

All of this has happened
before. All of this will
happen again.

James Preston



How do threat actors make their way in?

Valid
Accounts

Exploit Public-
Facing
Application

External
Remote
Services

Phishing

Supply Chain
Compromise

What do they do next?

Use the command line or PowerShell to execute malware

Create Scheduled Tasks

Exploit vulnerable processes to obtain credentials

Perform network scans

Use remote control services to move within the network

To do this they will also need to..

Destroy logs

Use Slack as a
Command-and-
Control
mechanism

Use Google Drive
to exfiltrate data

But what are their goals?

Deny access
from
accounts

Encrypt or
destroy data

Deny access
to network
services

Inhibit System
Recovery

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/5)	Acquire Infrastructure (0/7)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/9)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits (0/1)	Data Destruction
Gather Victim Identity Information (0/4)	Compromise Infrastructure (0/7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Credentials from Password Stores (0/8)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/4)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/1)	Phishing (0/3)	Inter-Process Communication (0/3)	Browser Extensions	Boot or Logon Initialization Scripts (0/5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (0/3)	Clipboard Data	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/3)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forge Web Credentials	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/3)	Create Account (0/3)	Domain Policy Modification (0/2)	Deploy Container	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (0/4)	Event Triggered Execution (0/16)	Direct Volume Access	Modify Authentication Process (0/7)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Ingress Tool Transfer	Exfiltration Over Web Service (0/2)	Firmware Corruption
Search Open Websites/Domains (0/3)		Valid Accounts (0/4)	Shared Modules	Event Triggered Execution (0/16)	Escape to Host	Domain Policy Modification (0/2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Multi-Stage Channels	Scheduled Transfer	Inhibit System Recovery
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Multi-Factor Authentication Request Generation	File and Directory Discovery		Data from Local System	Non-Application Layer Protocol	Transfer Data to Cloud Account	Resource Hijacking
			System Services (0/2)	Hijack Execution Flow (0/12)	Hijack Execution Flow (0/12)	Exploitation for Defense Evasion	Network Sniffing	File and Directory Permissions Modification (0/2)		Data from Network Shared Drive	Non-Standard Port		Service Stop
			User Execution (0/3)	Implant Internal Image	Process Injection (0/12)	File and Directory Permissions Modification (0/2)	OS Credential Dumping (0/8)	Hide Artifacts (0/13)		Data from Removable Media	Protocol Tunneling		System Shutdown/Reboot
			Windows Management Instrumentation	Modify Authentication Process (0/7)	Scheduled Task/Job (0/3)	Indicator Removal (0/9)	Steal Application Access Token	Hijack Execution Flow (0/12)		Data Staged (0/2)	Proxy (0/4)		
				Office Application Startup (0/6)	Pre-OS Boot (0/3)	Indirect Command Execution	Steal or Forge Kerberos Tickets (0/4)	Impair Defenses (0/9)		Email Collection (0/3)	Remote Access Software		
				Pre-OS Boot (0/3)	Scheduled Task/Job (0/3)	Masquerading (0/7)	Steal or Forge Authentication Certificates	Impair Defenses (0/9)		Input Capture (0/4)	Traffic Signaling (0/2)		
				Scheduled Task/Job (0/3)	Server Software Component (0/4)	Modify Authentication Process (0/7)	Steal Web Session Cookie	Indicator Removal (0/9)		Screen Capture	Web Service (0/3)		
				Traffic Signaling (0/2)	Traffic Signaling (0/2)	Modify Cloud Compute Infrastructure (0/4)	Unsecured Credentials (0/7)	Execution Guardrails (0/1)		Video Capture			
				Valid Accounts (0/4)	Valid Accounts (0/4)	Modify Registry		Group Policy Discovery					
						Modify System Image (0/2)		File and Directory Discovery					
						Network Boundary Bridging (0/7)		File and Directory Discovery					
						Obfuscated Files or Information (0/3)		File and Directory Discovery					
						Plist File Modification		File and Directory Discovery					
						Pre-OS Boot (0/3)		File and Directory Discovery					
						Process Injection (0/12)		File and Directory Discovery					
						Reflective Code Loading		File and Directory Discovery					
						Rogue Domain Controller		File and Directory Discovery					
						Rootkit		File and Directory Discovery					
						Subvert Trust Controls (0/6)		File and Directory Discovery					
						System Binary Proxy Execution (0/13)		File and Directory Discovery					
						System Script Proxy Execution (0/1)		File and Directory Discovery					
						Template Injection		File and Directory Discovery					
						Traffic Signaling (0/2)		File and Directory Discovery					
						Trusted Developer Utilities Proxy Execution (0/1)		File and Directory Discovery					
						Unused/Unsupported Cloud Regions		File and Directory Discovery					
						Use Alternate Authentication Material (0/4)		File and Directory Discovery					
						Valid Accounts (0/4)		File and Directory Discovery					
						Virtualization/Sandbox Evasion (0/3)		File and Directory Discovery					
						Weaken Encryption (0/2)		File and Directory Discovery					

By the end of this presentation, you will:

- Understand how you can use the MITRE ATT&CK matrix to:
 - Establish your Cyber Security maturity.
 - Identify the areas to target for improvement first.
- Know how to check your likely exposure against emerging threats.
- Please hold questions to the end.

Who are MITRE?

- American non-profit.
- Research and development focused (including cyber security).
- Founded the Centre for Threat-Informed Defence, along with Microsoft, BAE Systems, IBM Security, and Centre for Internet Security.
- Big on using GitHub to publish software and receive feedback.

Tell me about ATT&CK...

- Selection of:
 - Tactics.
 - Techniques.
 - Procedures.
- To achieve an action on an objective.
- Linked to known attacks by known threat groups including:
 - CozyBear.
 - Deep Panda.
 - BlackOasis.

Tell me about ATT&CK...

