Incident Handling around the world in 80 ms. (Well not really that fast...)

Steve Mancini
Greg Bassett
with special guest star...

Russ McRee
The opinions expressed in this presentation are those of the authors (or at least the one talking) and do not reflect the opinions of our employers.

Any resemblance to real persons living, dead or undead is purely coincidental. No animals were harmed in the making of this presentation or program.

Any resemblance to any place in cyberspace is entirely coincidental.

No other warranty expressed or implied.

Contents may settle during shipment.

Void where prohibited by law.

Some assembly required.

Batteries not included.

Use only as directed.
• Brief Explanation: What is RAPIER
• Establishing a RAPIER results repository
• Coffee Break
• RAPIER Module Writing 101
• Module Analysis Deep Dive
• Feature Requests / Feedback
To avoid redundancy and for the sake of time we are avoiding explaining things:

– Order of Volatility
– Definitions of “forensically sound”

Hopefully you all had the opportunity to attend Par’s and Russ’ presentation on Monday; they did a great job covering this content. Yes they stole my thunder 😊
WHAT IS RAPIER
• Modular
• Stand Alone
• Client / Server
• Automated
• Configurable
• Expandable
• CLI
• FREE
Why would I need it?

• The worst time to learn how to acquire information from a system is *during the incident.*
• Expertise does not scale (to most enterprise environments)
• Not everyone knows how to acquire the requested information
• Not everyone acquires it in the same fashion
• Common (1st) responses may trample valuable information
  — Run Scanners, Patch System, Update Apps
RAPIER Output

**Volatile Information**
- complete list of running processes
- locations of those processes on disk
- ports those processes are using
- Checksums for all running processes
- Dump memory for all running processes
- All DLLS currently loaded and their checksum
- Capture last Modify/Access/Create times for designated areas
- All files that are currently open
- Net (start/share/user/file/session)
- Output from nbtstat and netstat
- Document all open shares/exports on system
- Capture current routing tables
- list of all network connections
- Layer3 traffic samples
- capture logged in users

**Static Information**
- System Name
- Basic system info (peripherals, BIOS, drivers, etc)
- System Startup Commands
- MAC address
- List of installed services
- Local account and policy information
- Current patches installed on system
- Current AV versions
- Files with alternate data streams
- Discover files marked as hidden
- List of all installed software on system (known to registry)
- Capture system logs
- Capture of AV logs
- Copies of application caches (temporary internet files) – IE, FF, Opera
- Export entire registry
- Search/retrieve files based on search criteria.
“Forensically Sound?”

Topic has come up.

Some say yes...
Some say no...
Some say HELL NO!

“Forensics Integrity Check” option exists.
RAPIER SERVER
RAPIER Workflow

1. Download RAPIER Zip File
2. Run RAPIER
3. Results Upload
4. Analyst retrieves Results
5. Results Analysis

Suspect Machine
RAPIER Server
RAPIER Results Storage
RAPIER Analyst
RAPIER Report
Considerations

• Audience has fundamental understanding of system administration and web server setup is assumed...

• Non-denominational OS Disclaimer
  – The following configuration focuses on a Windows server running WAMP
  – Does **not** have to be Windows/WAMP!
  – Web server **is** necessary (WAMP, LAMP, IIS)
  – Web written in PHP, can be done in .NET

• Web Server with at least 20GB
Storage

• RAPIER results size depends on modules run
  – Average Fast Scan dump ~ 15MB
  – Add File capture, WebCache ~ 1GB
  – Physical Memory Dump – size of memory - ~1 GB+
  – Recommend at least 20 GB for typical usage
  – Need to size according to site use

• Website
  – Small size ~300 MB
  – RAPIER executables, web support files
• RAPIER_Analysts group access to RAPIER_Results directory
• RAPIER_Dev group access for module configs and updates
Notifications

- Client and Server utilize blat to send email
- RAPIER Results Notification
  - Sent from Client, configured in RAPIER.conf
  - Notification that Results file was uploaded
- Upload Notification
  - Sent from Server, configured in index.php
  - Notification that Malware sample was uploaded
Firewall

