Hunting Your Adversary - How to Operate and Leverage an Incident Response Hunt Team

Rob Lee, SANS rlee@sans.org
Three Items to Discuss Today

- Evolution of Current Threats
- Changing Tactics of Incident Response
- Rise of Cyber Threat Intelligence
Organizations Fail to Detect Intrusions

If organizations detect a breach, how long did it take them to detect it?

- Time to compromise
- Time to discovery

205 days is the median number of days that threat groups were present on a victim's network before detection.

How Compromises Are Being Detected:
- 31% victims discovered the breach internally
- 69% victims notified by an external entity
Threat Evolution
Nation State Adversaries
Offense Develops Faster - Defense “Tying Hands behind Our Back”
IR Process and Forensics

- Preparation
- Identification and Scoping
- Containment / Intelligence Gathering
- Eradication / Remediation
- Recovery
- Follow Up / Lessons Learned

No Identification = No Containment

- Malware Detection
- Lateral Movement Detection
- Data Collection Detection
- Data Exfil Detection
- Forensic Analysis

Follow Up / Lessons Learned
Recovery
Eradication / Remediation
Preparation
Identification and Scoping
Containment / Intelligence Gathering
Malware Detection
Lateral Movement Detection
Data Collection Detection
Data Exfil Detection
Forensic Analysis
"CTI" is the new "APT"
Phases of a successful intrusion operation

1. Recon
   - Detection: Spear Phishing
   - Chance to Degrade or Stop Operation

2. Exploitation
   - Detection: Pivot
   - Chance to Degrade or Stop Operation

3. Privilege Escalation
   - Detection: Exfil
   - Chance to Degrade or Stop Operation

4. Data Collection

5. Lateral Movement

6. Data Exfiltration
3 Possible Detection Situations

- Malware active
- Malware exists, but not active
- No Malware, but system compromised
NINJAS
There are four of them in this picture.
In this autoruns output, there is malware: Can you see it?

