Using Home Advantage

Combating Anti-Forensics and Linkage Blindness in Enterprise Entrenchment

“know when to hold em”

Eoghan Casey       Chris Daywalt
Quick?

When an incident has been detected and analyzed, it is important to contain it before the spread of the incident overwhelms resources or the damage increases. Most incidents require containment, so it is important to consider it early in the course of handling each incident.

- NIST SP800-61 Rev. 1, page 3-19
Effective Incident Response, Part 1

- Scope
- Scope scope scope
- Scope scope
- Scope, scopity scope scope scope
Definitions

• Linkage blindness
  – failure to recognize that crimes were committed by the same offender because they occurred in different jurisdictions

• Tandem modus operandi
  – use parallel but distinct methods of operating on compromised systems

These complicate scope assessment
Target Selection & Admin

WORKSTATIONS
MORE WORKSTATIONS
APP SERVERS
DOMAIN CONTROLLERS

Poison Ivy - [Listening on Port: 3460 (Connections: 2)]

Connections  Statistics  Settings
ID   WAN   LAN   Con. Type
Test_3  192.168.184.136  192.168.184.136  Direct
Test_4  192.168.184.132  192.168.184.132  Direct
Enterprise Credential Theft/Injection

Set objOU = GetObject("LDAP://OU=Any OU, dc=Domain Name, dc=Domain Extension")
Set objUser = objOU.Create("User", "cn=User Name")
objUser.Put "sAMAccountName", "User Name"
objUser.SetInfo
objUser.ChangePassword ", "Password"
objUser.AccountDisabled = FALSE
objUser.SetInfo
Linkage Analysis: Think Global

x All Local and Network Logons
# Tool Variance

<table>
<thead>
<tr>
<th>Rootkit / Backdoor Package</th>
<th>Victim Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1-10 Workstations</td>
</tr>
<tr>
<td>1A (abc.exe)</td>
<td>X</td>
</tr>
<tr>
<td>1B (def.exe)</td>
<td></td>
</tr>
<tr>
<td>1C (ghi.exe)</td>
<td></td>
</tr>
<tr>
<td>2A (123.dll)</td>
<td>X</td>
</tr>
<tr>
<td>2B (456.dll)</td>
<td></td>
</tr>
<tr>
<td>2C (789.dll)</td>
<td></td>
</tr>
<tr>
<td>3A (xyz123.exe)</td>
<td></td>
</tr>
</tbody>
</table>
Host Linkage Analysis

![ssdeep output]

<table>
<thead>
<tr>
<th>Process</th>
<th>PID</th>
<th>Name</th>
<th>Size</th>
<th>Command Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>svchost.exe</td>
<td>1152</td>
<td>Micro... NT AUTHORITY...</td>
<td>C:\WINDOWS\system32\svchost.exe -k NetworkService</td>
<td></td>
</tr>
<tr>
<td>svchost.exe</td>
<td>1336</td>
<td>Micro... NT AUTHORITY...</td>
<td>C:\WINDOWS\system32\svchost.exe -k LocalService</td>
<td></td>
</tr>
<tr>
<td>spoolsv.exe</td>
<td>1456</td>
<td>Micro... NT AUTHORITY...</td>
<td>C:\WINDOWS\system32\spoolsv.exe</td>
<td></td>
</tr>
</tbody>
</table>

lsass.exe pid: 740
Command line: C:\WINDOWS\system32\lsass.exe

<table>
<thead>
<tr>
<th>Base Address</th>
<th>Size</th>
<th>Version</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x01000000</td>
<td>0x6000</td>
<td>5.01.2600.5512</td>
<td>C:\WINDOWS\system32\ntdll.dll</td>
</tr>
<tr>
<td>0x7c900000</td>
<td>0xaf000</td>
<td>5.01.2600.5512</td>
<td>C:\WINDOWS\system32\kernel32.dll</td>
</tr>
<tr>
<td>0x7c800000</td>
<td>0xf6000</td>
<td>5.01.2600.5512</td>
<td>C:\WINDOWS\system32\ADVAPI32.dll</td>
</tr>
<tr>
<td>0x77dd0000</td>
<td>0x9b000</td>
<td>5.01.2600.5512</td>
<td>C:\WINDOWS\system32\RPCRT4.dll</td>
</tr>
<tr>
<td>0x77e70000</td>
<td>0x92000</td>
<td>5.01.2600.5512</td>
<td></td>
</tr>
</tbody>
</table>
Command & Control Variance
Network Linkage Analysis

• Deep C&C traffic analysis
  – Common features in beacon packets
  – Discernible patterns in encrypted traffic

• Home Advantage
  – Deviations from normal traffic
Effective Incident Response, Part 2

NIST Incident Response Life Cycle

1. Preparation
2. Detection & Analysis
3. Containment, Eradication & Recovery
4. Post-Incident Activity
Re-infection Vectors

1. “Cleaned / Remediated” Workstations
2. Discovered Not Yet Remediated
3. IDS Sensor
4. Compromised Systems Undiscovered by Responders
Containment Strategies

CLASSIC:
- Block bad attacker IP addresses
- Block C&C domain names
- Rebuild or clean compromised systems
- Reset compromised credentials

NEW:
- Active directory account validation sweep
- Change critical account names
- Restrict policies
- Establish internal perimeters
- Intensified monitoring
- WHITELISTING!!!11~
Organizational Preparedness

- Team structure and training
- Windows domain isolation
- Remote forensics capabilities
- Customize IDS signature/preprocessor
- Centralized host logging
- Network logging (perimeter & internal)
- Focused monitoring of critical assets
- Tools for detecting deviations
  - Host and network abnormalities
Scope!

- Contact eoghan@jhu.edu
- Sharing the knowledge