ATT&CK as a Teacher

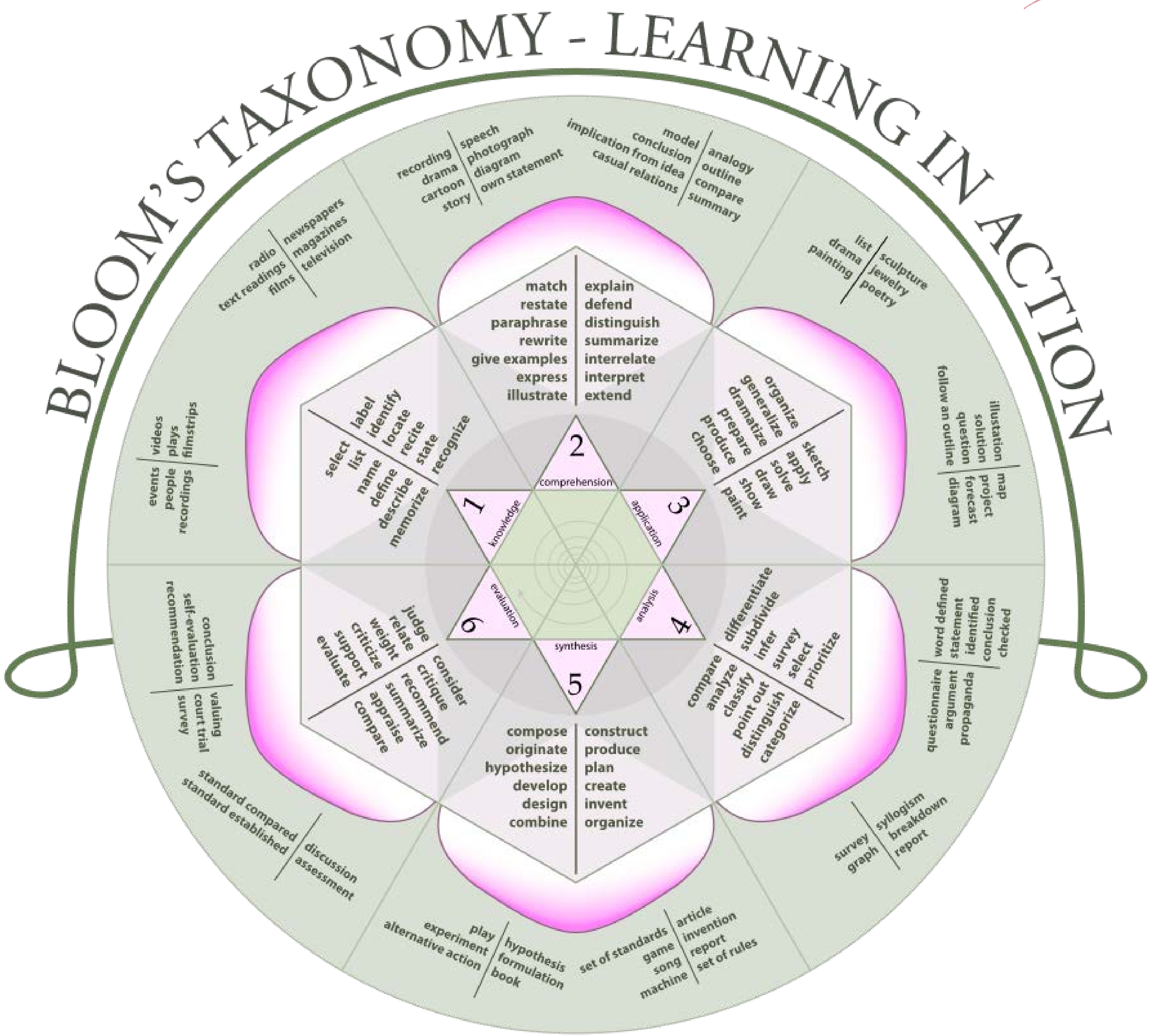
Travis Smith

Principal Security Researcher

Learning Objectives

Bloom's Taxonomy

1. Knowledge
2. Comprehension
3. Application
4. Analysis
5. Synthesis
6. Evaluation



Separating Techniques

Categories

T	Techniques Only	• Not really an exploit • Requires the use of other techniques to be truly viable • Example – Graphical User Interface
E	Exploitable to Anyone	• Easy to exploit (my mom could probably do it) • No need for POC malware, scripts, or other tools • Example – Accessibility Features
A	Additional Steps Required	• Need some sort of tooling such as Metasploit or POC scripts • Could be more advanced than those found in green • Example – Exploitation for *
C	Cost Prohibitive	• Requires additional infrastructure to be able to exploit • Some are quite easy, some can be more advanced. • Example – Web Shell
H	Hard	• Might require custom DLL/EXE • In-Depth Understanding of the OS • Example – Process Injection

