

Embark on a Journey: Threat Modeling with MITRE ATT&CK Framework

By: Brad Voris



“If you **know** the enemy and **know** yourself, you need not fear the **result** of a hundred battles.” – Sun Tzu

Brad Voris, (a whole bunch of acronyms)



- Lead InfoSec Architect @ Walmart Global Tech
- 25 years of experience IT/IS/CS
- Undergrad in Cybersecurity @ Wilmington University
- Certifications: CISSP, CISM, CCSP, CCSK, Network+, MTA, MCP, etc.
- Co-Author 2 books: Intrusion Detection Guide and Essentials of Cybersecurity for Peerlyst
- Cloud Security Alliance Zero Trust Training Contributor
- **NOT AN EXPERT**

MITRE ATT&CK: Lets make it simple

- Understand Threat Modeling
- Understand the Components of ATT&CK
- Select a Campaign, Industry, Threat Actor, etc.
- Create Your Model
- **ROCK IT!**



Threat modeling with ATT&CK

- *A process for improving security by identifying vulnerabilities and threats based on known attack vectors of threat actors*

Links you will need

- <https://attack.mitre.org/>
- <https://mitre-attack.github.io/attack-navigator/>
- <https://attack.mitre.org/campaigns/>
- <https://attack.mitre.org/matrices/enterprise/>

Additional Training

- <https://attack.mitre.org/resources/learn-more-about-attack/training/>

Could This Be Anymore Overwhelming?

layer ×+

?

Selection Controls

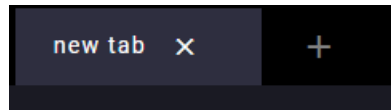
Layer Controls

Technique Controls

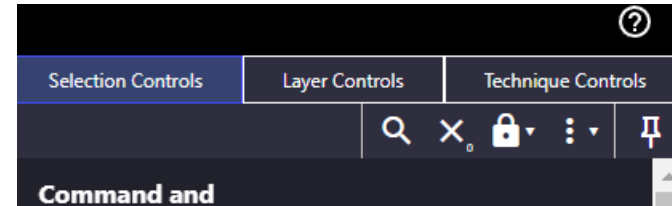
QX🔒⋮

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (0/3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (0/6)	Abuse Elevation Control Mechanism (0/6)	Abuse Elevation Control Mechanism (0/6)	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)	Acquire Infrastructure (0/8)	Drive-by Compromise	Command and Scripting Interpreter (0/10)	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	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Account Manipulation (0/6)	BITS Jobs	Credentials from Password Stores (0/6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Autostart Execution (0/14)	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Encoding (0/2)	Defacement (0/2)	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Compromise Host Software Binary (0/3)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (0/8)	Browser Session Hijacking	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Disk Wipe (0/2)
Phishing for Information (0/4)	Establish Accounts (0/3)	Phishing (0/4)	Inter-Process Communication (0/3)	Compromise Host Software Binary (0/3)	Boot or Logon Initialization Scripts (0/5)	Deploy Container	Forge Web Credentials (0/2)	Cloud Storage Object Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Endpoint Denial of Service (0/4)
Search Closed Sources (0/2)	Obtain Capabilities (0/7)	Replication Through Removable Media	Native API	Create Account (0/3)	Create or Modify System Process (0/5)	Direct Volume Access	Input Capture (0/4)	Container and Resource Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Financial Theft
Search Open Technical Databases (0/5)	Stage Capabilities (0/6)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/5)	Create or Modify System Process (0/5)	Domain or Tenant Policy Modification (0/2)	Domain or Tenant Policy Modification (0/2)	Modify Authentication Process (0/9)	Debugger Evasion	Taint Shared Content	Data from Configuration Repository (0/2)	Fallback Channels	Exfiltration Over Web Service (0/4)	Firmware Corruption
Search Open Websites/Domains (0/3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (0/16)	File and Directory Permissions Modification (0/2)	Exploitation for Defense Evasion (0/2)	Multi-Factor Authentication Interception	Device Driver Discovery	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Ingress Tool Transfer	Scheduled Transfer	Resource Hijacking
Search Victim-Owned Websites		Valid Accounts (0/4)	Shared Modules	External Remote Services	Escape to Host	Hide Artifacts (0/12)	Multi-Factor Authentication Request Generation	File and Directory Discovery		Data from Local System	Multi-Stage Channels	Transfer Data to Cloud Account	Service Stop
			Software Deployment Tools	Hijack Execution Flow (0/13)	Exploitation for Privilege Escalation (0/13)	Hijack Execution Flow (0/13)	Network Sniffing (0/8)	Group Policy Discovery		Data from Network Shared Drive	Non-Application Layer Protocol		System Shutdown/Reboot
			System Services (0/2)	Implant Internal Image (0/11)	Impersonation	Impair Defenses (0/11)	OS Credential Dumping (0/8)	Log Enumeration		Data from Removable Media	Non-Standard Port		
			User Execution (0/3)	Modify Authentication Process (0/9)	Process Injection	Indirect Command	Steal or Forge	Network Service Discovery		Data Staged (0/2)	Protocol Tunneling		
			Windows Management Instrumentation					Network Share Discovery		Email Collection	Proxy (0/4)		
								Network Sniffing			Remote Access Software		
								Password Policy Discovery			Traffic Signaling		

