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

MITRE ATT&CK™ Enterprise Framework

attack.mitre.org

MITRE

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?

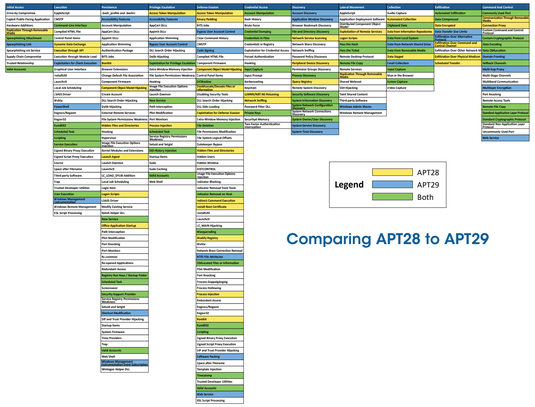
One way to get started using ATT&CK is to look at what data sources you're already collecting and use that data to detect ATT&CK techniques. On our website, we currently have 50 different data sources mapped to Enterprise ATT&CK techniques. In this diagram, we've chosen 12 of those data sources to show 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

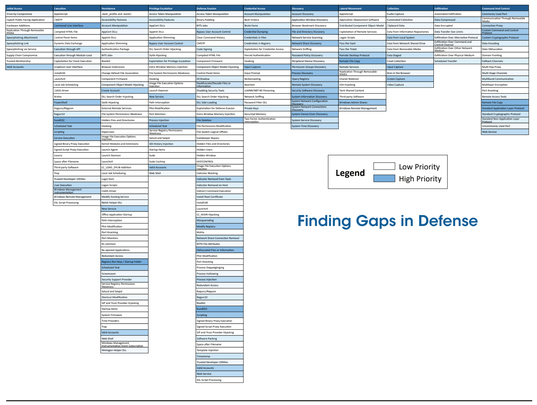
Cyber threat intelligence comes from many sources, including knowledge of past incidents, commercial threat feeds, information-sharing groups, government threat-sharing programs, and more. ATT&CK gives analysts a common language to communicate across reports and organizations, providing a way to structure,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



Comparing APT28 to APT29

Use ATT&CK to Build Your Defensive Platform

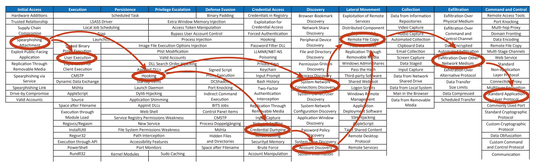
ATT&CK includes resources designed to help cyber defenders develop analytics that detect the techniques used by an adversary. Based on threat intelligence included in ATT&CK or provided by analysts, cyber defenders can create a comprehensive set of analytics to detect threats.

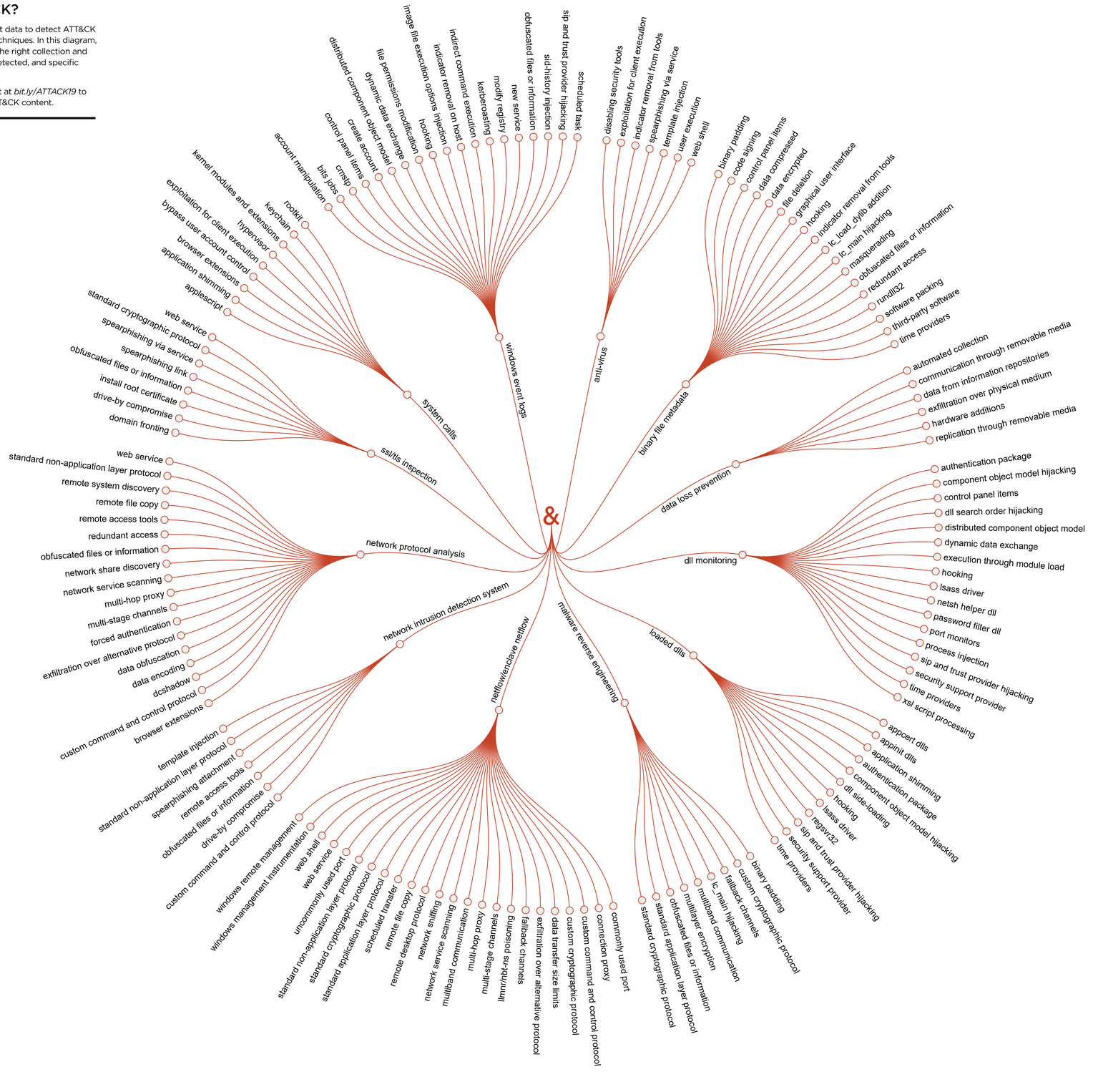


Finding Gaps in Defense

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.





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

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.

ATT&CK™ Enterprise Framework

MITRE