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

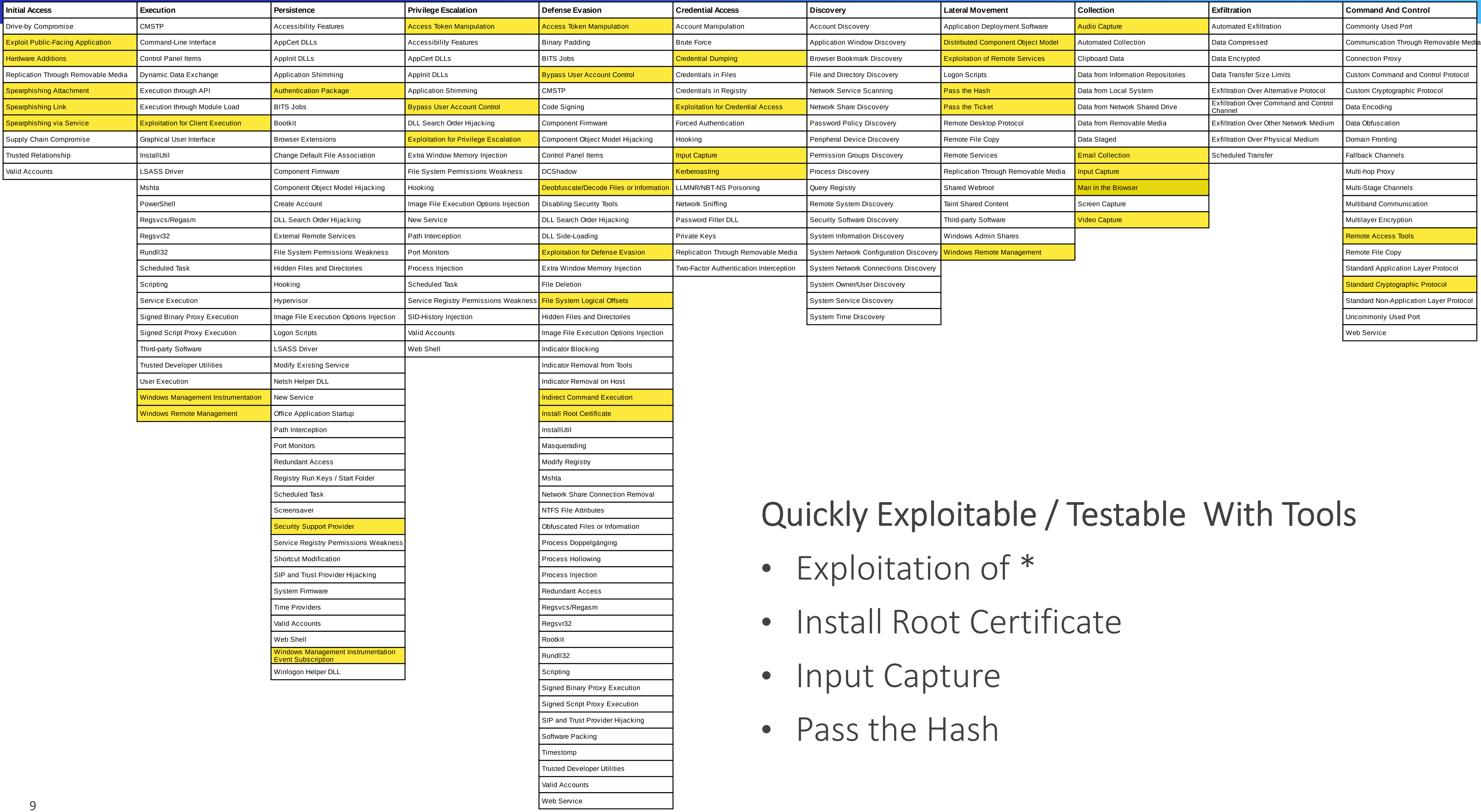
Use these to leverage other techniques

- Graphical User Interface
- User Execution
- Query Registry
- * Discovery

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

Easily Exploitable/Testable

- Accessibility Features
- Registry Run Keys / Start Folder
- Image File Execution Options
- PowerShell / Scripting



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

Quickly Exploitable / Testable With Tools

- Exploitation of *
- Install Root Certificate
- Input Capture
- Pass the Hash

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

Requires Additional Infrastructure / Setup

- Web Shell
- Taint Shared-Content
- Shared Webroot
- Exfiltration / Command and Control

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

Requires Advanced Knowledge or Custom Tools

- Misc DLL’s (PW Filter, AppCert, AppInit, etc.)
- Process Injection
- Bootkit / Rootkit
- System / Component Firmware

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

https://github.com/TravisFSmith/mitre_attack

ATT&CK Navigator

https://raw.githubusercontent.com/TravisFSmith/mitre_attack/master/teaching/All.json

All.json

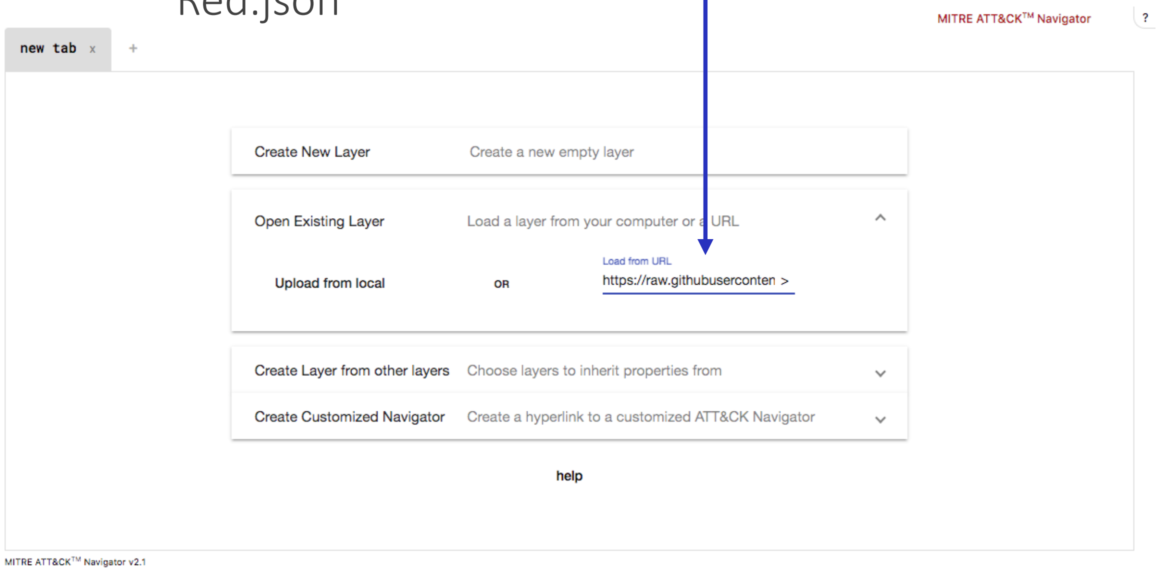
Blue.json

Green.json

Orange.json

Yellow.json

Red.json



MITRE ATT&CK™ Navigator ?

