

# ENDGAME.

■ ■ ■

## WHAT'S YOUR PLAN OF ATT&CK?

USING THE MITRE FRAMEWORK TO ASSESS AND  
IMPROVE YOUR SECURITY MATURITY

# THE RISE OF TARGETED ATTACKS

## NATION-STATES TARGETING GOVERNMENT & INFRASTRUCTURE

**SOUTH KOREA:**  
DARK SEOUL

Japan/USA:  
Sony Hack

Ukraine:  
Energy Grid

USA:  
Office of Personnel  
Management

USA:  
Democratic Party

Saudi Arabia:  
StoneDrill Wiper

Ukraine:  
Energy Grid

South Korea:  
Olympic Destroyer

Global:  
VPNFilter

## NATION-STATE RELATED ACTORS TARGETING INDUSTRY

USA:  
Energy Grid

USA:  
Casino Wiper

**USA:**  
YAHOO! HACK

USA:  
Health Insurer

Europe:  
Siemens AG,  
Moody's

Global:  
300+ Universities

Bangladesh:  
SWIFT Heist

Global:  
NotPetya

Global:  
BadRabbit

Global:  
Marriot Hotels

## CRIMINALS BROADLY ADOPTING AUTOMATED NATION-STATE TECHNIQUES



GameOver  
Zeus – 100K+

USA:  
J.P. Morgan

USA:  
Ashley Madison



Mirai Bot –  
164 Countries

Global:  
FIN7



Brickerbot –  
Millions of IoT

USA:  
Equifax Credit

Global:  
MassMiner

USA:  
Facebook

**NORWAY:**  
NORSK HYDRO



2013

2014

2015

2016

2017

2018

2019



**There's no one-size-fits-all for security,  
the era of set and forget is all but  
forgotten.**

**Ian McShane, Research Director Analyst, Gartner, 2018**

**E.**



# ATTACKS HAVE EVOLVED

**54%**

OF COMPANIES EXPERIENCED  
1+ ATTACKS THAT COMPROMISED DATA  
OR IT INFRASTRUCTURE

**77%**

OF THOSE ATTACKS UTILIZED EXPLOITS  
OR FILELESS TECHNIQUES

Cyber criminals have broadened their reach to bypass simple but popular security mechanisms and use bespoke software to target your organization



**1** RISE OF NATION-STATE  
HACKING GROUPS



**2** MALWARE NOW WORKS  
TO STAY HIDDEN



**3** AUTOMATED AND "MALWARE-AS-A-SERVICE" TOOLS HAVE MADE FILE-BASED DETECTION OBSOLETE





TODAY'S  
TARGETED  
ATTACKS ARE:

1. ADAPTIVE
2. EXTENDED
3. DIVERSE

NOT JUST MALWARE. NO SINGLE TECHNIQUE.



**“It’s time to evolve from a file-based focus  
to an adversary-based focus”**

Ian McShane, Research Director Analyst, Gartner, 2018



# ■ MITRE'S ADVERSARIAL TACTICS, TECHNIQUES, AND COMMON KNOWLEDGE (ATT&CK)

- Provides the most comprehensive model of modern attacker behavior
- Informs defensive coverage and gap assessments
  - allowing organizations to intelligently prioritize areas for additional data collection, analysis, and detection
- When operationalized -- the framework moves organizations from reactive to proactive postures
- Helps bridge the gap between practitioners and executives
  - enabling leadership to make more informed risk management and resource allocation decisions



