ATT&CK™ Your CTI
with Lessons Learned
from Four Years in the Trenches
Katie Nickels
ATT&CK Threat Intelligence Lead
The MITRE Corporation
@LiketheCoins

Brian Beyer
Co-founder & CEO
Red Canary
Outline

How is ATT&CK useful for CTI?

A tale of two ATT&CK mapping approaches

What we learned from our data

How you can apply this data to improve defenses
ATT&CK: A Knowledge Base of Adversary Behavior

Tactics: the adversary’s technical goals

Procedures: Specific technique implementation

Scheduled Task Examples

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APT18</td>
<td>APT18 actors used the native Windows task scheduler tool to use scheduled tasks for execution on a victim network.</td>
</tr>
<tr>
<td>APT20</td>
<td>APT20 used named and hijacked scheduled tasks to establish persistence.</td>
</tr>
</tbody>
</table>
Why ATT&CK is Useful for CTI

Adds structure to allow comparison

Moves from IOCs → Behaviors

Makes intel actionable for defense
5 years of reviewing and mapping

~400 publicly-available threat intel reports
All of the backdoors identified - excluding RoyalDNS - required APT15 to create batch scripts in order to install its persistence mechanism. This was achieved through the use of a simple Windows run key.

Analysis of the commands executed by APT15 reaffirmed the group’s preference to 'live off the land'. They utilised Windows commands for reconnaissance activities such as `tasklist.exe`, `ping.exe`, `netstat.exe`, `nbtstat.exe`, `systeminfo.exe`, `ipconfig.exe` and `bcp.exe`. APT15 was also observed using Mimikatz to dump credentials and generate Kerberos golden tickets. This allowed the group to persist in the victim's network in the event of a security breach. The group also used keyloggers and their own .NET tool to enumerate folders and dump data from Microsoft Exchange mailboxes.
~400 publicly-available threat intel reports

Collection based on threat intel reports

Methodology Consequences / Biases

+ Thorough
+ Nuanced
+ Able to find techniques that require human analysis

- Slow and challenging to learn
- Subject to human biases
- Requires reports to input
5 years of security operations monitoring + ~200 IR engagements
---
api_version: v1

uuid: 1074

name: WIN-AUTORUN-REGMOD-CMD

state: active

detections:

red_canary_behavioral:
matcher: |

regmod_value_write_path_includes_any?(*autorun_keys) && process_is_likely?('cmd')

context:

description: |
  # Description
  This detector identifies the modification of known Windows Registry keys which trigger an application to start at boot or user login, using the Windows Command Processor (`cmd.exe`).

normal_behavior_notes: |
  Normal modification of Windows Registry autorun keys using `cmd.exe` will occur from SCCM packages, or authorized software installers.

malicious_behavior_notes: |
  Malicious modification of Windows Registry autorun keys using `cmd.exe` will occur from interactive shell execution, through unauthorized within a suspicious chain of execution. An example of this would be a `cmd.exe` one-liner spawning from a malicious MS Word document.

threat_intelligence: none

attack_techniques: 
- T1060
5 years of security operations monitoring
+ ~200 IR engagements

Methodology Consequences / Biases
+ Able to process large quantities of data
+ Consistent
+ Fast
+ Highly structured
- Only maps known techniques
- No nuance/interpretation
- Maps only to detection-worthy events

Collection based on day-to-day security operations
~400 publicly-available threat intel reports

5 years of security operations monitoring

+ 

~200 IR engagements

Why don’t we have both?

MITRE

red canary

This data set

KnowYourMeme.com
IF YOU COULD SHOW ME YOUR DATA

THAT WOULD BE GREAT
<table>
<thead>
<tr>
<th>#</th>
<th>Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Standard App Layer Protocol</td>
</tr>
<tr>
<td>2</td>
<td>Remote File Copy</td>
</tr>
<tr>
<td>3</td>
<td>System Information Discovery</td>
</tr>
<tr>
<td>4</td>
<td>Command-Line Interface</td>
</tr>
<tr>
<td>5</td>
<td>File and Directory Discovery</td>
</tr>
<tr>
<td>6</td>
<td>Registry Run Key/Startup Folder</td>
</tr>
<tr>
<td>7</td>
<td>Obfuscated Files or Information</td>
</tr>
<tr>
<td>8</td>
<td>File Deletion</td>
</tr>
<tr>
<td>9</td>
<td>Process Discovery</td>
</tr>
<tr>
<td>10</td>
<td>System Network Configuration Discovery</td>
</tr>
<tr>
<td>11</td>
<td>Credential Dumping</td>
</tr>
<tr>
<td>12</td>
<td>Screen Capture</td>
</tr>
<tr>
<td>13</td>
<td>Input Capture</td>
</tr>
<tr>
<td>14</td>
<td>System Owner/User Discovery</td>
</tr>
<tr>
<td>15</td>
<td>Scripting</td>
</tr>
<tr>
<td>16</td>
<td>Commonly Used Port</td>
</tr>
<tr>
<td>17</td>
<td>Standard Cryptographic Protocol</td>
</tr>
<tr>
<td>18</td>
<td>PowerShell</td>
</tr>
<tr>
<td>19</td>
<td>Masquerading</td>
</tr>
<tr>
<td>20</td>
<td>New Service</td>
</tr>
<tr>
<td>Rank</td>
<td>Technique</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>1</td>
<td>PowerShell</td>
</tr>
<tr>
<td>2</td>
<td>Scripting</td>
</tr>
<tr>
<td>3</td>
<td>Regsvr32</td>
</tr>
<tr>
<td>4</td>
<td>Connection Proxy</td>
</tr>
<tr>
<td>5</td>
<td>Spearphishing Attachment</td>
</tr>
<tr>
<td>6</td>
<td>Masquerading</td>
</tr>
<tr>
<td>7</td>
<td>Credential Dumping</td>
</tr>
<tr>
<td>8</td>
<td>Registry Run Keys / Start Folder</td>
</tr>
<tr>
<td>9</td>
<td>Rundll32</td>
</tr>
<tr>
<td>10</td>
<td>Service Execution</td>
</tr>
<tr>
<td>11</td>
<td>Disabling Security Tools</td>
</tr>
<tr>
<td>12</td>
<td>Command-Line Interface</td>
</tr>
<tr>
<td>13</td>
<td>Account Discovery</td>
</tr>
<tr>
<td>14</td>
<td>Accessibility Features</td>
</tr>
<tr>
<td>15</td>
<td>Scheduled Task</td>
</tr>
<tr>
<td>16</td>
<td>WMI</td>
</tr>
<tr>
<td>17</td>
<td>Process Injection</td>
</tr>
<tr>
<td>18</td>
<td>Obfuscated Files or Information</td>
</tr>
<tr>
<td>19</td>
<td>Windows Admin Shares</td>
</tr>
<tr>
<td>20</td>
<td>Pass the Ticket</td>
</tr>
</tbody>
</table>
Red Canary Data: Top Defense Evasion Techniques

