THE SOC COUNTER ATT&CK

By Mathieu Saulnier

@ScoubiMtl

Disclamer

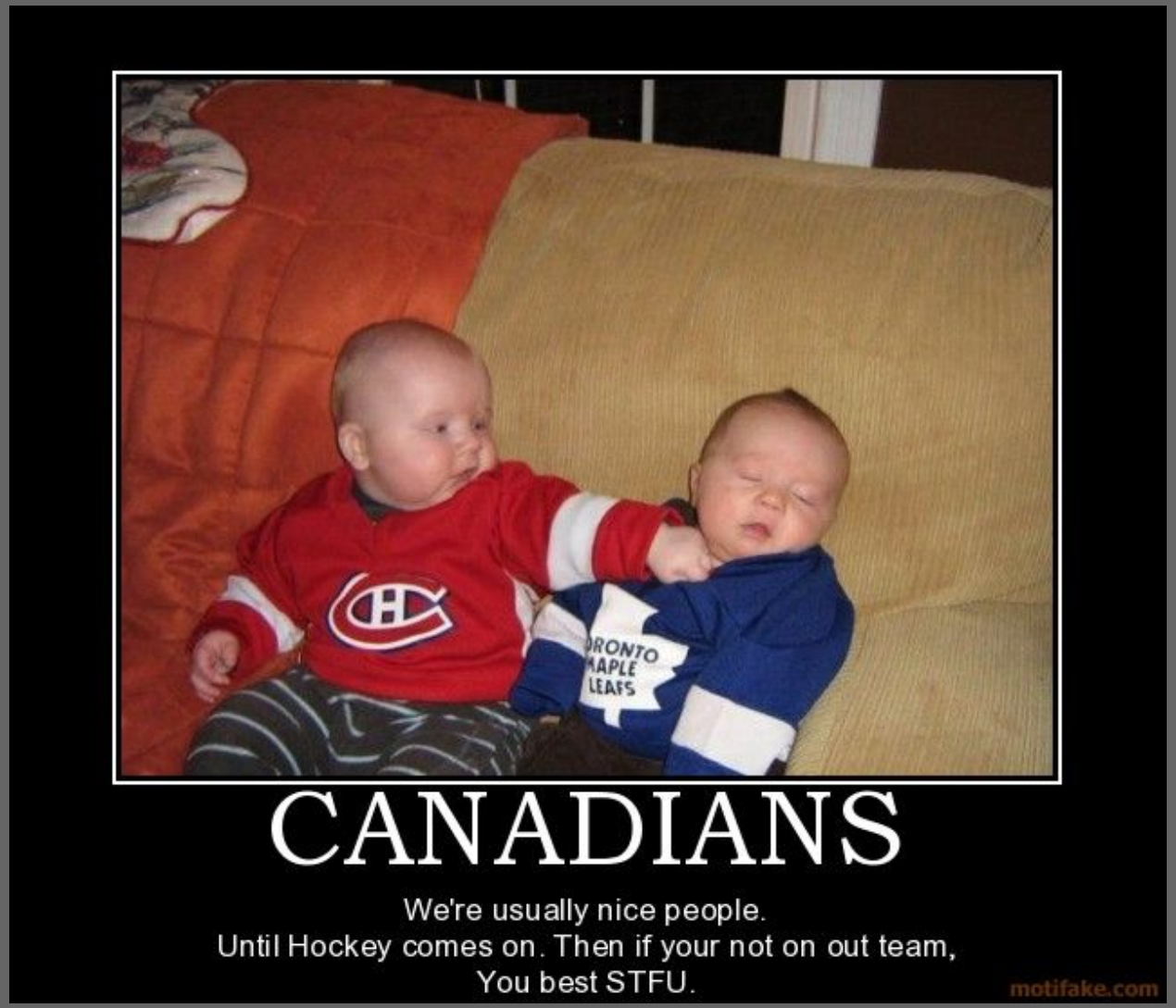
This presentation expresses and represents the views, opinions and/or personal positions of the presenter only and all comments made prior, during or following this presentation represent the views, opinions and/or personal positions of the presenter only and do not, in any way, represent those of my current employer or any of its affiliates and/or subsidiaries.

BIO

SOC Technical Manager
- Threat Hunting
- Adversary Detection

Defcon's BTV Volunteer

I'm from Montreal
- Don't pronounce 'h' or 's'



ATT&CK™

SECTOR

Agenda

ATT&CK Overview

ATT&CK-Navigator

Preliminary Assessment

ATT&CK & Open Sources

Building Detection

ATT&CK OVERVIEW

ATT&CK™

What is ATT&CK

Adversarial Tactics, Techniques, and Common Knowledge

Knowledgebase of Adversary Behavior (TTP)

- Tactics
- Techniques
- Procedures

Focus on Real Attacks

Provide a common language

Open Source

BSidesLV 2018 : ATT&CKing the Status Quo

https://youtu.be/p7Hyd7d9k-c

History

Created in September 2013

Need to systematically categorize adversary behavior

Enumerate and categorize adversary TTPs against Windows

- Now also covers MacOS & Linux

Release to the public in May 2015

- 9 Tactics
- 96 Techniques

Today (as of April 30th)

- ~~11~~ 12Tactics
- ~~223~~ 244 Techniques

Example

https://attack.mitre.org/techniques/T1208/

Kerberoasting

Service principal names (SPNs) are used to uniquely identify each instance of a Windows service. To enable authentication, Kerberos requires that SPNs be associated with at least one service logon account (an account specifically tasked with running a service [1]). [2] [3] [4] [5]

Adversaries possessing a valid Kerberos ticket-granting ticket (TGT) may request one or more Kerberos ticket-granting service (TGS) service tickets for any SPN from a domain controller (DC). [6] [7] Portions of these tickets may be encrypted with the RC4 algorithm, meaning the Kerberos 5 TGS-REP etype 23 hash of the service account associated with the SPN is used as the private key and is thus vulnerable to offline Brute Force attacks that may expose plaintext credentials. [7] [6] [5]

This same attack could be executed using service tickets captured from network traffic. [7]

Cracked hashes may enable Persistence, Privilege Escalation, and Lateral Movement via access to Valid Accounts. [4]