# OPEN SOURCE FRAMEWORK

# MITRE ATT&CK Framework

# 200+ ATTACKER TECHNIQUES

# MULTIPLE OS COVERAGE

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	EXFILTRATION	IMPACT
Drive-by Compromise	Application Shimming	Accessibility Features	Path Interception	Accessibility Features	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Command-Line	AppInit DLLs	Redundant Access	Access Token Manipulation	Binary Padding	Brute Force	Application Window Discovery	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
Hardware Additions	Interface Execution through API	Application Shimming	Registry Run Keys / Start Folder	AppInit DLLs	Bypass User Account Control	Create Account	File and Directory Discovery	Exploitation of Vulnerability	Clipboard Data	Data Encrypted	Defacement
Replication Through Removable Media	Execution through module load	Authentication Package	Scheduled Task	Application Shimming	Code Signing	Credential Dumping	Network Service Scanning	Logon Script	Data Staged	Data Transfer Size Limits	Disk Content Wipe
Spearfishing Attachment	Graphical User Interface	Bootkit	Security Support Provider	Bypass User Account Control	Component Firmware	Credentials in Files	Network Share Discovery	Pass the Hash	Data from Local System	Custom Command and Control Protocol	Disk Structure Wipe
Spearfishing Link	InstallUtil	Change Default File Association	Shortcut Modification	DLL Injection	Component Object	Exploitation of Vulnerability	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol
Spearfishing via Service	PowerShell	Component Firmware	Service Registry Permissions Weakness	DLL Search Order Hijacking	Model Hijacking	Obfuscated Files or Information	Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Data Encoding	Exfiltration Over Command and Control
Supply Chain Compromise	Process Hollowing	Component Object Model Hijacking	System Firmware	Exploitation of Vulnerability	Deobfuscate/Decode Files or Information	Process Hollowing	Permission Groups Discovery	Remote File Copy	Email Collection	Data Obfuscation	Channel Exfiltration Over Other Network
Trusted Relationship	Regsvcs/Regasm	Valid Accounts	Web Shell	File System Permissions Weakness	DLL Injection	Redundant Access	Process Discovery	Replication Through Removable Media	Input Capture	Fallback Channels	Multi-Stage Channels
Valid Accounts	Regsvr32	External Remote Services	Windows Management Instrumentation Event Subscription	Local Port Monitor	DLL Search Order Hijacking	Regsvcs/Regasm	Query Registry	Remote System Discovery	Screen Capture	Multi-Band Communication	Scheduled Transfer
	Rundl32	File System Permissions Weaknesses	Winlogon Helper DLL	New Service	DLL Side-Loading	Rootkit	Remote System Discovery	Shared Webroot	Video Capture	Multi-layer Encryption	Runtime Data Manipulation
	Scheduled Task	Hidden Files and Directories		Path Interception	Disabling Security Tools	Rundl32	Security Software Discovery	Taint Shared Content	Remote File Copy	Remote File Copy	Service Stop
	Scripting			Scheduled Task	Exploitation of Vulnerability	Scripting	System Information Discovery	Windows Admin Shares	Standard Application Layer Protocol		Stored Data Manipulation
	Service Execution	Hypervisor		Service Registry Permissions Weakness	File Deletion	Software Packing	System Network Discovery	Windows Remote Management	Standard Cryptographic Protocol		Transmitted Data Manipulation
	Third-party Software	Local Port Monitor		File System Logical Offsets	File System Logical Offsets	Trusted Developer Utilities	System Network Connections Discovery		Standard Non-Application Layer Protocol		
	Trusted Developer Utilities	Logon Scripts		Web Shell	Hidden Files and Directories	Valid Accounts	System Owner/User Discovery		Uncommonly Used Port		
	Windows Management Instrumentation	Modify Existing Service		Indicator Blocking	Indicator Blocking		System Service Discovery		Web Service		
	Windows Remote Management	Netsis Helper DLL		Indicator Removal from Tools	Indicator Removal from Tools		System Time Discovery				
		New Service		Indicator Removal on Host	Indicator Removal on Host						
		Office Application Startup									

# USING THE MITRE FRAMEWORK TO ASSESS AND IMPROVE YOUR SECURITY MATURITY

- Identify those groups who have previously targeted your corporate ecosystem (e.g., parent company, supply chain, industry).
- With this knowledge you can begin to prioritize your ATT&CK coverage against previously observed attacks.
- Evaluate your current security tools coverage of the appropriate ATT&CK vectors.

