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

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?

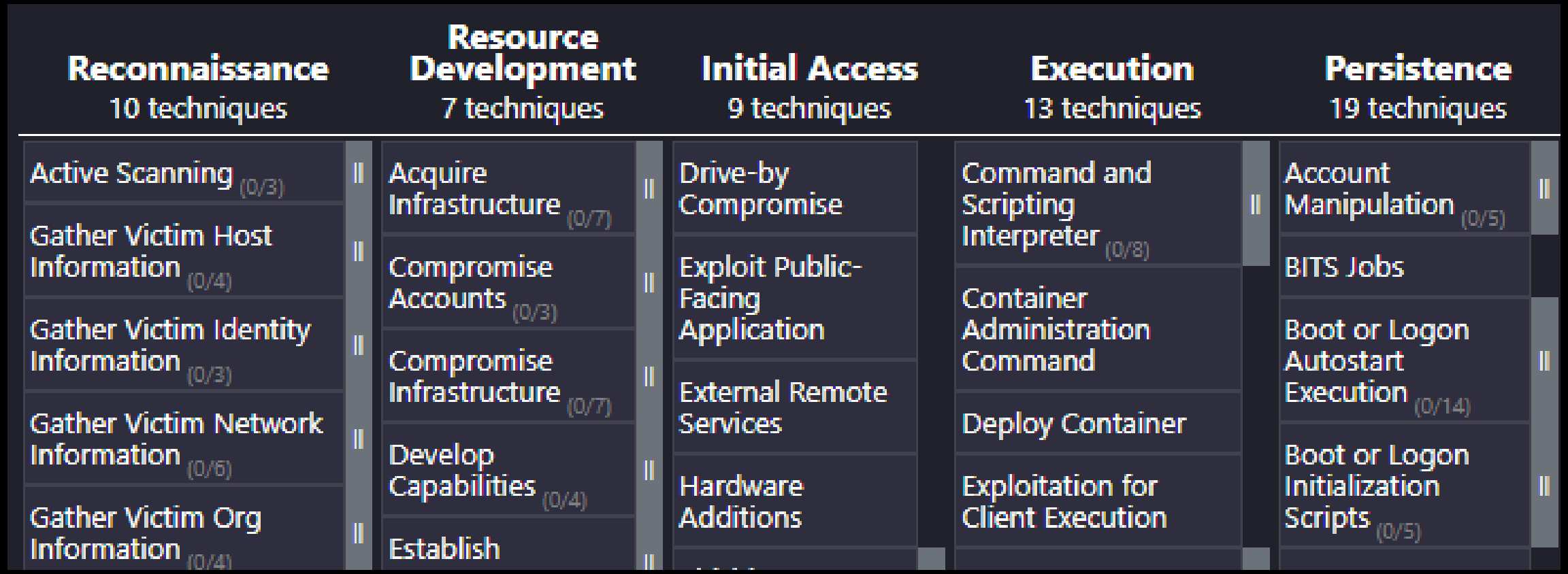
- American non-profit.
- Research and development focused (including cyber security).
- Founded the Centre for Threat-Informed Defence, along with Microsoft, BAE Systems, IBM Security, and Centre for Internet Security.
- Big on using GitHub to publish software and receive feedback.

Tell me about ATT&CK…

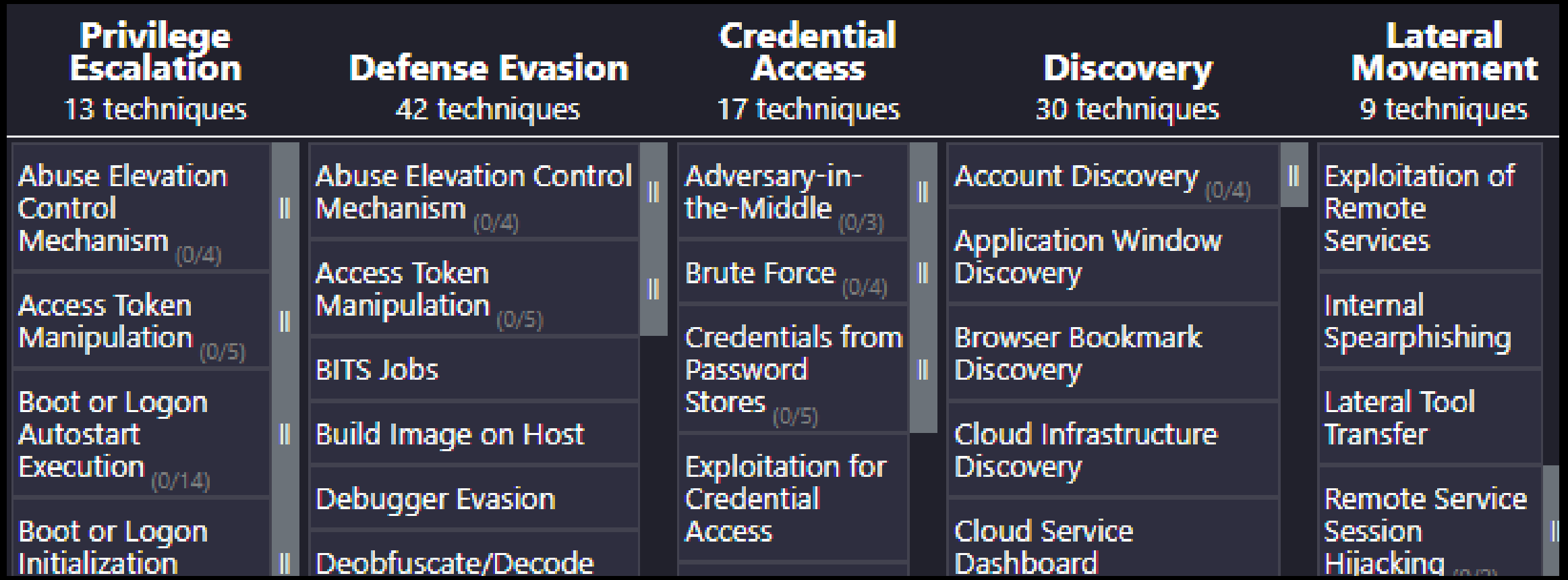
- Selection of:
  - Tactics.
  - Techniques.
  - Procedures.
- To achieve an action on an objective.
- Linked to known attacks by known threat groups including:
  - CozyBear.
  - Deep Panda.
  - BlackOasis.

