USING KNOWLEDGE OF ADVERSARY TTPs TO INFORM CYBER DEFENSE: MITRE'S ATT&CK™ FRAMEWORK

Richard Struse
Chief Strategist
Cyber Threat Intelligence

Approved for Public Release. Distribution unlimited. Case number 17-4500-1

MITRE

MITRE Was Established to Serve the Public Interest

established
1958

not-for-profit

conflict-free
environment

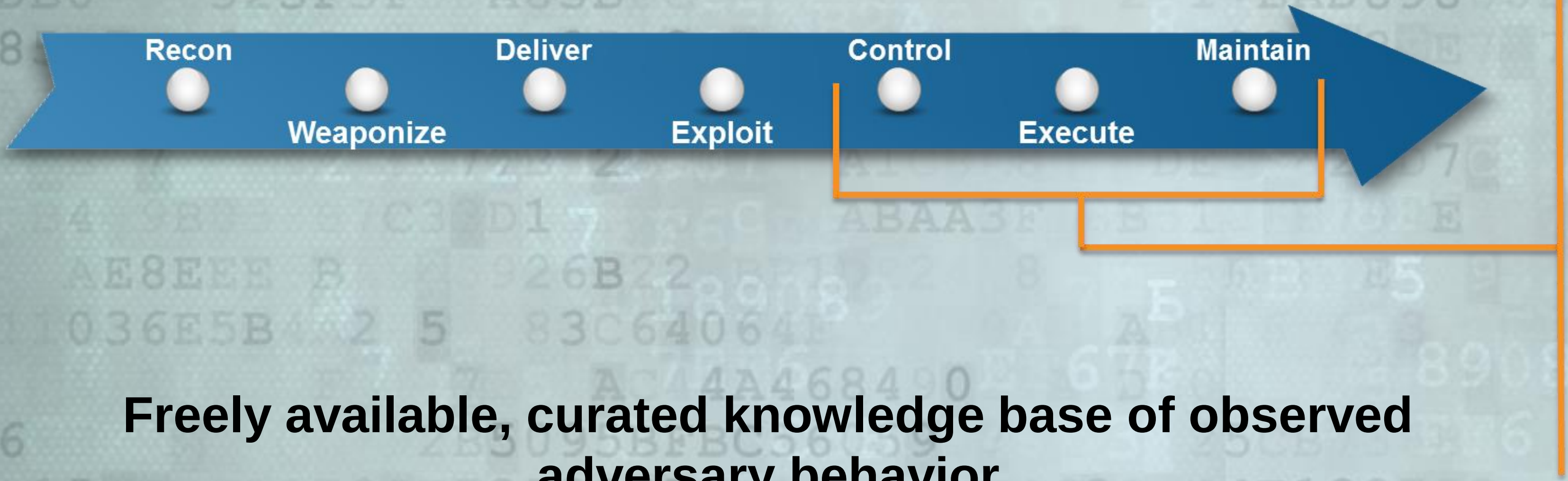
science **&**
technology

Part of the ecosystem of federal research centers

If I understood my adversary, I could…

- Perform gap analysis of my current defenses
- Prioritize detection/mitigation of heavily used techniques
- Track a specific adversary’s set of techniques
- Conduct adversary emulation (e.g. red-teaming)
- Better evaluate new security technologies

ATT&CK: Deconstructing the Lifecycle



- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Execution
- Collection
- Exfiltration
- Command and Control

