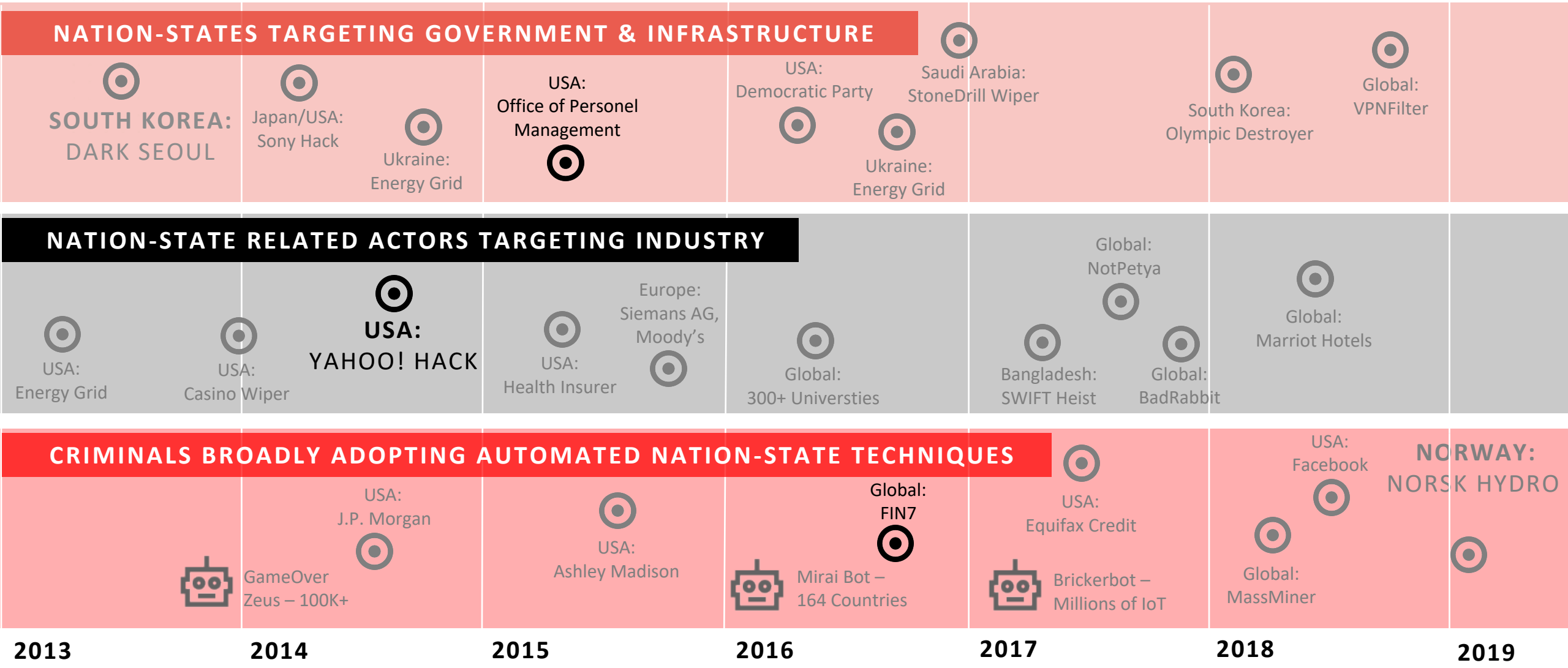
ENDGAME.

WHAT'S YOUR PLAN OF ATT&CK?