Framework Components



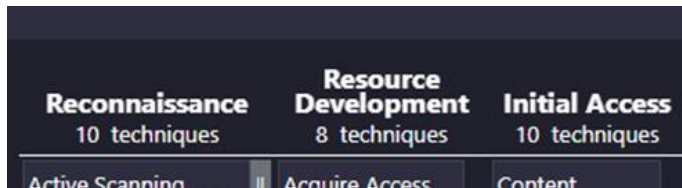
New Tab
For uh new
tabs...



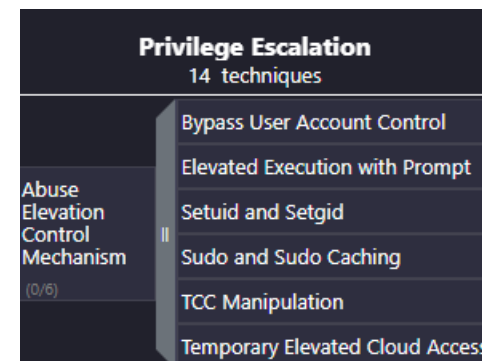
Matrix Control
Plane
Makes it
“**PRETTY**”

well maybe
not pretty...

TTPs: Threats, Tactics, Procedures



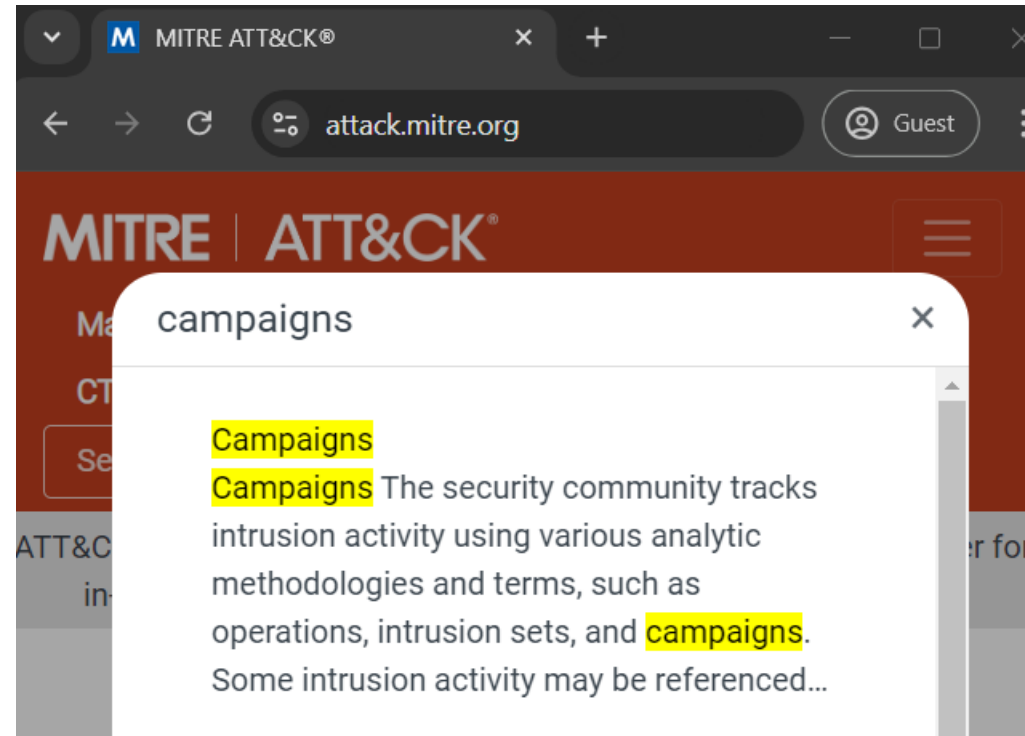
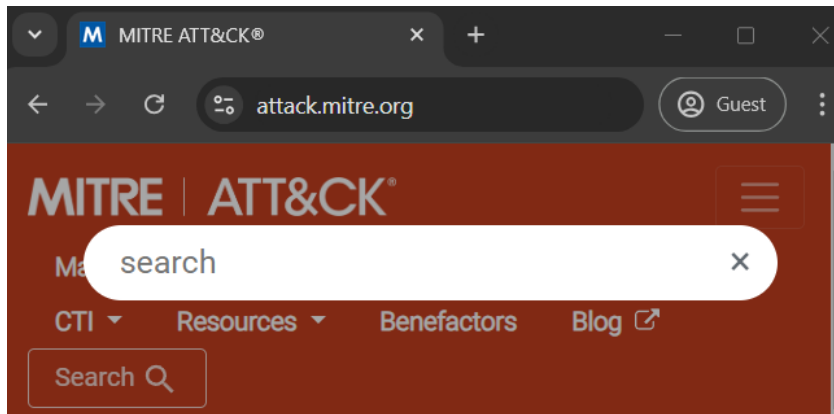
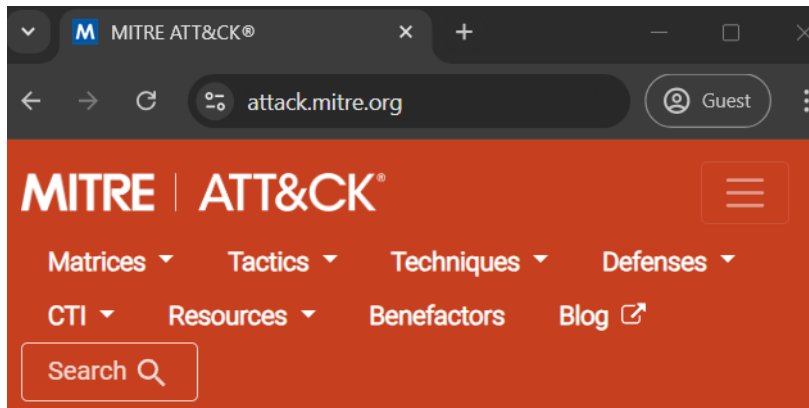
Attack
Tactics
The “**WHY**”



