Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 34 techniques	Credential Access 14 techniques	Discovery 24 techniques	Lateral Movement 9 techniques	Collection 16 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Valid Accounts ≡	Scheduled Task/Job ≡	Scheduled Task/Job ≡	Scheduled Task/Job ≡	Modify Authentication Process ≡	Modify Authentication Process ≡	System Service Discovery	Remote Services ≡	Data from Local System	Data Obfuscation ≡	Exfiltration Over Other Network Medium ≡	Data Destruction
Replication Through Removable Media	Windows Management Instrumentation	Valid Accounts ≡	Valid Accounts ≡	Valid Accounts ≡	Network Sniffing	Network Sniffing	Software Deployment Tools	Data from Removable Media	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Trusted Relationship	Software Deployment Tools	Hijack Execution Flow ≡	Hijack Execution Flow ≡	Hijack Execution Flow ≡	OS Credential Dumping ≡	Application Window Discovery	Replication Through Removable Media	Input Capture ≡	Application Layer Protocol ≡	Data Transfer Size Limits	Service Stop
Supply Chain Compromise ≡	Shared Modules	Boot or Logon Initialization Scripts ≡	Boot or Logon Initialization Scripts ≡	Direct Volume Access	Input Capture ≡	System Network Configuration Discovery	Internal Spearphishing	Data Staged ≡	Proxy ≡	Exfiltration Over C2 Channel	Inhibit System Recovery
Hardware Additions	User Execution ≡	Create or Modify System Process ≡	Create or Modify System Process ≡	Rootkit	Brute Force ≡	System Owner/User Discovery	Use Alternate Authentication Material ≡	Screen Capture	Communication Through Removable Media	Exfiltration Over Physical Medium ≡	Defacement ≡
Exploit Public-Facing Application	Exploitation for Client Execution	Event Triggered 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 Web Service ≡	Firmware Corruption
Phishing ≡	System Services ≡	Boot or Logon Autostart Execution ≡	Boot or Logon Autostart Execution ≡	Process Injection ≡	Exploitation for Credential Access	Permission Groups Discovery ≡	Taint Shared Content	Clipboard Data	Multi-Stage Channels	Automated Exfiltration	Resource Hijacking
External Remote Services	Command and Scripting Interpreter ≡	Account Manipulation ≡	Process Injection ≡	Access Token Manipulation ≡	Steal Web Session Cookie	File and Directory Discovery	Exploitation of Remote Services	Automated Collection	Ingress Tool Transfer	Exfiltration Over Alternative Protocol ≡	Network Denial of Service ≡
Drive-by Compromise	Native API	External Remote Services	Access Token Manipulation ≡	Group Policy Modification	Unsecured Credentials ≡	Peripheral Device Discovery	Remote Service Session Hijacking ≡	Audio Capture	Data Encoding ≡	Transfer Data to Cloud Account	Endpoint Denial of Service ≡
	Inter-Process Communication ≡	Office Application Startup ≡	Group Policy Modification	Abuse Elevation Control Mechanism ≡	Credentials from Password Stores ≡	Network Share Discovery		Video Capture	Traffic Signaling ≡		System Shutdown/Reboot
		Create Account ≡	Abuse Elevation Control Mechanism ≡	Indicator Removal on Host ≡	Steal or Forge Kerberos Tickets ≡	Password Policy Discovery		Man in the Browser	Remote Access Software		Account Access Removal
		Browser Extensions	Exploitation for Privilege Escalation	Modify Registry	Forced Authentication	Browser Bookmark Discovery		Data from Information Repositories ≡	Dynamic Resolution ≡		Disk Wipe ≡
		Traffic Signaling ≡		Trusted Developer Utilities Proxy Execution ≡	Steal Application Access Token	Virtualization/Sandbox Evasion ≡		Man-in-the-Middle ≡	Non-Standard Port		Data Manipulation ≡
		BITS Jobs		Traffic Signaling ≡	Man-in-the-Middle ≡	Cloud Service Dashboard		Archive Collected Data ≡	Protocol Tunneling		
		Server Software Component ≡		Signed Script Proxy Execution ≡		Software Discovery ≡		Data from Network Shared Drive	Encrypted Channel ≡		
		Pre-OS Boot ≡		Rogue Domain Controller		Query Registry		Data from Cloud Storage Object	Non-Application Layer Protocol		
		Compromise Client Software Binary		Indirect Command Execution		Remote System Discovery					
		Implant Container Image		BITS Jobs		Network Service Scanning					
				XSL Script Processing		Process Discovery					
				Template Injection		System Information Discovery					
				File and Directory Permissions Modification ≡		Account Discovery ≡					
				Virtualization/Sandbox Evasion ≡		System Time Discovery					
				Unused/Unsupported Cloud Regions		Domain Trust Discovery					
				Use Alternate Authentication Material ≡		Cloud Service Discovery					
				Impair Defenses ≡							
				Hide Artifacts ≡							
				Masquerading ≡							
				Deobfuscate/Decode Files or Information							
				Signed Binary Proxy Execution ≡							
				Exploitation for Defense Evasion							
				Execution Guardrails ≡							
				Modify Cloud Compute Infrastructure ≡							
				Pre-OS Boot ≡							
				Subvert Trust Controls ≡							

≡ Has sub-techniques

MITRE ATT&CK®
Enterprise Framework

attack.mitre.org