Getting Started with Risk-Based Alerting and MITRE

Bryan Turner
IT Security Analyst | Publix
During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.
Introduction

So what are we getting into?
Previous .conf Presentations

Check These Out!

If you want to know more about:

Building and Enriching Correlation Searches
• The Art of Detection
  - Doug Brown

Risk Framework
• Say Goodbye to Your Big Alert Pipeline, and Say Hello to Your New Risk-Based Approach
  - Jim Apger, Stuart McIntosh

Testing Your Detections
• Simulating the Adversary to Test Your Splunk Security Analytics
  - Dave Herrland, Kyle Champlin, Tim Frazier
Putting It All Together

Risk

Searches

Testing
1. What is Risk-Based Alerting?
2. Creating a Risk Matrix
3. Building Search Inventory
4. Developing Targeted Detections
5. Operationalizing Alerting
6. Ongoing Maintenance
Terminology

What are we talking about?

1. Alert: search that requires an action
2. Search: correlation searches
3. Entity: system or user
4. Asset: system
5. Identity: user
6. Fidelity: measurement of accuracy of an alert
What is Risk-Based Alerting?

Deriving value from atomic alerts
The Coffee Filter Problem

Moving Past a Messy Solution
Background
What is the old model and why doesn’t it work?

One to One Alert Model

- Alert fatigue – difficulties scaling
- Over-zealous Exclusions
- Little to no correlation
- Unanswered Questions
The Unanswered Questions

“So what’s going on?”
- Every Manager Ever

“Were there any other alerts?”
- The Concerned Manager

“Where did it come from?”
- The Curious Manager
Problem/Solution

Problem:

Alerts that provide little context and are not efficiently utilizing analyst's time.

Solution:

Build a risk-based alerting system that increases accuracy of alerts and provides a readily available "alert narrative."
“The Risk Analysis framework provides the ability to identify actions that raise the risk profile of individuals or assets.”

Risk Analysis framework in Splunk ES
Risk Monitoring - Mitre

This dashboard monitors aggregated risk events.

Time: Aug 1 through 16, 2019
Attack Phase Methodology: Mitre
Risk Object: bryanturner
Min Risk Score: 0
Threat Actor:

<table>
<thead>
<tr>
<th>Phase</th>
<th>Recon</th>
<th>Deliver</th>
<th>Exploit</th>
<th>Control</th>
<th>Execute</th>
<th>Maintain</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No results found.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No results found.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No results found.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Known Threat Actor</th>
<th>Known Threat Actor</th>
<th>Known Threat Actor</th>
<th>Known Threat Actor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Actor</td>
<td>Threat_Actor</td>
<td>Threat_Actor</td>
<td>Threat_Actor</td>
</tr>
<tr>
<td>Generic</td>
<td>1</td>
<td>Generic</td>
<td>2</td>
</tr>
<tr>
<td>No results found.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Risk Alerting Pipeline

Correlation Searches

Risk Profile Increases

Risk Alerts
How Does This Look in Practice?

Total Risk Score = 120

*Note: None of these searches had enough accuracy to be included in old model.*
“So what’s going on?”

“Were there any other alerts?”

“Where did it come from?”
Recap

One-to-One Model
Small inventory of high accuracy searches
Does not give context to related activity
Analysts investigate each alert
Does not scale smoothly
  • More searches typically means more tickets and analyst hours.

Risk-based Model
Large inventory of both high and low accuracy searches
Does give context to related activity
Analysts perform investigations on high risk entities
Scales smoothly
  • More searches doesn’t mean more investigations. Conditions still must be met.
## Phases of Development

**Building an Search Inventory**

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a Risk Matrix</td>
<td></td>
</tr>
<tr>
<td>Building a Search Inventory</td>
<td></td>
</tr>
<tr>
<td>Developing Targeted Detections</td>
<td></td>
</tr>
<tr>
<td>Operationalize Alerting</td>
<td></td>
</tr>
<tr>
<td>Ongoing Maintenance</td>
<td></td>
</tr>
</tbody>
</table>
Creating a Risk Matrix

“Begin, the rest is easy”
Recommended Prerequisites
Things we had in place prior to starting the move to risk-based alerting… or wish we had.

