Not Enough Mitre

You You Require More Vespene ATT&CK



By Wade Wells

@WadingThruLogs

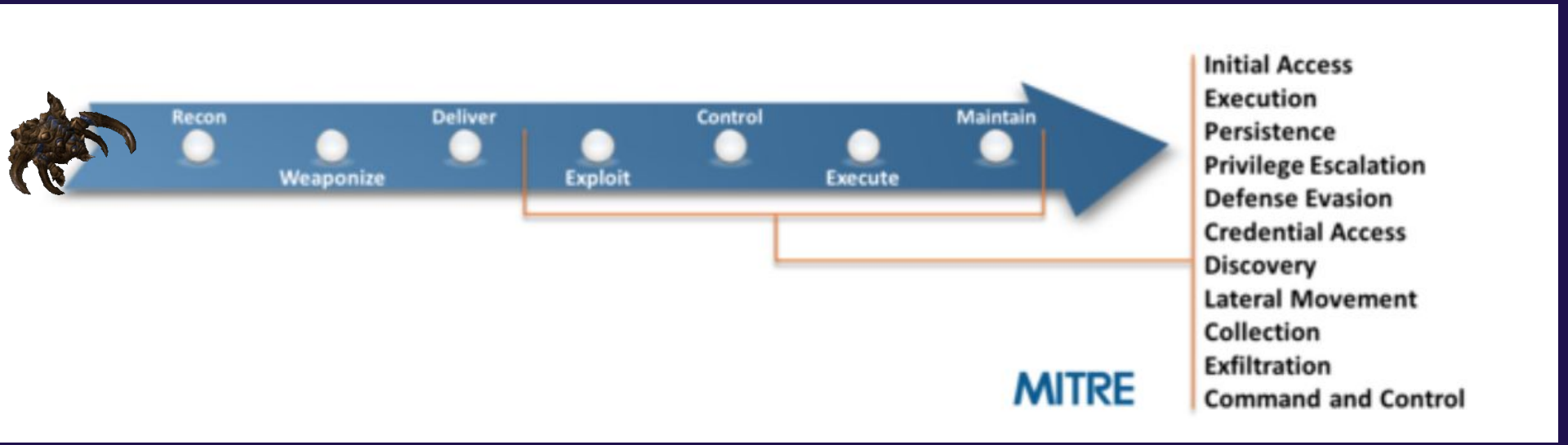

ATT&CK™
DeTT&CT
Attack
Navigator
Episode I
Atomic Red
Team
Episode III
DeTT&CT
Episode II
Free
Open Source