USING THE MITRE FRAMEWORK TO ASSESS AND

IMPROVE YOUR SECURITY MATURITY

THE RISE OF TARGETED ATTACKS



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

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

ENDGAME

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

MITRE ATT&CK Framework

- OPEN SOURCE 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	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	Exploitation of Vulnerability	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	Logon Script	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Replication Through Removable Media	Execution through module load	Authentication Package	Scheduled Task	Application Shimming	Code Signing	Modify Registry	Credential Dumping	Network Service Scanning	Pass the Hash	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	Network Share Connection Removal	Credentials in Files	Network Share Discovery	Pass the Ticket	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Link	InstallUtil	Change Default File Association	Shortcut Modification	DLL Injection	Component Object	NTFS Extended Attributes	Exploitation of Vulnerability	Peripheral Device Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Data Encoding	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	Obfuscated Files or Information	Input Capture	Permission Groups Discovery	Remote File Copy	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	Process Discovery	Remote Services	Email Collection	Fallback Channels	Medium Exfiltration Over Physical Medium	Inhibit System Recovery
Trusted Relationship	Regsvcs/Regasm	DLL Search Order Hijacking	Valid Accounts	File System Permissions Weakness	DLL Injection	Redundant Access	Private Keys	Query Registry Remote System Discovery	Replication Through Removable Media	Input Capture	Multi-Stage Channels	Scheduled Transfer	Network Denial of Service
Valid Accounts	Regsvr32	External Remote Services	Web Shell	Local Port Monitor	DLL Search Order Hijacking	Regsvcs/Regasm	Two-Factor Authentication Interception	Security Software Discovery	Shared Webroot	Screen Capture	Multiband Communication		Resource Hijacking
	Rundll32	File System Permissions Weaknesses	Windows Management Instrumentation Event Subscription	New Service	DLL Side-Loading	Regsvr32		System Information Discovery	Taint Shared Content	Video Capture	Multilayer Encryption		Runtime Data Manipulation
	Scheduled Task	Hidden Files and Directories	Winlogon Helper DLL	Path Interception	Disabling Security Tools	Rootkit		System Network Discovery	Third-party Software		Remote File Copy		Service Stop
	Scripting	Hypervisor		Scheduled Task	Exploitation of Vulnerability	Rundll32		System Network Connections Discovery	Windows Admin Shares		Standard Application Layer Protocol		Stored Data Manipulation
	Service Execution	Local Port Monitor		Service Registry Permissions Weakness	File Deletion	Scripting		System Owner/User Discovery	Windows Remote Management		Standard Cryptographic Protocol		Transmitted Data Manipulation
	Third-party Software	Logon Scripts		Valid Accounts	File System Logical Offsets	Software Packing		System Service Discovery			Standard Non-Application Layer Protocol		
	Trusted Developer Utilities	Modify Existing Service		Web Shell	Hidden Files and Directories	Timestomp		System Time Discovery			Uncommonly Used Port		
	Windows Management Instrumentation	Netsh Helper DLL			Indicator Blocking	Trusted Developer Utilities					Web Service		
	Windows Remote Management	New Service			Indicator Removal from Tools	Valid Accounts							
		Office Application Startup			Indicator Removal on Host								