Splunk Enterprise Security

Identity Management
• Systems (assets)
• Users (identities)

Search Inventory Lookup
• Contain all correlation searches
• Need to be easily scalable
# Alert Matrix

## Getting Started

### Fidelity

<table>
<thead>
<tr>
<th>Risk</th>
<th>&gt;50%</th>
<th>10%-50%</th>
<th>&lt;10%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>High</td>
<td>Low</td>
<td>Informational</td>
</tr>
<tr>
<td>Moderate</td>
<td>High</td>
<td>Low</td>
<td>Informational</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Informational</td>
<td>Informational</td>
</tr>
</tbody>
</table>

**Fidelity** is a historical measurement of the alert’s capability to successfully detect malicious activity.

**Potential Risk** is a categorical measurement based on a confluence of data sensitivity, business impact, and likelihood.
Risk Matrix
Getting Started

<table>
<thead>
<tr>
<th>Severity</th>
<th>Base Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informational</td>
<td>20</td>
</tr>
<tr>
<td>Low</td>
<td>50</td>
</tr>
<tr>
<td>High</td>
<td>100</td>
</tr>
</tbody>
</table>

- Risk is assigned through the Risk Analysis Alert action
- Risk is assigned to a user or system
- Set with threshold of 100 in mind
<table>
<thead>
<tr>
<th>ATTACK</th>
<th>Technique</th>
<th>RiskObjectType</th>
<th>RiskScore</th>
<th>RuleName</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deliver</td>
<td>T1193 - Spearphishing Attachment</td>
<td>user</td>
<td>20</td>
<td>Suspicous Subject in Email</td>
</tr>
<tr>
<td>Exploit</td>
<td>T1203 - Exploitation for Client Execution</td>
<td>user</td>
<td>20</td>
<td>Outlook Opening Office</td>
</tr>
<tr>
<td>Exploit</td>
<td>T1203 - Exploitation for Client Execution</td>
<td>user</td>
<td>20</td>
<td>Office Opening Browser</td>
</tr>
<tr>
<td>Control</td>
<td>T1203 - Exploitation for Client Execution</td>
<td>system</td>
<td>50</td>
<td>Blocked IDS Outbound</td>
</tr>
<tr>
<td>Deliver</td>
<td>T1192 - Spearphishing Link</td>
<td>user</td>
<td>20</td>
<td>Suspicious Link in Email</td>
</tr>
<tr>
<td>Exploit</td>
<td>T1192 - Spearphishing Link</td>
<td>user</td>
<td>20</td>
<td>Suspicious Link Clicked From Email</td>
</tr>
<tr>
<td>Exploit</td>
<td>T1023 - Shortcut Modification</td>
<td>user</td>
<td>20</td>
<td>LNK File Run From Browser</td>
</tr>
<tr>
<td>Execute</td>
<td>T1047 - Windows Management Instrumentation</td>
<td>system</td>
<td>50</td>
<td>WMIC.exe Downloading from External Site</td>
</tr>
<tr>
<td>Execute</td>
<td>T1197 - BITS Jobs</td>
<td>system</td>
<td>100</td>
<td>Bitsadmin.exe Downloading from External Site</td>
</tr>
<tr>
<td>Execute</td>
<td>T1140 - Deobfuscate/Decode Files or Information</td>
<td>system</td>
<td>100</td>
<td>Certutil.exe Used to Decode Payload</td>
</tr>
<tr>
<td>Execute</td>
<td>T1117 - Regsvr32</td>
<td>system</td>
<td>20</td>
<td>Regsvr32 Executed</td>
</tr>
<tr>
<td>Execute</td>
<td>T1115 - Clipboard Data</td>
<td>system</td>
<td>20</td>
<td>OpenClipboard() or GetClipboardData() Executed</td>
</tr>
<tr>
<td>Execute</td>
<td>T1083 - Credential Access</td>
<td>system</td>
<td>100</td>
<td>Use Password Recovery Tool Netpass Detected</td>
</tr>
</tbody>
</table>
Adaptive Response Actions

+ Add New Response Action

- Risk Analysis
  - Risk Score*: 100
  - Risk Object Field*: host
  - Risk Object Type*: system

Learn more about risk modifiers.

