Malcode Analysis Techniques for Incident Handlers

Russ McRee        holisticinfosec.org
Seattle Secureworld Expo 2007

© Russ McRee - HolisticInfoSec.org
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
  - IDS & Firewall logs
IDENTIFICATION PHASE

Where’s Waldo?
Mandiant Red Curtain

- 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.”
• 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.
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. [1]
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:

- 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:

Don’t just look for the pretty red alert with a high score, look at entry point sigs and anomaly counts.
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.
## Network module results - fport:

<table>
<thead>
<tr>
<th>Pid</th>
<th>Process</th>
<th>Port</th>
<th>Protocol</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>908</td>
<td>svchost</td>
<td>135</td>
<td>TCP</td>
<td>C:\WINDOWS\system32\svchost.exe</td>
</tr>
<tr>
<td>4</td>
<td>System</td>
<td>139</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>System</td>
<td>443</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>1056</td>
<td>svchost</td>
<td>1025</td>
<td>TCP</td>
<td>C:\WINDOWS\system32\svchost.exe</td>
</tr>
<tr>
<td>4</td>
<td>System</td>
<td>1030</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>1964</td>
<td>Explorer</td>
<td>1798</td>
<td>TCP</td>
<td>C:\WINDOWS\explorer.exe</td>
</tr>
<tr>
<td>1964</td>
<td>Explorer</td>
<td>1799</td>
<td>TCP</td>
<td>C:\WINDOWS\explorer.exe</td>
</tr>
<tr>
<td>820</td>
<td>winadll</td>
<td>1813</td>
<td>TCP</td>
<td>C:\WINDOWS\system32\winadll.exe</td>
</tr>
<tr>
<td>1264</td>
<td></td>
<td>5000</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>System</td>
<td>133</td>
<td>UDP</td>
<td>C:\WINDOWS\system32\svchost.exe</td>
</tr>
<tr>
<td>0</td>
<td>System</td>
<td>137</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>System</td>
<td>138</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>System</td>
<td>445</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>1056</td>
<td>svchost</td>
<td>500</td>
<td>UDP</td>
<td>C:\WINDOWS\system32\svchost.exe</td>
</tr>
<tr>
<td>4</td>
<td>System</td>
<td>1026</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>1964</td>
<td>Explorer</td>
<td>1033</td>
<td>UDP</td>
<td>C:\WINDOWS\explorer.exe</td>
</tr>
<tr>
<td>1964</td>
<td>Explorer</td>
<td>1397</td>
<td>UDP</td>
<td>C:\WINDOWS\explorer.exe</td>
</tr>
<tr>
<td>820</td>
<td>winadll</td>
<td>1398</td>
<td>UDP</td>
<td>C:\WINDOWS\system32\winadll.exe</td>
</tr>
<tr>
<td>1264</td>
<td></td>
<td>1399</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>System</td>
<td>1400</td>
<td>UDP</td>
<td></td>
</tr>
<tr>
<td>1964</td>
<td>Explorer</td>
<td>1401</td>
<td>UDP</td>
<td>C:\WINDOWS\explorer.exe</td>
</tr>
<tr>
<td>1964</td>
<td>Explorer</td>
<td>1417</td>
<td>UDP</td>
<td>C:\WINDOWS\explorer.exe</td>
</tr>
<tr>
<td>820</td>
<td>winadll</td>
<td>1418</td>
<td>UDP</td>
<td>C:\WINDOWS\system32\winadll.exe</td>
</tr>
<tr>
<td>0</td>
<td>System</td>
<td>1900</td>
<td>UDP</td>
<td></td>
</tr>
</tbody>
</table>

Execute Duration (in seconds)=1
# RAPIER 3.2 - Client

## SecCheck module results – Process List:
- Confirms what we saw in Process Explorer.

<table>
<thead>
<tr>
<th>Process List:</th>
</tr>
</thead>
<tbody>
<tr>
<td>PID</td>
</tr>
<tr>
<td>PID</td>
</tr>
<tr>
<td>PID</td>
</tr>
<tr>
<td>PID</td>
</tr>
<tr>
<td>PID</td>
</tr>
<tr>
<td>PID</td>
</tr>
</tbody>
</table>
# RAPIER 3.2 - Client

