



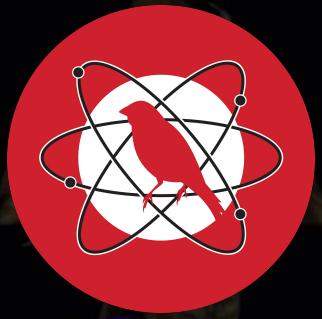
Not Enough Mitre

You You Require More Vespene ATT&CK



By Wade Wells

@WadingThruLogs

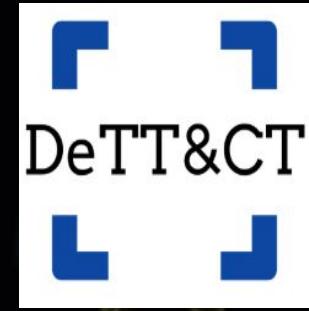


Atomic Red
Team
Episode III



Attack
Navigator
Episode I

Free
Open Source



DeTT&CT
Episode II



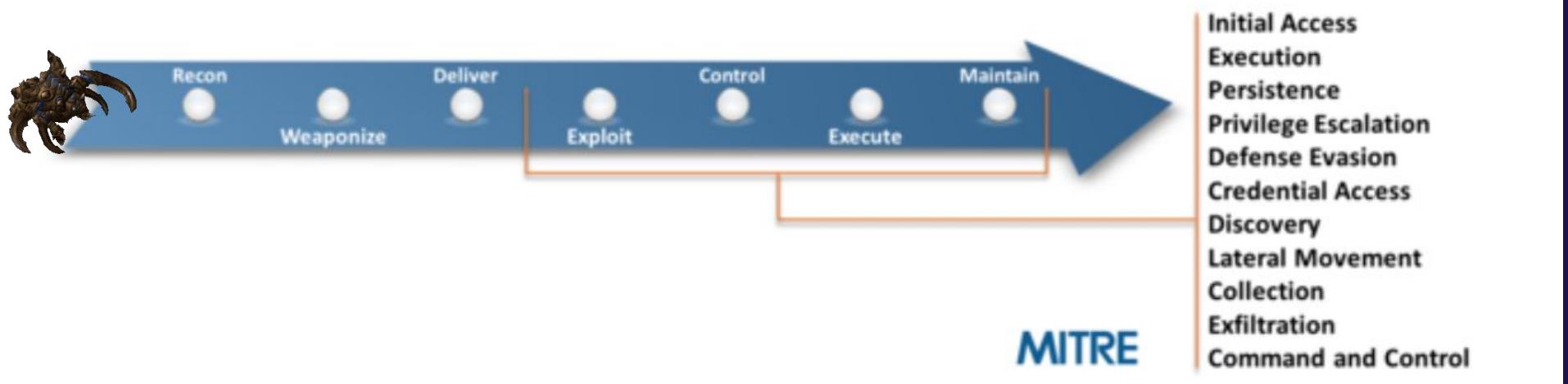
What can we DeTT&CT?



How do we keep track of what we can detect?

Adversarial Tactics, Techniques, and Common Knowledge Framework

Mitre ATT&CK Enterprise Framework



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise		Scheduled Task		Binary Padding		Network Sniffing	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application		Launchctl		Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services		Local Job Scheduling		Bypass User Account Control	Bash History	Application Window Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Defacement	
Hardware Additions		LSASS Driver		Extra Window Memory Injection	Brute Force		Data from Information Repositories	Connection Proxy	Data Transfer Size Limits	Disk Content Wipe	
Replication Through Removable Media	Trap			Process Injection	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Custom Command and Control Protocol	Exfiltration Over Other Network Medium	Disk Structure Wipe	Endpoint Denial of Service
	AppleScript		DLL Search Order Hijacking	Credentials in Files		Domain Trust Discovery	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Firmware Corruption	Inhibit System Recovery
	CMSTP		Image File Execution Options Injection			File and Directory Discovery	Data from Network Shared Drive	Data Encoding	Exfiltration Over Alternative Protocol	Network Denial of Service	Runtime Data Manipulation
Spearphishing Attachment	Command-Line Interface		Plist Modification		Exploitation for Credential Access	Network Service Scanning	Pass the Hash	Data Staged	Data Obfuscation	Service Stop	
Spearphishing Link	Compiled HTML File		Valid Accounts			Network Share Discovery	Pass the Ticket	Remote Desktop Protocol	Email Collection	Domain Fronting	
Spearphishing via Service	Control Panel Items	Accessibility Features		BITS Jobs	Forced Authentication		Remote File Copy	Input Capture	Domain Generation Algorithms	Resource Hijacking	
Supply Chain Compromise	Dynamic Data Exchange	AppCert DLLs		Clear Command History	Hooking	Password Policy Discovery	Remote Services	Man in the Browser	Scheduled Transfer	Stored Data Manipulation	
Trusted Relationship	Execution through API	AppInit DLLs		CMSTP	Input Capture	Peripheral Device Discovery					
		Application Shimming		Code Signing	Input Prompt	Permission Groups Discovery					
Valid Accounts	Execution through Module Load	Dylib Hijacking		Compiled HTML File	Kerberoasting	Process Discovery	Replication Through Removable Media	Screen Capture	Fallback Channels		
		File System Permissions Weakness		Component Firmware	Keychain	Query Registry		Video Capture	Multiband Communication		
Graphical User Interface		Hooking		Component Object Model Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery			Multi-hop Proxy		
	InstallUtil	Launch Daemon		Control Panel Items	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery			Multilayer Encryption		
	Mshra	New Service		DCShadow	LLMNR/NBT-NS Poisoning and Relay	System Information Discovery			Multi-Stage Channels		
	PowerShell	Path Interception		Deobfuscate/Decode Files or Information	Private Keys	Taint Shared Content			Port Knocking		
	Regsvcs/Regasm	Port Monitors		Securityd Memory		Third-party Software			Remote Access Tools		
	Regsvr32	Service Registry Permissions Weakness		Two-Factor Authentication Interception		Windows Admin Shares			Remote File Copy		
	Rundll32	Setuid and Setgid		Disabling Security Tools		System Network Configuration Discovery			Standard Application Layer Protocol		
	Scripting	Startup Items		DLL Side-Loading		System Network Connections Discovery			Standard Cryptographic Protocol		
		Web Shell		Execution Guardrails		System Owner/User Discovery			Standard Non-Application Layer Protocol		
Service Execution	bash_profile and bashrc		Exploitation for Privilege Escalation	Exploitation for Defense Evasion		System Service Discovery			Uncommonly Used Port		
	Signed Binary Proxy Execution	Account Manipulation		SID-History Injection	File Deletion	System Time Discovery			Web Service		
	Signed Script Proxy Execution	Authentication Package		Sudo	File Permissions Modification	Virtualization/Sandbox Evasion					
	Source	Browser Extensions		File System Logical Offsets							
	Space after Filename	Change Default File Association		Gatekeeper Bypass							
	Third-party Software			Group Policy Modification							
Trusted Developer Utilities		Component Firmware		Hidden Files and Directories							
User Execution		Component Object Model Hijacking		Hidden Users							
	Windows Management Instrumentation	Create Account		Hidden Window							
	Windows Remote Management	External Remote Services		HISTCONTROL							
		Hidden File and Directories		Indicator Blocking							
	XSL Script Processing	Hypervisor		Indicator Removal from Tools							
		Kernel Modules and Extensions		Indicator Removal on Host							
		Launch Agent		Indirect Command Execution							
		LC_LOAD_DYLIB Addition		Install Root Certificate							
		Login Item		InstallUtil							
		Logon Scripts		Launchctl							
		Modify Existing Service		LC_MAIN Hijacking							
		Netsh Helper DLL		Masquerading							
		Office Application Startup		Modify Registry							
		Port Knocking		Mshta							
		Rc.common		Network Share Connection Removal							
		Redundant Access		NTFS File Attributes							
		Registry Run Keys / Startup Folder		Obfuscated Files or Information							