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/3)	Acquire Infrastructure (0/7)	Drive-by Compromise	Command and Scripting Interpreter (0/6)	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Archive Collected Data (0/3)	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/14)	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Audio Capture	Audio Capture	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/5)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	BITS Jobs	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Automated Collection	Automated Collection	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/3)	Phishing (0/3)	Inter-Process Communication (0/3)	Browser Extensions	Boot or Logon Initialization Scripts (0/5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Browser Session Hijacking	Browser Session Hijacking	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/5)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forge Web Credentials	Cloud Service Discovery	Clipboard Data	Clipboard Data	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/5)	Create Account (0/3)	Domain Policy Modification (0/2)	Deploy Container	Input Capture (0/4)	Cloud Storage Object Discovery	Data from Cloud Storage	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)	Valid Accounts (0/4)	Trusted Relationship	Serverless Execution	Create or Modify System Process (0/4)	Escape to Host	Direct Volume Access	Multi-Factor Authentication Process (0/7)	Container and Resource Discovery	Data from Configuration Repository (0/2)	Data from Configuration Repository (0/2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (0/3)		Valid Accounts (0/4)	Shared Modules	Event Triggered Execution (0/16)	Event Triggered Execution (0/16)	Domain Policy Modification (0/2)	Multi-Factor Authentication Interception	Debugger Evasion	Data from Information Repositories (0/3)	Data from Information Repositories (0/3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Multi-Factor Authentication Request Generation	Domain Trust Discovery	Data from Local System	Data from Local System	Non-Application Layer Protocol	Resource Hijacking	Network Denial of Service (0/2)
			System Services (0/2)	Hijack Execution Flow (0/12)	File and Directory Permissions Modification (0/2)	Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery	Data from Network Shared Drive	Data from Network Shared Drive	Protocol Tunneling	Service Stop	System Shutdown/Reboot
			User Execution (0/3)	Implant Internal Image	Hide Artifacts (0/10)	File and Directory Permissions Modification (0/2)	OS Credential Dumping (0/4)	Group Policy Discovery	Data from Removable Media	Data from Removable Media	Proxy (0/4)		
			Windows Management Instrumentation	Modify Authentication Process (0/7)	Hijack Execution Flow (0/12)	Hide Artifacts (0/10)	Steal Application Access Token	Network Service Discovery	Data Staged (0/2)	Data Staged (0/2)	Remote Access Software		
				Scheduled Task/Job (0/5)	Impair Defenses (0/3)	Hijack Execution Flow (0/12)	Steal or Forge Authentication Certificates	Network Share Discovery	Email Collection (0/3)	Email Collection (0/3)	Traffic Signaling (0/2)		
				Office Application Startup (0/16)	Indicator Removal (0/5)	Impair Defenses (0/3)	Steal or Forge Kerberos Tickets (0/4)	Network Sniffing	Input Capture (0/4)	Input Capture (0/4)	Web Service (0/3)		
				Pre-OS Boot (0/5)	Indirect Command Execution	Masquerading (0/2)	Steal Web Session Cookie	Network Sniffing	Screen Capture	Screen Capture			
				Scheduled Task/Job (0/5)	Masquerading (0/2)	Masquerading (0/2)	Unsecured Credentials (0/7)	OS Credential Dumping (0/4)	Video Capture	Video Capture			
				Server Software Component (0/5)	Modify Authentication Process (0/7)	Masquerading (0/2)		Steal Application Access Token					
				Traffic Signaling (0/2)	Modify Cloud Compute Infrastructure (0/4)	Modify Authentication Process (0/7)		Steal or Forge Kerberos Tickets (0/4)					
				Valid Accounts (0/4)	Modify Registry	Modify Cloud Compute Infrastructure (0/4)		Steal Web Session Cookie					
					Modify System Image (0/2)	Modify Registry		Unsecured Credentials (0/7)					
					Network Boundary Bridging (0/1)	Modify System Image (0/2)							
					Obfuscated Files or Information (0/5)	Network Boundary Bridging (0/1)							
					Plist File Modification	Obfuscated Files or Information (0/5)							
					Pre-OS Boot (0/5)	Plist File Modification							
					Process Injection (0/12)	Pre-OS Boot (0/5)							
					Reflective Code Loading	Process Injection (0/12)							
					Rogue Domain Controller	Reflective Code Loading							
					Rootkit	Rogue Domain Controller							
					Subvert Trust Controls (0/4)	Rootkit							
					System Binary Proxy Execution (0/13)	Subvert Trust Controls (0/4)							
					System Script Proxy Execution (0/1)	System Binary Proxy Execution (0/13)							
					Template Injection	System Script Proxy Execution (0/1)							
					Traffic Signaling (0/2)	Template Injection							
					Trusted Developer Utilities Proxy Execution (0/3)	Traffic Signaling (0/2)							
					Unused/Unsupported Cloud Regions	Trusted Developer Utilities Proxy Execution (0/3)							
					Use Alternate Authentication Material (0/4)	Unused/Unsupported Cloud Regions							
					Valid Accounts (0/4)	Use Alternate Authentication Material (0/4)							
					Virtualization/Sandbox Evasion (0/3)	Valid Accounts (0/4)							
					Weaken Encryption (0/2)	Virtualization/Sandbox Evasion (0/3)							
						Weaken Encryption (0/2)							

ATT&CK navigator

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques
Active Scanning <small>(0/3)</small>	Acquire Infrastructure <small>(0/7)</small>	Drive-by Compromise	Command and Scripting Interpreter <small>(0/3)</small>	Account Manipulation <small>(0/5)</small>
Gather Victim Host Information <small>(0/4)</small>	Compromise Accounts <small>(0/3)</small>	Exploit Public-Facing Application	Container Administration Command	BITS Jobs
Gather Victim Identity Information <small>(0/3)</small>	Compromise Infrastructure <small>(0/7)</small>	External Remote Services	Deploy Container	Boot or Logon Autostart Execution <small>(0/14)</small>
Gather Victim Network Information <small>(0/6)</small>	Develop Capabilities <small>(0/4)</small>	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts <small>(0/5)</small>
Gather Victim Org Information <small>(0/4)</small>	Establish			

ATT&CK navigator

Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques
Abuse Elevation Control Mechanism <small>(0/4)</small>	Abuse Elevation Control Mechanism <small>(0/4)</small>	Adversary-in-the-Middle <small>(0/3)</small>	Account Discovery <small>(0/4)</small>	Exploitation of Remote Services
Access Token Manipulation <small>(0/5)</small>	Access Token Manipulation <small>(0/5)</small>	Brute Force <small>(0/4)</small>	Application Window Discovery	Internal Spearphishing
Boot or Logon Autostart Execution <small>(0/14)</small>	BITS Jobs	Credentials from Password Stores <small>(0/5)</small>	Browser Bookmark Discovery	Lateral Tool Transfer
Boot or Logon Initialization	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking <small>(0/1)</small>
	Debugger Evasion		Cloud Service Dashboard	
	Deobfuscate/Decode			

ATT&CK navigator

Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Adversary-in-the-Middle <small>(0/3)</small>	Application Layer Protocol <small>(0/4)</small>	Automated Exfiltration <small>(0/1)</small>	Account Access Removal
Archive Collected Data <small>(0/3)</small>	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Audio Capture	Data Encoding <small>(0/2)</small>	Exfiltration Over Alternative Protocol <small>(0/3)</small>	Data Encrypted for Impact
Automated Collection	Data Obfuscation <small>(0/3)</small>	Exfiltration Over C2 Channel	Data Manipulation <small>(0/3)</small>
Browser Session Hijacking		Exfiltration Over	Defacement <small>(0/2)</small>
			Disk Wipe

Mobile devices

Initial Access 4 techniques	Execution 3 techniques	Persistence 7 techniques	Privilege Escalation 3 techniques	Defense Evasion 14 techniques	Credential Access 5 techniques	Discovery 8 techniques	Lateral Movement 2 techniques	Collection 13 techniques	Command and Control 8 techniques	Exfiltration 2 techniques	Impact 9 techniques
Drive-By Compromise	Command and Scripting Interpreter (0/1) Native API Scheduled Task/Job	Boot or Logon Initialization Scripts Compromise Application Executable Compromise Client Software Binary Event Triggered Execution (0/1) Foreground Persistence Hijack Execution Flow (0/1) Scheduled Task/Job	Abuse Elevation Control Mechanism (0/1) Exploitation for Privilege Escalation Process Injection (0/1)	Download New Code at Runtime	Access Notifications	File and Directory Discovery	Exploitation of Remote Services	Access Notifications	Application Layer Protocol (0/1)	Exfiltration Over Alternative Protocol (0/1) Exfiltration Over C2 Channel	Account Access Removal
Lockscreen Bypass				Execution Guardrails (0/1)	Clipboard Data	Location Tracking (0/2)		Replication Through Removable Media	Adversary-in-the-Middle		Call Control
Replication Through Removable Media				Foreground Persistence	Credentials from Password Store (0/1)	Network Service Scanning	Archive Collected Data	Dynamic Resolution (0/1)	Data Encrypted for Impact		
Supply Chain Compromise (0/3)				Hide Artifacts (0/2)	Input Capture (0/2)	Process Discovery				Encrypted Channel (0/2)	Data Manipulation (0/1)
				Hooking	Steal Application Access Token (0/1)	Software Discovery (0/1)		Audio Capture	Ingress Tool Transfer		Data Denial of Service
				Impair Defenses (0/3)		System Information Discovery		Call Control	Non-Standard Port		Endpoint Denial of Service
				Indicator Removal on Host (0/3)		System Network Configuration Discovery		Clipboard Data	Out of Band Data		Generate Traffic from Victim
				Input Injection		System Network Connections Discovery		Data from Local System	Web Service (0/3)		Input Injection
				Native API				Input Capture (0/2)			Network Denial of Service
				Obfuscated Files or Information (0/2)				Location Tracking (0/2)			SMS Control
				Process Injection (0/1)				Protected User Data (0/4)			
				Proxy Through Victim				Screen Capture			
				Subvert Trust Controls (0/1)				Stored Application Data			
				Virtualization/Sandbox Evasion (0/1)				Video Capture			

