ELK and Sysmon
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.
HOMES ON

WILD WEST HOCKIN' FEST

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 Elevation</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>Accessibilty Features</td>
<td>BITS Jobs</td>
<td>Bash History</td>
<td>Application Windows 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>Aplinit 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>Appinit 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>Spear phishing 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:
- Is logging working?
- Are we logging too much?
- How much does logging cost?
- What the hell is a Data Lake?
- What is my team actually doing?
- Things are not getting better...

“I am a Youngblood! I will avenge my fallen classmates!”
Sysmon

- Basically…
  - Windows logging is just bad
  - Finding anything is tough
- Sysmon makes it better
  - In like… Five minutes
  - See last webcast

YOUR LOGS SUCK
AND YOU SHOULD FEEL BAD!
Something Different Now.. ELK
Why ELK?

- Let’s talk about data for a moment
- Structured data vrs lots of different documents/data
- A different type of “database” is needed
- The right tool for the right job
But Why ELK?

- Logstash
- Multiple different types of “log” feeds
- Sysmon, Netflow, etc.
- Need some way to get it all to the same place
But Why ELK?

- Kibana
- Need for a dashboard that has crazy cool (and useful visualizations!)
- Ability to create and save dashboards
- Ability to create and save searches
BUT.. WHY ELK?
But all this is only as good as the data you feed it!

- Enter Sysmon
- The data you actually want
- Yes, there are some other Windows logs you would want as well
- Easy to get to Elasticsearch
  - Via Winlogbeat

Any time I can work Weird Al in…. It’s a good time.
We Will Be Using HELK Today

- Still Alpha
- Still Alpha
- Pretty darn good
- Data normalization (we will be looking at some log files)
- Would not recommend for production
- Let’s begin!

So many things… All the things…
Moving Forward

- Bringing in Mick for this…
- He will be showing us all the ELK rock
  - And the suck…
- So many variants
- You will most likely be mixing and matching
Questions?
Answer!!