

Leveraging MITRE ATT&CK

Using ATT&CK (Navigator) in the enterprise

#SEC599 - Defeating Advanced Adversaries

Your hosts for the webcast

Stephen Sims @Steph3nSims

Erik Van Buggenhout @ErikVaBu



Your Hosts for Today



Erik Van Buggenhout
SANS Certified Instructor
Co-Founder NVISO
[@ErikVaBu](#)



Stephen Sims
SANS Fellow
[@Steph3nSims](#)

The Agenda for Today

WHAT WE'D LIKE TO DISCUSS



1. What is MITRE ATT&CK

Introduction



2. ATT&CK use cases

How can MITRE ATT&CK be used?



3. ATT&CK initiatives

Some interesting references



4. Demo - CALDERA

Demonstration of a tool



5. Q&A

Ask us your questions!



What is MITRE ATT&CK

Introduction

Kill Chain vs ATT&CK

Where does ATT&CK come from?



The Cyber Kill Chain provides a 30,000ft view of an attack

“Action on Objectives” covers a lot of stuff...
Good for a general overview, but how do you make this actionable?

MITRE ATT&CK?

What is MITRE ATT&CK

Adversarial Tactics, Techniques & Common Knowledge

ATT&CK Matrix for Enterprise

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control |
|-------------------------------------|-------------------------------|---------------------------|-----------------------------|-----------------------------|------------------------------------|------------------------------|------------------------------------|------------------------------------|---|---------------------------------------|
| Drive-by Compromise | AppleScript | .bash_profile and .bashrc | Access Token Manipulation | Access Token Manipulation | Account Manipulation | Account Discovery | AppleScript | Audio Capture | Automated Exfiltration | Commonly Used Port |
| Exploit Public-Facing Application | CMSTP | Accessibility Features | Accessibility Features | BITS Jobs | Bash History | Application Window Discovery | Application Deployment Software | Automated Collection | Data Compressed | Communication Through Removable Media |
| Hardware Additions | Command-Line Interface | Account Manipulation | AppCert DLLs | Binary Padding | Brute Force | Browser Bookmark Discovery | Distributed Component Object Model | Clipboard Data | Data Encrypted | Connection Proxy |
| Replication Through Removable Media | Compiled HTML File | AppCert DLLs | AppInit DLLs | Bypass User Account Control | Credential Dumping | File and Directory Discovery | Exploitation of Remote Services | Data Staged | Data Transfer Size Limits | Custom Command and Control Protocol |
| Spearphishing Attachment | Control Panel Items | AppInit DLLs | Application Shimming | CMSTP | Credentials in Files | Network Service Scanning | Logon Scripts | Data from Information Repositories | Exfiltration Over Alternative Protocol | Custom Cryptographic Protocol |
| Spearphishing Link | Dynamic Data Exchange | Application Shimming | Bypass User Account Control | Clear Command History | Credentials in Registry | Network Share Discovery | Pass the Hash | Data from Local System | Exfiltration Over Command and Control Channel | Data Encoding |
| Spearphishing via Service | Execution through API | Authentication Package | DLL Search Order Hijacking | Code Signing | Exploitation for Credential Access | Network Sniffing | Pass the Ticket | Data from Network Shared Drive | Exfiltration Over Other Network Medium | Data Obfuscation |
| Supply Chain Compromise | Execution through Module Load | BITS Jobs | Dylib Hijacking | Compiled HTML File | Forced Authentication | Password Policy Discovery | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Physical Medium | Domain Fronting |

MITRE has developed the ATT&CK Matrix as a central repository for adversary TTP's. It is used by red teams and blue teams alike. It is rapidly gaining traction as a de facto standard!

MITRE ATT&CK?

Tactics vs Techniques

TACTICS

ATT&CK Matrix for Enterprise

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control |
|-------------------------------------|-------------------------------|---------------------------|-----------------------------|-----------------------------|------------------------------------|------------------------------|------------------------------------|------------------------------------|---|---------------------------------------|
| Drive-by Compromise | AppleScript | .bash_profile and .bashrc | Access Token Manipulation | Access Token Manipulation | Account Manipulation | Account Discovery | AppleScript | Audio Capture | Automated Exfiltration | Commonly Used Port |
| Exploit Public-Facing Application | CMSTP | Accessibility Features | Accessibility Features | BITS Jobs | Bash History | Application Window Discovery | Application Deployment Software | Automated Collection | Data Compressed | Communication Through Removable Media |
| Hardware Additions | Command-Line Interface | Account Manipulation | AppCert DLLs | Binary Padding | Brute Force | Browser Bookmark Discovery | Distributed Component Object Model | Clipboard Data | Data Encrypted | Connection Proxy |
| Replication Through Removable Media | Compiled HTML File | AppCert DLLs | AppInit DLLs | Bypass User Account Control | Credential Dumping | File and Directory Discovery | Exploitation of Remote Services | Data Staged | Data Transfer Size Limits | Custom Command and Control Protocol |
| Spearphishing Attachment | Control Panel Items | AppInit DLLs | Application Shimming | CMSTP | Credentials in Files | Network Service Scanning | Logon Scripts | Data from Information Repositories | Exfiltration Over Alternative Protocol | Custom Cryptographic Protocol |
| Spearphishing Link | Dynamic Data Exchange | Application Shimming | Bypass User Account Control | Clear Command History | Credentials in Registry | Network Share Discovery | Pass the Hash | Data from Local System | Exfiltration Over Command and Control Channel | Data Encoding |
| Spearphishing via Service | Execution through API | Authentication Package | DLL Search Order Hijacking | Code Signing | Exploitation for Credential Access | Network Sniffing | Pass the Ticket | Data from Network Shared Drive | Exfiltration Over Other Network Medium | Data Obfuscation |
| Supply Chain Compromise | Execution through Module Load | BITS Jobs | Dylib Hijacking | Compiled HTML File | Forced Authentication | Password Policy Discovery | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Physical Medium | Domain Fronting |

TECHNIQUES

Technique: Component Object M x +

https://attack.mitre.org/techniques/T1122/

MITRE ATT&CK™

Matrices Tactics Techniques Groups Software Resources

Blog Contact

Search site

Thanks to all of our ATT&CKcon participants. All sessions are here, and individual presentations will be posted soon.

Home > Techniques > Enterprise > Component Object Model Hijacking

Component Object Model Hijacking

The ^[1] (COM) is a system within Windows to enable interaction between software components through the operating system. ^[1] Adversaries can use this system to insert malicious code that can be executed in place of legitimate software through hijacking the COM references and relationships as a means for persistence. Hijacking a COM object requires a change in the Windows Registry to replace a reference to a legitimate system component which may cause that component to not work when executed. When that system component is executed through normal system operation the adversary's code will be executed instead. ^[2] An adversary is likely to hijack objects that are used frequently enough to maintain a consistent level of persistence, but are unlikely to break noticeable functionality within the system as to avoid system instability that could lead to detection.

Examples

ENTERPRISE ▾

TECHNIQUES

- All
- Initial Access +
- Execution +
- Persistence -
- .bash_profile and .bashrc
- Accessibility Features
- Account Manipulation
- AppCert DLLs
- Applnit DLLs
- Application Shimming

ID: T1122

Tactic: Defense Evasion, Persistence

Platform: Windows

Permissions Required: User

Data Sources: Windows Registry, DLL monitoring, Loaded DLLs

Defense Bypassed: Autoruns Analysis

Contributors: ENDGAME

Version: 1.0

As an example, let's have a look at one of Turla's favorite techniques: COM object hijacking. In MITRE's ATT&CK framework, this technique is known as T1122, and it's part of the "Defense Evasion" and "Persistence" tactics for Windows.