Industrial Control Systems

Initial Access 12 techniques	Execution 9 techniques	Persistence 6 techniques	Privilege Escalation 2 techniques	Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 7 techniques	Collection 10 techniques	Command and Control 3 techniques	Inhibit Response Function 13 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Detect Operating Mode		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware	Rootkit	Spoof Reporting Message	Wireless Sniffing	Program Download		I/O Image		Block Serial COM	Unauthorized Command Message
Remote Services	Modify Controller Tasking	Valid Accounts				Remote Services	Valid Accounts			Monitor Process State	Data Destruction
Replication Through Removable Media	Native API					Point & Tag Identification	Program Upload	Device Restart/Shutdown	Denial of Service	Loss of Safety	
Rogue Master	Scripting					Screen Capture	Screen Capture	Manipulate I/O Image	Block Reporting Message	Loss of View	
Spearphishing Attachment	User Execution					Wireless Sniffing	Wireless Sniffing	Modify Alarm Settings	Block Reporting Message	Manipulation of Control	
Supply Chain Compromise								Rootkit	Block Reporting Message	Manipulation of View	
Transient Cyber Asset								Service Stop	Block Reporting Message	Theft of Operational Information	
Wireless Compromise								System Firmware	Block Reporting Message		

Filter to specific platforms

Initial Access 3 techniques	Execution 1 techniques	Persistence 6 techniques	Privilege Escalation 3 techniques	Defense Evasion 7 techniques	Credential Access 8 techniques	Discovery 5 techniques	Lateral Movement 3 techniques	Collection 2 techniques	Impact 3 techniques
Phishing <small>(0/1)</small>	Serverless Execution	Account Manipulation <small>(0/4)</small>	Domain Policy Modification <small>(0/1)</small>	Domain Policy Modification <small>(0/1)</small>	Brute Force <small>(0/4)</small>	Account Discovery <small>(0/2)</small>	Internal Spearphishing	Data from Information Repositories <small>(0/1)</small>	Account Access Removal
Trusted Relationship		Create Account <small>(0/1)</small>	Event Triggered Execution <small>(0/0)</small>	Hide Artifacts <small>(0/1)</small>	Forge Web Credentials <small>(0/1)</small>	Cloud Service Dashboard	Taint Shared Content	Email Collection <small>(0/2)</small>	Endpoint Denial of Service <small>(0/3)</small>
Valid Accounts <small>(0/2)</small>		Event Triggered Execution <small>(0/0)</small>	Valid Accounts <small>(0/2)</small>	Impair Defenses <small>(0/0)</small>	Modify Authentication Process <small>(0/2)</small>	Cloud Service Discovery	Use Alternate Authentication Material <small>(0/2)</small>		Network Denial of Service <small>(0/3)</small>
		Modify Authentication Process <small>(0/2)</small>		Indicator Removal <small>(0/1)</small>	Multi-Factor Authentication Request Generation	Permission Groups Discovery <small>(0/1)</small>			Network Denial of Service <small>(0/2)</small>
		Office Application Startup <small>(0/6)</small>		Modify Authentication Process <small>(0/2)</small>	Steal Application Access Token	Software Discovery <small>(0/1)</small>			
		Valid Accounts <small>(0/2)</small>		Use Alternate Authentication Material <small>(0/2)</small>	Steal or Forge Authentication Certificates				
			Valid Accounts <small>(0/2)</small>	Steal Web Session Cookie					
				Unsecured Credentials <small>(0/0)</small>					

platforms

- Linux
- macOS
- Windows
- Network
- PRE
- Containers
- Office 365
- SaaS
- Google Workspace
- IaaS
- Azure AD

ATT&CK navigator

<https://mitre-attack.github.io/attack-navigator/>

MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

[help](#) [changelog](#) [themes](#)

dark

light

use system

Create a new empty layer

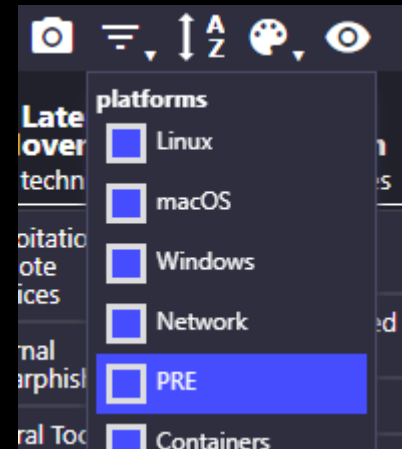
Load a layer from your computer

Create New Layer

Create a new e

Enterprise

More Options



ATT&CK navigator

Initial Access 9 techniques	Execution 13 techniques
Drive-by Compromise	Drive-by Compromise (T1189) Interpreter pin/unpin tooltip Container Administration Command select add to selection Deploy Container remove from selection
Exploit Public-Facing Application	
External Remote Services	
Hardware Additions	
Phishing (0/3)	select all Execution deselect all
Replication Through Removable Media	invert selection Communication select annotated Native API select unannotated
Supply Chain Compromise (0/3)	select all techniques in tactic Execution
Trusted Relationship	deselect all techniques in tactic Business Execution
Valid Accounts (0/4)	view technique view tactic Deployment Tools

Drive-by Compromise

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring Application Access Token.

Multiple ways of delivering exploit code to a browser exist, including:

- A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting.
- Malicious ads are paid for and served through legitimate ad providers.
- Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.^[1]

ID: T1189

Sub-techniques: No sub-techniques

① Tactic: Initial Access

① Platforms: Linux, SaaS, Windows, macOS

① Permissions Required: User

Contributors: Jeff Sakowicz, Microsoft Identity Developer Platform Services (IDPM Services); Saisha Agrawal, Microsoft Threat Intelligent Center (MSTIC)

Version: 1.4

Created: 18 April 2018

Last Modified: 08 March 2022

[Version Permalink](#)

The detail

Typical drive-by compromise process:

1. A user visits a website that is used to host the adversary controlled content.
2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version.
 - The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes.
3. Upon finding a vulnerable version, exploit code is delivered to the browser.
4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place.
 - In some cases a second visit to the website after the initial scan is required before exploit code is delivered.

