ATT&CK™

Using Adversary Behavior to Strengthen Cyber Defense

No matter how strong your firewall or anti-virus software, a determined cyber adversary will find a way into your network. But what if you had a good idea of the intruder's battle plan, so you could detect the threat and implement resilience strategies?

ATT&CK™ is a MITRE-developed, globally accessible knowledge base of adversary tactics and techniques based on real-world observations of adversaries' operations against computer networks. ATT&CK helps you understand how adversaries might operate so you can plan how to detect or stop that behavior. Armed with this knowledge, you can better understand the different ways adversaries prepare for, launch, and execute their attacks.

ATT&CK has grown from an internal MITRE project to a framework that's referenced in conferences across the world and used by organizations as varied as Microsoft, Palo Alto, and Pfizer. It's 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.

Bringing the Cyber Community Together for Collaborative Defense

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.

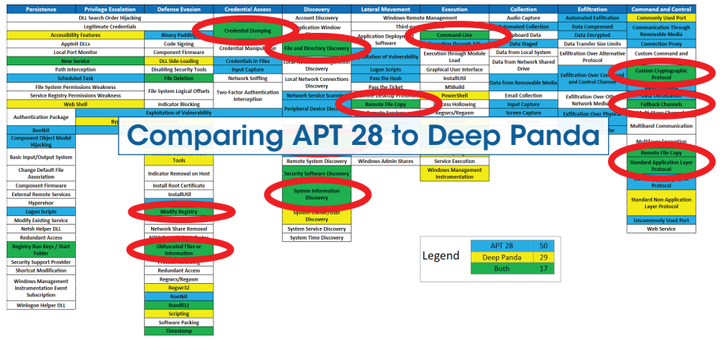
MITRE

Informing Defense Across the Adversary Lifecycle

ATT&CK is thorough and easy to understand. Organizations use it in many ways as part of a balanced security plan that includes classic cyber-defense approaches as well as new cyber resiliency techniques. ATT&CK is especially useful for informing cyber threat intelligence, building an analytics platform, and red teaming.

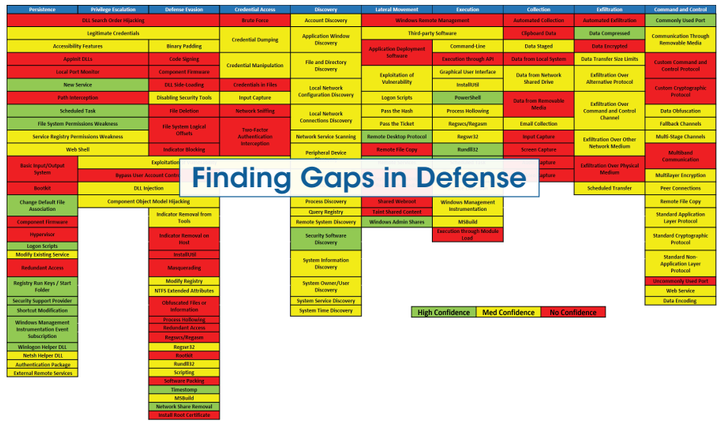
Use ATT&CK for Cyber Threat Intelligence

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 your analysts, cyber defenders can create a comprehensive set of analytics to detect the threats you face.



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 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

Follow us on Twitter

@MITREattack

Join the ATT&CK Community of Contributors

attack.mitre.org

MITRE is building a community around ATT&CK so that experts in different domains and technologies can come together to refine and extend the knowledge contained in the framework. MITRE encourages other researchers, analysts, and cyber defenders to join our community and contribute new techniques, categories of actions, clarifying information, examples, methods of detection or mitigation, and data sources. MITRE provides a conflict-free environment to create, collect, share, and manage this information, making it available to everyone.

To get involved or for more information, visit attack.mitre.org.

MITRE Enterprise ATT&CK™ Framework

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

attack.mitre.org

MITRE