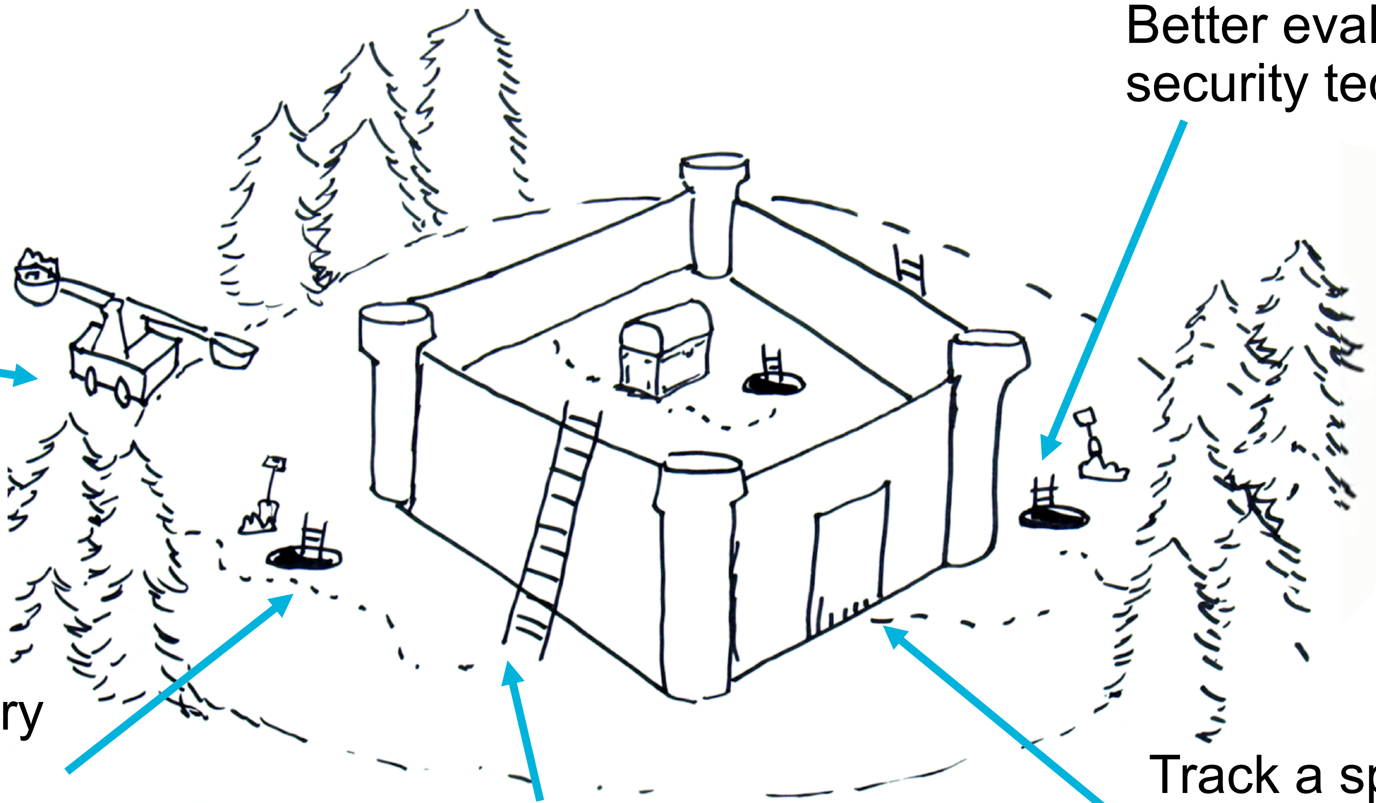
ATT&CK™ in 15 minutes

Richard Struse
Chief Strategist, Cyber Threat Intelligence

© 2018 The MITRE Corporation. All rights reserved. Approved for Public Release - Case # 17-4500-7

Cybersecurity should be *threat-informed*

Knowledge of my adversary can help me…



Prioritize detection/mitigation of heavily used techniques

Better evaluate new security technologies

Conduct adversary emulation (e.g. red-teaming)

