



➡ 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 identified 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 Administrator Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	First Form (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)	Credentials from Password Stores (5)	Browser Bookmark Discovery	Local Tool Transfer	Audio Capture	Data Encoding (2)	Cybercrime Over Alternative Protocol (1)	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	Stomper Session Hijacking	Data Manipulation (2)	Data Manipulation (2)
Gather Victim Org Information (4)	Establish Accounts (5)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Deepfake/Deepfake File or Information	Deepfake/Deepfake File or Information	Escaped Authentication	Cloud Service Dashboard	Remote Service Session Hijacking (2)	Stomper Session Hijacking	Clipboard Data	Deny or Abuse (3)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Supply Chain Compromise (3)	Native API	Domain Name System Binary	Create or Modify System Process (4)	Create or Modify System Process (4)	Escape Web Credentials (2)	Cloud Storage Object Discovery	Remote Services (2)	Copy from Cloud Storage	Encrypted Channel (2)	Exploitation Over Out-of-Band Channel	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (6)	Trusted Relationship	Scheduled Task/Job (5)	Domain Account (3)	Domain Policy Modification (2)	Domain Policy Modification (2)	Input Capture (4)	Container and Resource Discovery	Application Through Removable Media	Copy from Configuration Repository (2)	Fail-back Channels	Exploitation Over Physical Medium (1)	Firmware Corruption
Search Open Technical Datafeeds (5)			Serverless Execution	Create or Modify System Process (4)	Domain Policy Modification (2)	Domain Policy Modification (2)	Modify Authentication Process (2)	Debugger Evasion	Software Deployment Tools	Cybercrime Over Web Service (2)	Ignore Tool Transfer	Exploitation Over Web Service (2)	Network Denial of Service (2)
Search Open Websites/Domains (3)		Valid Accounts (4)	Shared Modules	Event Triggered Execution (14)	Event Triggered Execution (14)	Event Triggered Execution (14)	Multi-Factor Authentication Information	Domain Trust Discovery	Tool Shared Content	Cybercrime Over Web Service (2)	Multi-Stage Channels	Scheduled Transfer	Resource Hijacking
Search Victim Owned Websites			Software Deployment Tool	External Remote Services	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Multi-Factor Authentication Request Correlation	File and Directory Discovery	Use Alternative Authentication Material (4)	Cybercrime Over Web Service (2)	Non-Application Layer Protocol	Transfer Data to Cloud Account	System Shutdown/Reboot
			System Services (2)	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Multi-Factor Authentication Request Correlation	Group Policy Discovery		Cybercrime Over Web Service (2)	Non-Standard Port		
			User Execution (2)	Process Injection (12)	Process Injection (12)	Process Injection (12)	OS Credential Dumping (8)	Network Service Discovery		Cybercrime Over Web Service (2)	Protocol Tunneling		
			Windows Management Instrumentation	Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Share Discovery		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		
				Process Injection (12)	Process Injection (12)	Process Injection (12)	Indicator Removal (5)	Network Sniffing		Cybercrime Over Web Service (2)	Proxy (4)		

Last modified: 01 April 2022