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

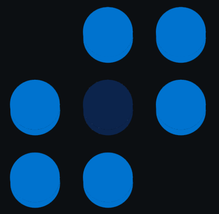
Documentary photographer

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

verage



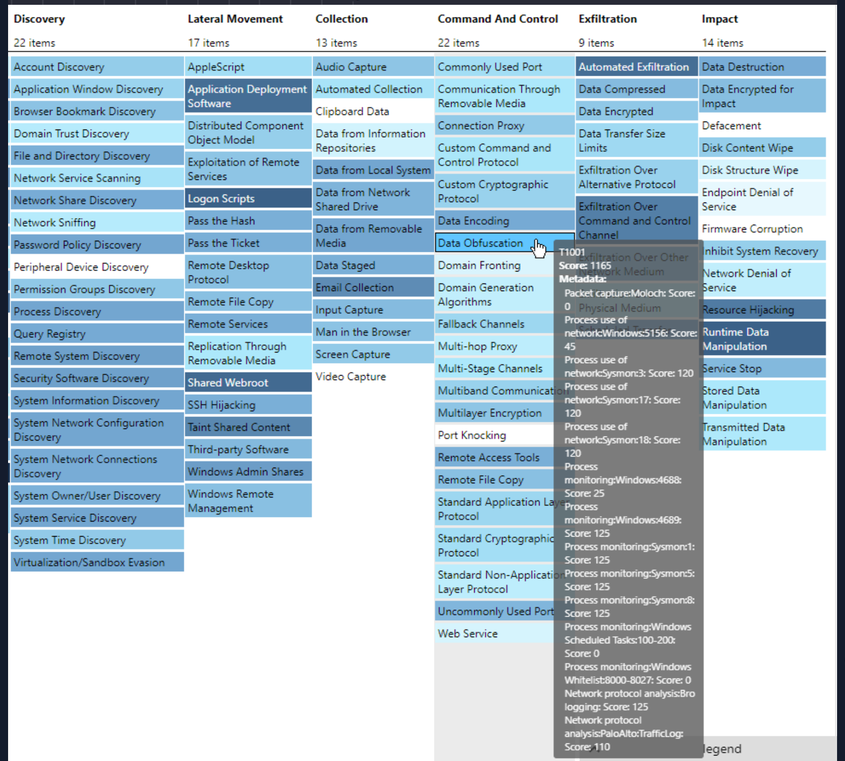
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Drive-by Compromise	CMSTP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

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"
                                            },
                                            {
```

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 se
T1002	Data Compressed	Binary file metadata,File monitoring,Process command-line parameters,Process monitoring	Linux,Windows,macOS	Compression software and compressed files can be detected in
T1003	Credential Dumping	API monitoring,Process monitoring,PowerShell logs,Process command-line parameters	Windows,Linux,macOS	### WindowsCommon credential dumpers such as [Mimikatz](ht
T1004	Winlogon Helper DLL	Windows Registry,File monitoring,Process monitoring	Windows	Monitor for changes to Registry entries associated with Winlog
T1005	Data from Local System	File monitoring,Process monitoring,Process command-line parameters	Linux,macOS,Windows	Monitor processes and command-line arguments for actions tha
T1006	File System Logical Offsets	API monitoring	Windows	Monitor handle opens on drive volumes that are made by proce
T1007	System Service Discovery	Process monitoring,Process command-line parameters	Windows	System and network discovery techniques normally occur throug
T1008	Fallback Channels	Malware reverse engineering,Netflow/Enclave netflow,Packet capture,Process monitoring,Process use of network	Linux,Windows,macOS	Analyze network data for uncommon data flows (e.g., a client se
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 signat
T1010	Application Window Discovery	API monitoring,Process monitoring,Process command-line parameters	macOS,Windows	System and network discovery techniques normally occur throug
T1011	Exfiltration Over Other Network Medium	User interface,Process monitoring	Linux,macOS,Windows	Processes utilizing the network that do not normally have netw
T1012	Query Registry	Windows Registry,Process monitoring,Process command-line parameters	Windows	System and network discovery techniques normally occur throug
T1013	Port Monitors	File monitoring,API monitoring,DLL monitoring,Windows Registry,Process monitoring	Windows	* Monitor process API calls to (Citation: AddMonitor) * Monitor
T1014	Rootkit	BIOS,MBR,System calls	Linux,macOS,Windows	Some rootkit protections may be built into anti-virus or operati
T1015	Accessibility Features	Windows Registry,File monitoring,Process monitoring	Windows	Changes to accessibility utility binaries or binary paths that do
T1016	System Network Configuration Discovery	Process monitoring,Process command-line parameters	Linux,macOS,Windows	System and network discovery techniques normally occur throug
