

Deloitte.



ATT&CK coverage assessment  
from a data perspective

Google Earth

# PS C:> whoami

---



Olaf Hartong  
Blue Team Specialist Leader

---

Currently having fun @

**Deloitte.**

## ABOUT ME

12+ years in Info Security

Consulted at banks, educational institutions and governmental organizations

- Built and/or led Security Operations Centers
- Threat hunting, IR and Compromise assessment engagements
- SOC Maturity engagements

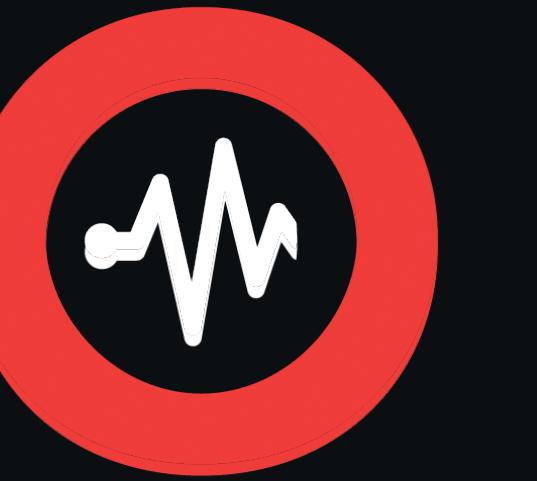
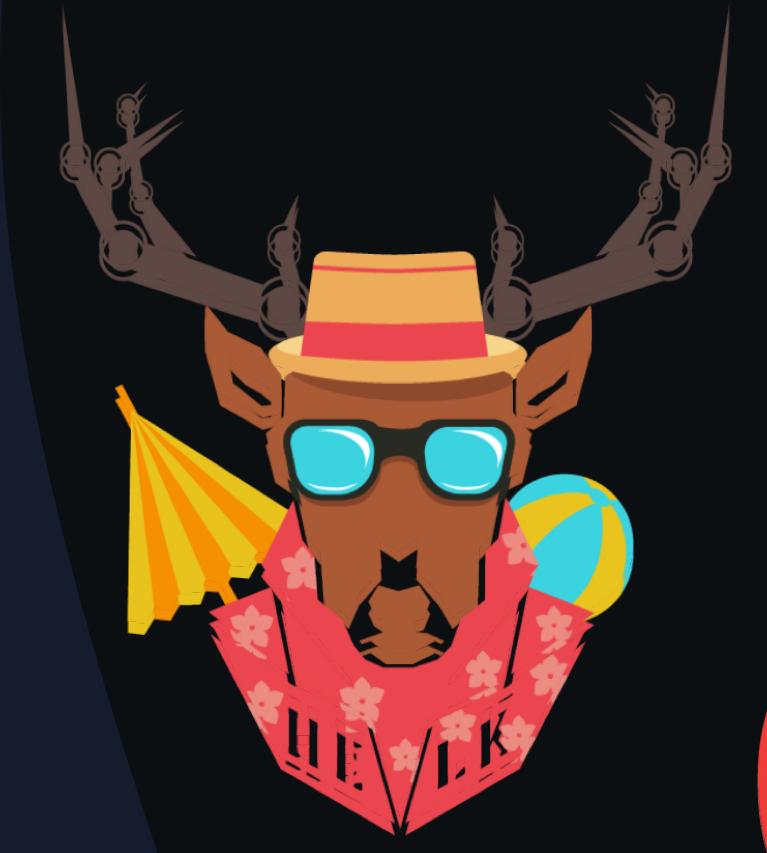
Documentary photographer

- 🐦 @olafhartong
- 🐱 github.com/olafhartong
- ✉️ ohartong@deloitte.nl
- 🌐 medium.com/@olafhartong

# MITRE ATT&CK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction	
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact	Data Encrypted	
External Remote Services	Compiled HTML File	AppCert DLLs	Accessibility Features	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Clipboard Data	Connection Proxy	Defacement	Data Encrypted	
Hardware Additions	Control Panel Items	Appln DLLs	AppCert DLLs	Bypass User Account Control	Credentials in Files	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Registry	File and Directory Discovery	File and Directory Discovery	Data from Local System	Exfiltration Over Alternative Protocol	Disk Content Wipe	
Spearphishing Attachment	Execution through API	Authentication Package	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Disk Structure Wipe	
Spearphishing Link	Execution through Module Load	BITS Jobs	BITS Jobs	Compile After Delivery	Forced Authentication	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Encoding	Endpoint Denial of Service	
Spearphishing via Service	Exploitation for Client Execution	Bootkit	DLL Search Order Hijacking	Compiled HTML File	Hooking	Network Sniffing	Pass the Ticket	Remote Desktop Protocol	Data Obfuscation	Firmware Corruption	
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Component Firmware	Component Object Model Hijacking	Component Firmware	Peripheral Device Discovery	Pass the Hash	Data Staged	Inhibit System Recovery	Exfiltration Over Other Network Medium	
Trusted Relationship	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Permission Groups Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Network Denial of Service	
Valid Accounts	LSASS Driver	Component Object Model Hijacking	DCShadow	Deobfuscate/Decode Files or Information	Input Prompt	Process Discovery	Remote Services	Input Capture	Exfiltration Over Physical Medium	Resource Hijacking	
	Mshta	File System Permissions Weakness	LLMNR/NBT-NS Poisoning and Relay	Network Sniffing	Kerberoasting	Query Registry	Replication Through Removable Media	Man in the Browser	Fallback Channels	Scheduled Transfer	
	PowerShell	Create Account	Network Sniffing	Network Sniffing	Process Discovery	Remote System Discovery	Shared Webroot	Screen Capture	Multi-hop Proxy	Runtime Data Manipulation	
	Regsvcs/Regasm	DLL Search Order Hijacking	Obfuscating Security Tools	Obfuscating Security Tools	Remote System Discovery	Security Software Discovery	Taint Shared Content	Video Capture	Multi-Stage Channels	Service Stop	
	Regsvr32	External Remote Services	Image File Execution Options Injection	>Password Filter DLL	System Information Discovery	Third-party Software			Multiband Communication	Stored Data Manipulation	
	Rundll32	File System Permissions Weakness	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Admin Shares			Multilayer Encryption	Transmitted Data Manipulation	
	Scheduled Task	Hidden Files and Directories	Path Interception	Two-Factor Authentication Interception	System Network Connections Discovery	Windows Remote Management			Remote Access Tools	Remote File Copy	
	Scripting	Port Monitors	Execution Guardrails							Standard Application Layer Protocol	
	Service Execution	Exploitation for Defense Evasion								Standard Cryptographic Protocol	
	Signed Binary Proxy Execution	Process Injection	Extra Window Memory Injection							Standard Non-Application Layer Protocol	
	Signed Script Proxy Execution	Hypervisor	Scheduled Task							Uncommonly Used Port	
	Third-party Software	Image File Execution Options Injection	Service Registry Permissions Weakness							Web Service	
	Trusted Developer Utilities	Logon Scripts	SID-History Injection								
	User Execution	LSASS Driver	Group Policy Modification								
	Windows Management Instrumentation	Valid Accounts	Hidden Files and Directories								
	Windows Remote Management	Modify Existing Service	Image File Execution Options Injection								
	XSL Script Processing	Web Shell	Indicator Blocking								
		Netsh Helper DLL	Indicator Removal from Tools								
		New Service	Indicator Removal on Host								
		Office Application Startup	Indirect Command Execution								
		Path Interception	Install Root Certificate								
		Port Monitors	InstallUtil								
		Redundant Access	Masquerading								
		Registry Run Keys / Startup Folder	Modify Registry								
		Scheduled Task	Mshta								
		Screensaver	Network Share Connection Removal								
		Security Support Provider	NTFS File Attributes								
		Service Registry Permissions Weakness	Obfuscated Files or Information								
		Shortcut Modification	Process Doppelgänging								
		SIP and Trust Provider Hijacking	Process Hollowing								
		System Firmware	Process Injection								
		Time Providers	Redundant Access								
		Valid Accounts	Regsvcs/Regasm								
		Web Shell	Regsvr32								
		Windows Management Instrumentation Event Subscription	Rootkit								
		Winlogon Helper DLL	Rundll32								
		Scripting	Scripting								
		Signed Binary Proxy Execution	Signed Binary Proxy Execution								
		Signed Script Proxy Execution	Signed Script Proxy Execution								
		SIP and Trust Provider Hijacking	SIP and Trust Provider Hijacking								
		Software Packing	Software Packing								
		Template Injection	Template Injection								
		Timestomp	Timestomp								
		Trusted Developer Utilities	Trusted Developer Utilities								
		Valid Accounts	Virtualization/Sandbox Evasion								
		Web Service	Web Service								
		XSL Script Processing	XSL Script Processing								