THE GOOD NEWS IS FULL COVERAGE IS NOT  
NEEDED TO MAKE A SIGNIFICANT  
IMPROVEMENT TO YOUR SECURITY  
PROGRAM



# MITRE ATT&CK MATRIX

INITIAL ACCESS	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	EXECUTION	COLLECTION	EXFILTRATION	COMMAND AND CONTROL
Drive-by Compromise	Accessibility Features	New Service	Accessibility Features	Account Manipulation	Account Discovery	Application Deployment Software	Application Shimming	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Applnit DLLs	Office Application Startup	Access Token Manipulation	Brute Force	Application Window Discovery	Exploitation of Vulnerability	Command-Line	Automated Collection	Clipboard Data	Communication Through Removable Media
Hardware Additions	Application Shimming	Path Interception	Applnit DLLs	Credential Dumping	File and Directory Discovery	Logon Scripts	Interface Execution through API	Clipboard Data	Data Staged	Collection Proxy
Replication Through Removable Media	Authentication Package	Redundant Access	Application Shimming	Credential Dumping	Network Service Scanning	Pass the Hash	Execution through module load	Data from Local System	Data from Network Shared Drive	Custom Command and Control Protocol
Spearphishing Attachment	Change Default File Association	Scheduled Task	Bypass User Account Control	Code Signing	Network Share Discovery	Pass the Ticket	Execution through module load	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Component Firmware	Security Support Provider	DLL Injection	Component Object	Connection Removal	Remote Desktop Protocol	Graphical User Interface	Data from Removable Media	Exfiltration Over Command and Control	Data Encoding
Spearphishing via Service	Component Object Model Hijacking	Shortcut Modification	DLL Search Order Hijacking	Model Hijacking	NTFS Extended Attributes	Remote File Copy	Graphical User Interface	Data from Removable Media	Channel Exfiltration Over Other Network	Data Obfuscation
Supply Chain Compromise	DLL Search Order Hijacking	Service Registry Permissions Weakness	Exploitation of Vulnerability	Deobfuscate/Decode Files or Information	Obfuscated Files or Information	Process Discovery	PowerShell	Data Collection	Medium Exfiltration Over Physical Medium	Fallback Channels
Trusted Relationship	External Remote Services	System Firmware	File System Permissions Weakness	DLL Injection	Process Hollowing	Two-Factor Authentication Interception	PowerShell	Input Capture	Scheduled Transfer	Multi-Stage Channels
Valid Accounts	File System Permissions Weaknesses	Valid Accounts	Local Port Monitor	DLL Search Order Hijacking	Redundant Access	Task Scheduling	Regsvcs/Regasm	Screen Capture	Scheduled Transfer	Multiband Communication
Hidden Files and Directories	Web Shell	Windows Management Instrumentation Event Subscription	DLL Side-Loading	DLL Side-Loading	Regsvcs/Regasm	Task Scheduling	Regsvr32	Video Capture	Scheduled Transfer	Multilayer Encryption
Hypervisor	Winlogon Helper DLL	Path Interception	Disabling Security Tools	Regsvr32	Regsvr32	Third-party Software	Rundll32	Video Capture	Scheduled Transfer	Remote File Copy
Local Port Monitor	Logon Scripts	Exploitation of Vulnerability	Exploitation of Vulnerability	Rootkit	Rootkit	System Network Discovery	Scheduled Task	Video Capture	Scheduled Transfer	Standard Application Layer Protocol
Modify Existing Service	Netsh Helper DLL	Winlogon Helper DLL	File Deletion	Rundll32	Rundll32	System Network Connections Discovery	Scripting	Video Capture	Scheduled Transfer	Standard Cryptographic Protocol
		Path Interception	File System Logical Offsets	Scripting	Scripting	System Owner/User Discovery	Service Execution	Video Capture	Scheduled Transfer	Standard Non-Application Layer Protocol
		Path Interception	Logical Offsets	Software Packing	Software Packing	System Service Discovery	Third-party Software	Video Capture	Scheduled Transfer	Uncommonly Used Port
		Path Interception	Web Shell	Hidden Files and Directories	Hidden Files and Directories	System Time Discovery	Trusted Developer Utilities	Video Capture	Scheduled Transfer	Web Service
		Path Interception	Indicator Blocking	Indicator Blocking	Indicator Blocking		Windows Management Instrumentation	Video Capture	Scheduled Transfer	
		Path Interception	Indicator Removal from Tools	Indicator Removal from Tools	Indicator Removal from Tools		Windows Remote Management	Video Capture	Scheduled Transfer	