- Notable

- Send email
Sendalert
Customer Alert Actions

Use the **sendalert** command to:

- Create notable events
- Add or Subtract risk scores
- Generate tickets
- And more!
sourcetype=WinEventLog Source=WinEventLog:Security EventCode=4688 Command="*psexec.exe*"
| table host user Process_Command_Line
| sendalert notable
| sendalert risk param._risk_object="User" param._risk_object_type="user" param.risk_score="50"
### Alert Matrix

#### Base Value

<table>
<thead>
<tr>
<th>Severity</th>
<th>Base Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informational</td>
<td>20</td>
</tr>
<tr>
<td>Low</td>
<td>40</td>
</tr>
<tr>
<td>Medium</td>
<td>60</td>
</tr>
<tr>
<td>High</td>
<td>80</td>
</tr>
<tr>
<td>Critical</td>
<td>100</td>
</tr>
</tbody>
</table>

#### Getting Fancy

<table>
<thead>
<tr>
<th>Fidelity</th>
<th>Multiplier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low &lt;10%</td>
<td>0.50</td>
</tr>
<tr>
<td>Medium 10%-50%</td>
<td>0.75</td>
</tr>
<tr>
<td>High &gt;50%</td>
<td>1.00</td>
</tr>
</tbody>
</table>

#### Criticality

<table>
<thead>
<tr>
<th>Asset/Identity</th>
<th>Multiplier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>1</td>
</tr>
<tr>
<td>Elevated</td>
<td>2</td>
</tr>
<tr>
<td>Enterprise</td>
<td>3</td>
</tr>
</tbody>
</table>

*Note: Use values that work best for YOUR environment*
Inline Coding

More Flexibility

```bash
| table _time host user Message RuleName
| lookup identities.csv identity as user OUTPUT identity_criticality
| lookup assets.csv nt_host as host OUTPUT asset_criticality
| lookup search_inventory.csv Rule_Name as RuleName OUTPUT Base_Value Fidelity
| eval risk_score=Base_Value * Fidelity * identity_criticality
| sendalert risk param._risk_object="user" param._risk_object_type="user" param._risk_score="risk_score"
| eval risk_score=Base_Value * Fidelity * asset_criticality
| sendalert risk param._risk_object="host" param._risk_object_type="system" param._risk_score="risk_score"
```
Building a Search Inventory

Laying the foundation
Search Inventory Sources
So where is all this information going to come from?

Existing Search Inventory
MITRE ATT&CK
Security Essentials
Content Update
# Enterprise Matrix

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

Last Modified: 2019-07-01 17:29:39.726000

<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>basic_profile</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Manipulation</td>
<td>Account Discovery</td>
<td>Audio Capture</td>
<td>Command Use Port</td>
<td>Automated Collection</td>
<td>Exfiltration</td>
<td>Data Destruction</td>
</tr>
<tr>
<td>Expert Public-Facing Application CMSTP</td>
<td>Accessibility Features</td>
<td>Accessibility Features</td>
<td>Binary Padding</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>
<td></td>
</tr>
<tr>
<td>External Remote Services Command-Line Interface</td>
<td>Account Manipulation</td>
<td>AppCert DLLs</td>
<td>BITS Jobs</td>
<td>Brute Force</td>
<td>Browser Bookmark Discovery</td>
<td>Distributed Component Object Model</td>
<td>Data Exfiltration</td>
<td>Data Exfiltration</td>
<td>Data Exfiltration</td>
<td>Data Exfiltration</td>
<td>Data Exfiltration</td>
</tr>
<tr>
<td>Hardware Additions</td>
<td>Compiled HTML File</td>
<td>AppCert DLLs</td>
<td>Bypass User Account Control</td>
<td>Credential Dumping</td>
<td>Domain Trust Discovery</td>
<td>Exportation of Remote Services</td>
<td>Data from Information Repositories</td>
<td>Custom Command and Control Protocol</td>
<td>Data Transfer Size Limits</td>
<td>Disk Content Wipe</td>
<td></td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>Control Panel Items</td>
<td>AppCert DLLs</td>
<td>Application Shimming</td>
<td>Clear Command History</td>
<td>Credentials in Files</td>
<td>File and Directory Discovery</td>
<td>Logon Scripts</td>
<td>Data from Local System</td>
<td>Custom Cryptographic Protocol</td>
<td>Exfiltration Over Alternative Protocol</td>
<td>Disk Structure Wipe</td>
</tr>
<tr>
<td>Spear phishing Attachment Dynamic Data Exchange</td>
<td>Application Shimming</td>
<td>Bypass User Account Control</td>
<td>CMSTP</td>
<td>Credentials in Registry</td>
<td>Network Service Scanning</td>
<td>Pass the Hash</td>
<td>Data from Network Shared Drive</td>
<td>Data Encoding</td>
<td>Exfiltration Over Command and Control Channel</td>
<td>Endpoint Denial of Service</td>
<td></td>
</tr>
<tr>
<td>Spear phishing Link</td>
<td>Execution through API</td>
<td>Authentication Package</td>
<td>DLL Search Over Hijacking</td>
<td>Code Signing</td>
<td>Exploitation for Credential Access</td>
<td>Network Share Discovery</td>
<td>Pass the Ticket</td>
<td>Data from Removable Media</td>
<td>Data Exfiltration</td>
<td>Exfiltration Over Other Network Medium</td>
<td>Firmware Corruption</td>
</tr>
<tr>
<td>Spear phishing via Service Execution through Module Load</td>
<td>BITS Jobs</td>
<td>Direct Hijacking</td>
<td>Compile After Delivery</td>
<td>Forced Authentication</td>
<td>Network Sniffing</td>
<td>Remote Desktop Protocol</td>
<td>Data Slaged</td>
<td>Domain Fronting</td>
<td>Exfiltration Over Physical Medium</td>
<td>Inhibit System Recovery</td>
<td></td>
</tr>
<tr>
<td>Supply Chain Compromise</td>
<td>Exploitation for Client Execution</td>
<td>Beostix</td>
<td>Exploitation for Privilege Escalation</td>
<td>Compiled HTML File</td>
<td>Hooking</td>
<td>Password Policy Discovery</td>
<td>Remote File Copy</td>
<td>Email Collection</td>
<td>Domain Generation Algorithms</td>
<td>Scheduled Transfer</td>
<td>Network Denial of Service</td>
</tr>
</tbody>
</table>
Account Discovery

