

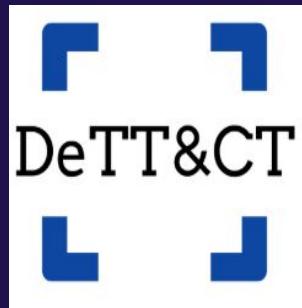
Mapping and Testing your Network to ATT&CK with Free Tools

By Wade Wells
@WadingThruLogs

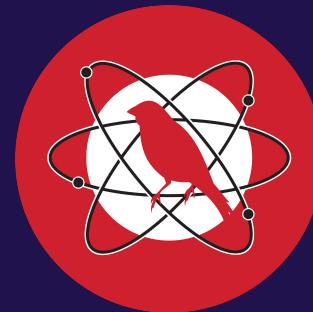
Quick Summary



ATT&Ck Navigator



DeTT&CT

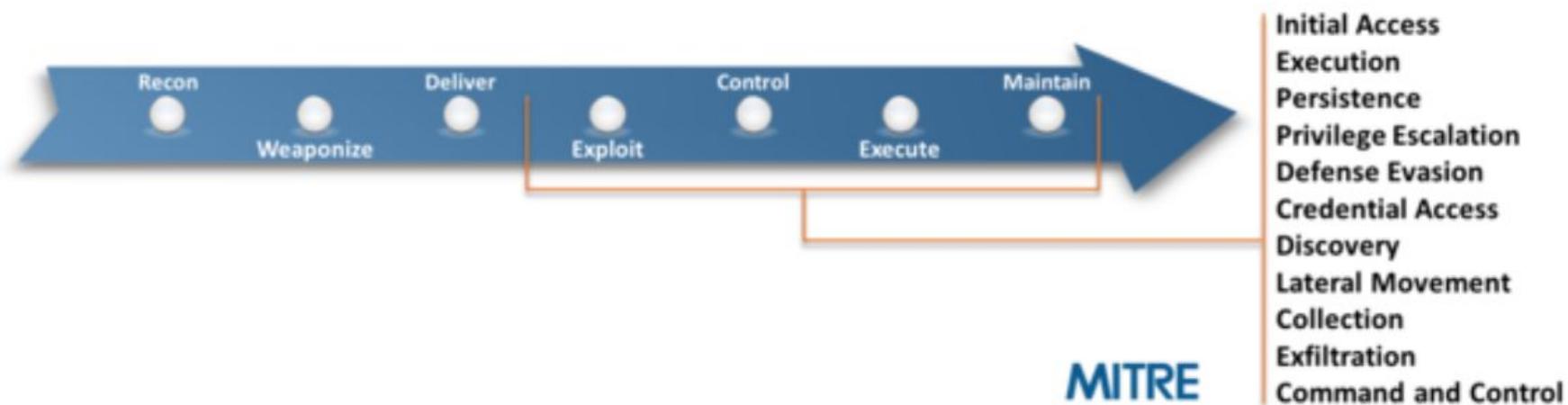


Atomic Read Team

- 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

Mitre ATT&CK Navigator

- Easily configurable
- Angular and Node.js version 8 or greater
- Run as Iframe
- Consumes . json files
- A lot of free resources

github.com/mitre-attack/attack-navigator

MITRE



Evals & Groups

MITRE | ATT&CK® Evaluations

[See Results »](#) [Read Methodology »](#) [Get Evaluated »](#)

Current Evaluations

Initial Cohort



Carbon Black.



CROWDSTRIKE



ENDGAME.



GOSECURE



Windows Defender ATP

MITRE | ATT&CK®

Matrices Tactics Techniques Mitigations Groups Software Resources Blog Contribute Search Q

JUST RELEASED: ATT&CK for Industrial Control Systems

GROUPS

[Overview](#)

admin@338
APT1
APT12
APT16
APT17
APT18
APT19
APT28
APT29
APT3
APT30

Home > Groups

Groups

Groups are sets of related intrusion activity that are tracked by a common name in the security community. Analysts track clusters of activities using various analytic methodologies and terms such as threat groups, activity groups, threat actors, intrusion sets, and campaigns. Some groups have multiple names associated with similar activities due to various organizations tracking similar activities by different names. Organizations' group definitions may partially overlap with groups designated by other organizations and may disagree on specific activity.

For the purposes of the Group pages, the MITRE ATT&CK team uses the term Group to refer to any of the above designations for a cluster of adversary activity. The team makes a best effort to track overlaps between names based on publicly reported associations, which are designated as "Associated Groups" on each page (formerly labeled "Aliases"), because we believe these overlaps are useful for analyst awareness. We do not represent these names as exact overlaps and encourage analysts to do additional research.

Groups are mapped to publicly reported technique use and original references are included. The information provided does not represent all possible technique use by Groups, but rather a subset that is available solely through open source reporting. Groups are also mapped to reported Software used, and technique use for that Software is tracked separately on each Software page.