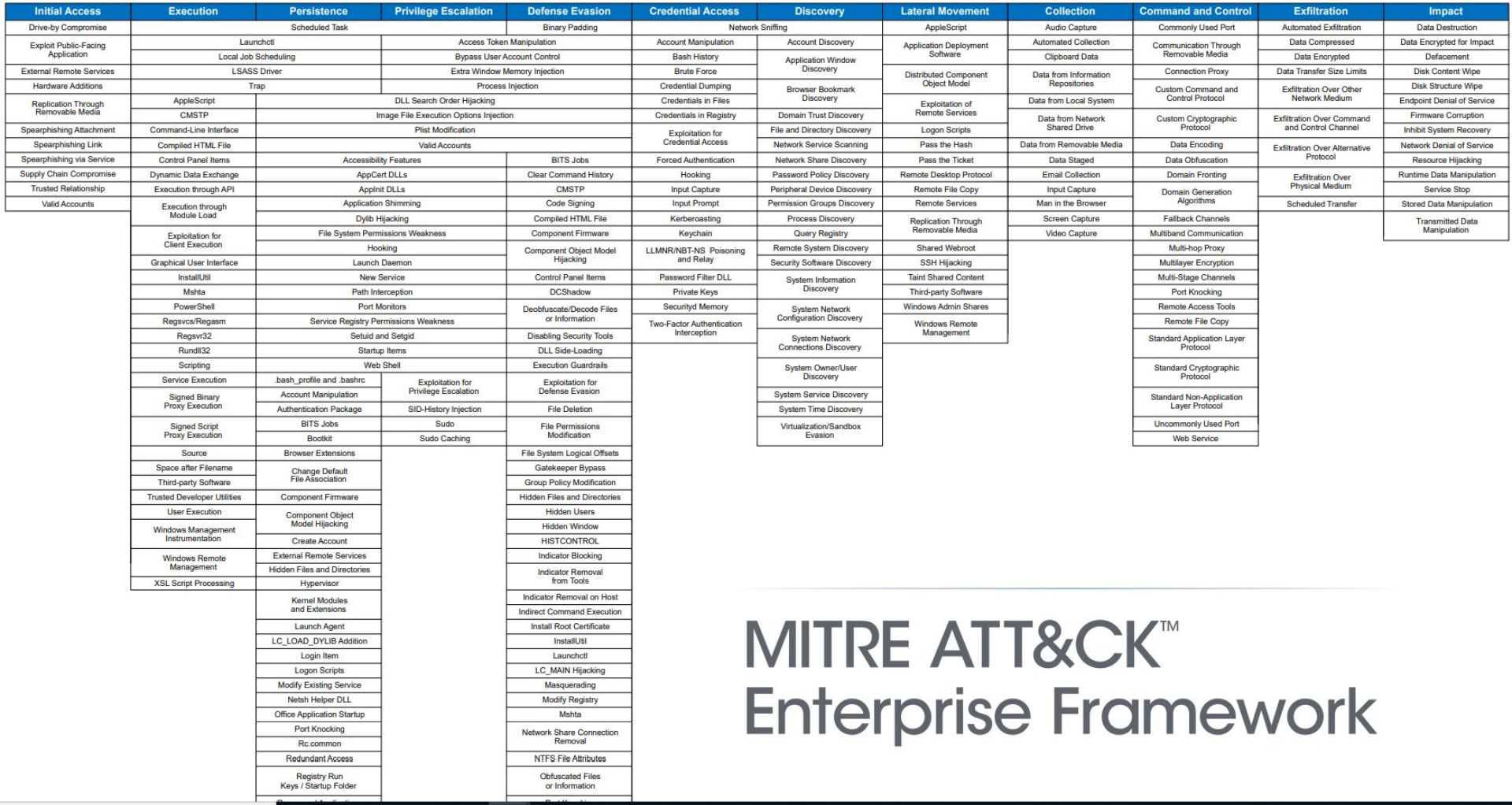
What can we DeTT&CT?

How do we keep track of what we can detect?

Adversarial Tactics, Techniques, and Common Knowledge Framework

Mitre ATT&CK Enterprise Framework




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

ATT&CK Navigator

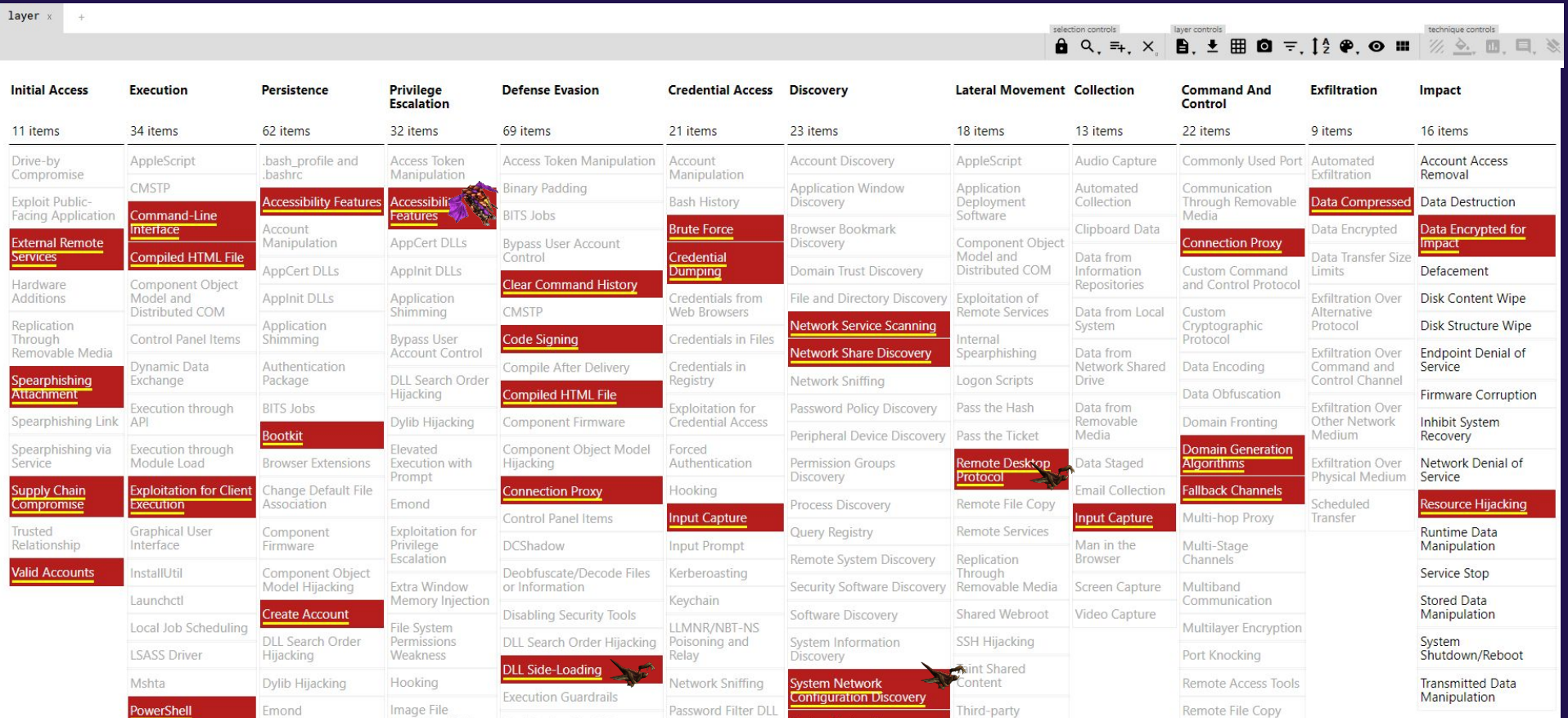
- Run as Iframe
- Consumes . json files
- Free data on Mitre Website