MITRE ATT&CK™
Enterprise Framework

ATT&CK Navigator

MITRE

ATT&CK™

- Run as Iframe
- Consumes . json files
- Free data on Mitre Website

- Easily configurable
- Angular and Node.js version 8 or greater

Start

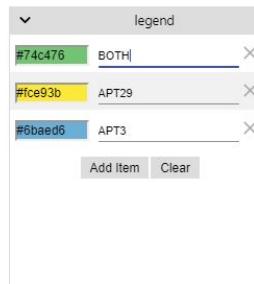
github.com/mitre-attack/attack-navigator

Zerg Tactics, Techniques and Procedures

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
CMSTP	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark	Component Object Model and Distributed COM	Clipboard Data	Data from Information Repositories	Data Encrypted	Data Encrypted for Impact
External Remote Services	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	File and Directory Discovery	Custom Command and Control Protocol	Custom Cryptographic Protocol	Data Transfer Size Limits	Defacement
Hardware Additions	Component Object Model and Distributed COM	Applinit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	Exploitation of Remote Services	File and Directory Discovery	Exploitation Over Alternative System	Exfiltration Over Command and Control Channel	Disk Content Wipe	Disk Structure Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Bypass User Account Control	Code Signing	Credentials in Files	Network Service Scanning	File and Directory Discovery	Internal Spearphishing	Data Encoding	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing Attachment	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Compiled HTML File	Credentials in Registry	Network Share Discovery	File and Directory Discovery	Data from Network Shared Drive	Data Obfuscation	Firmware Corruption	Inhibit System Recovery
Spearphishing Link	Execution through API	BITS Jobs	Dylib Hijacking	Component Firmware	Exploitation for Credential Access	Network Sniffing	File and Directory Discovery	Logon Scripts	Domain Fronting	Exfiltration Over Physical Medium	Network Denial of Service
Spearphishing via Service	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Component Object Model Hijacking	Forced Authentication	Password Policy Discovery	File and Directory Discovery	Pass the Hash	Remote Desktop Protocol	Exfiltration Over Physical Medium	Resource Hijacking
Supply Chain Compromise	Exploitation for Client Execution	Change Default File Association	Emond	Connection Proxy	Hooking	Peripheral Device Discovery	File and Directory Discovery	Pass the Ticket	Remote File Copy	Exfiltration Over Physical Medium	Runtime Data Manipulation
Trusted Relationship	Graphical User Interface	Component Firmware	Exploitation for Privilege Escalation	Control Panel Items	Input Capture	Permission Groups Discovery	File and Directory Discovery	Email Collection	Input Capture	Multi-hop Proxy	Service Stop
Valid Accounts	InstallUtil	Component Object Model Hijacking	Extra Window Memory Injection	DCShadow	Input Prompt	Process Discovery	File and Directory Discovery	Remote File Copy	Man in the Browser	Multi-Stage Channels	Stored Data Manipulation
	Launchctl	Create Account	File System Permissions Weakness	Deobfuscate/Decode Files or Information	Kerberoasting	Query Registry	File and Directory Discovery	Remote Services	Multi-band Communication	Multilayer Encryption	System Shutdown/Reboot
	Local Job Scheduling	DLL Search Order Hijacking	Disabling Security Tools	Keychain	Remote System Discovery	Remote System Discovery	File and Directory Discovery	Replication Through Removable Media	Port Knocking	Port Knocking	Transmitted Data Manipulation
	LSASS Driver	Mshta	DLL Side-Loading	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Screen Capture	File and Directory Discovery	Shared Webroot	Video Capture	Video Capture	Remote Access Tools
		Dylib Hijacking	Hooking	Network Sniffing	Software Discovery	System Information Discovery	File and Directory Discovery	SSH Hijacking	Third-party	Third-party	Remote File Copy
		PowerShell	Emond	Execution Guardrails	System Network Configuration Discovery	System Network Configuration Discovery	File and Directory Discovery	Print Shared Content			

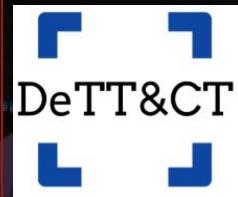
Comparing Threat Actors

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Data from Information Repositories	Data from Local System	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	Application Shimming	CMSTP	Credentials from Web Browsers	File and Directory Discovery	Exploitation of Remote Services	Data from Network Shared Drive	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Disk Content Wipe	Disk Structure Wipe
Spearphishing Attachment	Control Panel Items	Authentication Package	Code Signing	Credentials in Files	Network Share Discovery	Internal Spearphishing	Data Encoding	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Endpoint Denial of Service	Firmware Corruption
Spearphishing Link	Dynamic Data Exchange	DLL Search Order Hijacking	Compile After Delivery	Credentials In Registry	Logon Scripts	Network Sniffing	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Inhibit System Recovery	Network Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Complied HTML File	Pass the Hash	>Password Policy Discovery	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Resource Hijacking	Scheduled Transfer
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Component Firmware	Pass the Ticket	Peripheral Device Discovery	Domain Generation Algorithms	Email Collection	Fallback Channels	Runtime Data Manipulation	Service Stop
Trusted Relationship	Exploitation for Client Execution	Emond	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote Desktop Protocol	Input Capture	Input Capture	Man in the Browser	Screen Capture	Stored Data Manipulation
Valid Accounts	Graphical User Interface	Component Firmware	Exploitation for Privilege Escalation	Input Capture	Process Discovery	Remote Services	Input Capture	Input Capture	Multi-hop Proxy	Multi-Stage Channels	System Shutdown/Reboot
	InstallUtil	Component Object Model Hijacking	Extra Window Memory Injection	Input Prompt	Query Registry	Remote System Discovery	Input Capture	Input Capture	Port Knocking	Multi-layer Encryption	Transmitted Data Manipulation
	LaunchCtl	Create Account	File System Permissions Weakness	DCShadow	Kerberoasting	Security Software Discovery	Shared Webroot	Input Capture	Remote Access Tools	Remote File Copy	
	Local Job Scheduling	DLL Search Order Hijacking	Deobfuscate/Decode Files or Information	Keychain	Software Discovery	SSH Hijacking	Input Capture	Input Capture	Standard Application Layer Protocol	Standard Cryptographic Protocol	
	LSASS Driver	Dylib Hijacking	Image File Execution Options Injection	LMNR/NBT-NS Poisoning and Relay	System Information Discovery	Taint Shared Content	Input Capture	Input Capture	Standard Non-Application Layer Protocol	Standard Non-Application Layer Protocol	
	Msihta	Emond	Launch Daemon	Disabling Security Tools	System Network Configuration Discovery	Third-party Software	Input Capture	Input Capture	Uncommonly Used Port	Uncommonly Used Port	
	PowerShell	External Remote Services	DLL Side-Loading	DLL Search Order Hijacking	Network Sniffing	Windows Admin Shares	Input Capture	Input Capture	Web Service	Web Service	
	Regsvcs/Regasm	File System Permissions Weakness	New Service	Execution Guardrails	Password Filter DLL	Windows Remote Management	Input Capture	Input Capture	Input Capture	Input Capture	
	Regsvr32	Hidden Files and Directories	Parent PID Spoofing	Exploitation for Defense Evasion	Private Keys	Input Capture	Input Capture	Input Capture	Input Capture	Input Capture	
	Rundll32	Hooking	Path Interception	Extra Window Memory Injection	Securityd Memory	Input Capture	Input Capture	Input Capture	Input Capture	Input Capture	
	Scheduled Task	Hooking	Plist Modification	File and Directory Permissions Modification	System Network Connections Discovery	Input Capture	Input Capture	Input Capture	Input Capture	Input Capture	
	Scripting	Hypervisor	Port Monitors	Two-Factor Authentication Interception	System Owner/User Discovery	Input Capture	Input Capture	Input Capture	Input Capture	Input Capture	
	Service Execution	Image File Execution Options Injection	File Deletion	Virtualization/Sandbox Evasion	System Service Discovery	Input Capture	Input Capture	Input Capture	Input Capture	Input Capture	
	Signed Binary Proxy Execution	Kernel Modules and Extensions	PowerShell Profile	System Logical Offsets	System Time Discovery	Input Capture	Input Capture	Input Capture	Input Capture	Input Capture	
	Signed Script Proxy Execution	Launch Agent	Process Injection	Gatekeeper Bypass	Virtualization/Sandbox Evasion	Input Capture	Input Capture	Input Capture	Input Capture	Input Capture	
	Source	Launch Daemon	Scheduled Task	Group Policy Modification	Input Capture	Input Capture	Input Capture	Input Capture	Input Capture	Input Capture	
	Space after Filename	Launch Daemon	Service Registry Permissions Weakness	Hidden Files and Directories	Hidden Users	Input Capture	Input Capture	Input Capture	Input Capture	Input Capture	
	Third-party Software	LaunchCtl	Setuid and Setgid	Hidden Window	HISTCONTROL	Input Capture	Input Capture	Input Capture	Input Capture	Input Capture	
	Trap	LC_LOAD_DYLIB Addition	SID-History Injection	Indicator Blocking	Input Capture	Input Capture	Input Capture	Input Capture	Input Capture	Input Capture	
	Trusted Developer Utilities	Local Job Scheduling	Startup Items	Image File Execution Options Injection	Indicator Removal from Tools	Input Capture	Input Capture	Input Capture	Input Capture	Input Capture	
	User Execution	Login Item	Sudo	Sudo Caching	Indicator Blocking	Input Capture	Input Capture	Input Capture	Input Capture	Input Capture	
	Windows Management Instrumentation	Logon Scripts	sudo	Indicator Removal from Tools	Input Capture	Input Capture	Input Capture	Input Capture	Input Capture	Input Capture	
	Windows Remote	USASS Driver	Valid Accounts	Indicator Removal from Tools	Input Capture	Input Capture	Input Capture	Input Capture	Input Capture	Input Capture	