Tell me about ATT&CK…

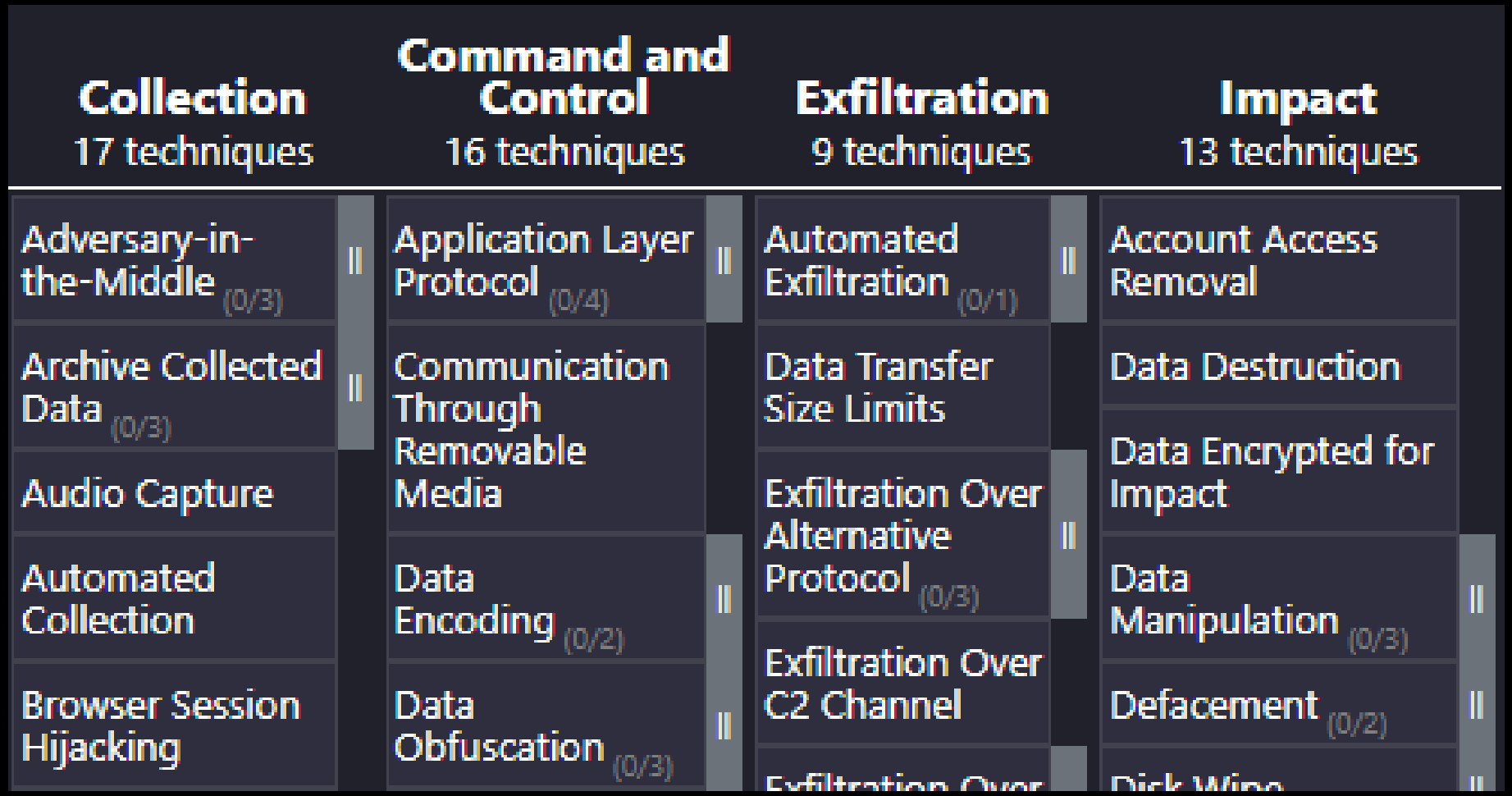
ATT&CK navigator



ATT&CK navigator



ATT&CK navigator

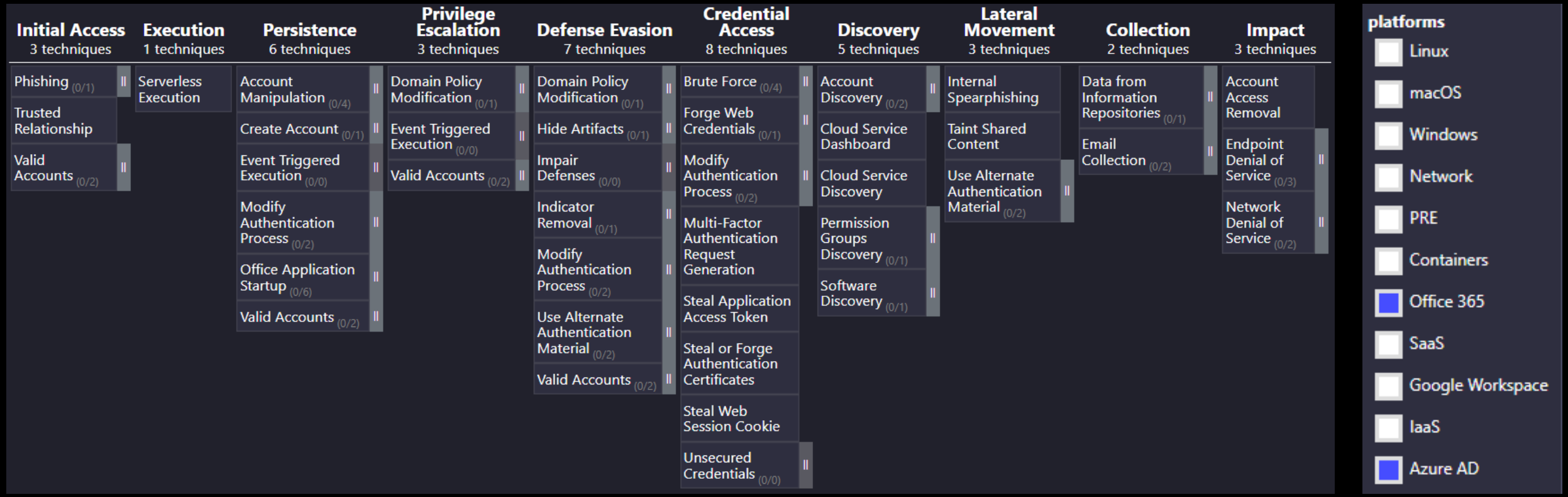


Mobile devices

Industrial Control Systems

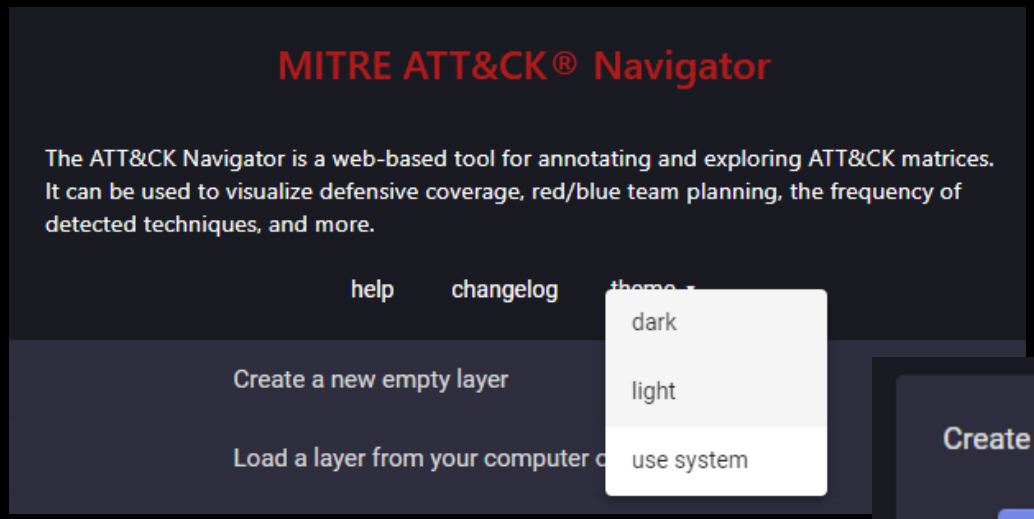
Initial Access 12 techniques	Execution 9 techniques	Persistence 6 techniques	Privilege Escalation 2 techniques	Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 7 techniques	Collection 10 techniques	Command and Control 3 techniques	Inhibit Response Function 13 techniques	Impair Process Control 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	Wireless Sniffing	Program Download	I/O Image		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

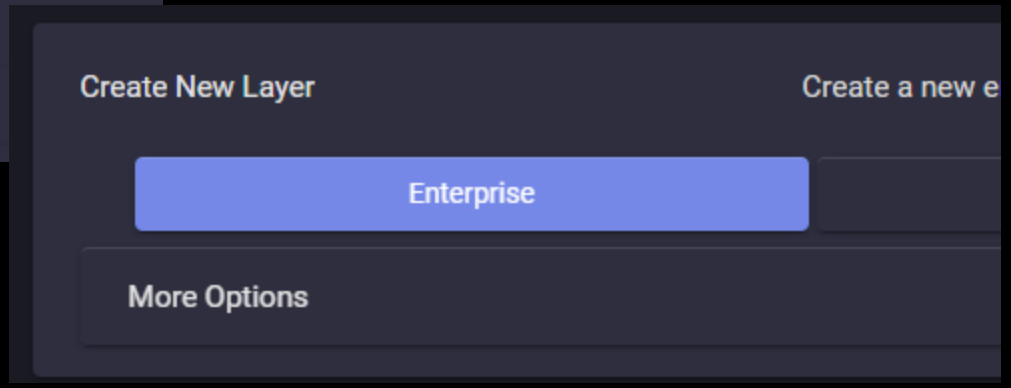
Filter to specific platforms

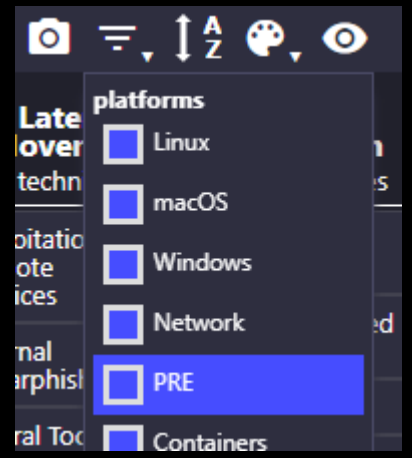


ATT&CK navigator

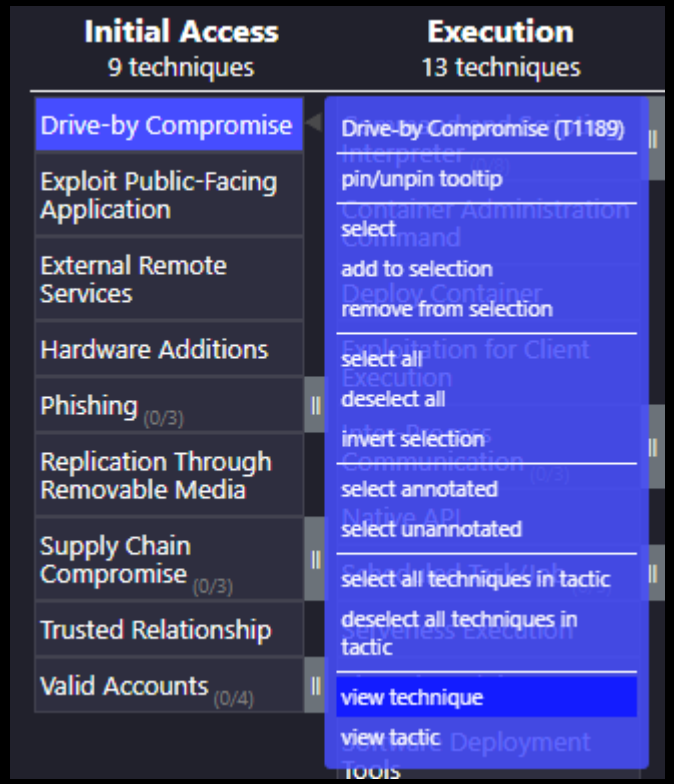
https://mitre-attack.github.io/attack-navigator/