new tab x +

Create New Layer — Create a new empty layer

Open Existing Layer — Load a layer from your computer or a URL

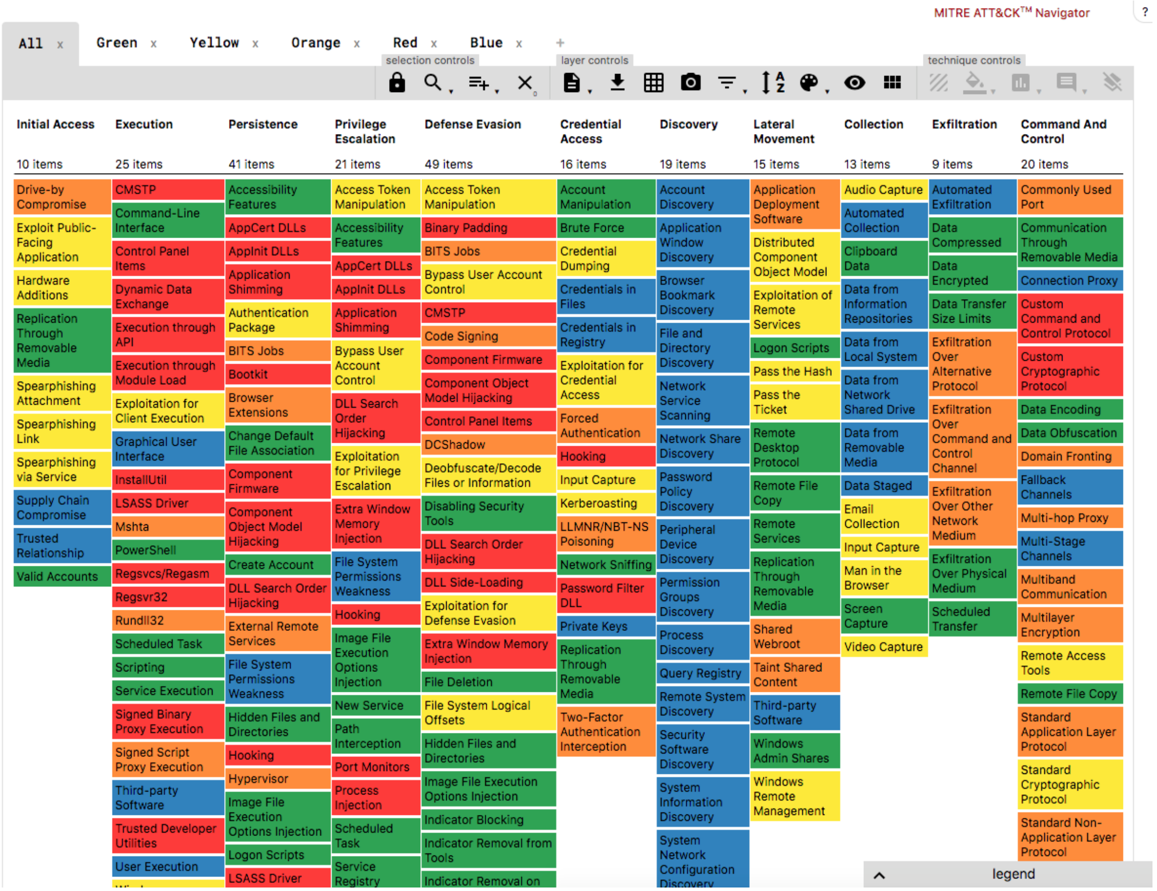
Upload from local OR Load from URL https://raw.githubuserconten >

Create Layer from other layers — Choose layers to inherit properties from

Create Customized Navigator — Create a hyperlink to a customized ATT&CK Navigator

help

MITRE ATT&CK™ Navigator v2.1



MITRE ATT&CK™ Navigator ?

All x Green x Yellow x Orange x Red x Blue x +

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	25 items	41 items	21 items	49 items	16 items	19 items	15 items	13 items	9 items	20 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	AppCert DLLs	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Control Panel Items	AppInit DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	AppInit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Execution through API	Authentication Package	Application Shimming	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through Module Load	BITS Jobs	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Exploitation for Client Execution	Bootkit	DLL Search Order Hijacking	Component Firmware	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Permission Groups Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Kerberoasting	Process Discovery	Replication Through Removable Media	Input Capture		Multi-hop Proxy
	Mshta	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning	Query Registry	Shared Webroot	Man in the Browser		Multi-Stage Channels
	PowerShell	Create Account	Image File Execution Options Injection	Disabling Security Tools	Network Sniffing	Remote System Discovery	Taint Shared Content	Screen Capture		Multiband Communication
	Regsvcs/Regasm	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Password Filter DLL	Security Software Discovery	Third-party Software	Video Capture		Multilayer Encryption
	Regsvr32	External Remote Services	Path Interception	DLL Side-Loading	Private Keys	System Information Discovery	Windows Admin Shares			Remote Access Tools
	Rundll32	File System Permissions Weakness	Port Monitors	Exploitation for Defense Evasion	Replication Through Removable Media	System Network Configuration Discovery	Windows Remote Management			Remote File Copy
	Scheduled Task	Hidden Files and Directories	Process Injection	Extra Window Memory Injection	Two-Factor Authentication Interception					Standard Application Layer Protocol
	Scripting	Hooking	Scheduled Task	File Deletion						Standard Cryptographic Protocol
	Service Execution	Hypervisor	Service Registry	File System Logical Offsets						Standard Non-Application Layer Protocol
	Signed Binary Proxy Execution	Image File Execution Options Injection		Hidden Files and Directories						
	Signed Script Proxy Execution	Logon Scripts		Image File Execution Options Injection						
	Third-party Software	LSASS Driver		Indicator Blocking						
	Trusted Developer Utilities			Indicator Removal from Tools						
	User Execution			Indicator Removal on						