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

Start

github.com/mitre-attack/attack-navigator

Zerg Tactics, Techniques and Procedures



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	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness	Path Interception	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Cryptographic Protocol		
	Rundll32	Hidden Files and Directories	Plist Modification	Exploitation for Defense Evasion	Steal Web Session Cookie	System Owner/User Discovery			Standard Non-Application Layer Protocol		
	Scheduled Task	Hooking	Port Monitors	Extra Window Memory Injection	Two-Factor Authentication Interception	System Service Discovery			Uncommonly Used Port		
	Scripting	Hypervisor	PowerShell Profile	File and Directory Permissions Modification		System Time Discovery			Web Service		
	Service Execution	Image File Execution Options Injection	Process Injection	File Deletion		Virtualization/Sandbox Evasion					
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Scheduled Task	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Service Registry Permissions Weakness	Gatekeeper Bypass							
	Source	Launch Daemon	Setuid and Setgid	Group Policy Modification							
	Space after Filename	Launchctl	SID-History Injection	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Startup Items	Hidden Users							
	Trap	Local Job Scheduling	Sudo	Hidden Window							
	Trusted Developer Utilities	Login Item	Sudo Caching	HISTCONTROL							
	User Execution	Logon Scripts	Valid Accounts	Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver		Indicator Blocking							
	Windows Remote			Indicator Removal from Tools							