For every one of these techniques, MITRE includes a dedicated entry with amongst others:

- Technique information
- Known adversaries that use it
- Detection opportunities
- Prevention opportunities

ATT&CK Navigator

Operationalizing ATT&CK

layer x +

selection controls layer controls technique controls

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Threat Groups | Exfiltration | Command And Control |
|-------------------------------------|-------------------------------|--|--|---|--|------------------------------|--|---|---|
| 10 items | 33 items | 58 items | 28 items | 63 items | 19 items | 20 items | APT1 view select deselect | Automated Exfiltration | Commonly Used Port |
| Drive-by Compromise | AppleScript | .bash_profile and .bashrc | Access Token Manipulation | Access Token Manipulation | Account Manipulation | Account Discovery | APT16 view select deselect | Data Compressed | Communication Through Removable Media |
| Exploit Public-Facing Application | CMSTP | Accessibility Features | Accessibility Features | Binary Padding | Bash History | Application Window Discovery | APT17 view select deselect | Data Encrypted | Connection Proxy |
| Hardware Additions | Command-Line Interface | Account Manipulation | AppCert DLLs | BITS Jobs | Brute Force | Browser Bookmark Discovery | APT18 view select deselect | Data Transfer Size Limits | Custom Command and Control Protocol |
| Replication Through Removable Media | Compiled HTML File | AppCert DLLs | AppCert DLLs | Bypass User Account Control | Credential Dumping | File and Directory Discovery | APT19 view select deselect | Exfiltration Over Alternative Protocol | Custom Cryptographic Protocol |
| Spearphishing Attachment | Control Panel Items | Applnit DLLs | Applnit DLLs | Clear Command History | Credentials in Files | Network Service Scanning | APT28 view select deselect | Exfiltration Over Command and Control Channel | Data Encoding |
| Spearphishing Link | Dynamic Data Exchange | Application Shimming | Application Shimming | Component Firmware | Credentials in Registry | Network Share Discovery | APT29 view select deselect | Exfiltration Over Other Network Medium | Domain Fronting |
| Spearphishing via Service | Execution through API | Authentication Package | Bypass User Account Control | Control Panel Items | Exploitation for Credential Access | Password Policy Discovery | ADVSTORESHELL | Exfiltration Over Physical Medium | Fallback Channels |
| Supply Chain Compromise | Execution through Module Load | BITS Jobs | DLL Search Order Hijacking | Control Panel Items | Forced Authentication | Peripheral Device Discovery | ASPXSpy | Scheduled Transfer | Multi-hop Proxy |
| Trusted Relationship | Graphical User Interface | Browser Extensions | Dylib Hijacking | DCShadow | Hooking | Permission Group Discovery | Agent.btz | Multi-Stage Channels | Multiband Communication |
| Valid Accounts | InstallUtil | Change Default File Association | Exploitation for Privilege Escalation | Deobfuscate/Decode Files or Information | Input Capture | Process Discovery | Arp | Multilayer Encryption | Multilayer Encryption |
| | Launchctl | Component Firmware | Extra Window Memory Injection | Disabling Security Tools | Input Prompt | SSH Hijacking | Autolt backdoor | Port Knocking | Port Knocking |
| | Local Job Scheduling | Component Object Model Hijacking | File System Permissions Weakness | DLL Search Order Hijacking | Kerberoasting | Taint Shared Content | | Remote Access Tools | Remote Access Tools |
| | LSASS Driver | Create Account | Hooking | DLL Side-Loading | Keychain | Third-party Software | | Remote File Copy | Remote File Copy |
| | Mshta | DLL Search Order Hijacking | Image File Execution Options Injection | Exploitation for Defense Evasion | Keychain | Windows Admin Shares | | Standard Application Layer Protocol | Standard Application Layer Protocol |
| | PowerShell | Dylib Hijacking | Launch Daemon | File Deletion | LLMNR/NBT-NS Poisoning | Windows Remote Management | | Standard Cryptographic Protocol | Standard Cryptographic Protocol |
| | Regsvcs/Regasm | External Remote Services | New Service | File Permissions Modification | Network Sniffing | | | Standard Non-Application Layer Protocol | Standard Non-Application Layer Protocol |
| | Regsvr32 | File System Permissions Weakness | Path Interception | File System Logical Offsets | Password Filter DLL | | | Uncommonly Used Port | Uncommonly Used Port |
| | Rundll32 | Hidden Files and Directories | Plist Modification | Gatekeeper Bypass | Private Keys | | | Web Service | Web Service |
| | Scheduled Task | Hidden Files and Directories | Port Monitors | Hidden Files and Directories | Securityd Memory | | | | |
| | Scripting | Hooking | Process Injection | Hidden Users | System Information Discovery | | | | |
| | Service Execution | Hypervisor | Scheduled Task | Hidden Window | System Network Configuration Discovery | | | | |
| | Signed Binary Proxy Execution | Image File Execution Options Injection | Service Registry Permissions Weakness | HISTCONTROL | System Network Connections Discovery | | | | |
| | Signed Script Proxy Execution | Kernel Modules and Extensions | Setuid and Setgid | Image File Execution Options | System Owner/User Discovery | | | | |
| | Source | Launch Agent | SID-History Injection | | System Service Discovery | | | | |
| | Space after Filename | | | | | | | | |

ATT&CK Evaluations

Using ATT&CK as a framework to evaluate products

MITRE evaluates cybersecurity products using an open methodology based on our ATT&CK™ framework. Our goals are to:

- Empower end-users with objective insights into how to use specific commercial security products to detect known adversary behaviors
- Provide transparency around the true capabilities of security products and services to detect known adversary behaviors
- Drive the security vendor community to enhance their capability to detect known adversary behaviors

These evaluations are not a competitive analysis. There are no scores, rankings, or ratings. Instead, we show how each vendor approaches threat detection in the context of the ATT&CK matrix.

Transparency in both process and results

MITRE's evaluation [methodology](#) is publicly available, and all evaluation results are publicly released. MITRE will continue to evolve the methodology and content to ensure a fair, transparent, and useful evaluation process.

ATT&CK™ Evaluations

[See Evaluations »](#)[Get Evaluated »](#)[Read Methodology »](#)

Carbon Black.





ATT&CK Use Cases

How can MITRE ATT&CK be used?

Key use cases for ATT&CK

ATT&CK as a common language!

ATT&CK Matrix for Enterprise



| | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control |
|------------|---------------------------|---------------------------|----------------------|--------------------|---------------------------------|----------------------|---------------------------------------|
| nd .bashrc | Access Token Manipulation | Access Token Manipulation | Account Manipulation | Account Discovery | AppleScript | Audio Capture | Commonly Used Port |
| eatures | Accessibility Features | BITS Jobs | Bash History | Application Window | Application Deployment software | Automated Collection | Communication Through Removable Media |