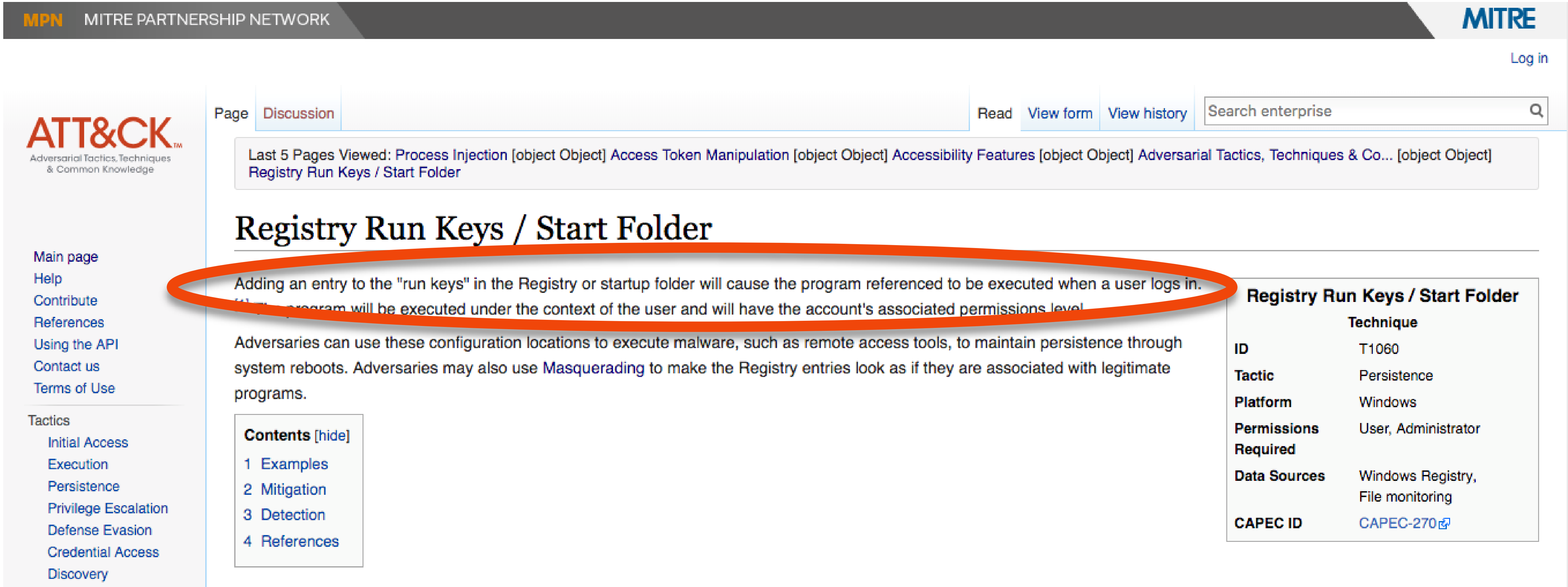
Teaching ATT&CK

In Practice

1. Choose a Tactic (Persistence)
   - Accessibility Features, Change Default File Association, Create Account, Hidden Files and Directories, Image File Execution Options Injection, Logon Scripts, Modify Existing Service, New Service, Office Application Startup, Path Interception, **Registry Run Keys / Start Folder**, Scheduled Task, Screensaver, Service Registry Permission Weakness, Shortcut Modification, Valid Accounts, Winlogon Helper DLL
2. Choose a Technique
   - How can you test/exploit this technique?
   - Follow the mitigation steps, can you still test/exploit it? If not, can you find a way to bypass it?
   - What artifacts are left behind when you test/exploit this? What artifacts are left behind when you bypass?
   - Can you find any which aren’t listed on the technique’s page?

Example: Registry Run Keys

How to test/exploit



Last 5 Pages Viewed: Process Injection [object Object] Access Token Manipulation [object Object] Accessibility Features [object Object] Adversarial Tactics, Techniques & Co... [object Object] Registry Run Keys / Start Folder

Registry Run Keys / Start Folder

Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in.[1] The program will be executed under the context of the user and will have the account's associated permissions level.

Adversaries can use these configuration locations to execute malware, such as remote access tools, to maintain persistence through system reboots. Adversaries may also use Masquerading to make the Registry entries look as if they are associated with legitimate programs.

Contents [hide]

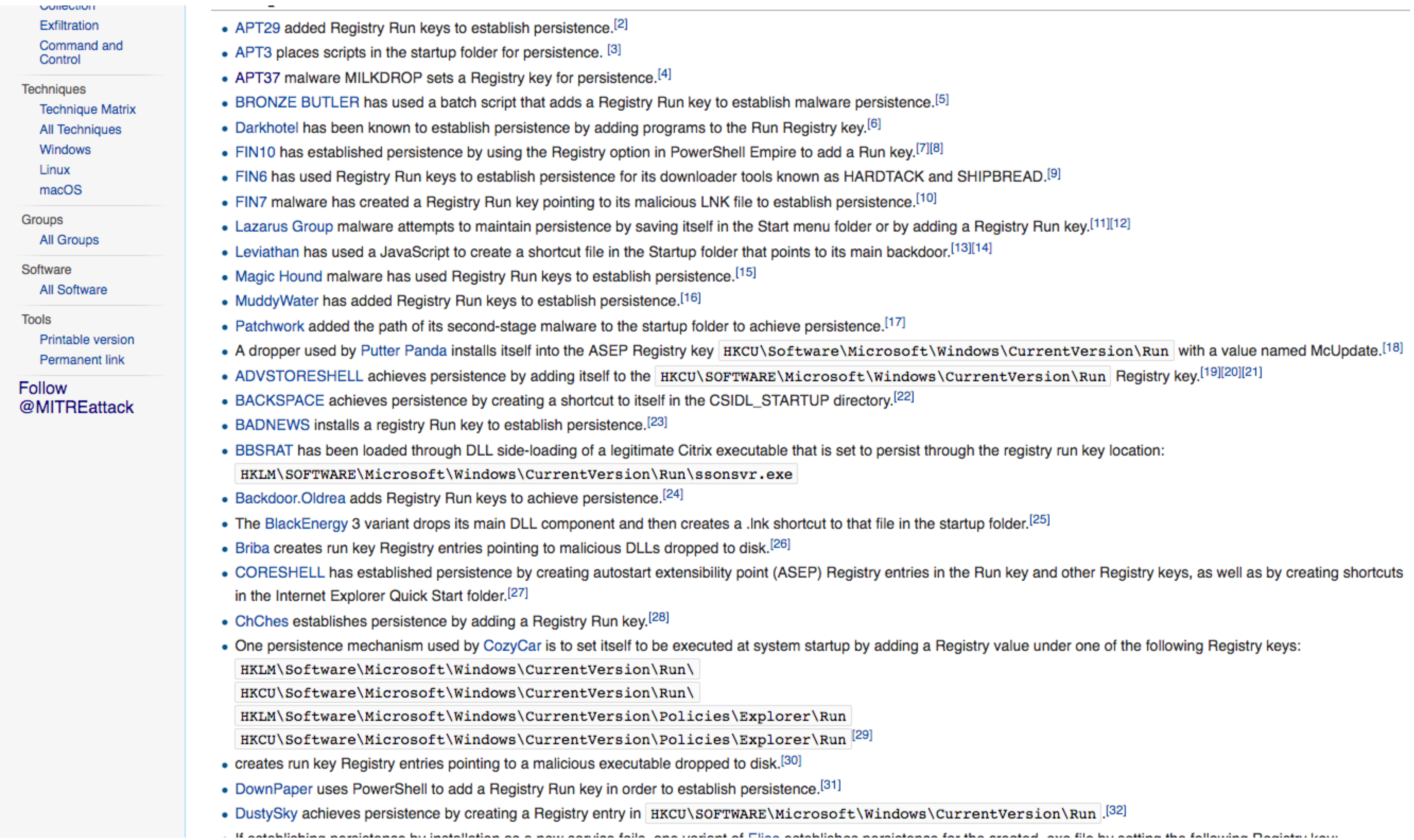
Registry Run Keys / Start Folder

Technique

ID	T1060
Tactic	Persistence
Platform	Windows
Permissions Required	User, Administrator
Data Sources	Windows Registry, File monitoring
CAPEC ID	CAPEC-270

Example: Registry Run Keys

What’s in the Example Section?