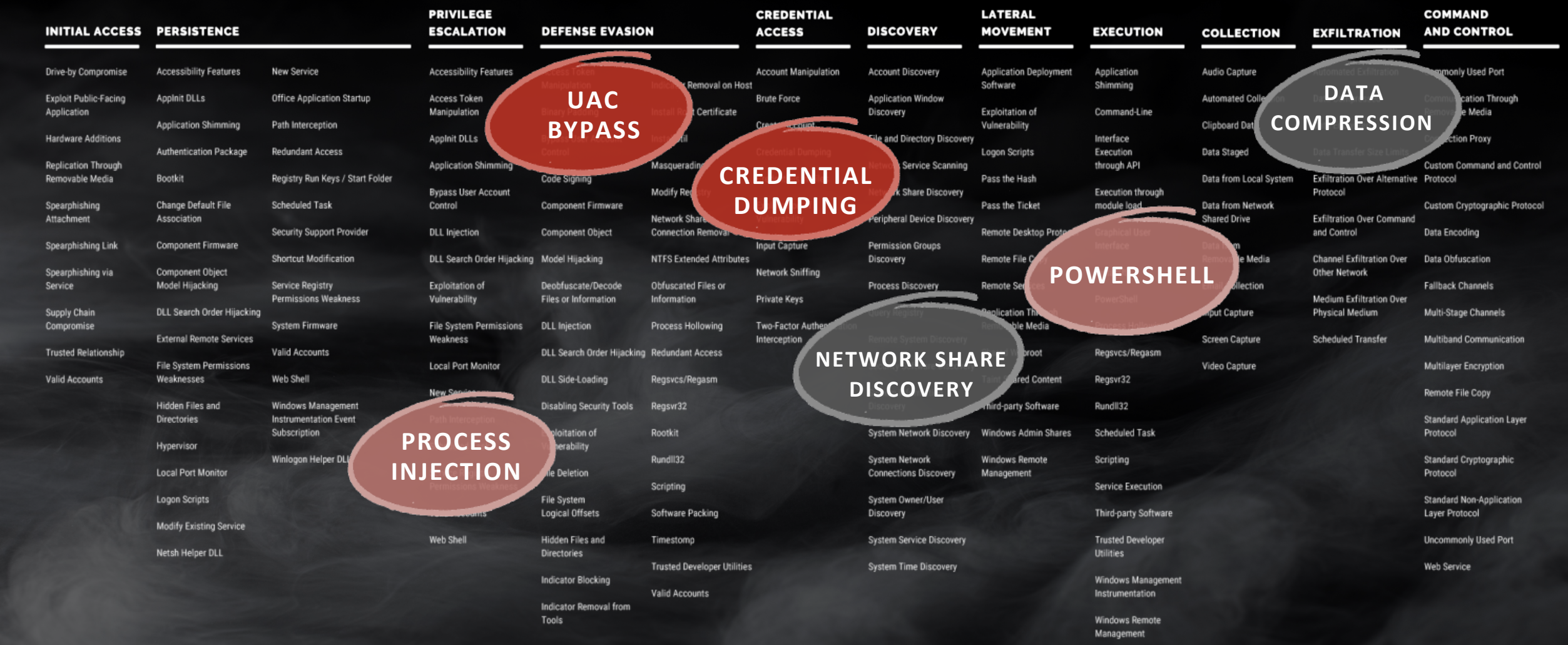
MITRE ATT&CK Matrix

USING THE MITRE FRAMEWORK TO ASSESS AND IMPROVE YOUR SECURITY MATURITY

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

- 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.

