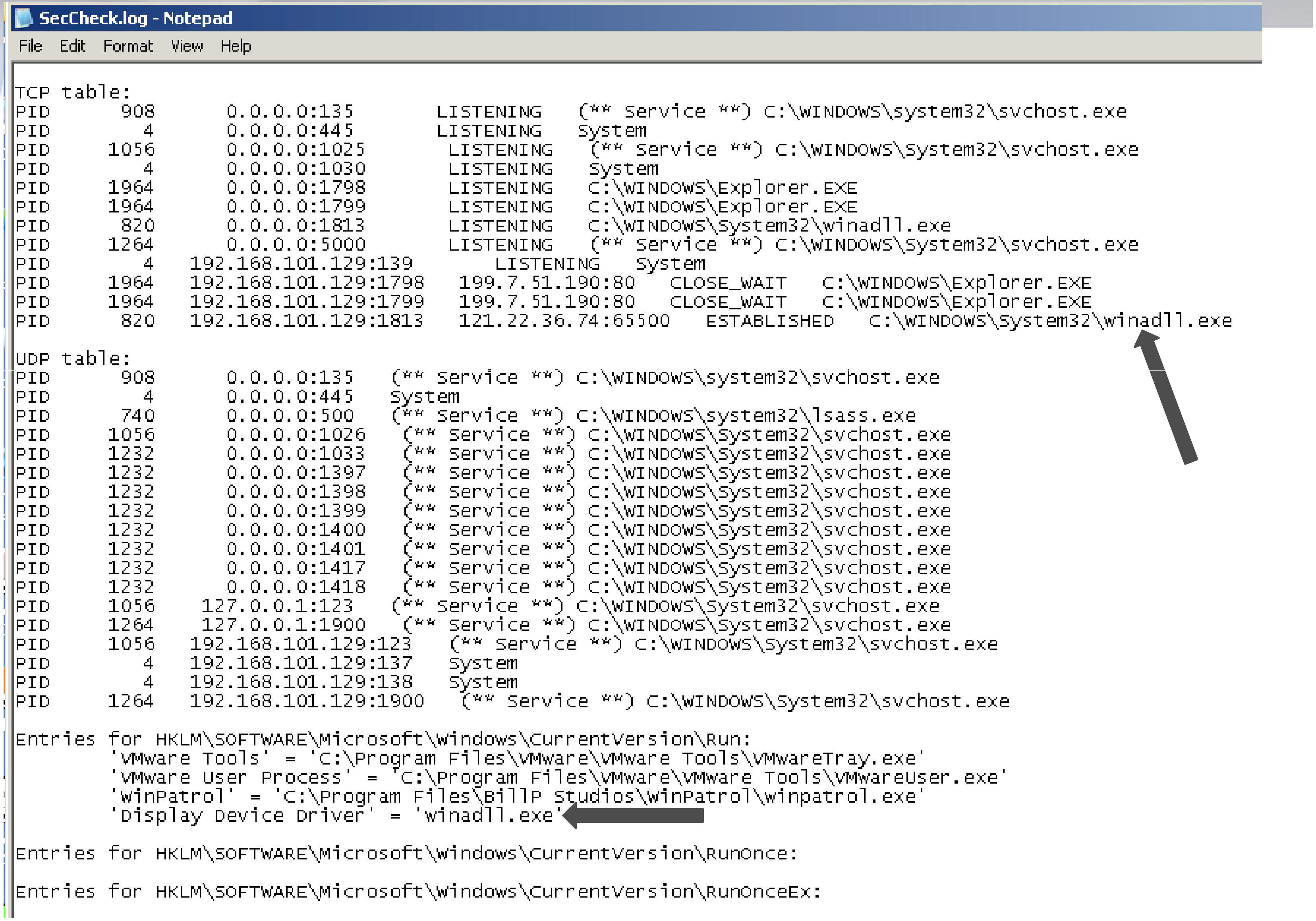
- Confirms what we saw in Process Explorer.



```
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=1024,3072,51
        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:

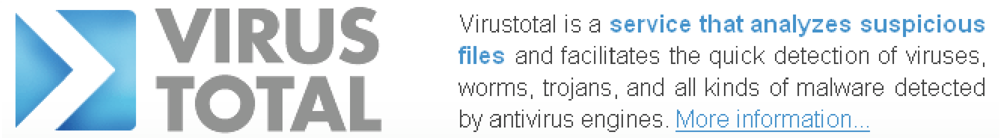


