Detection Showcase -
Distilling the top threats, techniques, and trends
Agenda

1. Introductions: Who am I?
2. Background: The Threat Detection Report
3. Trends
4. Threats
5. Techniques
6. Questions: Do you have any?
Evan Bredahl, CISSP

Evan is a Certified Information Systems Security Professional (CISSP) and US Army Veteran with over 10 years of progressive experience providing security and IT-related consulting and support. Prior to joining Red Canary as a Customer Solutions Engineer, he spent his time at a number of Fortune 100 companies and Department of Defense agencies, as well as in the financial sector, where he focused on compliance frameworks.
What is it?

- **NOT** Sales related
- Exists to help you understand and detect threats
- Based on nearly 40,000 confirmed threats impacting Red Canary customers
- Includes actionable insight into threats and adversary techniques, how the landscape is changing
How to use it?

- Explore the most prevalent and impactful threats, techniques, and trends that we’ve observed.
- Note how adversaries are evolving their tradecraft as organizations continue their shift to cloud-based identity, infrastructure, and applications.
- Learn how to emulate, mitigate, and detect specific threats and techniques.
- Shape and inform your readiness, detection, and response to critical threats.
What’s a “MITRE ATT&CK”?
A taxonomy of threats

ATT&CK transforms the nebulous, unbounded “threat landscape” into a finite list of tactics and techniques.
Using ATT&CK

- To classify threats consistently
- To communicate about threats effectively
- To organize detection coverage coherently
- To produce an awesome annual report
Methodology
Based on the petabytes of raw data and trillions of signals that our XDR platform consumes daily, interrogated by 3500 behavior detector analytics mapped to the MITRE ATT&CK Framework.

Because we know which ATT&CK techniques an analytic aims to detect, we are able to look at these over time and determine technique prevalence, correlation, and much more.
Trends

- Ransomware
- Initial access tradecraft
- Command and control frameworks
- Stealers
- Identity
- Email threats
- Adversary emulation and testing
Initial access tradecraft

- Email phishing
  - Increase in compressed file types, decrease in Macro enabled types
  - Delivery of Optical Disk Image (ISO) files and Virtual Hard Drive (VHD) files

- USB delivery
  - Increase in USB delivered infections
PREVENTION

What to do?

- Apply Group Policies that restrict who can read, write, and execute actions from USB devices
- If your users do not have a business need to mount container files, we recommend stopping Windows from auto-mounting container files.
Ransomware

- Visibility
  - How big is this problem? Detection is focused on early stages

- Affiliate Model
  - Different actors for different stages

- Extortion
  - Extortion only attacks
Ransomware doesn’t start here:

Process spawned by cmd.exe

c:\windows\system32\wbem\wmic.exe a2ef3f0ad95fda9262a5f9533b6dd1bd fa78c88dac91f082eac8736e6900ac1ec4ab7a388b8f77a23ffa7e80a4ad29f5a

... Command Line: `wmic shadowcopy delete`

Deleting shadowcopies is commonly observed as a precursor to ransomware.
Initial Access  Recon  Lateral Movement  Exfiltration  Encryption

Focus here...  ...to avoid this
## Threats

<table>
<thead>
<tr>
<th>Rank</th>
<th>Threat</th>
<th>Affected Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Qbot</td>
<td>6.1% of customers</td>
</tr>
<tr>
<td>2</td>
<td>Impacket</td>
<td>5.6%</td>
</tr>
<tr>
<td>3</td>
<td>AdSearch</td>
<td>5.3%</td>
</tr>
<tr>
<td>4</td>
<td>Gootloader</td>
<td>4.4%</td>
</tr>
<tr>
<td>5</td>
<td>Mimikatz</td>
<td>4.4%</td>
</tr>
<tr>
<td>6</td>
<td>SocGholish</td>
<td>4.3%</td>
</tr>
<tr>
<td>7</td>
<td>Raspberry Robin</td>
<td>3.9%</td>
</tr>
<tr>
<td>8</td>
<td>Cobalt Strike</td>
<td>3.0%</td>
</tr>
<tr>
<td>9</td>
<td>BloodHound</td>
<td>2.9%</td>
</tr>
<tr>
<td>10</td>
<td>Gamarue</td>
<td>2.4%</td>
</tr>
</tbody>
</table>
Threat

Why should you care?