- **Web server**
  - Port 80 – RAPIER Zip download
  - Defined port (8010) – RAPIER to server communications (Results file upload)
    - Separate port configured to provide functionality during port 80 malware outbreak
- **Results**
  - File share- port 445
  - SFTP- port 22
- **Notifications**
  - SMTP- port 25
- **RDP**
  - Port 3389
Web Functionality

• RAPIER Zip File
  – Provides download of Zip file
• RAPIER User guides
  – Provides download of User guides
• RAPIER Results Uploads
  – Provides upload support to RAPIER_Results
• Sample Uploads
  – Provides upload support for Malware found during RAPIER analysis
RAPIER
Rapid Assessment & Potential Incident Examination Report

RAPIER For Windows
Download RAPIER 3.1 Engine Only (1.3 MB)
Download RAPIER 3.1 Engine + all current modules (22 MB)
Download RAPIER 3.1 User Training in Microsoft PowerPoint Format
Download .NET Framework 1.1 SP1 Installer for all platforms (3.6 MB)
Feeling daring? Try RAPIER 3.2 Alpha 3 Engine + all current modules (18 MB)

RAPIER For Unix
Download RAPIER for UNIX 3.1 (7.9 MB)
RAPIER for UNIX 3.1 User’s Guide in MS PowerPoint Format

Please report Bugs, Issues and Enhancements using rapier-dev@....

If you need to upload non-RAPIER malware samples, please use the following:

File: [blank]  Browse  Upload

http://rapier-releases.RAPIER_3.1_Full.zip
Web Site Directory Structure

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>releases</td>
<td></td>
<td>File Folder</td>
</tr>
<tr>
<td>Results</td>
<td></td>
<td>File Folder</td>
</tr>
<tr>
<td>7za.exe</td>
<td>478 KB</td>
<td>Application</td>
</tr>
<tr>
<td>blat.exe</td>
<td>94 KB</td>
<td>Application</td>
</tr>
<tr>
<td>blat.log</td>
<td>11 KB</td>
<td>Text Document</td>
</tr>
<tr>
<td>checksum.php</td>
<td>5 KB</td>
<td>PHP File</td>
</tr>
<tr>
<td>CurrentVersionSHA1.txt</td>
<td>1 KB</td>
<td>Text Document</td>
</tr>
<tr>
<td>DotNetFW_Install.zip</td>
<td>40,512 KB</td>
<td>WinZip File</td>
</tr>
<tr>
<td>GenerateFullZIP.cmd</td>
<td>1 KB</td>
<td>Windows Command ...</td>
</tr>
<tr>
<td>GenerateFullZIP.vbs</td>
<td>16 KB</td>
<td>VBScript Script File</td>
</tr>
<tr>
<td>index.php</td>
<td>13 KB</td>
<td>PHP File</td>
</tr>
<tr>
<td>RAPIER 3.1 User Training.ppt</td>
<td>691 KB</td>
<td>PPT File</td>
</tr>
<tr>
<td>RAPIER 3.2 Server Setup.txt</td>
<td>4 KB</td>
<td>Text Document</td>
</tr>
<tr>
<td>RAPIER 3.2 User Training.ppt</td>
<td>721 KB</td>
<td>PPT File</td>
</tr>
<tr>
<td>RAPIER for UNIX 3.1 Users Guide.ppt</td>
<td>513 KB</td>
<td>PPT File</td>
</tr>
<tr>
<td>RAPIER.jpg</td>
<td>14 KB</td>
<td>JPEG Image</td>
</tr>
<tr>
<td>sha1sum.exe</td>
<td>54 KB</td>
<td>Application</td>
</tr>
<tr>
<td>test.html</td>
<td>1 KB</td>
<td>HTML Document</td>
</tr>
<tr>
<td>version.php</td>
<td>2 KB</td>
<td>PHP File</td>
</tr>
</tbody>
</table>
Web Server Setup