legend

#74c476	BOTH
#fce93b	APT29
#6baed6	APT3

Add Item Clear

DeTT&CT

Detect Tactics, Techniques & Combat Threats

DeTT&CT

- 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
 >>
```

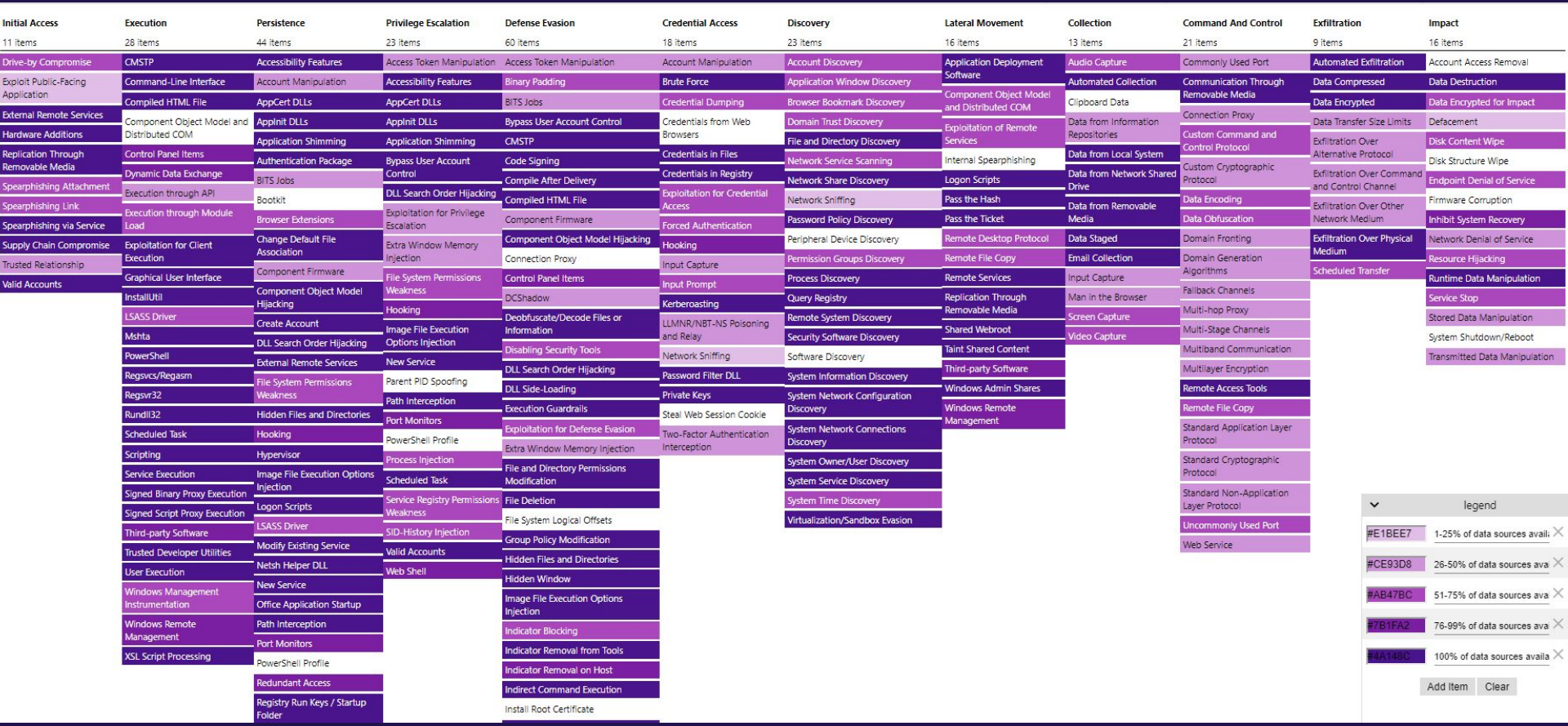
```
file_type: data-source-administration
name: Data sources
platform: windows
data_sources:
  # A data source is treated as not available when all dimensions of the data quality have a score of 0.
  # If desired you are free to add any key-value pairs.
  - data_source_name: Process monitoring
    date_registered: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

Data Source logging



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
System Information Discovery	
System Network Configuration Discovery	
System Network Connections Discovery	
System Owner/User Discovery	
System Service Discovery	
System Time Discovery	
Virtualization/Sandbox Evasion	

T1082

Metadata:

-Available data sources: Process monitoring, Process command-line parameters

-ATT&CK data sources: Process monitoring, Process command-line parameters

-Products: Carbonblack

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.

