







Endpoint Protection

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 12 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 10 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (2)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public-Facing Application	Compilant Admin-Scripting Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spoofing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limit	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Execution (14)	Boot or Logon Execution (14)	Boot or Logon Execution (14)	Credential from Password Stores (3)	Browser Bookmark Discovery	Legacy Tool Transfer	Audio Capture	Data Erasing (2)	Cyberlock Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (4)	Greenpwn Capabilities (4)	Hardware Addition	Exploitation for Client Execution	Boot or Logon (1) Malicious Script (5)	Boot or Logon (1) Malicious Script (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Flooding (2)	Cyberlock Over Network Protocol (3)	Data Manipulation (2)
Gather Victim Org Information (4)	Establish Accounts (3)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Deny/Authorize/Deceive File or Information	Debugger Evasion	Escaped Authentication	Cloud Service Dashboard	Remote Services (2)	Browser Session Hijacking	Denial of Service (3)	Cyberlock Over Web Service (2)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (3)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Deploy Container	Evade Web Content (2)	Cloud Service Discovery	Application Through Removable Media	Clipboard Data	Deny/Authorize/Deceive File or Information (3)	Cyberlock Over Web Service (2)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (3)	Supply Chain Compromise (3)	Scheduled Task Job (3)	Create or Modify System Process (4)	Domain Policy Modification (2)	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypt/Decrypt (2)	Encrypted Content (2)	Endpoint Denial of Service (4)
Search Open Technical Data Sets (2)	Stage Capabilities (3)	Trusted Relationship	Scheduled Task Job (3)	Create or Modify System Process (4)	Event Triggered Execution (14)	Domain Policy Modification (2)	Mobile Authentication Process (2)	Container and Resource Discovery	Tool Shared Content	Data from Configuration Repository (2)	Fallback Channels	Exfiltration Over Physical Medium (1)	Firmware Corruption
Search Open Websites/Domains (3)		Valid Accounts (4)	Serverless Execution	Event Triggered Execution (14)	Escape to Host	Execution Guardrails (1)	Multi-Factor Authentication Interception	Debugger Evasion	Tool Shared Content	Data from Local System	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Incident System Recovery
Search Victim-Owned Websites			Short Modules	External Remote Services	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	File and Directory Discovery	Use and Directory Discovery	Gate from Network Shared Drive	Multi-Stage Channels	Scheduled Transfer	Network Denial of Service (2)
			Software Deployment Tools	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Hide Artifacts (10)	Network Shifting	File and Directory Modification (2)	File and Directory Modification (2)	Gate from Remote Media	Non-Application Layer Protocol	Transfer Data to Cloud Account	Resource Hijacking
			System Services (2)	Inject Internal Image	Process Injection (12)	Hijack Execution Flow (12)	OS Credential Dumping (3)	Group Policy Discovery	File and Directory Discovery	Gate from Network Shared Drive	Protocol Tunneling		Service Stop
			User Execution (2)	Modify Authentication Process (7)	Inject Command Execution	Inject Command Execution	Password Policy Discovery	Network Service Discovery	File and Directory Discovery	Gate from Removable Media	Proxy (4)		System Shutdown/Reboot