DeTT&CT

Detect Tactics, Techniques & Combat Threats

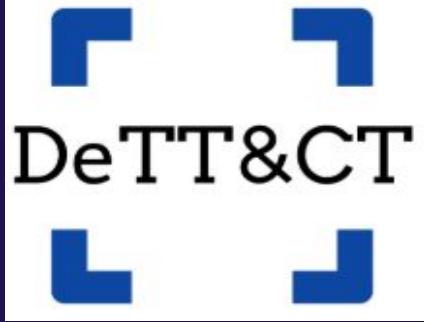


- ❖ Administer and score the quality of your data sources.
 - ❖ Get insight on the visibility you have on endpoints.
 - ❖ Map your detection coverage.
-
- Map TTP's
 - Compares visibility, detections and threats.
 - Uses ATT&CK Navigator.
 - Runs Via Python 3.

Start

github.com/rabobank-cdc/DeTTECT

How DeTT&CT works



Data source: Data sources are the raw logs or events generated by systems, security appliances, network devices, etc.

Visibility: Sufficient data sources with sufficient quality available, to be able to see traces of attacks.

```
-- DeTT&CT --
-- Detect Tactics, Techniques & Combat Threats --
version 1.2.0
```

Select a mode:

1. Data source mapping
 2. Visibility coverage mapping
 3. Detection coverage mapping
 4. Threat actor group mapping
 5. Updates
 6. Statistics
 9. Quit
- >>

```
file_type: data-source-administration
name: Data sources
platform: windows
data_sources:
    # A data source is treated as not available when all dimensions of the data quality have a score of 0.
    # If desired you are free to add any key-value pairs.
    - data_source_name: Process monitoring
        date_registered:
        date_connected:
        products: [EDR]
        available_for_data_analytics: True
        comment: ''
        data_quality:
            device_completeness: 3
            data_field_completeness: 4
            timeliness: 4
            consistency: 4
            retention: 3
    - data_source_name: File monitoring
        date_registered:
        date_connected:
        products: [EDR, DLP, Cloud DLP]
        available_for_data_analytics: true
        comment: ''
        data_quality:
            device_completeness: 3
            data_field_completeness: 4
            timeliness: 4
            consistency: 4
            retention: 3
```

Visibility & Scoring

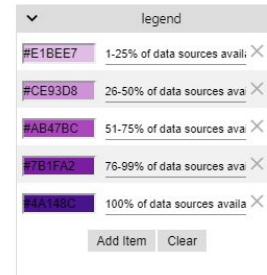
Visibility scores

Score	Score name	Description
0	None	No visibility at all.
1	Minimal	Sufficient data sources with sufficient quality available to be able to see one aspect of the technique's procedures.
2	Medium	Sufficient data sources with sufficient quality available to be able to see more aspects of the technique's procedures compared to "1/Minimal".
3	Good	Sufficient data sources with sufficient quality available to be able to see almost all known aspects of the technique's procedures.
4	Excellent	All data sources and required data quality necessary to be able to see all known aspects of the technique's procedures are available.

```
file_type: data-source-administration
name: Data sources
platform: windows
data_sources:
# A data source is treated as not available
# If desired you are free to add any key-value pairs here
- data_source_name: Process monitoring
  date_registered:
  date_connected:
  products: [EDR]
  available_for_data_analytics: True
  comment: ''
  data_quality:
    device_completeness: 3
    data_field_completeness: 4
    timeliness: 4
    consistency: 4
    retention: 3
- data_source_name: File monitoring
  date_registered:
  date_connected:
  products: [EDR, DLP, Cloud DLP]
  available_for_data_analytics: true
  comment: ''
  data_quality:
    device_completeness: 3
    data_field_completeness: 4
    timeliness: 4
    consistency: 4
    retention: 3
- data_source_name: Process command-line parameters
  date_registered:
  date_connected:
  products: [EDR]
  available_for_data_analytics: True
  comment: ''
  data_quality:
    device_completeness: 3
```