Perform gap analysis of current defenses

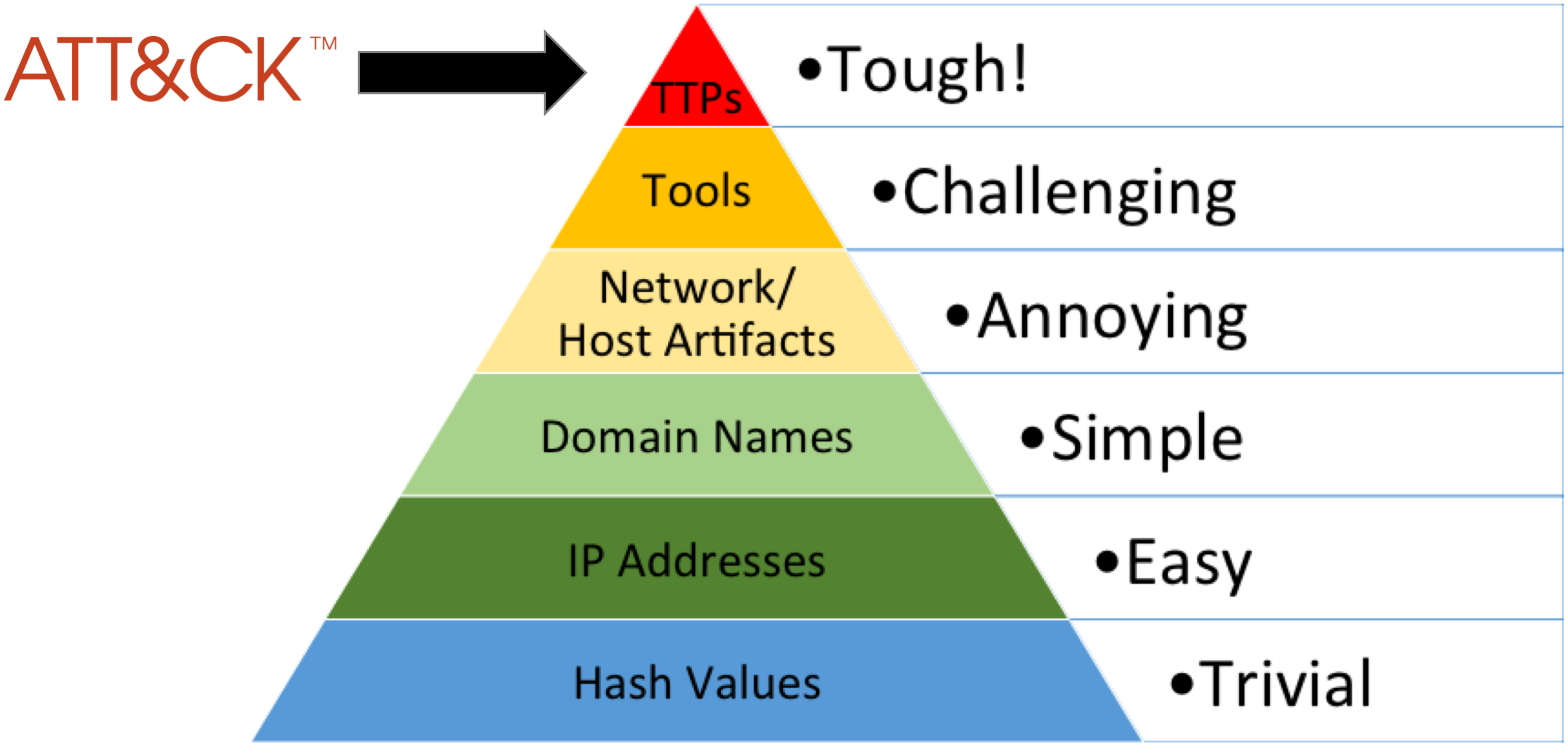
Track a specific adversary's set of techniques

© 2018 The MITRE Corporation. All rights reserved. Approved for Public Release - Case # 17-4500-7

Bianco’s Pyramid of ^ Pain

adversary

Difficulty/cost for the adversary to modify their attacks



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

© 2018 The MITRE Corporation. All rights reserved. Approved for Public Release - Case # 17-4500-7

ATT&CK™

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

ATT&CK™ is increasingly being used by the community as a common way to describe adversary behavior.

attack.mitre.org

© 2018 The MITRE Corporation. All rights reserved. Approved for Public Release - Case # 17-4500-7

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command & Control
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Audio Capture	Automated Exfiltration	Commonly Used Port
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Automated Collection	Data Compressed	Communication Through Removable Media
Accessibility Features		Binary Padding			Application Deployment Software	Command-Line	Clipboard Data	Data Encrypted	
AppInit DLLs		Code Signing	Credential Manipulation	File and Directory Discovery		Execution through API	Data Staged	Data Transfer Size Limits	Connection Proxy
Local Port Monitor		Component Firmware			Exploitation of Vulnerability	Execution through Module Load	Data from Local System	Exfiltration Over Alternative Protocol	Custom Command and Control Protocol
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery			Data from Network Shared Drive		
Path Interception		Disabling Security Tools	Input Capture		Logon Scripts	Graphical User Interface		Exfiltration Over Command and Control Channel	Custom Cryptographic Protocol
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Discovery	Pass the Hash	InstallUtil	Data from Removable Media		
File System Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception		Pass the Ticket	MSBuild			Data Encoding
Service Registry Permissions Weakness				Network Service Scanning	Remote Desktop Protocol	PowerShell	Email Collection	Exfiltration Over Other Network Medium	Data Obfuscation
Web Shell		Indicator Blocking		Peripheral Device Discovery	Remote File Copy	Process Hollowing	Input Capture		Fallback Channels
Authentication Package	Exploitation of Vulnerability				Remote Services	Regsvcs/Regasm	Screen Capture	Exfiltration Over Physical Medium	Multi-Stage Channels
	Bypass User Account Control			Permission Groups Discovery	Replication Through Removable Media	Regsvr32	Video Capture		
Bootkit	DLL Injection					Rundll32		Scheduled Transfer	Multiband Communication
Component Object Model Hijacking		Component Object Model Hijacking		Process Discovery	Shared Webroot	Scheduled Task			Multilayer Encryption
Basic Input/Output System		Indicator Removal from Tools		Query Registry	Taint Shared Content	Scripting			Remote File Copy
				Remote System Discovery	Windows Admin Shares	Service Execution			Standard Application Layer Protocol
Change Default File Association		Indicator Removal on Host		Security Software Discovery		Windows Management Instrumentation			Standard Cryptographic Protocol
Component Firmware		Install Root Certificate		System Information Discovery					
External Remote Services		InstallUtil							Standard Non-Application Layer Protocol
Hypervisor		Masquerading							
Logon Scripts		Modify Registry		System Owner/User Discovery					
Modify Existing Service		MSBuild							Uncommonly Used Port
Netsh Helper DLL		Network Share Removal		System Service Discovery					Web Service
Redundant Access		NTFS Extended Attributes		System Time Discovery					
Registry Run Keys / Start Folder		Obfuscated Files or Information							
Security Support Provider		Process Hollowing							
Shortcut Modification		Redundant Access							
Windows Management Instrumentation Event Subscription		Regsvcs/Regasm							
		Regsvr32							
		Rootkit							
Winlogon Helper DLL		Rundll32							
		Scripting							
		Software Packing							
		Timestomp							