- We define “threats” broadly as malware, tools, threat groups, or activity clusters
- These are the most prevalent threats occurring in our customer environments, so we can assume they are prevalent elsewhere.
- We include advice for responding to each threat and offer detection opportunities
Threat

Raspberry Robin

- Initial access from compromised USB devices. After publication of our blog post on this threat, we received feedback that infections appear to stem from USB’s previously used at print shops and mailing centers.
- Microsoft published a blog post that Raspberry Robin used in compromises had follow-on activity including BumbleBee, Cobalt Strike, and IcedID.

USB delivery example: Raspberry Robin

1. Infected USB drive attached
2. cmd.exe and msiexec.exe
3. Malicious DLL download
4. rundll32.exe and Windows utility misuse
5. Ongoing command & control activity
Raspberry Robin Detection

Detecting msiexec.exe making outbound network connections to download and install packages in the command-line interface will give you the opportunity to examine the activity and determine if it’s malicious or not.

```python
process == ('msiexec')
&&
command_includes == ('http:' || 'https:')
&&
command_includes == ('/q' || '-q')
```
Raspberry Robin Detection

It is unusual for the below processes to attempt network connections with an empty command line. This can indicate malicious command and control (C2) activity.

```python
process == ('regsvr32.exe' || 'rundll32.exe' || 'dllhost.exe')
&
command == ('""')*
&
has_network_connection
```
What to do?

- Apply Group Policies that restrict who can read, write, and execute actions from USB devices
- Rapid detection and response early in the infection chain prevents continued progression of this threat. (Consider automating some of this)
  - Remove malicious file
  - Block Network connection
  - Device Isolation
## Techniques

1. T1059.003: Windows Command Shell
2. T1059.001: PowerShell
3. T1047: Windows Management Instrumentation
4. T1027: Obfuscated Files or Information
5. T1218.011: Rundll32
6. T1105: Ingress Tool Transfer
7. T1055: Process Injection
8. T1569.002: Service Execution
9. T1036.003: Rename System Utilities
10. T1003.001: LSASS Memory
We break down what malicious looks like in the form of telemetry and the many places you can look to find that telemetry.

This section includes detection opportunities you can employ

Provide easy to follow testing examples that can be used to validate your security tools ability to detect those threats
Technique

T1047: Windows Management Instrumentation (WMI)

- WMI is used by administrators to automate tasks, execute processes or scripts, and to configure systems.
- Threat actors use it to move laterally, gather information, modify systems, and achieve persistence.
- Unlike many other techniques, malicious use of WMI typically manifests as one of two processes: wmic.exe or wmiprvse.exe.
WMI Office product Detection

It’s almost always malicious when wmic.exe spawns as a child process of Microsoft Office and similar products. As such, it makes sense to examine the chain of execution and follow-on activity when this occurs. The following is a non-exhaustive example analytic that will catch some of this activity

```
parent_process == ('winword.exe' || 'excel.exe')
&&
process == wmic.exe
```
WMI Recon Detection

Reconnaissance is harder to detect because it looks very similar to normal admin behavior. Even so, we detect a relatively high volume of adversaries leveraging WMI to quickly gather domain information such as users, groups, or computers in the domain. The following may help you detect related activity:

```bash
process == wmic.exe
&&
command_includes ('$ldap' || 'ntdomain')
```
What to do?

- With WMI being legitimate and regularly in use, it is NOT recommended to disable this service.
- Focus on collecting the right telemetry and building good detectors for monitoring abuse over prevention.
- Regularly test your detectors.
Uh... am I doing this right?
Test, test, test (again)

Atomic Red Team™ is a library of simple tests that any security team can execute to test their defenses.

Tests are focused, have few dependencies, and are defined in a structured format that can be used by automation frameworks.
CONCLUSION

The key takeaways are...

Understand the trends that dominate information security

Know the threats that make up those trends

Learn about the techniques leveraged by those threats
FEEDBACK

Q & A