T1017	Application Deployment Software	Application deployment software,Process use of network,Process monitoring	Linux,macOS,Windows	Monitor application deployments from a secondary system. Per
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 throug
T1019	System Firmware	API monitoring,BIOS,EFI	Windows	System firmware manipulation may be detected. (Citation: MITRE
T1020	Automated Exfiltration	File monitoring,Process monitoring,Process use of network	Linux,macOS,Windows	Monitor process file access patterns and network behavior. Unu
T1021	Remote Services	Authentication logs	Linux,macOS,Windows	Correlate use of login activity related to remote services with un
T1022	Data Encrypted	File monitoring,Process monitoring,Process command-line parameters,Binary file metadata	Linux,macOS,Windows	Encryption software and encrypted files can be detected in many
T1023	Shortcut Modification	File monitoring,Process monitoring,Process command-line parameters	Windows	Since a shortcut's target path likely will not change, modificatio
T1024	Custom Cryptographic Protocol	Packet capture,Netflow/Enclave netflow,Process use of network,Malware reverse engineering,Process monitoring	Linux,macOS,Windows	If malware uses custom encryption with symmetric keys, it may b
T1025	Data from Removable Media	File monitoring,Process monitoring,Process command-line parameters	Linux,macOS,Windows	Monitor processes and command-line arguments for actions tha
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 se
T1027	Obfuscated Files or Information	Network protocol analysis,Process use of network,File monitoring,Malware reverse engineering,Binary file metadata,Process command-line parameters,Enviro	Linux,macOS,Windows	Detection of file obfuscation is difficult unless artifacts are left b
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
T1029	Scheduled Transfer	Netflow/Enclave netflow,Process use of network,Process monitoring	Linux,macOS,Windows	Monitor process file access patterns and network behavior. Unu
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 se
T1031	Modify Existing Service	Windows Registry,File monitoring,Process monitoring,Process command-line parameters	Windows	Look for changes to service Registry entries that do not correlate
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 throug
T1034	Path Interception	File monitoring,Process monitoring	Windows	Monitor file creation for files named after partial directories and
T1035	Service Execution	Windows Registry,Process monitoring,Process command-line parameters	Windows	Changes to service Registry entries and command-line invocatio
T1036	Masquerading	File monitoring,Process monitoring,Binary file metadata	Linux,macOS,Windows	Collect file hashes; file names that do not match their expected