Freely available, curated knowledge base of observed adversary behavior

Higher fidelity on right-of-exploit, post-access phases

Describes behavior sans adversary tools

Working with world-class researchers to improve and expand

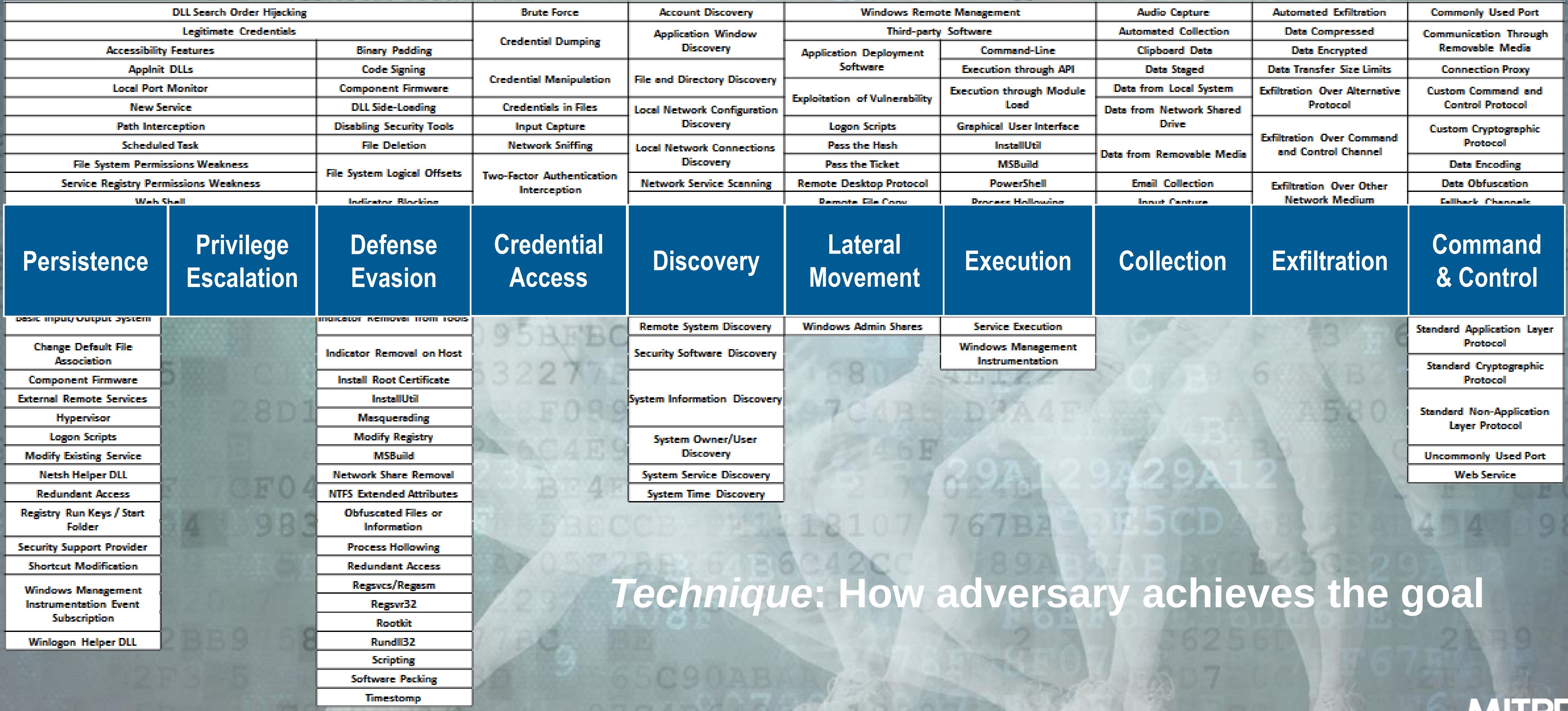
ATT&CK Matrix: *Tactics & Techniques*

Persistence	Privilege Escalation	Defense Evasion	Cre Ac	Execution	Collection	Exfiltration	Command & Control

Command & Control

Tactic: Technical goal of the adversary

MITRE



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				Execution through API	Data Staged	Data Transfer Size Limits	Connection Proxy
Local Port Monitor		Component Firmware	Credential Manipulation	File and Directory Discovery	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			Custom Cryptographic Protocol
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Discovery	Pass the Hash	InstallUtil		Exfiltration Over Command and Control Channel	
File System Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception		Pass the Ticket	MSBuild	Data from Removable Media		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			Remote File Copy	Process Hollowing	Input Capture		Fallback Channels
Persistence	**Privilege Escalation**	**Defense Evasion**	**Credential Access**	**Discovery**	**Lateral Movement**	**Execution**	**Collection**	**Exfiltration**	**Command & Control**
Basic Input/Output System		Indicator Removal from Tools		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					Standard Non-Application Layer Protocol
External Remote Services		InstallUtil		System Owner/User Discovery					Uncommonly Used Port
Hypervisor		Masquerading		System Service Discovery					Web Service
Logon Scripts		Modify Registry		System Time Discovery					
Modify Existing Service		MSBuild							
Netsh Helper DLL		Network Share Removal							
Redundant Access		NTFS Extended Attributes							
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							
Winlogon Helper DLL		Regsvr32							
		Rootkit							
		Rundll32							
		Scripting							
		Software Packing							
		Timestomp							

Technique: How adversary achieves the goal

Approved for Public Release. Distribution unlimited. Case number 17-4500-1

Example Tactic: Persistence

Persistence is any access, action, or configuration change to a system that gives an adversary a persistent presence on that system.