Data Source logging

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	28 items	44 items	23 items	60 items	18 items	23 items	16 items	13 items	21 items	9 items	16 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	Account Access Removal
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Automated Collection	Communication Through	Data Compressed	Data Destruction	
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Removable Media	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Component Object Model and Distributed COM	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials from Web Browsers	Domain Trust Discovery	Data from Information Repositories	Connection Proxy	Data Transfer Size Limits	Defacement	
Replication Through Removable Media	Control Panel Items	Authentication Package	Bypass User Account Control	Code Signing	Credentials in Files	File and Directory Discovery	Exploitation of Remote Services	Custom Command and Control Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe	
Spearphishing Attachment	Dynamic Data Exchange	BITS Jobs	Control	Compile After Delivery	Credentials in Registry	Network Service Scanning	Internal Spearphishing	Data from Local System	Custom Cryptographic Drive	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Bootkit	DLL Search Order Hijacking	Compiled HTML File	Exploitation for Credential Access	Network Share Discovery	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Other Media	Firmware Corruption
Spearphishing via Service	Execution through Module Load	Browser Extensions	Escalation	Component Firmware	Forced Authentication	Network Sniffing	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Network Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Change Default File Association	Component Object Model Hijacking	Extra Window Memory Injection	Hooking	>Password Policy Discovery	Pass the Ticket	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Network Denial of Service
Trusted Relationship	Graphical User Interface	Component Firmware	File System Permissions	Connection Proxy	Input Capture	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Domain Fronting	Resource Hijacking	
Valid Accounts	InstallUtil	Component Object Model Hijacking	Control Panel Items Weakness	DCShadow	Input Prompt	Permission Groups Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	
	LSASS Driver	Create Account	Hooking	Deobfuscate/Decode Files or Information	Input Capture	Process Discovery	Remote Services	Input Capture	Fallback Channels		Runtime Data Manipulation
	Mshta	DLL Search Order Hijacking	Image File Execution Options Injection	Disabling Security Tools	Input Prompt	Query Registry	Replication Through	Man in the Browser	Multi-hop Proxy		Service Stop
	PowerShell	External Remote Services	New Service	LMNR/NBT-NS Poisoning and Relay	Input Prompt	Remote System Discovery	Remote File Copy	Multi-hop Proxy	Multi-Stage Channels		Stored Data Manipulation
	Regsvcs/Regasm	File System Permissions	Parent PID Spoofing	DLL Search Order Hijacking	Input Prompt	Security Software Discovery	Shared Webroot	Multi-Stage Channels	Multi-band Communication		System Shutdown/Reboot
	Regsvr32	Weakness	Path Interception	DLL Side-Loading	Input Prompt	Network Sniffing	Taint Shared Content	Multi-layer Encryption			Transmitted Data Manipulation
	Rundl32	Hidden Files and Directories	Port Monitors	Private Keys	Input Prompt	Password Filter DLL	Third-party Software	Remote Access Tools			
	Scheduled Task	Hooking	PowerShell Profile	Execution Guardrails	Input Prompt	System Information Discovery	Shared Webroot	Remote File Copy			
	Scripting	Hypervisor	Process Injection	Steal Web Session Cookie	Input Prompt	System Network Configuration Discovery	Taint Shared Content	Standard Application Layer Protocol			
	Service Execution	Image File Execution Options Injection	Scheduled Task	Two-Factor Authentication Interception	Input Prompt	System Network Connections Discovery	System Owner/User Discovery	Standard Cryptographic Protocol			
	Signed Binary Proxy Execution	Service Registry Permissions	Service Registry Permissions	File Deletion	Input Prompt	System Service Discovery	System Service Discovery	Standard Non-Application Layer Protocol			
	Signed Script Proxy Execution	Logon Scripts	Weakness	File System Logical Offsets	Input Prompt	System Time Discovery	System Time Discovery	Uncommonly Used Port			
	Third-party Software	LSASS Driver	SID-History Injection	Group Policy Modification	Input Prompt	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Web Service			
Trusted Developer Utilities	Modify Existing Service	Valid Accounts	Hidden Files and Directories								
User Execution	Netshell Helper DLL	Web Shell	Hidden Window								
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								
			Indirect Command Execution								
			Install Root Certificate								





Discovery	Lateral Movement
23 items	16 items
Account Discovery	Application Deployment Software
Application Window Discovery	Component Object Model and Distributed COM
Browser Bookmark Discovery	Exploitation of Remote Services
Domain Trust Discovery	Internal Spearphishing
File and Directory Discovery	Logon Scripts
Network Service Scanning	Pass the Hash
Network Share Discovery	Pass the Ticket
Network Sniffing	Remote Desktop Protocol
Password Policy Discovery	Remote File Copy
Peripheral Device Discovery	Remote Services
Permission Groups Discovery	Replication Through Removable Media
Process Discovery	Shared Webroot
Query Registry	Taint Shared Content
Remote System Discovery	Third-party Software
Security Software Discovery	Windows Admin Shares
Software Discovery	
System Information Discovery T1082	Windows Remote
System Network Configuration Discovery	-Available data sources: Element -Process monitoring, Process command-line parameters -ATT&CK data sources: -Process monitoring, Process command-line parameters
System Network Connection Discovery	-ATT&CK data sources: -Process monitoring, Process command-line parameters
System Owner/User Discovery	-Products: Carbonblack
System Service Discovery	
System Time Discovery	
Virtualization/Sandbox Evasion	

Detection File & Scoring

Detection scores							
Score	Score name	Degree of detection	Timing	Coverage of the technique	Opportunities to bypass detection	False Negatives	False Positives
-1	None	None	N/A	None	N/A	N/A	N/A
0	Forensics / context	None	Possibly not real time	None	N/A	N/A	N/A
1	Basic	Signature based	Possibly not real time	Small number of aspects of the technique	Bypassing (evasion/obfuscation) could be possible	High	Possibly high
2	Fair	(Correlation) rule(s)	Possibly not real time	More aspects of the technique compared to "1/Basic"	Bypassing (evasion/obfuscation) could be possible	Less high	May be present
3	Good	More complex analytics	Real time	Many known aspects of the technique	Bypassing (evasion/obfuscation) could be possible	Present	May be present but are easy to recognize and can possibly be filtered out.
4	Very good	More complex analytics	Real time	Almost all known aspects of the technique	Bypassing (evasion/obfuscation) is hard	Low	May be present but are easy to recognize and can possibly be filtered out.
5	Excellent	More complex analytics	Real time	All known aspects of the technique	Bypassing (evasion/obfuscation) is hard	Very low	May be present but are easy to recognize and can possibly be filtered out.

```
technique_id: T1218
technique_name: Signed Binary Proxy Execution
detection:
  applicable_to:
    - all
  location:
    - 'EDR'
  comment: ''
  score_logbook:
    - date: 2019-07-24
      score: 4
      comment: 'Feed icon Signed Binary Proxy Execution Extrac32 | MSI downloading Installer | Signed Binary Proxy Execution - Bash.exe |
        - Findstr | Atbroker.exe| url.dll | advpack.dll - LaunchINFSection'
  visibility:
    applicable_to:
      - all
    comment: ''
```

Detection File



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	28 items	44 items	23 items	60 items	18 items	23 items	16 items	13 items	21 items	9 items	16 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	Account Access Removal
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Component Object Model and Distributed COM	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Clipboard Data	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Component Object Model and Distributed COM	Applnit DLLs	Applnit DLLs	Bypass User Account Control	Credentials from Web Browsers	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Control Panel Items	Application Shimming	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Dynamic Data Exchange	Authentication Package	Bypass User Account Control	Code Signing	Credentials in Registry	Network Service Scanning	Network Share Discovery	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Disk Structure Wipe	Endpoint Denial of Service
Spearphishing Link	BITS Jobs	DLL Search Order Hijacking	Compile After Delivery	Exploitation for Credential Access	Logon Scripts	Pass the Hash	Pass the Ticket	Data from Removable Media	Data Encoding	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service Load	Bootkit	Component Firmware	Component Firmware	Forced Authentication	Password Policy Discovery	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Data Obfuscation	Inhibit System Recovery	Network Denial of Service
Supply Chain Compromise	Execution for Client Execution	Change Default File Association	Extra Window Memory Injection	Hooking	Input Capture	Permission Groups Discovery	Remote File Copy	Email Collection	Domain Fronting	Exfiltration Over Physical Medium	Resource Hijacking
Trusted Relationship	Graphical User Interface	Component Firmware	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Input Collection	Fallback Channels	Scheduled Transfer	Runtime Data Manipulation
Valid Accounts	InstallUtil	Component Object Model Hijacking	Hooking	DCShadow	Kerberoasting	Query Registry	Shared Webroot	Man in the Browser	Multi-hop Proxy	Service Stop	Stored Data Manipulation
	LSASS Driver	Create Account	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content	Screen Capture	Multi-Stage Channels	System Shutdown/Reboot	Transmitted Data Manipulation
	Mshta	PowerShell	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Video Capture	Multiband Communication	Remote Access Tools	
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Search Order Hijacking	>Password Filter DLL	Software Discovery	Third-party Software	Windows Admin Shares	Multilayer Encryption	Remote File Copy	
	Regsvr32	File System Permissions Weakness	Path Interception	DLL Side-Loading	Private Keys	System Information Discovery	System Network Configuration Discovery	Windows Remote Management	Standard Application Layer Protocol	Standard Cryptographic Protocol	
	Rundl32	Hidden Files and Directories	Port Monitors	Execution Guardrails	Steal Web Session Cookie	System Network Connections Discovery	System Owner/User Discovery		Standard Non-Application Layer Protocol	Uncommonly Used Port	
	Scheduled Task	Hooking	PowerShell Profile	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Service Discovery	System Time Discovery		Web Service		
	Scripting	Hypervisor	Process Injection	Extra Window Memory Injection		System Time Discovery	Virtualization/Sandbox Evasion				
	Service Execution	Image File Execution Options Injection	Scheduled Task	File and Directory Permissions Modification							
	Signed Binary Proxy Execution	Logon Scripts	Service Registry Permissions Weakness	File Deletion							
	Signed Script Proxy Execution	LSASS Driver	SID-History Injection	File System Logical Offsets							
	Third-party Software	Modify Existing Service	Valid Accounts	Group Policy Modification							
	Trusted Developer Utilities	Ntsh Helper DLL	Web Shell	Hidden Files and Directories							
	User Execution	New Service		Hidden Window							
	Windows Management Instrumentation	Office Application Startup		Image File Execution Options Injection							
	Windows Remote Management	Path Interception		Indicator Blocking							
	XSL Script Processing	Port Monitors		Indicator Removal from Tools							
		PowerShell Profile		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							
		Server Software Component		Mshta							
		Service Registry Permissions		Network Share Connection Removal							



