Indicators of compromise are great.
Analytics move up the (obligatory) pyramid of pain.
What’s an analytic, really?

Indicators
- Fewer false positives
- More atomic
- Higher quantity

Analytics
- More false positives
- Broader
- Lower quantity
Example analytic:

reg.exe called from command shell
We need an organizing framework.

Analytics are great, but they need to be put into the context of which adversary technique they detect

• How do you know which ones you need?
• If you have some analytics shared with you, how do you know whether they’re additive or duplicative?
• If you see a new technique being used in a threat report, how do you know if your current set of analytics will cover it?
ATT&CK™ is a MITRE-developed, globally-accessible knowledge base of adversary tactics and techniques based on real-world observations of adversaries’ operations against computer networks.
What’s in ATT&CK™

1. List of techniques used by adversaries for each phase of the kill chain

2. Possible methods of detection and mitigation

3. Published references of adversary use of techniques

Image source: www.hasbro.com

Mr. Potato Head is a registered trademark of Hasbro Inc.
<table>
<thead>
<tr>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Execution</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLL Search Order Hijacking</td>
<td>Brute Force</td>
<td>Account Discovery</td>
<td>Windows Remote Management</td>
<td>Audio Capture</td>
<td>Automated Exfiltration</td>
<td>Commonly Used Control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legitimate Credentials</td>
<td>Binary Pudding</td>
<td>Credential Dumping</td>
<td>Application Window Discovery</td>
<td>Third-party Software</td>
<td>Command-Line</td>
<td>Clipboard Data</td>
<td>Automated Collection</td>
<td>Data Compressed</td>
<td>Communication Through Removable Media</td>
</tr>
<tr>
<td>Accessibility Features</td>
<td>Code Signing</td>
<td>Credential Manipulation</td>
<td>File and Directory Discovery</td>
<td>Application Deployment Software</td>
<td>Execution through API</td>
<td>Data Staged</td>
<td>Data Encrypted</td>
<td>Data Transfer Size Limits</td>
<td>Connection Proxy</td>
</tr>
<tr>
<td>AppInit DLLs</td>
<td>Component Firmware</td>
<td>Component Object Model Hijacking</td>
<td>File System Logical Offsets</td>
<td>File System Permissions Weakness</td>
<td>File System Permissions Weakness</td>
<td>File System Permissions Weakness</td>
<td>Two-Factor Authentication</td>
<td>Two-Factor Authentication</td>
<td>Two-Factor Authentication</td>
</tr>
<tr>
<td>Local Port Monitor</td>
<td>DLL Side Loading</td>
<td>Exploitation of Vulnerability</td>
<td>Execution through Module Load</td>
<td>Data from Local System</td>
<td>Data from Network Shared Drive</td>
<td>Exfiltration Over Alternative Protocol</td>
<td>Custom Command and Control Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Service</td>
<td>Credentials in Files</td>
<td>Local Network Configuration Discovery</td>
<td>Logon Scripts</td>
<td>Graphical User Interface</td>
<td>Pass the Hash</td>
<td>InstallUtil</td>
<td>Data from Removable Media</td>
<td>Custom Cryptographic Protocol</td>
<td></td>
</tr>
<tr>
<td>Path Interception</td>
<td>Input Capture</td>
<td>Local Network Connections</td>
<td>Network Sniffing</td>
<td>Data from Removable Media</td>
<td>Data from Removable Media</td>
<td>Data from Removable Media</td>
<td>Data from Removable Media</td>
<td>Data from Removable Media</td>
<td>Data from Removable Media</td>
</tr>
<tr>
<td>Scheduled Task</td>
<td>File Deletion</td>
<td>Two-Factor Authentication</td>
<td>Local Network Connections</td>
<td>Data from Removable Media</td>
<td>Data from Removable Media</td>
<td>Data from Removable Media</td>
<td>Data from Removable Media</td>
<td>Data from Removable Media</td>
<td></td>
</tr>
<tr>
<td>File System Permissions Weakness</td>
<td>File System Logical Offsets</td>
<td>Exploitation of Vulnerability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Registry Permissions Weakness</td>
<td>Two-Factor Authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Shell</td>
<td>Indicator Blocking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Component Object Model Hijacking</td>
<td>DLL Injection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Basic Input/Output System</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change Default File Association</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Component Firmware</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>External Remote Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hypervisor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logon Scripts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify Existing Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Netsh Helper DLL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Redundant Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registry Run Keys / Start Folder</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Support Provider</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shortcut Modification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Management Instrumentation Event Subscription</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Winlogon Helper DLL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Enables pivoting between red team and blue team**