T1037	Logon Scripts	File monitoring,Process monitoring	macOS,Windows	Monitor logon scripts for unusual access by abnormal users or u
T1038	DLL Search Order Hijacking	File monitoring,DLL monitoring,Process monitoring,Process command-line parameters	Windows	Monitor file systems for moving, renaming, replacing, or modify
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 th
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 o
T1041	Exfiltration Over Command and Control Channel	User interface,Process monitoring	Linux,macOS,Windows	Detection for command and control applies. Analyze network da
T1042	Change Default File Association	Windows Registry,Process monitoring,Process command-line parameters	Windows	Collect and analyze changes to Registry keys that associate file
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 se
T1044	File System Permissions Weakness	File monitoring,Services,Process command-line parameters	Windows	Look for changes to binaries and service executables that may
T1045	Software Packing	Binary file metadata	Windows	Use file scanning to look for known software packers or artifact
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 throug

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	25,25,25,25	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,Environ	8.8.8.8.8.9.10.8.9.8.8.8	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		
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	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
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	0	0	0	0.0
Windows event logs	Windows:4724, 4738,4728,4732	0	0	0	0.0
Windows event logs	Windows:1102	0	0	0	0.0
Windows Registry	Windows:4657	0	0	0	0.0

- Reference workbook
- Weights workbook
- Rating workbook

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,Environ	8;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	Exploitation of Remote Services	Clipboard Data
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Password Policy Discovery	Remote File Copy	Data Staged
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Email Collection
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Kerberoasting	Permission Groups Discovery	Replication Through Removable Media	Input Capture
	LSASS Driver	Component Firmware	Hooking	DCShadow	LLMNR/NBT-NS Poisoning	Process Discovery	Shared Webroot	Man in the Browser
	Mshta	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Network Sniffing	Query Registry	Taint Shared Content	Screen Capture
	PowerShell	Create Account	New Service	Disabling Security Tools	Password Filter DLL	Remote System Discovery	Third-party Software	Video Capture
	Regsvcs/Regasm	DLL Search Order Hijacking	Path Interception	DLL Search Order Hijacking	Private Keys	Security Software Discovery	Windows Admin Shares	