The detail

Procedure Examples

ID	Name	Description
G0138	Andariel	Andariel has used watering hole attacks, often with zero-day exploits, to gain initial access to victims within a specific IP range. ^{[3][4]}
G0073	APT19	APT19 performed a watering hole attack on forbes.com in 2014 to compromise targets. ^[5]
G0007	APT28	APT28 has compromised targets via strategic web compromise utilizing custom exploit kits. ^[6]
G0050	APT32	APT32 has infected victims by tricking them into visiting compromised watering hole websites. ^{[7][8]}
G0067	APT37	APT37 has used strategic web compromises, particularly of South Korean websites, to distribute malware. The group has also used torrent file-sharing sites to more indiscriminately disseminate malware to victims. As part of their compromises, the group has used a Javascript based profiler called RICECURRY to profile a victim's web browser and deliver malicious code accordingly. ^{[9][10][11]}
G0082	APT38	APT38 has conducted watering holes schemes to gain initial access to victims. ^{[12][13]}
G0001	Axiom	Axiom has used watering hole attacks to gain access. ^[14]
S0606	Bad Rabbit	Bad Rabbit spread through watering holes on popular sites by injecting JavaScript into the HTML body or a <code>.js</code> file. ^{[15][16]}

The detail

Mitigations

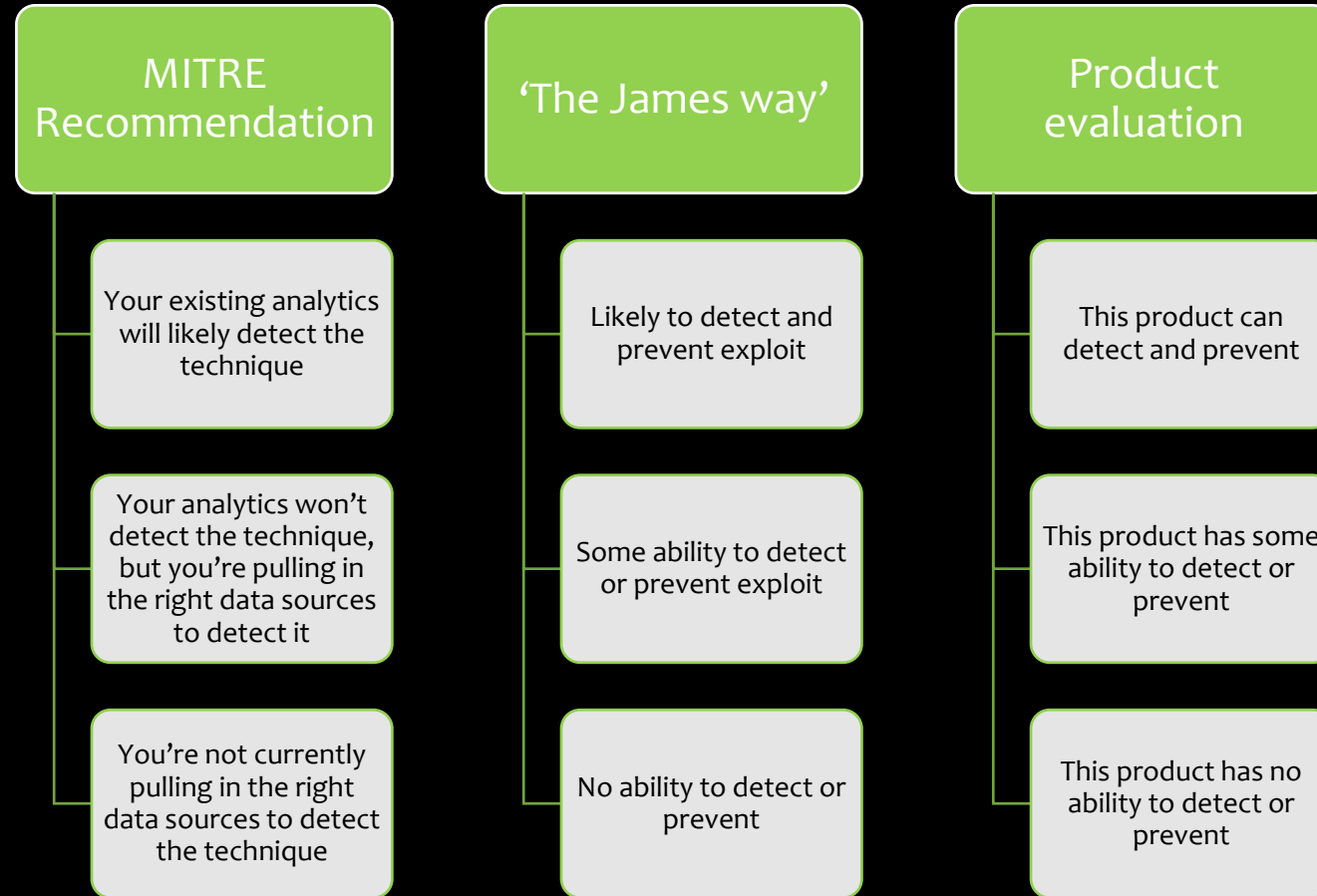
ID	Mitigation	Description
M1048	Application Isolation and Sandboxing	<p>Browser sandboxes can be used to mitigate some of the impact of exploitation, but sandbox escapes may still exist.^{[58][59]}</p> <p>Other types of virtualization and application microsegmentation may also mitigate the impact of client-side exploitation. The risks of additional exploits and weaknesses in implementation may still exist for these types of systems.^[59]</p>
M1050	Exploit Protection	<p>Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior.^[60] Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring.^[61] Many of these protections depend on the architecture and target application binary for compatibility.</p>
M1021	Restrict Web-Based Content	<p>For malicious code served up through ads, adblockers can help prevent that code from executing in the first place.</p> <p>Script blocking extensions can help prevent the execution of JavaScript that may commonly be used during the exploitation process.</p>
M1051	Update Software	<p>Ensure all browsers and plugins kept updated can help prevent the exploit phase of this technique. Use modern browsers with security features turned on.</p>

The detail

Detection

ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Firewalls and proxies can inspect URLs for potentially known-bad domains or parameters. They can also do reputation-based analytics on websites and their requested resources such as how old a domain is, who it's registered to, if it's on a known bad list, or how many other users have connected to it before.
DS0022	File	File Creation	Monitor for newly constructed files written to disk to gain access to a system through a user visiting a website over the normal course of browsing.
DS0029	Network Traffic	Network Connection Creation	Monitor for newly constructed network connections to untrusted hosts that are used to send or receive data.
		Network Traffic Content	Monitor for other unusual network traffic that may indicate additional tools transferred to the system. Use network intrusion detection systems, sometimes with SSL/TLS inspection, to look for known malicious scripts (recon, heap spray, and browser identification scripts have been frequently reused), common script obfuscation, and exploit code.
DS0009	Process	Process Creation	Look for behaviors on the endpoint system that might indicate successful compromise, such as abnormal behaviors of browser processes. This could include suspicious files written to disk, evidence of Process Injection for attempts to hide execution, or evidence of Discovery .

Paint by numbers



Some techniques have no known method to detect or prevent exploit!

ATT&CK navigator

The screenshot shows the configuration panel for the ATT&CK Navigator. It includes a 'Tactic Row Background' section with a 'show' checkbox and a color picker set to #dddddd. Below is the 'Scoring Gradient' section, which features a vertical color gradient bar. The 'Low value' is set to 1 and the 'High value' is set to 3. Three color swatches are visible: red (#ff6666), yellow (#ffe766), and green (#8ec843), each with a 'remove' button. An 'add another color' button is also present, along with a 'presets' dropdown menu.



The screenshot shows a technique control for 'Exfiltration of Sensitive Information'. It includes a 'technique controls' section with icons for a pattern, a brush, a bar chart, a speech bubble, and a refresh icon. Below the icons, the text 'and Exfiltration of Sensitive Information' is visible, along with a 'score' field set to 1 and a '9 techniques' label.

Initial Access

9 techniques

Drive-by
Compromise

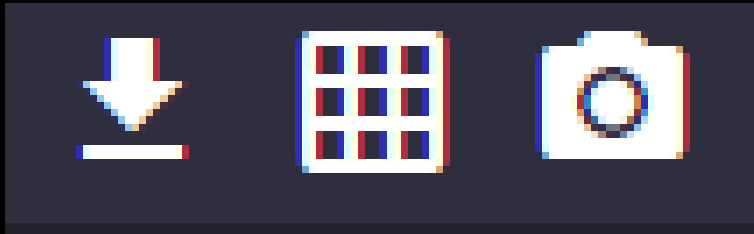
Initial Access

9 techniques

Drive-by
Compromise



Export options



in [grid icon] [arrow icon] [list icon] [eye icon] [download icon]

- show header
- show about
- show domain
- show filters
- show legend
- show gradient score
- sub-techniques
- show expanded
- cell border

Print

Copies: 1

Printer Printer Properties

Microsoft Print to PDF
Ready

Settings

Print Active Sheets
Only print the active sheets

Pages: [] to []

Collated
1,2,3 1,2,3 1,2,3

Landscape Orientation

A3
29.7 cm x 42 cm

Narrow Margins
Top: 1.91 cm Bottom: 1.91 cm...