Adversary emulation

Detection capability

ATT&CK™

Adversarial Tactics, Techniques & Common Knowledge



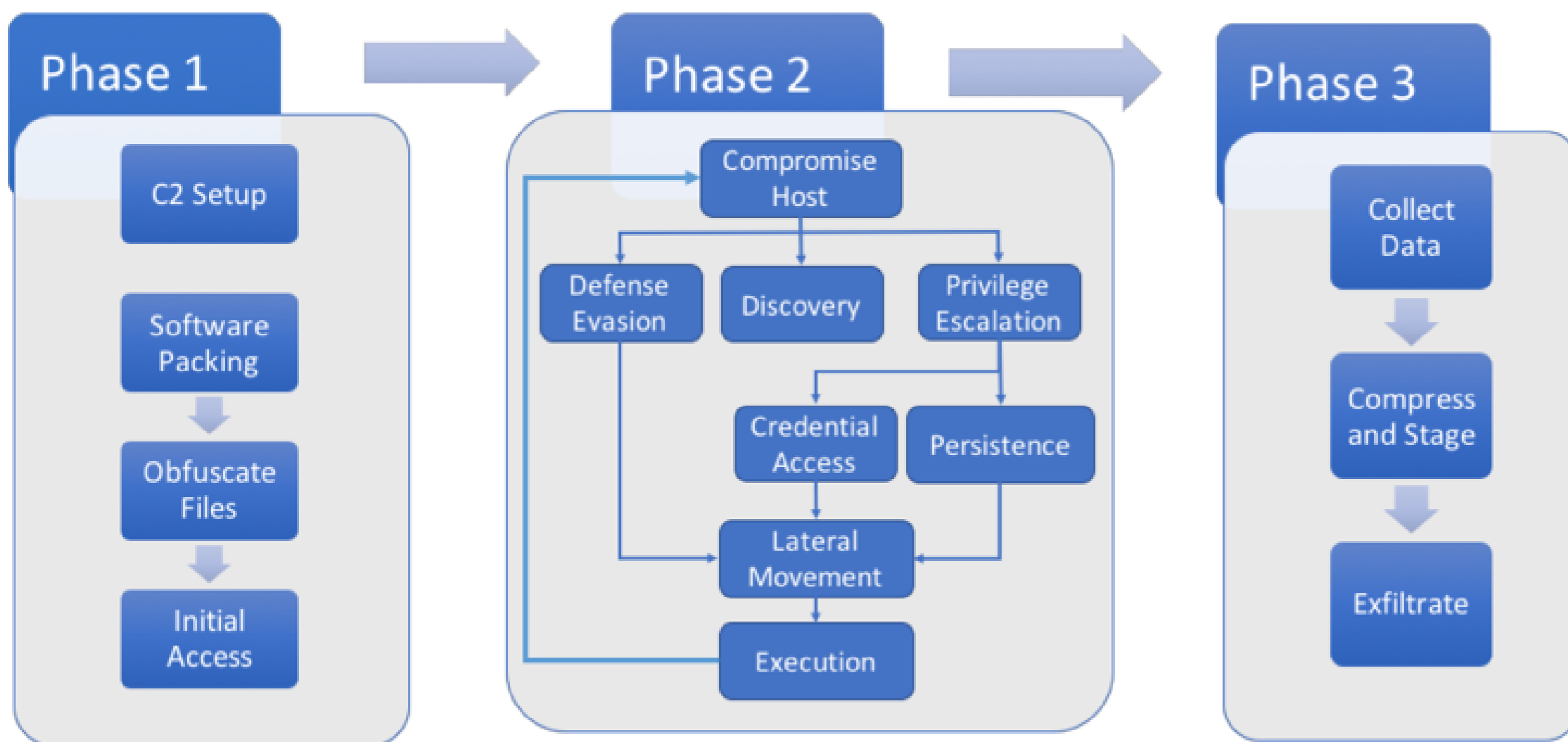
Prioritize defenses

Threat Intelligence

ATT&CK for adversary emulation



APT 3 Emulation Plan



Approved for Public Release; Distribution Unlimited. Case Number 17-3569. ©2018 The MITRE Corporation. All Rights Reserved

MITRE

When developing scenarios for red teaming / adversary emulation, red teams should use ATT&CK tactics and techniques to describe how the engagement will be delivered.

This will tremendously increase the value of the engagement, as it helps defenders map issues on a structured framework afterwards!

ATT&CK for threat intelligence



Mapping to ATT&CK: the Manual, Human Way

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**.

Scripting (T1064)

Registry Run Keys / Startup Folder (T1060)

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**, **systeminfo.exe**, **ipconfig.exe** and **bcp.exe**.

Command-Line Interface (T1059)

Discovery - T1057, T1018, T1049, T1082, T1016

Cred Dumping (T1003)

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

Pass the Ticket (T1097)

Input Capture (T1056)

The group also used **keyloggers** and their own .NET tool to enumerate folders and **dump data from Microsoft Exchange mailboxes**.

Email Collection (T1114)

<https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/>

ATT&CK techniques can be used to describe adversary activities in an understandable, structured, fashion.

The screenshot on the left provides is an example of an adversary report on APT-15 (by NCC Group), which is annotated by Katie Nickels (MITRE) and Brian Beyer (Red Canary). It was presented at SANS CTI Summit in January 2019!

ATT&CK for defense prioritization



“What techniques can you block in your organisation?”

- What ATT&CK techniques are covered by **hardening guidelines** (e.g. group policies or Ansible playbooks)?
- Travis Smith mapped the ATT&CK framework techniques to **CIS Controls**, which provides an interesting insight!

mitre_attack

Teaching

A listing of JSON files which can be used with the ATT&CK Navigator (October 2018 Release) to view the five different categories of techniques within the framework.

- **Blue** These are techniques which are not really exploitable, rather they use other techniques to be viable.
- **Green** These are the easiest techniques to exploit, there is no need for POC malware, scripts, or other tools.
- **Yellow** These techniques usually need some sort of tool, such as Metasploit.
- **Orange** These techniques require some level of infrastructure to setup. Once setup, some are easy and some are more advanced.
- **Red** These are the most advanced techniques which require an in-depth understanding of the OS or custom DLL/EXE files for exploitation.

<https://www.tripwire.com/state-of-security/security-data-protection/security-controls/mapping-the-attck-framework-to-cis-controls/>

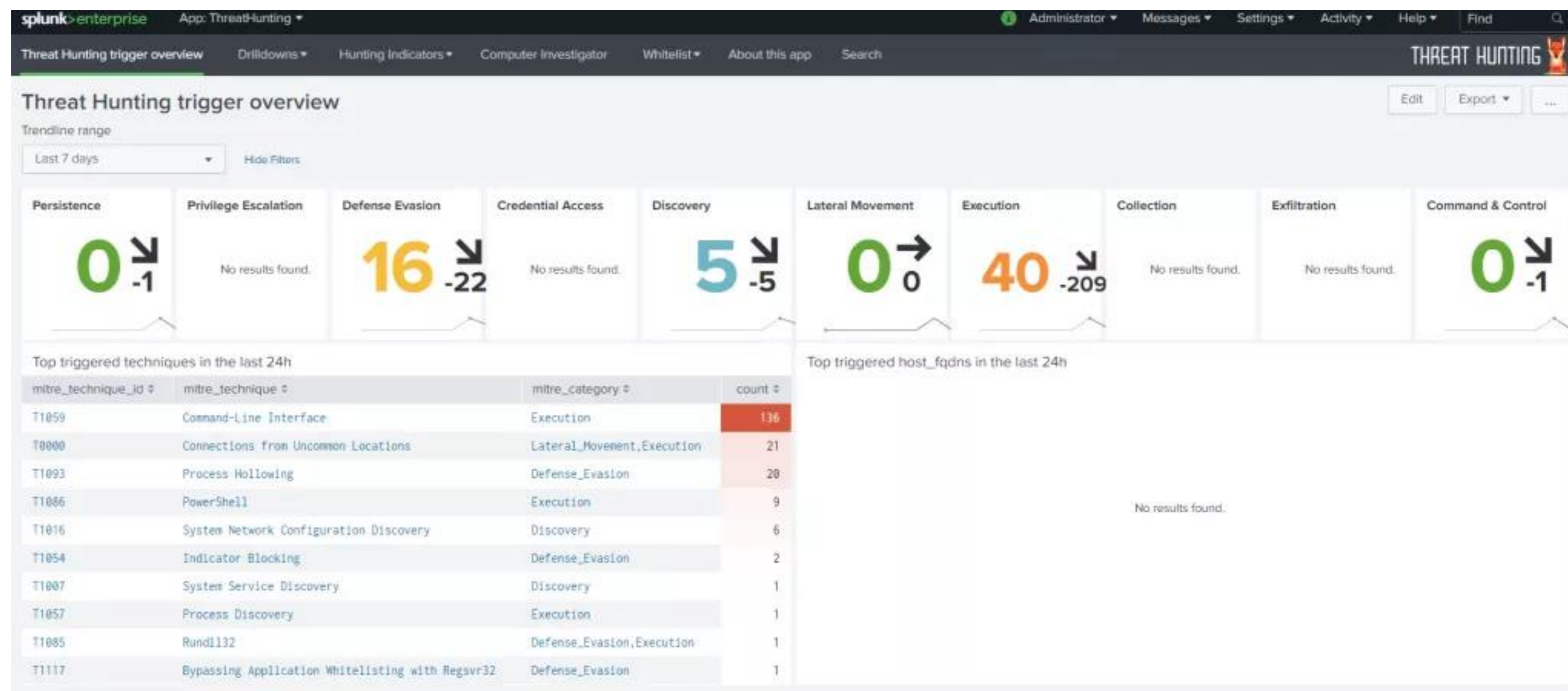
https://github.com/TravisFSmith/mitre_attack

ATT&CK for detection coverage



“What techniques can you detect in your organisation?”

- What techniques are covered by use cases in security monitoring?
- Do you collect the right log sources?
- What techniques can you cover using threat hunting efforts?



<https://cyberwardog.blogspot.com/2017/07/how-hot-is-your-hunt-team.html>
<https://github.com/olafhartong/ThreatHunting>

Key use cases for ATT&CK

ATT&CK as a common language!