	Regsvr32	External Remote Services	Port Monitors	DLL Side-Loading	Two-Factor Authentication Interception	System Information Discovery	Windows Remote Management	
	Rundll32	File System Permissions Weakness	Process Injection	Exploitation for Defense Evasion		System Network Configuration Discovery		
	Scheduled Task	Hidden Files and Directories	Scheduled Task	Extra Window Memory Injection		System Network Connections Discovery		
	Scripting	Hooking	Service Registry Permissions Weakness	File Deletion		System Owner/User Discovery		
	Service Execution	Hypervisor	SID-History Injection	File Permissions Modification		System Service Discovery		
	Signed Binary Proxy Execution	Image File Execution Options Injection	Valid Accounts	File System Logical Offsets		System Time Discovery		
	Signed Script Proxy Execution	Logon Scripts	Web Shell	Hidden Files and Directories		Virtualization/Sandbox Evasion		
	Third-party Software	LSASS Driver		Image File Execution Options Injection				
	Trusted Developer Utilities	Modify Existing Service		Indicator Blocking				
	User Execution	Netsh Helper DLL		Indicator Removal from Tools				
	Windows Management Instrumentation	New Service		Indicator Removal on Host				
	Windows Remote Management	Office Application Startup		Indirect Command Execution				
	XSL Script Processing	Path Interception		Install Root Certificate				
		Port Monitors		InstallUtil				
				Masquerading				

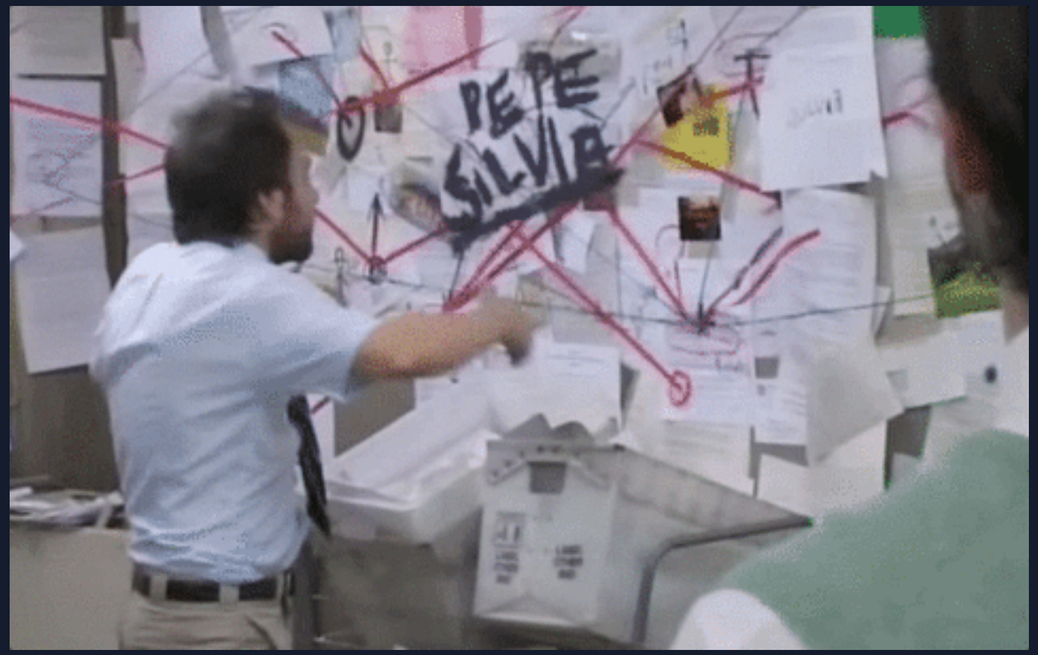
T1214
Score: 2500
Metadata:
Windows Registry:Windows:4657: Score: 0
Windows Registry:Sysmon:12: Score: 285
Windows Registry:Sysmon:13: Score: 285
Windows Registry:Sysmon:14: Score: 285
Process command-line parameters:Windows:4688: Score: 58
Process command-line parameters:Sysmon:1: Score: 290
Process command-line parameters:Windows:4688: Score: 58
Process monitoring:Windows:4688: Score: 59
Process monitoring:Windows:4689: Score: 295
Process monitoring:Sysmon:1: Score: 295
Process monitoring:Sysmon:5: Score: 295
Process monitoring:Sysmon:8: Score: 295
Process monitoring:Windows Scheduled Tasks:100-200: Score: 0
Process monitoring:Windows Whitelist:8000-8027: Score: 0

Administrator: Windows PowerShell

```
PS C:\Users\homerus\Desktop\attackdatamap> ls


    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>
```

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

legend

#ffffff	Low Coverage
#76aad4	Medium Coverage
#000000	Pretty Good Coverage

Add Item Clear

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	Accessibility Features	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	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials in Files	Domain Trust Discovery	Logon Scripts	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Registry	File and Directory Discovery	Pass the Hash	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Execution through API	Authentication Package	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Service