Adversaries will often need to maintain access to systems through interruptions such as system restarts, loss of credentials, or other failures that would require a remote access tool to restart or alternate backdoor for them to regain access.

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.
- **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, …
- **CAPEC ID:** CAPEC-550

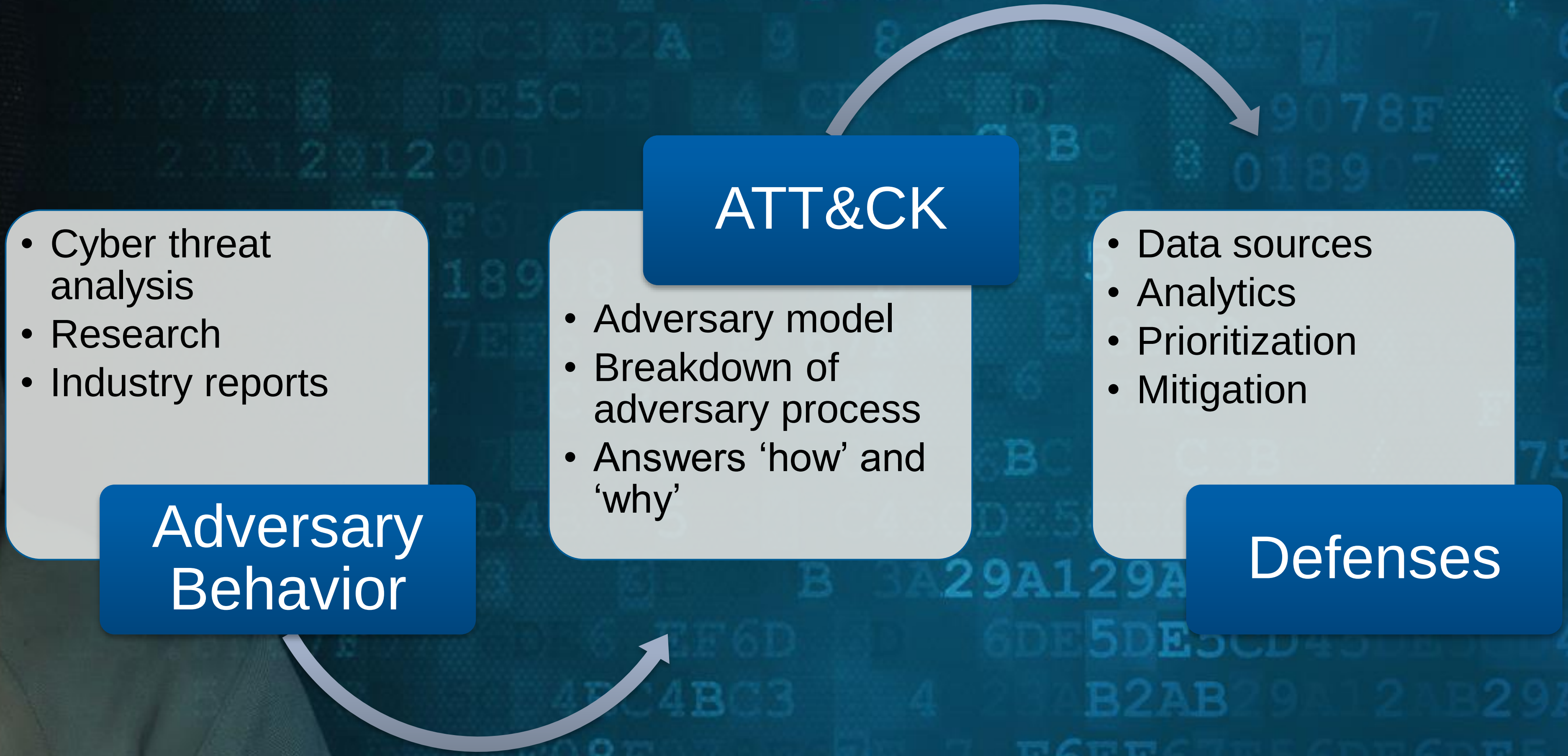
Where does ATT&CK come from?