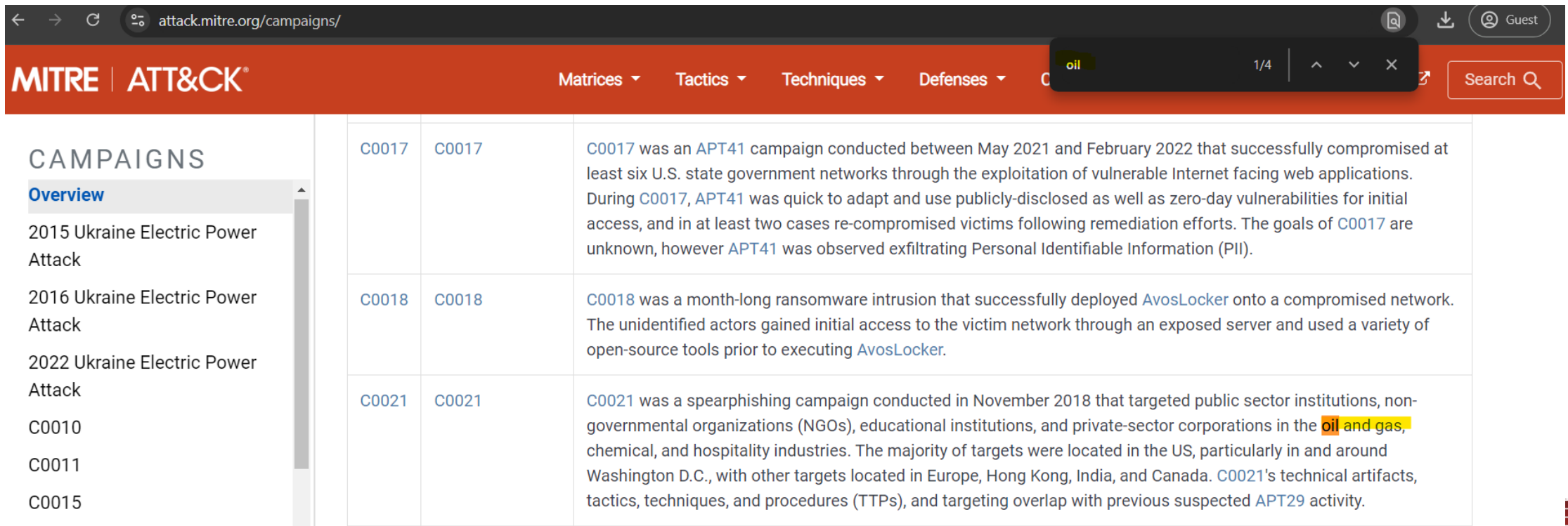
Attack
Techniques
The
“**HOWS**”

Select Your Model Context

- We will select a couple campaigns that focus on petroleum industry because this is HOUSTON. Here's how:



Quick Search (Yes I know I can use “Search”) Ctrl-f is so much better...