'erage



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction	
Explore Public-Facing Application	Command-Line Interface	Account Manipulation	Binary Padding	Brute Force	Application Window Discovery	Application Window Discovery	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact	
External Remote Services	Compiled HTML File	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data				Defacement
Hardware Additions	Control Panel Items	Applnit DLLs	AppCert DLLs	Credentials in Files	Domain Trust Discovery	File and Directory Discovery	File and Directory Discovery	Data from Information Repositories	Connection Proxy	Custom Command and Control Protocol	Disk Content Wipe
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Registry	File and Directory Discovery	File and Directory Discovery	Data from Local System	Custom Cryptographic Protocol	Custom Command and Control Protocol	Endpoint Denial of Service
Spearphishing Attachment	Execution through API	Authentication Package	Bypass User Account Control	Code Signing	Exploitation for Credential Access	File and Directory Discovery	File and Directory Discovery	Data from Network Shared Drive	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Firmware Corruption
Spearphishing Link	Execution through Module Load	BITS Jobs	Bootkit	Compiled HTML File	Forced Authentication	File and Directory Discovery	File and Directory Discovery	Data from Removable Media	Data Encoding	Exfiltration Over Command and Control Channel	Inhibit System Recovery
Spearphishing via Service	Exploitation for Client Execution	Browser Extensions	DLL Search Order Hijacking	Component Firmware	Hooking	File and Directory Discovery	File and Directory Discovery	Data Obfuscation	Domain Fronting	Exfiltration Over Other Network Medium	Network Denial of Service
Supply Chain Compromise	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	File and Directory Discovery	File and Directory Discovery	Email Collection	Domain Generation Algorithms	Exfiltration Over Physical Medium	Resource Hijacking
Trusted Relationship	InstallUtil	Component Firmware	Extra Window Memory Injection	Control Panel Items	Kerberoasting	File and Directory Discovery	File and Directory Discovery	Domain Generation Algorithms	Fallback Channels	Exfiltration Over Physical Medium	Routine Data Manipulation
	LSASS Driver	Component Object Model Hijacking	DCShadow	Deobfuscate/Decode Files or Information	Input Prompt	File and Directory Discovery	File and Directory Discovery	Domain Generation Algorithms	Multi-hop Proxy	Exfiltration Over Physical Medium	Service Stop
	Mshta	Create Account	File System Permissions Weakness	Deobfuscate/Decode Files or Information	Network Sniffing	File and Directory Discovery	File and Directory Discovery	Domain Generation Algorithms	Multi-Stage Channels	Exfiltration Over Physical Medium	Stored Data Manipulation
	PowerShell		Hooking	Disabling Security Tools	Network Sniffing	File and Directory Discovery	File and Directory Discovery	Domain Generation Algorithms	Multiband Communication	Exfiltration Over Physical Medium	Transmitted Data Manipulation
			DLL Search Order Hijacking	Image File Execution Options Injection	Network Sniffing	File and Directory Discovery	File and Directory Discovery	Domain Generation Algorithms	Multilayer Encryption	Exfiltration Over Physical Medium	
	Regsvcs/Regasm		External Remote Services	DLL Search Order Hijacking	Network Sniffing	File and Directory Discovery	File and Directory Discovery	Domain Generation Algorithms	Remote Access Tools	Exfiltration Over Physical Medium	
	Regsvr32			New Service	Network Sniffing	File and Directory Discovery	File and Directory Discovery	Domain Generation Algorithms	Remote File Copy	Exfiltration Over Physical Medium	
	Rundll32	File System Permissions Weakness		DLL Side-Loading	Network Sniffing	File and Directory Discovery	File and Directory Discovery	Domain Generation Algorithms	Standard Application Layer Protocol	Exfiltration Over Physical Medium	
	Scheduled Task			Execution Guardrails	Network Sniffing	File and Directory Discovery	File and Directory Discovery	Domain Generation Algorithms	Standard Cryptographic Protocol	Exfiltration Over Physical Medium	
	Scripting	Hidden Files and Directories		Port Monitors	Network Sniffing	File and Directory Discovery	File and Directory Discovery	Domain Generation Algorithms	Standard Non-Application Layer Protocol	Exfiltration Over Physical Medium	
	Service Execution			Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery	File and Directory Discovery	Domain Generation Algorithms	Uncommonly Used Port	Exfiltration Over Physical Medium	
	Signed Binary Proxy Execution			Process Injection	Network Sniffing	File and Directory Discovery	File and Directory Discovery	Domain Generation Algorithms	Web Service	Exfiltration Over Physical Medium	
	Signed Script Proxy Execution			Extra Window Memory Injection	Network Sniffing	File and Directory Discovery	File and Directory Discovery	Domain Generation Algorithms		Exfiltration Over Physical Medium	
	Third-party Software			Scheduled Task	File Deletion	File and Directory Discovery	File and Directory Discovery	Domain Generation Algorithms		Exfiltration Over Physical Medium	
	Trusted Developer Utilities				Service Registry Permissions Weakness	File and Directory Discovery	File and Directory Discovery	Domain Generation Algorithms		Exfiltration Over Physical Medium	
	Logon Scripts				SID-History Injection	File and Directory Discovery	File and Directory Discovery	Domain Generation Algorithms		Exfiltration Over Physical Medium	
	LSASS Driver				Valid Accounts	File and Directory Discovery	File and Directory Discovery	Domain Generation Algorithms		Exfiltration Over Physical Medium	
	User Execution				Web Shell	File and Directory Discovery	File and Directory Discovery	Domain Generation Algorithms		Exfiltration Over Physical Medium	
	Windows Management Instrumentation					Image File Execution Options Injection	Image File Execution Options Injection	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Indicator Blocking	Indicator Blocking	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Indicator Removal from Tools	Indicator Removal from Tools	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Indicator Removal on Host	Indicator Removal on Host	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Indirect Command Execution	Indirect Command Execution	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Install Root Certificate	Install Root Certificate	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						InstallUtil	InstallUtil	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Masquerading	Masquerading	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Modify Registry	Modify Registry	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Mshta	Mshta	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Network Share Connection Removal	Network Share Connection Removal	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						NTFS File Attributes	NTFS File Attributes	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Obfuscated Files or Information	Obfuscated Files or Information	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Process Doppelgänging	Process Doppelgänging	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Process Hollowing	Process Hollowing	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Process Injection	Process Injection	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Redundant Access	Redundant Access	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Regsvcs/Regasm	Regsvcs/Regasm	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Regsvr32	Regsvr32	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Rootkit	Rootkit	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Rundll32	Rundll32	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Scripting	Scripting	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Signed Binary Proxy Execution	Signed Binary Proxy Execution	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Signed Script Proxy Execution	Signed Script Proxy Execution	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						SIP and Trust Provider Hijacking	SIP and Trust Provider Hijacking	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Software Packing	Software Packing	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Template Injection	Template Injection	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Timestamp	Timestamp	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Developer Utilities	Developer Utilities	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Entitlements	Entitlements	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless Persistence	Fileless Persistence	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless Payload	Fileless Payload	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless Script	Fileless Script	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless Template	Fileless Template	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless XML	Fileless XML	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless ZIP	Fileless ZIP	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless PowerShell	Fileless PowerShell	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless Executable	Fileless Executable	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless DLL	Fileless DLL	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless EXE	Fileless EXE	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless JAR	Fileless JAR	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless ZIP	Fileless ZIP	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless PDF	Fileless PDF	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless Word	Fileless Word	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless Excel	Fileless Excel	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless PPT	Fileless PPT	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless PPS	Fileless PPS	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless PPSX	Fileless PPSX	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless PPTM	Fileless PPTM	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless PPSH	Fileless PPSH	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless PPSH2	Fileless PPSH2	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless PPSH3	Fileless PPSH3	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless PPSH4	Fileless PPSH4	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless PPSH5	Fileless PPSH5	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless PPSH6	Fileless PPSH6	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless PPSH7	Fileless PPSH7	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless PPSH8	Fileless PPSH8	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless PPSH9	Fileless PPSH9	Domain Generation Algorithms		Exfiltration Over Physical Medium	
						Fileless PPSH10	Fileless PPSH10	Domain Generation Algorithms		Exfiltration Over Physical Medium	

# Toolkit



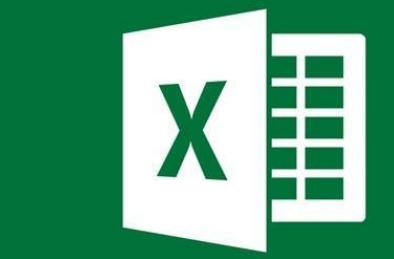
```
[{"name": "DataCoverage", "version": "2.1", "domain": "mitre-enterprise", "description": "2019-05-06", "filters": { "stages": [ "act" ], "platforms": [ "windows", "linux", "mac" ] }, "sorting": 0, "viewMode": 0, "hideDisabled": false, "techniques": [ { "score": 1165, "techniqueID": "T1001", "metadata": [ { "value": "Score: 0", "name": "Packet capture:Moloch" }, { "value": "Score: 45", "name": "Process use of network:Windows:5156" } ] } ] }
```

Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
22 items	17 items	13 items	22 items	9 items	14 items
Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Application Window Discovery	Application Deployment	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
Browser Bookmark Discovery	Software	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Domain Trust Discovery	Distributed Component Object Model	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
File and Directory Discovery	Exploitation of Remote Services	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Network Share Discovery	Pass the Hash	Data from Removable Media	Data Encoding	Data Obfuscation	Firmware Corruption
Network Sniffing					Inhibit System Recovery
Password Policy Discovery	Pass the Ticket				
Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Domain Fronting		
Permission Groups Discovery		Email Collection	Domain Generation Algorithms		
Process Discovery	Remote File Copy	Input Capture	Fallback Channels		
Query Registry	Remote Services	Man in the Browser	Multi-hop Proxy		
Remote System Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		
Security Software Discovery	Shared Webroot	Video Capture	Multiband Communication		
System Information Discovery	SSH Hijacking		Multilayer Encryption		
System Network Configuration Discovery	Taint Shared Content		Port Knocking		
System Network Connections Discovery	Third-party Software		Remote Access Tools		
System Owner/User Discovery	Windows Admin Shares		Remote File Copy		
System Service Discovery	Windows Remote Management		Standard Application Layer Protocol		
System Time Discovery			Standard Cryptographic Protocol		
Virtualization/Sandbox Evasion			Standard Non-Application Layer Protocol		
			Uncommonly Used Port		
			Web Service		

T1001 - Exfiltration Over Other Network Medium  
Metadata:  
Packet capture:Moloch: Score: 0  
Process use of network:Sysmon:3: Score: 120  
Process use of network:Sysmon:17: Score: 120  
Process use of network:Sysmon:18: Score: 120  
Process use of network:Sysmon:19: Score: 120  
Process monitoring:Windows:4688: Score: 25  
Process monitoring:Windows:4689: Score: 25  
Process monitoring:Windows:4690: Score: 125  
Process monitoring:Sysmon:1: Score: 125  
Process monitoring:Sysmon:5: Score: 125  
Process monitoring:Sysmon:8: Score: 125  
Process monitoring:Windows: Scheduled Tasks:100-200: Score: 0  
Process monitoring:Windows: Whitelist:8000-8027: Score: 0  
Network protocol analysis:Bro logging: Score: 125  
Network protocol analysis:PaloAltoTrafficLog: Score: 110



# Toolkit



Excel

ID	Name	Data Source	Platforms	Detection
T1001	Data Obfuscation	Packet capture,Process use of network,Process monitoring,Network protocol analysis	Linux,macOS,Windows	Analyze network data for uncommon data flows (e.g., a client server connection using compressed files) or file metadata.
T1002	Binary file metadata	Binary file metadata,File monitoring,Process command-line parameters,Process monitoring	Windows,Linux,macOS	Check if file metadata (e.g., file size, file type) is expected. If not, analyze file contents.
T1003	Credential Dumping	API monitoring,Process monitoring,PowerShell logs,Process command-line parameters	Windows,Linux,macOS	Monitor for changes to Registry entries associated with Windows services.
T1004	Winlogon Helper DLL	Windows Registry,file monitoring,Process monitoring	Windows	Monitor processes and command-line arguments for actions that affect system startup.
T1005	Data from Local System	File monitoring,Process monitoring,Process command-line parameters	Linux,macOS,Windows	Monitor handle opens on drive volumes that are made by process.
T1006	File System Logical Offsets	API monitoring	Windows	System and network discovery techniques normally occur through logical offsets.
T1007	System Service Discovery	Process monitoring,Process command-line parameters	Linux,Windows,macOS	Monitor for changes to Registry entries associated with Windows services.
T1008	File Padding	Memory reverse engineering,Netflow/Enclave netflow,Packet capture,Process monitoring,Process use of network	Linux,macOS,Windows	Analyze network data for uncommon data flows (e.g., a client server connection using compressed files).
T1009	Binary Padding	Binary file metadata,File monitoring,Malware reverse engineering	Linux,macOS,Windows	Depending on the method used to pad files, a file-based signature may be present.
T1010	Application Window Discovery	API monitoring,Process monitoring,Process command-line parameters	macOS,Windows	System and network discovery techniques normally occur through window titles.
T1011	Exfiltration Over Other Network Medium	User interface,Process monitoring	Linux,macOS,Windows	Processes utilizing the network that do not normally have network access.
T1012	Query Registry	Process monitoring,Process command-line parameters	Windows	System and network discovery techniques normally occur through registry keys.
T1013	Port Monitors	File monitoring,API monitoring,DLL monitoring,Windows Registry,Process monitoring	Windows,Linux,macOS	+ Monitor for port monitoring calls to (Client API) AddPortMonitored.
T1014	Rootkits	BIOS,MBR,system calls	Windows	Some rootkit protection tools will build anti-virus or operating system protection.
T1015	Accessibility Features	Windows Registry,File monitoring,Process monitoring	Windows	Changes to accessibility utility binaries or binary paths that do not normally occur.
T1016	System Configuration Discovery	Process monitoring,Process command-line parameters	Linux,macOS,Windows	System and network discovery techniques normally occur through configuration files.
T1017	Application Deployment Software	File monitoring,Process use of network,Process monitoring	Linux,macOS,Windows	Monitor application deployments from a secondary system. Permalinks.
T1018	Remote System Discovery	Network protocol analysis,Process monitoring,Process use of network,Process command-line parameters	Linux,macOS,Windows	System and network discovery techniques normally occur through network traffic.
T1019	System Configuration Monitoring	Process monitoring,BIOS,EFI	Windows	System configuration monitoring may be present.
T1020	Automated Exfiltration	File monitoring,Process monitoring,Process use of network	Linux,macOS,Windows	Monitor process file access patterns and network behavior.
T1021	Remote Services	Authentication logs	Linux,macOS,Windows	Correlate use of login activity related to remote services with user activity.
T1022	Data Encrypted	File monitoring,Process monitoring,Process command-line parameters,Binary file metadata	Linux,macOS,Windows	Encrypting software and encrypted files can be detected in many ways.
T1023	Shortcut Modification	File monitoring,Process monitoring,Process command-line parameters	Windows	Since a shortcut's target path likely will not change, modification detection is a way of detecting command and control.
T1024	Local Cryptographic Protocol	Packet capture,Netflow/Enclave netflow,Process use of network,Malware reverse engineering,Process monitoring	Linux,macOS,Windows	If malware uses custom cryptographic keys, it may vary.
T1025	Data from Removable Media	File monitoring,Process monitoring,Process command-line parameters	Linux,macOS,Windows	Monitor processes and command-line arguments for actions that affect removable media.
T1026	Multiband Communication	Packet capture,Netflow/Enclave netflow,Process use of network,Malware reverse engineering,Process monitoring	Linux,macOS,Windows	Analyze network data for uncommon data flows (e.g., a client server connection using compressed files).
T1027	Obfuscated Files or Information	Network protocol analysis,Process use of network,File monitoring,Malware reverse engineering,Binary file metadata,Process command-line parameters,Envirion	Linux,macOS,Windows	Detection of file obfuscation is difficult unless artifacts are left behind.
T1028	Windows Remote Management	File monitoring,Authentication logs,Netflow/Enclave netflow,Process monitoring,Process command-line parameters	Windows	Monitor use of WinRM within an environment by tracking service logs.
T1029	Scheduled Transfer	Netflow/Enclave netflow,Process use of network,Process monitoring	Linux,macOS,Windows	Monitor process file access patterns and network behavior.
T1030	Data Transfer Size Limits	Packet capture,Netflow/Enclave netflow,Process use of network,Process monitoring	Linux,macOS,Windows	Analyze network data for uncommon data flows (e.g., a client server connection using compressed files).
T1031	HTTP Header Manipulation	Windows Registry,File monitoring,Process monitoring,Process command-line parameters	Windows	Look for changes to header fields.
T1032	Standard Cryptographic Protocol	Packet capture,Netflow/Enclave netflow,Malware reverse engineering,Process use of network,Process monitoring,SSL/TLS inspection	Linux,macOS,Windows	SSL/TLS inspection is one way of detecting command and control.
T1033	System Owner/User Discovery	File monitoring,Process monitoring,Process command-line parameters	Linux,macOS,Windows	System and network discovery techniques normally occur through system configuration files.
T1034	Path Interception	Windows Registry,Process monitoring,Process command-line parameters	Windows	Monitor file creation for files named after partial directories and file extensions.
T1035	Service Execution	File monitoring,Process monitoring,Process command-line parameters	Windows	Changes to service Registry entries and command-line locations.
T1036	Memory Dumping	Memory dump,Process monitoring,Binary file metadata	Linux,macOS,Windows	Correlate memory dump files with their normal expected locations.
T1037	Logon Scripts	File monitoring,Process monitoring	macOS,Windows	Monitor logon scripts for unusual access by abnormal users or accounts.
T1038	DLL Search Order Hijacking	DLL monitoring,Process monitoring,Process command-line parameters	Windows	Monitor file systems for moving, renaming, replacing, or modifying DLLs.
T1039	Data from Network Shared Drive	File monitoring,Process monitoring,Process command-line parameters	Linux,macOS,Windows	Monitor processes and command-line arguments for actions that affect network shared drives.
T1040	Network Sniffing	Network device logs,Host network interface,Netflow/Enclave netflow,Process monitoring	Linux,macOS,Windows	Detecting the events leading up to sniffing network traffic may be present.
T1041	Endpoint Command and Control Channel	Process monitoring,Process command-line parameters	Linux,macOS,Windows	Detected command and control channels may be present.
T1042	Change Default File Association	Windows Registry,Process monitoring,Process command-line parameters	Windows	Collect and analyze changes to Registry keys that associate file types.
T1043	Commonly Used Port	Packet capture,Netflow/Enclave netflow,Process use of network,Process monitoring	Linux,macOS,Windows	Analyze network data for uncommon data flows (e.g., a client server connection using compressed files).
T1044	File System Permissions Weakness	File monitoring,Services,Process command-line parameters	Windows	Look for changes to binaries and service executables that may result in privilege escalation.
T1045	Software Packing	Binary file metadata	Windows	Use file scanning to look for known software packers or artifacts.
T1046	Network Service Scanning	Netflow/Enclave netflow,Network protocol analysis,Packet capture,Process command-line parameters,Process use of network	Linux,Windows,macOS	System and network discovery techniques normally occur through network traffic.