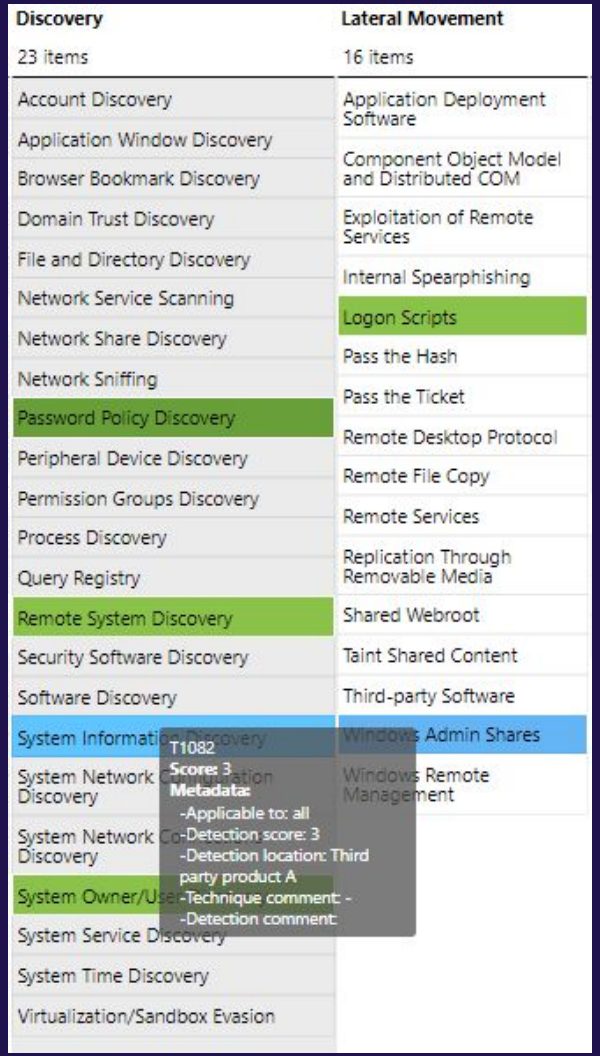
```
technique_id: T1218
technique_name: Signed Binary Proxy Execution
detection:
  applicable_to:
  - all
  location:
  - 'EDR'
  comment: ''
  score_logbook:
  - date: 2019-07-24
    score: 4
    comment: 'Feed icon Signed Binary Proxy Execution Extrac32 | MSI downloading Installer | Signed Binary Proxy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

Detection File

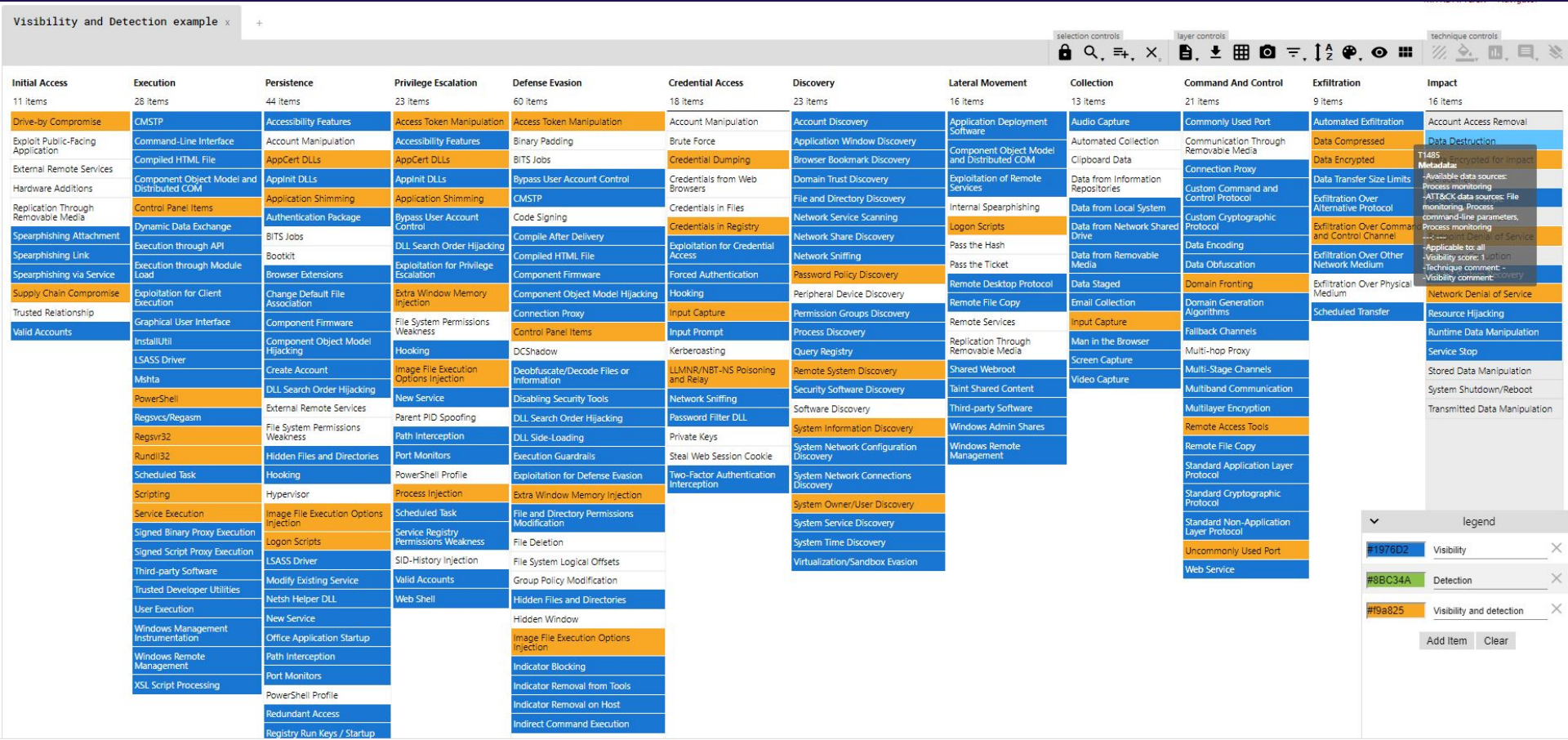
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	28 items	44 items	23 items	60 items	18 items	23 items	16 items	13 items	21 items	9 items	16 items
Drive-by Compromise	CMSTP	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	Exploitation of Remote Services	Clipboard Data	Connection Proxy	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	Internal Spearphishing	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	Logon Scripts	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	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Execution through API	BITS Jobs	DLL Search Order Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through Module Load	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Exploitation for Client Execution	Browser Extensions	Extra Window Memory Injection	Component Firmware	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Graphical User Interface	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	InstallUtil	Component Firmware	Hooking	Connection Proxy	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	LSASS Driver	Component Object Model Hijacking	Image File Execution Options Injection	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Mshta	Create Account	New Service	DCShadow	LLMNR/NBT-NS Poisoning and Relay	Query Registry	Taint Shared Content	Video Capture	Multiband Communication		Service Stop
	PowerShell	DLL Search Order Hijacking	Parent PID Spoofing	Deobfuscate/Decode Files or Information	Network Sniffing	Remote System Discovery	Third-party Software		Multilayer Encryption		Stored Data Manipulation
	Regsvcs/Regasm	External Remote Services	Path Interception	Disabling Security Tools	Password Filter DLL	Security Software Discovery	Windows Admin Shares		Remote Access Tools		System Shutdown/Reboot
	Regsvr32	File System Permissions Weakness	Port Monitors	DLL Search Order Hijacking	Private Keys	Software Discovery	Windows Remote Management		Remote File Copy		Transmitted Data Manipulation
	Rundll32	Hidden Files and Directories	PowerShell Profile	DLL Side-Loading	Steal Web Session Cookie	System Information Discovery			Standard Application Layer Protocol		
	Scheduled Task	Hooking	Process Injection	Execution Guardrails	Two-Factor Authentication Interception	System Network Configuration Discovery			Standard Cryptographic Protocol		
	Scripting	Hypervisor	Scheduled Task	Exploitation for Defense Evasion		System Network Connections Discovery			Standard Non-Application Layer Protocol		
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Extra Window Memory Injection		System Owner/User Discovery			Uncommonly Used Port		