Scanning	Pass the Ticket	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Compile After Delivery	Forced Authentication	Network Share Discovery	Remote Desktop Protocol	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Network Sniffing	Remote File Copy	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Password Policy Discovery	Remote Services	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Peripheral Device Discovery	Replication Through Removable Media	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Permission Groups Discovery	Shared Webroot	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Mshta	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	LLMNR/NBT-NS Poisoning and Relay	Process Discovery	Taint Shared Content	Screen Capture	Multi-Stage Channels		Service Stop
	PowerShell	Create Account	New Service	Deobfuscate/Decode Files or Information	Network Sniffing	Query Registry	Third-party Software	Video Capture	Multiband Communication		Stored Data Manipulation
	Regsvcs/Regasm	DLL Search Order Hijacking	Path Interception	Disabling Security Tools	Password Filter DLL	Remote System Discovery	Windows Admin Shares		Multilayer Encryption		Transmitted Data Manipulation
	Regsvr32	External Remote Services	Port Monitors	DLL Search Order Hijacking	Private Keys	Security Software Discovery	Windows Remote Management		Remote Access Tools		
	Rundll32	File System Permissions Weakness	Process Injection	DLL Side-Loading	Two-Factor Authentication Interception	System Information Discovery			Remote File Copy		
	Scheduled Task	Hidden Files and Directories	Scheduled Task	Execution Guardrails		System Network Configuration Discovery			Standard Application Layer Protocol		
	Scripting	Hooking	Service Registry Permissions Weakness	Exploitation for Defense Evasion		System Network Connections Discovery			Standard Cryptographic Protocol		
	Service Execution	Hypervisor	SID-History Injection	Extra Window Memory Injection		System Owner/User Discovery			Standard Non-Application Layer Protocol		
	Signed Binary Proxy Execution	Image File Execution Options Injection	Valid Accounts	File Deletion		System Service Discovery			Uncommonly Used Port		
	Signed Script Proxy Execution	Logon Scripts	Web Shell	File Permissions Modification		System Time Discovery			Web Service		
	Third-party Software	LSASS Driver		File System Logical Offsets		Virtualization/Sandbox Evasion					
	Trusted Developer Utilities	Modify Existing Service		Group Policy Modification							
	User Execution	Netsh Helper DLL		Hidden Files and Directories							
	Windows Management Instrumentation	New Service		Image File Execution Options Injection							
	Windows Remote Management	Office Application Startup		Indicator Blocking							
	XSL Script Processing	Path Interception		Indicator Removal from Tools							
		Port Monitors		Indicator Removal on Host							