ATT&CK navigator



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

Tactic: Initial Access

Platforms: Linux, SaaS, Windows, macOS

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 `.js` file. [15][16]

The detail

Mitigations

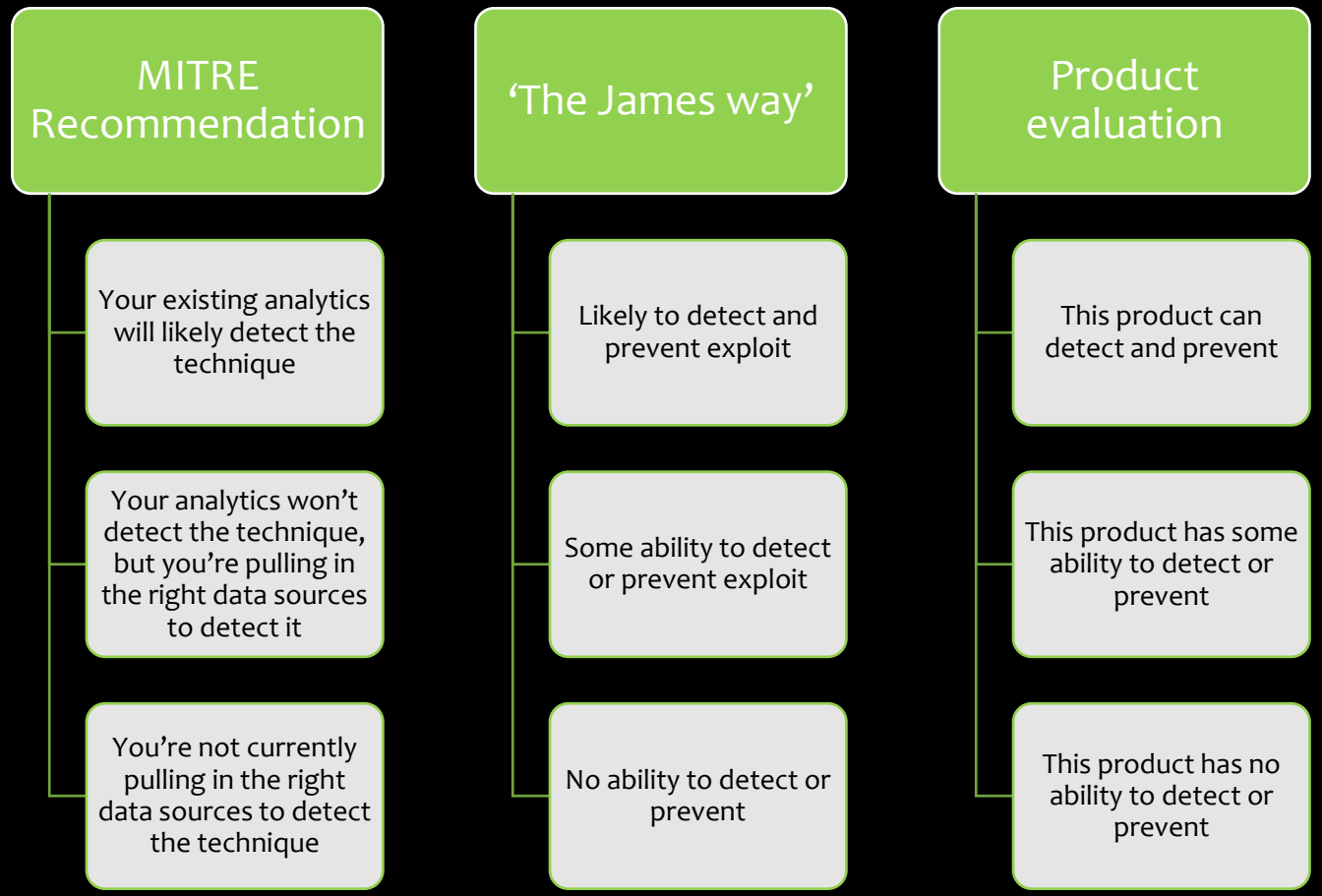
ID	Mitigation	Description
M1048	Application Isolation and Sandboxing	Browser sandboxes can be used to mitigate some of the impact of exploitation, but sandbox escapes may still exist.[58][59] Other types of virtualization and application microsegmentation may also mitigate the impact of client-side exploitation. The risks of additional exploits and weaknesses in implementation may still exist for these types of systems.[59]
M1050	Exploit Protection	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.
M1021	Restrict Web-Based Content	For malicious code served up through ads, adblockers can help prevent that code from executing in the first place. Script blocking extensions can help prevent the execution of JavaScript that may commonly be used during the exploitation process.
M1051	Update Software	Ensure all browsers and plugins kept updated can help prevent the exploit phase of this technique. Use modern browsers with security features turned on.

The detail

Detection

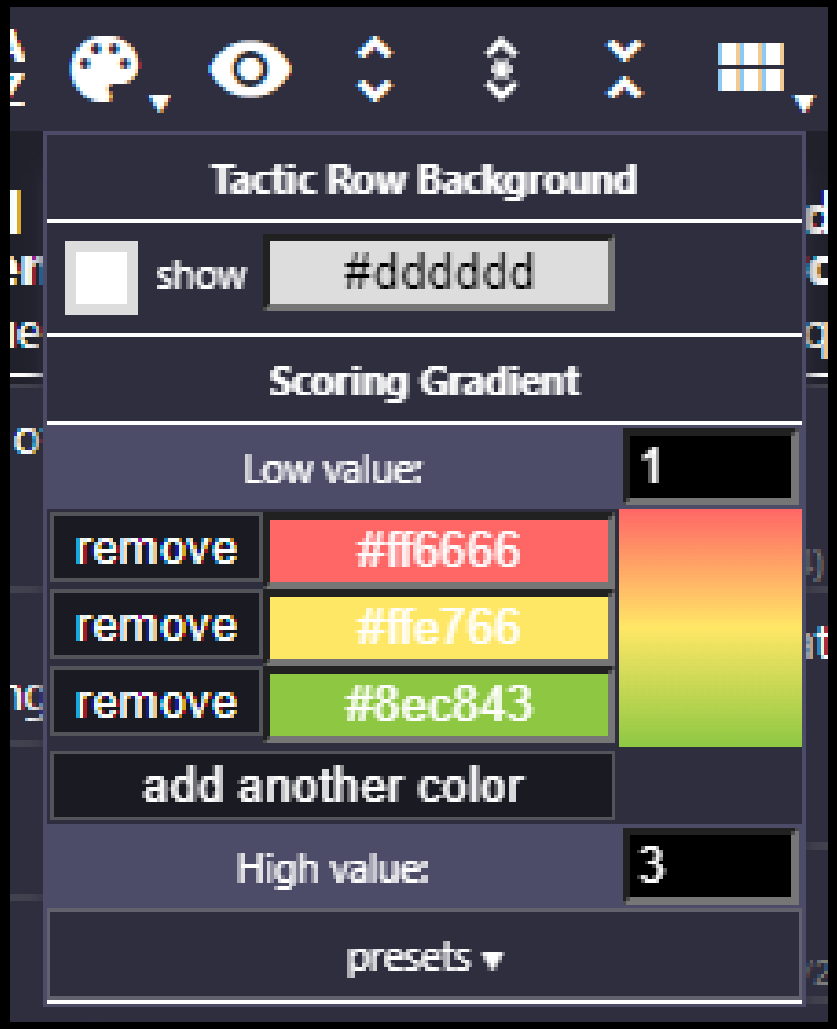
ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Firewalls and proxies can inspect URLs for potentially known-bad domains or parameters. They can also do reputation-based analytics on websites and their requested resources such as how old a domain is, who it's registered 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.