<table>
<thead>
<tr>
<th>Entry Location</th>
<th>Entry</th>
<th>Category</th>
<th>Image Path</th>
<th>Launch String</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>Fresponse</td>
<td>Services</td>
<td>C:\Windows\system32\f-response-ent.exe</td>
<td>f-response-ent.exe</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>Changer</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\Changer.sys</td>
<td>Changer</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>iZomgmt</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\iZomgmt.sys</td>
<td>iZomgmt</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>Ibrtdc</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\Ibrtdc.sys</td>
<td>Ibrtdc</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>mfeavfK01</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\mfeavfK01.sys</td>
<td>mfeavfK01</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>mfefireK01</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\mfefireK01.sys</td>
<td>mfefireK01</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>Memosyne</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\Memosyne\Memosyne.exe</td>
<td>Memosyne.exe</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>PCDump</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\PCIDump.sys</td>
<td>PCDump</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>PCOMP</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\PCOMP.sys</td>
<td>PCOMP</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>PDFRAME</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\PDFRAME.sys</td>
<td>PDFRAME</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>PDLREI</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\PDLREI.sys</td>
<td>PDLREI</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>PDRFAME</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\PDRFAME.sys</td>
<td>PDRFAME</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>Ymscspi</td>
<td>Drivers</td>
<td>C:\Windows\system32\Drivers\Ymscspi.sys</td>
<td>System32\DRIVERS\Ymscspi.sys</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>WICICA</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\WICICA.sys</td>
<td>WICICA</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Control\Print\Monitors</td>
<td>ThinPrint</td>
<td>Print</td>
<td>C:\Windows\system32\Tpvmon.sys</td>
<td>TpvMon.dll</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services\WinSock2</td>
<td>12</td>
<td>Network</td>
<td>C:\Program Files\VMware\vssocklib.dll</td>
<td>C:\Program Files\VMware\vssocklib.dll</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services\WinSock2</td>
<td>13</td>
<td>Network</td>
<td>C:\Program Files\VMware\vssocklib.dll</td>
<td>C:\Program Files\VMware\vssocklib.dll</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</td>
<td>QuickTime</td>
<td>Logon</td>
<td>C:\Program Files\Quicktime\QtTask.exe</td>
<td>&quot;C:\Program Files\Quicktime\QtTask.exe&quot; --atboot</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</td>
<td>svhost</td>
<td>Logon</td>
<td>C:\Windows\system32\svhost.exe</td>
<td>C:\Windows\system32\svhost.exe</td>
</tr>
<tr>
<td>HKLM\Software\Classes\ShellEx\ContextMenuHandlers</td>
<td>7-Zip</td>
<td>Explorer</td>
<td>C:\Program Files\7-Zip\7-Zip.dll</td>
<td>HKCR\CLSID{23170f69-40c1-278a-1000-000000001f8a}</td>
</tr>
<tr>
<td>HKLM\Software\Classes\ShellEx\ContextMenuHandlers</td>
<td>7-Zip</td>
<td>Explorer</td>
<td>C:\Program Files\7-Zip\7-Zip.dll</td>
<td>HKCR\CLSID{23170f69-40c1-278a-1000-000000001f8a}</td>
</tr>
<tr>
<td>HKLM\Software\Classes\ShellEx\DragDropHandlers</td>
<td>7-Zip</td>
<td>Explorer</td>
<td>C:\Program Files\7-Zip\7-Zip.dll</td>
<td>HKCR\CLSID{23170f69-40c1-278a-1000-000000001f8a}</td>
</tr>
<tr>
<td>HKLM\Software\Classes\CLSID{083863F1-70DE-11d0-BD40-00A00AOA00D0} Media</td>
<td>Codecs</td>
<td></td>
<td>C:\Program Files\Movie Maker\Wmmflit.dll</td>
<td>HKCR\CLSID{F689C580-F000-479F-886D-A01D09175F87}</td>
</tr>
<tr>
<td>HKLM\Software\Classes\CLSID{083863F1-70DE-11d0-BD40-00A00AOA00D0} ShotBoundary</td>
<td>Codecs</td>
<td></td>
<td>C:\Program Files\Movie Maker\Wmmflit.dll</td>
<td>HKCR\CLSID{FE48704D-DC92-4F10-91DE-C676E258A5}</td>
</tr>
<tr>
<td>HKLM\Software\Classes\CLSID{083863F1-70DE-11d0-BD40-00A00AOA00D0} Media</td>
<td>Codecs</td>
<td></td>
<td>C:\Program Files\Movie Maker\Wmmflit.dll</td>
<td>HKCR\CLSID{F689C580-F000-479F-886D-A01D09175F87}</td>
</tr>
<tr>
<td>HKLM\Software\Classes\CLSID{083863F1-70DE-11d0-BD40-00A00AOA00D0} ShotBoundary</td>
<td>Codecs</td>
<td></td>
<td>C:\Program Files\Movie Maker\Wmmflit.dll</td>
<td>HKCR\CLSID{FE48704D-DC92-4F10-91DE-C676E258A5}</td>
</tr>
<tr>
<td>HKLM\Software\Classes\CLSID{083863F1-70DE-11d0-BD40-00A00AOA00D0} Media</td>
<td>Codecs</td>
<td></td>
<td>C:\Program Files\Movie Maker\Wmmflit.dll</td>
<td>HKCR\CLSID{F689C580-F000-479F-886D-A01D09175F87}</td>
</tr>
<tr>
<td>HKLM\Software\Classes\CLSID{083863F1-70DE-11d0-BD40-00A00AOA00D0} ShotBoundary</td>
<td>Codecs</td>
<td></td>
<td>C:\Program Files\Movie Maker\Wmmflit.dll</td>
<td>HKCR\CLSID{FE48704D-DC92-4F10-91DE-C676E258A5}</td>
</tr>
</tbody>
</table>
What is Evil? What is Normal?
Importance of Knowing Key Windows Processes

**svchost.exe**

- **Image Path:** `%SystemRoot%\System32\svchost.exe`
- **Parent Process:** `services.exe`
- **Number of Instances:** Five or more
- **User Account:** Varies depending on svchost instance, though it typically will be Local System, Network Service, or Local Service accounts. Instances running under any other account should be investigated.
- **Start Time:** Typically within seconds of boot time. However, services can be started after boot, which might result in new instances of `svchost.exe` well after boot time.
- **Description:** The generic host process for Windows Services. It is used for running service DLLs. Windows will run multiple instances of `svchost.exe`, each using a unique “-k” parameter for grouping similar services. Typical “-k” parameters include Bfsrvcs, DcomLaunch, RpcSs, LocalServiceNetworkRestricted, netsvcs, LocalService, NetworkService, LocalServiceNoNetwork, sevsrvcs, and LocalServiceAndNtlmPersonation. Malware authors often take advantage of the ubiquitous nature of `svchost.exe` and use it either directly or indirectly to hide their malware. They use it directly by installing the malware as a service in a legitimate instance of `svchost.exe`. Alternatively, they use it indirectly by trying to blend in with legitimate instances of `svchost.exe`, either by slightly misspelling the name (e.g., `svchost.exe`) or spelling it correctly but placing it in a directory other than System32. Keep in mind that a legitimate `svchost.exe` should always run from `%SystemRoot%\System32`, should have `services.exe` as its parent, and should host at least one service. Also, on debut installations of Windows 7, all service executables and all service DLLs are signed by Microsoft.
In this autoruns output, there is malware: Can you see it?

