ATT&CK®

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is 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.

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.

ATT&CK Matrix for Enterprise

layout: side | show sub-techniques | hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Stealth	Defense Impairment	Credential Access	Discovery	Lateral Movement	Collection
12 techniques	9 techniques	11 techniques	20 techniques	22 techniques	13 techniques	30 techniques	18 techniques	17 techniques	34 techniques	9 techniques	17 techniques
Active Scanning (3)	Acquire Access	Content Injection	BITS Jobs	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Access Token Manipulation (5)	Disable or Modify System Firewall (3)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Cloud Administration Command	BITS Jobs	Access Token Manipulation (5)	BITS Jobs	Disable or Modify Tools (6)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Command and Scripting Interpreter (13)	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	Build Image on Host	Domain or Tenant Policy Modification (2)	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Container Administration Command	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Debugger Evasion	Downgrade Attack	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Deploy Container	Cloud Application Integration	Boot or Logon Initialization Scripts (5)	Delay Execution	Exploitation for Defense Impairment	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	ESXi Administration Command	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	File and Directory Permissions Modification (2)	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data
Query Public AI Services	Generate Content (2)	Replication Through Removable Media	Exploitation for Client Execution	Create Account (3)	Domain or Tenant Policy Modification (2)	Direct Volume Access	Modify Authentication Process (9)	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage
Search Closed Sources (2)	Obtain Capabilities (7)	Supply Chain Compromise (3)	Hijack Execution Flow (12)	Create or Modify System Process (5)	Escape to Host	Execution Guardrails (2)	Modify Cloud Compute Infrastructure (5)	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)
Search Open Technical Databases (5)	Stage Capabilities (6)	Trusted Relationship	Input Injection	Event Triggered Execution (18)	Event Triggered Execution (18)	Exploitation for Stealth	Modify Cloud Resource Hierarchy	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (6)
Search Open Websites/Domains (3)		Valid Accounts (4)	Inter-Process Communication (3)	Exclusive Control	Exploitation for Privilege Escalation	Hide Artifacts (14)	Modify Registry	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System
Search Threat Vendor Data		Wi-Fi Networks	Native API	External Remote Services	Process Injection (12)	Hijack Execution Flow (12)	Modify System Image (2)	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive
Search Victim-Owned Websites			Poisoned Pipeline Execution	Implant Internal Image	Scheduled Task/Job (5)	Indicator Removal (8)	Network Boundary Bridging (1)	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media
			Scheduled Task/Job (5)	Modify Authentication Process (9)	Valid Accounts (4)	Indirect Command Execution	Plist File Modification	Steal Application Access Token	Group Policy Discovery		Data Staged (2)
			Serverless Execution	Modify Registry		Masquerading (12)	Prevent Command History Logging	Steal or Forge Authentication Certificates	Local Storage Discovery		Email Collection (3)
			Shared Modules	Office Application Startup (6)		Obfuscated Files or Information (18)	Rogue Domain Controller	Steal or Forge Kerberos Tickets (5)	Log Enumeration		Input Capture (4)
			Software Deployment Tools	Power Settings		Pre-OS Boot (5)	Safe Mode Boot	Steal Web Session Cookie	Network Service Discovery		Screen Capture
			System Services (3)	Pre-OS Boot (5)		Process Injection (12)	Subvert Trust Controls (6)	Unsecured Credentials (8)	Network Share Discovery		Video Capture
			Trusted Developer Utilities Proxy Execution (3)	Scheduled Task/Job (5)		Reflective Code Loading	Weaken Encryption (2)		Network Sniffing		
			User Execution (5)	Server Software Component (6)		Rootkit			Password Policy Discovery		
			Windows Management Instrumentation	Software Extensions (2)		Selective Exclusion			Peripheral Device Discovery		
				Traffic Signaling (2)		Social Engineering (2)			Permission Groups Discovery (3)		
				Valid Accounts (4)		System Binary Proxy Execution (14)			Process Discovery		
						System Script Proxy Execution (2)			Query Registry		
						Template Injection			Remote System Discovery		
						Traffic Signaling (2)			Software Discovery (2)		
						Trusted Developer Utilities Proxy Execution (3)			System Information Discovery		
						Unused/Unsupported Cloud Regions			System Location Discovery (1)		
						Valid Accounts (4)			System Network Configuration Discovery (2)		
						Virtualization/Sandbox Evasion (3)			System Network Connections Discovery		
						XSL Script Processing			System Owner/User Discovery		
									System Service		