Hunting Threats in Your Enterprise

Hunting Threats In your Enterprise
Who am I?

- Abdulrahman Al-Nimari
- 25 Years IT & Infosec Experience
- Lead Enterprise Security Architect
- Mantech International Corporation, Riyadh, KSA
- CISSP, CISM, CCISO, PMP, GCIH, GCIA, GCUX, GREM, GSEC
- @nimari
- https://www.linkedin.com/in/alnimari/
- alnimari@gmail.com
Agenda

- What is Threat Hunting?
- Threat Hunting Plan
- Hunt Cycle
- Hunting in Action
- Hunt Maturity Level
- Measuring Success (Metrics)
- Resources
Hunting Threats in Your Enterprise

Verizon Data Breach Investigations Report, 2018

Most compromises took minutes, or less (87%)

Only 3% are discovered as quickly

Two-thirds went undiscovered for months or more (68%)

Elapsed time:
- Months
- Weeks
- Days
- Hours
- Minutes

✓ What is threat hunting?

✓ **Cyber threat hunting** is "the process of **proactively** and **iteratively** searching through networks to detect and isolate advanced threats that evade existing security solutions"  

   (Wikipedia)

✓ **Cyber threat hunting** is “the practice of searching **iteratively** through data to detect advanced threats that evade traditional security solutions”  

   (sqrrl)
Hunting Threats in Your Enterprise

✔ Threat Hunting Plan
  ✔ Design Your Network For Hunting
  ✔ Get your Team Ready
  ✔ Know your Enterprise
  ✔ Know Your Adversary TTP
  ✔ Collect Hunt Data
  ✔ Create Hypotheses
  ✔ Start Hunting
Design Your Enterprise for Hunting
Design Your Enterprise for Hunting

Flat Switched Network

One large broadcast domain
Design Your Enterprise for Hunting

- Segmentation: Security Zones
- NTP: Network Time Protocol
- Protection/Detection: FW/IDS/IPS/DLP/Proxy
- Tapping: Dump PCAP Data
- Visibility: Enable Logging as required
Hunting Threats in Your Enterprise

✓ Know Your Enterprise
  ✓ Identify Assets
  ✓ Know Threats to Your Assets
  ✓ Prioritize (High Value / Critical Assets First)
  ✓ Baselining – Know what is normal?
A cyber kill chain is a ‘Lockheed Martin’ model that reveals the stages of a cyber attack from early reconnaissance to the goal of data exfiltration:

**RECON**
- Fingerprint
- Observation
- Open Source Intelligence (OSINT)

**WEAPONIZE**
- Lures
- Zero-Day / Exploit Kit (EK)
- Social Engineering

**DELIVERY**
- Waterhole
- Spear-phish
- Man-in-the-Middle Attack (MITM)

**EXPLOIT**
- Installation
- Dropper
- Downloader

**INSTALL**
- Installation
- Elevation of Privilege (EOP)/Gain Privilege
- Persistence

**Command & Control (C2)**
- Exploration
- Info gathering
- Lateral Movements

**ACTIONS**
- Exfiltration
- Destruction
- Compromise

Attacks in Planning
Attacks in Progress
Attacks already Happening

Hunting Threats in Your Enterprise

Know Your Adversary – Mitre ATT&CK

<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>Exfiltration</th>
<th>Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive-by Compromise</td>
<td>AppleScript</td>
<td>bash_profile and bashic</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>Automated Exfiltration</td>
<td>Commonly Used Port</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>Data Compressed</td>
<td>Communication Through Removable Media</td>
</tr>
<tr>
<td>Hardware Additions</td>
<td>Command-Line Interface</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>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>Appinit DLLs</td>
<td>AppInit DLLs</td>
<td>Bypass User Account Control</td>
<td>Credential Dumping</td>
<td>File and Directory Discovery</td>
<td>Exploitation of Remote Services</td>
<td>Data Slaged</td>
<td>Data Transfer Size Limits</td>
<td>Custom Command and Control</td>
<td></td>
</tr>
<tr>
<td>Spear phishing Attachment</td>
<td>Dynamic Data Exchange</td>
<td>Application Shimming</td>
<td>Application Shimming</td>
<td>CMSTP</td>
<td>Credentials in Files</td>
<td>Network Service Scanning</td>
<td>Logon Scripts</td>
<td>Data from Information Repositories</td>
<td>Exfiltration Over Alternative Protocol</td>
<td>Custom Cryptographic Protocol</td>
</tr>
<tr>
<td>Spear phishing Link</td>
<td>Execution through API</td>
<td>Authentication Package</td>
<td>Bypass User Account Control</td>
<td>Clear Command History</td>
<td>Credentials in Registry</td>
<td>Network Share Discovery</td>
<td>Pass the Hash</td>
<td>Data from Local System</td>
<td>Exfiltration Over Command and Control Channel</td>
<td>Data Encoding</td>
</tr>
<tr>
<td>Spear phishing via Service</td>
<td>Execution through Module Load</td>
<td>BITS Jobs</td>
<td>DLL Search Order Hijacking</td>
<td>Code Signing</td>
<td>Exploitation for Credential Access</td>
<td>Password Policy Discovery</td>
<td>Pass the Ticket</td>
<td>Data from Network Shared Drive</td>
<td>Exfiltration Over Other Network Medium</td>
<td>Data Obfuscation</td>
</tr>
<tr>
<td>Supply Chain Compromise</td>
<td>Exploitation for Client Execution</td>
<td>Bootkit</td>
<td>Dylib Hijacking</td>
<td>Component Firmware</td>
<td>Forced Authentication</td>
<td>Peripheral Device Discovery</td>
<td>Remote Desktop Protocol</td>
<td>Data from Removable Media</td>
<td>Exfiltration Over Physical Medium</td>
<td>Domain Fronting</td>
</tr>
<tr>
<td>Trusted Relationship</td>
<td>Graphical User Interface</td>
<td>Browser Extensions</td>
<td>Exploitation for Privilege Escalation</td>
<td>Component Object Model Hijacking</td>
<td>Hooking</td>
<td>Permission Groups Discovery</td>
<td>Remote File Copy</td>
<td>Email Collection</td>
<td>Scheduled Transfer</td>
<td>Fallback Channels</td>
</tr>
<tr>
<td>Valid Accounts</td>
<td>InstallUtil</td>
<td>Change Default File Association</td>
<td>Extra Window Memory Injection</td>
<td>Control Panel Items</td>
<td>Input Capture</td>
<td>Process Discovery</td>
<td>Remote Services</td>
<td>Input Capture</td>
<td>Multi-Stage Channels</td>
<td></td>
</tr>
</tbody>
</table>

ATT&CK = Adversarial Tactics, Techniques, and Common Knowledge

Abdulrahman Al-Nimari | BSides Conference, Dubai 27-28, November, 2018 | @nimari | https://www.linkedin.com/in/alnimari/
## Collect Hunt Data

### Data Domains:

<table>
<thead>
<tr>
<th>Network</th>
<th>Host</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Flow Data - NetFlow</td>
<td>- AV/EDR/FW</td>
<td>- Authentication</td>
</tr>
<tr>
<td>- PCAP</td>
<td>- Windows/Sysmon Events</td>
<td>- Transaction Logs</td>
</tr>
<tr>
<td>- DNS</td>
<td>- File System</td>
<td>- DB Logs</td>
</tr>
<tr>
<td>- Proxy Logs</td>
<td>- Autoruns</td>
<td>- Security Alerts</td>
</tr>
<tr>
<td>- FW/SW/Routers</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Log Data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PCAP Data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Netflow</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Threat Intelligence Data</td>
<td></td>
</tr>
</tbody>
</table>

- ✓ Log Data
- ✓ PCAP Data
- ✓ Netflow
- ✓ Threat Intelligence Data
Hunting Threats in Your Enterprise

✓ Threat Intelligence Feeds (Open Source)
  ✓ https://otx.alienvault.com/
  ✓ https://www.iocbucket.com/
  ✓ https://abuse.ch/
  ✓ https://www.blocklist.de/
  ✓ https://www.virustotal.com/
  ✓ https://malwr.com/
  ✓ ……
# Creating Hypothesis

<table>
<thead>
<tr>
<th>Hypotheses</th>
<th>Data (Where to Hunt)</th>
<th>What to look for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Staging/Exfiltration ?</td>
<td>PCAPS, NetFlow</td>
<td>Compressed Files</td>
</tr>
<tr>
<td>Lateral Movement ?</td>
<td>PCAPS, Logs</td>
<td>PSEXEC, Powershell</td>
</tr>
<tr>
<td>Fileless Malware ?</td>
<td>PCAPS, NetFlow</td>
<td>Powershell, WMI</td>
</tr>
<tr>
<td>Command &amp; Control (C2) ?</td>
<td>HTTP, Bro Logs</td>
<td>MaliciousURLs/Domains/User agent/DNS</td>
</tr>
<tr>
<td>...........</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Hunting Cycle

Iterate aggressively through this cycle

Hunting Maturity Model

INITIAL
- Relies primarily on automated alerting.
- Little or no routine data collection.