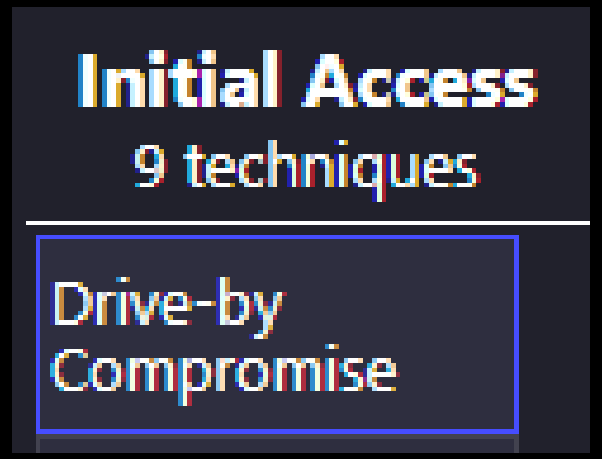
Paint by numbers

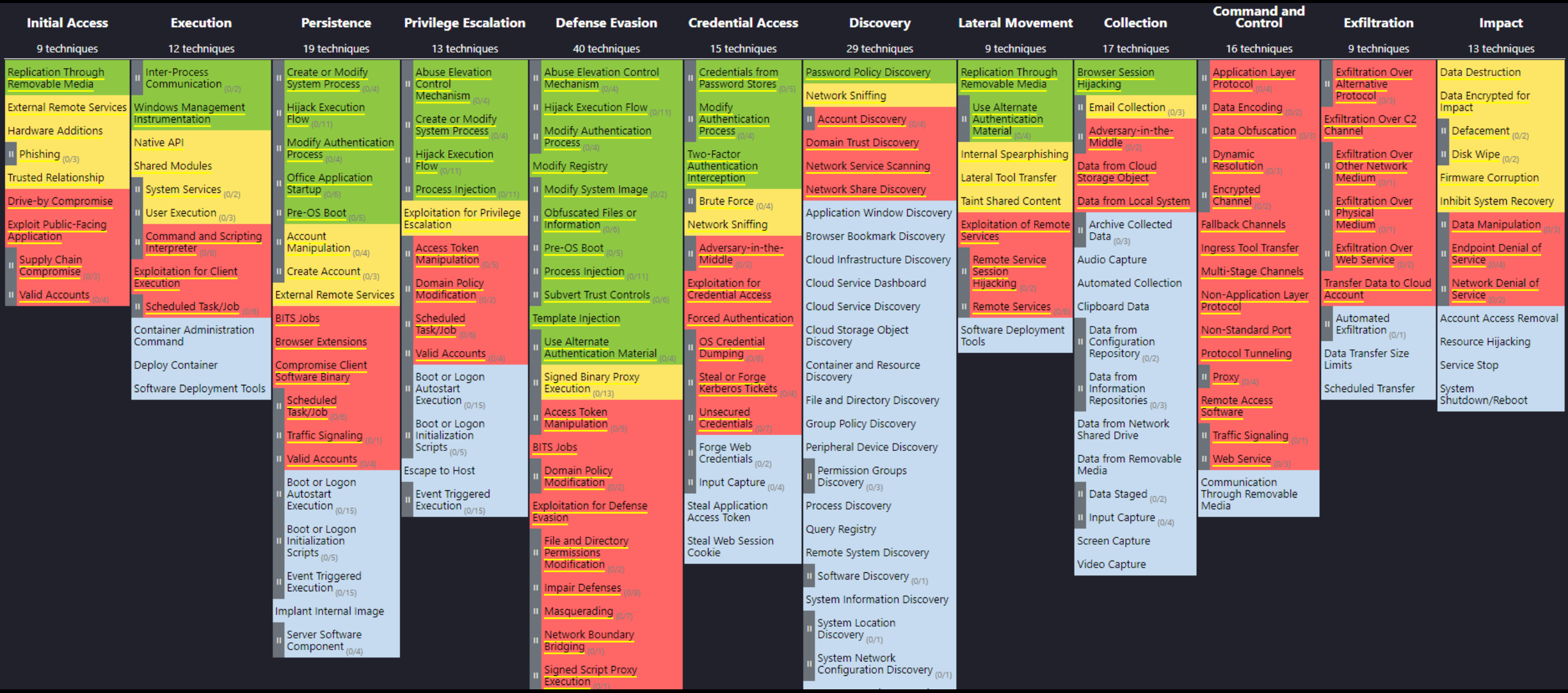


Some techniques have no known method to detect or prevent exploit!