ID: T1208

Tactic: Credential Access

Platform: Windows

Permissions Required: User

Data Sources: Windows event logs

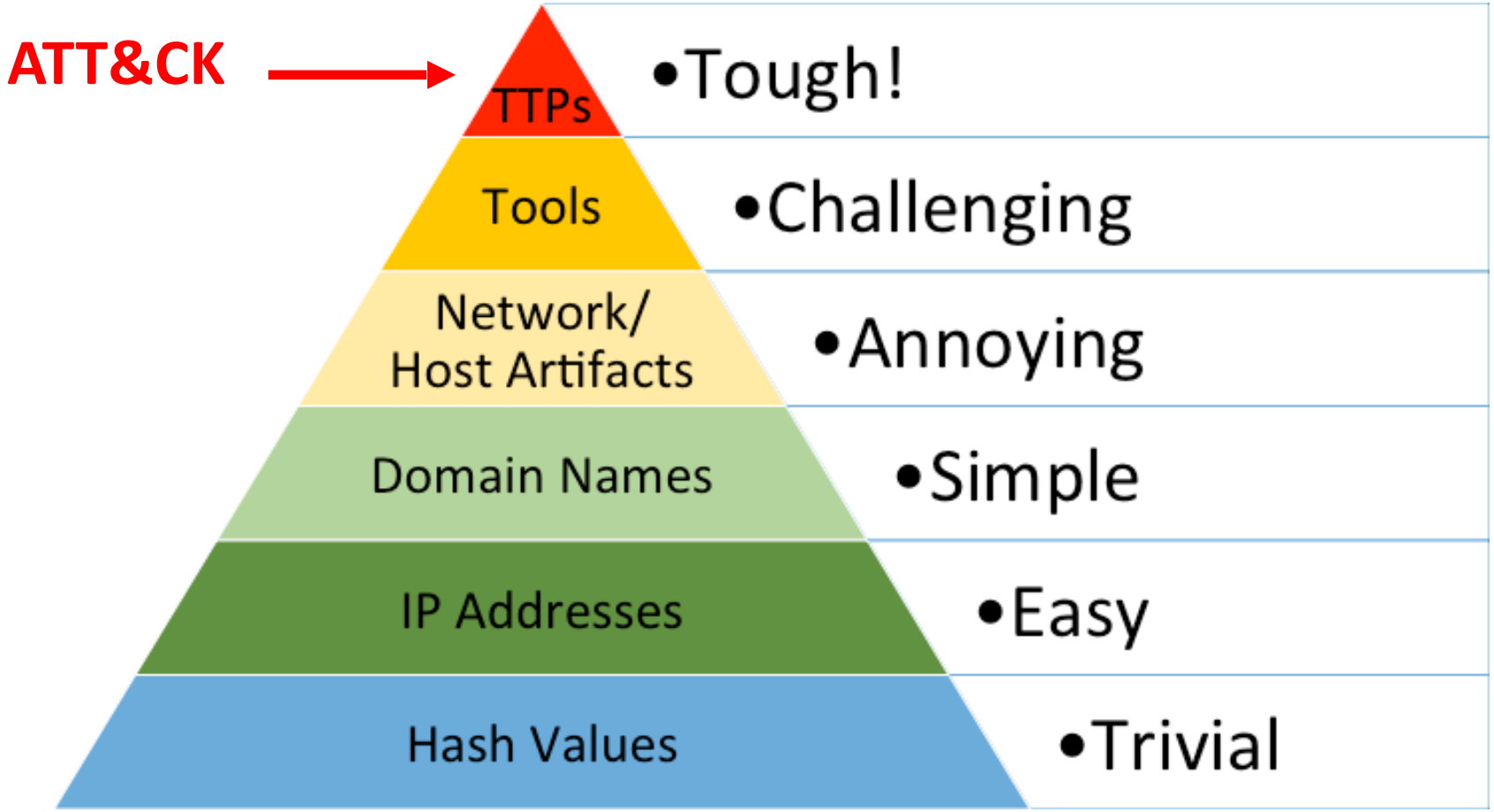
Contributors: Praetorian

Version: 1.0

Examples

Name	Description
PowerSploit	PowerSploit's `Invoke-Kerberoast` module can request service tickets and return crackable ticket hashes.[8][5]

Pyramid of Pain



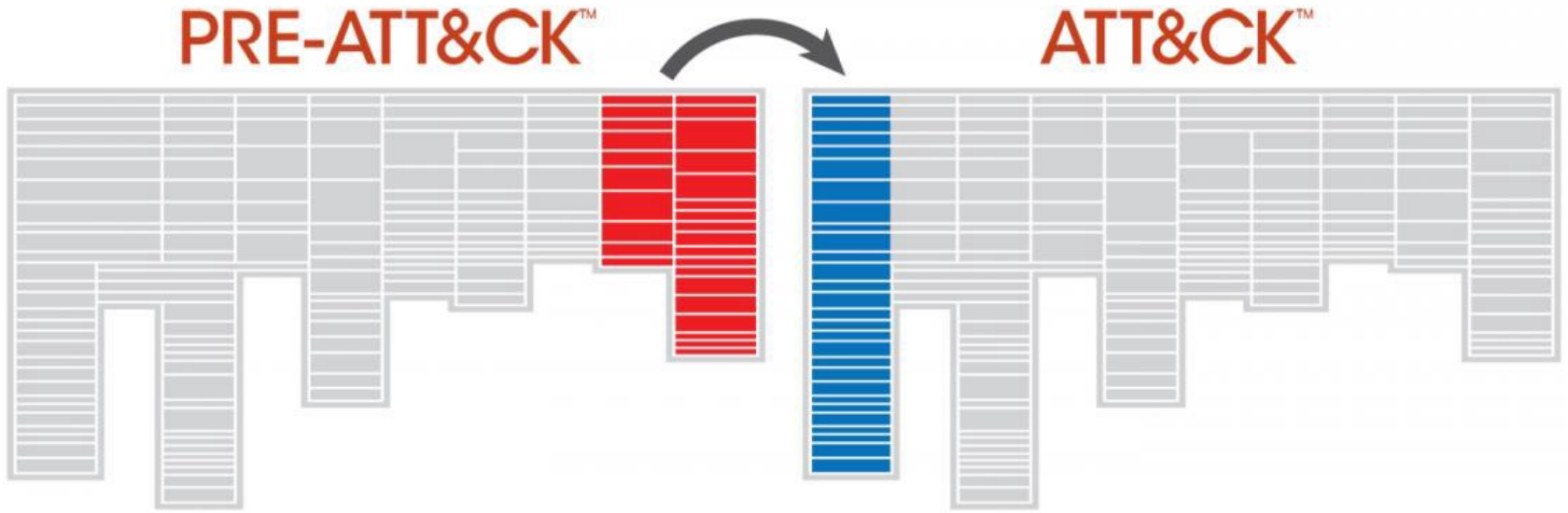
http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Multiple ATT&CK

Pre-ATT&CK

Enterprise

Mobile



ATT&CK – Cyber Kill Chain

PRE-ATT&CK™

Priority Definition
- Planning, Direction

Target Selection

Information Gathering
- Technical, People, Organizational

Weakness Identification
- Technical, People, Organizational

Adversary OpSec

Establish & Maintain Infrastructure

Persona Development

Build Capabilities

Test Capabilities

Stage Capabilities

Enterprise ATT&CK

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Exfiltration

Command and Control

ATT&CK™

SECTOR
Security Education Conference

ATT&CKcon

https://www.mitre.org/attackcon

2 Days in October 2018

Live Streaming on YouTube

20 Presentations

There will be another edition this year!