Tactic: **Adversary's technical goal**

***Technique*: How adversary achieves the goal**

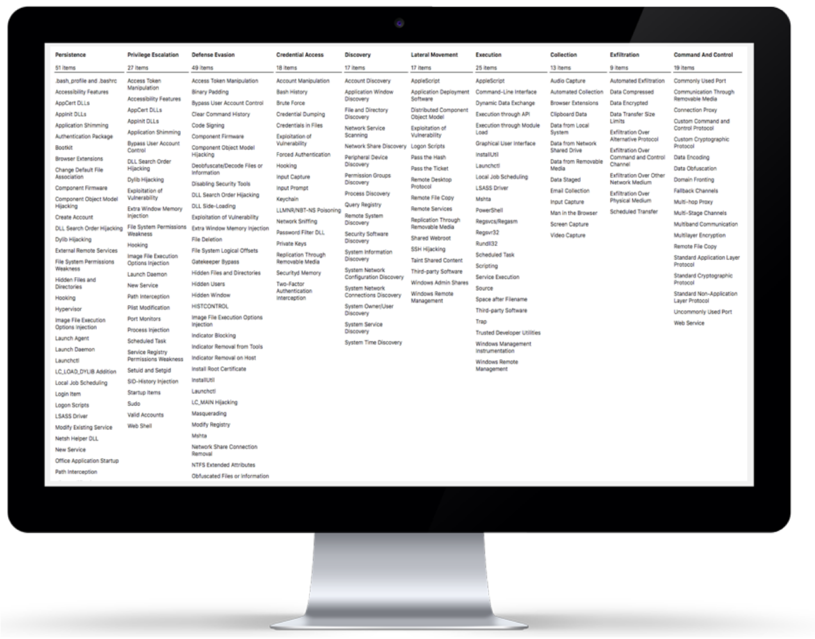
© 2018 The MITRE Corporation. All rights reserved. Approved for Public Release - Case #17-4500-7

Example of 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.
- **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
  - Tools such as Sysinternals Autoruns may be used to detect system changes that could be attempts at persistence
  - Monitor processes and command-line arguments for actions that could create services
- **Mitigation:**
  - Limit privileges of user accounts and remediate Privilege Escalation vectors
  - Identify and block unnecessary system utilities or potentially malicious software that may be used to create services
- **Data Sources:** Windows Registry, process monitoring, command-line parameters
- **Examples:** *Carbanak*, *Lazarus Group*, TinyZBot, Duqu, CozyCar, CosmicDuke, hcdLoader, …

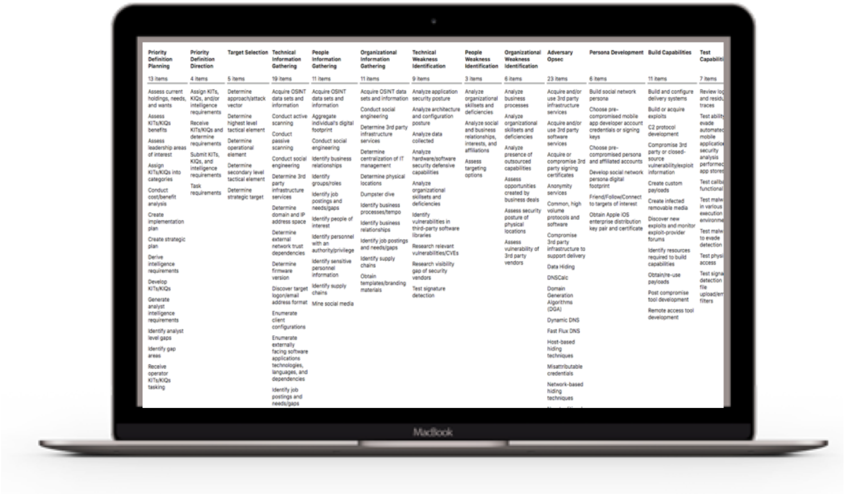
© 2018 The MITRE Corporation. All rights reserved. Approved for Public Release - Case # 17-4500-7