UAC BYPASS

CREDENTIAL DUMPING

POWERSHELL

NETWORK SHARE DISCOVERY

PROCESS INJECTION

DATA COMPRESSION



# TODAY

## SECURITY PROGRAMS

### MOST ORGANIZATIONS FOCUS HERE

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	EXFILTRATION	IMPACT
Drive-by Compromise	Application Shimming	Accessibility Features	Path Interception	Accessibility Features	Access Token Manipulation	Account Manipulation	Account Discovery	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Command-Line	AppInit DLLs	Redundant Access	Access Token Manipulation	Binary Padding	Brute Force	Application Window Discovery	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
Hardware Additions	Interface Execution through API	Application Shimming	Registry Run Keys / Start Folder	AppInit DLLs	Masquerading	Create Account	Exploitation of Vulnerability	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Replication Through Removable Media	Execution through module load	Authentication Package	Scheduled Task	Application Shimming	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Spearphishing Attachment	Graphical User Interface	Bootkit	Security Support Provider	Bypass User Account Control	Component Firmware	Credentials in Files	Network Service Scanning	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Link	Graphical User Interface	Change Default File Association	Shortcut Modification	DLL Injection	Component Object	Exploitation of Vulnerability	Network Share Discovery	Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Command and Control	Endpoint Denial of Service
Spearphishing via Service	PowerShell	Component Firmware	Service Registry Permissions Weakness	DLL Search Order Hijacking	Model Hijacking	Input Capture	Peripheral Device Discovery	Data from Removable Media	Data Encoding	Exfiltration Over Command and Control	Firmware Corruption
Supply Chain Compromise	Process Hollowing	Component Object Model Hijacking	System Firmware	Deobfuscate/Decode Files or Information	Obfuscated Files or Information	Network Sniffing	Remote File Copy	Email Collection	Data Obfuscation	Channel Exfiltration Over Other Network	Inhibit System Recovery
Trusted Relationship	Regsvcs/Regasm	Valid Accounts	Web Shell	Exploitation of Vulnerability	Process Hollowing	Private Keys	Remote Services	Fallback Channels	Channel Exfiltration Over Other Network	Medium Exfiltration Over Physical Medium	Network Denial of Service
Valid Accounts	Regsvr32	External Remote Services	Windows Management Instrumentation Event Subscription	File System Permissions Weakness	DLL Injection	Two-Factor Authentication Interception	Process Discovery	Input Capture	Multi-Stage Channels	Scheduled Transfer	Resource Hijacking
	Rundll32	File System Permissions Weaknesses	Winlogon Helper DLL	DLL Search Order Hijacking	Redundant Access	Query Registry	Replication Through Removable Media	Screen Capture	Multiband Communication	Scheduled Transfer	Runtime Data Manipulation
	Scheduled Task	Hidden Files and Directories	Winlogon Helper DLL	DLL Side-Loading	Disabling Security Tools	Remote System Discovery	Shared Webroot	Video Capture	Multilayer Encryption	Service Stop	Stored Data Manipulation
	Scripting	Hidden Files and Directories	Winlogon Helper DLL	Disabling Security Tools	Exploitation of Vulnerability	Security Software Discovery	Taint Shared Content	Third party Software	Standard Application Layer Protocol	Service Stop	Stored Data Manipulation
	Service Execution	Hypervisor	Winlogon Helper DLL	Scheduled Task	Exploitation of Vulnerability	System Information Discovery	Third party Software	Windows Admin Shares	Standard Application Layer Protocol	Service Stop	Stored Data Manipulation
	Third-party Software	Local Port Monitor	Winlogon Helper DLL	Service Registry Permissions Weakness	File Deletion	System Network Discovery	Windows Remote Management	Windows Admin Shares	Standard Application Layer Protocol	Service Stop	Stored Data Manipulation
	Trusted Developer Utilities	Login Scripts	Winlogon Helper DLL	File System Permissions Weakness	File System Logical Offsets	System Network Connections Discovery	Windows Remote Management	Windows Admin Shares	Standard Application Layer Protocol	Service Stop	Stored Data Manipulation
	Windows Management Instrumentation	Modify Existing Service	Winlogon Helper DLL	Web Shell	Hidden Files and Directories	System Owner/User Discovery	Windows Remote Management	Windows Admin Shares	Standard Application Layer Protocol	Service Stop	Stored Data Manipulation
	Windows Remote Management	Network Helper DLL	Winlogon Helper DLL	Indicator Blocking	Indicator Blocking	System Service Discovery	Windows Remote Management	Windows Admin Shares	Standard Application Layer Protocol	Service Stop	Stored Data Manipulation
	Windows Remote Management	New Service	Winlogon Helper DLL	Indicator Removal from Tools	Indicator Removal from Tools	System Time Discovery	Windows Remote Management	Windows Admin Shares	Standard Application Layer Protocol	Service Stop	Stored Data Manipulation
	Windows Remote Management	Office Application Startup	Winlogon Helper DLL	Indicator Removal on Host	Indicator Removal on Host	System Time Discovery	Windows Remote Management	Windows Admin Shares	Standard Application Layer Protocol	Service Stop	Stored Data Manipulation