```
TCP table:
PID      908      0.0.0.0:135       LISTENING   (** Service **) C:\WINDOWS\system32\svchost.exe
PID        4      0.0.0.0:445       LISTENING   System
PID     1056      0.0.0.0:1025       LISTENING   (** Service **) C:\WINDOWS\System32\svchost.exe
PID        4      0.0.0.0:1030       LISTENING   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

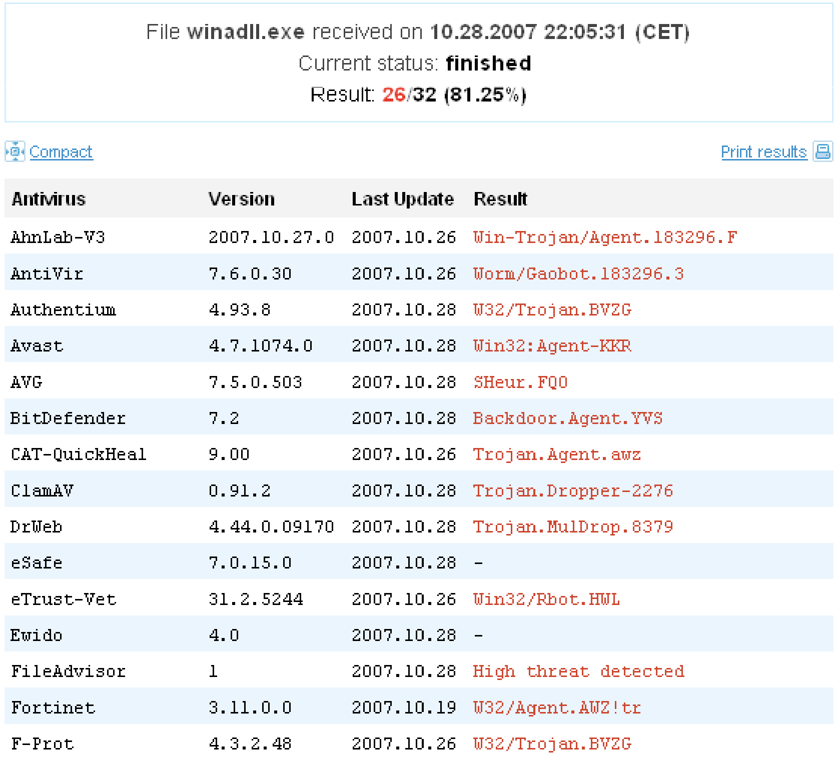
- With our unwelcome visitor identified how can we quickly learn more?
- Online scanners are invaluable: Is it a new variant with little coverage, or is it easily identified, denoting a gap in the victim host’s AV application.
- Be a good citizen, if coverage is light submit the sample directly to vendors.

