Adversarial Tactics, Techniques & Common Knowledge

Welcome to ATT&CK

MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's lifecycle and the platforms they are known to target. ATT&CK is useful for understanding security risk against known adversary behavior, for planning security improvements, and verifying defenses work as expected.

Note: A MITRE Partnership Network (MPN) account is not required to view and use the ATT&CK site.

PRE-ATT&CK | ATT&CK for Enterprise | ATT&CK Mobile Profile

API Migration (May 2018)

We are in the process of migrating to new infrastructure in the coming months. A new website will be stood up to display ATT&CK content and the MediaWiki API is being transitioned to a STIX/TAXII 2.0 API. Please see here for details. If you are using the MediaWiki API, please begin migrating and reach out to attack@mitre.org with questions. The MediaWiki site will be deprecated (will not be receiving content updates) when the new website is released in July 2018. At this time the Wiki will be moved and API will still be available but will eventually be taken offline at a date that is TBD, but will not be sooner than September 2018.

ATT&CK for Enterprise

ATT&CK for Enterprise is an adversary behavior model that describes the actions an adversary may take to compromise and operate within an enterprise network.

- Introduction and Overview
- All Techniques

Enterprise Platform Coverage

The MITRE ATT&CK Matrix™ is a visualization of the tactics and techniques. It aligns individual techniques under the tactics in which they can be applied.

- Windows Technique Matrix
- Mac Technique Matrix
- Linux Technique Matrix

News and Updates

News and Blogs

- June 4, 2018 - Using ATT&CK to Advance Cyber Threat Intelligence – Part 2
- May 24, 2018 - Using ATT&CK to Advance Cyber Threat Intelligence – Part 1

- ATT&CK Navigator
- Adversary Emulation Plans
- Cyber Analytics Repository
- ATT&CK expressed in STIX
- Related Efforts
- Using the API
- Contribute or contact us

- May 21, 2018 - Just Released! Version 2 of the ATT&CK Navigator
- May 14, 2018 - ATT&CK in STIX 2.0 via public TAXII server
- May 3, 2018 - ATT&CK 101
- January 5, 2018 - What's Next for ATT&CK

See Past Blogs for previous posts.

Updates

- April 2018
- January 2018

See Past Updates for previous changes.

ATT&CK Matrix for Enterprise

The full ATT&CK Matrix below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

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	BITS Jobs	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	Binary Padding	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 Staged	Data Transfer Size Limits	Custom Command and Control Protocol

Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	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 Network Shared Drive	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 from Removable Media	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-Stage Channels
	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	Launchctl	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	Kerberoasting	Remote System Discovery	SSH Hijacking	Screen Capture		Multiband Communication
	Local Job Scheduling	Create Account	Image File Execution Options Injection	DLL Side-Loading	Keychain	Security Software Discovery	Shared Webroot	Video Capture		Multilayer Encryption

	Mshta	DLL Search Order Hijacking	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	Disabling Security Tools	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	SID-History Injection	Gatekeeper Bypass	Two-Factor Authentication Interception					Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Scheduled Task	HISTCONTROL						Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Service Registry Permissions Weakness	Hidden Files and Directories						
	Signed Script Proxy Execution	LC_LOAD_DYLIB Addition	Setuid and Setgid	Hidden Users						
	Source	LSASS Driver	Startup	Hidden Window						

			Items								
	Space after Filename	Launch Agent	Sudo	Image File Execution Options Injection							
	Third-party Software	Launch Daemon	Sudo Caching	Indicator Blocking							
	Trap	Launchctl	Valid Accounts	Indicator Removal from Tools							
	Trusted Developer Utilities	Local Job Scheduling	Web Shell	Indicator Removal on Host							
	User Execution	Login Item		Indirect Command Execution							
	Windows Management Instrumentation	Logon Scripts		Install Root Certificate							
	Windows Remote Management	Modify Existing Service		InstallUtil							
		Netsh Helper DLL		LC_MAIN Hijacking							
		New Service		Launchctl							
		Office Application Startup		Masquerading							
		Path Interception		Modify Registry							
		Plist Modification		Mshta							
		Port Knocking		NTFS File Attributes							
		Port Monitors		Network Share Connection Removal							
		Rc.common		Obfuscated Files or Information							
		Re-opened Applications		Plist Modification							
		Redundant Access		Port Knocking							

		Registry Run Keys / Start Folder		Process Doppelgänging						
		SIP and Trust Provider Hijacking		Process Hollowing						
		Scheduled Task		Process Injection						
		Screensaver		Redundant Access						
		Security Support Provider		Regsvcs/Regasm						
		Service Registry Permissions Weakness		Regsvr32						
		Shortcut Modification		Rootkit						
		Startup Items		Rundll32						
		System Firmware		SIP and Trust Provider Hijacking						
		Time Providers		Scripting						
		Trap		Signed Binary Proxy Execution						
		Valid Accounts		Signed Script Proxy Execution						
		Web Shell		Software Packing						
		Windows Management Instrumentation Event Subscription		Space after Filename						
		Winlogon Helper DLL		Timestomp						
				Trusted Developer Utilities						

				Valid Accounts						
				Web Service						