ATT&CK Spans Multiple Technology Domains



Enterprise: Windows, Linux, Mac

Mobile: Android, iOS

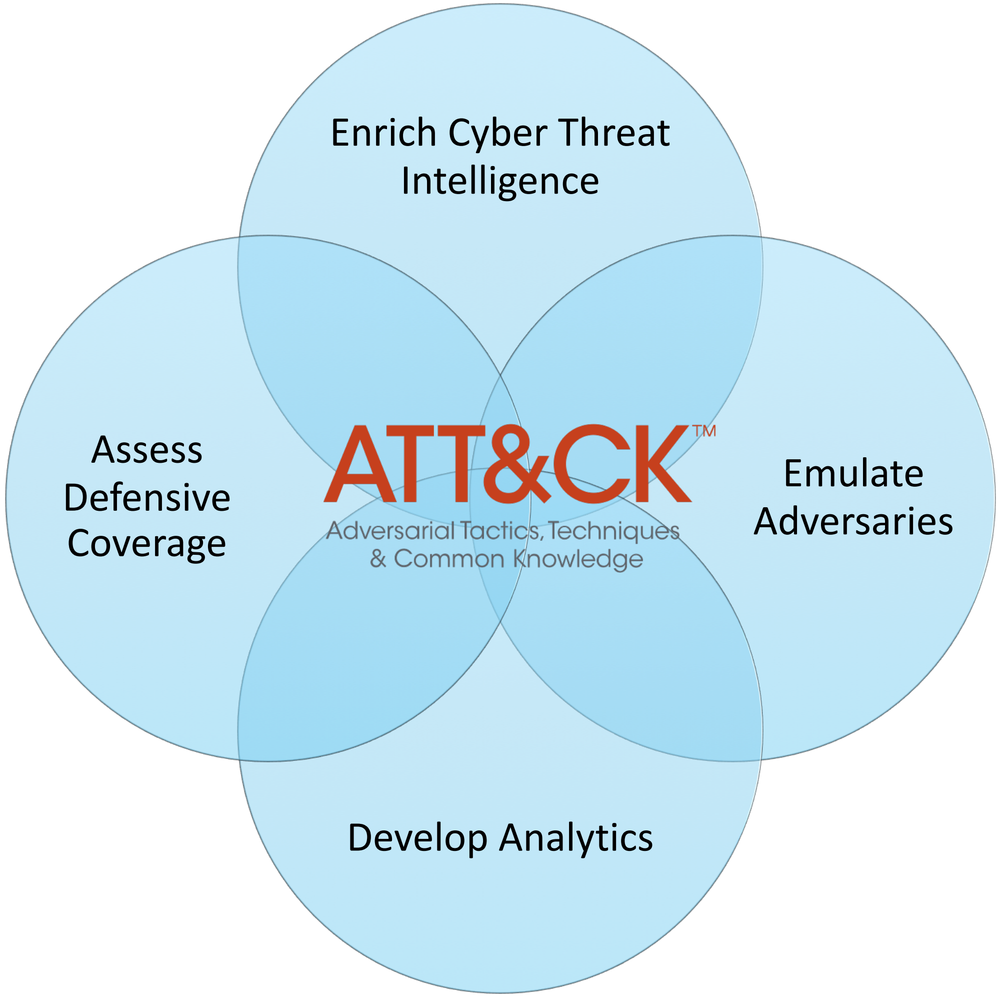


PRE-ATT&CK: left of exploit behaviors

© 2018 The MITRE Corporation. All rights reserved. Approved for Public Release - Case # 17-4500-7

Key use cases…

- **Guide threat hunting campaigns**
- **Emulate adversaries to measure defenses against relevant threats**
- **Leverage *threat intelligence* to prioritize technique detection**
- **Remediate gaps by mapping solutions back to ATT&CK techniques**


Enrich Cyber Threat Intelligence
Assess Defensive Coverage
ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge
Emulate Adversaries
Develop Analytics

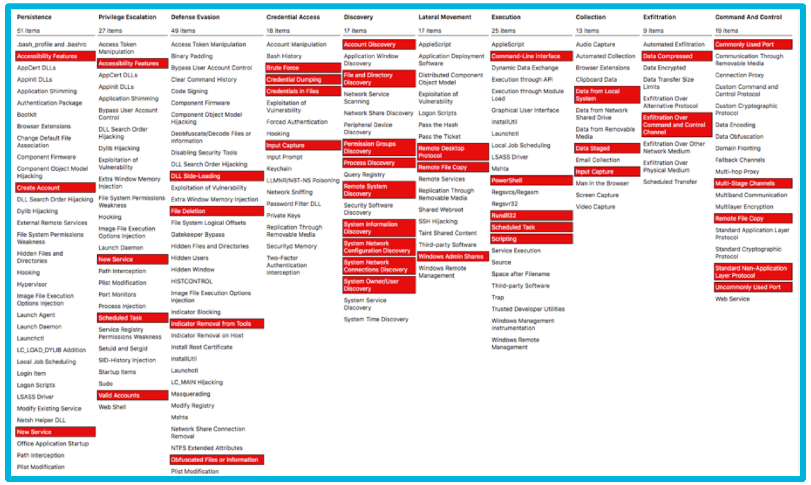
© 2018 The MITRE Corporation. All rights reserved. Approved for Public Release - Case # 17-4500-7