October 28-30, 2019

GETTING STARTED

ATT&CK™

MITRE ATT&CK™ Navigator

layer x +

selection controls | layer controls | technique controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command Control
11 items	33 items	59 items	28 items	67 items	19 items	22 items	17 items	13 items	22 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communica Through Removable
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery			
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery			
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery			
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning			
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery			
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing			
	Exploitation for Client Execution	Bootkit	Exploitation for Privilege	Compiled HTML File	Hooking	Password Policy Discovery			
	Graphical User Interface	Browser Extensions		Component Firmware	Input Capture	Peripheral Device Discovery			
		Change Default File Association		Component Object Model Hijacking	Input Prompt				
				Control Panel Items					
				DCShadow					

legend

#31a354	Multiple Detection
#74c476	Single Detection
#fdae6b	Dashboard
#fce93b	Report
#00ffff	Soaking

Add Item | Clear

MITRE ATT&CK™ Navigator

layer x +

selection controls | layer controls | technique controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command Control
11 items	33 items	59 items	28 items	67 items	19 items	22 items	17 items	13 items	22 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communica Through Removable
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery			
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery			
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery			
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning			
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery			
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing			
	Exploitation for Client Execution	Bootkit	Exploitation for Privilege	Compiled HTML File	Hooking	Password Policy Discovery			
	Graphical User Interface	Browser Extensions		Component Firmware	Input Capture	Peripheral Device Discovery			
		Change Default File Association		Component Object Model Hijacking	Input Prompt				
				Control Panel Items					
				DCShadow					

legend

#31a354	Multiple Detection
#74c476	Single Detection
#fdae6b	Dashboard
#fce93b	Report
#00ffff	Soaking

Add Item | Clear

MITRE ATT&CK™ Navigator

layer x +

selection controls | layer controls | technique controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command Control
11 items	33 items	59 items	28 items	67 items	19 items	22 items	17 items	13 items	22 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communica Through Removable
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery			
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery			
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery			
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning			
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery			
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing			
	Exploitation for Client Execution	Bootkit	Exploitation for Privilege	Compiled HTML File	Hooking	Password Policy Discovery			
	Graphical User Interface	Browser Extensions		Component Firmware	Input Capture	Peripheral Device Discovery			
		Change Default File Association		Component Object Model Hijacking	Input Prompt				
				Control Panel Items					
				DCShadow					

legend

#31a354	Multiple Detection
#74c476	Single Detection
#fdae6b	Dashboard
#fce93b	Report
#00ffff	Soaking

Add Item | Clear

layer x +

selection controls | layer controls | technique controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command Control
11 items	33 items	59 items	28 items	67 items	19 items	22 items	17 items	13 items	22 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communica Through Removable
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery			
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery			
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery			
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning			
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery			
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing			
	Exploitation for Client Execution	Bootkit	Exploitation for Privilege	Compiled HTML File	Hooking	Password Policy Discovery			
	Graphical User Interface	Browser Extensions		Component Firmware	Input Capture	Peripheral Device Discovery			
		Change Default File Association		Component Object Model Hijacking	Input Prompt				
				Control Panel Items					
				DCShadow					

legend

#31a354	Multiple Detection
#74c476	Single Detection
#fdae6b	Dashboard
#fce93b	Report
#00ffff	Soaking

Add Item | Clear

layer x +

selection controls | layer controls | technique controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command Control
11 items	33 items	59 items	28 items	67 items	19 items	22 items	17 items	13 items	22 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communica Through Removable
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery			
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery			
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery			
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning			
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery			
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing			
	Exploitation for Client Execution	Bootkit	Exploitation for Privilege	Compiled HTML File	Hooking	Password Policy Discovery			
	Graphical User Interface	Browser Extensions		Component Firmware	Input Capture	Peripheral Device Discovery			
		Change Default File Association		Component Object Model Hijacking	Input Prompt				
				Control Panel Items					
				DCShadow					

legend

#31a354	Multiple Detection
#74c476	Single Detection
#fdae6b	Dashboard
#fce93b	Report
#00ffff	Soaking

Add Item | Clear

layer x +

selection controls | layer controls | technique controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command Control
11 items	33 items	59 items	28 items	67 items	19 items	22 items	17 items	13 items	22 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communica Through Removable
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery			
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery			
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery			
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning			
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery			
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing			
	Exploitation for Client Execution	Bootkit	Exploitation for Privilege	Compiled HTML File	Hooking	Password Policy Discovery			
	Graphical User Interface	Browser Extensions		Component Firmware	Input Capture	Peripheral Device Discovery			
		Change Default File Association		Component Object Model Hijacking	Input Prompt				
				Control Panel Items					
				DCShadow					

legend

#31a354	Multiple Detection
#74c476	Single Detection
#fdae6b	Dashboard
#fce93b	Report
#00ffff	Soaking

Add Item | Clear

Preliminary Assessment

Basic Questions

- Logs
- Complexity
- Severity
- Probability
- Dependency on other teams
- Targets (Servers / Workstations)
- Open Source Project

Data Source

- Number
- Know what you have
- Focus on getting the one you don’t
- Plan your retention strategy

Quantify Your Hunt: Not Your Parents Red Teaming
https://youtu.be/w_kByDwB6J0 | https://youtu.be/u_RaWTzB1wA

ATT&CK™

SECTOR

Scoring

Each Question have points / weight

Score Each TTP (color)