..FOCUS ON EXECUTION

.. MISS COMMON ATTACKS AND BLAME END-USERS

ENDGAME.

MITRE ATT&CK Matrix

# WHY CURRENT STRATEGIES ARE NOT WORKING

- Inability to identify true gaps in defenses
  - Patchwork of one-off solutions
  - Outdated threat models
  - Lacking the ability to properly describe today's attacks



# ■ ATT&CK

## FRAMEWORK

## SECURITY

## BENEFITS

- Organizations can begin to optimize security program
  - Move from reactive to proactive defense postures
  - Expand defenses against other cells in the ATT&CK matrix to prepare against future attack vectors
  - Identify unknown security gaps -- verify defenses.



# IF YOU DO NOT KNOW WHERE TO BEGIN

- MITRE also offers a free open-source tool called [Navigator](#) to help organizations understand what areas of the Matrix should be prioritized.
- MITRE's [Groups](#) page provides an overview of attack groups and the industries they frequently target.



- **WITHOUT CONSIDERING YOUR ORGANIZATION'S OWN CONTEXT, ATT&CK IS JUST ANOTHER DATA-POINT**



# ATT&CK Detections?

*Will* be powerful

*Will* enable hunters

*Will* transform your SOC



# ATT&CK Detections?

*Will not* be as easy as described

*Will not* always lead to analytics

*Will not* be a silver bullet

# WHAT TO ASK A VENDOR

## 101 BASICS

Does prevention span the common attack vectors?

Do you provide FULL support across windows, MacOS, Linux?

Do you provide full protection, connected and disconnected?