Collection
Exfiltration
Command and Control

Techniques
Technique Matrix
All Techniques
Windows
Linux
macOS

Groups
All Groups

Software
All Software

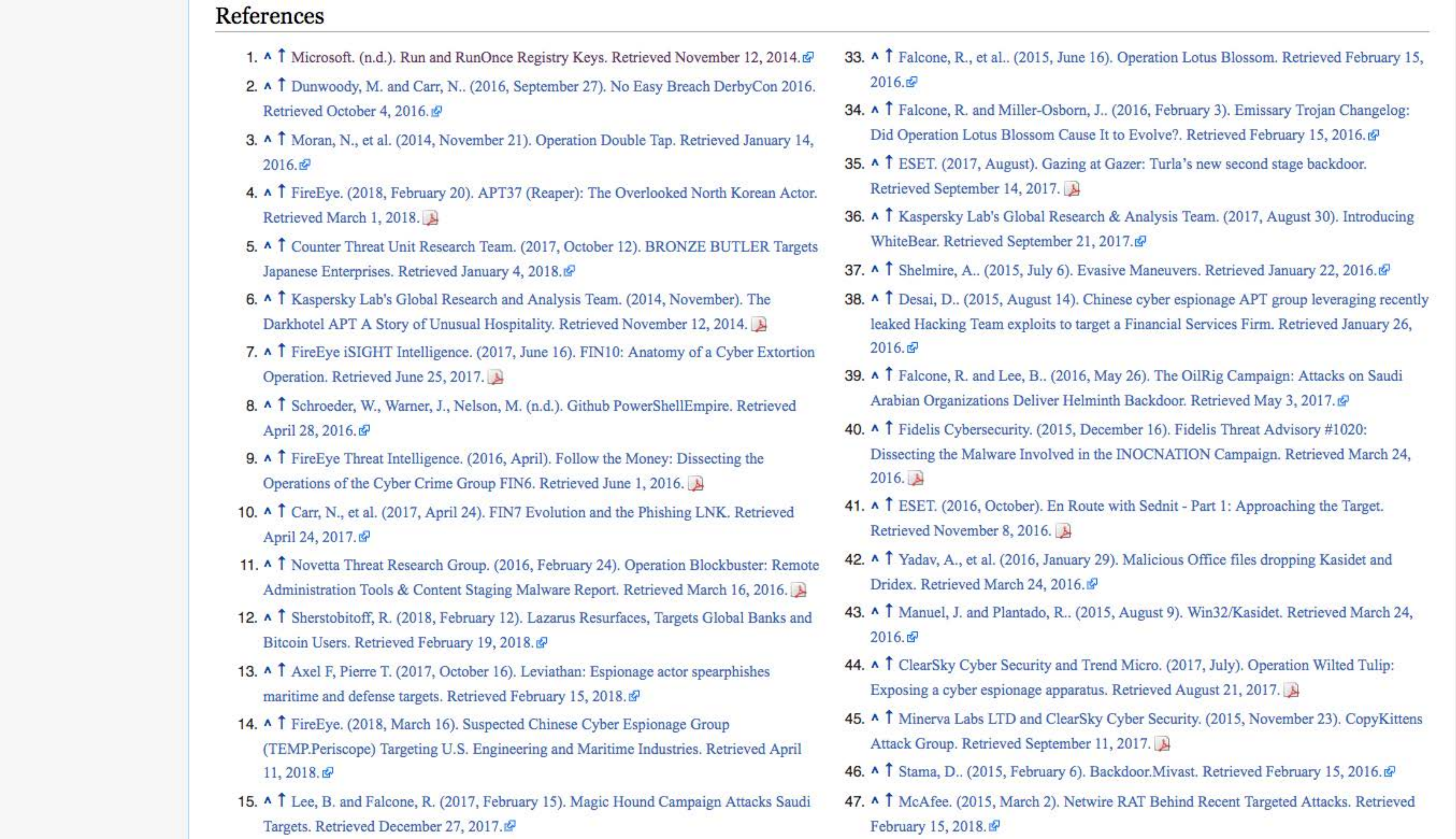
Tools
Printable version
Permanent link

Follow @MITREattack

- APT29 added Registry Run keys to establish persistence.[2]
- APT3 places scripts in the startup folder for persistence. [3]
- APT37 malware MILKDROP sets a Registry key for persistence.[4]
- BRONZE BUTLER has used a batch script that adds a Registry Run key to establish malware persistence.[5]
- Darkhotel has been known to establish persistence by adding programs to the Run Registry key.[6]
- FIN10 has established persistence by using the Registry option in PowerShell Empire to add a Run key.[7][8]
- FIN6 has used Registry Run keys to establish persistence for its downloader tools known as HARDTACK and SHIPBREAD.[9]
- FIN7 malware has created a Registry Run key pointing to its malicious LNK file to establish persistence.[10]
- Lazarus Group malware attempts to maintain persistence by saving itself in the Start menu folder or by adding a Registry Run key.[11][12]
- Leviathan has used a JavaScript to create a shortcut file in the Startup folder that points to its main backdoor.[13][14]
- Magic Hound malware has used Registry Run keys to establish persistence.[15]
- MuddyWater has added Registry Run keys to establish persistence.[16]
- Patchwork added the path of its second-stage malware to the startup folder to achieve persistence.[17]
- A dropper used by Putter Panda installs itself into the ASEP Registry key `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` with a value named McUpdate.[18]
- ADVSTORESHELL achieves persistence by adding itself to the `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` Registry key.[19][20][21]
- BACKSPACE achieves persistence by creating a shortcut to itself in the CSIDL_STARTUP directory.[22]
- BADNEWS installs a registry Run key to establish persistence.[23]
- BBSRAT has been loaded through DLL side-loading of a legitimate Citrix executable that is set to persist through the registry run key location: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ssonsvr.exe`
- Backdoor.Oldrea adds Registry Run keys to achieve persistence.[24]
- The BlackEnergy 3 variant drops its main DLL component and then creates a .lnk shortcut to that file in the startup folder.[25]
- Briba creates run key Registry entries pointing to malicious DLLs dropped to disk.[26]
- CORESHELL has established persistence by creating autostart extensibility point (ASEP) Registry entries in the Run key and other Registry keys, as well as by creating shortcuts in the Internet Explorer Quick Start folder.[27]
- ChChes establishes persistence by adding a Registry Run key.[28]
- One persistence mechanism used by CozyCar is to set itself to be executed at system startup by adding a Registry value under one of the following Registry keys:
  `HKLM\Software\Microsoft\Windows\CurrentVersion\Run\`
  `HKCU\Software\Microsoft\Windows\CurrentVersion\Run\`
  `HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run`
  `HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run` [29]
- creates run key Registry entries pointing to a malicious executable dropped to disk.[30]
- DownPaper uses PowerShell to add a Registry Run key in order to establish persistence.[31]
- DustySky achieves persistence by creating a Registry entry in `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`.[32]
- If establishing persistence by installation as a new service fails, one variant of Elise establishes persistence for the created .exe file by setting the following Registry key:

Example: Registry Run Keys

What's in the References?