Fit Sheet on One Page
Shrink the printout so that it...

Page Setup

Initial Access	Execution	Permissions	Privilege Escalation	Defense Evasion	Credential Access
Application Through Removable Media	Inter-Process Communication	Disable/Modify System Process	Abuse Execution Control Mechanism	Abuse Execution Control Mechanism	Credentials from Password Stores
External Remote Services	Windows Management Instrumentation	HiJack Execution Flow	Disable/Modify System Process	HiJack Execution Flow	Modify Authentication Process
Hardware Additions	Native API	Modify Authentication Process	HiJack Execution Flow	Modify Authentication Process	Account Hijacking
Phishing	Shared Modules	Office Application Startup	Process Injection	Modify Registry	Brute Force
Trusted Relationship	System Services	Pre-OS Boot	Exploitation for Privilege Escalation	Modify System Image	Network Sniffing
Drive-by Compromise	User Interaction	Account Manipulation	Access Token Manipulation	Obfuscated Files or Information	Adversary-in-the-Middle
Exploit Public-Facing Application	Command and Scripting Interpreter	Create Account	Domain Policy Modification	Pre-OS Boot	Exploitation for Credential Access
Supply Chain Compromise	Exploitation for Client Execution	External Remote Services	Scheduled Task/Job	Process Injection	Forced Authentication
Valid Accounts	Scheduled Task/Job	BITS Jobs	Valid Accounts	Subvert Trust Controls	OS Credential Dumping
	Container Administration Command	Browser Extensions	Boot or Logon Autostart Execution	Template Injection	Snarf or Forge Kerberos Tickets
	Deploy Container	Compromise Client Software Binary	Boot or Logon Initialization Scripts	Use Alternate Authentication Material	Unsecured Credentials
	Software Deployment Task	Scheduled Task/Job	Escape to Host	Signed Binary Proxy Execution	Forge Web Credentials
		Traffic Signaling	Event Triggered Execution	Access Token Manipulation	Input Capture
		Valid Accounts	Boot or Logon Autostart Execution	BITS Jobs	Shell Application Access To Token
		Boot or Logon Autostart Execution	Domain Policy Modification	Shell Web Session Cookie	Group Policy
		Boot or Logon Initialization Scripts	Exploitation for Defense Evasion		Peripheral Discovery
		Event Triggered Execution	File and Directory Permissions Modification		Permissions
		Impersonate Image	Impersonate Services		Process Discovery
		Server Software Component	Manipulating Network Boundaries		Query Remote System
			Signed Script Proxy Execution		Software Discovery
			Traffic Signaling		System Information
			Trusted Developer Utilities Proxy Execution		System Location
			Valid Accounts		System Network Discovery
			Weaken Encryption		System Network Discovery
			XSL Script Processing		System Operating System
			Build Image on Host		System Security
			(Deobfuscate)/Decode Files or Information		System Time
			Deploy Container		Virtualization
			Direct Volume Access		
			Execution Guardrails		
			Hide Artifacts		
			Indicators Removal on Host		
			Install/Uninstall Command Execution		
			Modify Cloud Compute Infrastructure		
			Reflective Code Loading		
			Regulate Domain Controller Behavior		
			Unusual/Unapproved Cloud Regions		
			Virtualization/Sandbox Evasion		

Map to threat groups

Threat Report 24th February 2023

The NCSC's threat report is drawn from recent open source reporting.



CYBERSECURITY ADVISORY

#StopRansomware: Royal Ransomware

Release Date: March 02, 2023

Alert Code: AA23-061A

EU agencies warn of malicious cyber activities by APT groups

The European Union Agency for Cybersecurity (ENISA) and Computer Emergency Response Team (CERT-EU) jointly published an alert last week about sustained cyber activity by specific threat actors.

The publication warned that the threat groups **APT27, APT30, APT31, Ke3chang, Gallium and Mustang Panda** had been observed targeting business and governments in the EU, with recent activity focused on information theft, primarily via establishing persistent footholds within networks.

Initial Access

Royal actors gain initial access to victim networks in a number of ways including:

- **Phishing.** According to third-party reporting, Royal actors most commonly (in 66.7% of incidents) gain initial access to victim networks via successful phishing emails **[T1566-01]**.
 - According to open-source reporting, victims have unknowingly installed malware that delivers Royal ransomware after receiving phishing emails containing malicious PDF documents **[T1566.001-01]** and malvertising **[T1566.002-01]** [2]
- **Remote Desktop Protocol (RDP).** The second most common vector Royal actors use (in 13.3% of incidents) for initial access is RDP compromise.
- **Public-facing applications.** FBI has also observed Royal actors gain initial access through exploiting public-facing applications **[T1190-01]**.
- **Brokers.** Reports from trusted third-party sources indicate that Royal actors may leverage brokers to gain initial access and source traffic by harvesting virtual private network (VPN) credentials from stealer logs.

Map to threat groups

selection controls

layer controls

select techniques across tactics

select sub-techniques with parent

selection controls

Techniques (566)

Abuse Elevation Control Mechanism	view	<input type="button" value="select"/>	<input type="button" value="deselect"/>
Abuse Elevation Control Mechanism : Bypass User Account Control	view	<input type="button" value="select"/>	<input type="button" value="deselect"/>
Abuse Elevation Control Mechanism : Elevated Execution	view	<input type="button" value="select"/>	<input type="button" value="deselect"/>

technique controls

selection controls

Threat Groups (128)

Cinnara	view	<input type="button" value="select"/>	<input type="button" value="deselect"/>
Cicaver	view	<input type="button" value="select"/>	<input type="button" value="deselect"/>
Cobalt Group	view	<input type="button" value="select"/>	<input type="button" value="deselect"/>
CopyKittens	view	<input type="button" value="select"/>	<input type="button" value="deselect"/>
CostaRicto	view	<input type="button" value="select"/>	<input type="button" value="deselect"/>
Dark Coreol	view	<input type="button" value="select"/>	<input type="button" value="deselect"/>

technique controls

layer controls

Map to threat groups

Initial Access 2 techniques	Execution 5 techniques	Persistence 4 techniques	Privilege Escalation 7 techniques	Defense Evasion 6 techniques	Discovery 2 techniques	Lateral Movement 1 techniques	Command and Control 5 techniques
<ul style="list-style-type: none"> Phishing (0/3) Supply Chain Compromise (0/3) 	<ul style="list-style-type: none"> Inter-Process Communication (0/2) User Execution (0/3) Command and Scripting Interpreter (0/8) Exploitation for Client Execution Scheduled Task/Job (0/6) 	<ul style="list-style-type: none"> Create or Modify System Process (0/4) Scheduled Task/Job (0/6) Boot or Logon Autostart Execution (0/15) Boot or Logon Initialization Scripts (0/5) 	<ul style="list-style-type: none"> Abuse Elevation Control Mechanism (0/4) Create or Modify System Process (0/4) Process Injection (0/11) Exploitation for Privilege Escalation Scheduled Task/Job (0/6) Boot or Logon Autostart Execution (0/15) Boot or Logon Initialization Scripts (0/5) 	<ul style="list-style-type: none"> Abuse Elevation Control Mechanism (0/4) Obfuscated Files or Information (0/6) Process Injection (0/11) Signed Binary Proxy Execution (0/13) XSL Script Processing Indicator Removal on Host (0/6) 	<ul style="list-style-type: none"> Network Service Scanning Software Discovery (0/1) 	<ul style="list-style-type: none"> Remote Services (0/6) 	<ul style="list-style-type: none"> Application Layer Protocol (0/4) Encrypted Channel (0/2) Ingress Tool Transfer Protocol Tunneling Remote Access Software

Case study!