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	EXFILTRATION	IMPACT		
Drive-by Compromise	Application Shimming	Accessibility Features	Path Interception	Accessibility Features	Access Token Manipulation	Install Root Certificate	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Command-Line	AppInit DLLs	Redundant Access	Access Token Manipulation	Binary Padding	InstallUtil	Brute Force	Application Window Discovery	Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
Hardware Additions	Interface Execution through API	Application Shimming	Registry Run Keys / Start Folder	AppInit DLLs	Bypass User Account Control	Masquerading	Create Account	File and Directory Discovery	Exploitation of Vulnerability	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Replication Through Removable Media	Execution through module load	Authentication Package	Scheduled Task	Application Shimming	Code Signing	Network Share Connection Removal	Credential Dumping	Network Service Scanning	Logon Script	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Spearfishing Attachment	Graphical User Interface	Bootkit	Security Support Provider	Bypass User Account Control	Component Firmware	Component Firmware	Credentials in Files	Network Service Scanning	Pass the Hash	Data from Local System	Custom Command and Control Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearfishing Link	InstallUtil	Change Default File Association	Shortcut Modification	DLL Injection	Component Object	NTFS Extended Attributes	Exploitation of Vulnerability	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Command and Control	Endpoint Denial of Service
Spearfishing via Service	PowerShell	Component Firmware	Service Registry Permissions Weakness	DLL Search Order Hijacking	Model Hijacking	Obfuscated Files or Information	Input Capture	Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Data Encoding	Firmware Corruption	Firmware Corruption
Supply Chain Compromise	Process Hollowing	Component Object Model Hijacking	System Firmware	Exploitation of Vulnerability	Deobfuscate/Decode Files or Information	Process Hollowing	Network Sniffing	Permission Groups Discovery	Remote File Copy	Data from Removable Media	Data Obfuscation	Inhibit System Recovery	Inhibit System Recovery
Trusted Relationship	Regsvcs/Regasm	Valid Accounts	Valid Accounts	DLL Search Order Hijacking	Redundant Access	Redundant Access	Private Keys	Process Discovery	Remote Services	Email Collection	Fallback Channels	Channel Exfiltration Over Other Network	Network Denial of Service
Valid Accounts	Regsvr32	External Remote Services	Windows Management Instrumentation Event Subscription	File System Permissions Weakness	DLL Search Order Hijacking	Regsvcs/Regasm	Two-Factor Authentication Interception	Query Registry	Replication Through Removable Media	Input Capture	Multi-Stage Channels	Medium Exfiltration Over Physical Medium	Resource Hijacking
	Rundll32	Windows Management Instrumentation Event Subscription	Local Port Monitor	DLL Search Order Hijacking	Regsvr32	Regsvr32	Two-Factor Authentication Interception	Query Registry Remote System Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels	Medium Exfiltration Over Physical Medium	Resource Hijacking
	Scheduled Task	File System Permissions Weaknesses	Winlogon Helper DLL	DLL Side-Loading	Regsvr32	Regsvr32	Two-Factor Authentication Interception	Query Registry Remote System Discovery	Shared Webroot	Video Capture	Multi-Stage Channels	Scheduled Transfer	Runtime Data Manipulation
	Scripting	Hidden Files and Directories	Path Interception	Disabling Security Tools	Rundll32	Rundll32	Two-Factor Authentication Interception	Query Registry Remote System Discovery	Taint Shared Content	Security Software Discovery	Third-party Software	Remote File Copy	Service Stop
	Service Execution	Hypervisor	Scheduled Task	Exploitation of Vulnerability	Scripting	Scripting	Two-Factor Authentication Interception	System Information Discovery	Windows Admin Shares	System Information Discovery	Windows Admin Shares	Standard Application Layer Protocol	Stored Data Manipulation
	Third-party Software	Local Port Monitor	Service Registry Permissions Weakness	File Deletion	Software Packing	Software Packing	Two-Factor Authentication Interception	System Network Discovery	Windows Remote Management	System Network Discovery	Windows Remote Management	Standard Cryptographic Protocol	Transmitted Data Manipulation
	Trusted Developer Utilities	Logon Scripts	Valid Accounts	File System Logical Offsets	Timestamp	Timestamp	Two-Factor Authentication Interception	System Network Connections Discovery	Standard Cryptographic Protocol	System Network Connections Discovery	Standard Cryptographic Protocol	Standard Cryptographic Protocol	Transmitted Data Manipulation
	Windows Management Instrumentation	Modify Existing Service	Web Shell	Hidden Files and Directories	Trusted Developer Utilities	Trusted Developer Utilities	Two-Factor Authentication Interception	System Owner/User Discovery	Standard Non-Application Layer Protocol	System Owner/User Discovery	Standard Non-Application Layer Protocol	Standard Non-Application Layer Protocol	Transmitted Data Manipulation
	Windows Remote Management	Netsh Helper DLL	Indicator Blocking	Indicator Blocking	Valid Accounts	Valid Accounts	Two-Factor Authentication Interception	System Service Discovery	Uncommonly Used Port	System Service Discovery	Uncommonly Used Port	Uncommonly Used Port	Transmitted Data Manipulation
		New Service	Indicator Removal from Tools	Indicator Removal from Tools	Indicator Blocking	Indicator Blocking	Two-Factor Authentication Interception	System Time Discovery	Web Service	System Time Discovery	Web Service	Web Service	Transmitted Data Manipulation
		Office Application Startup	Indicator Removal on Host	Indicator Removal on Host	Indicator Blocking	Indicator Blocking	Two-Factor Authentication Interception						Transmitted Data Manipulation

ENDGAME.



# WHAT TO ASK A VENDOR

## ADVANCED

Does prevention span the common attack vectors?

How can I translate detection to prevention?

How can I add my own detections and preventions?

