Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	CredentialAccess	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Scheduled Task		Trivilege Estation	XSL Script Processing			Windows Remote	Video Capture	Scheduled Transfer
Trusted Relationship	Trap		Process Injection		Two-Factor Authentication	System Time Discovery	Management	Screen Capture	Exfiltration Over
Supply Chain Compromise	LSASS Driver			Memory Injection	Interception	System Service Discovery	Third-party Software	Man in the Browser	Physical Medium
Spearphishing via Service	Local Job Scheduling		Bypass User Account Control		Private Keys	System Owner/User	Taint Shared Content	Input Capture	Exfiltration Over Command
Spearphishing Link	Launchctl		Access Token Manipulation		Password Filter DLL	Discovery	SSH Hijacking	Email Collection	and Control Channel
Spearphishing Attachment	XSL Script Processing		Valid Accounts		LLMNR/NBT-NS Poisoning	System Network	Shared Webroot	Data Staged	Data Transfer Size Limits
Replication Through	Windows Remote		Plist Modification		Keychain	Configuration Discovery	Replication Through	Data from Removable Media	Data Encrypted
Removable Media	Management Ima		nage File Execution Options Injection		Kerberoasting	Security Software Discovery	Removable Media	Data from Network	Data Compressed
Exploit Public-Facing	User Execution		DLL Search Order Hijacking		Input Prompt	Remote System Discovery	Remote File Copy	Shared Drive	Automated Exfiltration
Application	Trusted Developer Utilities	Web S	Shell	Web Service	Input Capture	Query Registry	Remote Desktop Protocol	Data from Information	Exfiltration Over Other
Hardware Additions	Third-party Software	Startup	Items	Trusted Developer Utilities	Hooking	Process Discovery	Pass the Ticket	Repositories	Network Medium
Drive-by Compromise	Space after Filename	Setuid an	d Setgid	Timestomp	Forced Authentication	Permission Groups Discovery	Pass the Hash	Automated Collection	Exfiltration Over
	Source	rce Service Registry Permissions Weakness		Template Injection	Exploitation for	Peripheral Device Discovery	Logon Scripts	Audio Capture	Alternative Protocol
	Signed Script Port Mo		onitors	Space after Filename	Credential Access	Password Policy Discovery	Exploitation of	Data from Local System	
	Proxy Execution	Path Inter	rception	Software Packing	Credentials in Files	Network Share Discovery	Remote Services	Clipboard Data	
	Service Execution	New Se	ervice	SIP and Trust	Credential Dumping	Network Service Scanning	Application Deployment		
	Scripting	Launch D	Daemon	Provider Hijacking	Brute Force	File and Directory Discovery	Software		
	Rundll32	Hook	king	Signed Binary	Bash History	Browser Bookmark Discovery	Windows Admin Shares		
	Regsvr32	File System Permis	ssions Weakness	Proxy Execution	Account Manipulation	Application Window	Remote Services		
	Regsvcs/Regasm	Dylib Hij	jacking	Rundll32	Securityd Memory	Discovery	Distributed Component		
	PowerShell	Application	Shimming	Rootkit	Credentials in Registry	System Network	Object Model		
	Mshta	Applnit	t DLLs	Regsvr32		Connections Discovery	AppleScript		
	InstallUtil	AppCer	t DLLs	Regsvcs/Regasm		System Information			
	Graphical User Interface	Accessibility	y Features	Redundant Access		Discovery			
	Exploitation for	Winlogon Helper DLL	Sudo Caching	Process Hollowing		Account Discovery			
	Client Execution	Windows Management	Sudo	Process Doppelganging					
	Execution through API	Instrumentation	SID-History Injection	Port Knocking					
	Dynamic Data Exchange	Event Subscription	Exploitation for	Obfuscated Files					
	Control Panel Items	SIP and Trust Provider	Privilege Escalation	or Information					
	Compiled HTML File	Hijacking		Network Share					
	Command-Line Interface	Security Support Provider		Connection Removal					
	CMSTP	Screensaver		Modify Registry					
	AppleScript	Registry Run		Masquerading					
	Windows Management	Keys / Startup Folder		LC_MAIN Hijacking					
	Instrumentation	Re-opened Applications		Launchetl					
	Signed Binary	Rc.common		InstallUtil					
	Proxy Execution	Port Knocking		Install Root Certificate					
	Execution through Module Load	Office Application Startup		Indirect Command Execution					
	iviodale Load	Netsh Helper DLL		Component Firmware Indicator Removal from Tools					
		Modify Existing Service					ATTO		
		Logon Scripts Login Item		Indicator Blocking HISTCONTROL		MITRE	$\Lambda \sqcup \sqcup X$		
		LC_LOAD_DYLIB Addition		Hidden Window		IVIIIIXL	AIIO		
		Launch Agent		Hidden Users					
		Kernel Modules		Hidden Files and Directories				_	
		and Extensions		Gatekeeper Bypass		Enterr	Trico	-romo	MAIOPI
		Hidden Files and Directories		File System Logical Offsets) SC		:VVC)IK
		External Remote Services		File Permissions Modification					
		Create Account		File Deletion		_			
		Component Object Model		Exploitation for					
		Hijacking		Defense Evasion					
		Change Default		Disabling Security Tools					
		File Association		Deobfuscate/Decode Files		attack.n	itro or		
		Bootkit		or Information		attatnill	IIII C'OI		
		BITS Jobs		Control Panel Items			•		
		Authentication Package		Component Object					
		Account Manipulation		Model Hijacking					
		.bash_profile and .bashrc		Compiled HTML File					
		Time Providers		Code Signing					
		System Firmware		CMSTP					
		Shortcut Modification		Clear Command History	1				