The screenshot shows the MITRE ATT&CK website with a search for 'oil' performed using a browser's Ctrl-F function. The search results are displayed in a table with three columns: ID, Name, and Description. The search bar at the top right shows 'oil' and a search icon. The table lists three campaigns: C0017, C0018, and C0021. The description for C0021 highlights 'oil and gas' in yellow.

ID	Name	Description
C0017	C0017	C0017 was an APT41 campaign conducted between May 2021 and February 2022 that successfully compromised at least six U.S. state government networks through the exploitation of vulnerable Internet facing web applications. During C0017, APT41 was quick to adapt and use publicly-disclosed as well as zero-day vulnerabilities for initial access, and in at least two cases re-compromised victims following remediation efforts. The goals of C0017 are unknown, however APT41 was observed exfiltrating Personal Identifiable Information (PII).
C0018	C0018	C0018 was a month-long ransomware intrusion that successfully deployed AvosLocker onto a compromised network. The unidentified actors gained initial access to the victim network through an exposed server and used a variety of open-source tools prior to executing AvosLocker.
C0021	C0021	C0021 was a spearphishing campaign conducted in November 2018 that targeted public sector institutions, non-governmental organizations (NGOs), educational institutions, and private-sector corporations in the oil and gas, chemical, and hospitality industries. The majority of targets were located in the US, particularly in and around Washington D.C., with other targets located in Europe, Hong Kong, India, and Canada. C0021's technical artifacts, tactics, techniques, and procedures (TTPs), and targeting overlap with previous suspected APT29 activity.

Campaigns/Threat Actors Selected

Home > Campaigns > Night Dragon

Night Dragon

Night Dragon was a cyber espionage campaign that targeted oil, energy, and petrochemical companies, along with individuals and executives in Kazakhstan, Taiwan, Greece, and the United States. The unidentified threat actors searched for information related to oil and gas field production systems, financials, and collected data from SCADA systems. Based on the observed techniques, tools, and network activities, security researchers assessed the campaign involved a threat group based in China.^[1]

Techniques Used

Domain	ID	Name
Enterprise	T1583 .004	Acquire Infrastructure: S
Enterprise	T1071 .001	Application Layer Protoc

Home > Campaigns > Operation Dust Storm

Operation Dust Storm

Operation Dust Storm was a long-standing persistent cyber espionage campaign that targeted multiple industries in Japan, South Korea, the United States, Europe, and several Southeast Asian countries. By 2015, the Operation Dust Storm threat actors shifted from government and defense-related intelligence targets to Japanese companies or Japanese subdivisions of larger foreign organizations supporting Japan's critical infrastructure, including electricity generation, oil and natural gas, finance, transportation, and construction.^[1]

Operation Dust Storm threat actors also began to use Android backdoors in their operations by 2015, with all identified victims at the time residing in Japan or South Korea.^[1]

Techniques Used

Domain	ID	Name	Use
Enterprise	T1583 .001	Acquire Infrastructure: Domains	For Operation Dust Storm, the threat actors established domains as part of their operational infrastructure. ^[1]

Home > Campaigns > C0021

C0021

C0021 was a spearphishing campaign conducted in November 2018 that targeted public sector institutions, non-governmental organizations (NGOs), educational institutions, and private-sector corporations in the oil and gas, chemical, and hospitality industries. The majority of targets were located in the US, particularly in and around Washington D.C., with other targets located in Europe, Hong Kong, India, and Canada. C0021's technical artifacts, tactics, techniques, and procedures (TTPs), and targeting overlap with previous suspected APT29 activity.^{[1][2]}

ID: C0021
First Seen: November 2018 ^{[2][1]}
Last Seen: November 2018 ^{[2][1]}
Version: 1.0
Created: 15 March 2023
Last Modified: 05 April 2023

Version Permalink

ATT&CK® Navigator Layers

s registered domains for use in C2.^[2]
tors used HTTP for some of their C2 communications.^[2]

ID: C0016
First Seen: January 2010 ^[1]
Last Seen: February 2016 ^[1]
Version: 1.1
Created: 29 September 2022
Last Modified: 11 April 2024