Adversaries may attempt to get a listing of local system or domain accounts.

Windows

Example commands that can acquire this information are `net user`, `net group`, and `net localgroup` using the Net utility or through use of `dsquery`. If adversaries attempt to identify the primary user, currently logged in user, or set of users that commonly uses a system, System Owner/User Discovery may apply.

Mac

On Mac, groups can be enumerated through the `groups` and `id` commands. In mac specifically, `dcs1 list /Groups` and `dscaheutil -q group` can also be used to enumerate groups and users.

Linux

On Linux, local users can be enumerated through the use of the `/etc/passwd` file which is world readable. In mac, this same file is only used in single-user mode in addition to the `/etc/master.passwd` file.

Also, groups can be enumerated through the `groups` and `id` commands.

Mitigations
MITRE
Techniques In-Depth

• Use examples to identify search terms
• Split into different severity alerts by fidelity
• Focus on threat actors that are the greatest risk

Table:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin@338</td>
<td>Used the following commands following exploitation of a machine with LOWBALL malware to enumerate user accounts.</td>
</tr>
<tr>
<td>Agent Tesla</td>
<td>Collects account information from the victim's machine.</td>
</tr>
<tr>
<td>APT1</td>
<td>Used the commands <code>net localgroup net user</code> and <code>net group</code> to find accounts on the system.</td>
</tr>
<tr>
<td>APT3</td>
<td>Has used a tool that can obtain info about local and global group users, power users, and administrators.</td>
</tr>
<tr>
<td>APT32</td>
<td>Enumerated administrative users and DC servers using the commands <code>net localgroup administrators</code> and <code>net group &quot;Domain Controllers&quot; /domain</code>.</td>
</tr>
<tr>
<td>Bankshot</td>
<td>Gathers domain and account names/information through process monitoring.</td>
</tr>
<tr>
<td>BRONZE BUTLER</td>
<td>Used the <code>net user</code> command to identify account information.</td>
</tr>
<tr>
<td>Carbon</td>
<td>Runs the <code>net group</code> command to list accounts on the system.</td>
</tr>
<tr>
<td>Connie</td>
<td>Uses the <code>net user</code> command.</td>
</tr>
</tbody>
</table>
Security Essentials

Security Content / Windows Event Log Clearing Events

Description
This use case looks for Windows event codes that indicate the Windows Audit Logs were tampered with.