• Install Web Server
• Install RAPIER Web Site
• Create/Share Results directory
• Configure Web Server
• Configure RAPIER
• Scheduled Tasks
• Testing
Web Server/Site Install

• Install WAMP/LAMP/IIS
  – WAMP5 Server 1.7.x or newer
  – MySQL is disabled!
• Install RAPIER Web site files
  – Web page, releases, user guides
Results Directory

• Create results directory
  – D:\wamp\www\RAPIER_results

• Configure access\sharing for RAPIER_Analysts
  – Windows File Sharing
  – Secure FTP
  – Secure Web hosting /directory browsing enabled
Configure httpd.conf

- **Listening Ports**
  - "Listen" line includes port 80 and port 8010
- **Add results directory paths below web root**
  - Alias /results "D:/wamp/www/results"
  - <Directory "D:/wamp/www/results">
- **Change Web Root defaults**
  - Allow/Deny for the web root to "Allow from all"
  - Remove "Indexes"
- **DAV Support**
  - Uncomment the following two modules:
    - LoadModule dav_module modules/mod_dav.so
    - LoadModule dav_fs_module modules/mod_dav_fs.so
Configure index.php

- **Target Path**
  - `$target_path="d:\wamp\www\Results";`
- **SMTP Server**
  - `$StrSMTPServer="my.smtp.server";`
- **Upload Notifications**
  - `$StrEmailAddressFrom="Malware.Samples@myorg";`
  - `$StrEmailAddressTo="RAPIER.Results.Notifications@myorg";`
  - `$StrEmailAddressCC="";`
  - `$StrEmailAddressBCC="";`
  - `$StrSubject="Malware Sample Upload Notification";`
- **Embedded Notification Information**
  - `$StrSampleLocation="\\RAPIERServer\\RAPIER_Results\\";`
  - `$StrHelpContact="";`
Configure RAPIER.conf

- Configuration of RAPIER.conf on server copy
  - Zip file created for distribution
- URLs
  - Define Base URL
    - RAPIERBaseURL=http://RAPIERURL:8010
  - Define Results URL
    - UploadURL=<RAPIERBaseURL>/Results/
- SMTP Server
  - Define SMTP server
    - SMTPServer=my.smtp.server
• Results Notifications
  – Required values
    • EmailFrom=RAPIER.Results@myorg
    • EmailTo=RAPIER.Results.Notification@myorg
      – EmailTo needs to be a valid address
  – Optional values
    • EmailCC=
    • EmailBCC=

• Embedded Results Information
  – Where results were loaded
    • SampleLocation=\\RAPIERServer\RAPIER_Results\n  – Who to contact for help
    • HelpContact=
Configure proxy.conf

- Modules that require a connection to the network
- AutoProxyURL=http://autoproxy:nnnn
- ProxyServer=proxy:nnn
Scheduled Tasks

• Need to keep AV DAT and MBSA CAB files updated
  – Modules\Special\ClamAVScan\Module.cmd updateDATonly – 2 hours
  – Modules\Special\McAfeeVirusScan\Module.cmd updateDATonly" - 2 hours
  – Modules\Fast\MBSA\Module.cmd updateCABonly" – Daily

• Need to keep RAPIER Zip file current
  – GenerateFullZIP.cmd – 10 minutes
• Results share
  – Determine policy/retention time for results
• Monitor Scheduled tasks
  – Tasks run as required- DATs get updated
• Other Server tasks
  – Monitor disk space, server availability
  – Patching, etc
Server Testing

- **http://RAPIERserver** – URL available?
  - Web server running, port blocked?
- Download RAPIER ZIP
  - ZIP file in releases directory?
- Run RAPIER with a few modules- runs with no errors?
  - Check .Net package, files extracted from ZIP
- Results upload with no errors
  - Web Server configuration
- Verify Results email – results email received?
  - SMTP/Notification settings, port blocked?
- Scheduled Tasks – do they run?
  - Proxy settings
Digression
MODULE CREATION
Module Architecture

- Based on VBScript
- RAPIER.vbi is a large library of VBScript functions to reference
- Modules can have individual conf files to allow for end user configuration
- Modules are stand alone
  - Can be added/removed/modified at will
  - Allows for independent development/testing
Module Creation

1. Find a cool tool you want to incorporate
2. Understand that tool’s CLI
3. Wrap
4. Test
5. Incorporate
A lot of discussions about prefetch lately.