SecCheck module results – TCP/UDP and Run Entries:

## TCP table:

<table>
<thead>
<tr>
<th>PID</th>
<th>0.0.0.0:135</th>
<th>0.0.0.0:445</th>
<th>0.0.0.0:1025</th>
<th>0.0.0.0:1030</th>
<th>0.0.0.0:1798</th>
<th>0.0.0.0:1799</th>
<th>0.0.0.0:1813</th>
<th>192.168.101.129:139</th>
<th>192.168.101.129:1798</th>
<th>192.168.101.129:1799</th>
<th>192.168.101.129:1811</th>
<th>192.168.101.129:1900</th>
</tr>
</thead>
<tbody>
<tr>
<td>PID</td>
<td>908</td>
<td>4</td>
<td>1056</td>
<td>4</td>
<td>1964</td>
<td>1964</td>
<td>820</td>
<td>1264</td>
<td>1264</td>
<td>1964</td>
<td>1964</td>
<td>1264</td>
</tr>
<tr>
<td>PID</td>
<td>908</td>
<td>0.0.0.0:135</td>
<td>0.0.0.0:445</td>
<td>0.0.0.0:1025</td>
<td>0.0.0.0:1030</td>
<td>0.0.0.0:1798</td>
<td>0.0.0.0:1799</td>
<td>0.0.0.0:1813</td>
<td>192.168.101.129:139</td>
<td>192.168.101.129:1798</td>
<td>192.168.101.129:1799</td>
<td>192.168.101.129:1811</td>
</tr>
<tr>
<td>PID</td>
<td>908</td>
<td>LISTENING</td>
<td>LISTENING</td>
<td>LISTENING</td>
<td>LISTENING</td>
<td>LISTENING</td>
<td>LISTENING</td>
<td>LISTENING</td>
<td>LISTENING</td>
<td>LISTENING</td>
<td>LISTENING</td>
<td>LISTENING</td>
</tr>
<tr>
<td>PID</td>
<td>908</td>
<td>/* Service */</td>
<td>/* Service */</td>
<td>/* Service */</td>
<td>/* Service */</td>
<td>/* Service */</td>
<td>/* Service */</td>
<td>/* Service */</td>
<td>/* Service */</td>
<td>/* Service */</td>
<td>/* Service */</td>
<td>/* Service */</td>
</tr>
<tr>
<td>PID</td>
<td>908</td>
<td>C:\WINDOWS\system32\svchost.exe</td>
<td>C:\WINDOWS\system32\svchost.exe</td>
<td>C:\WINDOWS\System32\svchost.exe</td>
<td>C:\WINDOWS\system32\svchost.exe</td>
<td>C:\WINDOWS\Explorer.EXE</td>
<td>C:\WINDOWS\Explorer.EXE</td>
<td>C:\WINDOWS\system32\winadll.exe</td>
<td>C:\WINDOWS\system32\svchost.exe</td>
<td>C:\WINDOWS\Explorer.EXE</td>
<td>C:\WINDOWS\Explorer.EXE</td>
<td>C:\WINDOWS\system32\winadll.exe</td>
</tr>
</tbody>
</table>