			Windows Management Instrumentation	Office Application Startup (3)	Malware (7)	Malware (7)	Steal Application Cookies	Network Share Discovery	File and Directory Discovery	Gate from Removable Media	Remote Access Software		
				Pre-OS Boot (3)	Modifiable Authentication Process (7)	Modifiable Authentication Process (7)	Steal or Forge Authentication Credentials	Network Sniffing	File and Directory Discovery	Gate from Removable Media	Traffic Signaling (2)		
				Scheduled Task Job (3)	Modifiable Cloud Compute Infrastructure (4)	Modifiable Cloud Compute Infrastructure (4)	Steal or Forge Session Cookies	Network Sniffing	File and Directory Discovery	Gate from Removable Media	Web Service (3)		
				Server Software Component (3)	Modifiable Registry	Modifiable Registry	Unsecure Credentials (2)	Peripheral Device Discovery	File and Directory Discovery	Gate from Removable Media			
				Traffic Signaling (2)	Modifiable System Image (2)	Modifiable System Image (2)		Process Discovery	File and Directory Discovery	Gate from Removable Media			
					Network Boundary Bridging (1)	Network Boundary Bridging (1)		Query Registry	File and Directory Discovery	Gate from Removable Media			
					Obfuscated Files or Information (3)	Obfuscated Files or Information (3)		Remote System Discovery	File and Directory Discovery	Gate from Removable Media			
					Prior File Modification	Prior File Modification		Software Discovery (1)	File and Directory Discovery	Gate from Removable Media			
					Pre-OS Boot (3)	Pre-OS Boot (3)		System Information Discovery	File and Directory Discovery	Gate from Removable Media			
					Process Injection (12)	Process Injection (12)		System Location Discovery (1)	File and Directory Discovery	Gate from Removable Media			
					Reflective Code Loading	Reflective Code Loading		System Network Configuration Discovery (1)	File and Directory Discovery	Gate from Removable Media			
					Regulate Domain Controller	Regulate Domain Controller		System Network Connections Discovery	File and Directory Discovery	Gate from Removable Media			
					Rootkit	Rootkit		System Owner/User Discovery	File and Directory Discovery	Gate from Removable Media			
					Subvert Trust Controls (4)	Subvert Trust Controls (4)		System Service Discovery	File and Directory Discovery	Gate from Removable Media			
					System Binary Proxy Execution (12)	System Binary Proxy Execution (12)		System Time Discovery	File and Directory Discovery	Gate from Removable Media			
					System Serial Proxy Execution (1)	System Serial Proxy Execution (1)		Virtualization/Sandbox Evasion (3)	File and Directory Discovery	Gate from Removable Media			
					Template Injection	Template Injection			File and Directory Discovery	Gate from Removable Media			
					Traffic Signaling (2)	Traffic Signaling (2)			File and Directory Discovery	Gate from Removable Media			
					Trusted Developer Utilities Proxy Execution (1)	Trusted Developer Utilities Proxy Execution (1)			File and Directory Discovery	Gate from Removable Media			
					Unapproved/Unsupported Trust Negotiation	Unapproved/Unsupported Trust Negotiation			File and Directory Discovery	Gate from Removable Media			
					Use Alternative Authentication Material (4)	Use Alternative Authentication Material (4)			File and Directory Discovery	Gate from Removable Media			
					Valid Accounts (4)	Valid Accounts (4)			File and Directory Discovery	Gate from Removable Media			
					Virtualization/Sandbox Evasion (3)	Virtualization/Sandbox Evasion (3)			File and Directory Discovery	Gate from Removable Media			
					Weaken Encryption (2)	Weaken Encryption (2)			File and Directory Discovery	Gate from Removable Media			
					XML Script Processing	XML Script Processing			File and Directory Discovery	Gate from Removable Media			