ID	Data Source	Weight	Datasources	Weights	Items in Refence vs Items in this sheet
T1001	Packet capture,Process use of network,Process monitoring,Network protocol analysis	25,25,25	4	4	0
T1002	Binary file metadata,File monitoring,Process command-line parameters,Process monitoring	20,20,30,30	4	4	
T1003	API monitoring,Process monitoring,PowerShell logs,Process command-line parameters	20,20,30,30	4	4	
T1004	Windows Registry,file monitoring,Process monitoring	50,20,30	3	3	
T1005	File monitoring,Process monitoring,Process command-line parameters	35,30,35	3	3	
T1006	API monitoring	100	1	1	
T1007	Process monitoring,Process command-line parameters	40,60	2	2	
T1008	Malware reverse engineering,Netflow/Enclave netflow,Packet capture,Process monitoring,Process use of network	15,23,22,15,25	5	5	
T1009	Binary file metadata,File monitoring,Malware reverse engineering	33,34,33	3	3	
T1010	API monitoring,Process monitoring,Process command-line parameters	35,25,40	3	3	
T1011	User interface,Process monitoring	49,51	2	2	
T1012	Windows Registry,Process monitoring,Process command-line parameters	30,20,50	3	3	
T1013	File monitoring,API monitoring,DLL monitoring,Windows Registry,Process monitoring	20,20,20,20,20	5	5	
T1014	BIOS,MBR,system calls	20,40,40	3	3	
T1015	Windows Registry,file monitoring,Process monitoring	40,30,30	3	3	
T1016	Process monitoring,Process command-line parameters	40,60	2	2	
T1017	File monitoring,Process use of network,Process monitoring	35,35,30	3	3	
T1018	Network protocol analysis,Process monitoring,Process use of network,Process command-line parameters	30,20,25,25	4	4	
T1019	API monitoring,BIOS,EFI	33,33,34	3	3	
T1020	File monitoring,Process monitoring,Process use of network	35,30,35	3	3	
T1021	Authentication logs	100	1	1	
T1022	File monitoring,Process monitoring,Process command-line parameters,Binary file metadata	40,15,25,20	4	4	
T1023	File monitoring,Process monitoring,Process command-line parameters	35,30,35	3	3	
T1024	Packet capture,Netflow/Enclave netflow,Process use of network,Malware reverse engineering,Process monitoring	20,20,20,20,20	5	5	
T1025	File monitoring,Process monitoring,Process command-line parameters	35,30,35	3	3	
T1026	Packet capture,Netflow/Enclave netflow,Process use of network,Malware reverse engineering,Process monitoring	20,20,20,20,20	5	5	
T1027	Network protocol analysis,Process use of network,File monitoring,Malware reverse engineering,Binary file metadata,Process command-line parameters,Envirion	8,8,8,8,9,10,9,8,8,8	12	12	
T1028	File monitoring,Authentication logs,Netflow/Enclave netflow,Process monitoring,Process command-line parameters	15,20,20,20,25	5	5	
T1029	Netflow/Enclave netflow,Process use of network,Process monitoring	35,35,30	3	3	
T1030	Packet capture,Netflow/Enclave netflow,Process use of network,Process monitoring	30,20,20,20	4	4	
T1031	Windows Registry,file monitoring,Process monitoring,Process command-line parameters	30,20,20,30	4	4	
T1032	Packet capture,Netflow/Enclave netflow,Malware reverse engineering,Process use of network,Process monitoring,SSL/TLS inspection	20,15,15,15,15,20	6	6	
T1033	File monitoring,Process monitoring,Process command-line parameters	25,25,50	3	3	
T1034	File monitoring,Process monitoring	40,60	2	2	
T1035	Windows Registry,Process monitoring,Process command-line parameters	35,30,35	3	3	
T1036	File monitoring,Process monitoring,Binary file metadata	35,35,30	3	3	

DataSource	Event	Completeness	Timeliness	Availability	Score
Network protocol analysis	Bio logging	5	5	5	5.0
Network protocol analysis	Paloalto,TrafficLog	4	4	5	4.4
Packet capture	Malicious	0	0	0	0.0
PowerShell logs	PowerShell 200-500	0	0	0	0.0
PowerShell logs	PowerShell 4100-4104	0	0	0	0.0
Process command-line parameters	Windows 4688	1	1	1	1.0
Process command-line parameters	Symson:2	5	5	5	5.0
Process command-line parameters	Windows 4688	1	1	1	1.0
Process monitoring	Windows 4689	5	5	5	5.0
Process monitoring	Symson:1	5	5	5	5.0
Process monitoring	Symson:5	5	5	5	5.0
Process monitoring	Symson:8	5	5	5	5.0
Process monitoring	Windows Scheduled Tasks 100-200	0	0	0	0.0
Process monitoring	Windows Whitelist 8000-8027	1	5	1	1.8
Process use of network	Windows 5156	5	4	5	4.8
Process use of network	Symson:3	5	4	5	4.8
Process use of network	Symson:17	5	4	5	4.8
Process use of network	Symson:18	5	4	5	4.8
Sensor health and status	Symson:4	5	5	5	5.0
Sensor health and status	Symson:16	5	5	5	5.0
Sensor health and status	Windows 6005	1	5	5	3.4
Sensor health and status	Windows Defender:1005,1006,1008,1010,2001,2003,2004,3002,5008	0	0	0	0.0
Sensor health and status	Windows 1100	0	0	0	0.0
Services	Windows Firewall:2003	0	0	0	0.0
Services	Windows 7040	0	0	0	0.0
Services	Windows 7045	0	0	0	0.0
SSL/TLS inspection	Palo Alto-ThreatLog	4	5	5	4.6
System calls		0	0	0	0.0
Third-party application logs		0	0	0	0.0
User interface		0	0	0	0.0
VBR		0	0	0	0.0
Windows Error Reporting	Windows:1000,1001				

