

RECONNAISSANCE 10 techniques	RESOURCE DEVELOPMENT 8 techniques	INITIAL ACCESS 9 techniques	EXECUTION 14 techniques	PERSISTENCE 19 techniques	PRIVILEGE ESCALATION 13 techniques	DEFENSE EVASION 42 techniques	CREDENTIAL ACCESS 17 techniques	DISCOVERY 31 techniques	LATERAL MOVEMENT 9 techniques	COLLECTION 17 techniques	COMMAND AND CONTROL 16 techniques	EXFILTRATION 9 techniques	IMPACT 13 techniques
Active Scanning	Acquire Infrastructure	Valid Accounts	Scheduled Task/Job										
Gather Victim Host Information	Compromise Accounts	Replication Through Removable Media	Windows Management Instrumentation		Valid Accounts		Network Sniffing		Software Deployment Tools	Data from Removable Media	Fallback Channels	Exfiltration Over Other Network Medium	Data Destruction
Gather Victim Identity Information	Compromise Infrastructure	Trusted Relationship	Software Deployment Tools		Hijack Execution Flow		OS Credential Dumping	Application Window Discovery	Replication Through Removable Media	Input Capture	Application Layer Protocol	Scheduled Transfer	Data Encrypted for Impact
Gather Victim Network Information	Establish Accounts	Supply Chain Compromise	Shared Modules		Boot or Logon Initialization Scripts	Direct Volume Access	Input Capture	System Network Configuration Discovery	Internal Spearphishing	Data Staged	Proxy	Data Transfer Size Limits	Service Stop
Gather Victim Org Information	Obtain Capabilities	Hardware Additions	User Execution		Create or Modify System Process	Rootkit	Brute Force	System Owner/User Discovery	Use Alternate Authentication Material	Screen Capture	Communication Through Removable Media	Exfiltration Over C2 Channel	Inhibit System Recovery
Phishing for Information	Develop Capabilities	Exploit Public-Facing Application	Exploitation for Client Execution		Event Triggered Execution	Obfuscated Files or Information	Two-Factor Authentication Interception	System Network Connections Discovery	Lateral Tool Transfer	Email Collection	Web Service	Exfiltration Over Physical Medium	Defacement
Search Closed Sources	Stage Capabilities	Phishing	System Services	Account Manipulation	Boot or Logon Autostart Execution		Exploitation for Credential Access	System Network Connections Discovery	Taint Shared Content	Clipboard Data	Multi-Stage Channels	Exfiltration Over Web Service	Resource Hijacking
Search Open Technical Databases	Acquire Access	External Remote Services	Command and Scripting Interpreter	External Remote Services	Access Token Manipulation		Steal Web Session Cookie	Permission Groups Discovery	Exploitation of Remote Services	Automated Collection	Ingress Tool Transfer	Automated Exfiltration	Endpoint Denial of Service
Search Open Websites/Domains		Drive-by Compromise	Native API	Office Application Startup	Abuse Elevation Control Mechanism		Unsecured Credentials	File and Directory Discovery	Remote Service Session Hijacking	Audio Capture	Data Encoding	Exfiltration Over Alternative Protocol	System Shutdown/Reboot
Search Victim-Owned Websites			Inter-Process Communication	Create Account	Domain Policy Modification		Credentials from Password Stores	Peripheral Device Discovery		Video Capture	Traffic Signaling	Transfer Data to Cloud Account	Account Access Removal
			Container Administration Command	Browser Extensions	Escape to Host	Indicator Removal on Host	Steal or Forge Kerberos Tickets	Network Share Discovery		Browser Session Hijacking	Remote Access Software		Disk Wipe
			Deploy Container	Traffic Signaling	Exploitation for Privilege Escalation	Modify Registry	Forced Authentication	Password Policy Discovery		Data from Information Repositories	Dynamic Resolution		Data Manipulation
			Serverless Execution	Server Software Component		Trusted Developer Utilities Proxy Execution	Steal Application Access Token	Browser Information Discovery		Adversary-in-the-Middle	Non-Standard Port		
			Cloud Administration Command	Pre-OS Boot		Traffic Signaling	Adversary-in-the-Middle	Virtualization/Sandbox Evasion		Archive Collected Data	Protocol Tunneling		
				Compromise Client Software Binary		Signed Script Proxy Execution	Forge Web Credentials	Cloud Service Dashboard		Data from Network Shared Drive	Encrypted Channel		
				Implant Internal Image		Rogue Domain Controller	Multi-Factor Authentication Request Generation	Software Discovery		Data from Cloud Storage Object	Non-Application Layer Protocol		
				Modify Authentication Process		Indirect Command Execution	Steal or Forge Authentication Certificates	Query Registry		Data from Configuration Repository			
						BITS Jobs		Remote System Discovery					
						XSL Script Processing		Network Service Scanning					
						Template Injection		Process Discovery					
						File and Directory Permissions Modification		System Information Discovery					
						Virtualization/Sandbox Evasion		Account Discovery					
						Unused/Unsupported Cloud Regions		System Time Discovery					
						Use Alternate Authentication Material		Domain Trust Discovery					
						Impair Defenses		Cloud Service Discovery					
						Hide Artifacts		Container and Resource Discovery					
						Masquerading		Cloud Infrastructure Discovery					
						Deobfuscate/Decode Files or Information		System Location Discovery					
						Signed Binary Proxy Execution		Cloud Storage Object Discovery					
						Exploitation for Defense Evasion		Group Policy Discovery					
						Execution Guardrails		Debugger Evasion					
						Modify Cloud Compute Infrastructure		Device Driver Discovery					
						Pre-OS Boot							
						Subvert Trust Controls							
						Build Image on Host							
						Deploy Container							
						Modify System Image							
						Network Boundary Bridging							
						Weaken Encryption							
						Reflective Code Loading							
						Debugger Evasion							
						Plist File Modification							

≡ Has sub-techniques

MITRE | ATT&CK® Enterprise Framework

attack.mitre.org