Discovery	Lateral Movement
23 items	16 items
Account Discovery	Application Deployment Software
Application Window Discovery	Component Object Model and Distributed COM
Browser Bookmark Discovery	Exploitation of Remote Services
Domain Trust Discovery	Internal Spearphishing
File and Directory Discovery	Logon Scripts
Network Service Scanning	Pass the Hash
Network Share Discovery	Pass the Ticket
Network Sniffing	Remote Desktop Protocol
>Password Policy Discovery	Remote File Copy
Peripheral Device Discovery	Remote Services
Permission Groups Discovery	Replication Through Removable Media
Process Discovery	Shared Webroot
Query Registry	Taint Shared Content
Remote System Discovery	Third-party Software
Security Software Discovery	Windows Admin Shares
Software Discovery	Windows Remote Management
System Information Discovery	<p>T1082</p> <p>Score: 3</p> <p>Metadata:</p> <ul style="list-style-type: none"> -Applicable to: all -Detection score: 3 -Detection location: Third party product A <p>System Owner/User: -Technique comment: -</p> <p>System Service Discovery: -Detection comment: -</p>
System Time Discovery	Virtualization/Sandbox Evasion
Virtualization/Sandbox Evasion	

Detection + Logging

Visibility and Detection example x +

selection controls layer controls technique controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	28 items	44 items	23 items	60 items	18 items	23 items	16 items	13 items	21 items	9 items	16 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	Account Access Removal
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Component Object Model and Distributed COM	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Domain Trust Discovery	Clipboard Data	Connection Proxy	Data Encrypted	T1485 Metadata encrypted for impact
Hardware Additions	Component Object Model and Distributed COM	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials from Web Browsers	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	- Available data sources: Process monitoring - ATT&CK data sources: File monitoring, Process command-line parameters, Process monitoring
Replication Through Removable Media	Control Panel Items	Application Shimming	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Internal Spearphishing	Data from Local System	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Exfiltration Over Command and Control Channel
Spearphishing Attachment	Dynamic Data Exchange	Authentication Package	Bypass User Account Control	Code Signing	Credentials in Registry	Network Share Discovery	Logon Scripts	Custom Cryptographic Protocol	Data Encoding	Data Obfuscation	Exfiltration Over Physical Medium
Spearphishing Link	Execution through API	BITS Jobs	DLL Search Order Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Hash	Data from Removable Media	Data Staged	Domain Fronting	Exfiltration Over Network Medium
Spearphishing via Service	Execution through Module Load	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Component Firmware	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Network Denial of Service
Supply Chain Compromise	Exploitation for Client execution	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Pass the Ticket	Remote File Copy	Input Capture	Fallback Channels	Scheduled Transfer
Trusted Relationship	Graphical User Interface	Change Default File Association	Extra Window Memory Injection	Connection Proxy	Input Capture	Permission Groups Discovery	Process Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy	Resource Hijacking
Valid Accounts	Component Firmware	File System Permissions Weakness	File System Permissions Weakness	File System Permissions Weakness	Input Prompt	Query Registry	Remote System Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels	Runtime Data Manipulation
	Component Object Model Hijacking	Control Panel Items	Hooking	DCShadow	Kerberoasting	Security Software Discovery	Taint Shared Content	Third-party Software	Video Capture	Multiband Communication	Service Stop
	Create Account	Image File Execution Options Injection	Image File Execution Options Injection	LLMNR/NBT-NS Poisoning and Relay	Network Sniffing	Software Discovery	Windows Admin Shares	Windows Remote Management		Multilayer Encryption	Stored Data Manipulation
	DLL Search Order Hijacking	New Service	Disabling Security Tools	DLL Search Order Hijacking	>Password Filter DLL	System Information Discovery				Remote Access Tools	System Shutdown/Reboot
	PowerShell	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys	System Network Configuration Discovery				Remote File Copy	Transmitted Data Manipulation
	Regsvcs/Regasm	File System Permissions Weakness	Path Interception	Execution Guardrails	Steal Web Session Cookie	System Network Connections Discovery				Standard Application Layer Protocol	
	Regsvr32	Hidden Files and Directories	Port Monitors	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery				Standard Cryptographic Protocol	
	Rundll32	PowerShell	Scheduled Task	Extra Window Memory Injection		System Service Discovery				Standard Non-Application Layer Protocol	
	Scheduled Task	Hypervisor	Service Registry Permissions Weakness	Scheduled Task		System Time Discovery				Uncommonly Used Port	
	Scripting	Image File Execution Options Injection	Logon Scripts	File and Directory Permissions Modification		Virtualization/Sandbox Evasion				Web Service	
Service Execution	Service Execution	Signed Binary Proxy Execution	Signed Script Proxy Execution	Service Registry Permissions Weakness	File Deletion						
	Signed Binary Proxy Execution	Signed Script Proxy Execution	LSASS Driver	SID-History Injection	File System Logical Offsets						
	Signed Script Proxy Execution	Third-party Software	Modify Existing Service	Valid Accounts	Group Policy Modification						
	Third-party Software	Trusted Developer Utilities	User Execution	Web Shell	Hidden Files and Directories						
	Trusted Developer Utilities	Windows Management Instrumentation	Windows Management Instrumentation		Hidden Window						
	User Execution	Office Application Startup	Office Application Startup		Image File Execution Options Injection						
	Windows Management Instrumentation	Windows Remote Management	Path Interception		Indicator Blocking						
	Windows Remote Management	Port Monitors	Port Monitors		Indicator Removal from Tools						
	Port Monitors	XSL Script Processing	PowerShell Profile		Indicator Removal on Host						
	PowerShell Profile	Redundant Access	Registry Run Keys / Startup		Indirect Command Execution						