ID	Data Source	Weight	Datasources	Weights
T1001	Packet capture,Process use of network,Process monitoring,Network protocol analysis	25;25;25;25	4	4
T1002	Binary file metadata,File monitoring,Process command-line parameters,Process monitoring	20;20;30;30	4	4
T1003	API monitoring,Process monitoring,PowerShell logs,Process command-line parameters	20;20;30;30	4	4
T1004	Windows Registry,File monitoring,Process monitoring	50;20;30	3	3
T1005	File monitoring,Process monitoring,Process command-line parameters	35;30;35	3	3
T1006	API monitoring	100	1	1
T1007	Process monitoring,Process command-line parameters	40;60	2	2
T1008	Malware reverse engineering,Netflow/Enclave netflow,Packet capture,Process monitoring,Process use of network	15;23;22;15;25	5	5
T1009	Binary file metadata,File monitoring,Malware reverse engineering	33;34;33	3	3
T1010	API monitoring,Process monitoring,Process command-line parameters	35;25;40	3	3
T1011	User interface,Process monitoring	49;51	2	2
T1012	Windows Registry,Process monitoring,Process command-line parameters	30;20;50	3	3
T1013	File monitoring,API monitoring,DLL monitoring,Windows Registry,Process monitoring	20;20;20;20;20	5	5
T1014	BIOS,MBR,System calls	20;40;40	3	3
T1015	Windows Registry,File monitoring,Process monitoring	40;30;30	3	3
T1016	Process monitoring,Process command-line parameters	40;60	2	2
T1017	File monitoring,Process use of network,Process monitoring	35;35;30	3	3
T1018	Network protocol analysis,Process monitoring,Process use of network,Process command-line parameters	30;20;25;25	4	4
T1019	API monitoring,BIOS,EFI	33;33;34	3	3
T1020	File monitoring,Process monitoring,Process use of network	35;30;35	3	3
T1021	Authentication logs	100	1	1
T1022	File monitoring,Process monitoring,Process command-line parameters,Binary file metadata	40;15;25;20	4	4
T1023	File monitoring,Process monitoring,Process command-line parameters	35;30;35	3	3
T1024	Packet capture,Netflow/Enclave netflow,Process use of network,Malware reverse engineering,Process monitoring	20;20;20;20;20	5	5
T1025	File monitoring,Process monitoring,Process command-line parameters	35;30;35	3	3
T1026	Packet capture,Netflow/Enclave netflow,Process use of network,Malware reverse engineering,Process monitoring	20;20;20;20;20	5	5
T1027	Network protocol analysis,Process use of network,File monitoring,Malware reverse engineering,Binary file metadata,Process command-line parameters,Environment	8;8;8;8;9;10;8;9;8;8;8	12	12
T1028	File monitoring,Authentication logs,Netflow/Enclave netflow,Process monitoring,Process command-line parameters	15;20;20;20;25	5	5
T1029	Netflow/Enclave netflow,Process use of network,Process monitoring	35;35;30	3	3
T1030	Packet capture,Netflow/Enclave netflow,Process use of network,Process monitoring	30;30;20;20	4	4
T1031	Windows Registry,File monitoring,Process monitoring,Process command-line parameters	30;20;20;30	4	4
T1032	Packet capture,Netflow/Enclave netflow,Malware reverse engineering,Process use of network,Process monitoring,SSL/TLS inspection	20;15;15;15;15;20	6	6



DataSource	Event	Completeness	Timeliness	Availability	Score
File monitoring	Windows:4663	0	0	0	0,0
File monitoring	Sysmon:2	2	4	5	3,6
File monitoring	Sysmon:11	2	4	5	3,6
File monitoring	Sysmon:15	2	4	5	3,6
File monitoring	Windows:5140,5145	0	0	0	0,0
Host network interface		0	0	0	0,0
Kernel drivers	Sysmon:6	3	5	5	4,2
Kernel drivers	Windows:5038,6281	0	0	0	0,0
Loaded DLLs	Sysmon:7	3	5	5	4,2
Malware reverse engineering	Cuckoo sandbox	0	0	0	0,0
Malware reverse engineering	Palo Alto:WildFire	3	3	5	3,8
MBR		0	0	0	0,0
Netflow/Enclave netflow		0	0	0	0,0
Network device logs	Palo Alto:DeviceLog	0	0	0	0,0
Network protocol analysis	Bro logging	5	5	5	5,0
Network protocol analysis	PaloAlto:TrafficLog	4	4	5	4,4
Packet capture	Moloch	0	0	0	0,0
PowerShell logs	PowerShell:200-500	0	0	0	0,0
PowerShell logs	PowerShell:4100-4104	0	0	0	0,0
Process command-line parameters	Windows:4688	1	1	1	1,0
Process command-line parameters	Sysmon:1	5	5	5	5,0
Process command-line parameters	Windows:4688	1	1	1	1,0
Process monitoring	Windows:4688	1	1	1	1,0
Process monitoring	Windows:4689	5	5	5	5,0
Process monitoring	Sysmon:1	5	5	5	5,0
Process monitoring	Sysmon:5	5	5	5	5,0
Process monitoring	Sysmon:8	5	5	5	5,0
Process monitoring	Windows Scheduled Tasks:100-200	0	0	0	0,0
Process monitoring	Windows Whitelist:8000-8027	0	0	0	0,0
Process use of network	Windows:5156	1	5	1	1,8
Process use of network	Sysmon:3	5	4	5	4,8
Process use of network	Sysmon:17	5	4	5	4,8
Process use of network	Sysmon:18	5	4	5	4,8
Sensor health and status	Sysmon:4	5	5	5	5,0
Sensor health and status	Sysmon:16	5	5	5	5,0
Sensor health and status	Windows:6005	1	5	5	3,4



# PowerShell script

---

```
function Get-ATTACKdata {  
    <#  
    .SYNOPSIS  
    Downloads the MITRE ATT&CK Enterprise  
    JSON file  
    #>  
  
    function Invoke-ATTACK-UpdateExcel {  
        <#  
        .SYNOPSIS  
        Generates MITRE ATT&CK relevant  
        fields into a table and creates or  
        updates a worksheet in an Excel sheet  
        Requires module ImportExcel, Install  
        it like this PS C:> Install-Module  
        ImportExcel  
        #>
```

```
function Request-ATTACKjson {  
    <#  
    .SYNOPSIS  
    Generates a JSON file to be  
    imported into the ATT&CK Navigator.  
    Based on a template and a filled  
    Excel sheet  
    Requires module ImportExcel,  
    Install it like this PS C:>  
    Install-Module ImportExcel  
    #>
```



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
10 items	27 items	42 items	21 items	53 items	15 items	20 items	15 items	13 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection
Hardware Additions	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Clipboard Data	Data from Information Repositories
Replication Through Removable Media	Control Panel Items	Applnt DLLs	Applnt DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Exploitation of Remote Services	Data from Local System
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Registry	T1214 Score: 2500k Service Scanning	Logon Scripts	Data from Network Share Drive
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Metadata: Network Share Discovery Windows Registry:Windows:4657: Score: 0	Pass the Hash	Data from Removable Media
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Compiled HTML File	Forced Authentication	Registry:Windows:4657: Score: 0	Pass the Ticket	Data Staged
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Component Firmware	Component Object Model Hijacking	Hooking	Windows Registry:Sysmon:12: Score: 0	Remote Desktop Protocol	Email Collection
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Windows Registry:Sysmon:13: Score: 285	Remote File Copy	Input Capture
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Kerberoasting	Peripheral Device Discovery Windows Registry:Sysmon:13: Score: 285	Remote Services	Man in the Browser
	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	LLMNR/NBT-NS Poisoning	Session Groups Windows Registry:Sysmon:14: Score: 285	Replication Through Removable Media	Screen Capture
	Mshta	Component Object Model Hijacking	Hijacking	Deobfuscate/Decode Files or Information	Network Sniffing	Process command-line parameters:Windows:4688: Score: 58	Shared Webroot	Video Capture
	PowerShell	Create Account	Hooking	Disabling Security Tools	Password Filter DLL	Query Registry Process command-line parameters:Sysmon:1: Score: 290	Taint Shared Content	Third-party Software
	Regsvcs/Regasm	DLL Search Order Hijacking	Image File Execution Options Injection	DLL Search Order Hijacking	Private Keys	System Discovery Security Software Discovery	Windows Admin Shares	Windows Remote Management
	Regsvr32	External Remote Services	New Service	DLL Side-Loading	Two-Factor Authentication	Process command-line parameters:Windows:4688: Score: 58		
	Rundll32	File System Permissions Weakness	Path Interception	Exploitation for Defense Evasion	Interception	System Information Discovery Process command-line parameters:Windows:4688: Score: 58		
	Scheduled Task	Hidden Files and Directories	Port Monitors	Extra Window Memory Injection		System Network monitoring:Windows:4688: Configuration Discovery Score: 59		
	Scripting	Hooking	Process Injection	File Deletion		Process system monitoring:Windows:4688: Configuration Discovery Score: 59		
	Service Execution	Hypervisor	Scheduled Task	File Permissions Modification		Process system monitoring:Windows:4689: Configuration Discovery Score: 295		
	Signed Binary Proxy Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	File System Logical Offsets		Process monitoring:Sysmon:1: Score: 295		
	Signed Script Proxy Execution	Logon Scripts	SID-History Injection	Hidden Files and Directories		Process monitoring:Sysmon:5: System Service Discovery Score: 295		
	Third-party Software	LSASS Driver	Valid Accounts	Image File Execution Options Injection		Process monitoring:Sysmon:8: System Service Discovery Score: 295		
	Trusted Developer Utilities	Web Shell		Indicator Blocking		Process monitoring:Sysmon:8: System Service Discovery Score: 295		
	User Execution	Modify Existing Service		Indicator Removal from Tools		Process monitoring:Windows Scheduled Tasks:100-200: Score: 0		
	Windows Management Instrumentation	Netsh Helper DLL		Indicator Removal on Host		Process monitoring:Windows Whitelist:8000-8027: Score: 0		
	Windows Remote Management	New Service		Indirect Command Execution				
	XSL Script Processing	Office Application Startup		Install Root Certificate				
		Path Interception		InstallUtil				
		Port Monitors		Masquerading				