Version Permalink

ATT&CK® Navigator Layers



Download the Campaign Data for Each

age campaign that targeted
; and several Southeast Asian
from government and defense-
bdivisions of larger foreign
ectricity generation, oil and

doors in their operations by
th Korea.^[1]

ID: C0016
First Seen: January 2010 ^[1]
Last Seen: Enterprise Layer
Version: 1.1 **download**
Created: 29
Last Modified: Mobile Layer
download
view

ATT&CK® Navigator Layers ▾

cal
United
production
hniques,
at group

ID: C0002
First Seen: November 2009 ^[1]
Last Seen: February 2011 ^[1]
Version: 1.1
Created: 08 September 2022
Last Modified: 11 April 2024

Version Permalink

threat actors purchased hoste
2.^[1]

ATT&CK® Navigator Layers ▾
Enterprise Layer
download
view

ID: C0021
First Seen: November 2018 ^[2]^[1]
Last Seen: November 2018 ^[2]^[1]
Version: 1.0
Created: 15 March 2023
Last Modified: 05 April 2023

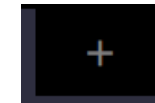
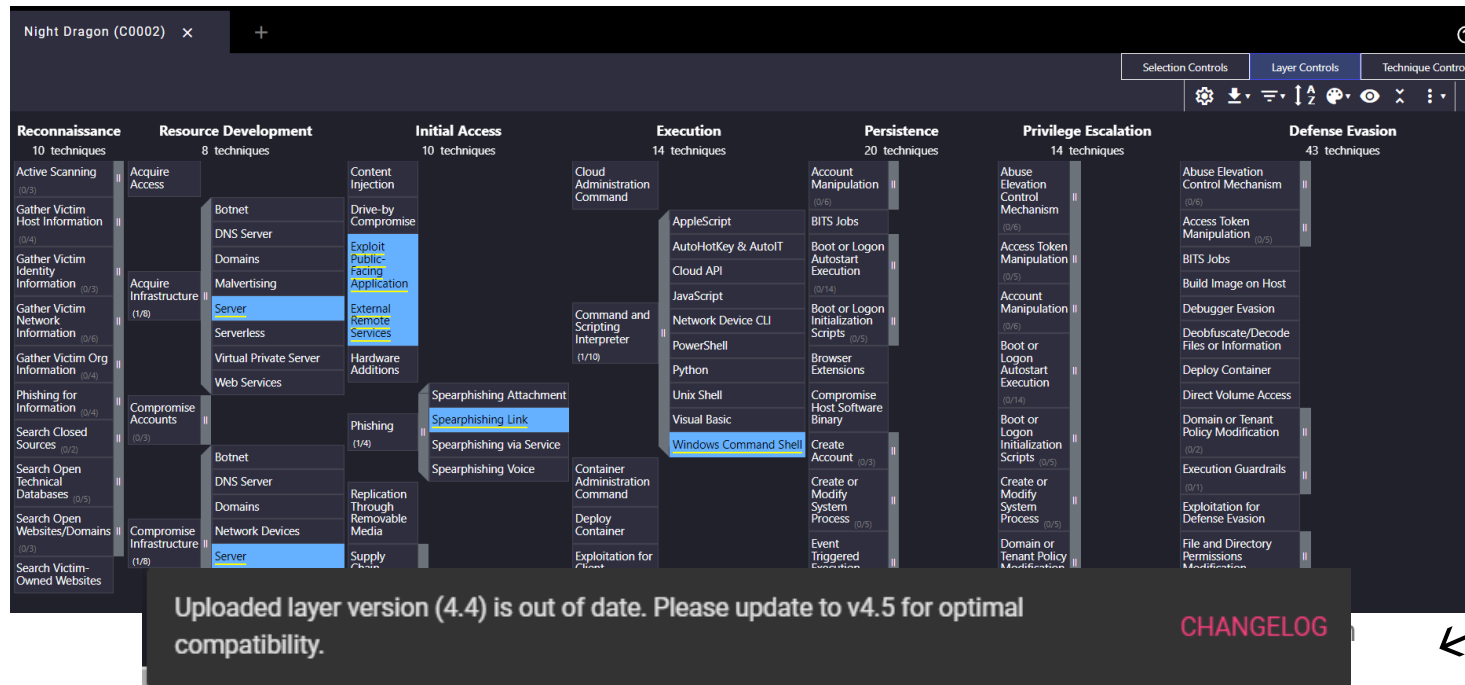
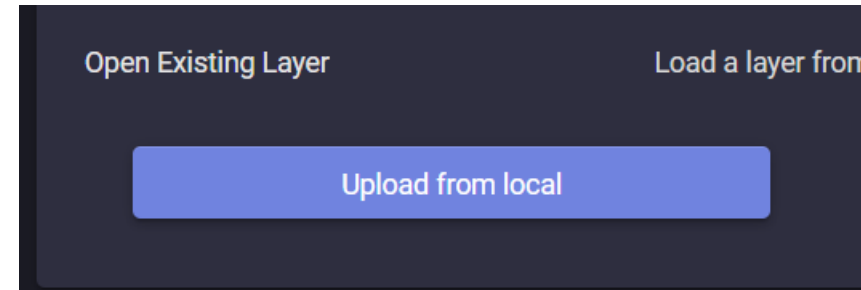
Version Permalink