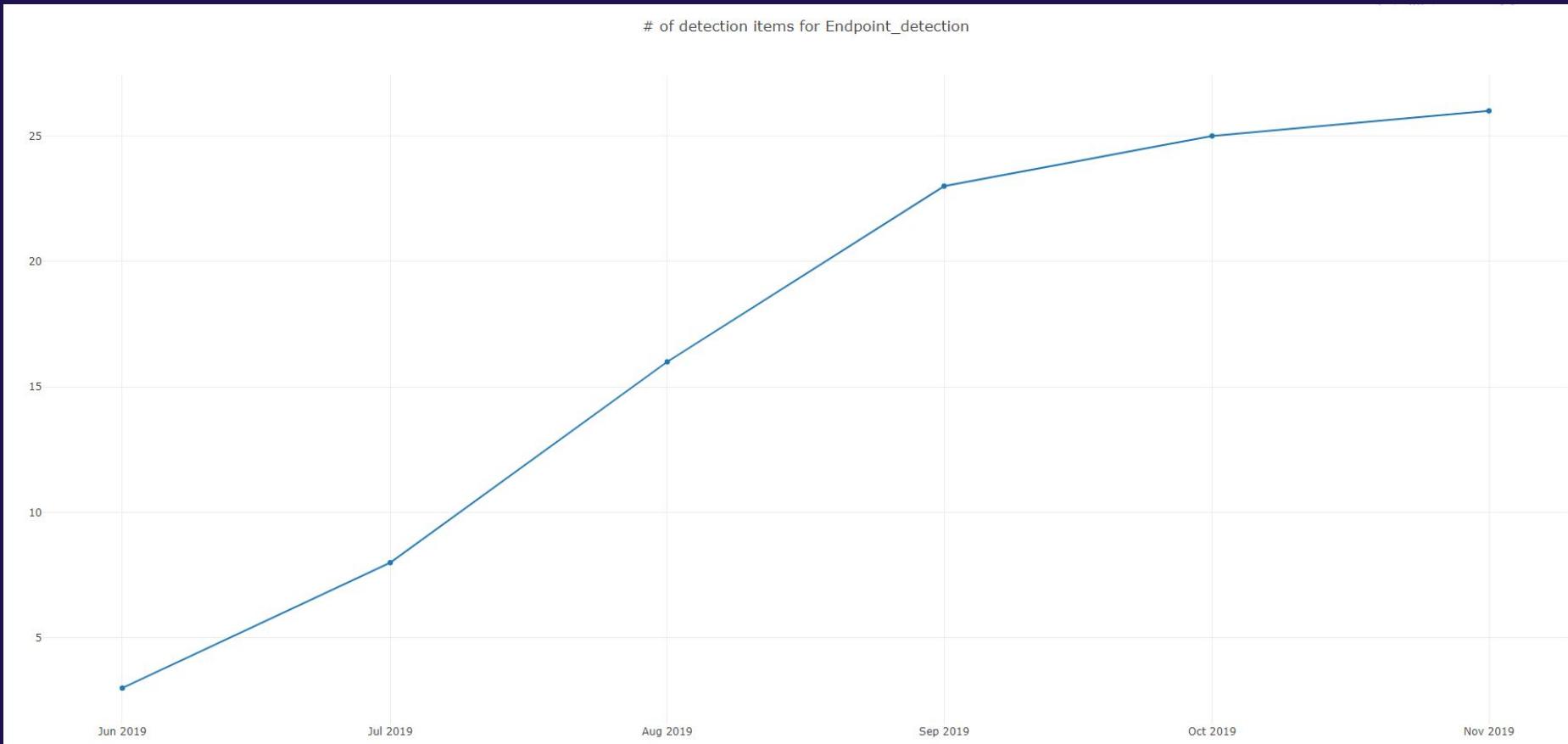
selection controls layer controls technique controls

Legend:

- #1976D2 Visibility
- #BBC34A Detection
- #f9a825 Visibility and detection

Add Item Clear

Improvement Graph



Attacker APT Heat Map

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
11 items	28 items	44 items	23 items	60 items	18 items	23 items	16 items	13 items	21 items	9 items
Spearphishing Attachment	PowerShell	Registry Run Keys / Startup Folder	Scheduled Task	Obfuscated Files or Information	Credential Dumping	System Network Configuration Discovery	Remote File Copy	Screen Capture	Remote File Copy	Data Compressed
Spearphishing Link	Scripting	Scheduled Task	Valid Accounts	Scripting	Brute Force	System Owner/User Discovery	Remote Desktop Protocol	Input Capture	Commonly Used Port	Exfiltration Over Alternative Protocol
Valid Accounts	User Execution	Valid Accounts	Web Shell	File Deletion	Input Capture	File and Directory Discovery	R1033 Services	Email Collection	Standard Application Layer Protocol	
Spearphishing via Service	Command-Line Interface	Redundant Access	Bypass User Account Control	Valid Accounts	Credentials in Files	Network Service Scanning	T1034 Object Model	Automated Collection	Uncommonly Used Port	Data Encrypted
Drive-by Compromise	Scheduled Task	Web Shell	Exploitation for Privilege Escalation	Connection Proxy	Account Manipulation	Process Discovery	T1035 -Groups: MuddyWater, APT39, Magic Hound, OilRig Software	Audio Capture	Automated Exfiltration	Uncommonly Used Port
External Remote Services	Rundll32	Account Manipulation	Deobfuscate/Decode Files or Information	Credentials from Web Browsers	System Information Discovery	Clipboard Data	Clipboard Data	Connection Proxy	Data Transfer Size Limits	Standard Cryptographic Protocol
Exploit Public-Facing Application	Windows Management Instrumentation	Create Account	Access Token Manipulation	Hidden Window	Network Sniffing	Account Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Exfiltration Over Command and Control Channel
Hardware Additions	CMSTP	External Remote Services	Accessibility Features	Redundant Access	Credentials in Registry	Network Sniffing	Internal Spearphishing	Data from Local System	Data from Local System	Exfiltration Over Other Network Medium
Replication Through Removable Media	Compiled HTML File	Shortcut Modification	AppCert DLLs	Rundll32	Exploitation for Credential Access	Password Policy Discovery	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Physical Medium
Supply Chain Compromise	Component Object Model and Distributed COM	Accessibility Features	AppInit DLLs	AppInit DLLs	Software Packing	Permission Groups Discovery	Pass the Hash	Data from Removable Media	Fallback Channels	Scheduled Transfer
Trusted Relationship	Dynamic Data Exchange	AppCert DLLs	DLL Search Order Hijacking	Bypass User Account Control	Forced Authentication	Query Registry	Pass the Ticket	Replication Through Removable Media	Multi-Stage Channels	Web Service
	Exploitation for Client Execution	AppInit DLLs	Extra Window Memory Injection	CMSTP	Hooking	Remote System Discovery	Data Staged	Man in the Browser	Communication Through Removable Media	Custom Cryptographic Protocol
	Mshta	Application Shimming	Code Signing	Input Prompt	Kerberoasting	Security Software Discovery	Taint Shared Content	Video Capture	Data Obfuscation	
	Authentication Package	File System Permissions Weakness	Compile After Delivery	LLMNR/NBT-NS Poisoning and Relay	System Network Connections Discovery	System Service Discovery	Third-party Software	Windows Admin Shares	Domain Fronting	
	Control Panel Items	BITS Jobs	Compiled HTML File	password Filter DLL	Application Window Discovery	Windows Remote Management	Windows Remote Management	Windows Remote Management	Domain Generation Algorithms	
	Execution through API	Bootkit	Hooking	Execution Guardrails	Browser Bookmark Discovery	Domain Trust Discovery	Domain Trust Discovery	Domain Trust Discovery	Multi-hop Proxy	
	Execution through Module Load	Browser Extensions	Image File Execution Options Injection	Indicator Removal from Tools	Steal Web Session Cookie	Network Share Discovery	Network Share Discovery	Network Share Discovery	Multiband Communication	
	Graphical User Interface	Change Default File Association	New Service	Masquerading	Two-Factor Authentication Interception	Peripheral Device Discovery	Peripheral Device Discovery	Peripheral Device Discovery	Peripheral Device Discovery	
	InstallUtil	Component Firmware	Parent PID Spoofing	Mshta	Two-Factor Authentication Interception	Peripheral Device Discovery	Peripheral Device Discovery	Peripheral Device Discovery	Peripheral Device Discovery	
	LSASS Driver	Component Object Model	Path Interception	Web Service	Peripheral Device Discovery	Peripheral Device Discovery	Peripheral Device Discovery	Peripheral Device Discovery	Peripheral Device Discovery	