The screenshot shows the YouTube channel page for LinusTechTipsTemp (@temporaryhandle). The channel has 15.3M subscribers and 4.9K videos. The page features a navigation menu with options like HOME, VIDEOS, SHORTS, LIVE, PLAYLISTS, COMMUNITY, CHANNELS, and ABOUT. Under the 'LIVE' section, there are two live streams: 'OpenAI GPT-4: The Game-Changing AI Technology' (756 watching) and 'LinusTechTips & Elon Musk Special Crypto Giveaway!' (829 watching). Below the live streams, there is a section for 'Our members' and a 'Videos' section with a 'Play all' button. The video thumbnails include 'Tech Talk Pilot Episode NCIX & Hardware Canucks' (12K views), 'Cyclone vs Stock Cooler.wmv', 'Joe Rocket Ballistic Jacket & Pants Unboxing.wmv', 'Call of Duty Modern Warfare 2 Eyefinity.wmv', '600T.wmv', and 'Testing.wmv'. At the bottom, there is a section for 'As Fast As Possible' with a 'Play all' button and a row of video thumbnails.



My Channel Was Deleted Last Night

Linus Tech Tips ✓ 506K views • 3 hours ago

Thanks to dbrand for sponsoring this video! Use code FIVEFOOTONE at <http://shortlinus.com> for 15% off everything site wide. Discuss on the forum: <https://linustechtips.com/topic/1496158-my-chann...>

The screenshot shows a tweet from the user @I_AM_T3X. The tweet text reads: 'Yo @LinusTech @linusgsebastian @Brandon_Y_Lee @luke_lafr LTT GOT HACKED, IT IS CURRENTLY LIVES STREAMING ELON'. The tweet is dated 6:14 AM · Mar 23, 2023 and has 107 views. Below the tweet are interaction icons for reply, retweet, like, and share, along with a 'Promote' button. A reply from the same user is visible below, stating: 'Replying to @I_AM_T3X @TeamYouTube'. The reply also has interaction icons and a '10' view count.

Case study!

Initial Access

3 techniques

Exploit Public-Facing Application

Phishing (0/1)

Trusted Relationship

Execution

2 techniques

Exploitation for Client Execution

User Execution (0/1)

Defense Evasion

1 techniques

Use Alternate Authentication Material (0/1)

Credential Access

1 techniques

Steal Web Session Cookie

Impact

5 techniques

Account Access Removal

Data Destruction

Data Manipulation (0/0)

Defacement (0/0)

Inhibit System Recovery

My top 6 - early stage

- Valid accounts.
 - Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access. Compromised credentials may even be used for persistent access to remote systems and externally available services, such as VPNs, network devices, and remote desktop.
- Have a look at intelx.io and plug your domain in.
- Fix with:
 - Strong authentication – just MFA is not enough anymore.
 - Security certificates for VPN access.
- Sub techniques consider:
 - Default, Domain, Local, and Cloud accounts.

My top 6 - mid stage

- Exploitation for Defence Evasion.
 - Adversaries may exploit a system or application vulnerability to bypass security features.
- Unpatched or misconfigured applications.
- Fix it with:
 - Vulnerability management tool.
 - Automated patch management tools.
 - People, Process, and Policy.

My top 6 - early stage

- Browser extensions.
 - Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality and customize aspects of Internet browsers. They can be installed directly or through a browser's app store and generally have access and permissions to everything that the browser can access.
- Cookie theft! TOTP capture, clipboard capture, clipboard manipulation.
- Carry out an audit of your browser extensions in use.
- Fix with:
 - Group Policy management of Browser Extensions.

My top 6 - mid stage

- Exploitation for Defence Evasion.
 - Adversaries may exploit a system or application vulnerability to bypass security features.
- Unpatched or misconfigured applications.
- Fix it with:
 - Vulnerability management tool.
 - Automated patch management tools.
 - People, Process, and Policy.

My top 6 - mid stage

- Unsecured Credentials.
 - Adversaries may search compromised systems to find and obtain insecurely stored credentials. These credentials can be stored and/or misplaced in many locations on a system, including plaintext files (Bash History), operating system or application-specific repositories (Credentials in Registry), or other specialized files/artifacts (Private Keys).
- Strong password stores.
- Fix with:
 - Review Group Policy for credentials stored within policy.
 - Run a search for passwords.xlsx.
 - Review file share permissions with a 'zero-trust' mindset.

My top 6 - late stage

- Exfiltration Over Web Service
 - Exfiltration to Code Repository
 - Exfiltration to Cloud Storage



My top 6 – late stage

- Exfiltration Over Web Service
 - Exfiltration to Code Repository
 - Exfiltration to Cloud Storage

~~Web service providers also commonly use SSL/TLS encryption, giving adversaries an added level of protection.~~

Web service providers also commonly use SSL/TLS encryption, giving adversaries an added level of protection.

~~Web service providers also commonly use SSL/TLS encryption, giving adversaries an added level of protection.~~

What now?

Educate

Remediate and Mitigate

Show improvement over time

Use ATT&CK in your product evaluations





A Scalable, Automated Adversary Emulation Platform

CALDERA™ is a cybersecurity framework developed by MITRE that empowers cyber practitioners to save time, money, and energy through automated security assessments.

Get Involved

[Contributing](#)[Get Started](#)[Join on Slack](#)[Discussions](#)

What does CALDERA do?

CALDERA helps cybersecurity professionals reduce the amount of time and resources needed for routine cybersecurity testing.

CALDERA empowers cyber teams in three main ways:

Autonomous Adversary Emulation

With CALDERA, your cyber team can build a specific threat (adversary) profile and launch it in a network to see where you may be susceptible. This helps with testing defenses and training blue teams on how to detect specific threats.


SCENARIO



Backdoors & Breaches

INITIAL COMPROMISE


Created by: **BLACK HILLS** | Information Security



Backdoors & Breaches

PIVOT and ESCALATE

Created by: **BLACK HILLS** | Information Security



Backdoors & Breaches

C2 and EXFIL

Created by: **BLACK HILLS** | Information Security



Backdoors & Breaches

PERSISTENCE

Created by: **BLACK HILLS** | Information Security

PROCEDURES

Established Procedures:

CYBER DECEPTION

The attackers go after one of your deception technologies. This could be a Word Web Bug, Honey Account, or a full honeypot.

TOOLS

ENDPOINT ANALYSIS

This is where the Defenders use their SANS IR Cheat Sheets to detect attacks on workstations. Time to bring in the Help Desk... and pray.

TOOLS

ENDPOINT SECURITY PROTECTION ANALYSIS

We know, you have AV. Great! Do you actually get alerts and logs? Do you immediately review them? Or, do you simply turn it on and walk away while the network explodes like you're in a bad action movie?

TOOLS

MEMORY ANALYSIS

Incident Response Team pulls the memory from the suspect system and reviews it for possible malicious activity.

TOOLS

Other Procedures:

SERVER ANALYSIS

The ability to baseline a system and verify that it is operating in a normal state. By the way, this is more than simply running Task Manager and looking for evil_backdoor.exe.

TOOLS

CALL A CONSULTANT

Do you want help? Feeling stuck? Rolling badly? Need a different perspective on the incident? Then maybe it's time to phone a friend.

You can choose one Consultant Card to help your team with the incident.

The Consultant Card's modifier is offensive.

TOOLS

NETWORK THREAT HUNTING - ZEEK/RITA ANALYSIS

Does your organization capture and review network traffic? Good! Do you know how to parse and review it? Is that process documented? Or, do you just run Zeek/RITA/Security Onion/ELK because the cool kids are doing it?