Harlan Carvey has a great write up:
http://windowsir.blogspot.com/2007/05/prefetch-analysis.html

MiTec has created a tool called wfa (Windows File Analysis) that reports out about prefetch
http://www.mitec.cz/wfa.html

Dominik Jain has written a tool to mirror a directory.
http://home.in.tum.de/~jain/

We have everything we need...
## C:\Windows\Prefetch

### File and Folder Tasks
- Make a new folder
- Publish this folder to the Web
- Share this folder

### Other Places

### Details

Name | Size | Type | Date Modified
--- | --- | --- | ---
7ZA.EXE-2357570B.pf | 22 KB | PF File | 6/18/2008 9:37 PM
ACFNF5.EXE-0C7B39DE.pf | 29 KB | PF File | 6/24/2008 11:43 AM
ACMAINSUI.EXE-112BEB16.pf | 46 KB | PF File | 6/24/2008 11:46 AM
ACRORD32.EXE-355875A2.pf | 62 KB | PF File | 6/24/2008 12:24 PM
ACRORD32INFO.EXE-24548733.pf | 71 KB | PF File | 6/24/2008 2:30 PM
ACTRAY.EXE-2FEB36C3.pf | 21 KB | PF File | 6/24/2008 2:01 PM
ACCLICON.EXE-3ADBE191.pf | 20 KB | PF File | 6/24/2008 2:01 PM
ADOBEUPDATER.EXE-1AB51BCE.pf | 38 KB | PF File | 6/24/2008 11:40 AM
AGENTLOGGER.EXE-045CAAF5.pf | 17 KB | PF File | 6/24/2008 11:40 AM
AGENTSRV.EXE-04301287.pf | 11 KB | PF File | 6/24/2008 11:40 AM
AHV.EXE-1021AAF7.pf | 46 KB | PF File | 6/19/2008 3:26 PM
BEESVENTIU.EXE-13FA5318.pf | 37 KB | PF File | 6/24/2008 11:36 AM
CBSYSTRAY.EXE-2C9881A9.pf | 13 KB | PF File | 6/24/2008 2:01 PM
CMD.EXE-067B4001.pf | 15 KB | PF File | 6/23/2008 2:45 PM
CIBACKUP.EXE-2F7A6CC43.pf | 79 KB | PF File | 6/24/2008 11:40 AM
COMMUNICATOR.EXE-0C59C037.pf | 59 KB | PF File | 6/24/2008 2:01 PM
CONF.EXE-1DE08E38.pf | 48 KB | PF File | 6/19/2008 3:16 AM
CSCRIPT.EXE-1C26180C.pf | 50 KB | PF File | 6/20/2008 8:48 AM
CSRSS.EXE-126B63473.pf | 15 KB | PF File | 6/23/2008 10:48 AM
CURL.EXE-042D992B.pf | 20 KB | PF File | 6/18/2008 9:37 PM
DD.EXE-068A974E.pf | 24 KB | PF File | 6/23/2008 2:34 PM
DD.EXE-02529E12.pf | 5 KB | PF File | 6/23/2008 2:27 PM
DEFRAG.EXE-273F131E.pf | 26 KB | PF File | 6/20/2008 12:48 PM
DEXPOT.EXE-25130640.pf | 30 KB | PF File | 6/24/2008 2:01 PM
DFGRMTFS.EXE-263967DF.pf | 105 KB | PF File | 6/24/2008 2:01 PM
DOT1XCFG.EXE-087CDE23.pf | 56 KB | PF File | 6/24/2008 2:01 PM
A lot of discussions about prefetch lately.