	Signed Binary Proxy Execution	Logon Scripts	SID-History Injection	File and Directory Permissions Modification		System Service Discovery			Web Service		
	Signed Script Proxy Execution	LSASS Driver	Valid Accounts	File Deletion		System Time Discovery					
	Third-party Software	Modify Existing Service	Web Shell	File System Logical Offsets		Virtualization/Sandbox Evasion					
	Trusted Developer Utilities	Netsh Helper DLL		Group Policy Modification							
	User Execution	New Service		Hidden Files and Directories							
	Windows Management Instrumentation	Office Application Startup		Hidden Window							
	Windows Remote Management	Path Interception		Image File Execution Options Injection							
	XSL Script Processing	Port Monitors		Indicator Blocking							
		PowerShell Profile		Indicator Removal from Tools							
		Redundant Access		Indicator Removal on Host							
		Registry Run Keys / Startup Folder		Indirect Command Execution							
		Scheduled Task		Install Root Certificate							
		Screensaver		InstallUtil							
		Security Support Provider		Masquerading							
		Server Software Component		Modify Registry							
		Service Registry Permissions		Mshta							
				Network Share Connection Removal							

legend

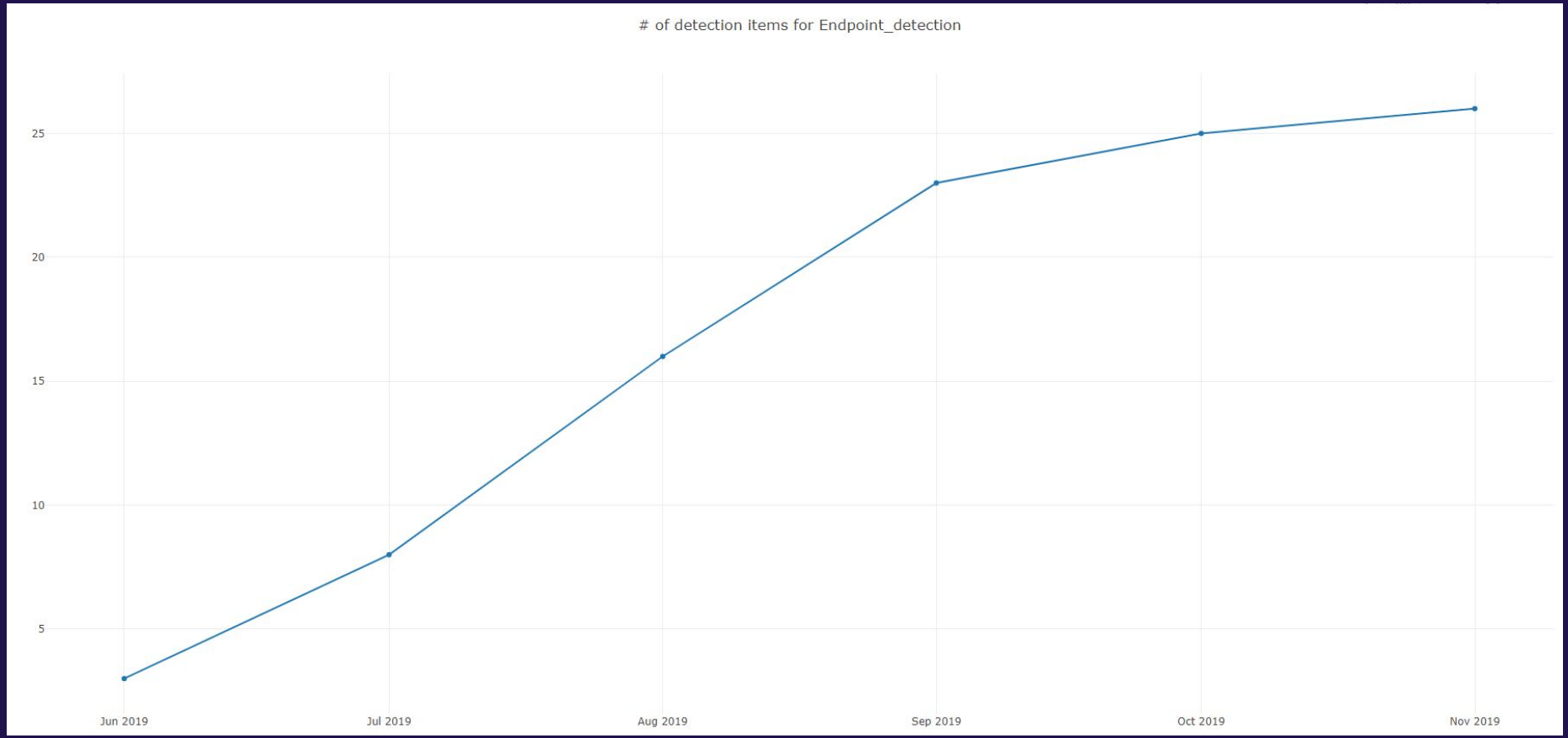
#64B5F6	Detection score 0: Forensics
#DCEDC8	Detection score 1: Basic
#AED581	Detection score 2: Fair
#8BC34A	Detection score 3: Good
#689F38	Detection score 4: Very good
#33691E	Detection score 5: Excellent


Discovery
23 items
Account Discovery
Application Window Discovery
Browser Bookmark Discovery
Domain Trust Discovery
File and Directory Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Security Software Discovery
Software Discovery
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion
T1082
Score: 3
Metadata:
-Applicable to: all
-Detection score: 3
-Detection location: Third party product A
-Technique comment: -
-Detection comment:
Lateral Movement
16 items
Application Deployment Software
Component Object Model and Distributed COM
Exploitation of Remote Services
Internal Spearphishing
Logon Scripts
Pass the Hash
Pass the Ticket
Remote Desktop Protocol
Remote File Copy
Remote Services
Replication Through Removable Media
Shared Webroot
Taint Shared Content
Third-party Software
Windows Admin Shares
Windows Remote Management

Detection + Logging



Improvement Graph



Attacker APT Heat Map

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	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	AppInit DLLs	Application Shimming	Bypass User Account Control	Credential Dumping	Cloud Service Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Command History	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
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 Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Code Signing	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
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	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Email Collection	Fallback Channels	Transfer Data to Cloud Account	Network Denial of Service
