

Using Adversary Behavior to Strengthen Cyber Defense

No matter how strong your patching, compliance and security software, a determined cyber adversary can typically find a way into your network.

But how did the attacker get in? How are they moving around? And how can you use that knowledge to detect, mitigate and prevent future attacks? The MITRE ATT&CK™ framework answers those questions by providing a globally accessible knowledge base of adversary tactics and techniques that are based on real-world observations of adversaries' operations against computer networks. Armed with this knowledge, organizations and security vendors can work toward improving detection and prevention methods.

Pioneering with the Cyber Community for Collaborative Defense

ATT&CK was first created by a MITRE internal research program using our own data and operations. Now based on published, open source threat information, MITRE provides the framework as a resource to the cyber community. Anyone is free to leverage it, and everyone is free to use and contribute to ATT&CK.

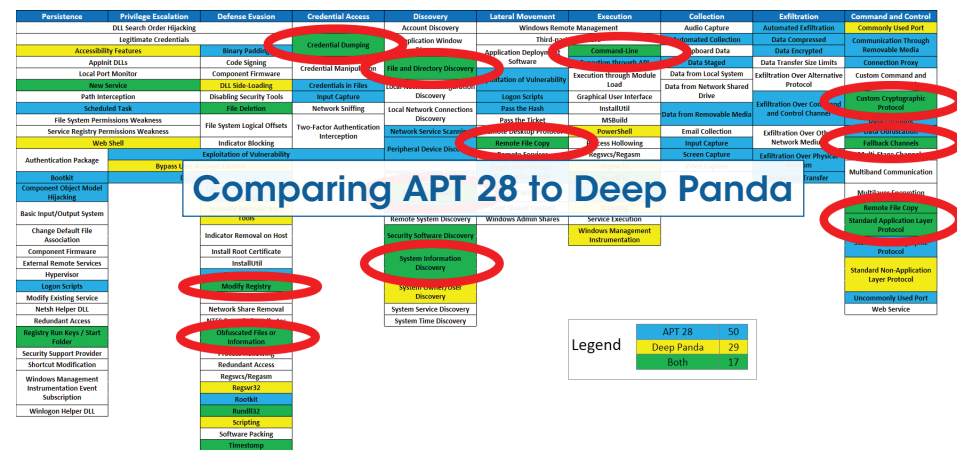
By making the ATT&CK knowledge base globally accessible, MITRE supports a growing community that is fostering innovation in open source tools, products and services based on the framework. ATT&CK is experiencing significant growth across the cybersecurity community, with wide adoption from industry, government and security vendors including organizations like Microsoft, IBM, USAA, JPMorgan Chase, and Palo Alto.

With the creation of ATT&CK, MITRE is partnering with the cyber community to fulfill its mission to solve problems for a safer world.

Get Started with ATT&CK

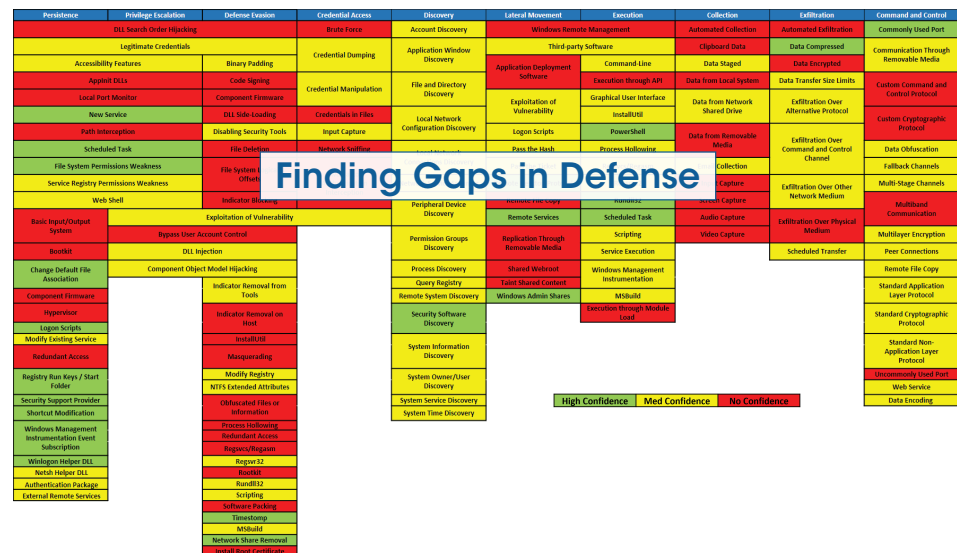
Use ATT&CK for Cyber Threat Intelligence

Cyber threat intelligence comes from many sources, including knowledge of past incidents, commercial threat feeds, information-sharing groups, government threat-sharing programs, and more. ATT&CK gives analysts a common language to communicate across reports and organizations, providing a way to structure, compare, and analyze threat intelligence.



Use ATT&CK to Build Your Defensive Platform

ATT&CK includes resources designed to help cyber defenders develop analytics that detect the techniques used by an adversary. Based on threat intelligence included in ATT&CK or provided by analysts, cyber defenders can create a comprehensive set of analytics to detect threats.



Use ATT&CK for Adversary Emulation and Red Teaming

The best defense is a well-tested defense. ATT&CK provides a common adversary behavior framework based on threat intelligence that red teams can use to emulate specific threats. This helps cyber defenders find gaps in visibility, defensive tools and processes—and then fix them.

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	Command-Line	Automated Collection	Automated Exfiltration	Commonly Used Port
Apprent Dlls	Apprent Dlls	Bypass User Account Control	Credential Dumping	Application 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
Bookkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	PowerShell	Data from Local System	Transfer Size Limits	Custom Cryptographic Protocol
Change Default File Handlers	DLL Search Order Hijacking	DLL Injection	Exploitation of Vulnerability	Local Network Connection Discovery	Pass the Ticket	Process Hollowing	Data from Removable 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	Discard 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	Medium	Multiband Communication
Legitimate Credentials	New Service	Disabling Security Tools	Exploitation of Vulnerability	Process Discovery	Replication Through Removable Media	Third-party Software	Screen Capture	Scheduled Transfer	Multilayer Encryption

Join the ATT&CK Community

MITRE encourages other researchers, analysts and cyber defenders to join our community and contribute new techniques and information.

MITRE ATT&CK Resources

attack.mitre.org

- Access ATT&CK technical information
- Contribute to ATT&CK
- Follow our blog
- Watch ATT&CK presentations

@MITREattack

Follow us on Twitter for the latest news.




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

The MITRE ATT&CK™ Enterprise Framework

attack.mitre.org

© 2019 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case Number 15-1288.



The MITRE ATT&CK™
Enterprise Framework

attack.mitre.org