Script to apply to the JSON file

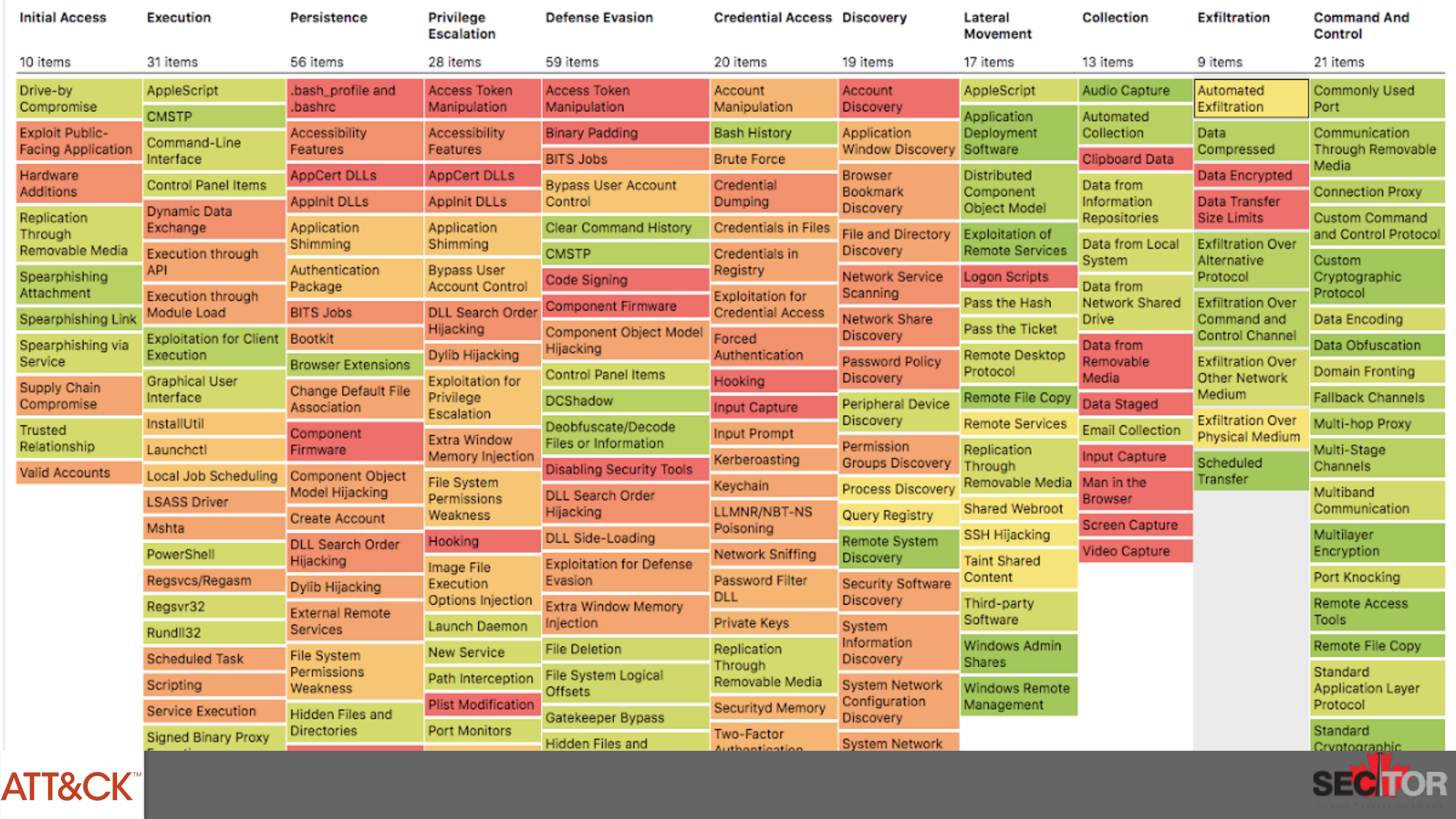
Example of Questions

How Many log sources do I have for this Technique?	35%
What is the probability to be targeted by this?	30%
Does this target Linux server?	25%
Open Source Project?	10%

0 - 35	= RED	-> Low Dev Priority
36 - 75	= ORANGE	-> Medium Dev Priority
76 - 100	= GREEN	-> High Dev Priority

ATT&CK™

SECTOR


Initial Access
10 items
Drive-by Compromise
Exploit Public-Facing Application
Hardware Additions
Replication Through Removable Media
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Execution
31 items
AppleScript
CMSTP
Command-Line Interface
Control Panel Items
Dynamic Data Exchange
Execution through API
Execution through Module Load
Exploitation for Client Execution
Graphical User Interface
InstallUtil
Launchctl
Local Job Scheduling
LSASS Driver
Mshta
PowerShell
Regsvcs/Regasm
Regsvr32
Rundll32
Scheduled Task
Scripting
Service Execution
Signed Binary Proxy
Persistence
56 items
.bash_profile and .bashrc
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Authentication Package
BITS Jobs
Bootkit
Browser Extensions
Change Default File Association
Component Firmware
Component Object Model Hijacking
Create Account
DLL Search Order Hijacking
Dylib Hijacking
External Remote Services
File System Permissions Weakness
Hidden Files and Directories
Privilege Escalation
28 items
Access Token Manipulation
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Bypass User Account Control
DLL Search Order Hijacking
Dylib Hijacking
Exploitation for Privilege Escalation
Extra Window Memory Injection
File System Permissions Weakness
Hooking
Image File Execution Options Injection
Launch Daemon
New Service
Path Interception
Plist Modification
Port Monitors
Defense Evasion
59 items
Access Token Manipulation
Binary Padding
BITS Jobs
Bypass User Account Control
Clear Command History
CMSTP
Code Signing
Component Firmware
Component Object Model Hijacking
Control Panel Items
DCShadow
Deobfuscate/Decode Files or Information
Disabling Security Tools
DLL Search Order Hijacking
DLL Side-Loading
Exploitation for Defense Evasion
Extra Window Memory Injection
File Deletion
File System Logical Offsets
Gatekeeper Bypass
Hidden Files and
Credential Access
20 items
Account Manipulation
Bash History
Brute Force
Credential Dumping
Credentials in Files
Credentials in Registry
Exploitation for Credential Access
Forced Authentication
Hooking
Input Capture
Input Prompt
Kerberoasting
Keychain
LLMNR/NBT-NS Poisoning
Network Sniffing
Password Filter DLL
Private Keys
Replication Through Removable Media
Securityd Memory
Two-Factor
Discovery
19 items
Account Discovery
Application Window Discovery
Browser Bookmark Discovery
File and Directory Discovery
Network Service Scanning
Network Share Discovery
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Security Software Discovery
System Information Discovery
System Network Configuration Discovery
System Network
Lateral Movement
17 items
AppleScript
Application Deployment Software
Distributed Component Object Model
Exploitation of Remote Services
Logon Scripts
Pass the Hash
Pass the Ticket
Remote Desktop Protocol
Remote File Copy
Remote Services
Replication Through Removable Media
Shared Webroot
SSH Hijacking
Taint Shared Content
Third-party Software
Windows Admin Shares
Windows Remote Management
Collection
13 items
Audio Capture
Automated Collection
Clipboard Data
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Man in the Browser
Screen Capture
Video Capture
Exfiltration
9 items
Automated Exfiltration
Data Compressed
Data Encrypted
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over Command and Control Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Scheduled Transfer
Command And Control
21 items
Commonly Used Port
Communication Through Removable Media
Connection Proxy
Custom Command and Control Protocol
Custom Cryptographic Protocol
Data Encoding
Data Obfuscation
Domain Fronting
Fallback Channels
Multi-hop Proxy
Multi-Stage Channels
Multiband Communication
Multilayer Encryption
Port Knocking
Remote Access Tools
Remote File Copy
Standard Application Layer Protocol
Standard Cryptographic

Track Progress & Coverage

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
10 items	33 items	58 items	28 items	63 items	19 items	20 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery
	Launchctl	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Keychain	Remote System Discovery
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools	LLMNR/NBT-NS Poisoning	Security Software Discovery
	Mshta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Network Sniffing	System Information Discovery
	PowerShell	Dylib Hijacking	Path Interception	DLL Side-Loading	Password Filter DLL	
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	
	Regsvr32	File System Permissions Weakness		Extra Window Memory Injection	Securityd Memory	
	Rundll32	Hidden Files and Directories		File Deletion	Two-Factor Authentication Interception	
	Scheduled Task					
	Scripting					

ATT&CK™

SECTOR

Track Progress & Coverage

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
10 items	33 items	58 items	28 items	63 items	19 items	20 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery
	Launchctl	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Keychain	Remote System Discovery
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools	LLMNR/NBT-NS Poisoning	Security Software Discovery
	Mshta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Network Sniffing	System Information Discovery
	PowerShell	Dylib Hijacking	Path Interception	DLL Side-Loading	Password Filter DLL	
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	
	Regsvr32	File System Permissions Weakness		Extra Window Memory Injection	Securityd Memory	
	Rundll32	Hidden Files and Directories		File Deletion	Two-Factor Authentication Interception	
	Scheduled Task					
	Scripting					