Adversary emulation

Define red team scenarios using ATT&CK

Link vulnerabilities & findings to ATT&CK



Detection capability

Assess detection coverage using ATT&CK

Define hypotheses for threat hunting using ATT&CK



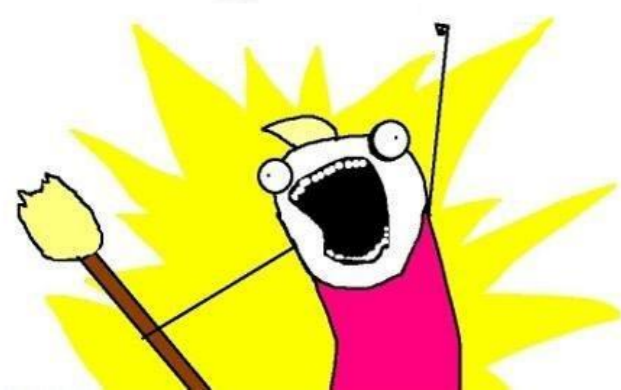
Threat Intelligence

Categorize / tag indicators & techniques with ATT&CK



Prioritize defenses

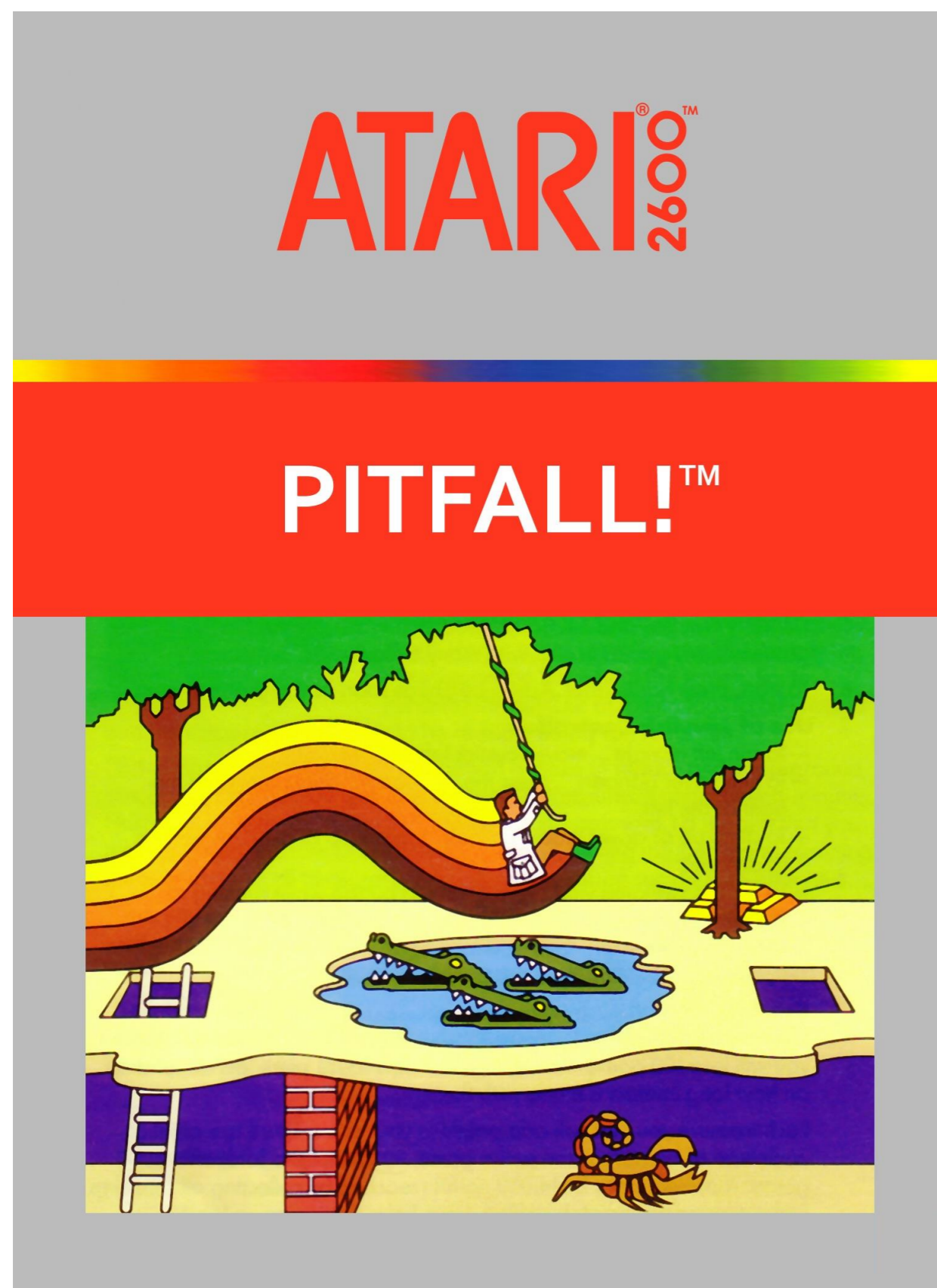
What ATT&CK techniques are you blocking?



ATT&CK all the things!

Common pitfalls

How to not use ATT&CK



Pitfall 1

Consider all techniques equal

Pitfall 2

Try to do everything at once

Pitfall 3

Misunderstand your coverage rating *(it's usually not binary)*

All techniques are equal...

But some techniques are more equal than others

In January 2019, MITRE & Red Canary combined efforts and presented a joint view on ATT&CK at the SANS CTI Summit:



All techniques are equal...

But some techniques are more equal than others

| Technique | Red Canary Rank | MITRE Rank | Red Canary Count | MITRE Count |
|--|-----------------|------------|------------------|-------------|
| T1086 PowerShell | 1 | 18 | 1,774 | 46 |
| T1064 Scripting | 2 | 15 | 794 | 53 |
| T1059 Command-Line Interface | 12 | 4 | 294 | 112 |
| T1060 Registry Run Keys / Startup Folder | 8 | 6 | 377 | 93 |
| T1036 Masquerading | 6 | 19 | 419 | 45 |
| T1027 Obfuscated Files or Information | 18 | 7 | 120 | 88 |
| T1003 Credential Dumping | 7 | 11 | 405 | 61 |

All techniques are equal...

But some techniques are more equal than others

2019 GLOBAL THREAT REPORT
ADVERSARY TRADECRAFT AND THE IMPORTANCE OF SPEED

Figure 8.
Global MITRE ATT&CK Heat Map³

Number of Intrusions Where Technique Was Observed
Least Prevalent Most Prevalent

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion |
|-------------------------------------|------------------------------------|--|--|---|
| Drive-by Compromise | AppleScript | .bash_profile and .bashrc | Access Token Manipulation | Access Token Manipulation |
| Exploit Public-Facing Application | CMSTP | Accessibility Features | Accessibility Features | Binary Padding |
| Hardware Additions | Command-Line Interface | Account Manipulation | AppCert DLLs | BITS Jobs |
| Replication Through Removable Media | Compiled HTML File | AppCert DLLs | AppInIt DLLs | Bypass User Account Control |
| Spearphishing Attachment | Control Panel Items | AppInIt DLLs | Application Shimming | Clear Command History |
| Spearphishing Link | Dynamic Data Exchange | Application Shimming | Bypass User Account Control | CMSTP |
| Spearphishing via Service | Execution through API | Authentication Package | DLL Search Order Hijacking | Code Signing |
| Supply Chain Compromise | Execution through Module Load | BITS Jobs | Dylib Hijacking | Compiled HTML File |
| Trusted Relationship | Exploitation for Client Execution | Bootkit | Exploitation for Privilege Escalation | Component Firmware |
| Valid Accounts | Graphical User Interface | Browser Extensions | Extra Window Memory Injection | Component Object Model Hijacking |
| | InstallUtil | Change Default File Association | File System Permissions Weakness | Control Panel Items |
| | Launchctl | Component Firmware | Hooking | DCShadow |
| | Local Job Scheduling | Component Object Model Hijacking | Image File Execution Options Injection | Deobfuscate/Decode Files or Information |
| | LSASS Driver | Create Account | Launch Daemon | Disabling Security Tools |
| | Mshata | DLL Search Order Hijacking | New Service | DLL Search Order Hijacking |
| | PowerShell | Dylib Hijacking | Path Interception | DLL Side-Loading |
| | Regsvcs/Regasm | External Remote Services | Plist Modification | Exploitation for Defense Evasion |
| | Regsvr32 | File System Permissions Weakness | Port Monitors | Extra Window Memory Injection |
| | Rundll32 | Hidden Files and Directories | Process Injection | File Deletion |
| | Scheduled Task | Hooking | Scheduled Task | File Permissions Modification |
| | Scripting | Hypervisor | Service Registry Permissions Weakness | File System Logical Offsets |
| | Service Execution | Image File Execution Options Injection | Setuid and Setgid | Gatekeeper Bypass |
| | Signed Binary Proxy Execution | Kernel Modules and Extensions | SID-History Injection | Hidden Files and Directories |
| | Signed Script Proxy Execution | Launch Agent | Startup Items | Hidden Users |
| | Source | Launch Daemon | Sudo | Hidden Window |
| | Space after Filename | Launchctl | Sudo Caching | HISTCONTROL |
| | Third-party Software | LC_LOAD_DYLIB Addition | Valid Accounts | Image File Execution Options Injection |
| | Trap | Local Job Scheduling | Web Shell | Indicator Blocking |
| | Trusted Developer Utilities | Login Item | | Indicator Removal from Tools |
| | User Execution | Logon Scripts | | Indicator Removal on Host |
| | Windows Management Instrumentation | LSASS Driver | | Indirect Command Execution |
| | Windows Remote Management | Modify Existing Service | | Install Root Certificate |
| | XSL Script Processing | Netsh Helper DLL | | InstallUtil |
| | | New Service | | Launchctl |