Groups: 94

Name	Associated Groups	Description
admin@338		admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as Poison Ivy, as well as some non-public backdoors.

Iranian 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 Discovery	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	Exploitation of Remote Services	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Hardware Additions	Component Object Model and Distributed COM	ApplnIt DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	Network Service Scanning	File from Local System	Exploitation Over Alternative Protocol	Custom Cryptographic Protocol	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 Share Discovery	Internal Spearphishing	Data from Network Shared Drive	Data Encoding	Data Obfuscation	Endpoint Denial of Service
Spearphishing Attachment	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Compile After Delivery	Credentials in Registry	Network Sniffing	Logon Scripts	Data from Removable Media	Data from Removable Media	Domain Fronting	Firmware Corruption
Spearphishing Link	Execution through API	BITS Jobs	Compiled HTML File	Compiled HTML File	Exploitation for Credential Access	Password Policy Discovery	Pass the Hash	Exfiltration Over Other Network Medium	Exfiltration Over Physical Medium	Domain Generation Algorithms	Inhibit System Recovery
Spearphishing via Service	Execution through Module Load	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Pass the Ticket	Data Staged	Fallback Channels	Fallback Channels	Network Denial of Service
Supply Chain Compromise	Exploitation for Client Execution	Browser Extensions	Elevated Execution with Prompt	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote Desktop Protocol	Email Collection	Multi-hop Proxy	Multi-hop Proxy	Resource Hijacking
Trusted Relationship	Change Default File Association	Emond	Connection Proxy	Component Firmware	Input Capture	Process Discovery	Remote File Copy	Input Capture	Man in the Browser	Man in the Browser	Runtime Data Manipulation
Valid Accounts	Graphical User Interface	Control Panel Items	Control Panel Items	Control Panel Items	Input Prompt	Query Registry	Remote Services	Input Capture	Multi-Stage Channels	Multi-Stage Channels	Service Stop
	InstallUtil	DCShadow	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Replication Through Removable Media	Input Capture	Multiband Communication	Multiband Communication	Stored Data Manipulation
	Launchctl	Keychain	Extra Window Memory Injection	Disabling Security Tools	Keychain	Security Software Discovery	Screen Capture	Input Capture	Multilayer Encryption	Multilayer Encryption	System Shutdown/Reboot
	Local Job Scheduling	LLMNR/NBT-NS Poisoning and Relay	File System Permissions Weakness	LLMNR/NBT-NS Poisoning and Relay	Software Discovery	Shared Webroot	Video Capture	Input Capture	Port Knocking	Port Knocking	Transmitted Data Manipulation
	LSASS Driver	MSasn1	DLL Search Order Hijacking	DLL Side-Loading	System Information Discovery	SSH Hijacking	Taint Shared Content	Input Capture	Remote Access Tools	Remote Access Tools	Transmitted Data Manipulation
	Mshta	MSasn1	Dylib Hijacking	Hooking	Network Sniffing	System Network Configuration Discovery	Third-party	Input Capture	Remote File Copy	Remote File Copy	Transmitted Data Manipulation
	PowerShell	MSasn1	Emond	Image File	Execution Guardrails	System Network Configuration Discovery					

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	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Runtime Data Manipulation	Service Stop
Trusted Relationship	Exploitation for Client Execution	Emond	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Fallback Channels	Input Capture	Failback Channels	Stored Data Manipulation	System Shutdown/Reboot
Valid Accounts	Graphical User Interface	Component Firmware	Exploitation for Privilege Escalation	Connection Proxy	Process Discovery	Remote Services	Man in the Browser	Input Capture	Multi-hop Proxy	Transmitted Data Manipulation	
	InstallUtil	Component Object Model Hijacking	Extra Window Memory Injection	Control Panel Items	Query Registry	Remote System Discovery	Replication Through Removable Media	Input Capture	Multi-Stage Channels		
	LaunchCtl	Create Account	File System Permissions Weakness	DCShadow	Kerberoasting	Security Software Discovery	Shared Webroot	Input Capture	Video Capture	Multiband Communication	
	Local Job Scheduling	DLL Search Order Hijacking	Deobfuscate/Decode Files or Information	Keychain	Software Discovery	SSH Hijacking	SSH Hijacking	Input Capture	Multi-layer Encryption		
	LSASS Driver	Dylib Hijacking	Image File Execution Options Injection	LMNR/NBT-NS Poisoning and Relay	System Information Discovery	Taint Shared Content	Taint Shared Content	Input Capture	Port Knocking		
	Mshta	Emond	Launch Daemon	Disabling Security Tools	System Network Configuration Discovery	Third-party Software	Third-party Software	Input Capture	Remote Access Tools		
	PowerShell	External Remote Services	DLL Side-Loading	DLL Search Order Hijacking	Network Sniffing	Windows Admin Shares	Windows Admin Shares	Input Capture	Remote File Copy		
	Regsvcs/Regasm	File System Permissions Weakness	New Service	Execution Guardrails	Password Filter DLL	System Network Connections Discovery	System Network Connections Discovery	Input Capture	Standard Application Layer Protocol		
	Regsvr32	Hidden Files and Directories	Parent PID Spoofing	Exploitation for Defense Evasion	Private Keys	System Owner/User Discovery	System Owner/User Discovery	Input Capture	Standard Cryptographic Protocol		
	Rundll32	Hooking	Path Interception	Extra Window Memory Injection	Steal Web Session Cookie	System Service Discovery	System Service Discovery	Input Capture	Standard Non-Application Layer Protocol		
	Scheduled Task	Launch Daemon	Plist Modification	File and Directory Permissions Modification	Two-Factor Authentication Interception	System Time Discovery	System Time Discovery	Input Capture	Uncommonly Used Port		
	Scripting	Hypervisor	Port Monitors	File Deletion		Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Input Capture	Web Service		
	Service Execution	Image File Execution Options Injection	PowerShell Profile	File System Logical Offsets							
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Process Injection	Gatekeeper Bypass							
	Signed Script Proxy Execution	Launch Agent	Scheduled Task	Group Policy Modification							
	Source	Service Registry Permissions Weakness	Hidden Files and Directories	Hidden Users							
	Space after Filename	Launch Daemon	Setuid and Setgid	Hidden Window	HISTCONTROL						
	Third-party Software	LaunchCtl	SID-History Injection								
	Trap	LC_LOAD_DYLIB Addition									
	Trusted Developer Utilities	Local Job Scheduling	Startup Items								
	User Execution	Login Item	Sudo	Image File Execution Options Injection							
	Windows Management Instrumentation	Logon Scripts	Sudo Caching	Indicator Blocking							
	Windows Remote	LSASS Driver	Valid Accounts	Indicator Removal from Tools							