Clear Command History

BITS Jobs

Signed Script Proxy Execution

Scripting

NTFS File Attributes

Mshta

Indicator Removal on Host

DLL Side-Loading

DCShadow



Shortcut Modification

Redundant Access

Hypervisor

Component Firmware

Browser Extensions

Command and Control

Web Service

Uncommonly Used Port

Standard Non-Application **Layer Protocol**

Standard Application Layer Protocol

Remote Access Tools

Port Knocking

Multilayer Encryption

Multiband Communication

Multi-Stage Channels

Multi-hop Proxy

Fallback Channels

Domain Fronting

Data Obfuscation

Data Encoding

Custom Cryptographic Protocol

Connection Proxy

Communication Through Removable Media

Standard Cryptographic Protocol

Remote File Copy

Custom Command and Control Protocol

Commonly Used Port

MITRE ATT&CK" Techniques Mapped to Data Sources

About This Diagram

How can I use data I already have to get started with ATT&CK?

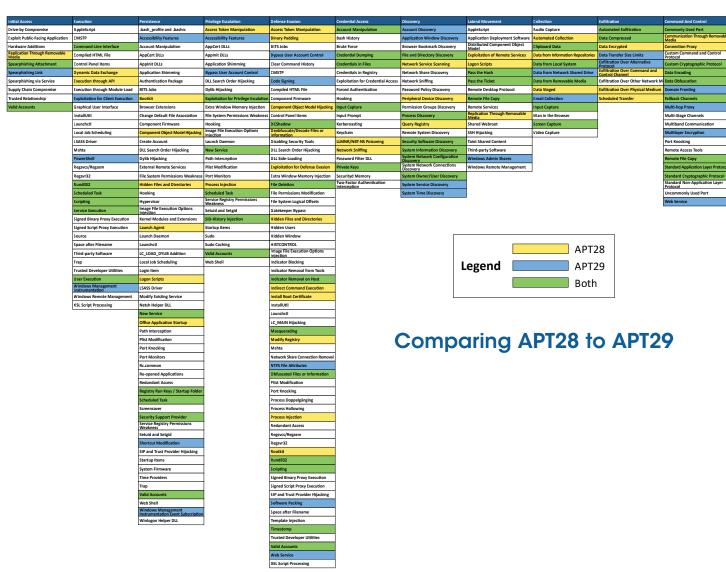
One way to get started using ATT&CK is to look at what data sources you're already collecting and use that data to detect ATT&CK techniques. On our website, we currently have 50 different data sources mapped to Enterprise ATT&CK techniques. In this diagram, we've chosen 12 of those data sources to show the techniques each of them might be able to detect with the right collection and analytics. Check out our website at *attack.mitre.org* for more information on how each technique can be detected, and specific adversary examples you can use to start detecting adversary behavior with ATT&CK.

You can visualize how your own data sources map to adversary behavior with ATT&CK. Read our blog post at *bit.ly/ATTACK19* to learn how we generated this diagram, check out the code, and begin building your own diagrams from ATT&CK content.