**Decouples the problem from the solution**

**Transforms thinking by focusing on post-exploit adversary behavior**

![MTRE Logo](https://www.mitre.org/publications/whitepapers/whitepapers.png)
<table>
<thead>
<tr>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Execution</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLL Search Order Hijacking</td>
<td>Credential Dumping</td>
<td>Process Hollowing</td>
<td>Data Encrypted</td>
<td>File and Directory Discovery</td>
<td>Data from Network Shared Drive</td>
<td>Data from Removable Media</td>
<td>Data Compressed</td>
<td>Data Staged</td>
<td>Data Transfer Rule Violation</td>
</tr>
<tr>
<td>Brute Force</td>
<td>Windows Remote Management</td>
<td>Local Network Configuration Discovery</td>
<td>Data Obfuscation</td>
<td>Terminal Service Discovery</td>
<td>Data Over Alternative Protocol</td>
<td>Data Over Command and Control Channel</td>
<td>Data Compressed</td>
<td>Data Transfer Rule Violation</td>
<td>Data Over Command and Control Channel</td>
</tr>
<tr>
<td>Account Discovery</td>
<td>Local Network Configuration Discovery</td>
<td>Process Discovery</td>
<td>Taint Shared Content</td>
<td>Key Reuse Management</td>
<td>Data Over Alternative Protocol</td>
<td>Data Over Command and Control Channel</td>
<td>Data Compressed</td>
<td>Data Transfer Rule Violation</td>
<td>Data Over Command and Control Channel</td>
</tr>
<tr>
<td>Access Discovery</td>
<td>Local Network Configuration Discovery</td>
<td>Remote File Copy</td>
<td>Taint Shared Content</td>
<td>Key Reuse Management</td>
<td>Data Over Alternative Protocol</td>
<td>Data Over Command and Control Channel</td>
<td>Data Compressed</td>
<td>Data Transfer Rule Violation</td>
<td>Data Over Command and Control Channel</td>
</tr>
<tr>
<td>Windows Admin Shares</td>
<td>Local Network Configuration Discovery</td>
<td>Remote Desktop Protocol</td>
<td>Taint Shared Content</td>
<td>Key Reuse Management</td>
<td>Data Over Alternative Protocol</td>
<td>Data Over Command and Control Channel</td>
<td>Data Compressed</td>
<td>Data Transfer Rule Violation</td>
<td>Data Over Command and Control Channel</td>
</tr>
<tr>
<td>Third-party Software</td>
<td>Local Network Configuration Discovery</td>
<td>Remote Desktop Protocol</td>
<td>Taint Shared Content</td>
<td>Key Reuse Management</td>
<td>Data Over Alternative Protocol</td>
<td>Data Over Command and Control Channel</td>
<td>Data Compressed</td>
<td>Data Transfer Rule Violation</td>
<td>Data Over Command and Control Channel</td>
</tr>
<tr>
<td>Command Line</td>
<td>Local Network Configuration Discovery</td>
<td>Remote Desktop Protocol</td>
<td>Taint Shared Content</td>
<td>Key Reuse Management</td>
<td>Data Over Alternative Protocol</td>
<td>Data Over Command and Control Channel</td>
<td>Data Compressed</td>
<td>Data Transfer Rule Violation</td>
<td>Data Over Command and Control Channel</td>
</tr>
<tr>
<td>Executed Through API</td>
<td>Local Network Configuration Discovery</td>
<td>Remote Desktop Protocol</td>
<td>Taint Shared Content</td>
<td>Key Reuse Management</td>
<td>Data Over Alternative Protocol</td>
<td>Data Over Command and Control Channel</td>
<td>Data Compressed</td>
<td>Data Transfer Rule Violation</td>
<td>Data Over Command and Control Channel</td>
</tr>
<tr>
<td>Execution Through API</td>
<td>Local Network Configuration Discovery</td>
<td>Remote Desktop Protocol</td>
<td>Taint Shared Content</td>
<td>Key Reuse Management</td>
<td>Data Over Alternative Protocol</td>
<td>Data Over Command and Control Channel</td>
<td>Data Compressed</td>
<td>Data Transfer Rule Violation</td>
<td>Data Over Command and Control Channel</td>
</tr>
<tr>
<td>Execution Through Module</td>
<td>Local Network Configuration Discovery</td>
<td>Remote Desktop Protocol</td>
<td>Taint Shared Content</td>
<td>Key Reuse Management</td>
<td>Data Over Alternative Protocol</td>
<td>Data Over Command and Control Channel</td>
<td>Data Compressed</td>
<td>Data Transfer Rule Violation</td>
<td>Data Over Command and Control Channel</td>
</tr>
<tr>
<td>Execution Through Module Load</td>
<td>Local Network Configuration Discovery</td>
<td>Remote Desktop Protocol</td>
<td>Taint Shared Content</td>
<td>Key Reuse Management</td>
<td>Data Over Alternative Protocol</td>
<td>Data Over Command and Control Channel</td>
<td>Data Compressed</td>
<td>Data Transfer Rule Violation</td>
<td>Data Over Command and Control Channel</td>
</tr>
<tr>
<td>Execution Through Module Load</td>
<td>Local Network Configuration Discovery</td>
<td>Remote Desktop Protocol</td>
<td>Taint Shared Content</td>
<td>Key Reuse Management</td>
<td>Data Over Alternative Protocol</td>
<td>Data Over Command and Control Channel</td>
<td>Data Compressed</td>
<td>Data Transfer Rule Violation</td>
<td>Data Over Command and Control Channel</td>
</tr>
</tbody>
</table>

