



MITRE ATT&CK Matrix with CIS Controls 2–6 and Tripwire Mapping

It's not enough to cast a wide cybersecurity net and hope you catch the adversaries trying to compromise your data. Instead, you need to narrow your focus to make your efforts truly impactful.

But which of the countless potential cybersecurity attacks out there should you choose to prioritize? MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework and the Center for Internet Security's CIS Controls are two industry-leading sources clearly stating which cybersecurity best practices organizations and agencies should heed.

» **MITRE** is a not-for-profit organization that operates federally-funded research and development centers. Their ATT&CK framework is a useful cybersecurity model illustrating how adversaries behave and explaining the tactics you should use to mitigate risk and improve security.

» **The Center for Internet Security (CIS)** is a nonprofit organization that sources knowledge from IT experts around the world. The CIS Controls is a list of top 20 critical security controls prioritized to protect from attack vectors. We'll focus on the first six controls, known as their "basic controls" (note that Control 1 does not apply to the ATT&CK framework).

How MITRE ATT&CK and CIS Controls Intersect

Both MITRE ATT&CK framework and the CIS Controls provide the crucial intelligence you need in order to maintain a strong cybersecurity stance. Where MITRE focuses on specific actions taken by adversaries in an enterprise network and shows you how to combat them proactively, CIS lays out a step-by-step process for securing your data in terms of configuration management and other system hardening processes.

Both empower you to take charge of your data's and systems' safety. All in all, these are two distinct models addressing similar issues. It's not a matter of picking which institution's guidelines to follow—you should be utilizing both of these resources simultaneously and ensuring your alignment with them often.

MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's lifecycle and the platforms they are known to target. ATT&CK is useful for understanding security risk against known adversary behavior, for planning security improvements, and verifying defenses work as expected.

— MITRE

Many organizations facing the current cybersecurity environment are overwhelmed by what we call the "Fog of More"—a constant stream of new information and problems. ... The CIS Controls are designed to bring priority and focus to this daunting task, to harness the power of a large expert community to identify and support high-value practices and foundational steps, and to stop "admiring the problem."

— Center for Internet Security



MITRE ATT&CK Matrix — Where Tripwire Helps (Windows)

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



MITRE ATT&CK Matrix — ■=with CIS Control 2 overlay ■=Where Tripwire helps (Windows)

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



MITRE ATT&CK Matrix — ■=with CIS Control 3 overlay ■=Where Tripwire helps (Windows)

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



MITRE ATT&CK Matrix — ■=with CIS Control 4 overlay■=Where Tripwire helps (Windows)

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



MITRE ATT&CK Matrix — ■=with CIS Control 5 overlay ■=Where Tripwire helps (Windows)

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



MITRE ATT&CK Matrix — ■=with CIS Control 6 overlay ■=Where Tripwire helps (Windows)

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



Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

The State of Security: News, trends and insights at tripwire.com/blog
Connect with us on [LinkedIn](#), [Twitter](#) and [Facebook](#)