▼ legend

- #74c476 BOTM
- #fce93b APT29
- #6baed6 APT3

[Add Item](#) [Clear](#)



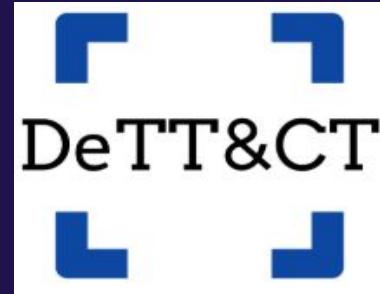
Detect Tactics, Techniques & Combat Threats

- Map your Mitre logging/detection coverage.
- Compares visibility, detections and threats.
- Uses ATT&CK Navigator.
- Runs Via Python 3.

```
-- 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
>>
```

How I use



Filling out Data source file

- What are you logging
- How good is that logging

Filling out Administration Techniques File

- What alerts you have written that cover that attack

Data Source Scoring

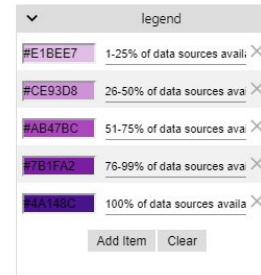
Visibility scores

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
```

Logging Visibility

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	Application Shimming	Application Shimming	CMSTP	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	Authentication Package	Bypass User Account Control	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	Compile After Delivery	Exploitation for Credential Access	Network Share Discovery	Logon Scripts	Data from Network Shared Drive	Data Encoding	Firmware Corruption
Spearphishing via Service	Execution through Module Load	Browser Extensions	Exploitation for Privilege Escalation	Component Firmware	Forced Authentication	Network Sniffing	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Inhibit System Recovery
Supply Chain Compromise	Execution for Client Association	Change Default File Association	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Pass the Ticket	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Network Denial of Service
Trusted Relationship	Graphical User Interface	Component Firmware	File System Permissions	Connection Proxy	Permission Groups Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Resource Hijacking	
Valid Accounts	InstallUtil	Component Object Model Hijacking	Control Panel Items Weakness	DCShadow	Input Capture	Process Discovery	Remote Services	Input Capture	Fallback Channels	Runtime Data Manipulation	
	LSASS Driver	Create Account	Hooking	Deobfuscate/Decode Files or Information	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy	Service Stop	
	Mshta	DLL Search Order Hijacking	Image File Execution Options Injection	Disabling Security Tools	Kerberoasting	Remote System Discovery	Screen Capture	Multi-hop Proxy	Multi-Stage Channels	Stored Data Manipulation	
	PowerShell	External Remote Services	New Service	LMNR/NBT-NS Poisoning and Relay	Network Sniffing	Security Software Discovery	Shared Webroot	Taint Shared Content	Multi-band Communication	System Shutdown/Reboot	
	Regsvcs/Regasm	File System Permissions	Parent PID Spoofing	DLL Search Order Hijacking	Password Filter DLL	Software Discovery	Video Capture	Third-party Software	Multi-layer Encryption	Transmitted Data Manipulation	
	Regsvr32	Weakness	Path Interception	DLL Side-Loading	System Information Discovery	Windows Admin Shares	Windows Remote Management	Windows Admin Shares	Remote Access Tools		
	Rundl32	Hidden Files and Directories	Port Monitors	Execution Guardrails	Private Keys	System Network Configuration Discovery	Windows Remote Management	Windows Remote Management	Remote File Copy		
	Scheduled Task	Hooking	PowerShell Profile	Exploitation for Defense Evasion	Steal Web Session Cookie	System Network Connections Discovery		Standard Application Layer Protocol			
	Scripting	Hypervisor	Process Injection	Extra Window Memory Injection	Two-Factor Authentication Interception	System Owner/User Discovery		Standard Cryptographic Protocol			
	Service Execution	Image File Execution Options Injection	Scheduled Task	File and Directory Permissions Modification		System Service Discovery		Standard Non-Application Layer Protocol			
	Signed Binary Proxy Execution	Service Registry Permissions	Logon Scripts	File Deletion		System Time Discovery		Standard Non-Application Layer Protocol			
	Signed Script Proxy Execution	Weakness	LSASS Driver	File System Logical Offsets		Virtualization/Sandbox Evasion		Uncommonly Used Port			
	Third-party Software	SID-History Injection	Modify Existing Service	Group Policy Modification				Web Service			