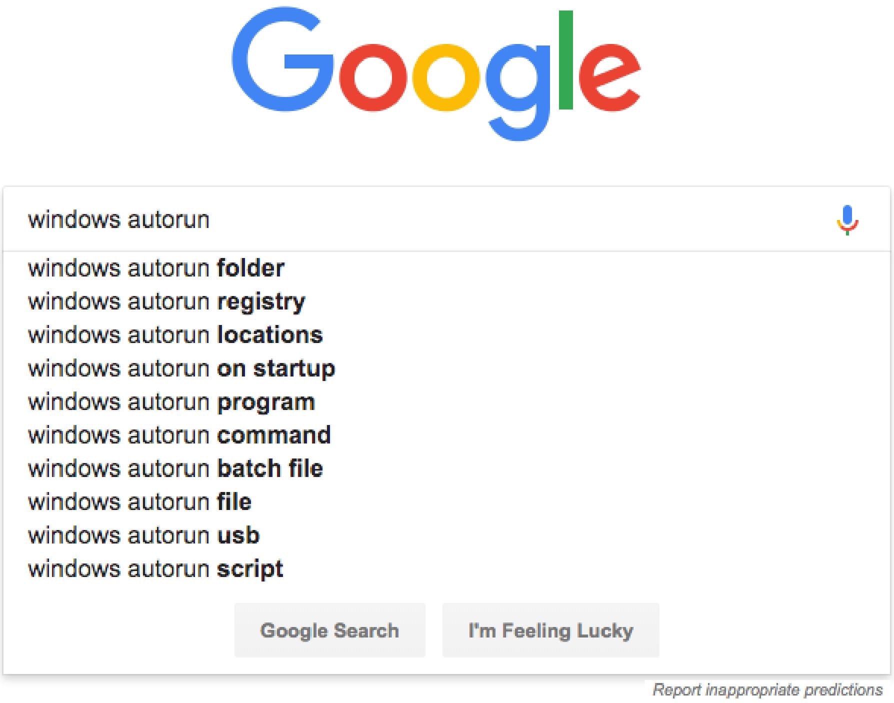
References

1. ^ ↑ Microsoft. (n.d.). Run and RunOnce Registry Keys. Retrieved November 12, 2014.
2. ^ ↑ Dunwoody, M. and Carr, N.. (2016, September 27). No Easy Breach DerbyCon 2016. Retrieved October 4, 2016.
3. ^ ↑ Moran, N., et al. (2014, November 21). Operation Double Tap. Retrieved January 14, 2016.
4. ^ ↑ FireEye. (2018, February 20). APT37 (Reaper): The Overlooked North Korean Actor. Retrieved March 1, 2018.
5. ^ ↑ Counter Threat Unit Research Team. (2017, October 12). BRONZE BUTLER Targets Japanese Enterprises. Retrieved January 4, 2018.
6. ^ ↑ Kaspersky Lab's Global Research and Analysis Team. (2014, November). The Darkhotel APT A Story of Unusual Hospitality. Retrieved November 12, 2014.
7. ^ ↑ FireEye iSIGHT Intelligence. (2017, June 16). FIN10: Anatomy of a Cyber Extortion Operation. Retrieved June 25, 2017.
8. ^ ↑ Schroeder, W., Warner, J., Nelson, M. (n.d.). Github PowerShellEmpire. Retrieved April 28, 2016.
9. ^ ↑ FireEye Threat Intelligence. (2016, April). Follow the Money: Dissecting the Operations of the Cyber Crime Group FIN6. Retrieved June 1, 2016.
10. ^ ↑ Carr, N., et al. (2017, April 24). FIN7 Evolution and the Phishing LNK. Retrieved April 24, 2017.
11. ^ ↑ Novetta Threat Research Group. (2016, February 24). Operation Blockbuster: Remote Administration Tools & Content Staging Malware Report. Retrieved March 16, 2016.
12. ^ ↑ Sherstobitoff, R. (2018, February 12). Lazarus Resurfaces, Targets Global Banks and Bitcoin Users. Retrieved February 19, 2018.
13. ^ ↑ Axel F, Pierre T. (2017, October 16). Leviathan: Espionage actor spearphishes maritime and defense targets. Retrieved February 15, 2018.
14. ^ ↑ FireEye. (2018, March 16). Suspected Chinese Cyber Espionage Group (TEMP.Periscope) Targeting U.S. Engineering and Maritime Industries. Retrieved April 11, 2018.
15. ^ ↑ Lee, B. and Falcone, R. (2017, February 15). Magic Hound Campaign Attacks Saudi Targets. Retrieved December 27, 2017.

33. ^ ↑ Falcone, R., et al.. (2015, June 16). Operation Lotus Blossom. Retrieved February 15, 2016.
34. ^ ↑ Falcone, R. and Miller-Osborn, J.. (2016, February 3). Emissary Trojan Changelog: Did Operation Lotus Blossom Cause It to Evolve?. Retrieved February 15, 2016.
35. ^ ↑ ESET. (2017, August). Gazing at Gazer: Turla's new second stage backdoor. Retrieved September 14, 2017.
36. ^ ↑ Kaspersky Lab's Global Research & Analysis Team. (2017, August 30). Introducing WhiteBear. Retrieved September 21, 2017.
37. ^ ↑ Shelmire, A.. (2015, July 6). Evasive Maneuvers. Retrieved January 22, 2016.
38. ^ ↑ Desai, D.. (2015, August 14). Chinese cyber espionage APT group leveraging recently leaked Hacking Team exploits to target a Financial Services Firm. Retrieved January 26, 2016.
39. ^ ↑ Falcone, R. and Lee, B.. (2016, May 26). The OilRig Campaign: Attacks on Saudi Arabian Organizations Deliver Helminth Backdoor. Retrieved May 3, 2017.
40. ^ ↑ Fidelis Cybersecurity. (2015, December 16). Fidelis Threat Advisory #1020: Dissecting the Malware Involved in the INOCNATION Campaign. Retrieved March 24, 2016.
41. ^ ↑ ESET. (2016, October). En Route with Sednit - Part 1: Approaching the Target. Retrieved November 8, 2016.
42. ^ ↑ Yadav, A., et al. (2016, January 29). Malicious Office files dropping Kasidet and Dridex. Retrieved March 24, 2016.
43. ^ ↑ Manuel, J. and Plantado, R.. (2015, August 9). Win32/Kasidet. Retrieved March 24, 2016.
44. ^ ↑ ClearSky Cyber Security and Trend Micro. (2017, July). Operation Wilted Tulip: Exposing a cyber espionage apparatus. Retrieved August 21, 2017.
45. ^ ↑ Minerva Labs LTD and ClearSky Cyber Security. (2015, November 23). CopyKittens Attack Group. Retrieved September 11, 2017.
46. ^ ↑ Stama, D.. (2015, February 6). Backdoor.Mivast. Retrieved February 15, 2016.
47. ^ ↑ McAfee. (2015, March 2). Netwire RAT Behind Recent Targeted Attacks. Retrieved February 15, 2018.