# Endpoint Protection

## ➡ Mitre Attack Matrix

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 12 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 10 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (3)	Account Manipulation (3)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exploitation (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public-Facing Application	Compiler Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communications Through Removable Media	Data Transfer Size Limit	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Subsequent Execution (14)	Boot or Logon Subsequent Execution (14)	BITS Jobs	Credentials from Password Stores (3)	Browser Bookmark Discovery	Keylog Tool (ransack)	Audio Capture	Data Encoding (2)	Exploitation Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (4)	Green/Grey Capabilities (4)	Hardware Addition	Exploitation for Client Execution	Boot or Logon Subsequent Execution (14)	Boot or Logon Subsequent Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exploitation Over OS Channel	Data Manipulation (2)
Gather Victim Org Information (4)	Establish Accounts (3)	Phishing (7)	Inter-Process Communication (5)	Browser Extensions	Boot or Logon Subsequent Execution (14)	Debugger Evasion	Keypair Authentication	Cloud Service Dashboard	Remote Service Hijacking (2)	Automated Collection	Dynamic Address (3)	Exploitation Over Physical Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (3)	Application Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Dehydration/Decore File or Information	Forge Web Credentials (3)	Cloud Service Discovery	Remote Service Hijacking (2)	Automated Collection	Encrypted Channel (2)	Exploitation Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (3)	Trusted Relationship	Scheduled Task/Job (5)	Create or Modify System Process (4)	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Clipboard Data	Keys from Cloud Storage	Exploitation Over Physical Medium (1)	Encrypted Denial of Service (4)
Search Open Technical Databases (2)		Valid Accounts (4)	Serverless Execution	Event Triggered Execution (14)	Domain Policy Modification (2)	Direct Volume Access	Modify Authentication Process (7)	Container and Resource Discovery	Use Alternative Authentication Material (4)	Data from Cloud Storage	Keys from Configuration Repository (2)	Exploitation Over Physical Medium (1)	Firmware Corruption
Search Open Websites/Domains (3)			Shared Modules	External Remote Services	Escape to Host	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion		Data from Local System	Keys from Network Shared Drive	Inhibit System Recovery	
Search Victim-Owned Websites			Software Deployment Tools	Hijack Execution Flow (12)	Exploitation for Privilege Escalation	Execution Quantities (1)	Multi-Factor Authentication Request Interception	Domain Trust Discovery		Data from Network Shared Drive	Keys from Remote Media	Network Denial of Service (2)	Service Stop
			System Services (2)	Inject into Internal Image		Exploitation for Defense Evasion	Multi-Factor Authentication Request Interception	File and Directory Discovery		Data from Remote Media	Non-Application Layer Protocol	Scheduled Transfer	Resource Hijacking
			Jar Execution (3)	Process Injection (12)		File and Directory Permissions Modification (2)	OS Credential Dumping (8)	Group Policy Discovery		Data Staged (2)	Non-Standard Port	Protocol Tunneling	System Shutdown/Reboot
			Windows Management Instrumentation	Scheduled Task/Job (5)		Hide Artifacts (16)	Steal Application Access Token	Network Service Discovery		Email Collection (3)	Proxy (4)		
				Valid Accounts (4)		Hijack Execution Flow (12)	Steal or Forge Authentication Credentials	Network Share Discovery		Input Capture (4)	Regiole Access Software		
						Process Injection (12)	Steal or Forge Session Cookies	Network Sniffing		Screen Capture	Traffic Signaling (2)		
						Inject Command Execution	Unsecured Credentials (3)	Password Policy Discovery		Video Capture	Web Service (3)		
						Masking (7)		Peripheral Device Discovery					
						Modify Authentication Process (7)		Permission Groups Discovery (3)					
						Modify Cloud Compute Infrastructure (4)		Process Discovery					
						Modify Registry		Query Registry					
						Modify System Image (2)		Remote System Discovery					
						Network Boundary Bridging (1)		Software Discovery (5)					
						Obfuscated Files or Information (3)		System Information Discovery					
						Print File Modification		System Location Discovery (1)					
						Pre-OS Boot (3)		System Network Configuration Discovery (1)					
						Process Injection (12)		System Network Connections Discovery					
						Reflective Code Loading		System Owner/User Discovery					
						Regiole Domain Controller		System Service Discovery					
						Reorder		System Time Discovery					
						Subvert Trust Controls (6)		Virtualization/Sandbox Evasion (3)					
						System Binary Proxy Execution (13)							
						System Script Proxy Execution (1)							
						Template Injection							
						Traffic Signaling (2)							
						Trusted Developer Utilities Proxy Execution (1)							
						Unusual/Unapproved Root Registry							
						Use Alternative Authentication Material (4)							
						Valid Accounts (4)							
						Virtualization/Sandbox Evasion (3)							
						Weaken Encryption (2)							
						API Script Processing							

Last modified: 01 April 2022