	Trusted Developer Utilities	Netsh Helper DLL	Valid Accounts	Hidden Files and Directories							
	User Execution	New Service	Web Shell	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							
				Indicator Removal on Host							
				Indirect Command Execution							
				Install Root Certificate							



Credential Access	Discovery
16 items	22 items
Account Manipulation	Account Discovery
Brute Force	Application Window Discovery
Credential Dumping	Browser Bookmark Discovery
Credentials in T1003 File Metadata:	Domain Trust Discovery
Credentials in Registry	- Available data sources: Process monitoring, PowerShell logs, Work Service Scanning
Exploitation for Credential Access	- ATT&CK data sources: API monitoring, Process Share Discovery
Forced Authentication	monitoring, PowerShell logs, Process command-line
Hooking	parameters
Input Capture	- Products: Windows event log
Input Prompt	Discovery
Kerberoasting	Peripheral Device Discovery
LLMNR/NBT-NS Poisoning and Relay	Permission Groups Discovery
Network Sniffing	Process Discovery
Password Filter DLL	Query Registry
Private Keys	Remote System Discovery
Two-Factor Authentication Interception	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

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	Bootkit	Execution through API	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 through Module Load	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Remote File Copy	Email Collection	Domain Fronting	Domain Generation Algorithms	Fallback Channels	Resource Hijacking
Trusted Relationship	Exploitation for Client Execution	Change Default File Association	Extra Window Memory Injection	Connection Proxy	Input Capture	Permission Groups Discovery	Input Capture	Input Capture	Input Capture	Multi-hop Proxy	Runtime Data Manipulation
Valid Accounts	Graphical User Interface	Component Firmware	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser	Man in the Browser	Screen Capture	Service Stop
InstallUtil	Component Object Model Hijacking	Hooking	Hooking	DCShadow	Kerberoasting	Query Registry	Shared Webroot	Screen Capture	Screen Capture	Video Capture	Stored Data Manipulation
LSASS Driver	Create Account	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content	Video Capture	Video Capture	Multi-Stage Channels	System Shutdown/Reboot
Mshta	PowerShell	External Remote Services	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software	Windows Admin Shares	Windows Admin Shares	Multiband Communication	Transmitted Data Manipulation
Regsvcs/Regasm	File System Permissions Weakness	Parent PID Spoofing	DLL Search Order Hijacking	DLL Side-Loading	Password Filter DLL	System Information Discovery	Windows Remote Management	Windows Remote Management	Windows Remote Management	Multilayer Encryption	Remote Access Tools
Regsvr32	Hidden Files and Directories	Path Interception	DLL Side-Loading	Private Keys	Steal Web Session Cookie	System Network Configuration Discovery	System Network Connections Discovery	System Owner/User Discovery	System Owner/User Discovery	Standard Application Layer Protocol	Remote File Copy
Rundl32	Scheduled Task	Port Monitors	Execution Guardrails	Two-Factor Authentication Interception	System Network Connections Discovery	System Service Discovery	System Time Discovery	System Time Discovery	System Time Discovery	Standard Cryptographic Protocol	Standard Non-Application Layer Protocol
Scheduled Task	Hooking	PowerShell Profile	Exploitation for Defense Evasion	System Network Configuration Discovery	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion	Uncommonly Used Port	Uncommonly Used Port	Web Service	Uncommonly Used Port
Scripting	Hypervisor	Process Injection	Extra Window Memory Injection								
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								

Legend:

- #64B5F6 Detection score 0: Forensic
- #DCECDC8 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	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	
Network Share Discovery	Pass the Hash
Network Sniffing	Pass the Ticket
>Password Policy Discovery	Remote Desktop Protocol