		Redundant Access		Indirect Command Execution							
		Registry Run Keys / Startup Folder		Install Root Certificate							
		Scheduled Task		InstallUtil							
		Screensaver		Masquerading							
		Security Support Provider		Modify Registry							
		Service Registry Permissions Weakness		Mshta							
		Shortcut Modification		Network Share Connection Removal							
		SIP and Trust Provider Hijacking		NTFS File Attributes							
		System Firmware		Obfuscated Files or Information							
		Time Providers		Process Doppelgänging							
		Valid Accounts		Process Hollowing							
		Web Shell		Process Injection							
		Windows Management Instrumentation Event Subscription		Redundant Access							
		Winlogon Helper DLL		Regsvcs/Regasm							
				Regsvr32							
				Rootkit							
				Rundll32							
				Scripting							
				Signed Binary Proxy Execution							
				Signed Script Proxy Execution							
				SIP and Trust Provider Hijacking							
				Software Packing							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				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	2,5
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

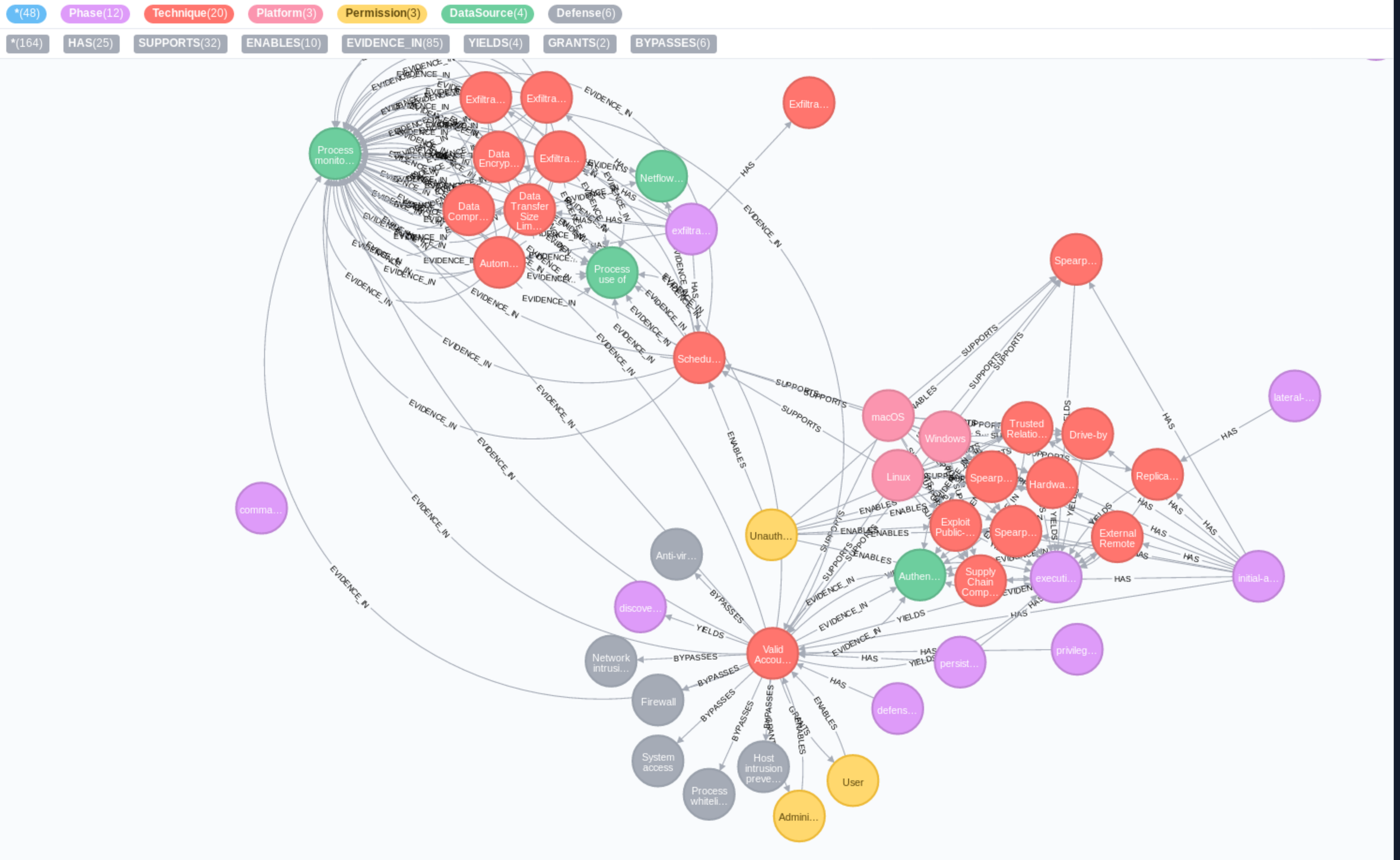
ID	Name	Use case	Data source(s) used	Data score	Coverage	Upkeep	Confidence	Score
T1001	Data Obfuscation	123-zxy-name	Process use of network,Process Monitoring		4	3	4	3,8
T1002	Data Compressed	123-zxy-name2	Process Monitoring, Process command-line parameters		2	4	2	2,4
T1003	Credential Dumping	123-zxy-mimilove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

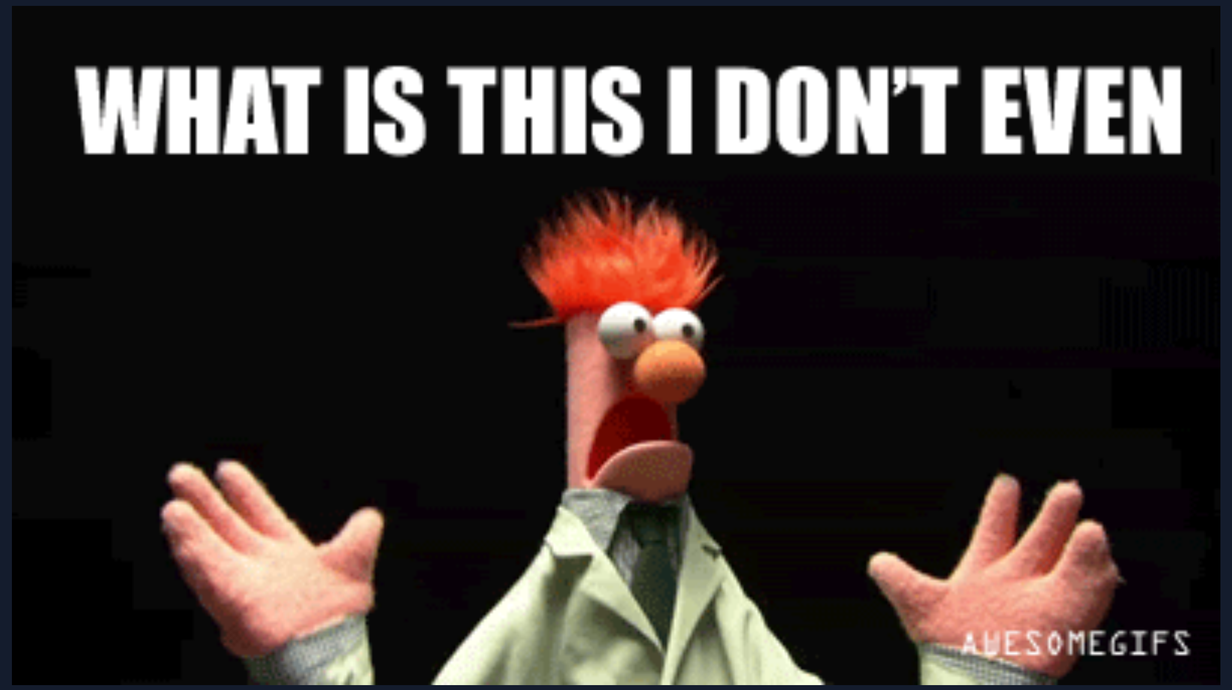
ID	Data Source	Weight	Datasources	Weights
T1006	File monitoring,File system access controls	50;50	2	2
T1009	Signature-based detection,Anti-virus	50;50	2	2
T1014	File monitoring,Host intrusion prevention systems,Process whitelisting,Signature-based detection,System access controls,Whitelisting by file name or path,Anti	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 f	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	2,5
Exploit Prevention		3	3	2	2,5
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


*(48)
Phase(12)
Technique(20)
Platform(3)
Permission(3)
DataSource(4)
Defense(6)
*(164)
HAS(25)
SUPPORTS(32)
ENABLES(10)
EVIDENCE_IN(85)
YIELDS(4)
GRANTS(2)
BYPASSES(6)
Exfiltra…
Exfiltra…
Exfiltra…
Exfiltra…
Process monito…
Data Encryp…
Netflow…
Data Compr…
Data Transfer Size Lim…
exfiltra…
Autom…
Process use of
Schedu…
Spearp…
macOS
Windows
Trusted Relatio…
Drive-by
lateral-…
Linux
Spearp…
Hardwa…
Replica…
comma…
Unauth…
Exploit Public-…
Spearp…
External Remote
Anti-vir…
Authen…
Supply Chain Comp…
executi…
initial-a…
discove…
Valid Accou…
persist…
privileg…
Network intrusi…
Firewall
defens…
System access
Host intrusion preve…
Process whiteli…
User
Admini…

Thank you



Questions?

@olafhartong
github.com/olafhartong
ohartong@deloitte.nl

Deloitte.