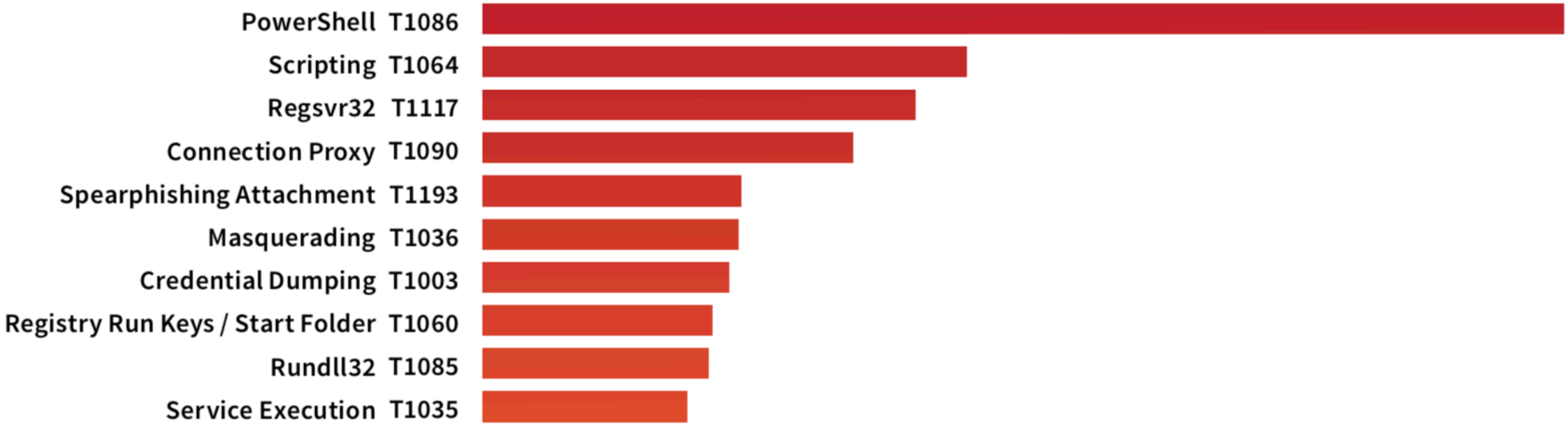
ATT&CK™

SECTOR

Management Questions

March 19 : Red Canary - Threat Detection Report

https://redcanary.com/resources/guides/threat-detection-report/



ATT&CK™

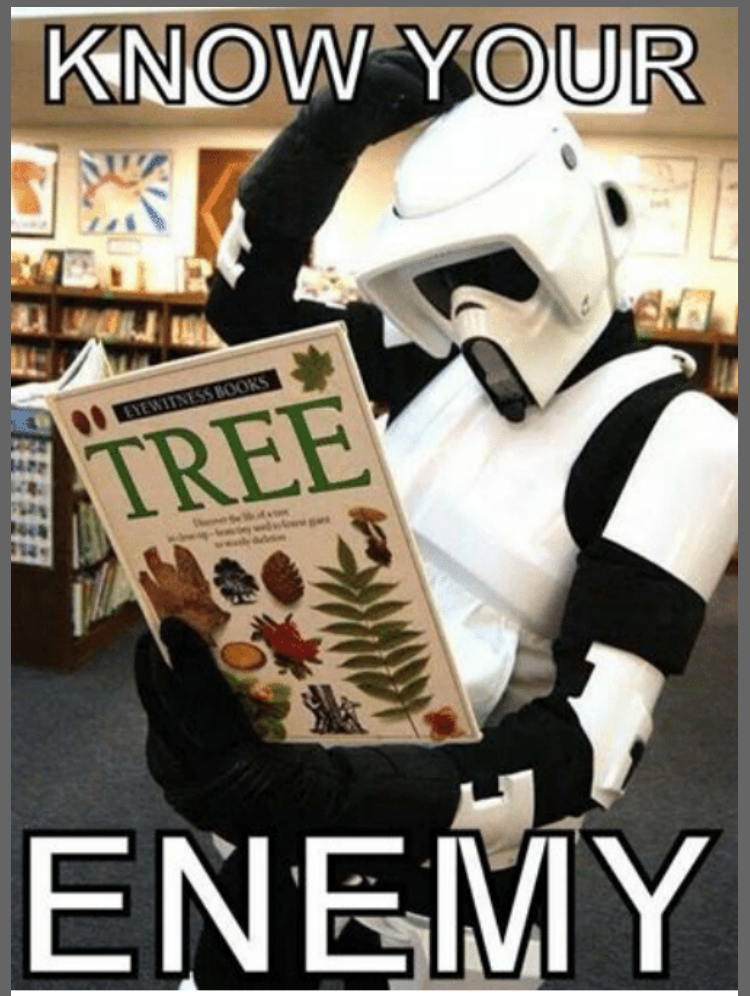
SECTOR

Know Your Enemy

Threat Model

Threat Actors

TTP



Can a Speederbike Trooper read if he can't see trees ??

ATT&CK™

SECTOR

Metrics & KPI

Good

Show Monthly Progression

Show Coverage

Prioritize Data Source

Alerting vs Hunting

Single vs Multiple

Bad

Assuming all TTP are equal

Falling for Coverage vs Depth

Some TTP are not for Alerting

Not counting Non ATT&CK

Convert all rules from a project to an Alert

5 Ways to Screw Up Your Security Program with ATT&CK
https://youtu.be/MBVxaE9oaMQ

ATT&CK™

SECTOR

ATT&CK & OPEN SOURCE

Sigma

https://github.com/Neo23x0/sigma

Generic Signature Format for SIEM Systems

Florian Roth

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
11 items	33 items	59 items	28 items	67 items	19 items	22 items	17 items	13 items	22 items	9 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels	
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy	
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels	
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication	
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption	
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking	
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools	
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy	
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol	
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol	
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol	
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery			Uncommonly Used Port	
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service	
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets						
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass						
	Source	Launch Daemon	Sudo	Group Policy Modification						
	Space after Filename	Launchctl	Sudo Caching	Hidden Files and Directories						
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Users						
	Trap	Local Job Scheduling	Web Shell	Hidden Window						
	Trusted Developer Utilities	Login Item		HISTCONTROL						
	User Execution	Logon Scripts		Image File Execution Options Injection						
	Windows Management Instrumentation	LSASS Driver		Indicator Blocking						
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools						
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host						
		New Service		Indirect Command Execution						
		Office Application Startup		Install Root Certificate						
		Path Interception		InstallUtil						
		Plist Modification		Launchctl						
		Port Knocking		LC_MAIN Hijacking						
		Port Monitors		Masquerading						
		Rc.common		Modify Registry						
		Re-opened Applications		Mshta						
		Redundant Access		Network Share Connection Removal						
		Registry Run Keys / Startup Folder		NTFS File Attributes						
		Scheduled Task		Obfuscated Files or Information						
		Screensaver		Plist Modification						
		Security Support Provider		Port Knocking						
		Service Registry Permissions Weakness		Process Doppelgänging						
		Setuid and Setgid		Process Hollowing						
		Shortcut Modification		Process Injection						
		SIP and Trust Provider Hijacking		Redundant Access						
		Startup Items		Regsvcs/Regasm						
		System Firmware		Regsvr32						
		Systemd Service		Rootkit						
		Time Providers		Rundll32						
		Trap		Scripting						
		Valid Accounts		Signed Binary Proxy Execution						
		Web Shell		Signed Script Proxy Execution						
		Windows Management Instrumentation Event Subscription		SIP and Trust Provider Hijacking						
		Winlogon Helper DLL		Software Packing						
				Space after Filename						
				Template Injection						
				Timestomp						
				Trusted Developer Utilities						
				Valid Accounts						
				Virtualization/Sandbox Evasion						
				Web Service						
				XSL Script Processing						