Peripheral Device Discovery	Remote File Copy
Permission Groups Discovery	Remote Services
Process Discovery	Replication Through Removable Media
Query Registry	Shared Webroot
Remote System Discovery	Taint Shared Content
Security Software Discovery	Third-party Software
Software Discovery	
System Information Discovery	Windows Admin Shares
System Network Configuration Metadata	Windows Remote Management
-Applicable to: all	
System Network Co-Detection score: 3	
Discovery	-Detection location: Third party product A
System Owner/User	-Technique comment: -
System Service Discovery	-Detection comment:
System Time Discovery	
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	Data from 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	Domain Fronting	Email Collection	Network Denial of Service
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	Domain Generation Algorithms	Input Capture	Resource Hijacking
Supply Chain Compromise	Exploitation for Client execution	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Process Discovery	Remote File Copy	Fallback Channels	Man in the Browser	Runtime Data Manipulation
Trusted Relationship	Graphical User Interface	Change Default File Association	Extra Window Memory Injection	Connection Proxy	Input Capture	Permission Groups Discovery	Query Registry	Replication Through Removable Media	Multi-hop Proxy	Screen Capture	Service Stop
Valid Accounts	Component Firmware	File System Permissions Weakness	File System Permissions Weakness	File System Permissions Weakness	Input Prompt	Process Discovery	Remote System Discovery	Shared Webroot	Multi-Stage Channels	Video Capture	Stored Data Manipulation
	Component Object Model Hijacking	Control Panel Items	Hooking	DCShadow	Kerberoasting	Query Registry	Security Software Discovery	Taint Shared Content	Multiband Communication	Third-party Software	System Shutdown/Reboot
	Create Account	Image File Execution Options Injection	Image File Execution Options Injection	LLMNR/NBT-NS Poisoning and Relay	Network Sniffing	Remote System Discovery	Software Discovery	Windows Admin Shares	Multilayer Encryption	Windows Remote Management	Transmitted Data Manipulation
	DLL Search Order Hijacking	New Service	Disabling Security Tools	DLL Search Order Hijacking	>Password Filter DLL	Shared Webroot	System Information Discovery	Windows Remote Management	Remote Access Tools		
	PowerShell	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys	System Network Configuration Discovery	System Network Connections Discovery		Remote File Copy		
	Regsvcs/Regasm	File System Permissions Weakness	Path Interception	Execution Guardrails	Steal Web Session Cookie	System Network Configuration Discovery	System Owner/User Discovery		Standard Application Layer Protocol		
	Regsvr32	Hidden Files and Directories	PowerShell Profile	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Network Connections Discovery	System Service Discovery		Standard Cryptographic Protocol		
	Rundll32	Scheduled Task	Process Injection	Extra Window Memory Injection		System Network Connections Discovery	System Time Discovery		Standard Non-Application Layer Protocol		
	Scheduled Task	Hooking	Scheduled Task	Scheduled Task		System Network Connections Discovery	Virtualization/Sandbox Evasion		Uncommonly Used Port		
	Scripting	Hypervisor	Image File Execution Options Injection	File and Directory Permissions Modification		System Network Connections Discovery			Web Service		
	Service Execution	New Service	Signed Binary Proxy Execution	Service Registry Permissions Weakness	File Deletion	System Network Connections Discovery					
	Signed Binary Proxy Execution	Office Application Startup	Signed Script Proxy Execution	SID-History Injection	File System Logical Offsets	System Network Connections Discovery					
	Signed Script Proxy Execution	Path Interception	LSASS Driver	Valid Accounts	Group Policy Modification	System Network Connections Discovery					
	Third-party Software	Port Monitors	Modify Existing Service	Web Shell	Hidden Files and Directories	System Network Connections Discovery					