Use Case
Advanced Threat Detection

Category
Endpoint Compromise

Alert Volume
Low

SPL Difficulty
Basic

Stage 1
MITRE ATT&CK Tactics
- Defensive Evasion
- Kill Chain Phases
- Actions on Objective
- Data Sources
- Windows Security

Related Splunk Capabilities
- How to Implement
- Known False Positives
- How To Respond
- Show Search
- Help
Content Update
Using MITRE for Targeted Detections

Building your narratives
Prioritizing Alert Creation

What tools do you need?

MITRE ATT&CK
ATT&CK Navigator
Malware Archaeology
OSINT
### ATT&CK NAVIGATOR

- **List techniques by threat actor or malware**
- **Layer different views to form a heat map**

#### Initial Access
- **Application**:-artifact
- **Injection**:-artifact
- **Local Security Mitigations**:-artifact
- **Remote Services**:-artifact
- **Trusted Relationship**:-artifact
- **Valid Accounts**:-artifact

#### Execution
- **Application**:-artifact
- **Code**:-artifact
- **Operating System**:-artifact
- **Remote Services**:-artifact
- **Trusted Relationship**:-artifact
- **Valid Accounts**:-artifact

#### Persistence
- **Application**:-artifact
- **Code**:-artifact
- **Operating System**:-artifact
- **Remote Services**:-artifact
- **Trusted Relationship**:-artifact
- **Valid Accounts**:-artifact

#### Privilege Escalation
- **Application**:-artifact
- **Code**:-artifact
- **Operating System**:-artifact
- **Remote Services**:-artifact
- **Trusted Relationship**:-artifact
- **Valid Accounts**:-artifact

#### Defense Evasion
- **Application**:-artifact
- **Code**:-artifact
- **Operating System**:-artifact
- **Remote Services**:-artifact
- **Trusted Relationship**:-artifact
- **Valid Accounts**:-artifact

#### Credential Access
- **Application**:-artifact
- **Code**:-artifact
- **Operating System**:-artifact
- **Remote Services**:-artifact
- **Trusted Relationship**:-artifact
- **Valid Accounts**:-artifact

#### Discovery
- **Application**:-artifact
- **Code**:-artifact
- **Operating System**:-artifact
- **Remote Services**:-artifact
- **Trusted Relationship**:-artifact
- **Valid Accounts**:-artifact

#### Lateral Movement
- **Application**:-artifact
- **Code**:-artifact
- **Operating System**:-artifact
- **Remote Services**:-artifact
- **Trusted Relationship**:-artifact
- **Valid Accounts**:-artifact

#### Collection
- **Application**:-artifact
- **Code**:-artifact
- **Operating System**:-artifact
- **Remote Services**:-artifact
- **Trusted Relationship**:-artifact
- **Valid Accounts**:-artifact

#### Command And Control
- **Application**:-artifact
- **Code**:-artifact
- **Operating System**:-artifact
- **Remote Services**:-artifact
- **Trusted Relationship**:-artifact
- **Valid Accounts**:-artifact

#### Exfiltration
- **Application**:-artifact
- **Code**:-artifact
- **Operating System**:-artifact
- **Remote Services**:-artifact
- **Trusted Relationship**:-artifact
- **Valid Accounts**:-artifact

#### Impact
- **Application**:-artifact
- **Code**:-artifact
- **Operating System**:-artifact
- **Remote Services**:-artifact
- **Trusted Relationship**:-artifact
- **Valid Accounts**:-artifact
<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>Command Line Interface</td>
<td>Compromised</td>
<td>Adobe, Microsoft</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Application Window Discovery</td>
<td>Audio Capture</td>
<td>Automated Exfiltration</td>
<td>Data Destruction</td>
<td>Cake</td>
<td>Data Exposed</td>
</tr>
<tr>
<td>Exploit Public-Facing Application</td>
<td></td>
<td>Compromised</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal Remote Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Heritage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Additions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Through</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Removable Media</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spoofing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attachment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spooling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Looping via</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply Chain Compromise</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trusted Relationship</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Valid Accounts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2019 SPLUNK INC.
Building a Heat Map

Identifying Priority

High Priority Items

• Command-Line Interface
• Scripting
• Credential Dumping
• Remote Desktop Protocol
• Data Compressed
# Malware Archaeology

[https://www.malwarearchaeology.com/logging](https://www.malwarearchaeology.com/logging)

Log sources by Tactic>Technique

Highlights whether coverage is:

- Good
- Incomplete
- None

<table>
<thead>
<tr>
<th>Tactic</th>
<th>Technique</th>
<th>Source</th>
<th>Process Execution</th>
<th>Process CMD Line</th>
<th>API monitoring</th>
<th>Events</th>
<th>DLL monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Discovery</strong></td>
<td>System Owner/User Discovery</td>
<td></td>
<td>4688</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>System Service Discovery</td>
<td></td>
<td>4688</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>System Time Discovery</td>
<td></td>
<td>4688</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Execution</strong></td>
<td>Command-Line Interface</td>
<td></td>
<td>4688</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dynamic Data Exchange</td>
<td></td>
<td>4688</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Execution through API</td>
<td></td>
<td>4688</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Execution through Module Load</td>
<td></td>
<td>4688</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Exploitation for Client Execution</td>
<td></td>
<td>4688</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Graphical User Interface</td>
<td></td>
<td>4688</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PowerShell</td>
<td></td>
<td>4688</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Malware Archaeology

https://www.malwarearchaeology.com/logging

Recommended Sources:

- Event Code 4688
  - Process Execution
  - Process CMD Line
- PowerShell
- Sysmon
OSINT
Digging Deeper

SANS
Talos
Microsoft
Twitter
Google
Personal Research
Operationalizing Alerting

Reading the narrative
Walkthrough
Astaroth – Known Techniques

- Astaroth
- Delivered via email
- Downloads additional payloads
- Installs a trojan to steal information
Walkthrough
Astaroth - OSINT

Microsoft Write-up

1. Arrival
2. WMIC abuse, part 1
3. WMIC abuse, part 2
4. Bitsadmin abuse
5. Certutil abuse
6. Regsvr32 abuse
7. Userinit abuse
Walkthrough

Astaroth – Building Detections

Shortcut Modification

• Malicious LNK shortcuts

Obfuscated Files or Information

• Obfuscated jscript

Deobfuscate/Decode Files or Information

• Uses fromCharCode()
<table>
<thead>
<tr>
<th>Tactic</th>
<th>Technique</th>
<th>RiskObject</th>
<th>RiskScore</th>
<th>RiskObject</th>
<th>RuleName</th>
<th>Threat Actor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deliver</td>
<td>Initial Access</td>
<td>user</td>
<td>20</td>
<td>recipient</td>
<td>Suspicious Subject in Email</td>
<td>Generic</td>
</tr>
<tr>
<td></td>
<td>Exploit Execution for Client Execution</td>
<td>user</td>
<td>20</td>
<td>Account</td>
<td>Outlook Opening Office</td>
<td>Generic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>user</td>
<td>20</td>
<td>Account</td>
<td>Office Opening Browser</td>
<td>Generic</td>
</tr>
<tr>
<td>Control</td>
<td>Execution</td>
<td>system</td>
<td>40</td>
<td>host</td>
<td>Blocked IDS Outbound</td>
<td>Generic</td>
</tr>
<tr>
<td></td>
<td>Exploit Execution for Client Execution</td>
<td>system</td>
<td>40</td>
<td>host</td>
<td>Blocked IDS Outbound</td>
<td>Generic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>user</td>
<td>10</td>
<td>recipient</td>
<td>Suspicious Link in Email</td>
<td>Generic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>user</td>
<td>20</td>
<td>Account_Name</td>
<td>Suspicious Link Clicked From Email</td>
<td>Astaroth</td>
</tr>
<tr>
<td></td>
<td></td>
<td>user</td>
<td>20</td>
<td>Account_Name</td>
<td>LNK File Run From Email</td>
<td>Astaroth</td>
</tr>
<tr>
<td>Execute</td>
<td>Execution</td>
<td>system</td>
<td>50</td>
<td>host</td>
<td>WMIC.exe Downloading from External Site</td>
<td>Astaroth</td>
</tr>
<tr>
<td></td>
<td>Defense Evasion</td>
<td>system</td>
<td>100</td>
<td>host</td>
<td>Bitsadmin.exe Downloading from External Site</td>
<td>Astaroth</td>
</tr>
<tr>
<td></td>
<td>Defense Evasion</td>
<td>system</td>
<td>100</td>
<td>host</td>
<td>Certutil.exe Used to Decode Payload</td>
<td>Astaroth</td>
</tr>
<tr>
<td></td>
<td></td>
<td>system</td>
<td>10</td>
<td>host</td>
<td>Regsvr32 Executed</td>
<td>Astaroth</td>
</tr>
<tr>
<td></td>
<td></td>
<td>system</td>
<td>10</td>
<td>host</td>
<td>Regsvr32 Executed</td>
<td>Astaroth</td>
</tr>
<tr>
<td></td>
<td>Collection</td>
<td>system</td>
<td>10</td>
<td>host</td>
<td>OpenClipboard() or GetClipboardData() Executed</td>
<td>Generic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>system</td>
<td>100</td>
<td>host</td>
<td>Use Password Recovery Tool Netpass Detected</td>
<td>Astaroth</td>
</tr>
<tr>
<td></td>
<td></td>
<td>system</td>
<td>100</td>
<td>host</td>
<td>Use Password Recovery Tool Netpass Detected</td>
<td>Astaroth</td>
</tr>
</tbody>
</table>
Walkthrough