## UDP table:

<table>
<thead>
<tr>
<th>PID</th>
<th>0.0.0.0:135</th>
<th>0.0.0.0:445</th>
<th>0.0.0.0:1025</th>
<th>0.0.0.0:1030</th>
<th>0.0.0.0:1798</th>
<th>0.0.0.0:1799</th>
<th>0.0.0.0:1813</th>
<th>192.168.101.129:139</th>
<th>192.168.101.129:1798</th>
<th>192.168.101.129:1799</th>
<th>192.168.101.129:1811</th>
<th>192.168.101.129:1900</th>
</tr>
</thead>
<tbody>
<tr>
<td>PID</td>
<td>908</td>
<td>4</td>
<td>1056</td>
<td>4</td>
<td>1964</td>
<td>1964</td>
<td>820</td>
<td>1264</td>
<td>1264</td>
<td>1964</td>
<td>1964</td>
<td>1264</td>
</tr>
<tr>
<td>PID</td>
<td>908</td>
<td>0.0.0.0:135</td>
<td>0.0.0.0:445</td>
<td>0.0.0.0:1025</td>
<td>0.0.0.0:1030</td>
<td>0.0.0.0:1798</td>
<td>0.0.0.0:1799</td>
<td>0.0.0.0:1813</td>
<td>192.168.101.129:139</td>
<td>192.168.101.129:1798</td>
<td>192.168.101.129:1799</td>
<td>192.168.101.129:1811</td>
</tr>
<tr>
<td>PID</td>
<td>908</td>
<td>/* Service */</td>
<td>/* Service */</td>
<td>/* Service */</td>
<td>/* Service */</td>
<td>/* Service */</td>
<td>/* Service */</td>
<td>/* Service */</td>
<td>/* Service */</td>
<td>/* Service */</td>
<td>/* Service */</td>
<td>/* Service */</td>
</tr>
<tr>
<td>PID</td>
<td>908</td>
<td>C:\WINDOWS\system32\svchost.exe</td>
<td>C:\WINDOWS\system32\svchost.exe</td>
<td>C:\WINDOWS\System32\svchost.exe</td>
<td>C:\WINDOWS\system32\svchost.exe</td>
<td>C:\WINDOWS\Explorer.EXE</td>
<td>C:\WINDOWS\Explorer.EXE</td>
<td>C:\WINDOWS\system32\winadll.exe</td>
<td>C:\WINDOWS\system32\svchost.exe</td>
<td>C:\WINDOWS\Explorer.EXE</td>
<td>C:\WINDOWS\Explorer.EXE</td>
<td>C:\WINDOWS\system32\winadll.exe</td>
</tr>
</tbody>
</table>

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

- "VMware Tools" = 'C:\Program Files\VMware\VMware Tools\VmmareTray.exe'
- "VMware User Process" = 'C:\Program Files\VMware\VMware Tools\VmmareUser.exe'
- "WinPatrol" = 'C:\Program Files\B11P Studios\WinPatrol\Winpatrol.exe'
- "Display Device Driver" = 'vwinadll.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 to vendors.
Online Resources - Virustotal

- Virustotal – most analysts are familiar with this service [http://www.virustotal.com/](http://www.virustotal.com/)

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...](http://www.virustotal.com/)

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Version</th>
<th>Last Update</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>AhnLab-V3</td>
<td>2007.10.27.0</td>
<td>2007.10.26</td>
<td>Win-Trojan-Agent.183296.7</td>
</tr>
<tr>
<td>AntiVax</td>
<td>7.6.0.30</td>
<td>2007.10.26</td>
<td>Hora/Geobot.183296.3</td>
</tr>
<tr>
<td>Authenium</td>
<td>4.95.8</td>
<td>2007.10.28</td>
<td>U32/Trojan.BVZ</td>
</tr>
<tr>
<td>Avast</td>
<td>4.7.1074.0</td>
<td>2007.10.28</td>
<td>Unihii-Agent-XXR</td>
</tr>
<tr>
<td>AVG</td>
<td>7.5.0.503</td>
<td>2007.10.28</td>
<td>SShoc.FQO</td>
</tr>
<tr>
<td>BitDefender</td>
<td>7.2</td>
<td>2007.10.28</td>
<td>BackDoor.Agent.T9S</td>
</tr>
<tr>
<td>CAT-Quick Heal</td>
<td>9.00</td>
<td>2007.10.26</td>
<td>Trojan.Agent.ezw</td>
</tr>
<tr>
<td>ClamAV</td>
<td>0.91.2</td>
<td>2007.10.28</td>
<td>Trojan.Dropper.2276</td>
</tr>
<tr>
<td>DoWeb</td>
<td>4.44.0.09170</td>
<td>2007.10.28</td>
<td>Trojan.MailDrop.0379</td>
</tr>
<tr>
<td>E-Safe</td>
<td>7.0.15.0</td>
<td>2007.10.28</td>
<td></td>
</tr>
<tr>
<td>eTrust-Vet</td>
<td>31.2.5244</td>
<td>2007.10.26</td>
<td>Win32/Bot.HVL</td>
</tr>
<tr>
<td>Ewido</td>
<td>4.0</td>
<td>2007.10.28</td>
<td></td>
</tr>
<tr>
<td>FileAdvisor</td>
<td>1</td>
<td>2007.10.20</td>
<td>High threat detected</td>
</tr>
<tr>
<td>Fortinet</td>
<td>3.11.0.0</td>
<td>2007.10.19</td>
<td>U32/Agent.AWZ1cz</td>
</tr>
<tr>
<td>F-Prot</td>
<td>4.3.2.40</td>
<td>2007.10.26</td>
<td>U32/Trojan.BVZ</td>
</tr>
</tbody>
</table>