TOOLS

USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)

It's like logging, but it actually works. UEBA looks for multiple concurrent logins, impossible logins based on geography, unusual file access, password sprays, and more!

TOOLS

CRISIS MANAGEMENT

Your Legal and Management Teams have procedures for effectively and ethically notifying impacted victims of compromises.

TOOLS

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) LOG ANALYSIS

Yeah... good luck with this one. Are you logging the right things? Do you regularly emulate attack scenarios to see if you can detect them?

TOOLS

FIREWALL LOG REVIEW

Can your organization analyze and understand firewall logs? Do you regularly emulate attack scenarios and verify that your procedures work?

TOOLS

SOP-ELK

PHYSICAL SECURITY REVIEW

Do you have security cameras? Do you have security guards? Do you have access badges for certain areas in your facilities? Can just anyone access your sensitive IT infrastructure? No? Are you sure?

TOOLS

ISOLATION

Your Network Team is on their game. They can easily isolate infected systems to prevent further harm.

TOOLS

EXTERNAL CLOUD ACCESS

The attackers gain access to your cloud resources. They use this access to pivot.

DETECTION

SIEM Log Analysis

TOOLS

SprayingToolkit
truffleHog
FireProx

SMB WEAKNESS

The attackers take advantage of a number of different Server Message Block (SMB) issues that can be used for post-exploitation. From SMB Signing disabled to using SMBv1.

DETECTION

User and Entity Behavior Analytics
SIEM Log Analysis
Firewall Log Review

TOOLS

GMAIL, TUMBLR, SALESFORCE, TWITTER AS C2

The attackers route traffic through third-party services. Many services, like Gmail, are ignored completely by many security tools.

DETECTION

Network Threat Hunting - Zeek/RITA Analysis
Firewall Log Review

TOOLS

MALICIOUS SERVICE

The attackers add a service that starts every time the system starts.

DETECTION

Endpoint Security Protection Analysis
Memory Analysis
Endpoint Analysis

TOOLS

Meterpreter Persistence Modules

PHYSICAL ACCESS

The attackers gain physical access to your organization and use this to pivot to your internal networks.

DETECTION

Physical Security Review
User Awareness Training

TOOLS

BROADCAST/MULTICAST PROTOCOL POISONING

For years, LANMAN was the worst thing in Windows. Then LLMNR said, "Stand Back and Hold My Beer!" Basically, LLMNR lets a host ask for name resolution from any system on the same network. The attackers perform Broadcast/Multicast protocol poisoning on your Active Directory Network.

DETECTION

Cyber Deception
User and Entity Behavior Analytics

TOOLS

GMAIL, TUMBLR, SALESFORCE, TWITTER AS C2

The attackers route traffic through third-party services. Many services, like Gmail, are ignored completely by many security tools.

DETECTION

Network Threat Hunting - Zeek/RITA Analysis
Firewall Log Review

TOOLS

APPLICATION SHIMMING

The attackers use the Application Compatibility Toolkit to trick applications into not seeing the ports, directories, files, and services the attackers want to hide.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis

TOOLS

Windows Assessment and Deployment Kit (ADK)

SUPPLY CHAIN ATTACK

The attackers insert malware in the update process of one of your key enterprise management tools. This gives them direct access to the heart of your infrastructure.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis
Network Threat Hunting - Zeek/RITA Analysis

TOOLS

SMB WEAKNESS

The attackers take advantage of a number of different Server Message Block (SMB) issues that can be used for post-exploitation. From SMB Signing disabled to using SMBv1.

DETECTION

User and Entity Behavior Analytics
SIEM Log Analysis
Firewall Log Review

TOOLS

HTTPS AS EXFIL

This is pretty basic: the attackers use HTTPS. Lots and lots of malware uses this. For example, Meterpreter has used this technique for a long time. It can be used in conjunction with other stego techniques.

DETECTION

Network Threat Hunting - Zeek/RITA Analysis
Firewall Log Review

TOOLS

EVENT TRIGGERED MALWARE

The attackers' malware triggers only when specific events occur. For example, when a specific DLL or service is started.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis
SIEM Log Analysis

TOOLS

I'd like to know more (sorry wrong franchise!)

- Ask questions...
- <https://attack.mitre.org/>
- <https://attack.mitre.org/resources/getting-started/>
- <https://mitre-attack.github.io/attack-navigator/>
- <https://caldera.mitre.org/>
- <https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/>
- The recording and presentation will be on myworldofit.net within 24 hours



SECURITY SERVICES

We help organisations reduce risk and simplify operational management. As part of that, we provide on-going security services for all aspects of an IT network.



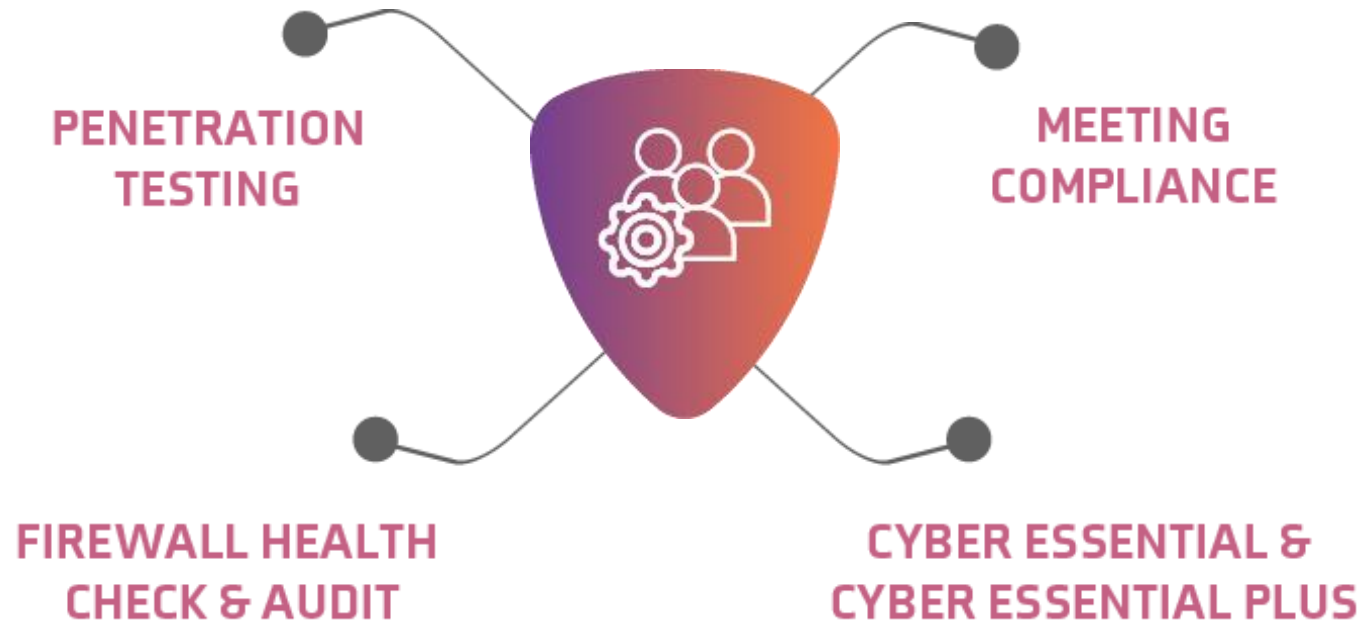
PROTECTING YOUR TOMORROW BY SECURING YOUR TODAY.





ADVISORY & AUDIT SERVICES

Our advisory & audit services are here to make sure you are well-prepared for audit and any framework changes.