	Trusted Developer Utilities	Netsh Helper DLL	User Execution		Hidden Window	System Network Connections Discovery					
	Windows Management Instrumentation	New Service	Windows Management Instrumentation		Image File Execution Options Injection	System Network Connections Discovery					
	Windows Remote Management	Office Application Startup	Windows Remote Management		Indicator Blocking	System Network Connections Discovery					
	XSL Script Processing	Path Interception	Port Monitors		Indicator Removal from Tools	System Network Connections Discovery					
		Port Monitors	PowerShell Profile		Indicator Removal on Host	System Network Connections Discovery					
		PowerShell Profile	Redundant Access		Indirect Command Execution	System Network Connections Discovery					
		Redundant Access	Registry Run Keys / Startup								

selection controls layer controls technique controls

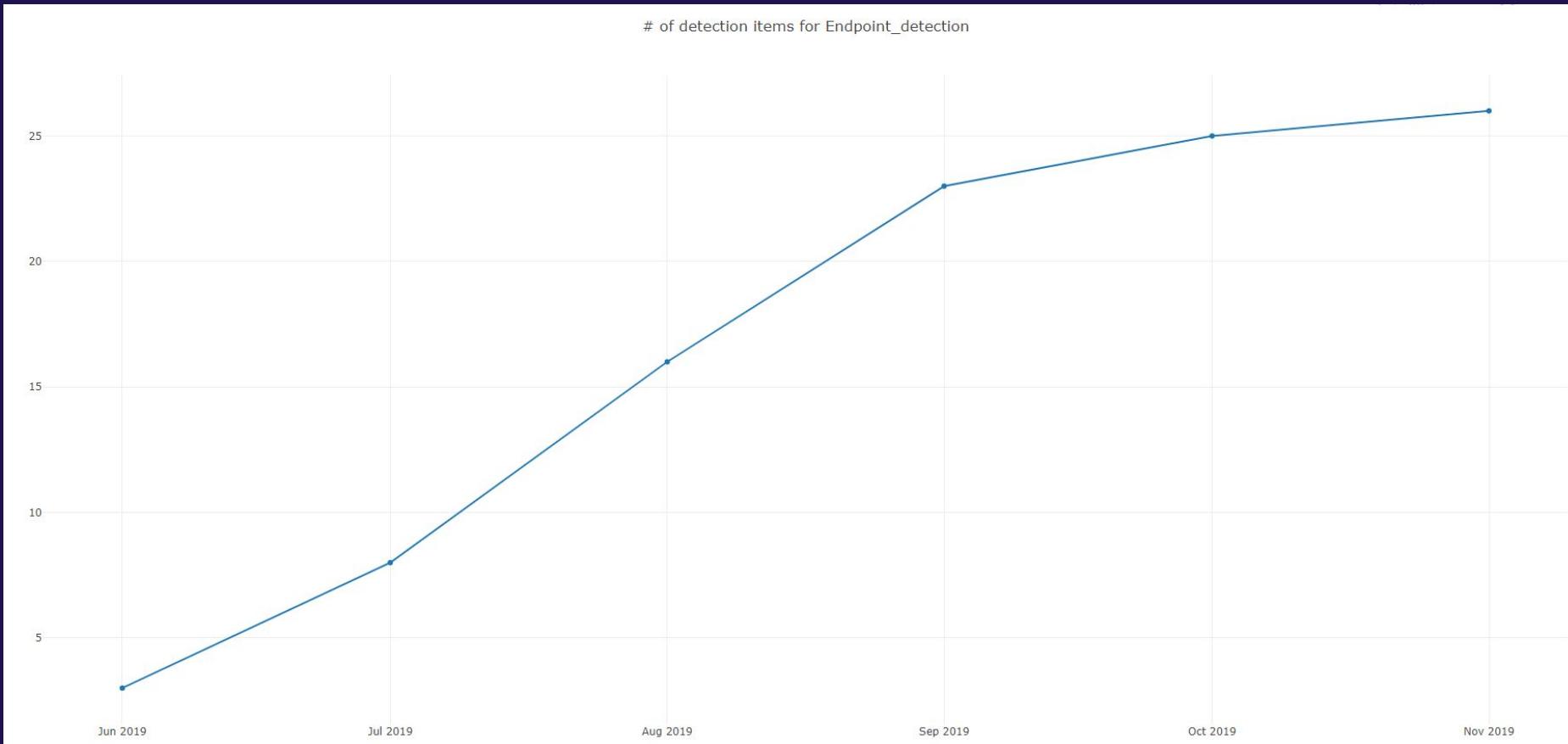
#1976D2 Visibility

#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 Magic Hound, OilRig Software	Audio Capture	Automated Exfiltration	Data Transfer Size Limits
External Remote Services	Rundll32	Account Manipulation	Deobfuscate/Decode Files or Information	Credentials from Web Browsers	System Information Discovery	Clipboard Data	Standard Cryptographic Protocol	Connection Proxy	Exfiltration Over Command and Control Channel	
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 Other Network Medium
Hardware Additions	CMSTP	External Remote Services	Accessibility Features	Redundant Access	Credentials in Registry	Network Sniffing	Internal Spearphishing	Data from Local System	Fallback Channels	Scheduled Transfer
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	Multi-Stage Channels	
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	Web Service	Exfiltration Over Physical Medium
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	Man in the Browser	Communication Through Removable Media
	Exploitation for Client Execution	AppInit DLLs	Extra Window Memory Injection	CMSTP	Hooking	Remote System Discovery	Data Staged	Shared Webroot	Video Capture	Custom Cryptographic Protocol
	Mshta	Application Shimming	Code Signing	Input Prompt	Kerberoasting	Security Software Discovery	Taint Shared Content	Third-party Software	Custom Obfuscation	Data Obfuscation
	Authentication Package	File System Permissions Weakness	Compile After Delivery	LLMNR/NBT-NS Poisoning and Relay	System Network Connections Discovery	System Service Discovery	Windows Admin Shares	Domain Fronting	Domain Generation Algorithms	Domain Generation Algorithms
	Control Panel Items	BITS Jobs	Compiled HTML File	Application Window Discovery	Shared Webroot	Windows Remote Management	Windows Remote Management	Multi-hop Proxy	Multiband Communication	Multiband Communication
	Execution through API	Bootkit	Hooking	Execution Guardrails	password Filter DLL	Browser Bookmark Discovery	Man in the Browser	Man in the Browser	Multi-hop Proxy	Multiband Communication
	Execution through Module Load	Browser Extensions	Image File Execution Options Injection	Indicator Removal from Tools	Private Keys	Domain Trust Discovery	Video Capture	Video Capture	Video Capture	Video Capture
	Graphical User Interface	Change Default File Association	New Service	Masquerading	Steal Web Session Cookie	Network Share Discovery	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol
	InstallUtil	Parent PID Spoofing	Mshta	Two-Factor Authentication Interception	Domain Trust Discovery	Peripheral Device Discovery	Domain Generation Algorithms	Domain Generation Algorithms	Domain Generation Algorithms	Domain Generation Algorithms
	LSASS Driver	Component Object Model	Path Interception	Web Service	Network Share Discovery	Peripherals	Multi-hop Proxy	Multi-hop Proxy	Multi-hop Proxy	Multi-hop Proxy

Attacker + Detections

Comprehensive Threat Landscape Analysis: Q3 2024											
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	T1192 Score: 4 Metadata: Applied to: all Detection score: 3	PowerShell	Scheduled Task	Scheduled Task	Modify Registry	Password Filter DLL	Account Discovery	Windows Remote Management	Screen Capture	Connection Proxy	Exfiltration Over Alternative Protocol