Get Started with ATT&CK

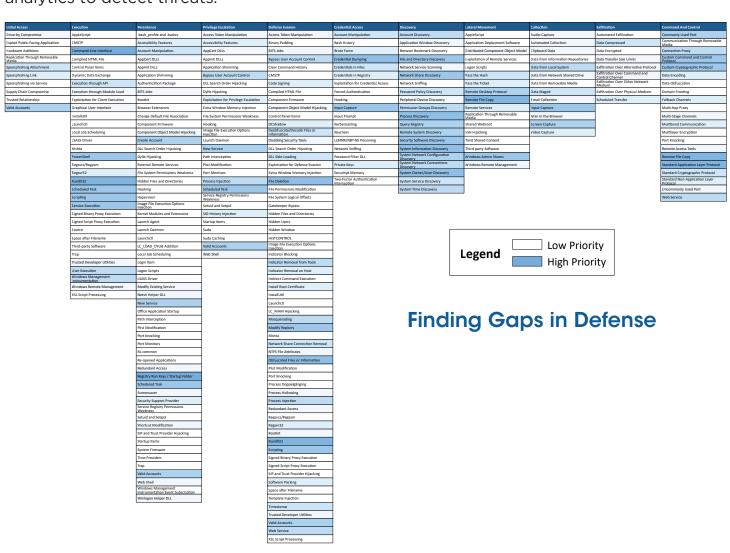
Use ATT&CK for Cyber Threat Intelligence

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

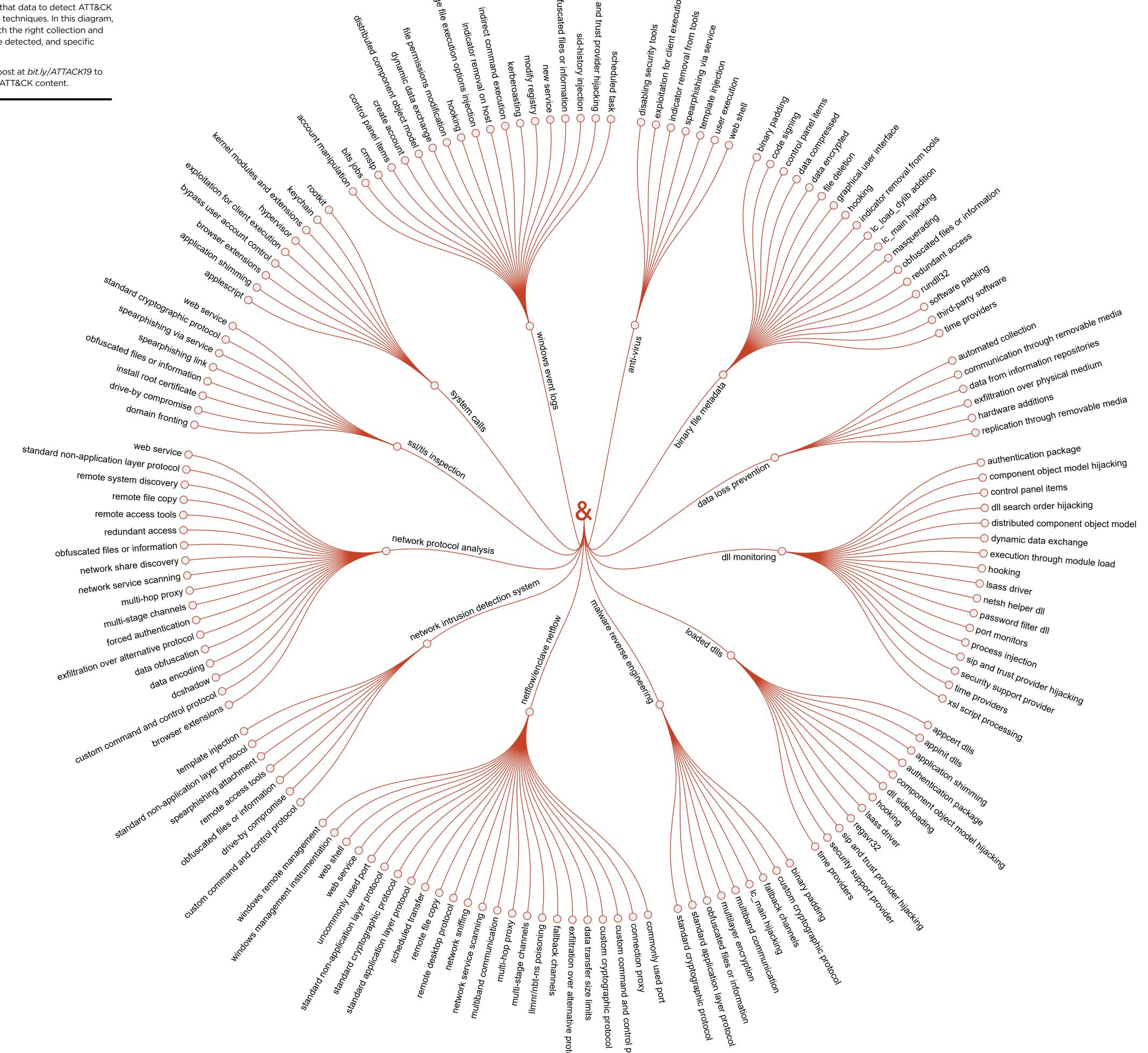
ATT&CK includes resources designed to help cyber defenders develop analytics that detect the techniques used by an adversary. Based on threat intelligence included in ATT&CK or provided by analysts, cyber defenders can create a comprehensive set of analytics to detect threats.