Harlan Carvey has a great write up:
http://windowsir.blogspot.com/2007/05/prefetch-analysis.html

MiTec has created a tool called wfa (Windows File Analysis) that reports out about prefetch
http://www.mitec.cz/wfa.html

Dominik Jain has written a tool to mirror a directory.
http://home.in.tum.de/~jain/

We have everything we need...
C:\Windows\Prefetch
A lot of discussions about prefetch lately.

Harlan Carvey has a great write up:
http://windowsir.blogspot.com/2007/05/prefetch-analysis.html

MiTec has created a tool called wfa (Windows File Analysis) that reports out about prefetch
http://www.mitec.cz/wfa.html

Dominik Jain has written a tool to mirror a directory.
http://home.in.tum.de/~jain/

We have everything we need...
First things first

Understand the output of the program:

```
C:\Documents and Settings\smancini>"C:\Documents and Settings\smancini\My Documents\Projects\RAPIER\Presentations\External\2008 06 FIRST Geekzone\Demo\Mirror.exe"

Mirror v1.30 (C) 2001-2002 by Dominik Jain

usage: mirror [source directory] [destination directory]

Mirror will make an exact copy of the source directory in the destination directory - including all subdirectories. The destination directory must exist already. Existing files will only be overwritten if necessary. Files or directories in the destination directory that don’t exist in the source will be deleted.

Returns 0 on success, 1 on error.

C:\Documents and Settings\smancini>.
```
• Easiest way is to copy another folder with like output and rework it.
• At minimum you want:
  – Module.cmd - the RAPIER wrapper
  – Module.wsf - the executable wrapper
  – Required_files.txt - what is needed
  – Your executable (in this case mirror.exe)
Define runtime constants:

'Define Constants
Const ModuleName="CmdLines"
Const Description="Determines the command line parameters associated with all running processes"
Const Author="Robbie Bytheway"
Define runtime constants:

'Define Constants
Const ModuleName="CopyPrefetch"
Const Description="Copies all files out of Prefetch directory"
Const Author="Steve Mancini"
Define Variables

'Define Variables
Dim StartTime, EndTime, ExecuteDuration, BitBucket, LogFile, Command

Startime, Endtime, Duration – used to calculate run time
BitBucket – all information written to the logfile
LogFile – defines where the logfile will reside
Command – the command to be executed
'Define Variables
Dim StartTime, EndTime, ExecuteDuration, BitBucket, LogFile, Command, Destination

Destination=CommandLineOptions() & "\" & ModuleName

We will need a destination directory – hence we add it and define it.
Next you want to put the command line in the “Command=“ section.

```plaintext
Command=CurrentWorkingDirectory() & "mirror.exe " & SystemDrive() & "\Windows\Prefetch" "" LogDirectory & "\Prefetch"

BitBucket=DirectoryMake(LogDirectory & "\PreFetch")

BitBucket=RunExternalApplication(Command)
```
Final Touches

Test (and re-test)
Roll into central distribution
Tell your incident handlers about the new module (and how to interpret)

(We’ll be adding prefetch to the distro once we get permission to roll mirror.exe into the bundle)
RAPIER MODULE ANALYSIS
You need to understand your (Microsoft’s) image before you try to analyze what’s going on:

- Systems to compare against = good
- File Integrity hashes = better
- System level integrity hashes = Superb
**Feature Module Output**

**Volatile Information**
- complete list of running processes
- locations of those processes on disk
- ports those processes are using
- Checksums for all running processes
- Dump memory for all running processes
- All DLLS currently loaded and their checksum
- Capture last Modify/Access/Create times for designated areas
- All files that are currently open
- Net (start/share/user/file/session)
- Output from nbtstat and netstat
- Document all open shares/exports on system
- Capture current routing tables
- list of all network connections
- Layer3 traffic samples
- capture logged in users