Attacker + Detections

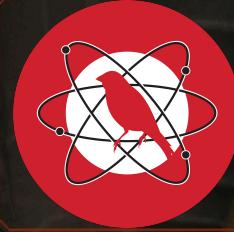
Without certain tools

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	63 items	32 items	73 items	23 items	25 items	20 items	14 items	22 items	10 items	16 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal	
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction	
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Data Encrypted	Data Encrypted for Impact	
Hardware Additions	Compiled HTML File	AppCert DLLs	AppNuit DLLs	BITS Jobs	Cloud Instance Metadata API	Cloud Service Dashboard	Component Object Model and Distributed COM	Data from Cloud Storage Object	Connection Proxy	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	Application Shimming	Bypass User Account Control	Credential Dumping	Cloud Service Discovery	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Exfiltration Over Alternative Protocol	
Spearphishing Attachment	Control Panel Items	Authentication Package	DLL Search Order Hijacking	CMSTP	Credentials in Files	File and Directory Discovery	Internal Spearphishing	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	
Spearphishing Link	Dynamic Data Exchange	BITS Jobs	Dylib Hijacking	Code Signing	Credentials in Registry	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	
Spearphishing via Service	Execution through API	Bootkit	Elevated Execution with Prompt	Compile After Delivery	Exploitation for Credential Access	Network Share Discovery	Pass the Hash	Domain Fronting	Domain Generation Algorithms	Inhibit System Recovery	
Supply Chain Compromise	Execution through Module Load	Browser Extensions	Emon	Compiled HTML File	Forced Authentication	Network Sniffing	Pass the Ticket	Data from Removable Media	Exfiltration Over Physical Medium	Network Denial of Service	
Trusted Relationship	Exploitation for Client Execution	Change Default File Association	Exploitation for Privilege Escalation	Component Firmware	Hooking	Password Policy Discovery	Remote Desktop Protocol	Data Staged	Fallback Channels	Resource Hijacking	
Valid Accounts	Graphical User Interface	Component Firmware	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote File Copy	Email Collection	Multi-hop Proxy	Runtime Data Manipulation	
InstallUtil	Component Object Model Hijacking	File System Permissions Weakness	Connection Proxy	Connection Prompt	Input Prompt	Permission Groups Discovery	Remote Services	Input Capture	Multi-Stage Channels	Service Stop	
Local Job Scheduling	Create Account	Control Panel Items	Kerberoasting	Process Discovery	Query Registry	Replication Through Removable Media	Man in the Browser	Shared Webroot	Port Knocking	Stored Data Manipulation	
LSASS Driver	DLL Search Order Hijacking	Dylib Hijacking	DCShadow	Keychain	Remote System Discovery	Screen Capture	Multiband Communication	SSH Hijacking	Remote Access Tools	System Shutdown/Reboot	
Mshta	DLL Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information Relay	LMNNR/NBT-NS Poisoning and Relay	Security Software Discovery	Shared Webroot	Multilayer Encryption	Stolen Webroot	Remote File Copy	Transmitted Data Manipulation	
PowerShell	Emond	Launch Daemon	DLL Search Order Hijacking	DLL Side-Loading	Software Discovery	SSH Hijacking	Port Knocking	Taint Shared Content	Standard Application Layer Protocol		
Regnix/Regasm	External Remote Services	New Service	DLL Side-Loading	Private Keys	System Information Discovery	Taint Shared Content	Remote Access Tools	System Network Configuration Discovery	Standard Cryptographic Protocol		
Regrv32	File System Permissions Weakness	Parent PID Spoofing	Execution Guardrails	Securityd Memory	System Network Configuration Discovery	Third-party Software	Remote File Copy	Steal Application Access Token	Standard Non-Application Layer Protocol		
Rundll32	Hidden Files and Directories	Path Interception	Exploitation for Defense Evasion	Steal Application Access Token	System Network Connections Discovery	Windows Admin Shares	Standard Application Layer Protocol	Steal Web Session Cookie	Uncommonly Used Port		
Scheduled Task	Hooking	Plist Modification	Extra Window Memory Injection	Steal Web Session Cookie	System Owner/User Discovery	Windows Remote Management	Standard Cryptographic Protocol	System Time Discovery	Web Service		
Scripting	Hypervisor	Port Monitor	PowerShell Profile	File and Directory Permissions Modification	System Service Discovery	Virtualization/Sandbox Evasion	Standard Non-Application Layer Protocol	Two-Factor Authentication Interception	Uncommonly Used Port		
Service Execution	Image File Execution Options Injection	Process Injection	File Deletion	File System Logical Offsets	Virtualization/Sandbox Evasion	Web Service	Uncommonly Used Port	Virtualization/Sandbox Evasion	Web Service		
Signed Binary Proxy Execution	Implant Container Image	Scheduled Task	Gatekeeper Bypass	Group Policy Modification	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Uncommonly Used Port	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion		
Signed Script Proxy Execution	Kernel Modules and Extensions	Service Registry Permissions Weakness	Hidden Files and Directories	Hidden Files and Directories	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Uncommonly Used Port	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion		
Source	Launch Agent	Setuid and Setgid	SID-History Injection	Hidden Users	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Uncommonly Used Port	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion		
Space after Filename	Launch Daemon	Launchd	Startup Item	Hidden Windows	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Uncommonly Used Port	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion		
Third-party Software	Launchctl	LC_LOAD_DYLIB Addition	Sudo	HISTCONTROL	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Uncommonly Used Port	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion		
Trap	Local Job Scheduling	Logon Item	Sudo Caching	Image File Execution Options Injection	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Uncommonly Used Port	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion		
Trusted Developer Utilities	Login Script	Web Shell	Valid Accounts	Indicator Blocking	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Uncommonly Used Port	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion		
Windows Management Instrumentation	Logon Scripts	Indicator Removal from Tools	Indicator Removal on Host	Indirect Command Execution	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Uncommonly Used Port	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion		
Windows Remote Management	LSASS Driver	Indicator Removal on Host	Install Root Certificate	Indirect Command Execution	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Uncommonly Used Port	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion		
XSL Script Processing	Modify Existing Service	New Service	Installutil	Indirect Command Execution	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Uncommonly Used Port	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion		
	Ntsh Helper DLL	Office Application Startup	Launchctl	LC_MAIN Hijacking	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Uncommonly Used Port	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion		
	New Service	Path Interception	LC_MAIN Hijacking	Masquerading	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Uncommonly Used Port	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion		
	Office Application Startup	Plug Modification	Port Knocking	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Uncommonly Used Port	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion		
	Path Interception	Port Monitors	Port Knocking	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Uncommonly Used Port	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion		