- Scripting
- Regsvr32
- Masquerading
- Rundll32
- Disabling Security Tools
- Process Injection
- Obfuscated Files or Information
- Background Intelligent Transfer Service
- Deobfuscate/Decode Files or Information
- Bypass User Account Control
- Indicator Removal on Host
- Mshta
- Trusted Developer Utilities
- Clear Command History
- Signed Binary Proxy Execution
- InstallUtil
- Regsvcs/Regasm
- Space after Filename
- Launchctl
- NTFS File Attributes
<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>Command Line Interface</td>
<td>Right to Access</td>
<td>Access Taken Manipulation</td>
<td>Scoping</td>
<td>Credential dumping</td>
<td>Account Discovery</td>
<td>Application Discovery</td>
<td>Audio Capture</td>
<td>Automated Exfiltration</td>
<td>Commonly Used Port</td>
</tr>
<tr>
<td>E-Mail Malware</td>
<td>Right to Access</td>
<td>Access Taken Manipulation</td>
<td>Access Taken Manipulation</td>
<td>Scoping</td>
<td>Credential dumping</td>
<td>Application Discovery</td>
<td>File and Directory Discovery</td>
<td>Data Captured</td>
<td>Data Encrypted</td>
<td>Commonly Used Port</td>
</tr>
</tbody>
</table>

Hashcat Additions

- Hashcat
- Access Taken Manipulation | Hashcat
- Access Taken Manipulation | Hashcat

Scripting Through Web Applications

- Accessibility Features
- Access Taken Manipulation

Flash Additions

- Flash
- Access Taken Manipulation
- Access Taken Manipulation

Spam Additions

- Spammer
- Access Taken Manipulation
- Access Taken Manipulation

Supply Chain Compromise

- Dynamic Data Exchange
- Authentication Package
- OAuth Hijacking

Tainted Relationship

- Execution through API
- Bots
- Execution for Privilege Evasion

Valid Accounts

- Passwords
- Bots
- Execution for Privilege Evasion

Putting it into Action

7 overlapping techniques - a place to start for defense
## Overlaps in Top 20 Techniques

<table>
<thead>
<tr>
<th>Technique</th>
<th>Red Canary Rank</th>
<th>MITRE Rank</th>
<th>Red Canary Count</th>
<th>MITRE Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1086 PowerShell</td>
<td>1</td>
<td>18</td>
<td>1,774</td>
<td>46</td>
</tr>
<tr>
<td>T1064 Scripting</td>
<td>2</td>
<td>15</td>
<td>794</td>
<td>53</td>
</tr>
<tr>
<td>T1059 Command-Line Interface</td>
<td>12</td>
<td>4</td>
<td>294</td>
<td>112</td>
</tr>
<tr>
<td>T1060 Registry Run Keys / Startup Folder</td>
<td>8</td>
<td>6</td>
<td>377</td>
<td>93</td>
</tr>
<tr>
<td>T1036 Masquerading</td>
<td>6</td>
<td>19</td>
<td>419</td>
<td>45</td>
</tr>
<tr>
<td>T1027 Obfuscated Files or Information</td>
<td>18</td>
<td>7</td>
<td>120</td>
<td>88</td>
</tr>
<tr>
<td>T1003 Credential Dumping</td>
<td>7</td>
<td>11</td>
<td>405</td>
<td>61</td>
</tr>
</tbody>
</table>
What Does This Mean for Defense?

Powershell

● Implement PowerShell v5 w/enforcement and ScriptBlock logging
● Be really good at collecting command lines and associated detection

Scripting

● Monitor parent/child execution related to common phishing attachments
● Deeply monitor activity associated with common script engines

Command Line Interface

● Understand common parentage for applications in your org
● Be really good at collecting command lines and associated detection
What Does This Mean for Defense?

Registry Run Keys / Startup
- Know your systems: configuration management and system change audit

Masquerading
- Validate binary metadata (signing) and execution paths
- Know trusted hash values for common system binaries

Obfuscated Files / Info
- Script Block logging, automated decompress/deobfuscate/decode

Credential Dumping
- Dive deep into library loads and execution of system tools (setspn, ntdsutil)
Putting it into Action for Yourself

7 overlapping techniques
Your data?
Your gaps?
As you use ATT&CK...

Know your limitations

Combine approaches and data

Share your data (stay tuned!)
Questions?

attack.mitre.org
attack@mitre.org
@MITREattack

redcanary.com
info@redcanary.com
@RedCanaryCo