**Static Information**
- System Name
- Basic system info (peripherals, BIOS, drivers, etc)
- System Startup Commands
- MAC address
- List of installed services
- Local account and policy information
- Current patches installed on system
- Current AV versions
- Files with alternate data streams
- Discover files marked as hidden
- List of all installed software on system (known to registry)
- Capture system logs
- Capture of AV logs
- Copies of application caches (temporary internet files) – IE, FF, Opera
- Export entire registry
- Search/retrieve files based on search criteria.
Module Output

System Configuration
Processes
Networking
Logs & Cache
Files
System Configuration

**Volatile Information**
- complete list of running processes
- locations of those processes on disk
- ports those processes are using
- Checksums for all running processes
- Dump memory for all running processes
- All DLLs currently loaded and their checksum
- Capture last Modify/Access/Create times for designated areas
- All files that are currently open
- **Net** (start/share/user/file/session)
- Output from nbtstat and netstat
- Document all open shares/exports on system
- Capture current routing tables
- list of all network connections
- Layer3 traffic samples
- capture logged in users

**Static Information**
- System Name
- Basic system info (peripherals, BIOS, drivers, etc)
- System Startup Commands
- MAC address
- List of installed services
- Local account and policy information
- Current patches installed on system
- Current AV versions
- Files with alternate data streams
- Discover files marked as hidden
- List of all installed software on system (known to registry)
- Capture system logs
- Capture of AV logs
- Copies of application caches (temporary internet files) – IE, FF, Opera
- **Export entire registry**
- Search/retrieve files based on search criteria.
Questions to Ask...

- Examine the startup information – anything starting you do not know/understand?
- Examine the startup services – anything you do not understand?
- Browse the patches installed – anything recent missing that would lead you to believe the system is not patched according to your org’s policy?
- Is your anti-virus current?
- Drivers – yep they can be vulnerable, are yours loaded from known/expected paths? Current?
- Any local accounts you do not recognize?
• Content parsing – known good lists for your org’s images are critical. Script a comparison tool vs output.
  – Run RAPIER on known good, compare
• MD5/SHA1 – just in case you find something interesting (default)
• PERL. Could be my unix background but it helps in parsing text files.
• Search Engines / Reputable Sites
Processes

Volatile Information
- complete list of running processes
- locations of those processes on disk
- ports those processes are using
- Checksums for all running processes
- Dump memory for all running processes
- All DLLs currently loaded and their checksum
- Capture last Modify/Access/Create times for designated areas
- All files that are currently open
- Net (start/share/user/file/session)
- Output from nbtstat and netstat
- Document all open shares/exports on system
- Capture current routing tables
- list of all network connections
- Layer3 traffic samples
- capture logged in users

Static Information
- System Name
- Basic system info (peripherals, BIOS, drivers, etc)
- System Startup Commands
- MAC address
- List of installed services
- Local account and policy information
- Current patches installed on system
- Current AV versions
- Files with alternate data streams
- Discover files marked as hidden
- List of all installed software on system (known to registry)
- Capture system logs
- Capture of AV logs
- Copies of application caches (temporary internet files) – IE, FF, Opera
- Export entire registry
- Search/retrieve files based on search criteria.
Questions to Ask...

About the processes:
- What’s running that you don’t know about?
- Anything not known, but in the registry?
- No surprises in the execution paths?
- What ports are they tied to? Anything unexpected
- Anything interesting in the strings output of the memory-dumped processes?

And the DLL’s (same deal)...
- How about in the paths to the loaded DLL’s?
- Do the checksums match those on a known good system?

Anything installed that shouldn’t be? (Kazaa, eMule)
Tools to Use...