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	EXFILTRATION	IMPACT		
Drive-by Compromise	Application Shimming	Accessibility Features	Path Interception	Accessibility Features	Access Token Manipulation	Install Root Certificate	Account Manipulation	Account Discovery	Application Deployment	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Command-Line	AppInit DLLs	Redundant Access	Access Token Manipulation	Binary Padding	InstallUtil	Brute Force	Application Window Discovery	Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
Hardware Additions	Interface Execution through API	Application Shimming	Registry Run Keys / Start Folder	AppInit DLLs	Bypass User Account Control	Masquerading	Create Account	File and Directory Discovery	Exploitation of Vulnerability	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Replication Through Removable Media	Execution through module load	Authentication Package	Scheduled Task	Application Shimming	Code Signing	Network Share Connection Removal	Credential Dumping	Network Service Scanning	Logon Script	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Spearfishing Attachment	Graphical User Interface	Bootkit	Security Support Provider	Bypass User Account Control	Component Firmware	NTFS Extended Attributes	Credentials in Files	Network Share	Pass the Hash	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearfishing Link	InstallUtil	Change Default File Association	Shortcut Modification	DLL Injection	Component Object	Exploitation of Vulnerability	Exploitation of Vulnerability	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control	Endpoint Denial of Service
Spearfishing via Service	PowerShell	Component Firmware	Service Registry Permissions Weakness	DLL Search Order Hijacking	Model Hijacking	Obfuscated Files or Information	Input Capture	Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Data Obfuscation	Channel Exfiltration Over Other Network	Firmware Corruption
Supply Chain Compromise	Process Hollowing	Component Object Model Hijacking	System Firmware	Exploitation of Vulnerability	Deobfuscate/Decode Files or Information	Process Hollowing	Network Sniffing	Permission Groups Discovery	Remote Services	Email Collection	Fallback Channels	Multi-Stage Channels	Inhibit System Recovery
Trusted Relationship	Regsvcs/Regasm	DLL Search Order Hijacking	Valid Accounts	File System Permissions Weakness	DLL Injection	Redundant Access	Private Keys	Process Discovery	Replication Through Removable Media	Input Capture	Multi-Stage Channels	Medium Exfiltration Over Physical Medium	Network Denial of Service
Valid Accounts	Regsvr32	External Remote Services	Web Shell	Local Port Monitor	File System Permissions Weakness	DLL Search Order Hijacking	Two-Factor Authentication Interception	Query Registry	Shared Webroot	Screen Capture	Multiband Communication	Scheduled Transfer	Resource Hijacking
	Rundll32	Windows Management Instrumentation Event Subscription	Winlogon Helper DLL	New Service	DLL Side-Loading	Regsvr32		Remote System Discovery	Taint Shared Content	Video Capture	Multilayer Encryption	Remote File Copy	Runtime Data Manipulation
	Scheduled Task	File System Permissions Weaknesses	Winlogon Helper DLL	Path Interception	Disabling Security Tools	Rundll32		Security Software Discovery	Third-party Software		Standard Application Layer Protocol		Service Stop
	Scripting	Hidden Files and Directories		Scheduled Task	Exploitation of Vulnerability	Scripting		System Information Discovery	Windows Admin Shares		Standard Application Layer Protocol		Stored Data Manipulation
	Service Execution	Hypervisor		Service Registry Permissions Weakness	File Deletion	Software Packing		System Network Discovery	Windows Remote Management		Standard Cryptographic Protocol		Transmitted Data Manipulation
	Third-party Software	Local Port Monitor		Valid Accounts	File System Logical Offsets	Timestamp		System Network Connections Discovery			Standard Non-Application Layer Protocol		
	Trusted Developer Utilities	Logon Scripts		Web Shell	Hidden Files and Directories	Trusted Developer Utilities		System Owner/User Discovery			Standard Non-Application Layer Protocol		
	Windows Management Instrumentation	Modify Existing Service			Indicator Blocking	Valid Accounts		System Service Discovery			Uncommonly Used Port		
	Windows Remote Management	Netsh Helper DLL			Indicator Removal from Tools			System Time Discovery			Web Service		
		New Service			Indicator Removal on Host								
		Office Application Startup											

ENDGAME.



**ENDGAME LEADS THE PACK IN  
REAL-TIME ALERT GENERATION ACROSS  
THE KILL CHAIN IN  
MITRE ATT&CK™**

**MITRE**

**Gartner**

 **virustotal**

**amtso**  
Anti-Malware Testing Standards Organization

 **SE Labs**



# ENDGAME.

## THANK YOU



ENDGAME



@ENDGAMEINC



ENDGAME.COM

How important is MITRE ATT&CK to your organization? Zero, growing, fundamental?