SysMon Modular

https://github.com/olafhartong/sysmon-modular

A repository of sysmon configuration modules

Olaf Hartong

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	Accessibility Features	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	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	AppInit 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	Application Shimming	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	Bypass User Account Control	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	DLL Search Order Hijacking	Component Firmware	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Permission Groups Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Kerberoasting	Process Discovery	Replication Through Removable Media	Input Capture		Multi-hop Proxy
	Mshta	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning	Query Registry	Shared Webroot	Man in the Browser		Multi-Stage Channels
	PowerShell	Create Account	Image File Execution Options Injection	Disabling Security Tools	Network Sniffing	Remote System Discovery	Taint Shared Content	Screen Capture		Multiband Communication
	Regsvcs/Regasm	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Password Filter DLL	Security Software Discovery	Third-party Software	Video Capture		Multilayer Encryption
	Regsvr32	External Remote Services	Path Interception	DLL Side-Loading	Private Keys	System Information Discovery	Windows Admin Shares			Remote Access Tools
	Rundll32	File System Permissions Weakness	Port Monitors	Exploitation for Defense Evasion	Replication Through Removable Media	System Network Configuration Discovery	Windows Remote Management			Remote File Copy
	Scheduled Task	Hidden Files and Directories	Process Injection	Extra Window Memory Injection	Two-Factor Authentication Interception	System Network Connections Discovery				Standard Application Layer Protocol
	Scripting	Hooking	Scheduled Task	File Deletion		System Owner/User Discovery				Standard Cryptographic Protocol
	Service Execution	Hypervisor	Service Registry Permissions Weakness	File System Logical Offsets		System Service Discovery				Standard Non-Application Layer Protocol
	Signed Binary Proxy Execution	Image File Execution Options Injection	SID-History Injection	Hidden Files and Directories		System Time Discovery				Uncommonly Used Port
	Signed Script Proxy Execution	Logon Scripts	Valid Accounts	Image File Execution Options Injection						Web Service
	Third-party Software	LSASS Driver	Web Shell	Indicator Blocking						
	Trusted Developer Utilities	Modify Existing Service		Indicator Removal from Tools						
	User Execution	Netsh Helper DLL		Indicator Removal on Host						
	Windows Management Instrumentation	New Service		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		Mshta						
		Scheduled Task		Network Share Connection Removal						
		Screensaver		NTFS File Attributes						
		Security Support Provider		Obfuscated Files or Information						
		Service Registry Permissions Weakness		Process Doppelgänging						
		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						

ATT&CK™

SECTOR
Security Education Conference

OSQuery-attck

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

Mapping the MITRE ATT&CK Matrix with Osquery

Filippo Mottini

ATT&CK™

SECTOR
Security Education Conference

OS

Windows ATT&CK MAPPING

- **windows-registry-monitoring.conf**
  - ATT&CK: T1015,T1138,T1131,T1037,T1128,T1060,T1180,T1004,T1058,T1103,T1112
- **windows-incorrect_parent_process.conf**
  - ATT&CK: T1173,T1086,T1204,T1183
- **windows_powershell_events.conf**
  - ATT&CK: T1086,T1064
- **windows_system_running_processes.conf**
  - ATT&CK: T1034,T1121,T1117,T1085
- **windows_persistence-startup_items.conf**
  - ATT&CK: T1060
- **windows_service-persistence.conf**
  - ATT&CK: T1050
- **windows_critical_service_status.conf**
  - ATT&CK: T1089
- **windows_scheduled_tasks.conf**
  - ATT&CK: T1053
- **network_connection_listening.conf**
  - ATT&CK: T1086,T1093,T1020,T1041,T1011,T1029,T1043,T1090,T1094,T1024,T1008,T1219,T1105,T1065
- **windows_anomaly_process-execution.conf**
  - ATT&CK: T1191,T1118,T1059,T1170,T1086,T1117,T1053,T1035,T1197,T1128,T1134,T1126,T1087,T1201,T1069,T1057,T1012,T1018,T1063,T1082,T1049,T1007,T1124,T1076
- **windows_generic_detection.conf**
  - ATT&CK: T1136,T1078,T1116,T1075,T1097
- **windows_browsere-extensions.conf**
  - ATT&CK: T1176
- **windows_new_dir_relevant_infection_path.conf**
  - ATT&CK: T1034,T1074,T1044,T1060,T1023
- **windows_new_file_relevant_infection_path.conf**
  - ATT&CK: T1034,T1074,T1044,T1060,T1023

Olaf Hartong's ThreatHunting

https://github.com/olafhartong/ThreatHunting

A Splunk app mapped to MITRE ATT&CK to guide your threat hunts

Olaf Hartong

ATT&CK™

SECTOR
Security Education Conference

Olaf Hartong's ThreatHunting

```
[[T1070] Indicator Removal on Host]
action.email.useNSSubject = 1
action.summary_index = 1
action.summary_index._name = threathunting
action.summary_index.mitre_category = Defense_Evasion
action.summary_index.mitre_technique = Indicator Removal on Host
action.summary_index.mitre_technique_id = T1070
alert.track = 0
cron_schedule = */15 * * * *
dispatch.earliest_time = -15m@m
dispatch.latest_time = now
enableSched = 1
request.ui_dispatch_app = ThreatHunting
request.ui_dispatch_view = search
search = `sysmon` event_id=1 (process_name="wevtutil.exe" OR process_command_line="*wevtutil* cl*")\
| eval mitre_technique_id="T1070" \
| eval hash_sha256= lower(hash_sha256)\
| `process_create_whitelist`\
| table _time event_description hash_sha256 host_fqdn user_name process_path process_guid process_parent_
```