• Strings.exe
• BitBlaze project (looks cool)  
  – http://bitblaze.cs.berkley.edu
• IDA (if you are really hardcore)
• PE Tools, Unpackers
• MD5/SHA1 – submit it sites that track malicious code
• Mandiant Red Curtain
• iDefense Malware Analysis Pack
Networking

**Volatile Information**
- complete list of running processes
- locations of those processes on disk
- ports those processes are using
- Checksums for all running processes
- Dump memory for all running processes
- All DLLS currently loaded and their checksum
- Capture last Modify/Access/Create times for designated areas
- All files that are currently open
- **Net** (start/share/user/file/session)
- **Output from nbtstat and netstat**
- **Document all open shares.exports on system**
- Capture current routing tables
- list of all network connections
- **Layer3 traffic samples**
- capture logged in users

**Static Information**
- System Name
- Basic system info (peripherals, BIOS, drivers, etc)
- System Startup Commands
- **MAC address**
- List of installed services
- Local account and policy information
- Current patches installed on system
- Current AV versions
- Files with alternate data streams
- Discover files marked as hidden
- List of all installed software on system (known to registry)
- Capture system logs
- Capture of AV logs
- Copies of application caches (temporary internet files) – IE, FF, Opera
- Export entire registry
- Search/retrieve files based on search criteria.
Questions to Ask...

All the shares make sense?
Anything in promiscuous mode?
Virtual NICs? Should they be there?
Wireless vs. Wired?

Netstat – connections make sense? (You connected to machines you have no reason to be?)
Where is the traffic going?
How is it getting there? (routing tables, proxy)
What ports are listening - should they be?
Any unknown services bound to ports?
Strange outbound traffic
- Samspade.org – oldie but goodie
- Maltego (http://www.paterva.com/maltego/)
- Proxy server logs? (who else is connecting)

Good Traffic Capture/Analysis Tools:
- Tcpdump
- WireShark
- Rumit
- Time-Based Network Visualizer (tnv)
- Snort (replay mode rocks)
- NSM-Console (packet analysis)
A single Storm infection as visualized with InetVis
Rumint

Visualized by
• Source IP,
• Dest IP,
• UDP Source,
• UDP Dest,
• TTL
using the same ecard.cap sample.

Greg Conti’s excellent offering.
Notice all the connections from hundreds of IPs to a single infected host and egress to a single external destination port.
<table>
<thead>
<tr>
<th>Logs &amp; Cache</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Volatile Information</strong></td>
</tr>
<tr>
<td>• complete list of running processes</td>
</tr>
<tr>
<td>• locations of those processes on disk</td>
</tr>
<tr>
<td>• ports those processes are using</td>
</tr>
<tr>
<td>• Checksums for all running processes</td>
</tr>
<tr>
<td>• Dump memory for all running processes</td>
</tr>
<tr>
<td>• All DLLS currently loaded and their checksum</td>
</tr>
<tr>
<td>• Capture last Modify/Access/Create times for designated areas</td>
</tr>
<tr>
<td>• All files that are currently open</td>
</tr>
<tr>
<td>• Net (start/share/user/file/session)</td>
</tr>
<tr>
<td>• Output from nbtstat and netstat</td>
</tr>
<tr>
<td>• Document all open shares/exports on system</td>
</tr>
<tr>
<td>• Capture current routing tables</td>
</tr>
<tr>
<td>• list of all network connections</td>
</tr>
<tr>
<td>• Layer3 traffic samples</td>
</tr>
<tr>
<td>• capture logged in users</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Static Information</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• System Name</td>
</tr>
<tr>
<td>• Basic system info (peripherals, BIOS, drivers, etc)</td>
</tr>
<tr>
<td>• System Startup Commands</td>
</tr>
<tr>
<td>• MAC address</td>
</tr>
<tr>
<td>• List of installed services</td>
</tr>
<tr>
<td>• Local account and policy information</td>
</tr>
<tr>
<td>• Current patches installed on system</td>
</tr>
<tr>
<td>• Current AV versions</td>
</tr>
<tr>
<td>• Files with alternate data streams</td>
</tr>
<tr>
<td>• Discover files marked as hidden</td>
</tr>
<tr>
<td>• List of all installed software on system (known to registry)</td>
</tr>
<tr>
<td>• <strong>Capture system logs</strong></td>
</tr>
<tr>
<td>• <strong>Capture of AV logs</strong></td>
</tr>
<tr>
<td>• <strong>Copies of application caches (temporary internet files) – IE, FF, Opera</strong></td>
</tr>
<tr>
<td>• Export entire registry</td>
</tr>
<tr>
<td>• Search/retrieve files based on search criteria.</td>
</tr>
</tbody>
</table>
Are the logs start / last date what you might expect?