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%)**

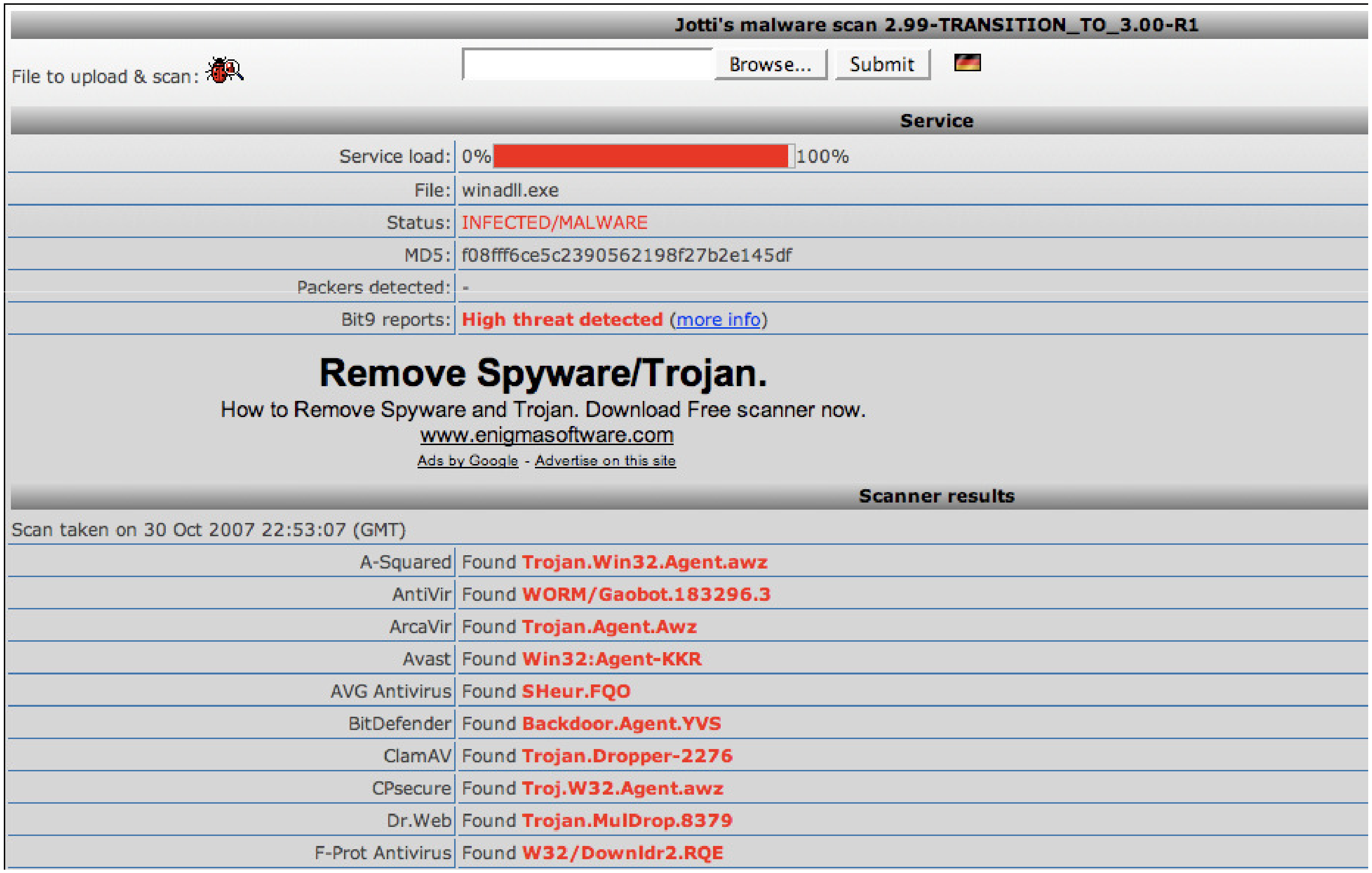
Antivirus	Version	Last Update	Result
AhnLab-V3	2007.10.27.0	2007.10.26	Win-Trojan/Agent.183296.F
AntiVir	7.6.0.30	2007.10.26	Worm/Gaobot.183296.3
Authentium	4.93.8	2007.10.28	W32/Trojan.BVZG
Avast	4.7.1074.0	2007.10.28	Win32:Agent-KKR
AVG	7.5.0.503	2007.10.28	SHeur.FQO
BitDefender	7.2	2007.10.28	Backdoor.Agent.YVS
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:

Service

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

Scanner results

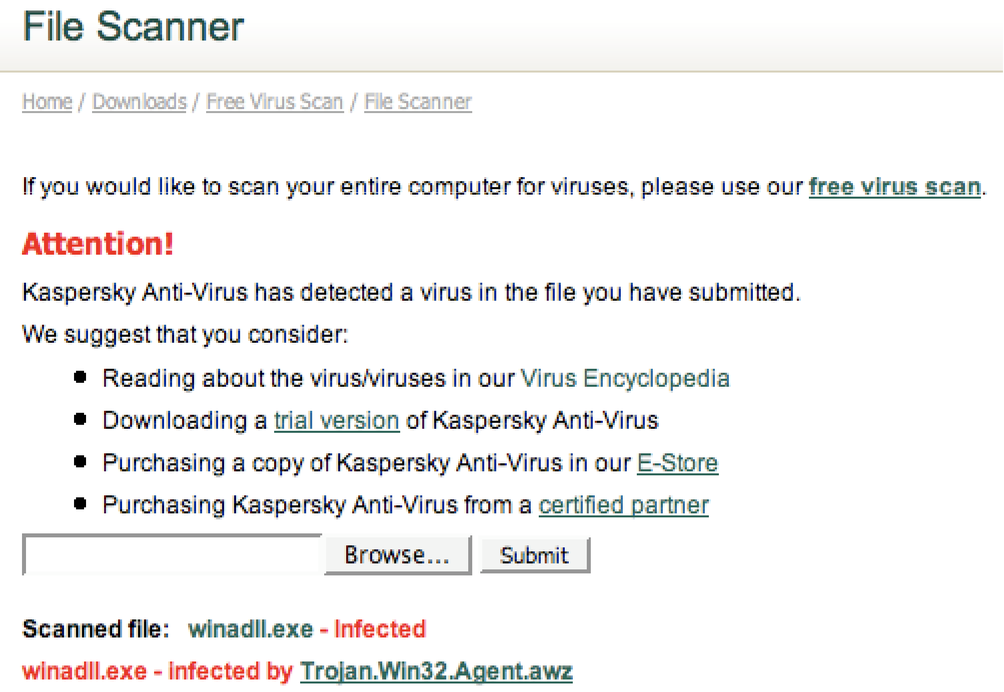
Scan taken on 30 Oct 2007 22:53:07 (GMT)

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.



File Scanner

Home / Downloads / Free Virus Scan / File Scanner

If you would like to scan your entire computer for viruses, please use our **free virus scan**.

Attention!

Kaspersky Anti-Virus has detected a virus in the file you have submitted.

We suggest that you consider:

- Reading about the virus/viruses in our Virus Encyclopedia
- Downloading a trial version of Kaspersky Anti-Virus
- Purchasing a copy of Kaspersky Anti-Virus in our E-Store
- Purchasing Kaspersky Anti-Virus from a certified partner