stered domains for u
1

ATT&CK® Navigator Layers ▾
Enterprise Layer
download
view



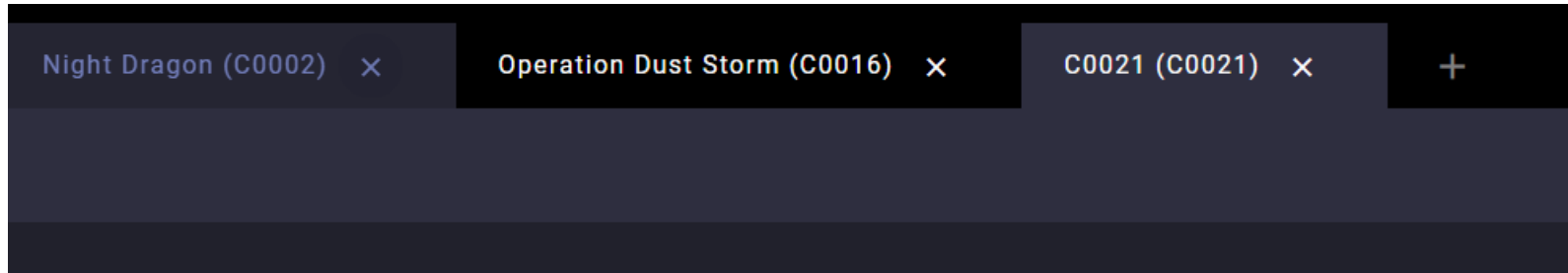
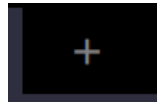
Import the Campaign Data for Each



← Hey MITRE: CHANGELOG Error with no context...



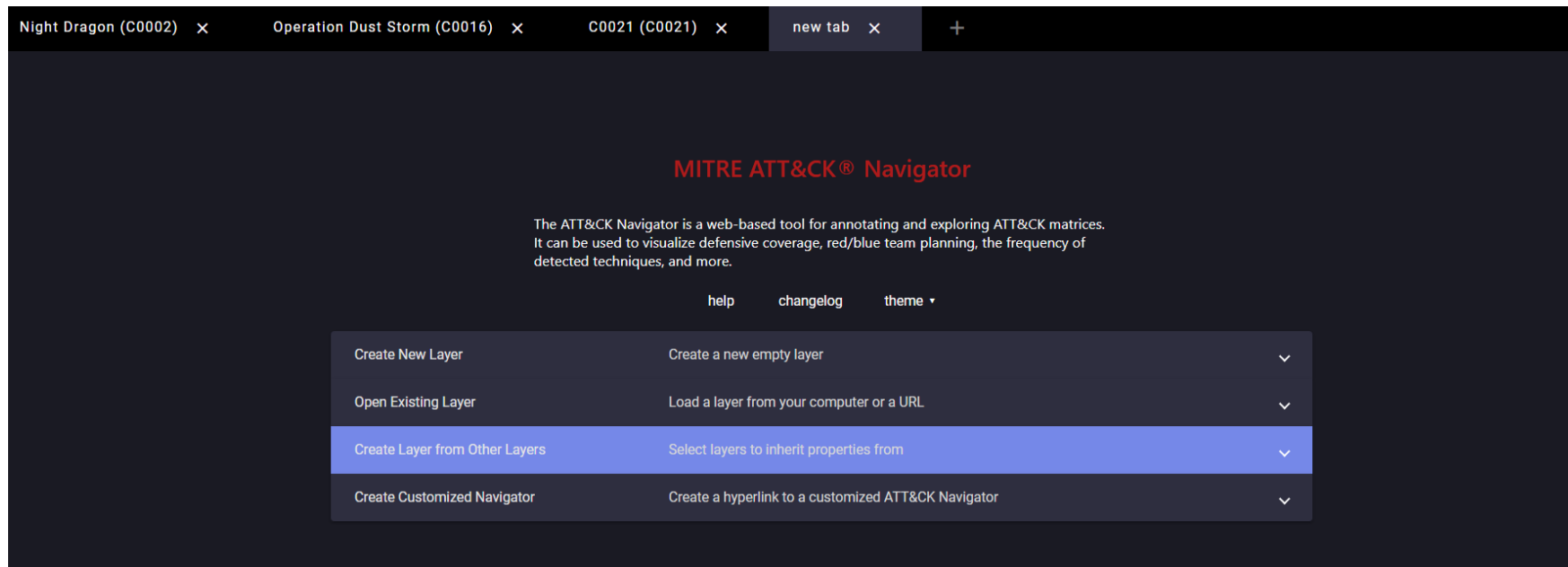
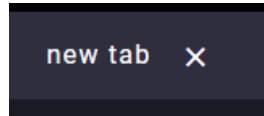
Once Campaign Data is Imported



