FORTRA™

GUIDE (TRIPWIRE)

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

FORTRA

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 18 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 the 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**

FORTRA™

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

INITIAL ACCESS
Drive-by Compromise
Exploit Public-Facing Application
Hardware Additions
Replication Through Removable Media
Spearphishing Attachments
Spearphishing Link
Spearphishing via Service
Supply Chain Compromise
Trusted Relationship
Valid Accounts

EXECUTION
AppleScript
CMSTP
Command-Line Interface
Control Panel Items
Dynamic Data Exchange
Execution through API
Execution through Module Load
Exploitation for Client Execution
Graphical User Interface
InstallUtil
LSASS Driver
Launchctl
Local Job Scheduling
Mshta
PowerShell
Regsvcs/Regasm
Regsvr32
Rundll32
Scheduled Task
Scripting
Service Execution
Signed Binary Proxy Execution
Signed Script Proxy Execution
Source
Space after Filename
Third-party Software
Trap
Trusted Developer Utilities
User Execution
Windows Management Instrumentation
Windows Remote Management

PERSISTENCE
.bash_profile and .bashrc
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Authentication Package
BITS Jobs
Bootkit
Browser Extensions
Change Default File Association
Component Firmware
Component Object Model Hijacking
DLL Search Order Hijacking
Dylib Hijacking
External Remote Services
File System Permissions Weakness
Hidden Files and Directories
Hooking
Hypervisor
Image File Execution Options Injection
Kernel Modules and Extensions
LC_LOAD_DYLIB Addition
LSASS Driver
Launch Agent
Launch Daemon
Launchctl
Local Job Scheduling
Login Item
Logon Scripts
Modify Existing Service
Netsh Helper DLL
New Service
Office Application Startup
Path Interception
Plist Modification
Port Knocking
Port Monitors
Rc.common
Re-opened Applications
Redundant Access
Registry Run Keys / Start Folder
SIP and Trust Provider Hijacking
Scheduled Task
Screensaver
Security Support Provider
Service Registry Permissions Weakness
Shortcut Modification
Startup Items
System Firmware
Time Providers
Trap
Valid Accounts
Web Shell
Windows Management Instrumentation Event Subscription
Winlogon Helper DLL
Create Account

PRIVILEGE ESCALATION
Access Token Manipulation
Accessibility Features
AppCert Dlls
AppInit DLLs
Application Shimming
Authentication Package
DLL Search Order Hijacking
Dylib Hijacking
Exploitation of Vulnerability
Extra Window Memory Injection
File System Permissions Weakness
Hooking
Image File Execution Options Injection
Launch Daemon
New Service
Path Interception
Plist Modification
Port Monitors
Process Injection
SID-History Injection
Scheduled Task
Service Registry Permissions Weakness
Setuid and Setgid
Startup Items
Sudo
Sudo Caching
Valid Accounts
Web Shell

DEFENSE EVASION
Access Token Manipulation
BITS Jobs
Binary Padding
Bypass User Account Control
CMSTP
Clear Command History
Code Signing
Component Firmware
Component Object Model Hijacking
Control Panel Items
DCShadow
DLL Search Order Hijacking
DLL Side-Loading
Deobfuscate/Decode Files or Information
Disabling Security Tools
Exploitation of Vulnerability
Extra Window Memory Injection
File Deletion
File System Logical Offsets
Gatekeeper Bypass
HISTCONTROL
Hidden Files and Directories
Image File Execution Options Injection
Hidden Users
Hidden Window
Indicator Blocking
Indicator Removal from Tools
Indicator Removal on Host
Install Root Certificate
InstallUtil
LC_MAIN Hijacking
Launchctl
Masquerading
Modify Registry
Mshta
NTFS Extended Attributes
Network Share Connection Removal
Obfuscated Files or Information
Plist Modification
Port Knocking
Process Doppelgänging
Process Hollowing
Process Injection
Redundant Access
Regsvcs/Regasm
Regsvr32
Rootkit
Rundll32
SIP and Trust Provider Hijacking
Scripting
Signed Binary Proxy Execution
Signed Script Proxy Execution
Software Packing
Space after Filename
Timestomp
Trusted Developer Utilities
Valid Accounts
Web Service

CREDENTIAL ACCESS
Account Manipulation
Bash History
Brute Force
Credential Dumping
Credentials in Files
Credentials in Registry
Exploitation for Credential Access
Forced Authentication
Hooking
Input Capture
Input Prompt
Kerberoasting
Keychain
LLMNR/NBT-NS Poisoning
Network Sniffing
Password Filter DLL
Private Keys
Replication Through Removable Media
Securityd Memory
Two-Factor Authentication Interception

DISCOVERY
Account Discovery
Application Window Discovery
Browser Bookmark Discovery
File and Directory Discovery
Network Service Scanning
Network Share Discovery
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Security Software Discovery
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery

LATERAL MOVEMENT
AppleScript
Application Deployment Software
Distributed Component Object Model
Exploitation of Remote Services
Logon Scripts
Pass the Hash
Pass the Ticket
Remote Desktop Protocol
Remote File Copy
Remote Services
Replication Through Removable Media
SSH Hijacking
Shared Webroot
Taint Shared Content
Third-party Software
Windows Admin Shares
Windows Remote Management

COLLECTION
Audio Capture
Automated Collection
Clipboard Data
Data Staged
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Email Collection
Input Capture
Man in the Browser
Screen Capture
Video Capture

EXFILTRATION
Automated Exfiltration
Data Compressed
Data Encrypted
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over Command and Control Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Scheduled Transfer

COMMAND AND CONTROL
Commonly Used Port
Communication Through Removable Media
Connection Proxy
Custom Command and Control Protocol
Custom Cryptographic Protocol
Data Encoding
Data Obfuscation
Domain Fronting
Fallback Channels
Multi-Stage Channels
Multi-hop Proxy
Multiband Communication
Multilayer Encryption
Port Knocking
Remote Access Tools
Remote File Copy
Standard Application Layer Protocol
Standard Cryptographic Protocol
Standard Non-Application Layer Protocol
Uncommonly Used Port
Web Service

FORTRA™

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						
		Rc.common		Obfuscated Files or Information						
		Re-opened Applications		Plist Modification						
		Redundant Access		Port Knocking						
		Registry Run Keys / Start Folder		Process Doppelgänging						
		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		Timestomp						
				Trusted Developer Utilities						
				Valid Accounts						
				Web Service						

FORTRA™

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	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		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 Doppelgänging						
		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		Timestomp						
				Trusted Developer Utilities						
				Valid Accounts						
				Web Service						

FORTRA™

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		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 Doppelgänging						
		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		Timestomp						
		Create Account		Trusted Developer Utilities						
				Valid Accounts						
				Web Service						

FORTRA™

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	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		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 Doppelgänging						
		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		Timestomp						
				Trusted Developer Utilities						
				Valid Accounts						
				Web Service						

FORTRA™

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	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		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 Doppelgänging						
		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		Timestomp						
		Create Account		Trusted Developer Utilities						
				Valid Accounts						
				Web Service						

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

(fta-tw-gd-0123-ri-hm)