MITRE ATT&CK MATRIX



HTTPS://ATTACK.MITRE.ORG/

TODAY

SECURITY PROGRAMS

..FOCUS ON EXECUTION

.. MISS COMMON ATTACKS AND BLAME END-USERS

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	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	Exploitation of Vulnerability	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	Logon Script	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Replication Through Removable Media	Execution through module load	Authentication Package	Scheduled Task	Application Shimming	Code Signing	Modify Registry	Credential Dumping	Network Service Scanning	Pass the Hash	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	Network Share Connection Removal	Credentials in Files	Network Share Discovery	Pass the Ticket	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Link	InstallUtil	Change Default File Association	Shortcut Modification	DLL Injection	Component Object Model Hijacking	NTFS Extended Attributes	Exploitation of Vulnerability	Peripheral Device Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Data Encoding	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	Obfuscated Files or Information	Input Capture	Permission Groups Discovery	Remote File Copy	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	Process Discovery	Remote Services	Email Collection	Fallback Channels	Medium Exfiltration Over Physical Medium	Inhibit System Recovery
Trusted Relationship	Regsvcs/Regasm	DLL Search Order Hijacking	Valid Accounts	File System Permissions Weakness	DLL Injection	Redundant Access	Private Keys	Query Registry Remote System Discovery	Replication Through Removable Media	Input Capture	Multi-Stage Channels	Scheduled Transfer	Network Denial of Service
Valid Accounts	Regsvr32	External Remote Services	Windows Management Instrumentation Event Subscription	Local Port Monitor	DLL Search Order Hijacking	Regsvcs/Regasm	Two-Factor Authentication Interception	Security Software Discovery	Shared Webroot	Screen Capture	Multiband Communication		Resource Hijacking
	Rundll32	File System Permissions Weaknesses	Winlogon Helper DLL	New Service	DLL Side-Loading	Regsvr32		System Information Discovery	Taint Shared Content	Video Capture	Multilayer Encryption		Runtime Data Manipulation
	Scheduled Task	Hidden Files and Directories		Path Interception	Disabling Security Tools	Rootkit		System Network Discovery	Third-party Software		Remote File Copy		Service Stop
	Scripting	Hypervisor		Scheduled Task	Exploitation of Vulnerability	Rundll32		System Network Connections Discovery	Windows Admin Shares		Standard Application Layer Protocol		Stored Data Manipulation
	Service Execution	Local Port Monitor		Service Registry Permissions Weakness	File Deletion	Scripting		System Owner/User Discovery	Windows Remote Management		Standard Cryptographic Protocol		Transmitted Data Manipulation
	Third-party Software	Logon Scripts		Valid Accounts	File System Logical Offsets	Software Packing		System Service Discovery			Standard Non-Application Layer Protocol		
	Trusted Developer Utilities	Modify Existing Service		Web Shell	Hidden Files and Directories	Timestomp		System Time Discovery			Uncommonly Used Port		
	Windows Management Instrumentation	Netsh Helper DLL			Indicator Blocking	Trusted Developer Utilities					Web Service		
	Windows Remote Management	New Service			Indicator Removal from Tools	Valid Accounts							
		Office Application Startup			Indicator Removal on Host								

MITRE ATT&CK Matrix

ENDGAME.

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	Exploitation of Vulnerability	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	Logon Script	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Replication Through Removable Media	Execution through module load	Authentication Package	Scheduled Task	Application Shimming	Code Signing	Modify Registry	Credential Dumping	Network Service Scanning	Pass the Hash	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	Network Share Connection Removal	Credentials in Files	Network Share Discovery	Pass the Ticket	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Link	InstallUtil	Change Default File Association	Shortcut Modification	DLL Injection	Component Object	NTFS Extended Attributes	Exploitation of Vulnerability	Peripheral Device Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Data Encoding	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	Obfuscated Files or Information	Input Capture	Permission Groups Discovery	Remote File Copy	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	Process Discovery	Remote Services	Email Collection	Fallback Channels	Medium Exfiltration Over Physical Medium	Inhibit System Recovery
Trusted Relationship	Regsvcs/Regasm	DLL Search Order Hijacking	Valid Accounts	File System Permissions Weakness	DLL Injection	Redundant Access	Private Keys	Query Registry	Replication Through Removable Media	Input Capture	Multi-Stage Channels	Scheduled Transfer	Network Denial of Service
Valid Accounts	Regsvr32	External Remote Services	Web Shell	Local Port Monitor	DLL Search Order Hijacking	Regsvcs/Regasm	Two-Factor Authentication Interception	Remote System Discovery	Shared Webroot	Screen Capture	Multiband Communication		Resource Hijacking
	Rundll32	File System Permissions Weaknesses	Windows Management Instrumentation Event Subscription	New Service	DLL Side-Loading	Regsvr32		Security Software Discovery	Taint Shared Content	Video Capture	Multilayer Encryption Remote File Copy		Runtime Data Manipulation
	Scheduled Task	Hidden Files and Directories	Winlogon Helper DLL	Path Interception	Disabling Security Tools	Rootkit		System Information Discovery	Third-party Software		Standard Application Layer Protocol		Service Stop
	Scripting	Hypervisor		Scheduled Task	Exploitation of Vulnerability	Rundll32		System Network Discovery	Windows Admin Shares		Standard Cryptographic Protocol		Stored Data Manipulation
	Service Execution	Local Port Monitor		Service Registry Permissions Weakness	File Deletion	Scripting		System Network Connections Discovery	Windows Remote Management		Standard Non-Application Layer Protocol		Transmitted Data Manipulation
	Third-party Software	Logon Scripts		Valid Accounts	File System Logical Offsets	Software Packing		System Owner/User Discovery			Uncommonly Used Port		
	Trusted Developer Utilities	Modify Existing Service		Web Shell	Hidden Files and Directories	Timestomp		System Service Discovery			Web Service		
	Windows Management Instrumentation	Netsh Helper DLL			Indicator Blocking	Trusted Developer Utilities		System Time Discovery					
	Windows Remote Management	New Service			Indicator Removal from Tools	Valid Accounts							
		Office Application Startup			Indicator Removal on Host								