Valid Account	Scheduled Task	BITS Jobs	Image File Execution Options Injection	Signed Binary Proxy Execution	Signed Binary Proxy Execution	Credential Dumping	System Owner/User Discovery	Component Object Model and Distributed COM	Audio Capture	Multi-Stage Channels	Data Compressed
Spearphishing	Applied to: all Detection score: 3	Signed Binary Proxy Execution	Image File Execution Options Injection	Valid Accounts	BITS Jobs	Credentials from Web Browsers	File and Directory Discovery	Automated Collection	Remote File Copy	Automated Exfiltration	Data Encrypted
Drive-by Compromises	Visibility score: 2 - Overlay: Detection	Compiled HTML File	LSASS Driver	Web Shell	Compiled HTML File	Credentials in Files	Process Discovery	Remote File Copy	Clipboard Data	Commonly Used Port	Data Transfer Size Limits
Exploit Public-Facing Application	Dynamic Data Exchange	Office Application Startup	Bypass User Account Control	Deobfuscate/Decode Files or Information	Access Token Manipulation	Account Manipulation	Security Software Discovery	Application Deployment Software	Data from Information Repositories	Communication Through Removable Media	Exfiltration Over Command and Control Channel
External Remote Services	LSASS Driver	Registry Run Keys / Startup Folder	Disabling Security Tools	DLL Side-Loading	Brute Force	System Information Discovery	Exploitation of Remote Services	Data from Local System	Custom Command and Control Protocol	Custom Cryptographic Protocol	Exfiltration Over Other Network Medium
Hardware Additions	Windows Management Instrumentation	Valid Accounts	Accessibility Features	Credentials in Registry	Exploitation for Credential Access	System Network Configuration Discovery	Internal Spearphishing	Data from Network Shared Drive	Data from Removable Media	Data Encoding	Exfiltration Over Physical Medium
Replication Through Removable Media	CMSTP	Windows Management Instrumentation Event Subscription	AppCert DLLs	Image File Execution Options Injection	Forced Authentication	Application Window Discovery	Logon Scripts	Custom Cryptographic Protocol	Data Staged	Data Obfuscation	Scheduled Transfer
Spearphishing via Service	InstallUtil	Rundll32	AppInit DLLs	Valid Accounts	Hooking	Browser Bookmark Discovery	Pass the Hash	Domain Fronting	Data from Removable Media	Domain Generation Algorithms	Fallback Channels
Supply Chain Compromise	Web Shell	Windows Remote Management	Application Shimming	CMSTP	Input Capture	Domain Trust Discovery	Pass the Ticket	Input Capture	Man in the Browser	Multi-hop Proxy	Multi-band Communication
Trusted Relationship	Accessibility Features	Accessibility Features	DLL Search Order Hijacking	InstallUtil	Input Prompt	Network Service Scanning	Remote Desktop Protocol	Input Capture	Video Capture	Shared Webroot	Multilayer Encryption
	Command-Line Interface	Account Manipulation	Exploitation for Privilege Escalation	Rundll32	Kerberoasting	Network Share Discovery	Remote Services	Input Capture	Peripheral Device Discovery	Shared Webroot	Multi-hop Proxy
	Component Object Model and Distributed COM	AppCert DLLs	Extra Window Memory Injection	Bypass User Account Control	LLMNR/NBT-NS Poisoning and Relay	Network Sniffing	Replication Through Removable Media	Input Capture	Man in the Browser	Shared Webroot	Multi-band Communication
	Mshta	AppInit DLLs	Compile After Delivery	Connection Proxy	Network Sniffing	Password Policy Discovery	Replication Through Removable Media	Input Capture	Fallback Channels	Shared Webroot	Multilayer Encryption
	Scripting	Application Shimming	File System Permissions Weakness	Masquerading	Private Keys	Peripheral Device Discovery	Third-party Software	Input Capture	Video Capture	Shared Webroot	Multi-hop Proxy
	User Execution	Authentication Package	Hooks	Malta	Query Registry	Permission Groups Discovery	Windows Admin Shares	Input Capture	Multi-hop Proxy	Shared Webroot	Multi-band Communication
	Control Panel Items	Bootkit	New Service	Steal Web Session Cookie	Remote System Discovery	Shared Webroot	Standard Application Layer Protocol	Input Capture	Multi-hop Proxy	Shared Webroot	Multilayer Encryption