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-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Man in the Browser	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Connection Proxy	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Screen Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Video Capture	Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Search Order Hijacking	Password Filter DLL	Software Discovery	Web Session Cookie		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness	Path Interception	DLL Side-Loading	Private Keys	System Information Discovery	Windows Admin Shares		Standard Cryptographic Protocol		
	Rundll32	Hidden Files and Directories	Plist Modification	Execution Guardrails	Securityd Memory	System Network Configuration Discovery	Windows Remote Management		Standard Non-Application Layer Protocol		
	Scheduled Task	Hooking	Port Monitors	Exploitation for Defense Evasion	Steal Application Access Token	System Network Connections Discovery			Uncommonly Used Port		
	Scripting	Hypervisor	PowerShell Profile	Extra Window Memory Injection	Steal Web Session Cookie	System Owner/User Discovery			Web Service		
	Service Execution	Image File Execution Options Injection	Process Injection	File and Directory Permissions Modification	Two-Factor Authentication Interception	System Service Discovery					
	Signed Binary Proxy Execution	Implant Container Image	Scheduled Task	File Deletion		System Time Discovery					
	Signed Script Proxy Execution	Kernel Modules and Extensions	Service Registry Permissions Weakness	File System Logical Offsets		Virtualization/Sandbox Evasion					
	Source	Launch Agent	Setuid and Setgid	Gatekeeper Bypass							
	Space after Filename	Launch Daemon	SID-History Injection	Group Policy Modification							
	Third-party Software	Launchctl	Startup Items	Hidden Files and Directories							
	Trap	LC_LOAD_DYLIB Addition	Sudo	Hidden Users							
	Trusted Developer Utilities	Local Job Scheduling	Sudo Caching	Hidden Window							
	User Execution	Login Item	Valid Accounts	HISTCONTROL							
	Windows Management Instrumentation	Logon Scripts	Web Shell	Image File Execution Options Injection							
	Windows Remote Management	LSASS Driver		Indicator Blocking							
	XSL Script Processing	Modify Existing Service		Indicator Removal from Tools							
		Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchctl							
		Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							

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 .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	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	AppInit DLLs	Application Shimming	Bypass User Account Control	Credential Dumping	Cloud Service Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Command History	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
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 Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Code Signing	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
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	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Email Collection	Fallback Channels	Transfer Data to Cloud Account	Network Denial of Service