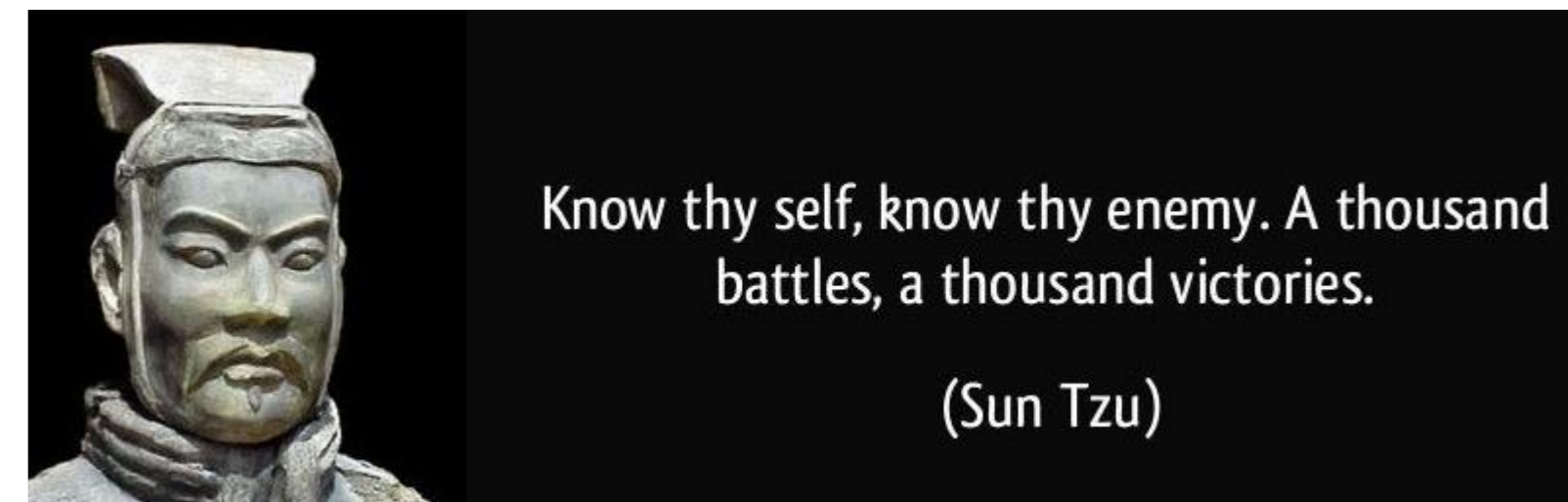
CrowdStrike released the “Global Threat Report” in February 2019 and added a “heat map” of MITRE ATT&CK, which can again be used to prioritize your efforts and attention!

The results are in line with the MITRE & Red Canary data previously seen!

<https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/>

All techniques are equal...

But some techniques are more equal than others



Next to the “technique popularity contest”, there is also the question of what techniques are most important TO YOUR ORGANIZATION:

1. Know what threat actors are relevant to you
2. Know what techniques these threat actors are known to use
3. Prioritize accordingly!

The screenshot displays the MITRE ATT&CK Navigator interface. The main table lists techniques across seven categories: Initial Access (10 items), Execution (33 items), Persistence (58 items), Privilege Escalation (28 items), Defense Evasion (63 items), Credential Access (19 items), and Discovery (20 items). A 'Threat Groups' dropdown menu is open, showing a list of groups with 'view', 'select', and 'deselect' options. The 'Software' group is expanded, listing various tools like 3PARA RAT, 4H RAT, ADVSTORESHELL, ASPXSpy, Agent.btz, Arp, AutoIt backdoor, Process Discovery, and SSH Hijacking. On the right side, there are additional categories like 'Command And Control' (21 items) and 'Data Encodings'.



ATT&CK initiatives

Here's some concrete ideas!

ATT&CK Initiatives - Detection

Many open-source tools align with ATT&CK

Malware archaeology

The folks over at Malware Archaeology made a mapping of Windows event IDs to the MITRE ATT&CK framework. It includes a coding scheme for most relevant event identifiers as well!

It's updated regularly and can be found at <https://www.malwarearchaeology.com/cheat-sheets>.

| Tactic | Technique Name | Technique ID | Data Source 1 | Data Source 2 | Data Source 3 |
|------------|------------------------------------|--------------|--------------------------|------------------------|------------------------------------|
| Collection | Audio Capture | T1123 | 4688 Process Execution | 4663 File monitoring | API monitoring |
| Collection | Automated Collection | T1119 | 4688 Process CMD Line | 4663 File monitoring | Data loss prevention |
| Collection | Clipboard Data | T1115 | API monitoring | | |
| Collection | Data from Information Repositories | T1213 | Application Logs | Authentication logs | Data loss prevention |
| Collection | Data from Local System | T1005 | 4688 Process Execution | 4688 Process CMD Line | 200-500, 4100-4104 PowerShell logs |
| Collection | Data from Network Shared Drive | T1039 | 4688 Process CMD Line | 4688 Process Execution | 5140/5145 Share connection |
| Collection | Data from Removable Media | T1025 | 4688 Process Execution | 4688 Process CMD Line | 4657 Windows Registry |
| Collection | Data Staged | T1074 | 4688 Process CMD Line | 4688 Process Execution | 4663 File monitoring |
| Collection | Email Collection | T1114 | 4688 Process Execution | 5156 Firewall Logs | 4624 Authentication logs |
| Collection | Man in the Browser | T1185 | 4624 Authentication logs | 4688 Process Execution | API monitoring |
| Collection | Screen Capture | T1113 | 4688 Process Execution | 4663 File monitoring | API monitoring |