© Russ McRee - HolisticInfoSec.org
Online Resources - Jotti

- When Virustotal’s load is too high, try Jotti (although Virustotal rebuilt recently and handles high demand well now): [http://virusscan.jotti.org/](http://virusscan.jotti.org/)

![Jotti's malware scan interface](image)
Online Resources - Kaspersky

• If you just want a quick, single source ID, try Kaspersky:
http://www.kaspersky.com/scanforvirus

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

Browse... | Submit

Scanned file: winadll.exe - Infected
winadll.exe - infected by Trojan.Win32.Agent.awz
ANALYSIS PHASE

Who’s Waldo?
Analysis cautions

- Sandbox the analysis phase!
- Avoid your corporate network.
- VMWare is great only if the malware isn’t virtualization-aware (becoming a prevalent issue).
- Only one non-commercial tool seems to avoid the virtualization issues.
  - Joe Stewart’s Truman, not for the timid or easily deterred as it unsupported and version 0.1.
- My host OS in typically Linux or Mac OS X, and I run Windows as a guest OS.
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.
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

• Report findings

<table>
<thead>
<tr>
<th>Monitored RegKeys</th>
<th>Registry Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>File: windll.exe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Size: 184320 Bytes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MDS: F08EFPDDCE5C29905562190F27B2E145DF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packer: File not found C:\iDEFENSE\SysAnalyzer\pcid.exe</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

File Properties: CompanyName
FileVersion
ProductName
ProductVersion

Exploit Signatures:

<table>
<thead>
<tr>
<th>Scanning for 49 signatures</th>
</tr>
</thead>
<tbody>
<tr>
<td>*** Found: RPC DCOM Exploit MS03-026</td>
</tr>
<tr>
<td>*** Found: Iis650s exploit - MS04-011</td>
</tr>
<tr>
<td>*** Found: Spreads Via Weak Passwords in MSSQL Server</td>
</tr>
<tr>
<td>*** Found: CA License Client Overflow v1.61</td>
</tr>
<tr>
<td>Scan Complete: 1196Kb in 0.062 seconds</td>
</tr>
<tr>
<td>Urls</td>
</tr>
</tbody>
</table>

RegKeys

Software\BioWare\Neverwinter
Software\Activision\Soldier of Fortune II - Double Helix
Software\Illusion Softworks\Hidden & Dangerous 2
Software\Teclan\Chrome
Software\Westwood\NOK
Software\Westwood\Red Alert 2
Software\Westwood\Red Alert
Software\Westwood\Tiberian Sun
Software\Red Storm Entertainment\RAVERSHEILD
Software\Electronic Arts\EA Sports\Nascar Racing 2003\ergc
Software\Electronic Arts\EA Sports\Need For Speed Underground\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\ergc
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

© Russ McRee - HolisticInfoSec.org
Malcode Analysis Software Tools – iDefense Labs

• Report findings (2)

ExeRefs

File: wincd11_dmp.exe
WinIP Professional [universal] lsass.exe
SOFTWARE\Microsoft\Windows\Shell\exe
explorer.exe
cmd.exe
wincd11.exe
wincd11.exe
ftp.exe
com.execute
%ls%exe
kill.exe
run.exe
rundll32.exe
d3dmpdsxe.exe
date.exe
ssate.exe
winsys.exe
winup.exe
SysMon.exe
bbsq.exe
Penis32.exe
msvcr32.exe
ssf.exe
PandaAVEngine.exe
F-AGOBOT.EXE
HIJACKTHIS.EXE
AVP.EXE
AVPCC.EXE
AVP32.EXE
ZONEALARM.EXE
ZONALARM2601.EXE
ZATUTOR.EXE
ZAPSETUP3001.EXE
ZAPRO.EXE
XPF202EN.EXE
UUVERNUSEXFW.EXE
WUPDT.EXE
WUPDATER.EXE
WSCBATE.EXE
WRCCTRL.EXE
WRADMIN.EXE
WNT.EXE
UNAD.EXE
Hook, line, and sinker...