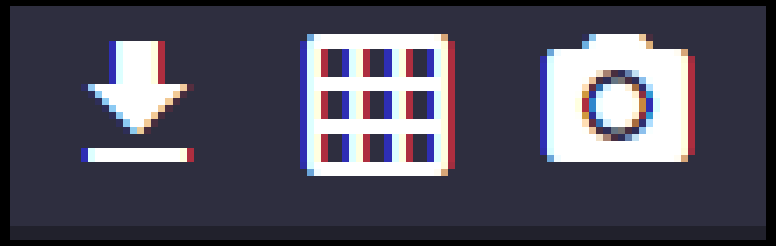
ATT&CK navigator

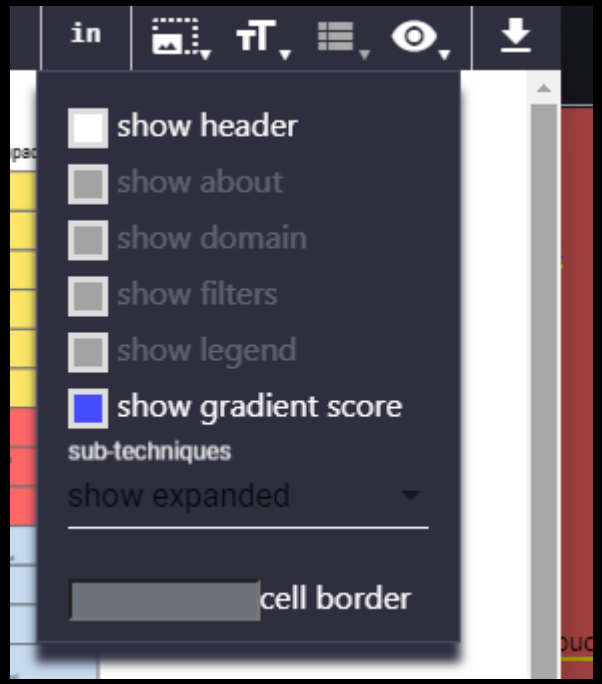


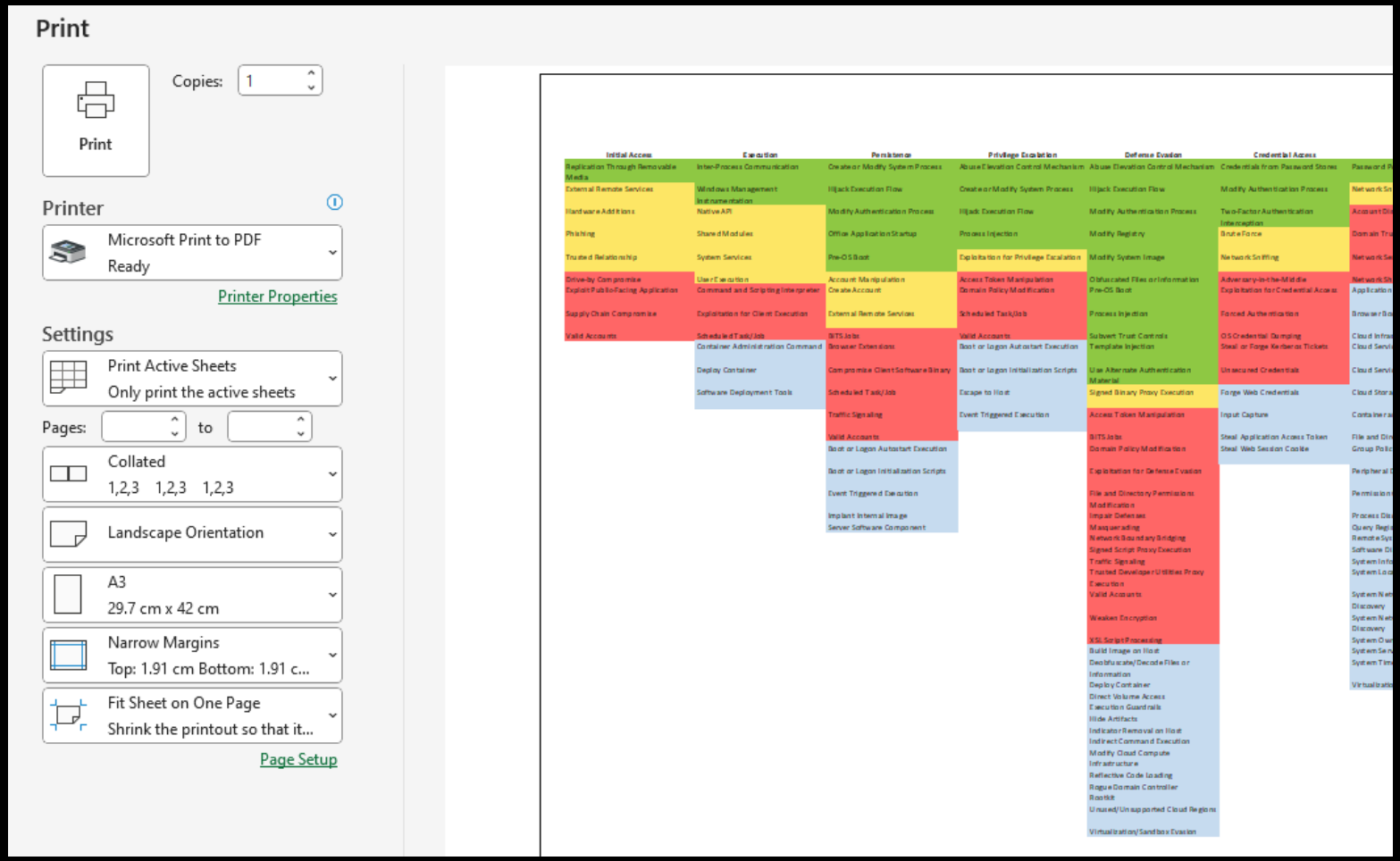



Initial Access
9 techniques
Replication Through Removable Media
External Remote Services
Hardware Additions
Phishing (0/3)
Trusted Relationship
Drive-by Compromise
Exploit Public-Facing Application
Supply Chain Compromise (0/3)
Valid Accounts (0/4)
Execution
12 techniques
Inter-Process Communication (0/2)
Windows Management Instrumentation
Native API
Shared Modules
System Services (0/2)
User Execution (0/3)
Command and Scripting Interpreter (0/8)
Exploitation for Client Execution
Scheduled Task/Job (0/6)
Container Administration Command
Deploy Container
Software Deployment Tools
Persistence
19 techniques
Create or Modify System Process (0/4)
Hijack Execution Flow (0/11)
Modify Authentication Process (0/4)
Office Application Startup (0/6)
Pre-OS Boot (0/5)
Account Manipulation (0/4)
Create Account (0/3)
External Remote Services
BITS Jobs
Browser Extensions
Compromise Client Software Binary
Scheduled Task/Job (0/6)
Traffic Signaling (0/1)
Valid Accounts (0/4)
Boot or Logon Autostart Execution (0/15)
Boot or Logon Initialization Scripts (0/5)
Event Triggered Execution (0/15)
Implant Internal Image
Server Software Component (0/4)
Privilege Escalation
13 techniques
Abuse Elevation Control Mechanism (0/4)
Create or Modify System Process (0/4)
Hijack Execution Flow (0/11)
Process Injection (0/11)
Exploitation for Privilege Escalation
Access Token Manipulation (0/5)
Domain Policy Modification (0/2)
Scheduled Task/Job (0/6)
Valid Accounts (0/4)
Boot or Logon Autostart Execution (0/15)
Boot or Logon Initialization Scripts (0/5)
Escape to Host
Event Triggered Execution (0/15)
Defense Evasion
40 techniques
Abuse Elevation Control Mechanism (0/4)
Hijack Execution Flow (0/11)
Modify Authentication Process (0/4)
Modify Registry
Modify System Image (0/2)
Obfuscated Files or Information (0/6)
Pre-OS Boot (0/5)
Process Injection (0/11)
Subvert Trust Controls (0/6)
Template Injection
Use Alternate Authentication Material (0/4)
Signed Binary Proxy Execution (0/13)
Access Token Manipulation (0/5)
BITS Jobs
Domain Policy Modification (0/2)
Exploitation for Defense Evasion
File and Directory Permissions Modification (0/2)
Impair Defenses (0/9)
Masquerading (0/7)
Network Boundary Bridging (0/1)
Signed Script Proxy Execution (0/1)
Credential Access
15 techniques
Credentials from Password Stores (0/5)
Modify Authentication Process (0/4)
Two-Factor Authentication Interception
Brute Force (0/4)
Network Sniffing
Adversary-in-the-Middle (0/2)
Exploitation for Credential Access
Forced Authentication
OS Credential Dumping (0/8)
Steal or Forge Kerberos Tickets (0/4)
Unsecured Credentials (0/7)
Forge Web Credentials (0/2)
Input Capture (0/4)
Steal Application Access Token
Steal Web Session Cookie
Discovery
29 techniques
Password Policy Discovery
Network Sniffing
Account Discovery (0/4)
Domain Trust Discovery
Network Service Scanning
Network Share Discovery
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
File and Directory Discovery
Group Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (0/3)
Process Discovery
Query Registry
Remote System Discovery
Software Discovery (0/1)
System Information Discovery
System Location Discovery (0/1)
System Network Configuration Discovery (0/1)
Lateral Movement
9 techniques
Replication Through Removable Media
Use Alternate Authentication Material (0/4)
Internal Spearphishing
Lateral Tool Transfer
Taint Shared Content
Exploitation of Remote Services
Remote Service Session Hijacking (0/2)
Remote Services (0/6)
Software Deployment Tools
Collection
17 techniques
Browser Session Hijacking
Email Collection (0/3)
Adversary-in-the-Middle (0/2)
Data from Cloud Storage Object
Data from Local System
Archive Collected Data (0/3)
Audio Capture
Automated Collection
Clipboard Data
Data from Configuration Repository (0/2)
Data from Information Repositories (0/3)
Data from Network Shared Drive
Data from Removable Media
Data Staged (0/2)
Input Capture (0/4)
Screen Capture
Video Capture
Command and Control
16 techniques
Application Layer Protocol (0/4)
Data Encoding (0/2)
Data Obfuscation (0/3)
Dynamic Resolution (0/3)
Encrypted Channel (0/2)
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (0/4)
Remote Access Software
Traffic Signaling (0/1)
Web Service (0/3)
Communication Through Removable Media
Exfiltration
9 techniques
Exfiltration Over Alternative Protocol (0/3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (0/1)
Exfiltration Over Physical Medium (0/1)
Exfiltration Over Web Service (0/2)
Transfer Data to Cloud Account
Automated Exfiltration (0/1)
Data Transfer Size Limits
Scheduled Transfer
Impact
13 techniques
Data Destruction
Data Encrypted for Impact
Defacement (0/2)
Disk Wipe (0/2)
Firmware Corruption
Inhibit System Recovery
Data Manipulation (0/3)
Endpoint Denial of Service (0/4)
Network Denial of Service (0/2)
Account Access Removal
Resource Hijacking
Service Stop
System Shutdown/Reboot

Export options







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.

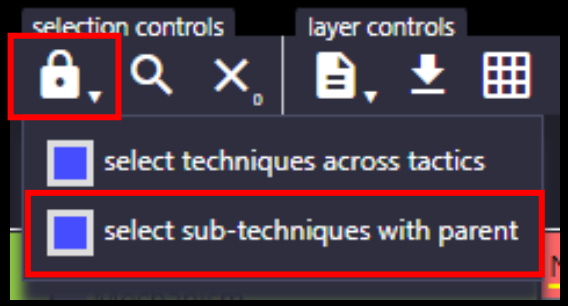
The publication warned that the threat groups APT27, APT30, APT31, Ke3chang, Gallium and Mustang Panda had been observed targeting business and governments in the EU, with recent activity focused on information theft, primarily via establishing persistent footholds within networks.

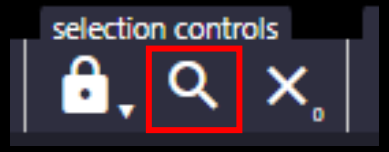
Initial Access

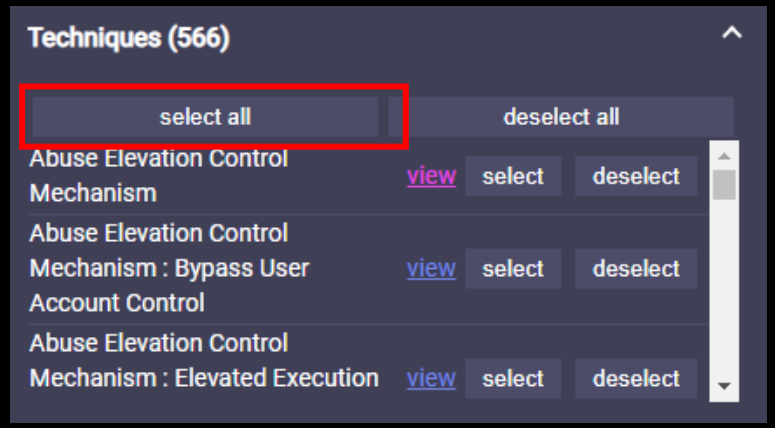
Royal actors gain initial access to victim networks in a number of ways including:

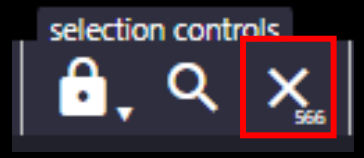
- **Phishing.** According to third-party reporting, Royal actors most commonly (in 66.7% of incidents) gain initial access to victim networks via successful phishing emails [T1566].
  - According to open-source reporting, victims have unknowingly installed malware that delivers Royal ransomware after receiving phishing emails containing malicious PDF documents [T1566.001] and malvertising [T1566.002] [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].
- **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.