ATT&CK™

SECTOR
Security Education Conference

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	27 items	42 items	21 items	53 items	15 items	20 items	15 items	13 items	9 items	19 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	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Custom Command and Control Protocol
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Data Transfer Size Limits	Custom Cryptographic Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Exfiltration Over Alternative Protocol	Data Encoding
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Obfuscation
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Other Network Medium	Domain Fronting
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Password Policy Discovery	Remote File Copy	Data Staged	Exfiltration Over Physical Medium	Fallback Channels
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Email Collection	Scheduled Transfer	Multi-hop Proxy
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Kerberoasting	Permission Groups Discovery	Replication Through Removable Media	Input Capture		Multi-Stage Channels
	LSASS Driver	Component Firmware	Hooking	DCShadow	LLMNR/NBT-NS Poisoning	Process Discovery	Shared Webroot	Man in the Browser		Multiband Communication
	Mshta	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Network Sniffing	Query Registry	Taint Shared Content	Screen Capture		Multilayer Encryption
	PowerShell	Create Account	New Service	Disabling Security Tools	Password Filter DLL	Remote System Discovery	Third-party Software	Video Capture		Remote Access Tools
	Regsvcs/Regasm	DLL Search Order Hijacking	Path Interception	DLL Search Order Hijacking	Private Keys	Security Software Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	External Remote Services	Port Monitors	DLL Side-Loading	Two-Factor Authentication Interception	System Information Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	File System Permissions Weakness	Process Injection	Exploitation for Defense Evasion		System Network Configuration Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hidden Files and Directories	Scheduled Task	Extra Window Memory Injection		System Network Connections Discovery				Standard Non-Application Layer Protocol
	Scripting	Hooking	Service Registry Permissions Weakness	File Deletion		System Owner/User Discovery				Uncommonly Used Port
	Service Execution	Hypervisor	SID-History Injection	File Permissions Modification		System Service Discovery				Web Service
	Signed Binary Proxy Execution	Image File Execution Options Injection	Valid Accounts	File System Logical Offsets		System Time Discovery				
	Signed Script Proxy Execution	Logon Scripts	Web Shell	Hidden Files and Directories						
	Third-party Software	LSASS Driver		Image File Execution Options Injection						
	Trusted Developer Utilities	Modify Existing Service		Indicator Blocking						
	User Execution	Netsh Helper DLL		Indicator Removal from Tools						
	Windows Management Instrumentation	New Service		Indicator Removal on Host						
	Windows Remote Management	Office Application Startup		Indirect Command Execution						
	XSL Script Processing	Path Interception		Install Root Certificate						
		Port Monitors		InstallUtil						
		Redundant Access		Masquerading						
		Registry Run Keys / Startup Folder		Modify Registry						
		Scheduled Task		Mshta						
		Screensaver		Network Share Connection Removal						
		Security Support Provider		NTFS File Attributes						
		Service Registry Permissions Weakness		Obfuscated Files or Information						
		Shortcut Modification		Process Doppelgänging						
		SIP and Trust Provider Hijacking		Process Hollowing						
		System Firmware		Process Injection						
		Time Providers		Redundant Access						
		Valid Accounts		Regsvcs/Regasm						
		Web Shell		Regsvr32						
		Windows Management Instrumentation Event Subscription		Rootkit						
		Winlogon Helper DLL		Rundll32						
				Scripting						
				Signed Binary Proxy Execution						
				Signed Script Proxy Execution						
				SIP and Trust Provider Hijacking						
				Software Packing						
				Template Injection						
				Timestomp						
				Trusted Developer Utilities						
				Valid Accounts						
				Web Service						
				XSL Script Processing						

ATT&CK™

SECTOR
Security Education Conference

Atomic Red Team

https://github.com/redcanaryco/atomic-red-team

Small and highly portable detection tests based on MITRE's ATT&CK.

Red Canary

Slack : https://slack.atomicredteam.io/

Atomic Friday's : https://bit.ly/2VpNRVT

ATT&CK™

SECTOR
Security Education Conference

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	33 items	59 items	28 items	67 items	19 items	22 items	17 items	13 items	22 items	9 items	14 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass							
	Source	Launch Daemon	Sudo	Group Policy Modification							
	Space after Filename	Launchctl	Sudo Caching	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Users							
	Trap	Local Job Scheduling	Web Shell	Hidden Window							
	Trusted Developer Utilities	Login Item		HISTCONTROL							
	User Execution	Logon Scripts		Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver		Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchctl							
		Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		Rc.common		Modify Registry							
		Re-opened Applications		Mshta							
		Redundant Access		Network Share Connection Removal							
		Registry Run Keys / Startup Folder		NTFS File Attributes							
		Scheduled Task		Obfuscated Files or Information							
		Screensaver		Plist Modification							
		Security Support Provider		Port Knocking							
		Service Registry Permissions Weakness		Process Doppelgänging							
		Setuid and Setgid		Process Hollowing							
		Shortcut Modification		Process Injection							
		SIP and Trust Provider Hijacking		Redundant Access							
		Startup Items		Regsvcs/Regasm							
		System Firmware		Regsvr32							
		Systemd Service		Rootkit							
		Time Providers		Rundll32							
		Trap		Scripting							
		Valid Accounts		Signed Binary Proxy Execution							
		Web Shell		Signed Script Proxy Execution							
		Windows Management Instrumentation Event Subscription		SIP and Trust Provider Hijacking							
		Winlogon Helper DLL		Software Packing							
				Space after Filename							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

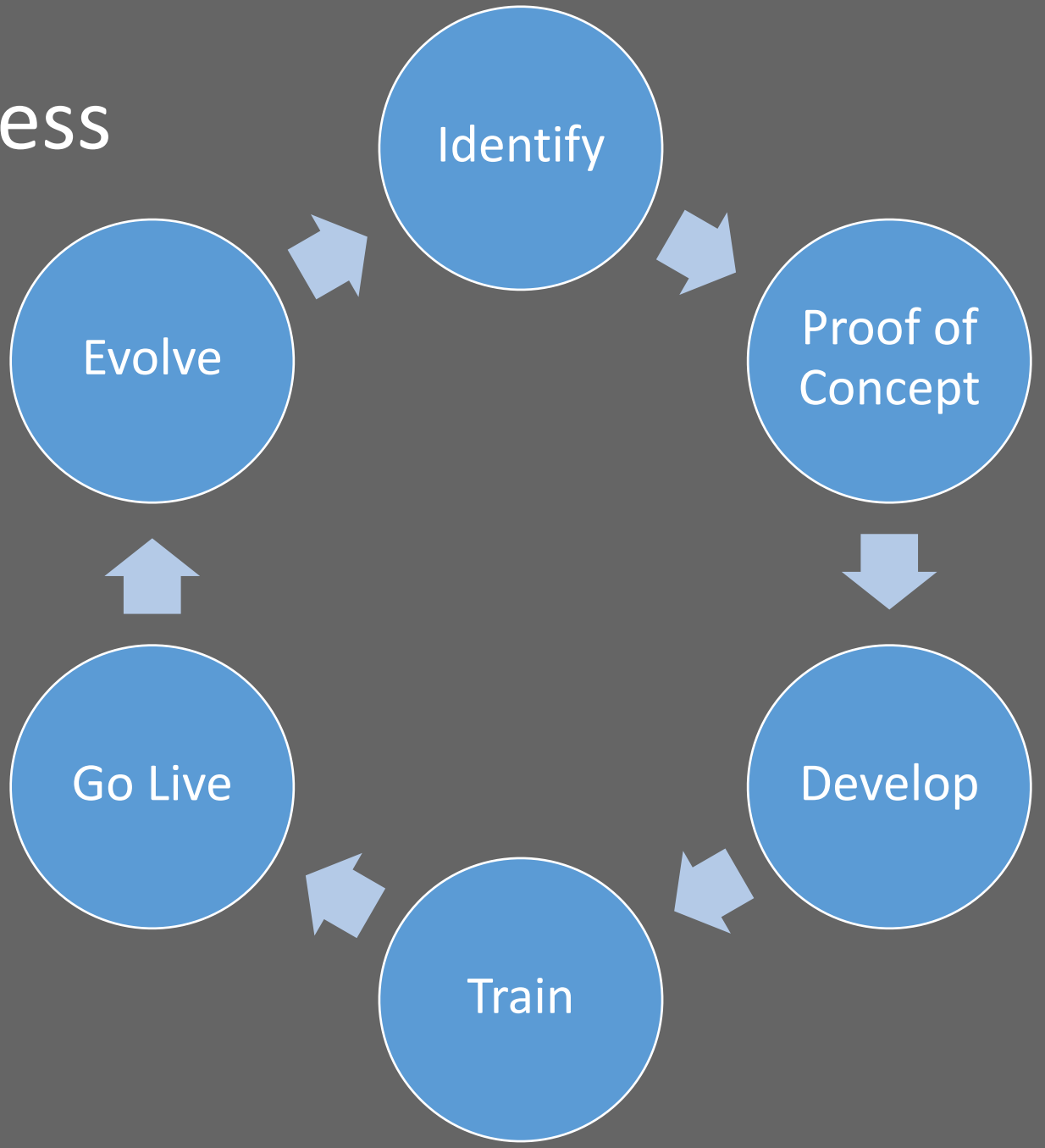
ATT&CK™

SECTOR
Security Education Conference

BUILDING DETECTION

ATT&CK™

The Process



ATT&CK™

SECTOR

T1170 - MSHTA

2. Search for “mshta” in our logs

   No hits

3. Build Alerting Pipeline (Easy content)
2. Built training on how MSHTA can be used by adversaries
3. Put detection in production
4. To date, zero false positive