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

- Hmm...am I a P2P Storm bot variant?
Malcode Analysis Software Tools – iDefense Labs

- Malcode Analysis Pack
- The value of hashing.
Malcode Analysis Software Tools – iDefense Labs

• Malcode Analysis Pack
  • Take the resulting MD5 output and search for it.

DISOG
They are sticking with the static MD5 sum of \texttt{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: \texttt{c05893a656b54164fb486028309bd89e} SHA1 Fingerprint:
8ad5096547710d61a6ac0613fdb1d290911f8e600. HTTP/1.1 200 OK Date: Sun, ...
www.castlecops.com/eCard_malware2641.html - Similar pages
Malcode Analysis Software Tools – iDefense Labs

Ascii Strings:

```
!This program cannot be run in DOS mode.
Rich
  text
    .rdata
  .data

KERNEL32.dll
t (ddos.a)
  Done with flood (%1KB/sec).
t (ddos.a)
  Send error: <%d>.
ddos random
ddos.sack
ddos.syn
t (icmp.a)
  Done with %s flood to IP: %s. Sent: %d packet(s) @ %dKB/sec (%dMB).
t (icmp.a)
  Error sending packets to IP: %s. Packets sent: %d. Returned: <%d>.
t (icmp.a)
  Invalid target IP.
t (icmp.a)
  Error: setsockopt() failed. returned: <%d>.
t (tcp.m)
  Error: setsockopt() failed. returned: <%d>.

[SUPERSYN]: Done with flood (%1KB/sec)
t (syn.a)
  Done with flood (%1KB/sec).
t (syn.a)
  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>.

q-gold
PayPal
StormFay
Vodafone
Poste Italiane
eBay
Yahoo!
Banco Sella
Email
Bank of America
exploit
Benvenuto a gail
```
Malcode Analysis Software Tools – iDefense Labs

Malcode Analysis Pack – Strings (2)

- What functionality do we see here?
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.
Wireshark

- Don’t forget the old standby!
- Tons of information in ye olde packet capture
- Follow TCP Stream is your friend.
Malicious delivery: accepted

Follow TCP Stream

Stream Content:

220 SCHDC.schombek.com Microsoft ESMTP MAIL Service, Version: 3.0.2195.6713 ready at Tue, 3 Jul 2007 01:42:00 -0400
250 SCHDC.schombek.com Hello [70-58-89-136]
MAIL From:<csh@alliedcontrol.com>
250 2.1.0 csh@alliedcontrol.com...Sender_OK
RCPT To:<stevens@schombek.com>
250 2.1.3 Stevens@Schombek.com
DATA
354 Start mail input; end with <CRLF><CRLF>
Received: from rvoog.ky ([65.68.52.200]) by 70-58-89-136.tukw.qwest.net with Microsoft SMTPSVC
(3.0.2195.6229); Mon, 2 Jul 2007 22:39:54 -0700
Message-ID: <6015f2c78d26f952f39af0824441ervog.ky>
From: "postcards.org" <csh@alliedcontrol.com>
To: <stevens@schombek.com>
Subject: You've received a greeting postcard from a school mate!
Date: Mon, 2 Jul 2007 22:39:54 -0700
MIME-Version: 1.0
Content-Type: text/plain;
  format=flowed;
  charset="windows-1252";
  reply-type=original
  Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MMMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.50.4522.1200
X-MimeOLE: Produced By Microsoft MimeOLE v5.50.4522.1200

Good day:
Your school mate has sent you a greeting postcard from postcards.org.

Send free ecards from postcards.org with your choice of colors, words and music.

Your ecard will be available with us for the next 30 days. If you wish to keep
the ecard longer, you may save it on your computer or take a print.

To view your ecard, choose from any of the following options:

-------------------
OPT1
-------------------

Click on the following Internet address or
copy & paste it into your browser's address box.
http://67.193.74.68/55456ec290b516c3c2cd3a7c0658e47
Malicious delivery: rejected
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...
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!
References

- Mandiant Red Curtain [http://mandiant.com/mrc](http://mandiant.com/mrc)