PS C:\Users\homerus\Desktop\attackdatamap> **1s**

Directory: C:\Users\homerus\Desktop\attackdatamap

Mode	LastWriteTime	Length	Name
-----	-----	-----	-----
d----	4/30/2019 8:44 PM		Sample results
-a---	4/30/2019 8:44 PM	2197	ATTACKdatamap.psd1
-a---	4/30/2019 8:44 PM	8653	ATTACKdatamap.psm1
-a---	4/30/2019 8:44 PM	1090	LICENSE
-a---	5/7/2019 1:52 PM	184587	mitre_data_assessment.xlsx
-a---	4/30/2019 8:44 PM	2339	README.md
-a---	4/30/2019 8:44 PM	807	template.json

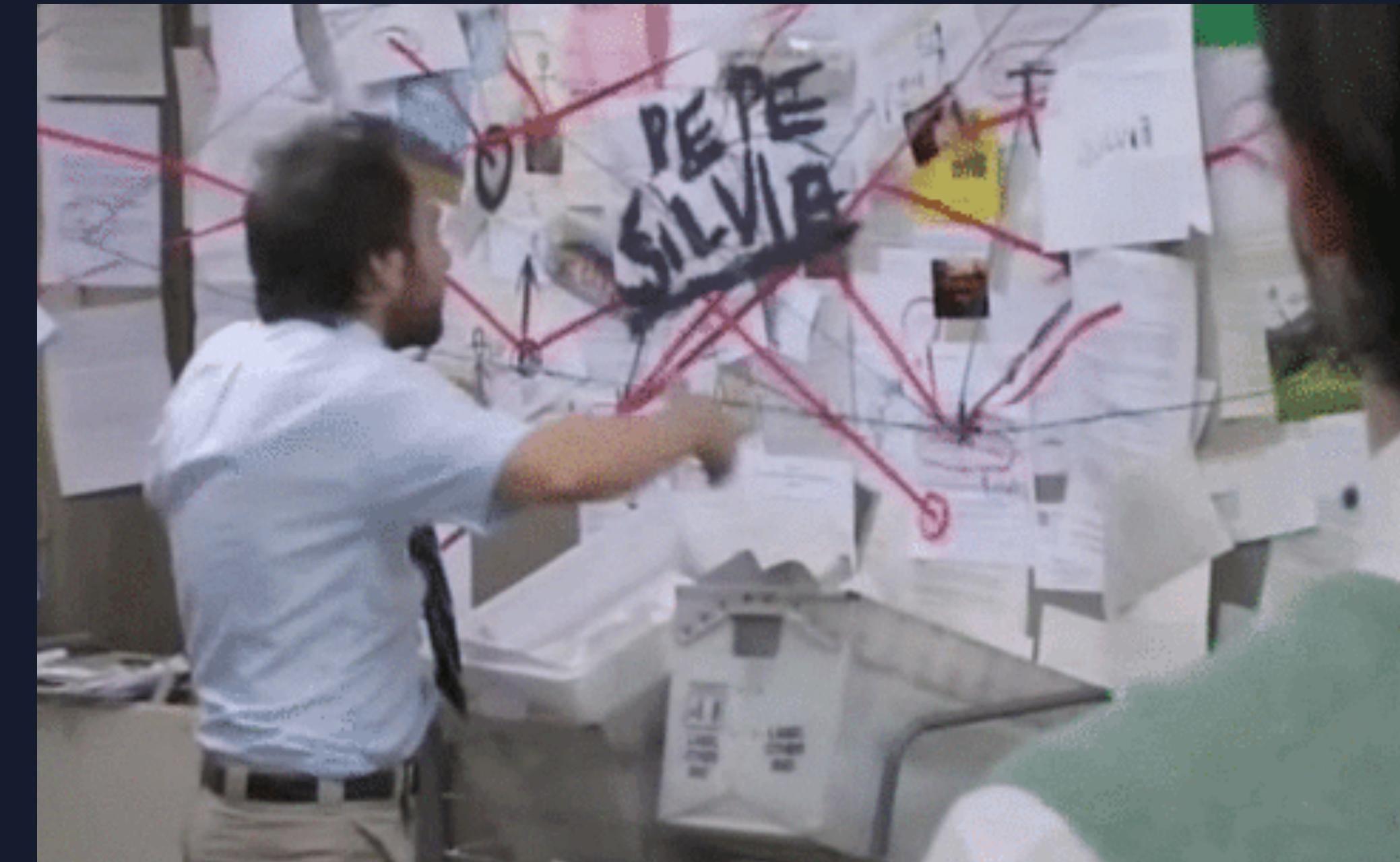
PS C:\Users\homerus\Desktop\attackdatamap&gt;



# ATT&CK Caveats

---

- Be aware that you will NOT be able to cover all techniques with an alerting use case, basically you can dissect them into 3 categories of use;
  - Alerting
  - Hunting
  - Incident Response & Forensics



# Sysmon potential coverage

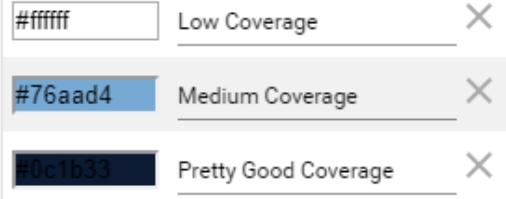


Mind you, this is purely based on its potential.