Night Dragon (C0002) × Operation Dust Storm (C0016) × C0021 (C0021) × +														Selection Controls Layer Controls Technique Controls		
Reconnaissance 10 techniques Resource Development 8 techniques Initial Access 10 techniques Execution 14 techniques Persistence 20 techniques Privilege Escalation 14 techniques Defense Evasion 43 techniques Credential Access 17 techniques Discovery 32 techniques Lateral Movement 9 techniques Collection 17 techniques Command and Control 18 techniques Exfiltration 9 techniques																
Active Scanning (0/4)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (0/6)	Abuse Elevation Control Mechanism (0/6)	Abuse Elevation Control Mechanism (0/6)	Adversary-in-the-Middle (0/4)	Account Discovery (0/4)	Exploitation of Remote Services (0/4)	Adversary-in-the-Middle (0/4)	DNS	Automated Exfiltration (0/1)				
Gather Victim Host Information (0/4)	Botnet	Drive-by Compromise		BITS Jobs (0/6)	Access Token Manipulation (0/6)	Access Token Manipulation (0/6)	Brute Force (0/4)	Application Window Discovery (0/4)	Internal Spearphishing (0/4)	Archive Collected Data (0/3)	File Transfer Protocols (0/1)	Data Transfer Size Limits (0/1)				
Gather Victim Identity Information (0/3)	DNS Server	Exploit Public-Facing Application		Boot or Logon Autostart Execution (0/14)	Build Image on Host (0/14)	Build Image on Host (0/14)	Credentials from Password Stores (0/6)	Browser Information Discovery (0/4)	Lateral Tool Transfer (0/4)	Audio Capture (0/4)	Mail Protocols (0/1)					
Gather Victim Network Information (0/6)	Acquire Infrastructure (1/6)	Malvertising		Cloud API (0/14)	Debugger Evasion (0/4)	Debugger Evasion (0/4)	Exploitation for Credential Access (0/4)	Cloud Infrastructure Discovery (0/4)	Remote Service Session Hijacking (0/2)	Automated Collection (0/3)	Web Protocols (0/1)	Exfiltration Over Alternative Protocol (0/3)				
Gather Victim Remote Information (0/6)	Server	External Remote Services	Command and Scripting Interpreter (1/6)	JavaScript (0/14)	Account Manipulation (0/6)	Account Manipulation (0/6)	Deobfuscate/Decode Files or Information (0/4)	Cloud Service Dashboard (0/4)	Remote Services (0/6)	Browser Session Hijacking (0/4)	Content Injection (0/4)	Exfiltration Over C2 Channel (0/1)				
Gather Victim Org Information (0/4)	Serverless	Hardware Additions		Network Device CLI (0/14)	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	Deploy Container (0/14)	Cloud Service Discovery (0/4)	Replication Through Removable Media (0/4)	Data Encoding (0/2)	Data Obfuscation (0/2)	Exfiltration Over Other Network Medium (0/1)				
Phishing for Information (0/4)	Virtual Private Server			PowerShell (0/14)	Browser Extensions (0/14)	Domain or Tenant Policy Modification (0/2)	Direct Volume Access (0/14)	Container and Resource Discovery (0/2)	Software Deployment Tools (0/4)	Data from Cloud Storage (0/4)	Dynamic Resolution (0/3)	Exfiltration Over Physical Medium (0/1)				
Search Closed Sources (0/2)	Web Services	Phishing (1/4)	Spearphishing Attachment	Python (0/14)	Compromise Host Software Binary (0/14)	Execution Guardrails (0/2)	Forge Web Credentials (0/2)	Debugger Evasion (0/4)	Taint Shared Content (0/4)	Encrypted Channel (0/2)	Asymmetric Cryptography (0/1)					
Search Open Technical Databases (0/3)	Compromise Accounts (0/2)	Spearphishing via Service	Spearphishing Link	Unix Shell (0/14)	Create Account (0/2)	Exploitation for Defense Evasion (0/2)	Input Capture (0/4)	Device Driver Discovery (0/4)	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/4)	Symmetric Cryptography (0/1)					
Search Open Websites/Domains (0/3)	Botnet	Spearphishing Voice		Visual Basic (0/14)	Create or Modify System Process (0/2)	File and Directory Permissions Modification (0/2)	Modify Authentication Process (0/4)	Domain Trust Discovery (0/4)	Group Policy Discovery (0/4)	Data from Local System (0/4)	Ingress Tool Transfer (0/4)					
Search Victim-Owned Websites (0/3)	DNS Server	Replication Through Removable Media (0/4)		Windows Command Shell (0/2)	Event Triggered Execution (0/2)	Hide Artifacts (0/12)	Multi-Factor Authentication Request Generation (0/4)	Log Enumeration (0/4)	Network Service Discovery (0/4)	Data from Network Shared Drive (0/4)	Transfer Data to Cloud Account (0/4)					
	Network Devices (0/3)	Supply Chain Compromise (0/3)	Container Administration Command		External Remote Services (0/14)	Hijack Execution Flow (0/12)	Multi-Factor Authentication Request Generation (0/4)	Network Sniffing (0/4)	Network Share Discovery (0/4)	Data from Removable Media (0/4)	Non-Application Layer Protocol (0/4)					
	Server	Trusted Relationship (0/3)	Deploy Container		Hijack Execution Flow (0/14)	Impersonation (0/12)	Multi-Factor Authentication Request Generation (0/4)	OS Credential Dumping (0/2)	Network Sniffing (0/4)	Data Staged (0/2)	Protocol Tunneling (0/4)					
	Serverless	Valid Accounts (0/4)	Exploitation for Client Execution (0/14)		Event Triggered Execution (0/14)	Indicator Removal (0/2)	Steal or Forge Authentication Certificates (0/4)	Steal or Forge Authentication Certificates (0/4)	Peripheral Device Discovery (0/4)	Email Collection (0/4)	Proxy (0/4)					
	Virtual Private Server		Inter-Process Communication (0/14)		Implant Internal Image (0/14)	Masquerading (0/12)	Steal or Forge									
	Web Services		Native API (0/14)		Modify Authentication Process (0/14)	Masquerading (0/12)										
	Develop Capabilities (0/4)		Scheduled Task/Job (0/14)		Office Application Startup (0/14)	Masquerading (0/12)										
	Establish Accounts (0/3)		Serverless Execution (0/14)		Software Deployment Tools (0/14)	Masquerading (0/12)										
	Artificial Intelligence		Shared Modules (0/14)			Masquerading (0/12)										
	Code Signing Certificates		Software Deployment Tools (0/14)			Masquerading (0/12)										
	Digital Certificates					Masquerading (0/12)										
	Obtain Capabilities					Masquerading (0/12)										
	Exploits					Masquerading (0/12)										