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-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Man in the Browser	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Connection Proxy	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Screen Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Video Capture	Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Search Order Hijacking	Password Filter DLL	Software Discovery	Web Session Cookie		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness	Path Interception	DLL Side-Loading	Private Keys	System Information Discovery	Windows Admin Shares		Standard Cryptographic Protocol		
	Rundll32	Hidden Files and Directories	Plist Modification	Execution Guardrails	Securityd Memory	System Network Configuration Discovery	Windows Remote Management		Standard Non-Application Layer Protocol		
	Scheduled Task	Hooking	Port Monitors	Exploitation for Defense Evasion	Steal Application Access Token	System Network Connections Discovery			Uncommonly Used Port		
	Scripting	Hypervisor	PowerShell Profile	Extra Window Memory Injection	Steal Web Session Cookie	System Owner/User Discovery			Web Service		
	Service Execution	Image File Execution Options Injection	Process Injection	File and Directory Permissions Modification	Two-Factor Authentication Interception	System Service Discovery					
	Signed Binary Proxy Execution	Implant Container Image	Scheduled Task	File Deletion		System Time Discovery					
	Signed Script Proxy Execution	Kernel Modules and Extensions	Service Registry Permissions Weakness	File System Logical Offsets		Virtualization/Sandbox Evasion					
	Source	Launch Agent	Setuid and Setgid	Gatekeeper Bypass							
	Space after Filename	Launch Daemon	SID-History Injection	Group Policy Modification							
	Third-party Software	Launchctl	Startup Items	Hidden Files and Directories							
	Trap	LC_LOAD_DYLIB Addition	Sudo	Hidden Users							
	Trusted Developer Utilities	Local Job Scheduling	Sudo Caching	Hidden Window							
	User Execution	Login Item	Valid Accounts	HISTCONTROL							
	Windows Management Instrumentation	Logon Scripts	Web Shell	Image File Execution Options Injection							
	Windows Remote Management	LSASS Driver		Indicator Blocking							
	XSL Script Processing	Modify Existing Service		Indicator Removal from Tools							
		Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchctl							
		Port Knocking		LC_MAIN Hijacking							
				Masquerading							

Atomic Red Team

- Developed by Red Canary
- Descriptions on how to run the attack yourself

- Includes Automation
- Organized by ATT&CK ID

AtomicRedTeam.io

Python, Ruby and Powershell Automation

```yaml
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 "*.txt"} | 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: qcxjb7)
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
```

Thanks

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

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

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

https://atomicredteam.io/