<table>
<thead>
<tr>
<th>Entry Location</th>
<th>Entry</th>
<th>Category</th>
<th>Image Path</th>
<th>Launch String</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>Fresponse</td>
<td>Services</td>
<td>c:\windows\system32\f-response-ent.exe</td>
<td>f-response-ent.exe</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>Changer</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\Changer.sys</td>
<td>Changer</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>l2omgmt</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\l2omgmt.sys</td>
<td>l2omgmt</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>lbttfcd</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\lbttfcd.sys</td>
<td>lbttfcd</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>mfeavf01</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\mfeavf01.sys</td>
<td>mfeavf01</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>mffeirek01</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\mffeirek01.sys</td>
<td>mffeirek01</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>Mmemosyne</td>
<td>Drivers</td>
<td>c:\windows\system32\mmemosynei386.sys</td>
<td>??(c:\windows\system32\mmemosynei386.sys</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>PCIDump</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\PCIDump.sys</td>
<td>PCIDump</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>PDCOMP</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\PDCOMP.sys</td>
<td>PDCOMP</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>PDFRAME</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\PDFRAME.sys</td>
<td>PDFRAME</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>PDRELI</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\PDRELI.sys</td>
<td>PDRELI</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>PDFRAME</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\PDFRAME.sys</td>
<td>PDFRAME</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>Vmmsci</td>
<td>Drivers</td>
<td>c:\windows\system32\Drivers\vmmsci.sys</td>
<td>System32\DRIVERS\vmmsci.sys</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services</td>
<td>Wdica</td>
<td>Drivers</td>
<td>File not found: C:\WINDOWS\System32\Drivers\Wdica.sys</td>
<td>Wdica</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Control\Print\Monitors</td>
<td>ThinPrint</td>
<td>Print</td>
<td>c:\windows\system32\tpvmon.dll</td>
<td>TPVMon.dll</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services\WinSock2</td>
<td>12</td>
<td>Network</td>
<td>c:\program files\vmware\vssocklib.dll</td>
<td>C:\Program Files\VMware\vssocklib.dll</td>
</tr>
<tr>
<td>HKLM\System\CurrentControlSet\Services\WinSock2</td>
<td>13</td>
<td>Network</td>
<td>c:\program files\vmware\vssocklib.dll</td>
<td>C:\Program Files\VMware\vssocklib.dll</td>
</tr>
</tbody>
</table>

- **Image Path** is `C:\Windows\System32\dllhost.exe`. It should be `C:\Windows\System32`
- **Parent Process** will not be `services.exe` since the process is not launched via `Services`, but at User Logon via the “AutoRuns” Registry Key.
- **Start time** will not be at boot, but when a user logs onto the system.
- **The launch string** should include a “-k” parameter with it.
“One Down. Billion to Go.”
Remote Enterprise IR & Forensics

Incident Responder

Enterprise Network
Breach Status Update

Initial IRT Call & Agent deployment
- Access Host
- Memory
- C-Drive
- Autostart Locations Examination
- Time: ~60 min

Final Memory Forensics
- Time: ~60-120 min

Timeline Analysis
- Time to Create Timeline – 5–60 minutes
- Analysis of Timeline Data – 150 min

Current Spreadsheet o’ Doom
- 10.3.58.7 – tdungan
- 10.3.58.5 – nromanoff
- 10.3.58.6 – nfury
- 10.3.58.4 – domain controller

Incident Response Total Time Elapsed: ~360 Min

Known Hosts Compromised

<table>
<thead>
<tr>
<th>Name</th>
<th>IP</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>tdungan</td>
<td>10.3.58.7</td>
<td>Workstation</td>
</tr>
</tbody>
</table>
Three Items to Discuss Today

• Evolution of Current Threats
• Changing Tactics of Incident Response
• Rise of Cyber Threat Intelligence

• Contact: Rob Lee -> rlee@sans.org
SANS DFIR
Digital Forensics & Incident Response

Website
digital-forensics.sans.org

SIFT Workstation
dfir.to/SANS-SIFT

Join The SANS DFIR Community
Blog: dfir.to/DFIRBlog
Twitter: @sansforensics
Facebook: sansforensics
Google+: gplus.to/sansforensics
Mailing list: dfir.to/MAIL-LIST
YouTube: dfir.to/DFIRCast

DFIR CURRICULUM

CORE
FOR408 Windows Forensics GCFE
SEC504 Hacker Tools, Techniques, Exploits & Incident Handling GCIH

OPERATING SYSTEM & DEVICE IN-DEPTH
FOR585 Advanced Smartphone Forensics
FOR518 Mac Forensics
FOR526 Memory Forensics In-Depth

INCIDENT RESPONSE & ADVERSARY HUNTING
FOR508 Advanced Incident Response GCFA
FOR572 Advanced Network Forensics and Analysis GNFA
FOR578 Cyber Threat Intelligence
LEARN R.E.M.
FOR610 REM: Malware Analysis GREM
MGT535 Incident Response Team Management