Was AV running continuously until RAPIER was executed?

Where did they go (websites) that were of interest? (examine output from cache)

Deep dive on the content of the logs (how many does VISTA have? Ugh..)
Tools to Use...

Microsoft Log Parser (http://www.logparser.com)
Regviewer (unix) – tool to look at exported registry
Splunk – www.splunk.com (freeware version limited to 500MB per day)
Perl – (the unix guy in me again)

References:
http://www.logparser.com/
http://www.eventid.net
http://www.net-security.org/dl/insecure/INSECURE-Mag-16.pdf (Rob Faber)
**Files**

**Volatile Information**
- complete list of running processes
- locations of those processes on disk
- ports those processes are using
- Checksums for all running processes
- Dump memory for all running processes
- All DLLS currently loaded and their checksum
- **Capture last Modify/Access/Create times for designated areas**
- All files that are currently open
- Net (start/share/user/file/session)
- Output from nbtstat and netstat
- Document all open shares/exports on system
- Capture current routing tables
- list of all network connections
- Layer3 traffic samples
- capture logged in users

**Static Information**
- System Name
- Basic system info (peripherals, BIOS, drivers, etc)
- System Startup Commands
- MAC address
- List of installed services
- Local account and policy information
- Current patches installed on system
- Current AV versions
- **Files with alternate data streams**
- Discover files marked as hidden
- List of all installed software on system (known to registry)
- Capture system logs
- Capture of AV logs
- Copies of application caches (temporary internet files) – IE, FF, Opera
- Export entire registry
- **Search/retrieve files based on search criteria.**
Questions to Ask...

- Any recently added or modified that doesn’t make sense?
- What is open? Why?
- Hidden files – should they be? (probably not)
- Alternate Data Streams?
Files

- Strings.exe
- MD5/SHA1 – submit it sites that track MD5’s of malicious code
- Search Engines
- Jesse Kornblum’s MissIdentify
- Mandiant Red Curtain
- iDefense Malware Analysis Pack
Over the horizon

- Sandman: Hibernation File examination
  - [http://www.darknet.org.uk/2008/05/sandman-read-the-windows-­hibernation-file/](http://www.darknet.org.uk/2008/05/sandman-read-the-windows-­hibernation-file/)
- Change Analysis Diagnostic Tool (MSFT)
- Virtual Machine (discover/acquisition)
- Vista Logging
- Jesse Kornblum’s MissIdentify (sourceforge.net)
- FCIV (file integrity prog from MSFT)
- SigVerif (MSFT) – verifies signed files
- MuiCache (application names/vers)
- Encrypt output (probably GPG)
- Par’s cool stuff 😊
QUESTIONS, FEATURE REQUESTS & FEEDBACK
Your Thoughts/Questions

#include “conversation.h”

Website:
http://code.google.com/p/rapier/

Discussion:
http://groups.google.com/group/RAPIER-ramblings

Email:
Rapier.SecurityTool@gmail.com
Gratitude

Lawrence Baldwin (SecCheck*)
Jem Berkes (md5sums*)
Frank Heynes (LADS* tool)
Nir Sofer (cprocess* )
Arne Vidstrom (macmatch*, pmdump*)
Kevin Stanush (dumpsec*)
Parmavex Software (winaudit*)
Didier Stevens (BPMTK) – in development
Russ McRee (Evangelist and Contributor)
Harlan Carvey (his blog windowsir.blogspot.com keeps me busy.)

Jesse Kornblum for FRED* as a source of inspiration for most of the IR tools out there. (imho)
THANK YOU

To be continued at nearest bar...