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command And Control |
|-------------------------------------|------------------------------------|---|--|---|--|--------------------------------------|--|------------------------------------|---|---|
| 10 items | 25 items | 41 items | 21 items | 49 items | 16 items | 19 items | 15 items | 13 items | 9 items | 20 items |
| Drive-by Compromise | CMSTP | Accessibility Features | Access Token Manipulation | Access Token Manipulation | Account Manipulation | Account Discovery | Application Deployment Software | Audio Capture | Automated Exfiltration | Commonly Used Port |
| Exploit Public-Facing Application | Command-Line Interface | AppCert DLLs | Access Token Manipulation | Binary Padding | Brute Force | Application Window Discovery | Distributed Component Object Model | Automated Collection | Data Compressed | Communication Through Removable Media |
| Hardware Additions | Control Panel Items | AppInit DLLs | Accessibility Features | BITS Jobs | Credential Dumping | Browser Bookmark Discovery | Exploitation of Remote Services | Clipboard Data | Data Encrypted | Connection Proxy |
| Replication Through Removable Media | Dynamic Data Exchange | Authentication Package | AppCert DLLs | Bypass User Account Control | Credentials in Files | File and Directory Discovery | Logon Scripts | Data from Information Repositories | Data Transfer Size Limits | Custom Command and Control Protocol |
| Spearphishing Attachment | Execution through API | Authentication Package | AppInit DLLs | CMSTP | Credentials in Registry | Network Service Scanning | Pass the Hash | Data from Local System | Exfiltration Over Alternative Protocol | Custom Cryptographic Protocol |
| Spearphishing Link | Execution through Module Load | BITS Jobs | Application Shimming | Code Signing | Exploitation for Credential Access | Network Share Discovery | Pass the Ticket | Data from Network Shared Drive | Exfiltration Over Command and Control Channel | Data Encoding |
| Spearphishing via Service | Exploitation for Client Execution | Bootkit | Bypass User Account Control | Component Firmware | Forced Authentication | Peripheral Device Discovery | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Other Network Medium | Data Obfuscation |
| Supply Chain Compromise | Graphical User Interface | Browser Extensions | DLL Search Order Hijacking | Component Object Model Hijacking | Hooking | Remote File Copy | Replication Through Removable Media | Data Staged | Exfiltration Over Physical Medium | Domain Fronting |
| Trusted Relationship | InstallUtil | Change Default File Association | Exploitation for Privilege Escalation | Control Panel Items | Input Capture | Remote Services | Screen Capture | Email Collection | Scheduled Transfer | Fallback Channels |
| Valid Accounts | LSASS Driver | Component Firmware | Extra Window Memory Injection | DCShadow | Kerberoasting | Security Software Discovery | System Information Discovery | Input Capture | System Network Configuration Discovery | Standard Application Layer Protocol |
| | Mshata | Component Object Model Hijacking | File System Permissions Weakness | Deobfuscate/Decode Files or Information | LLMNR/NBT-NS Poisoning | System Network Connections Discovery | System Network Configuration Discovery | Man in the Browser | System Owner/User Discovery | Standard Non-Application Layer Protocol |
| | PowerShell | Create Account | Hooking | Disabling Security Tools | Network Sniffing | System Service Discovery | System Time Discovery | Screen Capture | System Service Discovery | Uncommonly Used Port |
| | Regsvcs/Regasm | DLL Search Order Hijacking | Image File Execution Options Injection | DLL Search Order Hijacking | Password Filter DLL | System Time Discovery | | Video Capture | | Web Service |
| | Regsvr32 | External Remote Services | Image File Execution Options Injection | DLL Side-Loading | Private Keys | | | | | |
| | Rundll32 | File System Permissions Weakness | Image File Execution Options Injection | Exploitation for Defense Evasion | Replication Through Removable Media | | | | | |
| | Scheduled Task | Hidden Files and Directories | New Service | Extra Window Memory Injection | Two-Factor Authentication Interception | | | | | |
| | Scripting | Hooking | Path Interception | File Deletion | | | | | | |
| | Service Execution | Hypervisor | Port Monitors | File System Logical Offsets | | | | | | |
| | Signed Binary Proxy Execution | Image File Execution Options Injection | Process Injection | Hidden Files and Directories | | | | | | |
| | Signed Script Proxy Execution | Logon Scripts | Scheduled Task | Image File Execution Options Injection | | | | | | |
| | Third-party Software | LSASS Driver | Service Registry Permissions Weakness | Indicator Blocking | | | | | | |
| | Trusted Developer Utilities | Modify Existing Service | SID-History Injection | Indicator Removal from Tools | | | | | | |
| | User Execution | Netsh Helper DLL | Valid Accounts | Indicator Removal on Host | | | | | | |
| | Windows Management Instrumentation | New Service | Web Shell | Indirect Command Execution | | | | | | |
| | Windows Remote Management | Office Application Startup | | Install Root Certificate | | | | | | |
| | | Path Interception | | InstallUtil | | | | | | |
| | | Port Monitors | | Masquerading | | | | | | |
| | | Redundant Access | | Modify Registry | | | | | | |
| | | Registry Run Keys / Start Folder | | Mshata | | | | | | |
| | | Scheduled Task | | Network Share Connection Removal | | | | | | |
| | | Screen saver | | NTFS File Attributes | | | | | | |
| | | Security Support Provider | | Obfuscated Files or Information | | | | | | |
| | | Service Registry Permissions Weakness | | Process Doppelgänger | | | | | | |
| | | Shortcut Modification | | Process Hollowing | | | | | | |
| | | SIP and Trust Provider Hijacking | | Process Injection | | | | | | |
| | | System Firmware | | Redundant Access | | | | | | |
| | | Time Providers | | Regsvcs/Regasm | | | | | | |
| | | Valid Accounts | | Regsvr32 | | | | | | |
| | | Web Shell | | Rootkit | | | | | | |
| | | Windows Management Instrumentation Event Subscription | | Rundll32 | | | | | | |
| | | Winlogon Helper DLL | | Scripting | | | | | | |
| | | | | Signed Binary Proxy Execution | | | | | | |
| | | | | Signed Script Proxy Execution | | | | | | |
| | | | | SIP and Trust Provider Hijacking | | | | | | |
| | | | | Software Packing | | | | | | |
| | | | | Timestomp | | | | | | |
| | | | | Trusted Developer Utilities | | | | | | |
| | | | | Valid Accounts | | | | | | |
| | | | | Web Service | | | | | | |

Olaf Hartong Sysmon

Olaf Hartong has been doing some amazing work mapping Sysmon configurations to the MITRE ATT&CK framework. He strongly leverages the “tagging” feature that was added in Sysmon 8. Olaf based himself on the work that was already performed by SwiftOnSecurity, as he uses that configuration file as a starting point! He also wrote a blog post series called “Endpoint detection Superpowers on the cheap”!

ATT&CK Initiatives - Detection

Many open-source tools align with ATT&CK



```

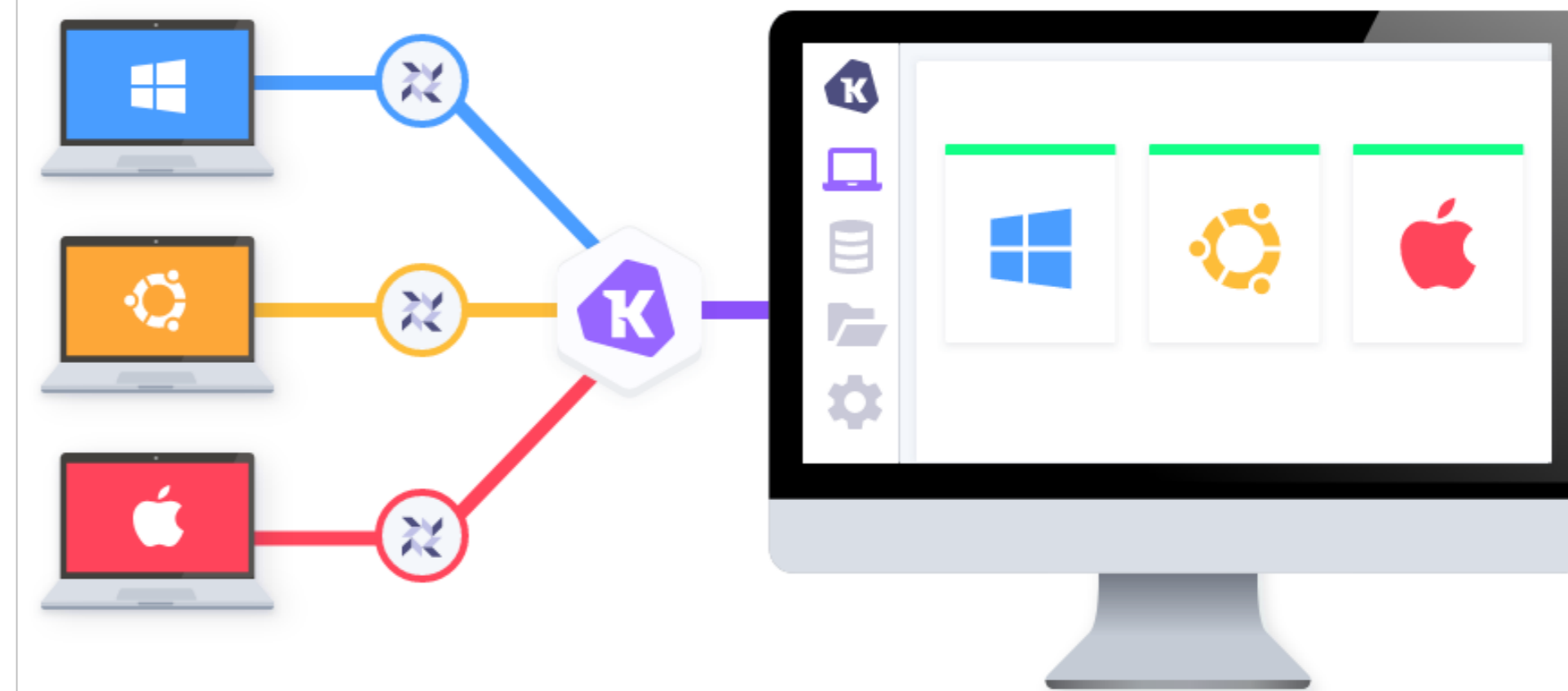
73 lines (72 sloc) | 6.34 KB
Raw Blame History
1 {
2   "platform": "windows",
3   "description": "ATT&CK: T1173,T1086,T1204,T1183",
4   "queries": {
5     "services.exe_incorrect_parent_process": {
6       "query": "SELECT name as bad_parent_child_name, pid bad_parent_child_pid FROM processes WHERE pid=(SELECT parent FROM processes WHE
7       "interval": 60,
8       "description": "Detect processes masquerading as legitimate Windows processes - ATT&CK T1204",
9       "removed": false
10    },
11    "lsass.exe_incorrect_parent_process": {
12      "query": "SELECT name as bad_parent_child_name, pid bad_parent_child_pid FROM processes WHERE pid=(SELECT parent FROM processes WHE
13      "interval": 60,
14      "description": "Detect processes masquerading as legitimate Windows processes - ATT&CK T1204",
15      "removed": false
16    },
17    "svchost.exe_incorrect_parent_process": {
18      "query": "SELECT name as bad_parent_child_name, pid bad_parent_child_pid FROM processes WHERE pid=(SELECT parent FROM processes WHE
19      "interval": 60,
20      "description": "Detect processes masquerading as legitimate Windows processes - ATT&CK T1204",
21      "removed": false
22    },