In practice this will be less due to performance reasons and current configuration limitations.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Manipulation	Binary Padding	Brute Force	Application Window Discovery	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact	Impact
External Remote Services	Compiled HTML File	AppCert DLLs	Accessibility Features	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Defacement	Disk Content Wipe
Hardware Additions	Control Panel Items	Applnit DLLs	AppCert DLLs	Bypass User Account Control	Credentials in Files	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Custom Cryptographic Protocol	Disk Structure Wipe
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	Applnit DLLs	CMSTP	Credentials in Registry	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Command and Control Protocol	Custom Cryptographic Protocol	Endpoint Denial of Service
Spearphishing Attachment	Execution through API	Authentication Package	Application Shimming	Code Signing	Exploitation for Credential Access	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Firmware Corruption
Spearphishing Link	Execution through Module Load	BITS Jobs	Bypass User Account Control	Compile After Delivery	Network Share Discovery	Pass the Hash	Logon Scripts	Data from Removable Media	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Inhibit System Recovery
Spearphishing via Service	Exploitation for Client Execution	Bootkit	Compiled HTML File	Forced Authentication	Network Sniffing	Pass the Ticket	Logon Scripts	Data Staged	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Network Denial of Service
Supply Chain Compromise	Graphical User Interface	Browser Extensions	DLL Search Order Hijacking	Component Firmware	Hooking	Password Policy Discovery	Logon Scripts	Domain Fronting	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel
Trusted Relationship	InstallUtil	Component Firmware	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Logon Scripts	Exfiltration Over Other Network Medium	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Resource Hijacking
Valid Accounts	LSASS Driver	Component Object Model Hijacking	Extra Window Memory Injection	Control Panel Items	Kerberoasting	Permission Groups Discovery	Logon Scripts	Exfiltration Over Physical Medium	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Scheduled Transfer
	Mshta	Component Object Model Hijacking	File System Permissions Weakness	DCShadow	LLMNR/NBT-NS Poisoning and Relay	Process Discovery	Logon Scripts	Fallback Channels	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Runtime Data Manipulation
	PowerShell	Create Account	File System Permissions Weakness	Deobfuscate/Decode Files or Information	Network Sniffing	Query Registry	Logon Scripts	Multi-hop Proxy	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Service Stop
	Regsvcs/Regasm	DLL Search Order Hijacking	Hooking	Disabling Security Tools	Password Filter DLL	Remote System Discovery	Logon Scripts	Multi-Stage Channels	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Stored Data Manipulation
	Regsvr32	External Remote Services	Image File Execution Options Injection	DLL Search Order Hijacking	Private Keys	Security Software Discovery	Logon Scripts	Multiband Communication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Transmitted Data Manipulation
	Rundll32	File System Permissions Weakness	New Service	DLL Side-Loading	Two-Factor Authentication Interception	System Information Discovery	Logon Scripts	Multilayer Encryption	Custom Cryptographic Protocol	Custom Cryptographic Protocol	
	Scheduled Task	Hidden Files and Directories	Path Interception	Execution Guardrails		System Network Configuration Discovery	Logon Scripts	Remote Access Tools	Custom Cryptographic Protocol	Custom Cryptographic Protocol	
	Scripting	Port Monitors	Port Monitors	Exploitation for Defense Evasion		System Network Connections Discovery	Logon Scripts	Remote File Copy	Custom Cryptographic Protocol	Custom Cryptographic Protocol	
	Service Execution	Process Injection	Process Injection	Extra Window Memory Injection		System Owner/User Discovery	Logon Scripts	Standard Application Layer Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	
	Signed Binary Proxy Execution	Hypervisor	Scheduled Task	File Deletion		System Service Discovery	Logon Scripts	Standard Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	
	Signed Script Proxy Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	File Permissions Modification		System Time Discovery	Logon Scripts	Standard Non-Application Layer Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	
	Third-party Software	Logon Scripts	SID-History Injection	File System Logical Offsets		Virtualization/Sandbox Evasion	Logon Scripts	Uncommonly Used Port	Custom Cryptographic Protocol	Custom Cryptographic Protocol	
	Trusted Developer Utilities	LSASS Driver	Valid Accounts	Group Policy Modification			Logon Scripts	Web Service	Pretty Good Coverage	Pretty Good Coverage	
	User Execution	Modify Existing Service	Web Shell	Image File Execution Options Injection				Add Item			
	Windows Management Instrumentation	Netsh Helper DLL		Indicator Blocking				Clear			
	Windows Remote Management	New Service		Indicator Removal from Tools							
	XSL Script Processing	Office Application Startup		Indicator Removal on Host							
		Path Interception		Indirect Command Execution							
		Port Monitors		Install Root Certificate							
		Redundant Access		InstallUtil							
		Registry Run Keys / Startup Folder		Masquerading							
		Scheduled Task		Modify Registry							
		Screensaver		Mshta							
		Security Support Provider		Network Share Connection Removal							
		Service Registry Permissions Weakness		NTFS File Attributes							
		Shortcut Modification		Obfuscated Files or Information							
		SIP and Trust Provider Hijacking		Process Doppelgänging							
		System Firmware		Process Hollowing							
		Time Providers		Process Injection							
		Valid Accounts		Redundant Access							
		Web Shell		Regsvcs/Regasm							
		Windows Management Instrumentation Event Subscription		Regsvr32							
		Winlogon Helper DLL		Rootkit							
				Rundll32							
				Scripting							
				Signed Binary Proxy Execution							
				Signed Script Proxy Execution							
				SIP and Trust Provider Hijacking							
				Software Packing							
				Template Injection							
				Timestamp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

▼ legend



# Sysmon actual coverage

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact	
External Remote Services	Compiled HTML File	AppCert DLLs	Accessibility Features	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Clipboard Data	Data Encrypted			
Hardware Additions	Control Panel Items	Applnit DLLs	AppCert DLLs	Bypass User Account Control	Credentials in Files	Domain Trust Discovery	Exploitation of Remote Services	Connection Proxy	Data Transfer Size	Defacement	
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	Applnit DLLs	CMSTP	Credentials in Registry	File and Directory Discovery	Data from Information Repositories	Custom Command and Control Protocol	Custom Command and Control Protocol	Disk Content Wipe	
Spearphishing Attachment	Execution through API	Authentication Package	Application Shimming	Code Signing	Exploitation for Credential Access	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Endpoint Denial of Service	
Spearphishing Link	Execution through Module Load	BITS Jobs	Bypass User Account Control	Compile After Delivery	Forced Authentication	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Firmware Corruption	
Spearphishing via Service	Exploitation for Client Execution	Bootkit	DLL Search Order Hijacking	Compiled HTML File	Hooking	Network Sniffing	Pass the Ticket	Data from Removable Media	Inhibit System Recovery		
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Component Firmware	Component Firmware	Input Capture	Password Policy Discovery	Remote Desktop Protocol	Data Encoding			
Trusted Relationship	InstallUtil	Change Default File Association	Extra Window Memory Injection	Component Object Model Hijacking	Input Prompt	Peripheral Device Discovery	Remote File Copy	Data Obfuscation			
	LSASS Driver	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Permission Groups Discovery	Remote Services	Domain Fronting			
Valid Accounts	Mshta	Deobfuscate/Decode Files or Information	DCShadow	Process Discovery	Query Registry	Replication Through Removable Media	Man in the Browser	Scheduled Transfer			
	PowerShell	Create Account	File System Permissions Weakness	Deobfuscate/Decode Files or Information	Network Sniffing	Remote System Discovery	Screen Capture	Runtime Data Manipulation			
Regsvcs/Regasm	DLL Search Order Hijacking	Hooking	Image File Execution Options Injection	Disabling Security Tools	Network Sniffing	Security Software Discovery	Video Capture	Service Stop			
	Regsvr32	External Remote Services	New Service	DLL Search Order Hijacking	Network Sniffing	System Information Discovery					
Rundll32	File System Permissions Weakness	Path Interception	Path Interception	Private Keys	Network Sniffing	System Network Configuration Discovery	Windows Admin Shares				
	Scheduled Task	Hidden Files and Directories	Port Monitors	Two-Factor Authentication Interception	Network Sniffing	System Network Connections Discovery	Windows Remote Management				
Scripting	Scripting	Service Execution	Port Monitors	Exploitation for Defense Evasion	Network Sniffing	System Owner/User Discovery					
	Service Execution	Hooking	Process Injection	Extra Window Memory Injection	Network Sniffing	System Service Discovery					
Signed Binary Proxy Execution	Signed Binary Proxy Execution	Hypervisor	Scheduled Task	File Deletion	Network Sniffing	System Time Discovery					
	Signed Script Proxy Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	File Permissions Modification	Network Sniffing	Virtualization/Sandbox Evasion					
Third-party Software	Third-party Software	Logon Scripts	SID-History Injection	File System Logical Offsets	Network Sniffing						
	Trusted Developer Utilities	LSASS Driver	Valid Accounts	Group Policy Modification	Network Sniffing						
User Execution	User Execution	Modify Existing Service	Web Shell	Hidden Files and Directories	Network Sniffing						
	Windows Management Instrumentation	Netsh Helper DLL	New Service	Image File Execution Options Injection	Network Sniffing						
Windows Remote Management	Windows Management Instrumentation	Office Application Startup	Indicator Blocking	Indicator Removal from Tools	Network Sniffing						
	XSL Script Processing	Path Interception	Port Monitors	Indicator Removal on Host	Network Sniffing						
XSL Script Processing	Redundant Access	Redundant Access	Redundant Access	Indirect Command Execution	Network Sniffing						
	Registry Run Keys / Startup Folder	Registry Run Keys / Startup Folder	Registry Run Keys / Startup Folder	Install Root Certificate	Network Sniffing						
XSL Script Processing	Scheduled Task	Scheduled Task	Scheduled Task	InstallUtil	Network Sniffing						
	Screensaver	Security Support Provider	Security Support Provider	Masquerading	Network Sniffing						
XSL Script Processing	Service Registry Permissions Weakness	Service Registry Permissions Weakness	Service Registry Permissions Weakness	Modify Registry	Network Sniffing						
	Shortcut Modification	Shortcut Modification	Shortcut Modification	Mshta	Network Share Connection Removal						
XSL Script Processing	SIP and Trust Provider Hijacking	SIP and Trust Provider Hijacking	SIP and Trust Provider Hijacking	Obfuscated Files or Information	NTFS File Attributes						
	System Firmware	System Firmware	System Firmware	Process Doppelgänging	Process Hollowing						
XSL Script Processing	Time Providers	Time Providers	Time Providers	Process Hollowing	Process Injection						
	Valid Accounts	Valid Accounts	Valid Accounts	Redundant Access	Redundant Access						
XSL Script Processing	Web Shell	Web Shell	Web Shell	Regsvcs/Regasm	Regsvr32						
	Windows Management Instrumentation Event Subscription	Windows Management Instrumentation Event Subscription	Windows Management Instrumentation Event Subscription	Rootkit	Rundll32						
XSL Script Processing	Winlogon Helper DLL	Winlogon Helper DLL	Winlogon Helper DLL	Scripting	Signed Binary Proxy Execution						
				Signed Script Proxy Execution	Signed Script Proxy Execution						
XSL Script Processing				SIP and Trust Provider Hijacking	SIP and Trust Provider Hijacking						
				Software Packing	Software Packing						
XSL Script Processing				Template Injection	Template Injection						
				Timestomp	Timestomp						
XSL Script Processing				Trusted Developer Utilities	Trusted Developer Utilities						
				Valid Accounts	Virtualization/Sandbox Evasion						
XSL Script Processing				Web Service	Web Service						
				XSL Script Processing	XSL Script Processing						