With tools

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	63 items	32 items	73 items	23 items	25 items	20 items	14 items	22 items	10 items	16 items
Drive-by Compromise	AppleScript	bash_profile and .zshrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	BITS Jobs	Cloud Instance Metadata API	Cloud Service Dashboard	Component Object Model and Distributed COM	Data from Cloud Storage Object	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	Application Shimming	Application Shimming	Bypass User Account Control	Credential Dumping	Cloud Service Discovery	Exploitation of Remote Services	Data from Information Repositories	Exfiltration Over Alternative Protocol	Disk Content Wipe	Disk Structure Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Command History	Credentials from Web Browser	Domain Trust Discovery	Internal Spearphishing	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Network Shared Drive	Data Obsfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through API	BITS Jobs	DLL Hijacking	Code Signing	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Removable Media	Domain Fronting	Domain Generation Algorithms	Inhibit System Recovery
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compile After Delivery	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data Staged	Fallback Channels	Exfiltration Over Physical Medium	Network Denial of Service
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Email Collection	Multi-hop Proxy	Fallback: Channels	Resource Hijacking
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Firmware	Hooking	Password Policy Discovery	Remote File Copy	Input Capture	Multi-Stage Channels	Scheduled Transfer	Transfer Data to Cloud Account
	InstallUtil	Component Firmware	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Man in the Browser	Multi-band Communication	Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Connection Proxy	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Input Capture	Screen Capture	Multilayer Encryption	Service Stop
	Local Job Scheduling	Create Account	Hooks	Kerberoasting	Process Discovery	Query Registry	Remote System Discovery	SSH Hijacking	Port Knocking	Taint Shared Content	Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	DCShadow	Keychain	Remote Services	Security Software Discovery	Security Software Discovery	Taint Shared Content	Third-party Software	Standard Application Layer Protocol	System Shutdown/Reboot
	Mshta	DYLB Hijacking	Image File Execution Options Injection	LMNR/NBT-NS Poisoning and Relay	Remote Services	Shared Webroot	Shared Webroot	SSH Hijacking	Standard Cryptographic Protocol	Standard Non-Application Layer Protocol	Transmitted Data Manipulation
	PowerShell	Emond	Launch Daemon	Relay	Remote System Discovery	Software Discovery	Software Discovery	Taint Shared Content	Standard Cryptographic Protocol	Standard Non-Application Layer Protocol	
	Regsvr/Regasm	External Remote Services	New Service	Reliable Side-Loading	Security Software Discovery	System Information Discovery	System Network Configuration Discovery	System Owner/User Discovery	Standard Cryptographic Protocol	Uncommonly Used Port	
	Regsvr32	File System Permissions Weakness	Parent PID Spoofing	Execution Guardrails	System Network Connections Discovery	System Network Connections Discovery	System Service Discovery	System Time Discovery	Standard Cryptographic Protocol	Web Service	
	Rundll32	Hidden Files and Directories	Path Interception	Security Memory	Steal Application Access Token	System Owner/User Discovery	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Plist Modification	Steal Application Access Token	Steal Web Session Cookie	System Service Discovery			Standard Cryptographic Protocol		
	Scripting	Hypervisor	Port Monitors	Steal Application Access Token	Two-Factor Authentication Interception	System Time Discovery			Standard Cryptographic Protocol		
	Service Execution	Image File Execution Options Injection	PowerShell Profile	File and Directory Permissions Modification	Two-Factor Authentication Interception	Virtualization/Sandbox Evasion			Standard Cryptographic Protocol		
	Signed Binary Proxy Execution	Implant Container Image	Process Injection	File Deletion					Standard Cryptographic Protocol		
	Signed Script Proxy Execution	Kernel Modules and Extensions	Scheduled Task	File System Logical Offsets					Standard Cryptographic Protocol		
	Source	Launch Agent	Service Registry Permissions Weakness	Gatekeeper Bypass					Standard Cryptographic Protocol		
	Space after Rfilename	Launch Daemon	Setuid and Setgid	Group Policy Modification					Standard Cryptographic Protocol		
	Third-party Software	Launchctl	SID-History Injection	Hidden Files and Directories					Standard Cryptographic Protocol		
	Trap	LC_LOAD_DYLIB Addition	Startup Items	Hidden Users					Standard Cryptographic Protocol		
	Trusted Developer Utilities	Local Job Scheduling	Sudo	Hidden Window					Standard Cryptographic Protocol		
	User Execution	Login Item	Sudo Caching	HISTCONTROL					Standard Cryptographic Protocol		
	Windows Management Instrumentation	Logon Scripts	Valid Accounts	Image File Execution Options Injection					Standard Cryptographic Protocol		
	Windows Remote Management	LSASS Driver	Web Shell	Indicator Blocking					Standard Cryptographic Protocol		
	XSL Script Processing	Modify Existing Service		Indicator Removal from Tools					Standard Cryptographic Protocol		
		Netsvc Helper DLL		Indicator Removal on Host					Standard Cryptographic Protocol		
		New Service		Indirect Command Execution					Standard Cryptographic Protocol		
		Office Application Startup		Install Root Certificate					Standard Cryptographic Protocol		
		Path Interception		InstallUtil					Standard Cryptographic Protocol		
		Plist Modification		Launchctl					Standard Cryptographic Protocol		
		Port Knocking		LC_MAIN Hijacking					Standard Cryptographic Protocol		
		Process Interception		Masquerading					Standard Cryptographic Protocol		

Atomic Red Team



- Developed by Red Canary
- Descriptions on how to run the attack yourself
- Includes Automation
- Organized by ATT&CK ID

AtomicRedTeam.info

Start

Python, Ruby and Powershell Automation

```
attack_technique: T1105
display_name: Remote File Copy

atomic_tests:
- name: rsync remote file copy (push)
  description: |
    Utilize rsync to perform a remote file copy (push)
  supported_platforms:
    - linux
    - macos
  input_arguments:
    local_path:
      description: Path of folder to copy
      type: Path
      default: /tmp/adversary-rsync/
  username:
    description: User account to authenticate on remote host
    type: String
    default: victim
  remote_host:
    description: Remote host to copy toward
    type: String
    default: victim-host
  remote_path:
    description: Remote path to receive rsync
    type: Path
    default: /tmp/victim-files
  executor:
    name: bash
    command: |
      rsync -r #{local_path} #{username}@#{remote_host}:#{remote_path}
```

```
> T1105
=====
Remote File Copy - T1105
0.

-----
Name: certutil download (urlcache)
Description: Use certutil -urlcache argument to download a file from the web. Note - /urlcache also works!
Platforms: windows

Arguments:
remote_file: URL of file to copy (default: https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/LICENSE.txt)

local_path: Local path to place file (default: Atomic-license.txt)

Launcher: command_prompt
Command: cmd /c certutil -urlcache -split -f #{remote_file} #{local_path}

1.

-----
Name: certutil download (verifyctl)
Description: Use certutil -verifyctl argument to download a file from the web. Note - /verifyctl also works!
Platforms: windows

Arguments:
remote_file: URL of file to copy (default: https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/LICENSE.txt)

local_path: Local path to place file (default: Atomic-license.txt)

Launcher: powershell
Command: $datePath = "certutil-$((Get-Date -format yyyy_MM_dd_HH_mm))"
New-Item -Path $datePath -ItemType Directory
Set-Location $datePath
certutil -verifyctl -split -f #{remote_file}
Get-ChildItem | Where-Object {$__.Name -notlike "*.*"} | Foreach-Object { Move-Item $_.Name -Destination #{local_path} }

2.

-----
Name: Windows - BITSAdmin BITS Download
Description: This test uses BITSAdmin.exe to schedule a BITS job for the download of a file.
This technique is used by Qbot malware to download payloads.
Platforms: windows

Arguments:
bits_job_name: Name of the created BITS job (default: qcxb7)
remote_file: URL of file to copy (default: https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/LICENSE.txt)

local_path: Local path to place file (default: Atomic-license.txt)

Launcher: command_prompt
```

 MITRE

ATT&CK™

 Thanks

<https://github.com/mitre-attack/attack-navigator>

<https://github.com/rabobank-cdc/DeTTECT>

<https://atomicredteam.io/>



Marcus Bakker
(Twitter: @bakk3rm)
and Ruben Bouman
(Twitter:
@rubenb_2).