Our Living Lab – The Fort Meade Experiment (FMX)

MITRE’s Annapolis Junction, MD site

- Approx. 250 unclassified computers
- Primarily user desktops running Windows

ATT&CK's Threat-based Modeling



Adversary Behavior

- Cyber threat analysis
- Research
- Industry reports

ATT&CK

- Adversary model
- Breakdown of adversary process
- Answers 'how' and 'why'

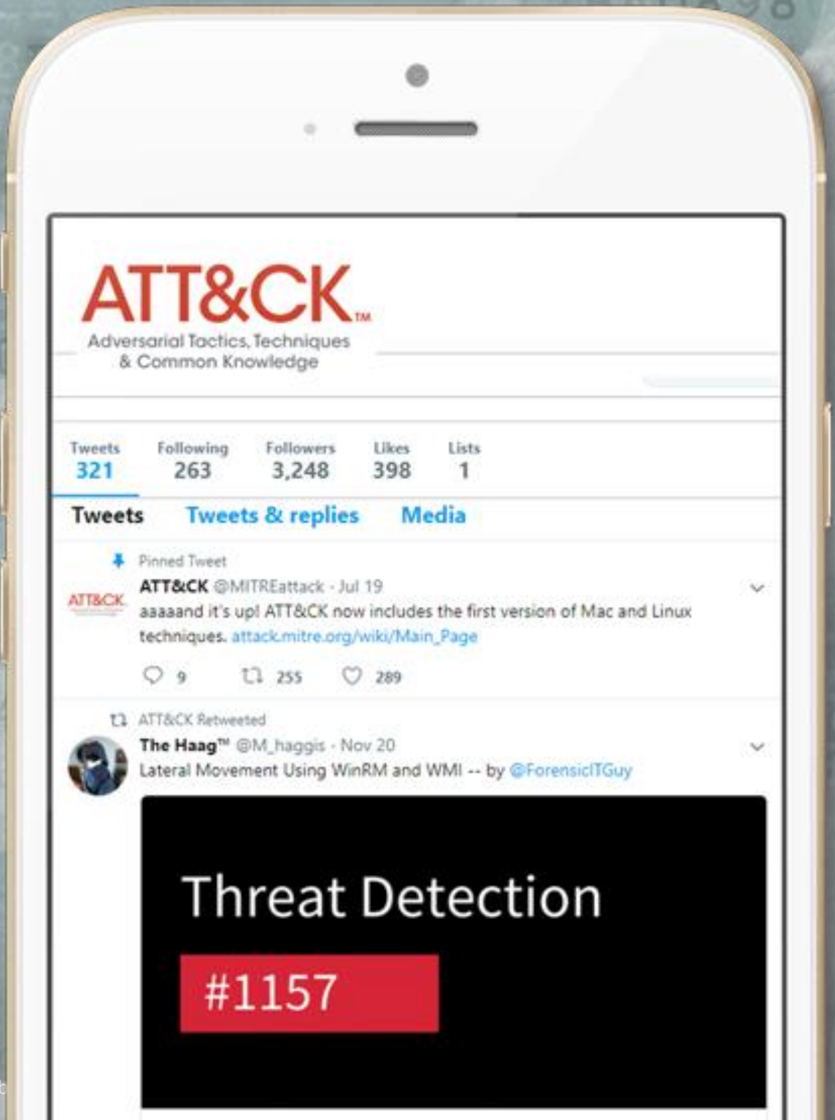
Defenses

- Data sources
- Analytics
- Prioritization
- Mitigation

Approved for Public Release. Distribution unlimited. Case number 17-4500-1

Who’s using ATT&CK?