MINIMAL
- Incorporates threat intelligence indicator searches.
- Moderate or high level of routine data collection.

PROCEDURAL
- Follows data analysis procedures created by others.
- High or very high level of routine data collection.

INNOVATIVE
- Creates new data analysis procedures.
- High or very high level of routine data collection.
- Automates the majority of successful data analysis procedures.
- High or very high level of routine data collection.

Hunting Threats in Your Enterprise

Pyramid of Pain

http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Abdulrahman Al-Nimari | BSides Conference, Dubai 27-28, November, 2018 | @nimari | https://www.linkedin.com/in/alnimari/
Hunting in Action #1

1. Malicious IP Address(es) → Network Flow → Internal IP
2. Network Flow → Anomaly → Time Stamp
3. Investigate PCAP/Logs
Hunting Threats in Your Enterprise

Hunting in Action #2

<table>
<thead>
<tr>
<th>Autorun Entry</th>
<th>Description</th>
<th>Publisher</th>
<th>Image Path</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</td>
<td>SecurityHealth: Windows Defender notification...</td>
<td>Microsoft Corporation</td>
<td>9/7/2018 3:56 PM</td>
<td></td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</td>
<td>VMware User Processare Tools Core Service</td>
<td>VMware, Inc.</td>
<td>3/22/2018 12:23 PM</td>
<td></td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</td>
<td>MEGAsync\link</td>
<td>MEGAsync</td>
<td>8/20/2018 7:06 PM</td>
<td></td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components</td>
<td>Google Chrome</td>
<td>Google Inc.</td>
<td>5/23/2018 8:49 PM</td>
<td></td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</td>
<td>Themes Setup</td>
<td>Google Chrome Installer</td>
<td>8/8/2018 1:05 AM</td>
<td></td>
</tr>
<tr>
<td>HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</td>
<td>OneDrive</td>
<td>Microsoft Corporation</td>
<td>8/1/2018 5:11 AM</td>
<td></td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Classes\Protocol\Handler</td>
<td>mso-mnsb-16</td>
<td>Microsoft Office 2016</td>
<td>11/24/2017 1:24 PM</td>
<td></td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Classes\Protocol\Handler</td>
<td>mso-mnsb-16</td>
<td>Microsoft Office 2016</td>
<td>11/24/2017 1:24 PM</td>
<td></td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Classes\Protocol\Handler</td>
<td>ost-roaming-16</td>
<td>Microsoft Office 2016</td>
<td>11/24/2017 1:24 PM</td>
<td></td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Classes\Protocol\Handler</td>
<td>ost-16</td>
<td>Microsoft Office 2016</td>
<td>11/24/2017 1:24 PM</td>
<td></td>
</tr>
<tr>
<td>HKCU\SOFTWARE\Classes\ShellEx\ContextMenuHandlers</td>
<td>FileSyncEx</td>
<td>Microsoft OneDrive Shell Ex</td>
<td>8/1/2018 5:10 AM</td>
<td></td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Classes\ShellEx\ContextMenuHandlers</td>
<td>7-Zip Shell Extension</td>
<td>Igor Pavlov</td>
<td>5/13/2015 8:24 PM</td>
<td></td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Classes\ShellEx\ContextMenuHandlers</td>
<td>ANotepad++-64 ShellHandler for Notepad++</td>
<td></td>
<td>5/12/2014 12:49 PM</td>
<td></td>
</tr>
</tbody>
</table>
Hunting Threats in Your Enterprise

Hunting in Action #2

1. Deploy autorunsc.exe to EP
2. Collect Results in SIEM
3. Compare to Baseline/VT Hash DB
4. Anomalies
5. Investigate
6. Automate
Hunting Threats in Your Enterprise

✓ Measuring Success (Metrics)

✓ Number of Incidents by severity
✓ Number of Compromised Hosts
✓ Dwell Time of Incidents Discovered.
✓ Logging Gaps Identified and Corrected
✓ Vulnerabilities Identified
✓ Insecure Practices Identified and Corrected
✓ Hunts Transitioned to Analytics
✓ New Visibilities Gained

Hunting Threats in Your Enterprise

✓ Resources

✓ https://www.threathunting.net/
✓ https://threathunting.org/
✓ https://intel.criticalstack.com/
✓ https://www.mitre.org/
✓ https://www.elastic.co/
✓ https://github.com/Cyb3rWard0g/ThreatHunter-Playbook
✓ https://nxlog.co/
✓ https://docs.microsoft.com/en-us/sysinternals/
Q & A
Thank You