Execution through API	Browser Extensions	Parent PID Spoofing	Obfuscated Files or Information	Two-Factor Authentication Interception	Software Discovery	Standard Application Layer Protocol	Standard Cryptographic	Input Capture	Multi-hop Proxy	Shared Webroot	Multilayer Encryption
Execution through Module	Change Default File Association	Path Interception	Scripting	System Network Connections	System Network Connections	Standard Cryptographic	Standard Cryptographic	Input Capture	Multi-hop Proxy	Shared Webroot	Multilayer Encryption

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

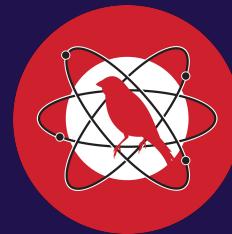
With tools

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 .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	Transfer Data to Cloud Account	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	Service Stop	Runtime Data Manipulation
	InstallUtil	Component Firmware	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Man in the Browser	Multiband Communication	Stored Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Connection Proxy	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Query Registry	Screen Capture	Multi-layer Encryption	System Shutdown/Reboot
	Local Job Scheduling	Create Account	Hooks	Kerberoasting	Process Discovery	Remote System Discovery	SSH Hijacking	Shared Webroot	Video Capture	Port Knocking	Transmitted Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	DCShadow	Keychain	Remote Services	Security Software Discovery	Taint Shared Content	Steal Application Access Token		Remote Access Tools	
	Mshta	DYLB Hijacking	Image File Execution Options Injection	LMNR/NBT-NS Poisoning and Relay	Replication Through Removable Media	Software Discovery	Third-party Software	Steal Web Session Cookie		Remote File Copy	
	PowerShell	Emond	Deobfuscates/Decode Files or Information	Relay	Security Software Discovery	System Information Discovery	Web Session Cookie	System Owner/User Discovery		Standard Application Layer Protocol	
	Regsvr/Regasm	External Remote Services	Disabling Security Tools	Network Sniffing	System Network Configuration Discovery	System Network Connections Discovery	Windows Admin Shares	System Service Discovery		Standard Cryptographic Protocol	
	Regsvr32	File System Permissions Weakness	DLL Search Order Hijacking	Network Sniffing	System Network Connections Discovery	System Time Discovery	Windows Remote Management	System Time Discovery		Standard Non-Application Layer Protocol	
	Rundll32	Hidden Files and Directories	DLL Side-Loading	>Password Filter DLL	System Time Discovery	Virtualization/Sandbox Evasion				Uncommonly Used Port	
	Scheduled Task	Hooking	Execution Guardrails	Private Keys						Web Service	
	Scripting	Hypervisor	Exploitation for Defense Evasion	Security Memory							
	Service Execution	Image File Execution Options Injection	Steal Application Access Token								
	Signed Binary Proxy Execution	Implant Container Image	Steal Web Session Cookie								
	Signed Script Proxy Execution	Kernel Modules and Extensions	System Owner/User Discovery								
	Source	Launch Agent	System Service Discovery								
	Space after Rename	Launch Daemon	System Time Discovery								
	Third-party Software	Launchctl	Virtualization/Sandbox Evasion								
	Trap	LC_LOAD_DYLIB Addition									
	Trusted Developer Utilities	Local Job Scheduling	Sudo								
	User Execution	Login Item	Sudo Caching								
	Windows Management Instrumentation	Logon Scripts	Image File Execution Options Injection								
	Windows Remote Management	LSASS Driver	Valid Accounts	Indicator Blocking							
	XSL Script Processing	Modify Existing Service	Web Shell	Indicator Removal from Tools							
		Netshell 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



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)

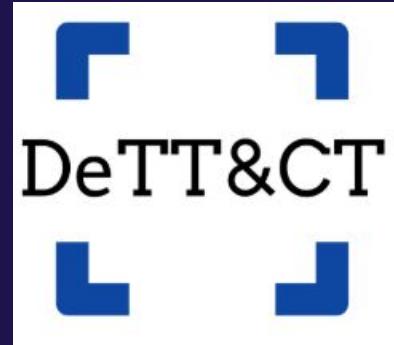
local_path: Local path to place file (default: Atomic-license.txt)

Launcher: command_prompt
```

Thanks

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

<https://atomicredteam.io/>



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

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