**Note:** ATT&CK is a framework used to understand adversary behavior and improve defense strategies. Use ATT&CK to understand your defense.
**Example:** Bypass User Account Control (T1088)
Example: Bypass User Account Control (T1088)

A Windows security feature that limits application software to standard user privileges until an administrator authorizes an increase or elevation

- Seen used by APT29, Patchwork, BlackEnergy, and others
- Some issues are patched by Microsoft, some are not
Example: Bypass User Account Control (T1088)

UACME - List of specific procedures to carry out this technique
https://github.com/hfiref0x/UACME

There are... 41!
Filling the gaps is hard, time-consuming, and expensive.

- There are a lot of prevalent techniques
- Adversary practices are always evolving
- Techniques have a wide set of procedures
- We all have limited resources
- Requires in-depth expertise of system internals
We’re making this a team sport.

Tackling the problem together is the only way we can keep up
• More brainpower = faster progress
• A broader array of expertise = broader coverage

But there are some sensitivities you should be aware of...
• The analytics you write and share can have operational security impacts

Multi-faceted approach
• Start out in small working groups
• Not everyone is a producer, feedback is just as important
• Combined with public, open-source, sharing
NH-ISAC Working Group:
Building out and sharing analytics to cover techniques in the ATT&CK matrix

- NH-ISAC Working group, led by Pfizer
  *Particular thanks to Bill Barnes*
- Healthcare companies
- Security vendors
- HHS
- MITRE
Challenge: Sensor coverage varies.

- Organizations have different types of sensors
- Organizations have different sensors even for the same data
- Sensors are not enough, you need to be able to collect data from your sensors
Challenge: Operational environments vary.

Each environment is unique and will have unique false positives:
- Lots of developers vs. few
- Use of Tool A vs. Tool B

Configurations of OS or other tools differ and cause analytics targeting them to differ.
Challenge: There is no common language or taxonomy.

No common
- Query language
- Data taxonomy

Manual conversions are tractable, for now
- Simpler analytics
- Lower volume

Need to look to the future
Where we’re going

• Validating that what we’re doing works and helps

• Putting analytics in context
  • How do you assess your threat model and your coverage? How do you track it over time?
  • Need tooling

• Increasing our pace via standardization and automation
Take action

Figure out where you are
  • Define your threat model in ATT&CK.
  • Assess your gaps. Ask your vendors.
  • Are you where you want to be?

Figure out where to go and how to participate
  • Can you use analytics now?
  • Can you create analytics yourself?

Find a community to join
  • Talk to your ISAO/ISAC, vendors, partners, friends
  • Talk to me
  • Find open source analytics (look at CAR!)
Making it easy

ATT&CK
https://attack.mitre.org

CAR
https://car.mitre.org

Unfetter
https://github.com/unfetter-discover/unfetter

Me
jwunder@mitre.org