- End-users
- Security vendors
- Government organizations



ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

Tweets 321
Following 263
Followers 3,248
Likes 398
Lists 1

Pinned Tweet

ATT&CK @MITREattack · Jul 19
aaaaand it's up! ATT&CK now includes the first version of Mac and Linux techniques. attack.mitre.org/wiki/Main_Page

ATT&CK Retweeted

The Haag™ @M_haggis · Nov 20
Lateral Movement Using WinRM and WMI -- by @ForensicITGuy

Threat Detection
#1157

ATT&CK: Additional metadata

- **Threat Groups**
- **Software**
  - Malware
  - Tools
  - Utilities
- **Analytics**

Example Group: Deep Panda

- **Description:** Deep Panda is a suspected Chinese threat group known to target many industries, including government, defense, financial, and telecommunications.[1] The intrusion into healthcare company Anthem has been attributed to Deep Panda.[2]
- **Aliases:** Deep Panda, Shell Crew, WebMasters, KungFu Kittens, PinkPanther, Black Vine
- **Techniques**
  - PowerShell
  - Windows Management Instrumentation
  - Web Shell
  - Windows Admin Shares
  - Process Discovery
  - Scripting
  - Indicator Removal from Tools
  - Regsvr32
  - Accessibility Features

– **Software:** Net, Tasklist, Sakula, Mivast, Derusbi

– **References**

1. Alperovitch, D. (2014, July 7). Deep in Thought: Chinese Targeting of National Security Think Tanks. Retrieved November 12, 2014.
2. ThreatConnect Research Team. (2015, February 27). The Anthem Hack: All Roads Lead to China. Retrieved January 26, 2016.

Example Built-in Software: Tasklist

Description: The Tasklist utility displays a list of applications and services with its Process ID (PID) for all tasks running on either a local or a remote computer. It is packaged with Windows operating systems and can be executed from the command line[1].

Aliases: Tasklist

Type: Utility

Techniques Used:

Process Discovery: Tasklist can be used to discover processes running on a system.

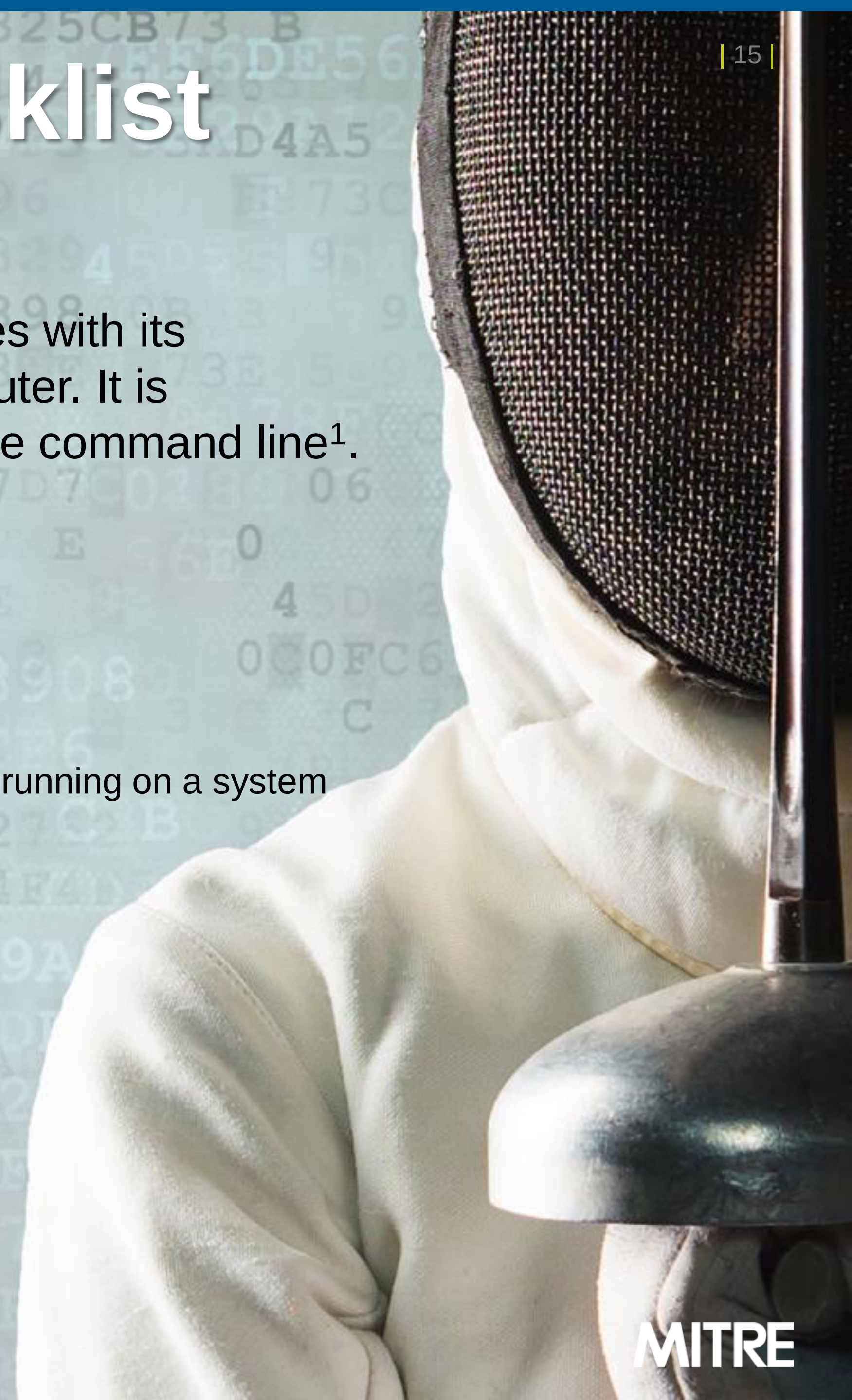
Security Software Discovery: Tasklist can be used to enumerate security software currently running on a system by process name of known products.