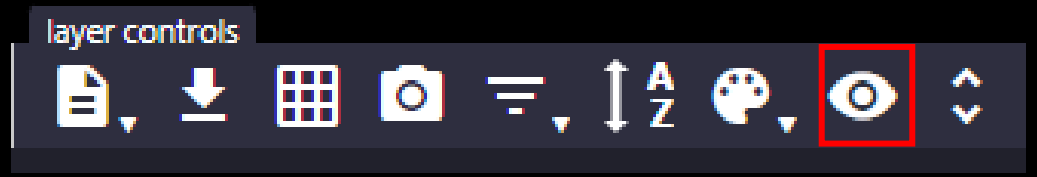
Map to threat groups



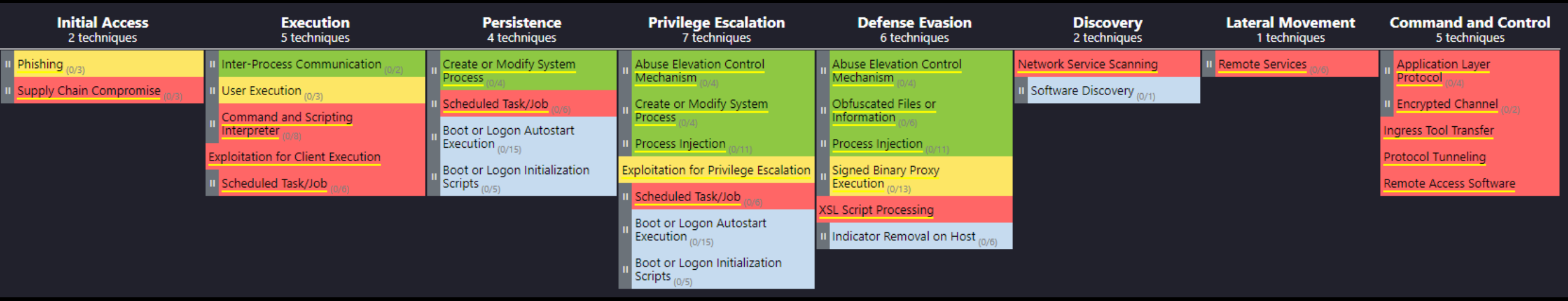




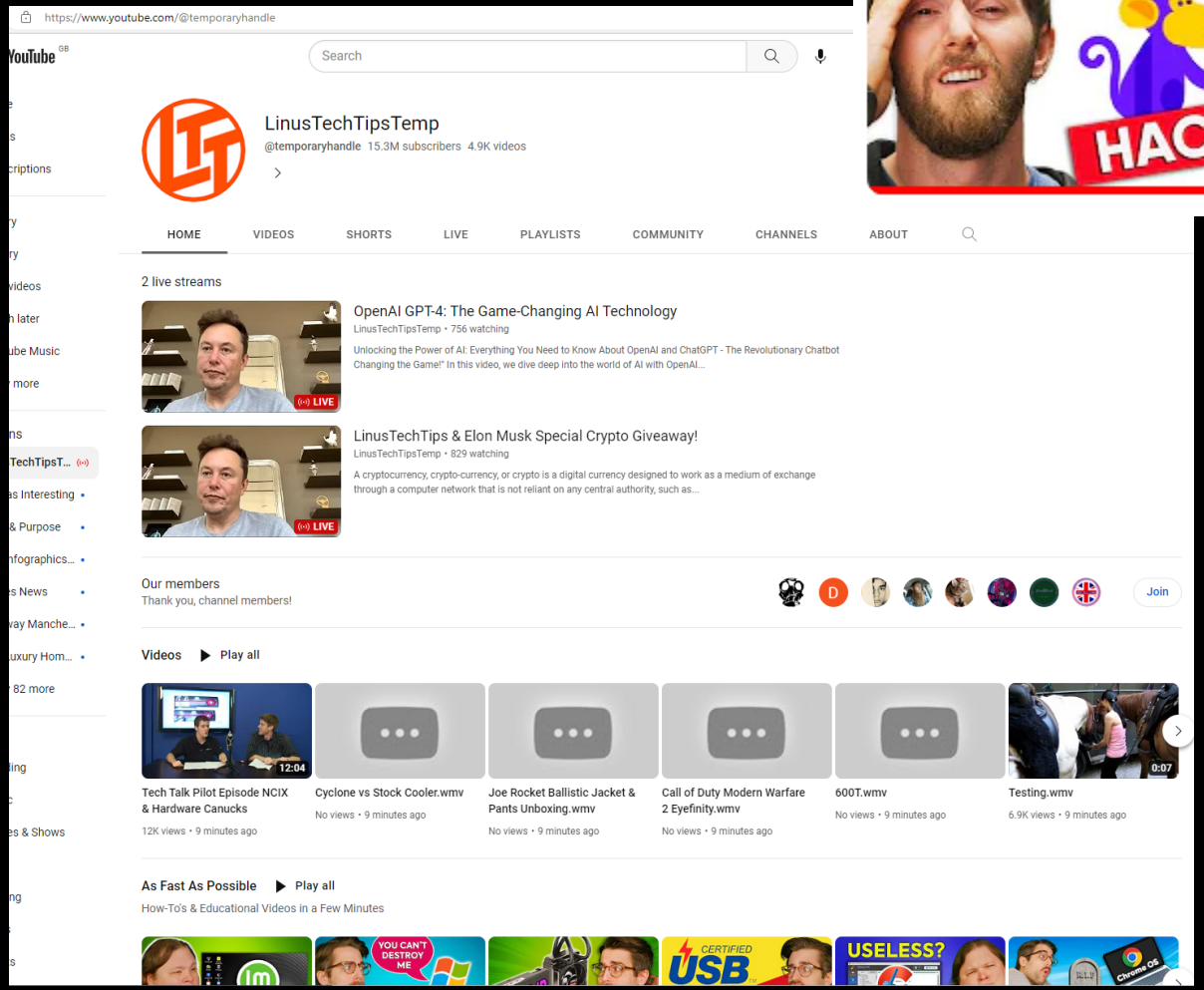


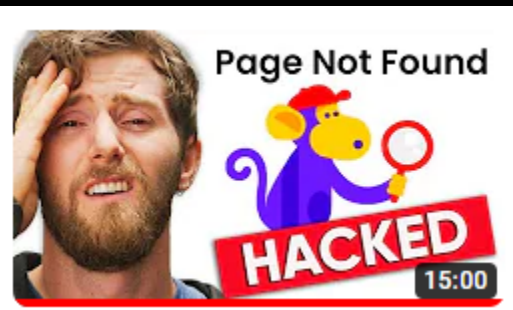


Map to threat groups



Case study!