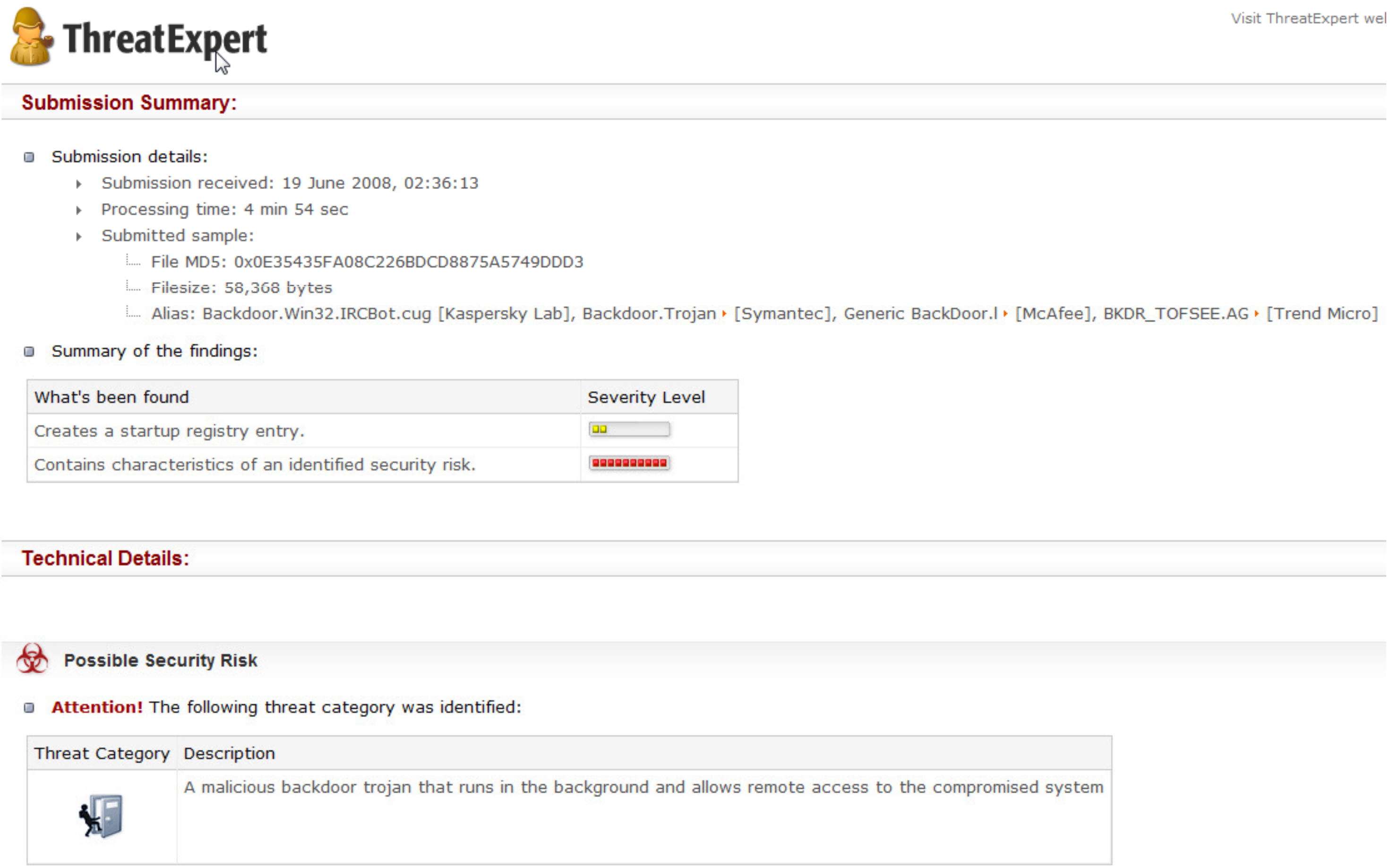
Scanned file: winadll.exe - Infected

winadll.exe - infected by Trojan.Win32.Agent.awz

http://www.kaspersky.com/scanforvirus

Online Resources - ThreatExpert

- Does a lot of the analysis work for you.



Visit ThreatExpert wel

Submission Summary:

- Submission details:
  - Submission received: 19 June 2008, 02:36:13
  - Processing time: 4 min 54 sec
  - Submitted sample:
    - File MD5: 0x0E35435FA08C226BDCD8875A5749DDD3
    - Filesize: 58,368 bytes
    - Alias: Backdoor.Win32.IRCBot.cug [Kaspersky Lab], Backdoor.Trojan [Symantec], Generic BackDoor.l [McAfee], BKDR_TOFSEE.AG [Trend Micro]
- Summary of the findings:

What's been found	Severity Level
Creates a startup registry entry.	🟨🟨
Contains characteristics of an identified security risk.	🟥🟥🟥🟥🟥🟥🟥🟥🟥🟥

Technical Details:

Possible Security Risk

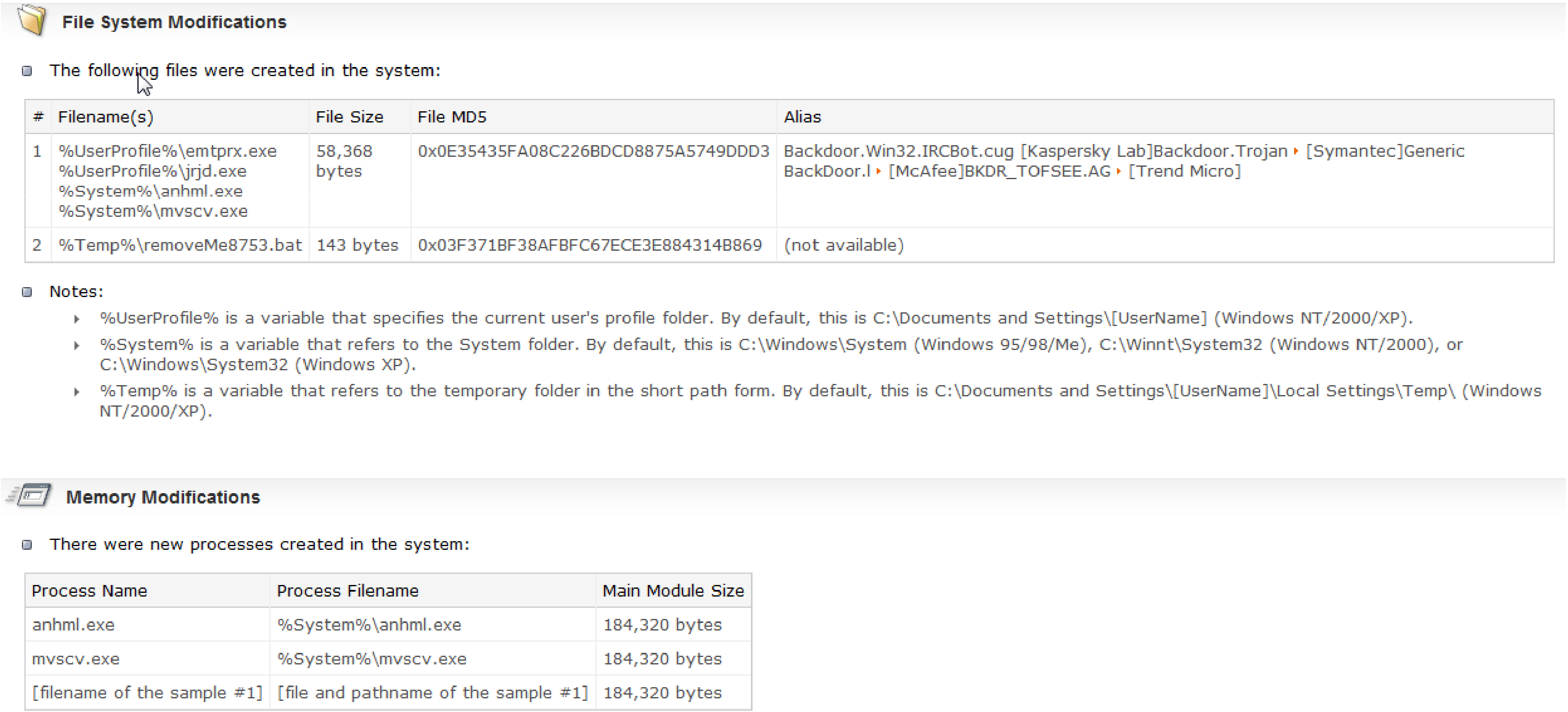
- **Attention!** The following threat category was identified:

Threat Category	Description
	A malicious backdoor trojan that runs in the background and allows remote access to the compromised system