System Service Discovery: Tasklist can be used to discover services running on a system.

Groups: Deep Panda, Turla, Naikon, APT1

References

1. **Microsoft. (n.d.). Tasklist. Retrieved December 23, 2015.**



Example Malware: Mivast

Description: Mivast is a backdoor that has been used by Deep Panda. It was reportedly used in the Anthem breach.[1]

Aliases: Mivast

Type: Malware

Techniques Used:

- ***Registry Run Keys / Start Folder*:** Mivast creates the following Registry entry: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Micromedia.
- ***Commonly Used Port*:** Mivast communicates over port 80 for C2.
- ***Command-Line Interface*:** Mivast has the capability to open a remote shell and run basic commands.
- ***Remote File Copy*:** Mivast has the capability to download and execute .exe files.
- ***Credential Dumping*:** Mivast has the capability to gather NTLM password information.

Groups: Deep Panda

References

1. **DiMaggio, J.. (2015, August 6). The Black Vine cyberespionage group. Retrieved January 26, 2016**

How do I use ATT&CK?

- Resource for threat modeling
- Red-team/blue-team planning
- Enhance threat intelligence
- Defensive planning

Example: APT 28 Reported Techniques

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

Legend 🟦 APT 28

Example: Comparing Groups APT 28 vs. Deep Panda

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and 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		Multiband Communication
🟦 Bootkit	DLL Injection					🟦 Rundll32		Scheduled Transfer	
🟦 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			
Component Firmware		Install Root Certificate		System Information Discovery					Standard Cryptographic Protocol
External Remote Services		InstallUtil							
Hypervisor		Masquerading							Standard Non-Application Layer Protocol
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							

Legend

🟦 APT 28

🟨 Deep Panda

Approved for Public Release. Distribution unlimited. Case number 17-4500-1

MITRE

Example: Notional Defense Gaps

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

🟩 High Confidence 🟨 Med Confidence 🟥 No Confidence

Approved for Public Release. Distribution unlimited. Case number 17-4500-1

Example: Adversary Visibility at the Perimeter

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and 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	
Applnit 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		🟨 Multiband Communication
Bootkit	DLL Injection					Rundll32		🟨 Scheduled Transfer	
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							

🟩 High Confidence 🟨 Med Confidence 🟥 No Confidence

ATT&CK Resources

- Website: attack.mitre.org
- Email: attack@mitre.org
- Twitter: @MITREattack
- STIX 2 representations of ATT&CK knowledge base: https://github.com/mitre/cti

Thank you!

Questions?

rjs@mitre.org

Approved for Public Release. Distribution unlimited. Case number 17-4500-1