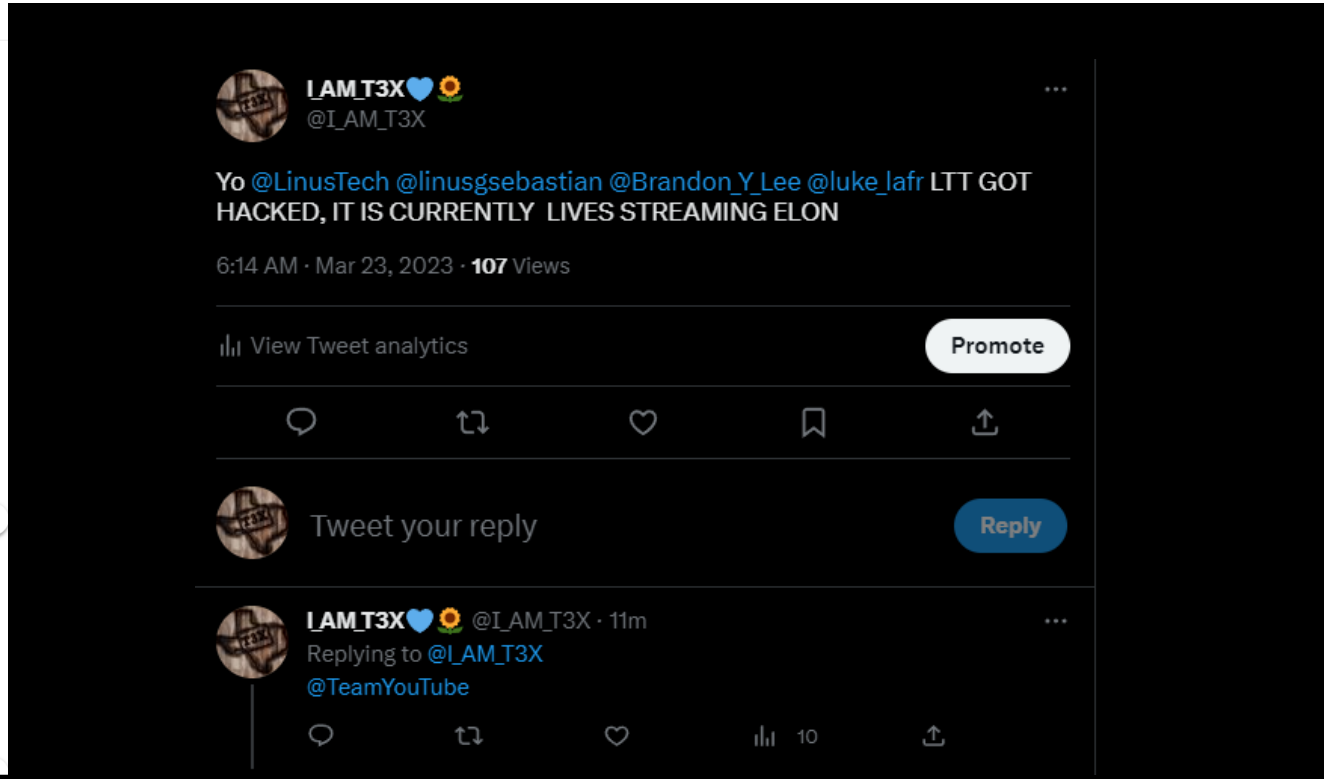




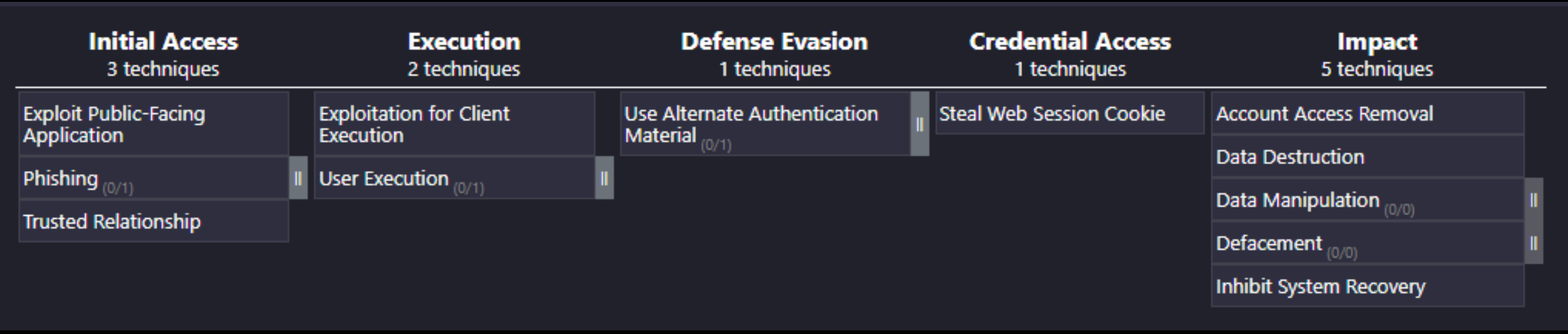
My Channel Was Deleted Last Night

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...



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 – 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

- 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 – mid stage

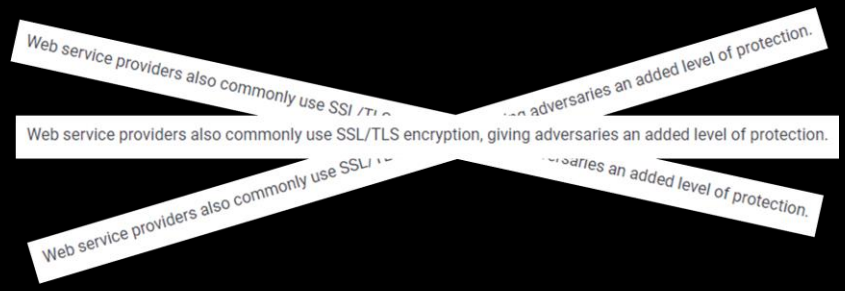
- Exploitation for Defence Evasion.
  - Adversaries may exploit a system or application vulnerability to bypass security features.
- Unpatched or misconfigured applications.
- Fix it with:
  - Vulnerability management tool.
  - Automated patch management tools.
  - People, Process, and Policy.

My top 6 – mid stage

- 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.

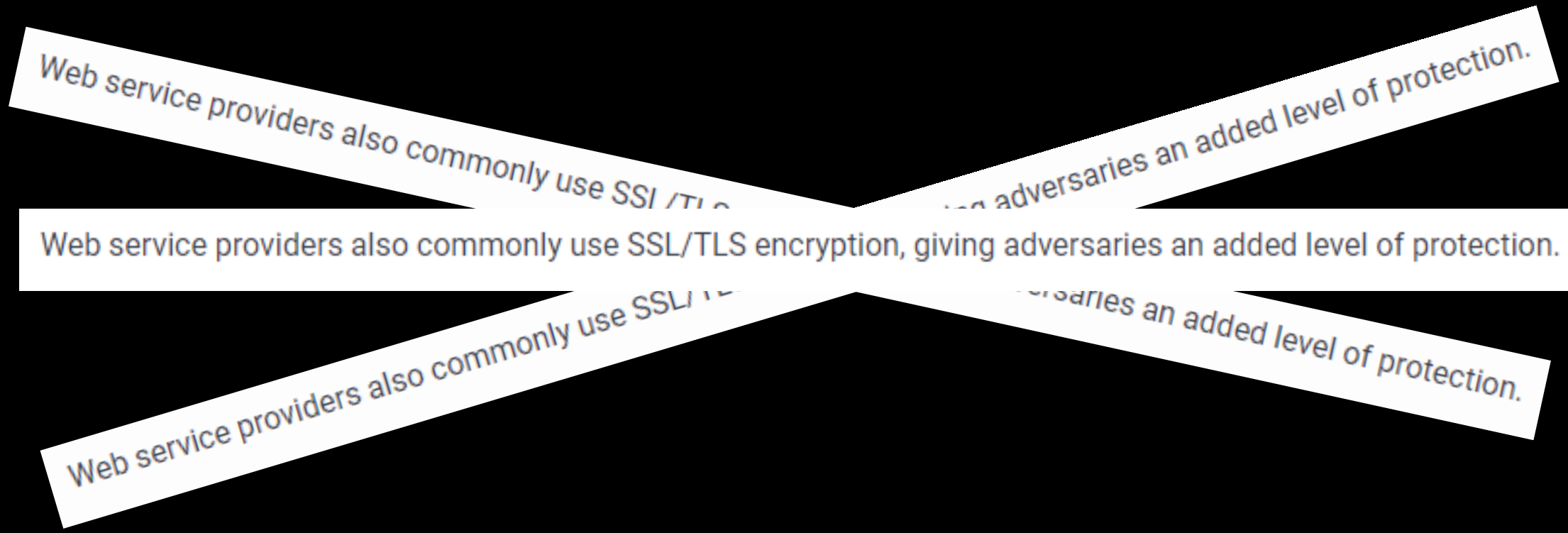
My top 6 – late stage

- 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



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

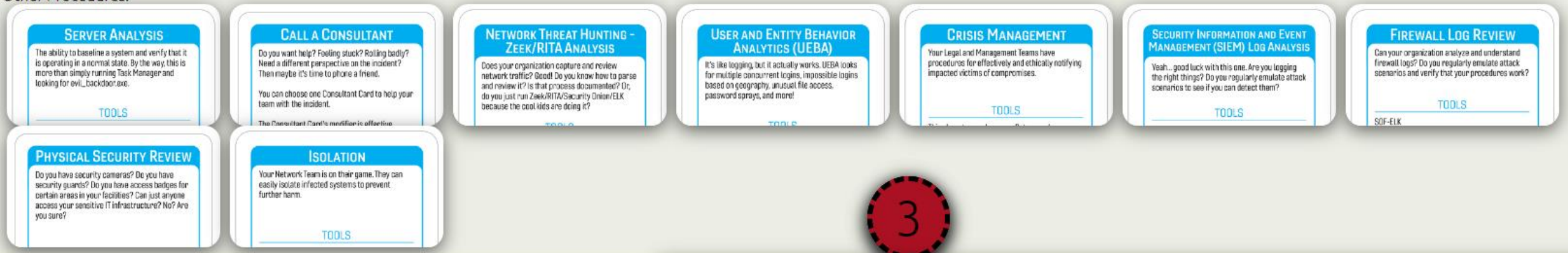
With CALDERA, your cyber team can build a specific threat (adversary) profile and launch it in a network to see where you may be susceptible. This helps with testing defenses and training blue teams on how to detect specific threats.