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

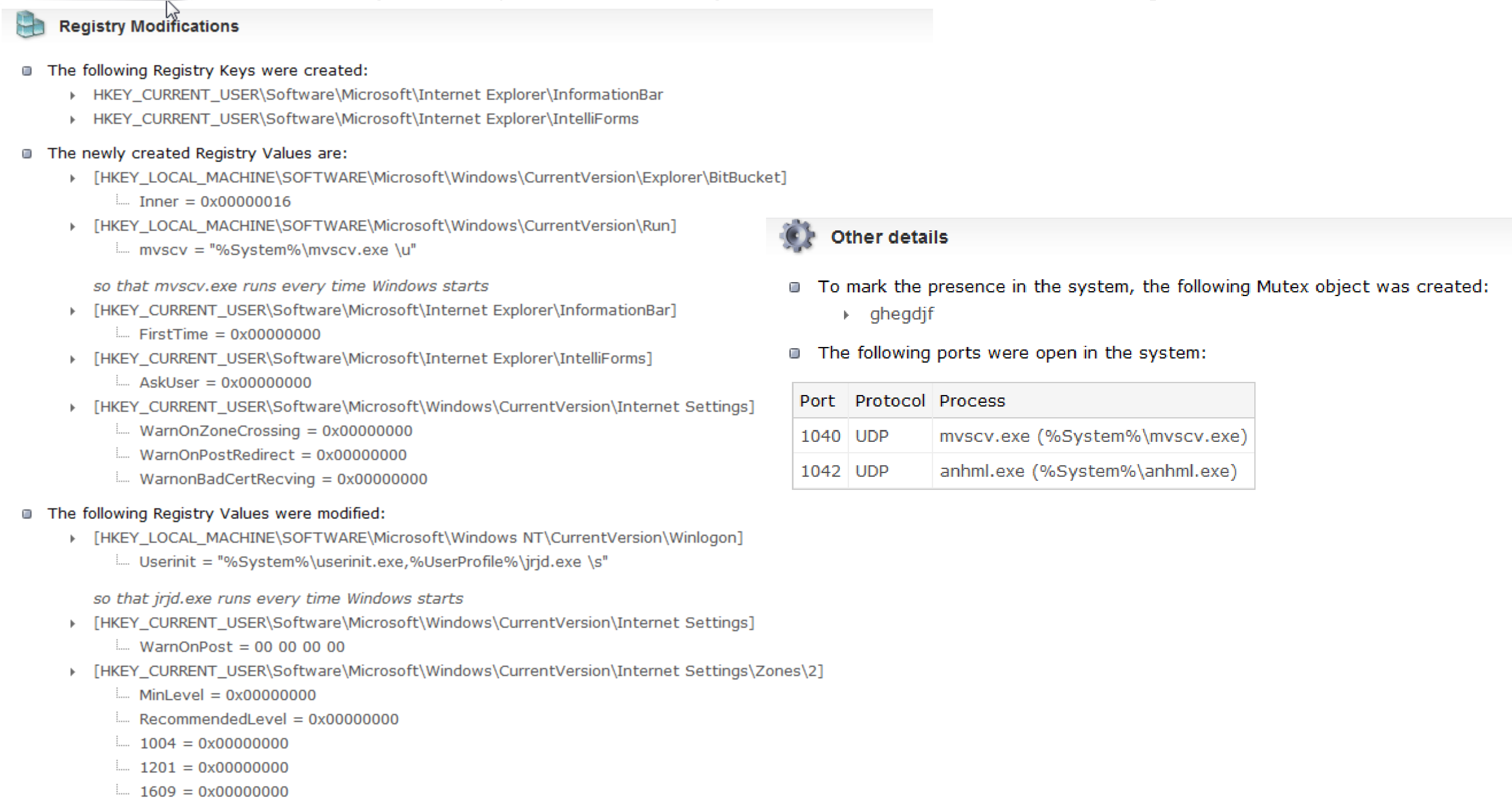
- There were new processes created in the system:

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.

```
ERROR: undefined
OFFENDING COMMAND: ‘~

STACK:
```