ATT&CK can help you…

Develop Analytics

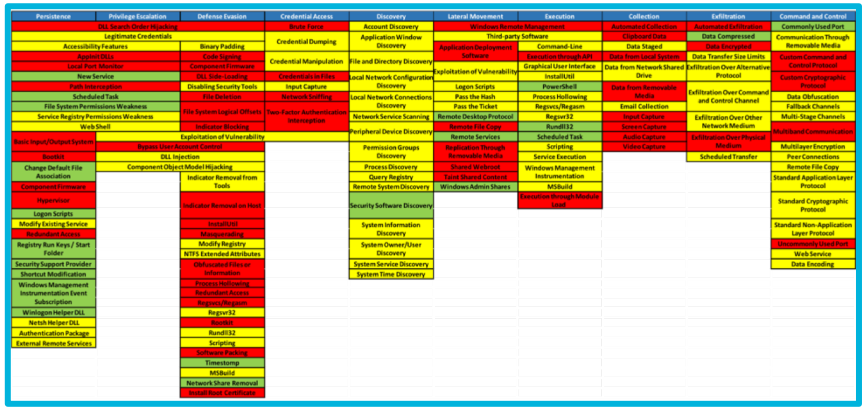
```
processes = search Process:Create
reg = filter processes where (exe == "reg.exe" and parent_exe
== "cmd.exe")
cmd = filter processes where (exe == "cmd.exe" and
parent_exe != "explorer.exe"")
reg_and_cmd = join (reg, cmd) where (reg.ppid == cmd.pid and
reg.hostname == cmd.hostname)
output reg_and_cmd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

See The Threat



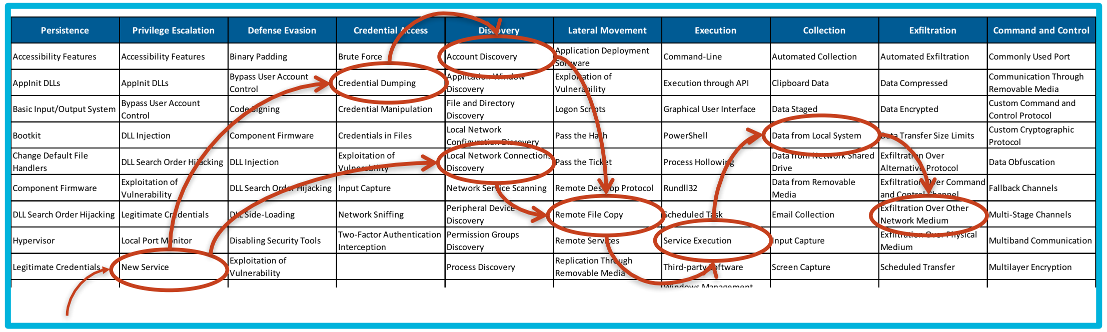
Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command And Control
51 items	27 items	49 items	18 items	17 items	17 items	25 items	13 items	9 items	19 items
.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Data Compressed	Communication Through Removable Media
AppCert DLLs	AppCert DLLs	Bypass User Account Control	Brute Force	File and Directory Discovery	Distributed Component Object Model	Dynamic Data Exchange	Browser Extensions	Data Encrypted	Connection Proxy
AppInit DLLs	AppInit DLLs	Clear Command History	Credential Dumping	Network Service Scanning	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Transfer Size Limits	Custom Command and Control Protocol
Application Shimming	Application Shimming	Code Signing	Credentials in Files	Network Share Discovery	Logon Scripts	Execution through Module Load	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Authentication Package	Bypass User Account Control	Component Firmware	Exploitation of Vulnerability	Peripheral Device Discovery	Pass the Hash	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Bootkit	DLL Search Order Hijacking	Component Object Model Hijacking	Forced Authentication	Permission Groups Discovery	Pass the Ticket	InstallUtil	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Browser Extensions	Dylib Hijacking	Deobfuscate/Decode Files or Information	Hooking	Process Discovery	Remote Desktop Protocol	Launchctl	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Change Default File Association	Exploitation of Vulnerability	Disabling Security Tools	Input Capture	Query Registry	Remote File Copy	Local Job Scheduling	Email Collection	Scheduled Transfer	Fallback Channels
Component Firmware	Extra Window Memory Injection	DLL Search Order Hijacking	Input Prompt	Remote System Discovery	Remote Services	LSASS Driver	Input Capture		Multi-hop Proxy
Component Object Model Hijacking	File System Permissions Weakness	DLL Side-Loading	Keychain	Security Software Discovery	Replication Through Removable Media	Mshta	Man in the Browser		Multi-Stage Channels
Create Account	Hooking	Exploitation of Vulnerability	LLMNR/NBT-NS Poisoning	System Information Discovery	Shared Webroot	PowerShell	Screen Capture		Multiband Communication
DLL Search Order Hijacking	Image File Execution Options Injection	Extra Window Memory Injection	Network Sniffing	System Network Configuration Discovery	SSH Hijacking	Regsvcs/Regasm	Video Capture		Multilayer Encryption
Dylib Hijacking	Launch Daemon	File Deletion	Password Filter DLL	System Network Connections Discovery	Taint Shared Content	Regsvr32			Remote File Copy
External Remote Services	New Service	File System Logical Offsets	Private Keys	System Owner/User Discovery	Third-party Software	Rundll32			Standard Application Layer Protocol
File System Permissions Weakness	Path Interception	Gatekeeper Bypass	Replication Through Removable Media	System Service Discovery	Windows Admin Shares	Scheduled Task			Standard Cryptographic Protocol
Hidden Files and Directories	Plist Modification	Hidden Files and Directories	Securityd Memory	System Time Discovery	Windows Remote Management	Scripting			Standard Non-Application Layer Protocol
Hooking	Port Monitors	Hidden Users	Two-Factor Authentication Interception			Service Execution			Uncommonly Used Port
Hypervisor	Process Injection	Hidden Window				Source			Web Service