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 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	Exploitation of Vulnerability	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	Logon Script	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Replication Through Removable Media	Execution through module load	Authentication Package	Scheduled Task	Application Shimming	Code Signing	Modify Registry	Credential Dumping	Network Service Scanning	Pass the Hash	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	Network Share Connection Removal	Credentials in Files	Network Share Discovery	Pass the Ticket	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Link	InstallUtil	Change Default File Association	Shortcut Modification	DLL Injection	Component Object	NTFS Extended Attributes	Exploitation of Vulnerability	Peripheral Device Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Data Encoding	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	Obfuscated Files or Information	Input Capture	Permission Groups Discovery	Remote File Copy	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	Process Discovery	Remote Services	Email Collection	Fallback Channels	Medium Exfiltration Over Physical Medium	Inhibit System Recovery
Trusted Relationship	Regsvcs/Regasm	DLL Search Order Hijacking	Valid Accounts	File System Permissions Weakness	DLL Injection	Redundant Access	Private Keys	Query Registry	Replication Through Removable Media	Input Capture	Multi-Stage Channels	Scheduled Transfer	Network Denial of Service
Valid Accounts	Regsvr32	External Remote Services	Web Shell	Local Port Monitor	DLL Search Order Hijacking	Regsvcs/Regasm	Two-Factor Authentication Interception	Remote System Discovery	Shared Webroot	Screen Capture	Multiband Communication		Resource Hijacking
	Rundll32	File System Permissions Weaknesses	Windows Management Instrumentation Event Subscription	New Service	DLL Side-Loading	Regsvr32		Security Software Discovery	Taint Shared Content	Video Capture	Multilayer Encryption Remote File Copy		Runtime Data Manipulation
	Scheduled Task	Hidden Files and Directories	Winlogon Helper DLL	Path Interception	Disabling Security Tools	Rootkit		System Information Discovery	Third-party Software		Standard Application Layer Protocol		Service Stop
	Scripting	Hypervisor		Scheduled Task	Exploitation of Vulnerability	Rundll32		System Network Discovery	Windows Admin Shares		Standard Cryptographic Protocol		Stored Data Manipulation
	Service Execution	Local Port Monitor		Service Registry Permissions Weakness	File Deletion	Scripting		System Network Connections Discovery	Windows Remote Management		Standard Non-Application Layer Protocol		Transmitted Data Manipulation
	Third-party Software	Logon Scripts		Valid Accounts	File System Logical Offsets	Software Packing		System Owner/User Discovery			Uncommonly Used Port		
	Trusted Developer Utilities	Modify Existing Service		Web Shell	Hidden Files and Directories	Timestomp		System Service Discovery			Web Service		
	Windows Management Instrumentation	Netsh Helper DLL			Indicator Blocking	Trusted Developer Utilities		System Time Discovery					
	Windows Remote Management	New Service			Indicator Removal from Tools	Valid Accounts							
		Office Application Startup			Indicator Removal on Host								

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 ADVANCED ENDPOINT PROTECTION NSS RECOMMENDED AV comparatives

ENDGAME.

THANK YOU

 ENDGAME

 @ENDGAMEINC

 ENDGAME.COM

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