

➡ Historic anti-virus - signature based detection

→ Heristic and heuristic based deduction

➡ Implemented as an extension to the kernel often with user-space components

➡ Passive or Active mode, event logging and streaming

➡ Often featuring a cloud component for incident investigation
and security overview



Still software when can be maintained vulnerabilities

Endpoint Protection

Endpoint Protection

- ➡ Historic anti-virus - signature based detection
- ➡ Heuristics and behavioural based detection
- ➡ Implemented as an extension to the kernel often with user-space components
- ➡ Passive or Active mode, event logging and streaming
- ➡ Often featuring a cloud component for incident investigation and security overview
- ➡ Still software hence can be contain vulnerabilities

Endpoint Protection

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	13 techniques	12 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	17 techniques	10 techniques	9 techniques	13 techniques
Active Scanning (3)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (8)	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 Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (5)	Exploit Publishing Application	Compromise Administrative Command	RITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	First Force (4)	Application Window Discovery	Internal Spoofing	Archive Collected Data (5)	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 (Automatic Execution) (14)	Boot or Logon (Automatic Execution) (14)	Boot or Logon (Automatic Execution) (14)	Credential from Saved Stores (3)	Browser Bookmark Discovery	Local Tool Transfer	Audio Capture		Cybertron Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (4)	Enumerate Capabilities (4)	Hardware Addition	Exploitation for Client Execution	Boot or Logon (Manual Script) (5)	Boot or Logon (Manual Script) (5)	Boot or Logon (Manual Script) (5)	Exploitation for Critical Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection		Data Manipulation (2)	Data Manipulation (2)
Gather Victim Org Information (4)	Establish Accounts (5)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Deepfake/Device File or Information	Deepfake/Device File or Information	Escaped Authentication	Cloud Service Dashboard	Remote Session Hijacking	Browser Session Hijacking		Defacement (2)	
Enabling for Information (3)	Enumerate Capabilities (4)	Application Through Removable Media	Native API	Domain Name System Binary	Deploy Container	Deploy Container	Escape Web Credentials (2)	Cloud Service Discovery	Remote Services (2)	Clipboard Data		Exploitation Over Other Network Medium (1)	Disc Wipe (2)
Search Closed Sources (2)	Stage Capabilities (4)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Domain Account (3)	Direct Volume Access	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Application Through Removable Media	Data from Cloud Storage		Exploitation Over Physical Medium (1)	Encrypted Denial of Service (4)
Search Open Technical Datafeeds (5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (4)	Domain Policy Modification (2)	Domain Policy Modification (2)	Modify Authentication Process (2)	Container and Resource Discovery	Software Deployment Tools	File from Cloud Storage		Exploitation Over Physical Medium (1)	Firmware Corruption
Search Open Websites/Domains (3)		Valid Accounts (4)	Shared Modules	Event Triggered Execution (14)	Escape to Host	Escape to Host	Multi-Factor Authentication Interception	Debugger Evasion	Tool Shared System	File from Local Storage		Exploitation Over Web Service (2)	Inhibit System Recovery
Search Victim Owned Websites			Software Deployment Tools	External Remote Services	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Multi-Factor Authentication Interception	Domain Trust Discovery	Use Alternative Authentication Material (4)	File and Directory Discovery		Non-Application Layer Protocol	Resource Hijacking
			System Services (7)	Hijack Execution Flow (12)	File and Directory Discovery	File and Directory Discovery	Multi-Factor Authentication Request Correlation	EIC and Directory Discovery		Group Policy Discovery		Non-Standard Port	Service Stop
			Java Execution (2)	Implement Internal Image	Hide Artifacts (10)	Hide Artifacts (10)	Network Shifting	Network Service Discovery		Network Share Discovery		Protocol Tunneling	System Shutdown/Reboot
			Windows Management Instrumentation	Modify Authentication Process (7)	Hijack Execution Flow (12)	Hijack Execution Flow (12)	OS Credential Dumping (8)	Network Sniffing		Network Sniffing		Proxy (4)	
				Office Application Startup (6)	Indicator Removal (4)	Indicator Removal (4)	Password Policy Discovery	Peripheral Device Discovery		Password Policy Discovery		Remote System Discovery	
				Pre-OS Boot (5)	Indirect Command Execution	Indirect Command Execution	Peripheral Device Discovery	Permissions Groups Discovery (3)		Peripheral Device Discovery		Remote System Discovery	
				Scheduled Task/Job (5)	Masking (7)	Masking (7)	Process Discovery	Process Groups Discovery (3)		Process Discovery		Remote System Discovery	
				Server Software Component (5)	Modifiable Authentication Process (7)	Modifiable Authentication Process (7)	Query Registry	Remote System Discovery		Query Registry		Remote System Discovery	
				Traffic Signaling (2)	Modifiable Cloud Compute Infrastructure (4)	Modifiable Cloud Compute Infrastructure (4)	Steal or Forge Authentication Material (4)	Software Discovery (5)		Remote System Discovery		Remote System Discovery	
				Valid Accounts (4)	Modifiable Registry	Modifiable Registry	Steal Web Session Cookies	System Information Discovery		System Information Discovery		Remote System Discovery	
					Modifiable System Image (2)	Modifiable System Image (2)	Unsecured Credentials (2)	System Location Discovery		System Location Discovery		Remote System Discovery	
					Network Boundary Bridging (1)	Network Boundary Bridging (1)		System Network Configuration Discovery (1)		System Network Configuration Discovery (1)		Remote System Discovery	
					Obfuscated Files or Information (3)	Obfuscated Files or Information (3)		System Network Connections Discovery		System Network Connections Discovery		Remote System Discovery	
					Plan File Modification	Plan File Modification		System Owner/Admin Discovery		System Owner/Admin Discovery		Remote System Discovery	
					Pre-OS Boot (5)	Pre-OS Boot (5)		System Service Discovery		System Service Discovery		Remote System Discovery	
					Process Injection (12)	Process Injection (12)		System Time Discovery		System Time Discovery		Remote System Discovery	
					Reflective Code Loading	Reflective Code Loading		Virtualization/Sandbox Evasion (3)		Virtualization/Sandbox Evasion (3)		Remote System Discovery	
					Regio Domain Controller Router	Regio Domain Controller Router						Remote System Discovery	
					Subvert Trust Controls (6)	Subvert Trust Controls (6)						Remote System Discovery	
					Symlink Binary Proxy Execution (13)	Symlink Binary Proxy Execution (13)						Remote System Discovery	
					Symlink Script Proxy Execution (1)	Symlink Script Proxy Execution (1)						Remote System Discovery	
					Template Injection	Template Injection						Remote System Discovery	
					Traffic Signaling (2)	Traffic Signaling (2)						Remote System Discovery	
					Trusted Developer Utilities Proxy Execution (1)	Trusted Developer Utilities Proxy Execution (1)						Remote System Discovery	
					Unused/Unsupported Cloud Region	Unused/Unsupported Cloud Region						Remote System Discovery	
					Use Alternative Authentication Material (4)	Use Alternative Authentication Material (4)						Remote System Discovery	
					Valid Accounts (4)	Valid Accounts (4)						Remote System Discovery	
					Virtualization/Sandbox Evasion (3)	Virtualization/Sandbox Evasion (3)						Remote System Discovery	
					Weaken Encryption (2)	Weaken Encryption (2)						Remote System Discovery	
					WSA Script Processing	WSA Script Processing						Remote System Discovery	

Last modified: 01 April 2022