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.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Hardware Additions		Scheduled Task		Binary Padding	Credentials in Registry	Browser Bookmark	Exploitation of Remote	Data from Information	Exfiltration Over	Remote Access Tools
Trusted Relationship	LSASS	Driver Extra Window M		Nemory Injection	Exploitation for	Discovery	Services	Repositories	Physical Medium	Port Knocking
Supply Chain	Local Job S	Scheduling	Access Token Manipulation		Credential Access	Network Share	Distributed Component	Video Capture	Exfiltration Over	Multi-hop Proxy
Compromise	Ĭ	Trap		Bypass User Account Control		Discovery	-	Audio Capture	Command and	Domain Fronting
Spearphishing	Laun	chct	Process	Injection	Hooking	Peripheral Device	Remote File Copy	Automated Collection	Control Channel	Data Encoding
Attachment	Sweed Binary	swied Binary Image		File Execution Options Injection		Discovery	I assmenet	Clipboard Data	Datencrypted	Remote File Copy
Exploit Public-Facing	Proxy Execution		Plist Modification		LLMNR/NBT-NS	File and Directory	Replication Theough	Email Collection	Automated Exfiltration	Multi-Stage Channels
Application	User Execution		Valid Accounts		Poisoning	Discovery	Removable Media	Screen Capture	Exfiltration Over Other	Web Service
Replication Through	Expressional		DLL Search Order Wjacking	5	Private Keys	Permission Groups	Windows Admin Shares	Data Staged	Network Medium	Standard
Removable Media	Client Execution	Apple	ort DLLs	Signed Script	Keychain	Discovery	Pass the Ha	Input Capture	Exhitration Over	Non-Apolication
Spearphishing via	CMSTP	Hoo	oking	Prox, Execution	Input Prompt	rocess Discovery	Third-party Sof ware	Data from Network	Alternative Protocol	Layer Protocol
Service	Dynamic Data Exchange	Startu	pricems	DCShadow	Bash History	System Network	Shared Web oot	Shared Drive	Data Transfer	Connection
Spearphishing Link	Mshta	Launch	Daemon	Port Knocking	Two-Factor	Connections Discovery	Logon Scripts	Data from Local System	Size Limits	Multilaver Encountion
Drive-by Compromise	AppleScript	Dylib Hijacking		Indirect Command	Authentication	System Owner/User	Windows R mote	Man in the Browser	Data Compressed	standard Application
Valid Accounts	Source	Application	n Shimming	Execution	Interception	Discovery	Management	Data from Removable	Scheduled Transfer	Laver Protocol
	Space after Filename	Appln	it DLLs	BITS Jobs	Replication Through	System Network	Application	Media]	Commonly Used Port
	Execution through	Web	Shell	Control Panel Items	Removable Media	Configuration Discovery	Deployment Software			Standard Cryptographic
	Module Load	Service Registry Permissions Weakness		CMSTP	Inpl Capture	Application Window	SSH Hijacking			Protocol
	Regsvcs/Regasm	New Service		Process Doppelgänging	Notwood Coiffing	Discovery	ppleScript			Custom Cryptographic
	InstallUtil	File System Permissions Weakness		Mshta	Credential Dumping	Password Policy	Tajut Shared Content			Protocol
	Regsvr32	Path Interception		Hidden Files	Acrocrossing	iscovery	Remote Desktop			Data Obfuscation
	Execution through API	Accessibility Features		and Directories	Securityd Memory	System 1 me Discovery	Protocol			Custom Command
	PowerShell	Port Monitors		Space after Filename	Brute Force	Account Discovery	Remote Services			and Control Protocol
	Rundll32	Kernel Modules	Sudo Caching		Account Manipulation	System mormation				Communication



Resources

attack.mitre.org

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



attackevals.mitre.org

MITRE ATT&CK Evaluations

MITRE

To help cyber defenders gain a common understanding of the threats they face, MITRE developed the ATT&CK framework. It's a globally-accessible knowledge base of adversary tactics and techniques based on real world observations and open source research contributed by the cyber community.

Used by organizations around the world, ATT&CK provides a shared understanding of adversary tactics, techniques and procedures and how to detect, prevent, and/or mitigate them.

ATT&CK is open and available to any person or organization for use at no charge.

For sixty years, MITRE has tackled complex problems that challenge public safety, stability, and well-being. Pioneering together with the cyber community, we're building a stronger, threat-informed defense for a safer world.

