AppLocker and Sysmon

WELL THEN

THIS JUST GOT A LITTLE AWKWARD
Backdoors & Breaches

Incident Response Card Game

Launching in September 2019

Request a Deck!

Type "Backdoors & Breaches" into the Questions Window

We'll randomly select a few requests to get a deck before the official launch.
Brought To You By!

AI HUNTER™
Network Threat Hunting Solution

ANALYZE
Network Traffic

IDENTIFY
Compromised Systems

HUNT
Menacing Threats

BEACONS MODULE
LONG CONNECTIONS MODULE
DEEP DIVE MODULE
ALERTING

Request a Personal Demo
Type “Demo” in Questions Window
WILD WEST HACKIN’ FEST
2019

Training 10/22 - 23
Conference 10/23 - 25
DEADWOOD, SD

wildwesthackinfest.com
# Problem Statement

The full ATT&CK Matrix™ below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.


<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Command and Control</th>
<th>Exfiltration</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive-by Compromise</td>
<td>AppleScript</td>
<td>.bash_profile and .bashrc</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>AppleScript</td>
<td>Audio Capture</td>
<td>Commonly Used Port</td>
<td>Automated Exfiltration</td>
<td>Data Destruction</td>
</tr>
<tr>
<td>Exploit Public-Facing Application</td>
<td>CMSTP</td>
<td>Accessibility Features</td>
<td>Accessibility Features</td>
<td>BITS Jobs</td>
<td>Bash History</td>
<td>Application Window Discovery</td>
<td>Application Deployment Software</td>
<td>Automated Collection</td>
<td>Communication Through Removable Media</td>
<td>Data Compressed</td>
<td>Data Encrypted for Impact</td>
</tr>
<tr>
<td>External Remote Services</td>
<td>Command-Line Interface</td>
<td>Account Manipulation</td>
<td>AppCert DLLs</td>
<td>Binary Padding</td>
<td>Brute Force</td>
<td>Browser Bookmark Discovery</td>
<td>Distributed Component Object Model</td>
<td>Clipboard Data</td>
<td>Connection Proxy</td>
<td>Data Encrypted</td>
<td>Defacement</td>
</tr>
<tr>
<td>Hardware Additions</td>
<td>Compiled HTML File</td>
<td>AppCert DLLs</td>
<td>Apinin DLLs</td>
<td>Bypass User Account Control</td>
<td>Credential Dumping</td>
<td>Domain Trust Discovery</td>
<td>Exploitation of Remote Services</td>
<td>Data Staged</td>
<td>Custom Command and Control Protocol</td>
<td>Data Transfer Size Limits</td>
<td>Disk Content Wipe</td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>Control Panel Items</td>
<td>Appinin DLLs</td>
<td>Application Shimming</td>
<td>CMSTP</td>
<td>Credentials in Files</td>
<td>File and Directory Discovery</td>
<td>Logon Scripts</td>
<td>Data from Information Repositories</td>
<td>Custom Cryptographic Protocol</td>
<td>Exfiltration Over Alternative Protocol</td>
<td>Disk Structure Wipe</td>
</tr>
<tr>
<td>Spearphishing Attachment</td>
<td>Dynamic Data Exchange</td>
<td>Application Shimming</td>
<td>Bypass User Account Control</td>
<td>Clear Command History</td>
<td>Credentials in Registry</td>
<td>Network Service Scanning</td>
<td>Pass the Hash</td>
<td>Data from Local System</td>
<td>Data Encoding</td>
<td>Exfiltration Over Command and Control Channel</td>
<td>Endpoint Denial of Service</td>
</tr>
</tbody>
</table>
Executive Problem Statement

Basic Questions:

- Are our tools working?
- What can we detect?
- What are our gaps?
- Why does M$ logging suck so bad?
- What existing tools can fill them?
- What do we have to buy?
- Do we need to buy something expensive?

“Maybe, I can take the Sequel Police’s ship to Command headquarters to get a TimePod…”
Sysmon

- Basically…
  - Windows logging is just bad.
  - Finding anything is tough
- Sysmon makes it better
  - In like.. Five minutes
  - Like Heroin!
- Demo!

“NOT ALL DRUGS ARE GOOD…
SOME OF THEM ARE GREAT”

- BILL HICKS

Sysmon… Is a great drug..
These were the logs you were looking for!

Process Create:
RuleName:
UtcTime: 2019-07-29 16:49:44.838
ProcessGuid: {ac6a4e42-23a8-5d3f-0000-0010f8353400}
ProcessId: 6816
Image: C:\Users\Sec504\Downloads\msf.exe
FileVersion: 2.2.14
Description: ApacheBench command line utility
Product: Apache HTTP Server
Company: Apache Software Foundation
OriginalFileName: ab.exe
CommandLine: "C:\Users\Sec504\Downloads\msf.exe"
CurrentDirectory: C:\Users\Sec504\Downloads\nUser: THEBOSS\Sec504
LogonGuid: {ac6a4e42-61bd-5d37-0000-002033200700}
LogonId: 0x72033
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: MD5=532FA545F9B01DCA5E0991B7AB85E326,SHA256=4960AD6540BF6D8991ED93
ParentProcessGuid: {ac6a4e42-61c2-5d37-0000-001092270800}
ParentProcessId: 1772
ParentImage: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
ParentCommandLine: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"
Implementing Sysmon Via GPO

- Great Article via Syspanda

```bash
1 copy /z /y "\domain.com\apps\config.xml" "C:\windows\
2 sysmon -c c:\windows\config.xml
3 sc query "Sysmon" | Find "RUNNING"
4 If "%ERRORLEVEL%" EQU "1" (  
5 goto startsysmon  
6 )
7 :startsysmon  
8 net start Sysmon  
9 :installsysmon  
10 If "%ERRORLEVEL%" EQU "1" (  
11 goto installsysmon  
12 )
13 :installsysmon  
14 "\domain.com\apps\sysmon.exe" /accepteula -i c:\windows\config.xml
```
AppLocker

- Let’s create a very basic AppLocker profile
  - Just the Defaults
- And let’s push it out via GPO
- Need the OU, the Policy and the Service configured
- Demo
AppLocker Bypass

- Pretty much any bypass technique will work
  - Rundll32, EvilGrade-ISR, Service exploits, .sct files, etc.
- But 95%+ of the drive-by download attacks will fail
  - (That’s most attacks BTW)

Bypasses never seem to end.
They just go on and on my friends!
SubTee, started hacking and not knowing what it was..
Now we will just keep on hacking it forever
Just because..
Implementation Principles

- Start small. With your own team
- Start in Audit mode!
- Roll out in stages to other “techy” teams
- No need to go super detailed to start

Roll it out to these people first. They know things..
Questions?
Answer!!