Image File Execution Options Injection	Scheduled Task	HISTCONTROL				Space after Filename			
Launch Agent	Service Registry Permissions Weakness	Image File Execution Options Injection				Third-party Software			
Launch Daemon	Setuid and Setgid	Indicator Blocking				Trap			
Launchctl	SID-History Injection	Indicator Removal from Tools				Trusted Developer Utilities			
LC_LOAD_DYLIB Addition	Startup Items	Indicator Removal on Host				Windows Management Instrumentation			
Local Job Scheduling	Sudo	Install Root Certificate				Windows Remote Management			
Login Item	Valid Accounts	InstallUtil							
Logon Scripts	Web Shell	Launchctl							
LSASS Driver		LC_MAIN Hijacking							
Modify Existing Service		Masquerading							
Netsh Helper DLL		Modify Registry							
New Service		Mshta							
Office Application Startup		Network Share Connection Removal							
Path Interception		NTFS Extended Attributes							
Plist Modification		Obfuscated Files or Information							
		Plist Modification							

Assess Your Defenses



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking	DLL Search Order Hijacking	DLL Search Order Hijacking	Brute Force	Account Discovery	Windows Remote Management	Windows Remote Management	Automated Collection	Automated Exfiltration	Commonly Used Port
Legitimate Credentials	Legitimate Credentials	Legitimate Credentials	Credential Dumping	Application Window Discovery	Third-party Software	Third-party Software	Clipboard Data	Data Compressed	Communication Through Removable Media
Accessibility Features	Accessibility Features	Binary Padding	Credential Manipulation	File and Directory Discovery	Application Deployment Software	Command-Line	Data Staged	Data Encrypted	Custom Command and Control Protocol
AppInit DLLs	AppInit DLLs	Code Signing	Credentials in Files	Local Network Configuration Discovery	Exploitation of Vulnerability	Execution through API	Data from Local System	Data Transfer Size Limits	Custom Cryptographic Protocol
Local Port Monitor	Local Port Monitor	Component Firmware	Input Capture	Local Network Connections Discovery	Logon Scripts	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Data Obfuscation
New Service	New Service	DLL Side-Loading	Network Sniffing	Network Service Scanning	Pass the Hash	InstallUtil	Data from Removable Media	Exfiltration Over Command and Control Channel	Fallback Channels
Path Interception	Path Interception	Disabling Security Tools	Two-Factor Authentication Interception	Peripheral Device Discovery	Pass the Ticket	PowerShell	Email Collection	Exfiltration Over Other Network Medium	Multi-Stage Channels
Scheduled Task	Scheduled Task	File Deletion	Exploitation of Vulnerability	Permission Groups Discovery	Remote Desktop Protocol	Process Hollowing	Input Capture	Exfiltration Over Physical Medium	Multiband Communication
File System Permissions Weakness	File System Permissions Weakness	File System Logical Offsets		Process Discovery	Remote File Copy	Regsvcs/Regasm	Screen Capture	Scheduled Transfer	Multilayer Encryption
Service Registry Permissions Weakness	Service Registry Permissions Weakness	Indicator Blocking		Query Registry	Remote Services	Regsvr32	Audio Capture		Peer Connections
Web Shell	Web Shell	Exploitation of Vulnerability		Remote System Discovery	Replication Through Removable Media	Rundll32	Video Capture		Remote File Copy
Basic Input/Output System	Exploitation of Vulnerability	Bypass User Account Control		Security Software Discovery	Shared Webroot	Scheduled Task			Standard Application Layer Protocol
Bootkit	Bypass User Account Control	DLL Injection		System Information Discovery	Taint Shared Content	Scripting			Standard Cryptographic Protocol
Change Default File Association	DLL Injection	Component Object Model Hijacking		System Owner/User Discovery	Windows Admin Shares	Service Execution			Standard Non-Application Layer Protocol