SCENARIO

PROCEDURES

Established Procedures:

Other Procedures:



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

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

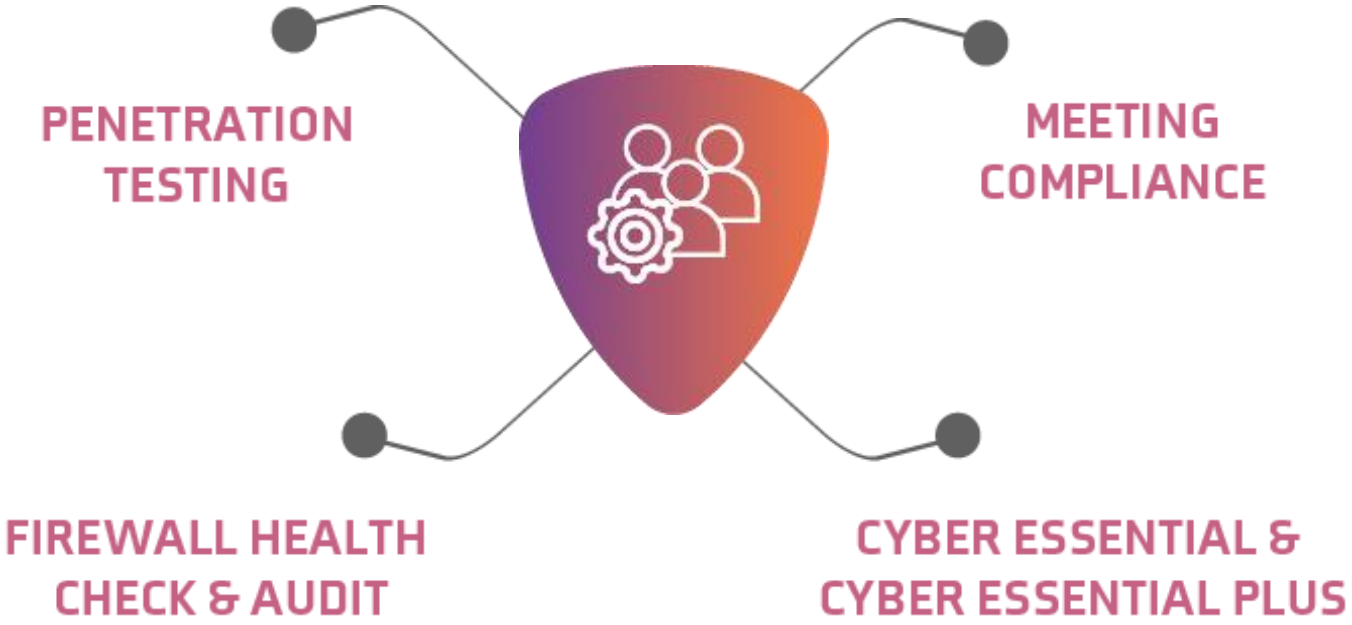
We help organisations reduce risk and simplify operational management. As part of that, we provide on-going security services for all aspects of an IT network.

PROTECTING YOUR TOMORROW BY SECURING YOUR TODAY.

ANSECURITY

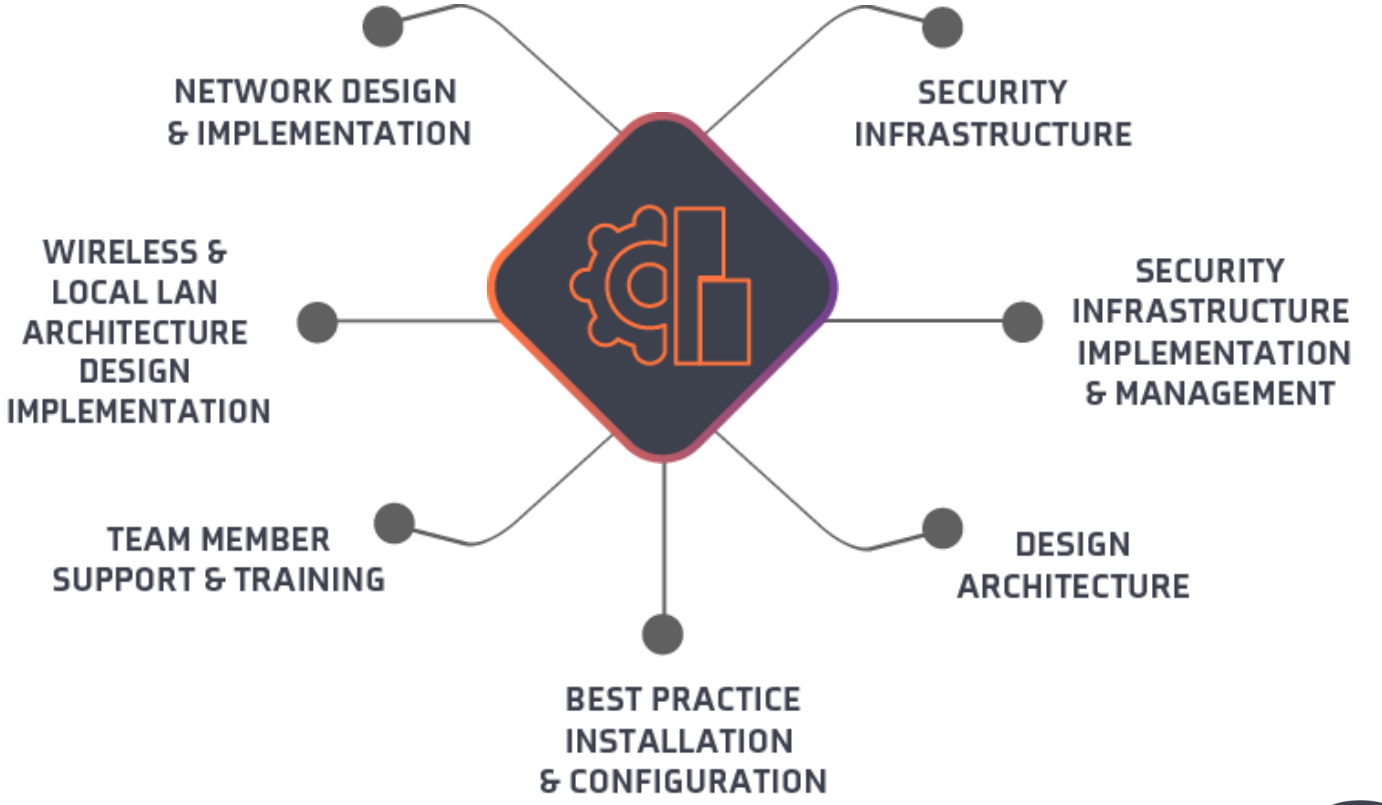
ADVISORY & AUDIT SERVICES

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



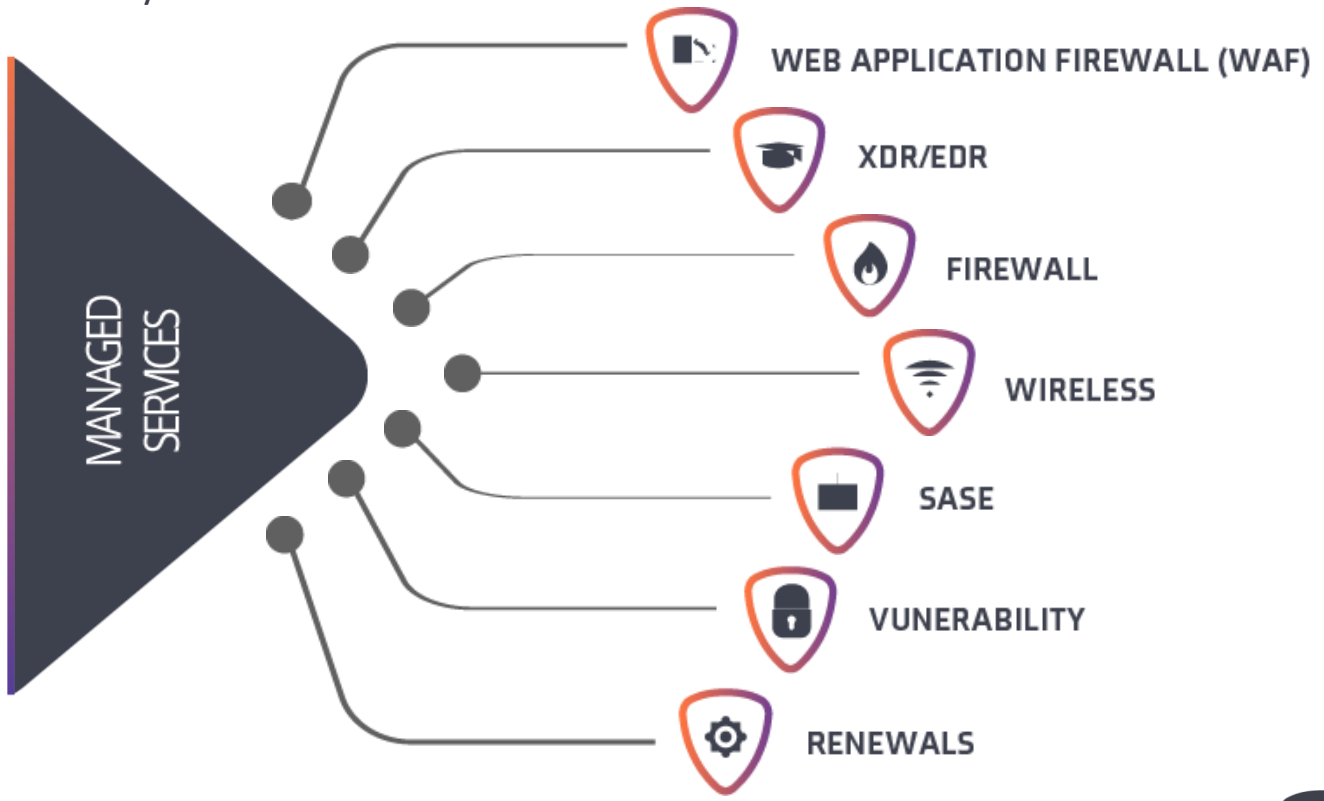
INFRASTRUCTURE SERVICES

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



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.

ANSECURITY

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