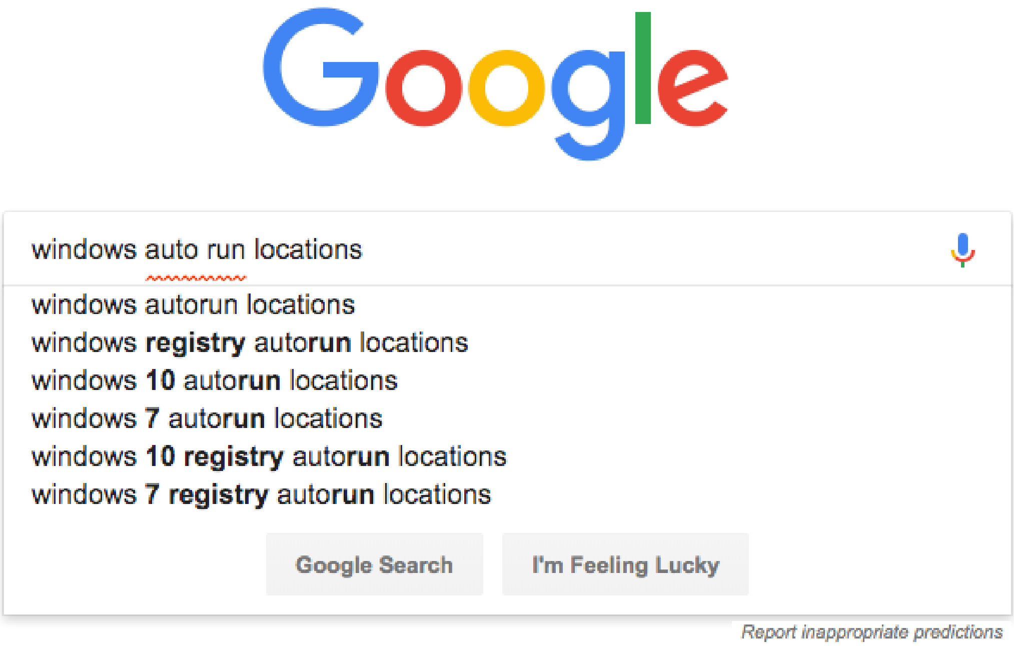
Example: Registry Run Keys

Do your own research, what's missing?



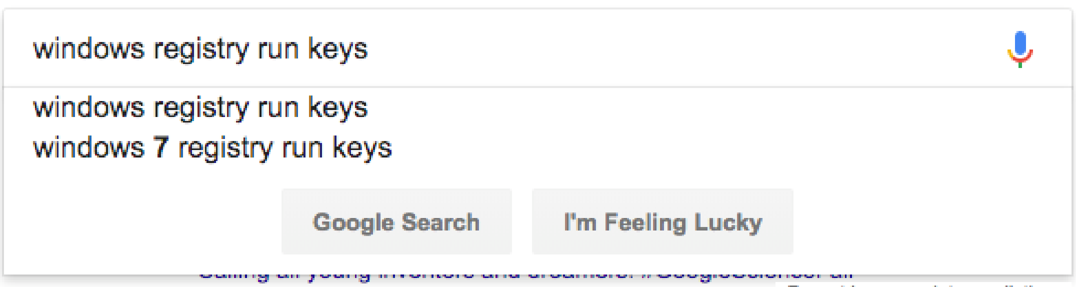
windows autorun

windows autorun **folder**
windows autorun **registry**
windows autorun **locations**
windows autorun **on startup**
windows autorun **program**
windows autorun **command**
windows autorun **batch file**
windows autorun **file**
windows autorun **usb**
windows autorun **script**



windows auto run locations

windows autorun locations
windows **registry** autorun locations
windows **10** autorun locations
windows **7** autorun locations
windows **10 registry** autorun locations
windows **7 registry** autorun locations