Component Firmware	Component Object Model Hijacking	Indicator Removal from Tools		System Service Discovery		Windows Management Instrumentation			Uncommonly Used Port
Hypervisor		Indicator Removal on Host		System Time Discovery		MSBuild			Web Service
Logon Scripts		InstallUtil				Execution through Module Load			Data Encoding
Modify Existing Service		Masquerading							
Redundant Access		Modify Registry							
Registry Run Keys / Start Folder		NTFS Extended Attributes							
Security Support Provider		Obfuscated Files or Information							
Shortcut Modification		Process Hollowing							
Windows Management Instrumentation Event Subscription		Redundant Access							
Winlogon Helper DLL		Regsvcs/Regasm							
Netsh Helper DLL		Regsvr32							
Authentication Package		Rootkit							
External Remote Services		Rundll32							
		Scripting							
		Software Packing							
		Timestomp							
		MSBuild							
		Network Share Removal							
		Install Root Certificate							

Emulate Adversaries



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line	Automated Collection	Automated Exfiltration	Commonly Used Port
AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Compressed	Communication Through Removable Media
Basic Input/Output System	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Graphical User Interface	Data Staged	Data Encrypted	Custom Command and Control Protocol
Bootkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	PowerShell	Data from Local System	Data Transfer Size Limits	Custom Cryptographic Protocol
Change Default File Handlers	DLL Search Order Hijacking	DLL Injection	Exploitation of Vulnerability	Local Network Connections Discovery	Pass the Ticket	Process Hollowing	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Data Obfuscation
Component Firmware	Exploitation of Vulnerability	DLL Search Order Hijacking	Input Capture	Network Service Scanning	Remote Desktop Protocol	Rundll32	Data from Removable Media	Exfiltration Over Command and Control Channel	Fallback Channels
DLL Search Order Hijacking	Legitimate Credentials	DLL Side-Loading	Network Sniffing	Peripheral Device Discovery	Remote File Copy	Scheduled Task	Email Collection	Exfiltration Over Other Network Medium	Multi-Stage Channels
Hypervisor	Local Port Monitor	Disabling Security Tools	Two-Factor Authentication Interception	Permission Groups Discovery	Remote Services	Service Execution	Input Capture	Exfiltration Over Physical Medium	Multiband Communication
Legitimate Credentials	New Service	Exploitation of Vulnerability		Process Discovery	Replication Through Removable Media	Third-party Software	Screen Capture	Scheduled Transfer	Multilayer Encryption
						Windows Management			

© 2018 The MITRE Corporation. All rights reserved. Approved for Public Release - Case # 17-4500-7

Some ATT&CK Resources

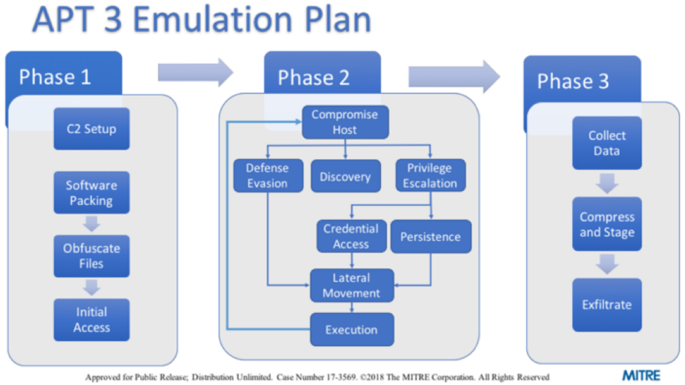
Public ATT&CK Knowledge Base

STIX™ TAXII™

Automated Adversary Emulation (Caldera)

Automated Blue Team Investigations (Cascade)

Adversary Emulation Plans



APT 3 Emulation Plan

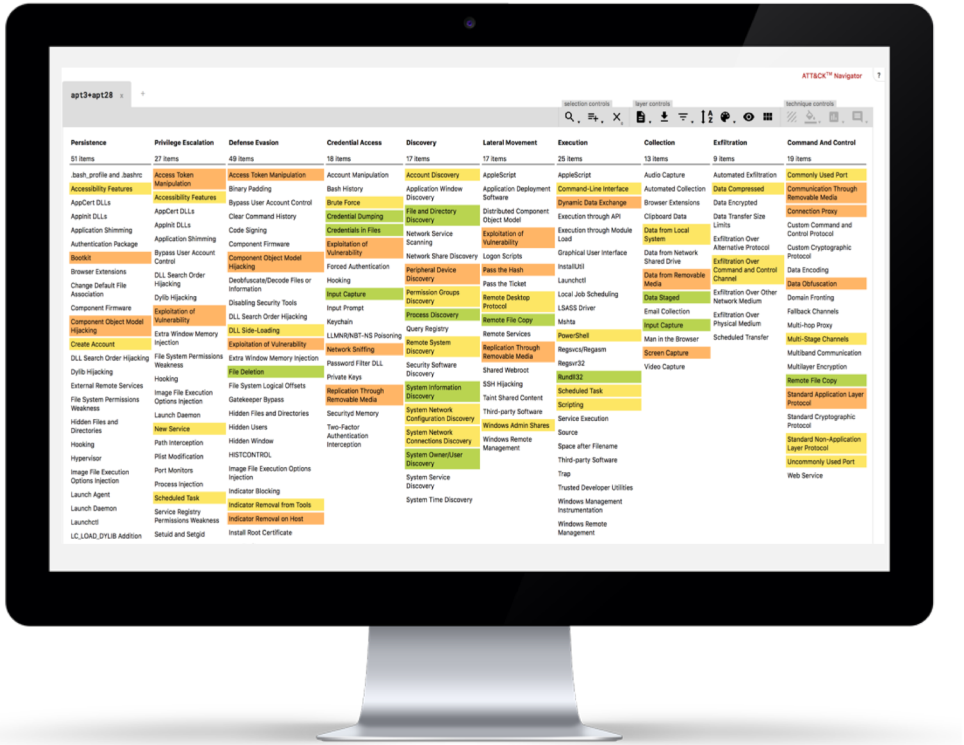
Phase 1
C2 Setup
Software Packing
Obfuscate Files
Initial Access

Phase 2
Compromise Host
Defense Evasion
Discovery
Privilege Escalation
Credential Access
Persistence
Lateral Movement
Execution

Phase 3
Collect Data
Compress and Stage
Exfiltrate

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

MITRE



Persistence
51 items
.bash_profile and .bashrc
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Authentication Package
Bootkit
Browser Extensions
Change Default File Association
Component Firmware
Component Object Model Hijacking
Create Account
DLL Search Order Hijacking
Dylib Hijacking
External Remote Services
File System Permissions Weakness
Hidden Files and Directories
Hooking