```

<https://github.com/teoseller/osquery-attck>

Kolide Fleet

Open Source Osquery Manager




osquery (by Facebook) allows you to easily ask questions about your Linux, Windows, and macOS infrastructure.

A GitHub repository was created by “teoseller” that maps queries to the MITRE ATT&CK framework!

ATT&CK Initiatives - Detection

Many open-source tools align with ATT&CK

Branch: master [sigma](#) / [rules](#) / [windows](#) / [builtin](#) / [win_alert_mimikatz_keywords.yml](#) Find file Copy path

 thomaspatzke ATT&CK tagging QA 81515b5 on Sep 20, 2018

1 contributor

26 lines (25 sloc) | 677 Bytes Raw Blame History

```

1 title: Mimikatz Use
2 description: This method detects mimikatz keywords in different Eventlogs (some of them only appear in older Mimikatz version that are howe
3 author: Florian Roth
4 tags:
5   - attack.s0002
6   - attack.t1003
7   - attack.lateral_movement
8   - attack.credential_access
9 logsource:
10  product: windows
11 detection:
12  keywords:
13    - mimikatz
14    - mimilib
15    - <3 eo.oe
16    - eo.oe.kiwi
17    - privilege::debug
18    - sekurlsa::logonpasswords
19    - lsadump::sam
20    - mimidrv.sys
21  condition: keywords
22 falsepositives:
23   - Naughty administrators
24   - Penetration test
25 level: critical

```

SIGMA

Sigma is a project by Florian Roth which tries to provide a generic, vendor-neutral, rule format that can be used to describe suspicious or malicious behavior. Most SIGMA rules are also mapped to MITRE's ATT&CK framework.

Sigma Format

Generic Signature Description

Sigma Converter

Applies Predefined and Custom Field Mapping

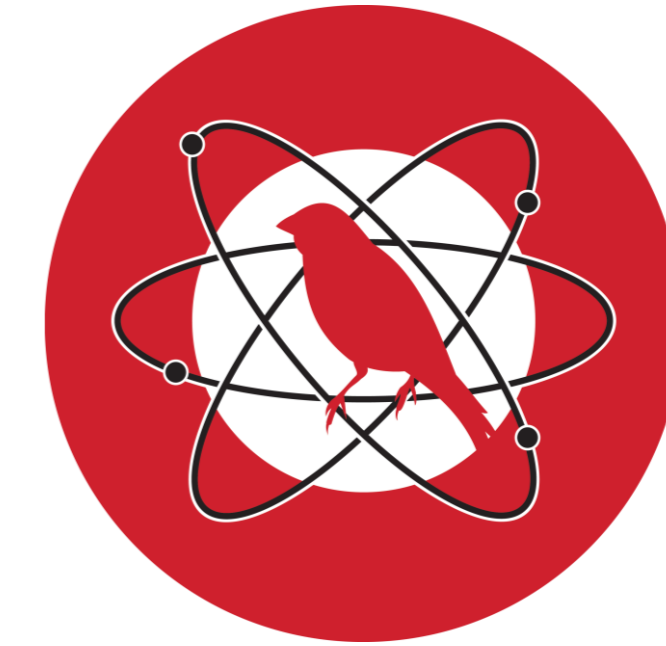
Elastic Search Queries

Splunk Searches

...

ATT&CK Initiatives - Emulation

Many open-source tools align with ATT&CK



redcanaryco / [atomic-red-team](#) Watch 197 Star 1,788 Fork 545

[Code](#) [Issues 7](#) [Pull requests 5](#) [Insights](#)

Branch: master [atomic-red-team / atomics /](#) [Create new file](#) [Find file](#) [History](#)

caseysmithrc and zacbrown T1055 process injection (#460) ... Latest commit a668ff0 4 days ago

| | | |
|-------------------------|---|--------------|
| .. | | |
| RC13378 | Systemd Service Creation Test | 7 months ago |
| T1002 | Generate docs from job=validate_atomics_generate_docs branch=master | a month ago |
| T1003 | Update t1003 url (#405) | 15 days ago |
| T1004 | Generate docs from job=validate_atomics_generate_docs branch=master | 2 months ago |
| T1005 | Generate docs from job=validate_atomics_generate_docs branch=master | 8 days ago |
| T1007 | Generate docs from job=validate_atomics_generate_docs branch=master | 2 months ago |
| T1009 | Generate docs from job=validate_atomics_generate_docs branch=master | a month ago |
| T1010 | Generate docs from job=validate_atomics_generate_docs branch=master | 2 months ago |
| T1012 | Generate docs from job=validate_atomics_generate_docs branch=master | 3 months ago |
| T1014 | Generate docs from job=validate_atomics_generate_docs branch=master | 3 months ago |
| T1015 | Generate docs from job=validate_atomics_generate_docs branch=master | 3 months ago |
| T1016 | Generate docs from job=validate_atomics_generate_docs branch=master | 3 months ago |
| T1018 | Generate docs from job=validate_atomics_generate_docs branch=master | 3 months ago |
| T1022 | Generate docs from job=validate_atomics_generate_docs branch=master | 3 months ago |

Red Canary developed “Atomic Red Team”, which is a series of “simple” tests that can be used to emulate the behavior of adversaries in the environment.

The tests are linked to **MITRE ATT&CK!**

ATT&CK Initiatives - Emulation

Many open-source tools align with ATT&CK

The screenshot displays the CALDERA web interface. The top navigation bar includes 'CALDERA', 'Threat', 'Networks', 'Operations', and 'Debug'. On the right, there are links for 'Script Editor', 'Settings', and 'admin (Admin)'. A dropdown menu is open under 'Threat', listing options: 'ATT&CK Matrix', 'View Steps', 'View Adversaries', 'Create Adversary', 'View Artifact Lists', and 'Create Artifact List'. The main area shows a network diagram with five red circular nodes labeled 'win7x01', 'win7x02', 'win7x03', 'win7x04', and 'win2012xdc'. To the right, a table titled 'Network mountainpeak.local' lists the hosts and their status.

| hostname | Status |
|------------|--------|
| win7x01 | active |
| win7x04 | active |
| win7x02 | active |
| win7x03 | active |
| win2012xdc | active |

Below the table is a section titled 'Add a New Host' with a blue '+' button and a text input field.

CALDERA is a tool built by MITRE, with the express purpose of doing adversary emulation. It requires a bit of setup (as a server needs to be installed) and it will actively “attack” target systems by deploying custom backdoors. CALDERA’s attack steps are fully linked to the ATT&CK framework techniques!

ATT&CK Initiatives - Something new...