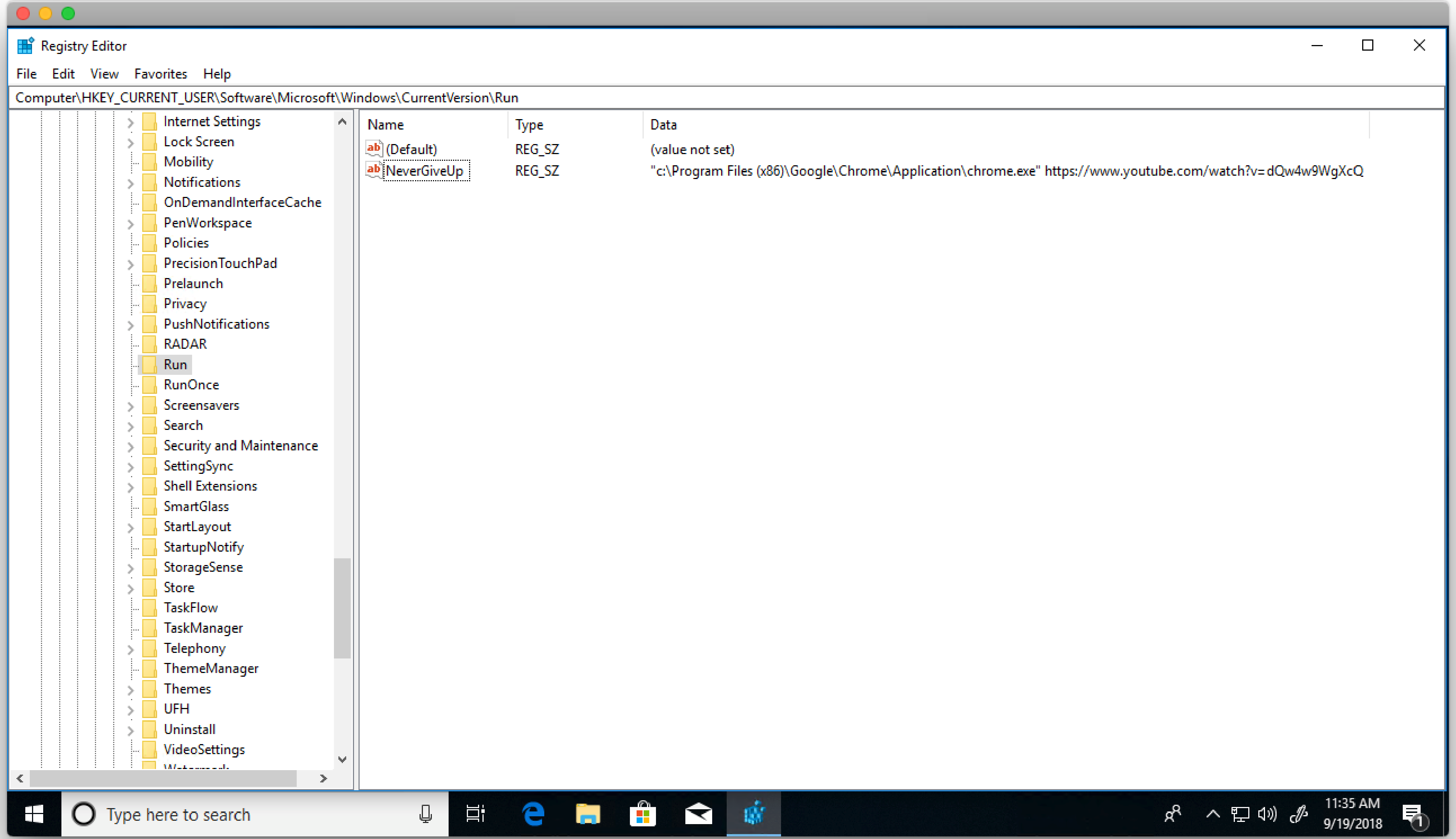


windows registry run keys

windows registry run keys
windows **7** registry run keys

Example: Registry Run Keys

Test it

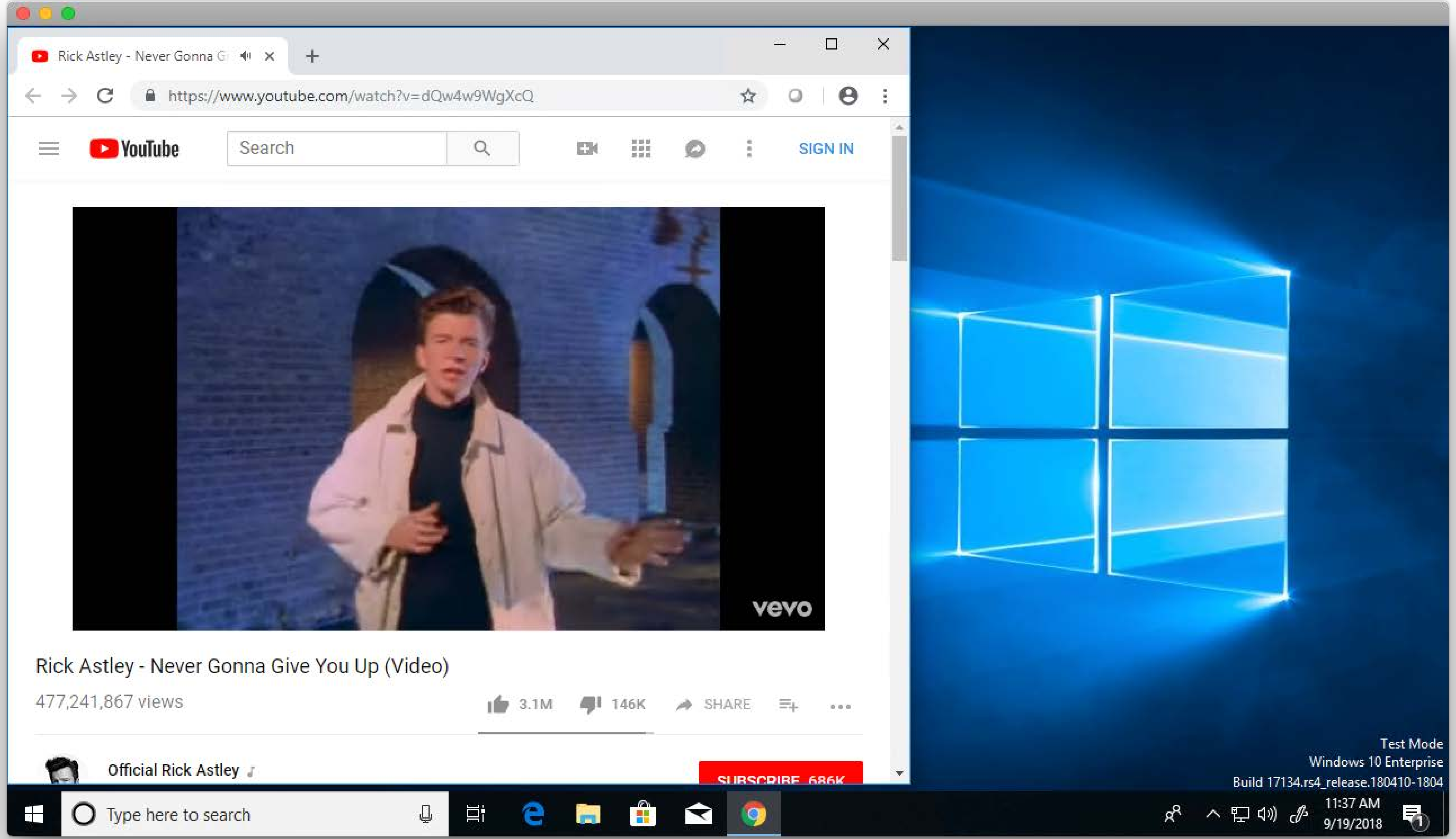


Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
NeverGiveUp	REG_SZ	"c:\Program Files (x86)\Google\Chrome\Application\chrome.exe" https://www.youtube.com/watch?v=dQw4w9WgXcQ

Example: Registry Run Keys

Test it



Learning Outcomes

What Did You Learn	
Was it in ATT&CK?	Was it From Original Research

Mitigations	
Did they work?	Can any be added?

Detections	
Did they work?	Can any be added?

Testing Coverage

Source: MITRE/GitHub

- http://attack.mitre.org/wiki/Adversary_Emulation_Plans
- https://github.com/NextronSystems/APTSimulator
- https://github.com/redcanaryco/atomic-red-team

Thank You

tripwire.com | @TripwireInc