Hypervisor
Image File Execution Options Injection
Launch Agent
Launch Daemon
Launchctl
LC_LOAD_DYLIB Addition

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

Defense Evasion
49 items
Access Token Manipulation
Binary Padding
Bypass User Account Control
Clear Command History
Code Signing
Component Firmware
Component Object Model Hijacking
Deobfuscate/Decode Files or Information
Disabling Security Tools
DLL Search Order Hijacking
DLL Side-Loading
Exploitation of Vulnerability
Extra Window Memory Injection
File Deletion
File System Logical Offsets
Gatekeeper Bypass
Hidden Files and Directories
Hidden Users
Hidden Window
HISTCONTROL
Image File Execution Options Injection
Indicator Blocking
Indicator Removal from Tools
Indicator Removal on Host
Install Root Certificate

Credential Access
18 items
Account Manipulation
Bash History
Brute Force
Credential Dumping
Credentials in Files
Exploitation of Vulnerability
Forced Authentication
Hooking
Input Capture
Input Prompt
Keychain
LLMNR/NBT-NS Poisoning
Network Sniffing
Password Filter DLL
Private Keys
Replication Through Removable Media
Securityd Memory
Two-Factor Authentication Interception

Discovery
17 items
Account Discovery
Application Window Discovery
File and Directory Discovery
Network Service Scanning
Network Share 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

Lateral Movement
17 items
AppleScript
Application Deployment Software
Distributed Component Object Model
Exploitation of Vulnerability
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

Execution
25 items
AppleScript
Command-Line Interface
Dynamic Data Exchange
Execution through API
Execution through Module Load
Graphical User Interface
InstallUtil
Launchctl
Local Job Scheduling
LSASS Driver
Mshta
PowerShell
Regsvcs/Regasm
Regsvr32
Rundll32
Scheduled Task
Scripting
Service Execution
Source
Space after Filename
Third-party Software
Trap
Trusted Developer Utilities
Windows Management Instrumentation
Windows Remote Management

Collection
13 items
Audio Capture
Automated Collection
Browser Extensions
Clipboard Data
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Man in the Browser
Screen Capture
Video Capture

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

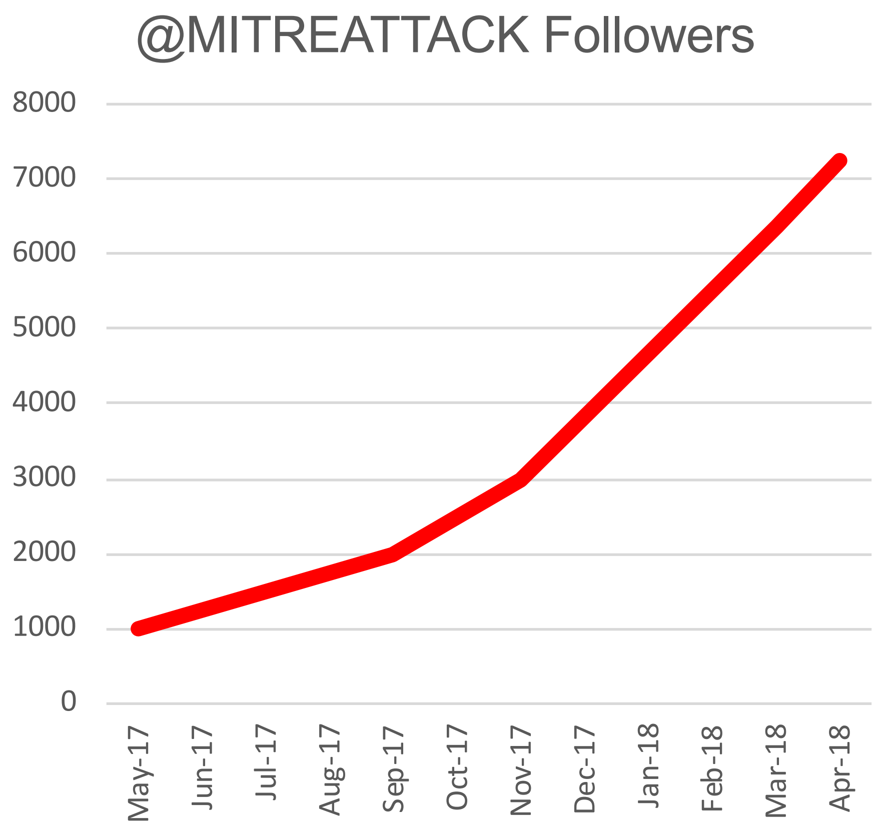
Command And Control
19 items
Commonly Used Port
Communication Through Removable Media
Connection Proxy
Custom Command and Control Protocol
Custom Cryptographic Protocol
Data Encoding
Data Obfuscation
Domain Fronting
Fallback Channels
Multi-hop Proxy
Multi-Stage Channels
Multiband Communication
Multilayer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

ATT&CK Navigator visualization tool

© 2018 The MITRE Corporation. All rights reserved. Approved for Public Release - Case # 17-4500-7

MITRE

ATT&CK: A Growing Community



- **Endgame** - links to ATT&CK within the Endgame platform.
- **Tripwire** – aligns reporting against ATT&CK
- **Cobalt Strike** - ATT&CK reporting
- **Palo Alto Networks** - ATT&CK-based adversary playbook viewer
- **AttackIQ** - organization of scenarios and tests to ATT&CK.
- **Red Canary** - Atomic Red Team use of ATT&CK
- **CERT Australia** – aligns threat reporting for CIKR to ATT&CK
- And many more…

© 2018 The MITRE Corporation. All rights reserved. Approved for Public Release - Case # 17-4500-7

What's next for ATT&CK?

Develop new technology domains (where appropriate)

Continue to expand the ATT&CK community

Open up the development and governance of ATT&CK

Invest in additional infrastructure to make ATT&CK easier to use

© 2018 The MITRE Corporation. All rights reserved. Approved for Public Release - Case # 17-4500-7

ATT&CK™

Questions?

attack.mitre.org

@MITREAttack

rjs@mitre.org

© 2018 The MITRE Corporation. All rights reserved. Approved for Public Release - Case # 17-4500-7