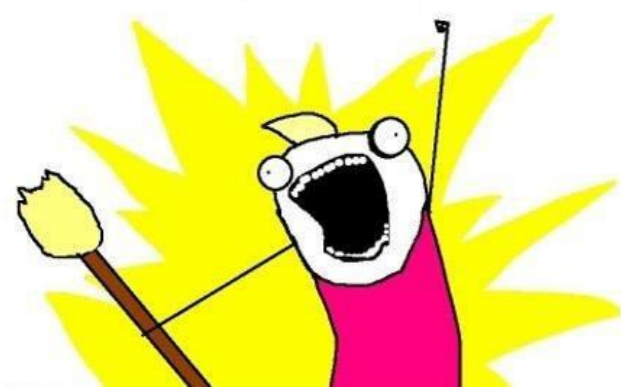
Many open-source tools align with ATT&CK

In February 2019, Atomic Threat Coverage was released by:

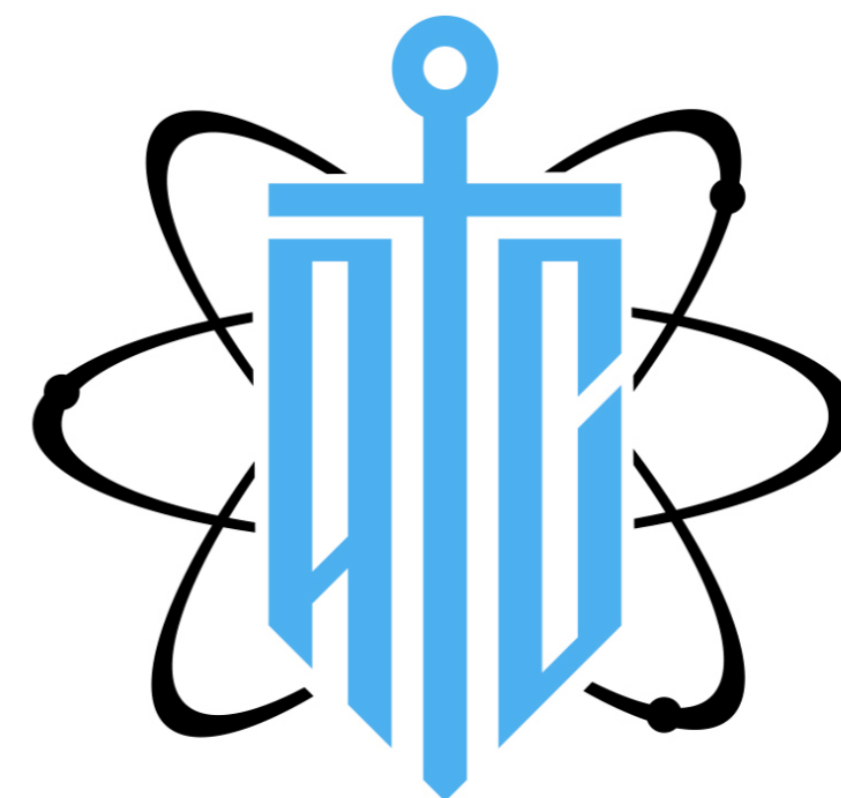
- Daniil Yugoslavskiy (@yugoslavskiy)
- Jakob Weinzettl (@mrblacyk)
- Mateusz Wydra (@sn0w0tter)
- Mikhail Aksenov (@AverageS)

Their goal is to have an “all-in-one” solution for detection, response, mitigation and simulation using MITRE ATT&CK!

<https://github.com/krakov2600/atomic-threat-coverage>



ATT&CK all the things!



Atomic Threat Coverage is tool which allows you to automatically generate knowledge base of analytics, designed to combat threats (based on the [MITRE ATT&CK](#) adversary model) from Detection, Response, Mitigation and Simulation perspectives:

- **Detection Rules** based on [Sigma](#) — Generic Signature Format for SIEM Systems
- **Data Needed** to be collected to produce detection of specific Threat
- **Logging Policies** need to be configured on data source to be able to collect Data Needed
- **Enrichments** for specific Data Needed which required for some Detection Rules
- **Triggers** based on [Atomic Red Team](#) — detection tests based on MITRE's ATT&CK
- **Response Actions** which executed during Incident Response
- **Response Playbooks** for reacting on specific threat, constructed from atomic Response Actions
- **Hardening Policies** need to be implemented to mitigate specific Threat
- **Mitigation Systems** need to be deployed and configured to mitigate specific Threat

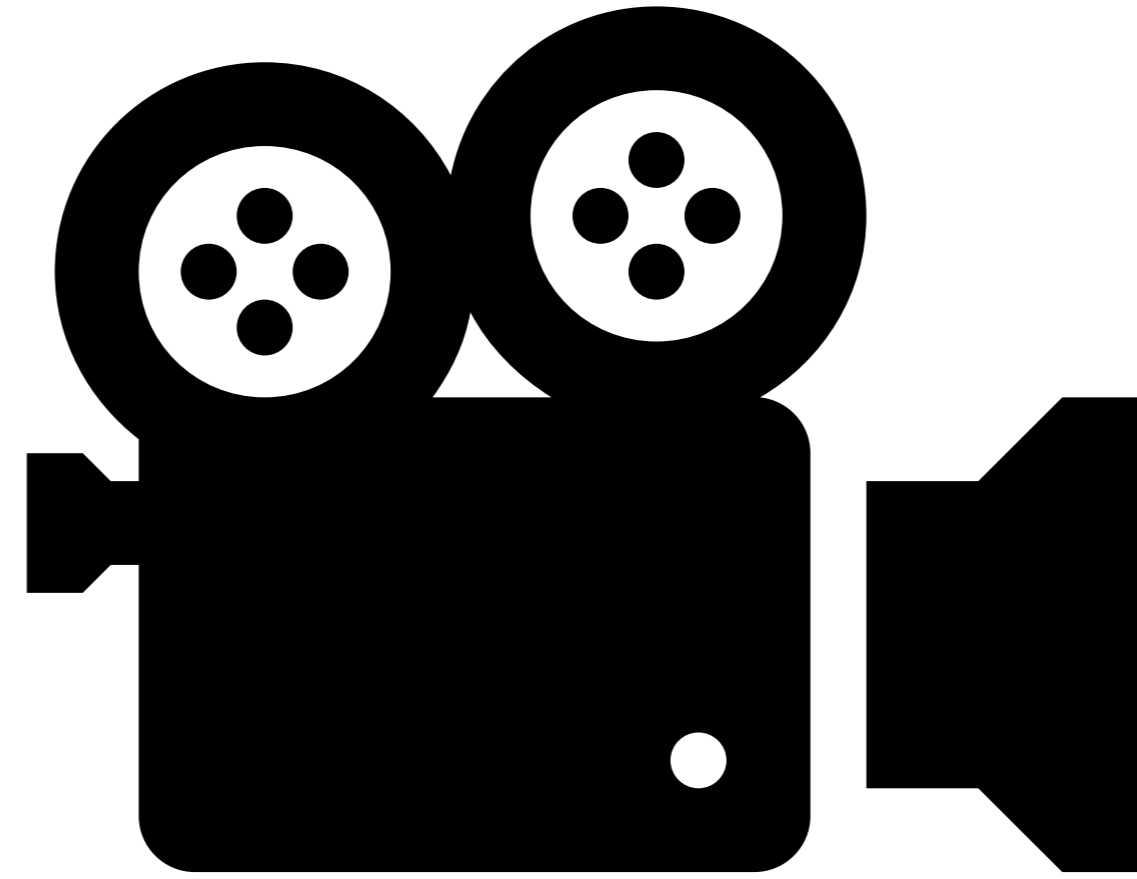


Demo

Demonstrating Caldera & ATT&CK Navigator

Demo

ATT&CK Navigator and CALDERA in action



- ATT&CK should be used as a “**common language**” by a variety of security functions in the organisation (adversary emulation, security monitoring, threat hunting,...)
- ATT&CK is huge and covering all techniques from the start is not feasible, **prioritize** according to popularity of techniques (general) and your own organization (based on relevant threat actors)!
- Don't reinvent the wheel: Leverage and contribute to **existing projects** to hit the ground running!

Want more?

Some additional links & references

- **ATT&CKCon 2018 presentations**
<https://www.slideshare.net/attackcon2018/presentations>
- **ATT&CK™ Your CTI with Lessons Learned from Four Years in the Trenches - Katie Nickels (MITRE) & Bryan Beyer (Red Canary)**
<https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1548090281.pdf>
- **ATT&CK™ Is Only as Good as Its Implementation: Avoiding Five Common Pitfalls (Kyle Rainey - Red Canary)**
<https://www.redcanary.com/blog/avoiding-common-attack-pitfalls/>



Q&A

Any questions?