ATT&CK™

SECTOR

T1197 - BITS Jobs

2. Search for “bitsadmin” and “Start-BitsTransfer” in our logs

   Few hits on all end points

   i. Research

   Process Creation (Sysmon ID: 1)

   bitsadmin.exe /transfer /Dowr /priority

   ii. File creation (Sysmon ID: 11)

   BITXXX.tmp

   “C:\Windows\SoftwareDistribution\Download\”

   Windows Update

T1197 - BITS Admin

3. Build Alerting Pipeline
4. Built training on why BITS Admin is important
5. Put detection in production
6. To date, zero false positive

T1085 - Rundll32

2. Search for “rundll32” in our logs
   Gazillions of hits
3. Build Alerting Pipeline (Whitelisting for months)
4. Built training on why Rundll32 is important
5. Put detection in production
6. Keep on generating FP
   Solution : Dashboard that is reviewed weekly

CONCLUSION

ATT&CK™

Key Takeaways

ATT&CK address the highest level of the PoP

Perform a Preliminary Assessment of all Techniques

- Choose the right questions
- Define scores
- Track in Enterprise-Navigator
- https://mitre-attack.github.io/attack-navigator/enterprise/

Use Open Source Projects to improve coverage

Don’t confuse Alerting and Hunting

When there is too many FP, use dashboards

Stop, Drop and Assess Your SOC

- https://youtu.be/SMKVkpzGhOs

Call For Action

Red Teams share their tools

Bloodhound	Silent Trinity	Mimikatz
SET	Metasploit	Responder

Why aren't more Blue Teams that share?

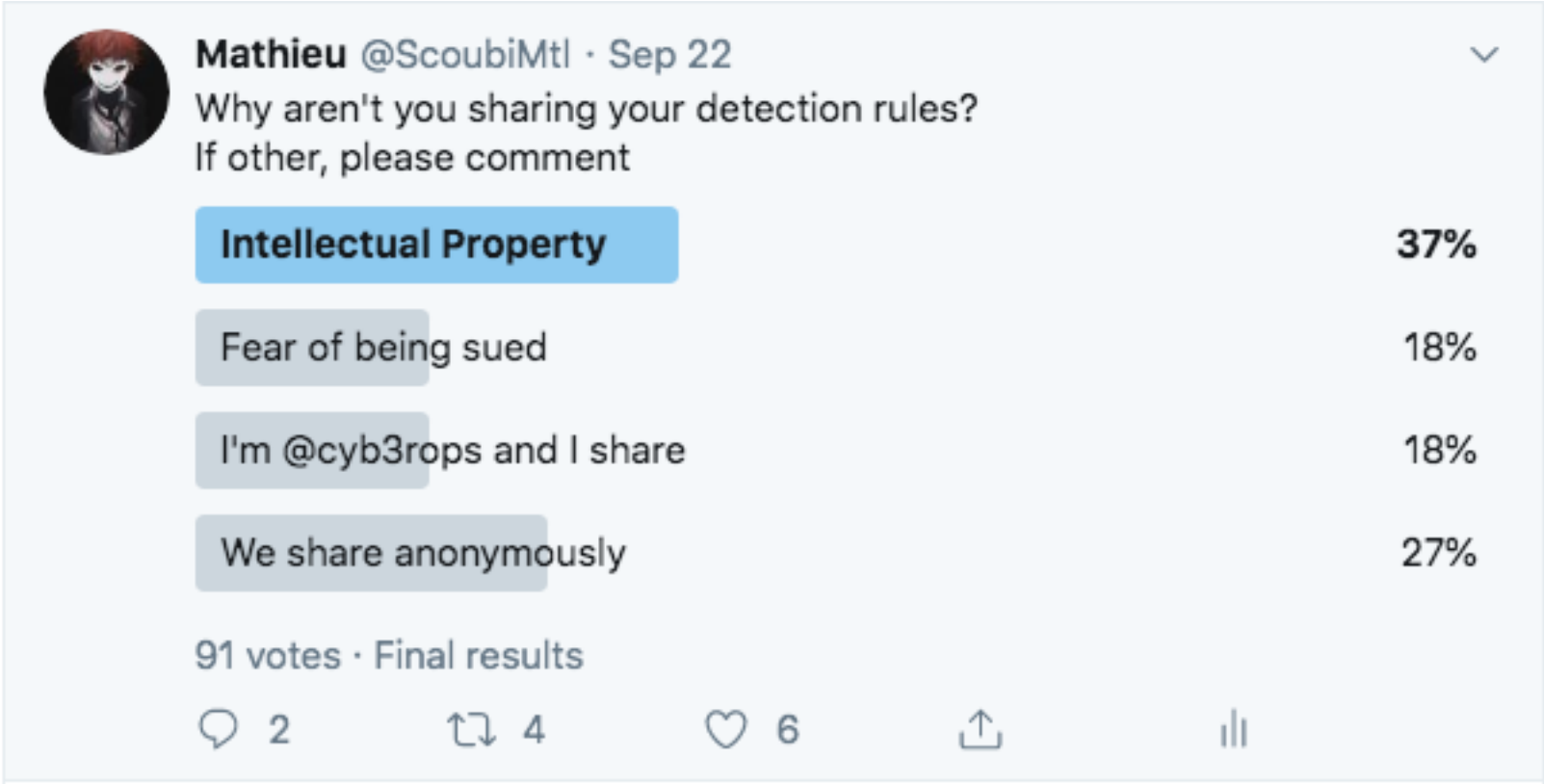
Sigma	ART
ATT&CK	ADS

Share via anonymous blogs

Create anonymous Github

Share to the Sigma project

Create a Slack Group to exchange


Mathieu @ScoubiMtl · Sep 22
Why aren't you sharing your detection rules?
If other, please comment
Intellectual Property
37%
Fear of being sued
18%
I'm @cyb3rops and I share
18%
We share anonymously
27%
91 votes · Final results
2
4
6

Call For Action

Red Teamers Thanks For :

- All of your research
- Trade craft
- Tools

But Please :

- Give something to the Blue Team
- What do we need to get visibility on this
- How can we detect this

Thanks @mattifestation

http://ig2.me/DL

ATT&CK™

SECTOR
Security Education Conference

Thank You

@Grifter801, @PyroTek3, @danielhbohannon

@cyb3rops, @olafhartong, Filippo Mottini, @redcanaryco

@MITREcorp, @MITREattack

My former team, @SecTorCa

ATT&CK™

SECTOR
Security Education Conference

Slides

https://www.slideshare.net/28Z4dWveWKYcFu

customink.com/fundraising/bloodhound-swag
https://t.co/oO3SRNnAnU

@ScoubiMtl

ATT&CK™

SECTOR
Security Education Conference