Building a Dashboard

- Searches Risk and Notable indexes
- Aggregates Risk Score
- Identifies:
  - Phase
  - Count
  - Tactic
  - Technique
  - Threat Actor
Risk Monitoring - Mitre

This dashboard monitors aggregated risk events.

<table>
<thead>
<tr>
<th>Time</th>
<th>Attack Phase Methodology</th>
<th>Risk Object</th>
<th>Min Risk Score</th>
<th>Threat Actor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part of a Day</td>
<td>Mitre</td>
<td>byranturner</td>
<td>100</td>
<td>*</td>
</tr>
</tbody>
</table>

Recon

No results found.

Deliver

1

Exploit

2

Control

No results found.

Execute

No results found.

Maintain

No results found.

Tactic - Technique

Mitre_Tactic 

Initial Access

Persistence

No results found.

Tactic - Technique

Mitre_Technique 

T1023 - Shortcut Notification

T1192 - Spearphishing Link

No results found.

Known Threat Actor

No results found.

Known Threat Actor

No results found.

Known Threat Actor

No results found.

Known Threat Actor

No results found.

All Threat Actors

No results found.

Antarmath 2

Generic 1
Walkthrough Incident Review

- Search by risk object and severity
- Add all events to the same investigation
Walkthrough Building Investigations

• Add risk objects as artifacts
• Automate Data Gathering
  – Vulnerabilities
  – Risk Profiles
  – Web Activity
Ongoing Maintenance

Where do we go from here?
Next Steps

Maintenance

Risk Score Adjustment
Search Review
Threat Intelligence
Test Detections
Risk Score Adjustment

1. Calculation of fidelity
   • Changes lowered or raised percent

2. Criticality of entity
   • Do you need additional levels

3. Search weight
   • Is this causing too much noise
   • Is it not raising risk score fast enough
Search Review

1. Validate logic
   • Log format changes
   • Additional / Removed systems

2. Identify additional or deprecated search terms

3. Research additional detections
   • Is this search still needed?
Threat Intelligence

1. Efficient, Repeatable Process

2. Dedicated, Ongoing Investment
   - Sporadic research is not enough
   - More searches = better!

3. Re-evaluate Past Actors
   - We mature and so do they
Test Detections

Otherwise how do you know they work?

Internal Pentest

• Red Canary – Atomic Red Team
  – https://github.com/redcanaryco/atomic-red-team/tree/master/atomics

External Pentest

• Simulate threat differently

Annual Testing

• Things change!
Key Takeaways

Why do I care again?

1. Risk-based alerting will save you time and improve detection accuracy

2. Use MITRE to build an “alert narrative” to understand the context around an event

3. Investing more time in building a comprehensive risk framework will garner better results
RBA Related Sessions

SEC 1556 – Building Behavioral Detections: Cross-Correlating Suspicious Activity with the MITRE ATT&CK Framework
   – Tuesday, October 22, 1:45 PM – 2:30 PM

SEC1803 – Modernize and Mature Your SOC with Risk-Based Alerting
   – Tuesday, October 22, 3:00 PM – 3:45 PM

SEC1908 – Tales from a Threat Team: Lessons and Strategies for Succeeding with a Risk-Based Approach
   – Wednesday, October 23, 3:00 PM – 3:45 PM

Birds of the Feather – The RBA Community – join the RBA slack channel
   – SUGARCANE Raw Bar Grill – Tuesday 6:30 – 8:30
Thank You!

Go to the .conf19 mobile app to RATE THIS SESSION