# Roadmap

# Technique applicability

ID	Name	Data score	Rule based detection	Hunting	Forensics	Score
T1001	Data Obfuscation	Packet capture,Process use of network,Process monitoring,Network protocol analysis	3	3	4	3,4
T1002	Data Compressed	Binary file metadata,File monitoring,Process command-line parameters,Process monitoring	3	4	4	3,6
T1003	Credential Dumping	API monitoring,Process monitoring,PowerShell logs,Process command-line parameters	4	4	4	4,0
T1004	Winlogon Helper DLL	Windows Registry,File monitoring,Process monitoring	4	5	5	4,6
T1005	Data from Local System	File monitoring,Process monitoring,Process command-line parameters	2	4	4	3,2
T1006	File System Logical Offsets	API monitoring	0	1	1	0,6
T1007	System Service Discovery	Process monitoring,Process command-line parameters	4	5	5	4,6
T1008	Fallback Channels	Malware reverse engineering,Netflow/Enclave netflow,Packet capture,Process monitoring,Process use of network	2	3	4	3,0
T1009	Binary Padding	Binary file metadata,File monitoring,Malware reverse engineering	1	3	4	2,6
T1010	Application Window Discovery	API monitoring,Process monitoring,Process command-line parameters	1	2	2	1,6
T1011	Exfiltration Over Other Network Medium	User interface,Process monitoring	1	2	3	2,0

# Use case scoring

ID	Name	Use case	Data source(s) used	Data score	Coverage	Upkeep	Confidence	Score
T1001	Data Obfuscation	123-zxy-name	Process use of network,Process Monitoring	4	3	4	3,8	
T1002	Data Compressed	123-zxy-name2	Process Monitoring,Process command-line parameters	2	4	2	2,4	
T1003	Credential Dumping	123-zxy-mimilove	Process monitoring,PowerShell logs,Process command-line parameters	4	3	4	3,8	
T1004	Winlogon Helper DLL			0	0	0	0,0	

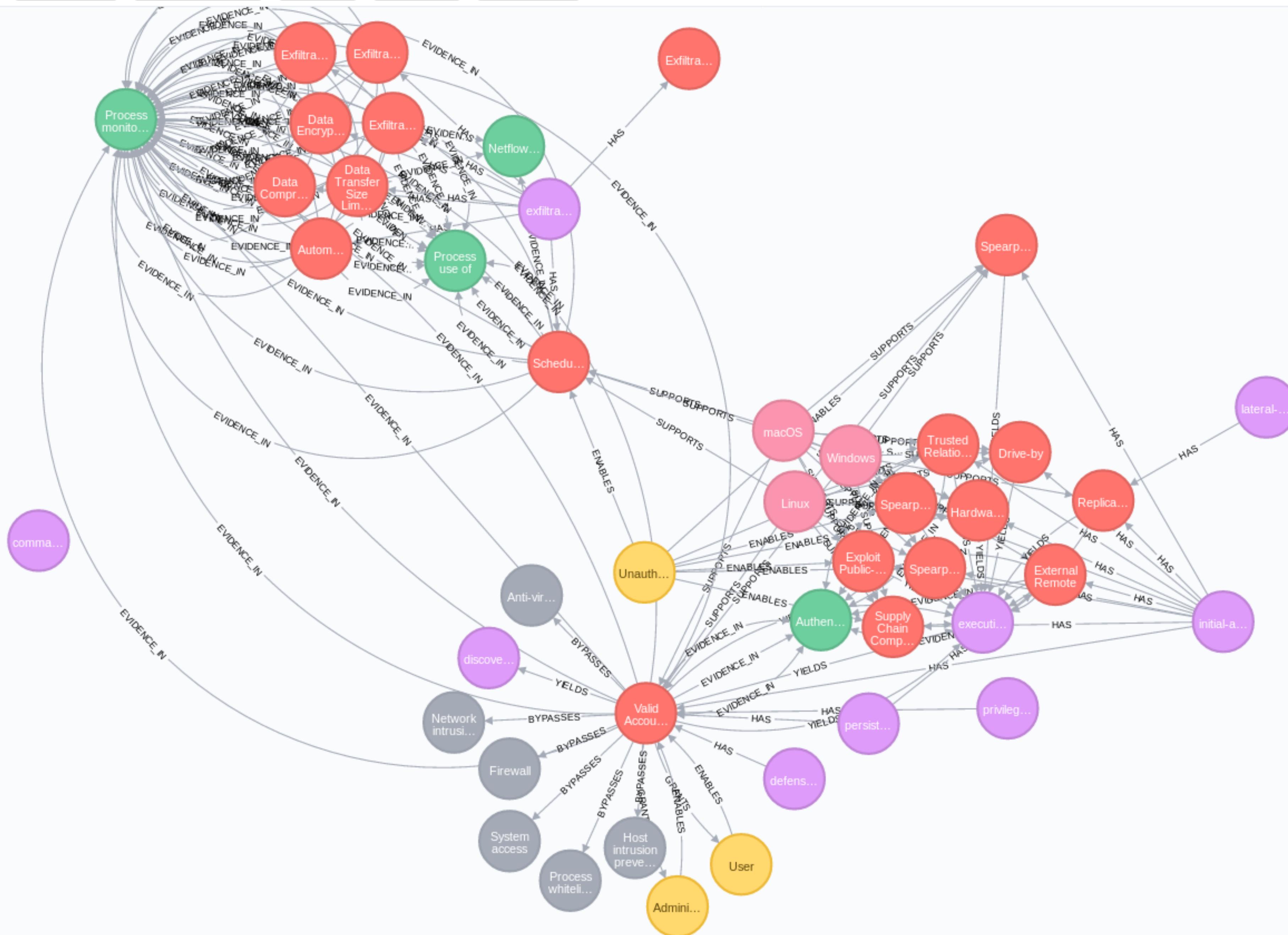
# Detection Bypassed weights

ID	Data Source	Weight	Datasources	Weights
T1006	File monitoring,File system access controls	50;50	2	2
T1009	Signature-based detection,Anti-virus	50;50	2	2
T1014	File monitoring,Host intrusion prevention systems,Process whitelisting,Signature-based detection,System access controls,Whitelisting by file name or path,Anti-virus	10;20;15;15;10;10;20	7	7
T1027	Host forensic analysis,Signature-based detection,Host intrusion prevention systems,Application whitelisting,Process whitelisting,Log analysis,Whitelisting by file name or path,Anti-virus	10;20;20;10;10;20;10	7	7
T1045	Signature-based detection,Anti-virus,Heuristic detection	30;35;35	3	3
T1054	Anti-virus,Log analysis,Host intrusion prevention systems	35;35;30	3	3
T1055	Process whitelisting,Anti-virus	50;50	2	2
T1064	Process whitelisting,Data Execution Prevention,Exploit Prevention	33;33;34	3	3
T1066	Log analysis,Host intrusion prevention systems,Anti-virus	35;35;30	3	3
T1070	Log analysis,Host intrusion prevention systems,Anti-virus	35;35;30	3	3
T1073	Process whitelisting,Anti-virus	50;50	2	2
T1078	Firewall,Host intrusion prevention systems,Network intrusion detection system,Process whitelisting,System access controls,Anti-virus	20;20;10;20;20;10	6	6
T1085	Anti-virus,Application whitelisting	35;65	2	2

# Detection rating

Name	Rationale	Coverage	Maintainability	Confidence	Score
Anti-virus		5	4	3	4,0
Application whitelisting		1	1	2	1,4
Autoruns Analysis		3	3	4	3,4
Binary Analysis		0	0	0	0,0
Data Execution Prevention		0	0	0	0,0
Digital Certificate Validation		3	3	2	2,6
Exploit Prevention		3	3	2	2,6
File monitoring		2	2	2	2,0
File system access controls		2	1	2	1,8
Firewall		3	3	4	3,4
Heuristic detection		5	4	3	4,0
Host forensic analysis		5	1	4	3,8
Host intrusion prevention systems		3	4	4	3,6
Log analysis		4	4	4	4,0
Network intrusion prevention systems		3	4	4	3,6
Process Whitelisting		0	0	0	0,0
Signature-based detection		4	4	3	3,6
System access controls		3	4	4	3,6
User Mode Signature Validation		3	4	3	3,2
Whitelisting by file name or path		0	0	0	0,0





Thank you

---



Questions?

 [@olafhartong](https://twitter.com/olafhartong)  
 [github.com/olafhartong](https://github.com/olafhartong)  
 [ohartong@deloitte.nl](mailto:ohartong@deloitte.nl)



Deloitte.