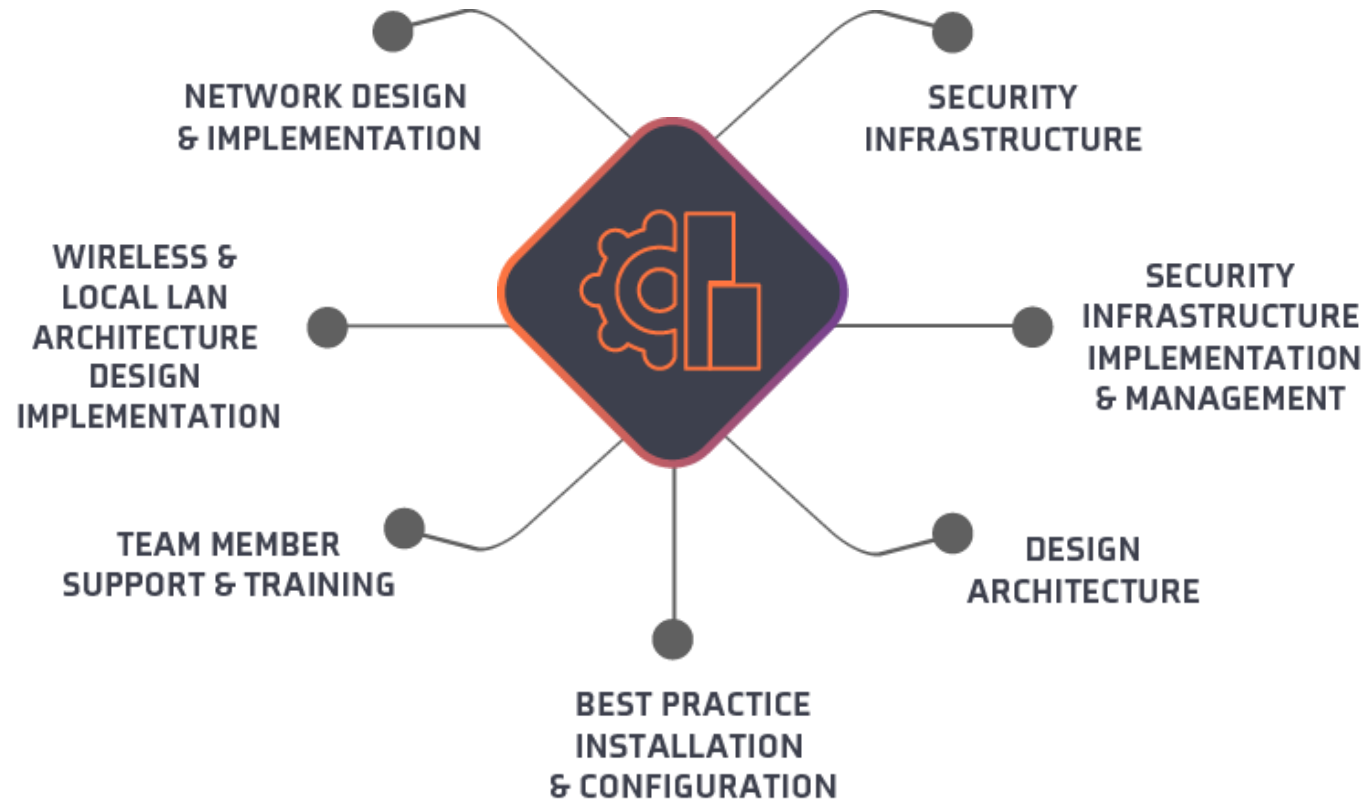


PROTECTING YOUR TOMORROW BY SECURING YOUR TODAY.



INFRASTRUCTURE SERVICES

Our infrastructure services are here to help you solve several major challenges of new network architecture.



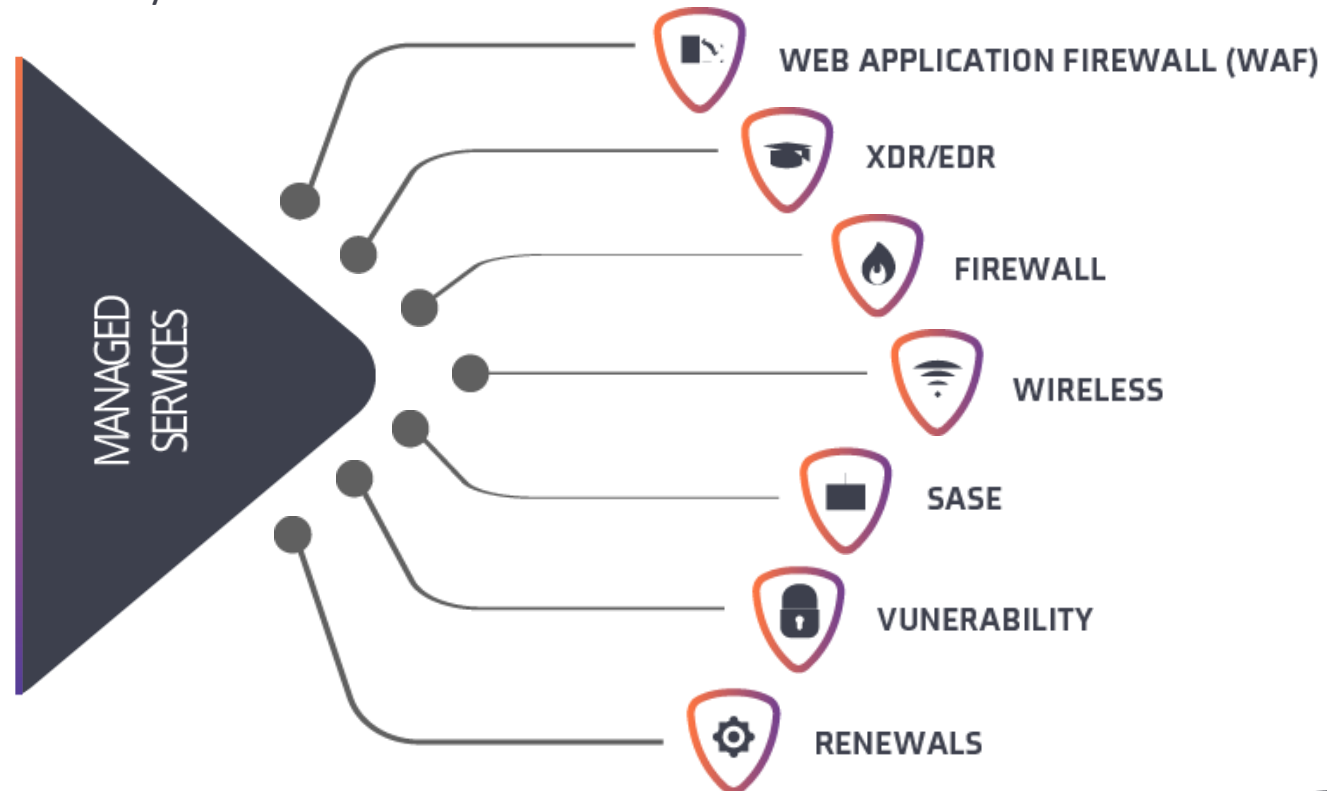
PROTECTING YOUR TOMORROW BY SECURING YOUR TODAY.





MANAGED SERVICES

Our managed services are flexible and consistent enough to meet the unique requirements of each situation, with a guaranteed level of service delivery.



PROTECTING YOUR TOMORROW BY SECURING YOUR TODAY.



Any questions?

- Ask questions...
- <https://attack.mitre.org/>
- <https://attack.mitre.org/resources/getting-started/>
- <https://mitre-attack.github.io/attack-navigator/>
- <https://caldera.mitre.org/>
- <https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/>
- The recording and presentation will be on myworldofit.net within 24 hours

jp@myworldofit.net
jpreston@ansecurity.com