Create a New Layer From Other Layers



Select Enterprise ATT&CK MITRE ATT&CK v15

Create Layer from Other Layers

domain*

Enterprise ATT&CK MITRE ATT&CK v15

Enterprise ATT&CK MITRE ATT&CK v10

Enterprise ATT&CK MITRE ATT&CK v11

Enterprise ATT&CK MITRE ATT&CK v12

Enterprise ATT&CK MITRE ATT&CK v13

Enterprise ATT&CK MITRE ATT&CK v14

Enterprise ATT&CK MITRE ATT&CK v15

Select layers to inherit properties from

Select the domain for the new layer. Only layers of the same domain and version can be merged.

Use constants (numbers) and layer variables (yellow, above) to write an expression for the initial value of scores in the new layer. A full list of supported operations can be found [here](#) . Leave blank to initialize scores to 0. Here's a list of available layer variables:

- **a** (Night Dragon (C0002))
- **b** (Operation Dust Storm (C0016))
- **c** (C0021 (C0021))

Select which layer to import the scoring gradient from. Leave blank to initialize with the default scoring gradient.

A+B+C no this isn't Pythagorean or ABC conjecture... I promise....

The screenshot shows the MITRE ATT&CK Navigator interface with three tabs: "Night Dragon (C0002)", "Operation Dust Storm (C0016)", and "C0021 (C0021)". The "Create Layer from Other Layers" dialog is open, allowing a new layer to be created by inheriting properties from existing layers.

Create Layer from Other Layers

domain*
Enterprise ATT&CK MITRE ATT&CK v

score expression
a+b+c

gradient

coloring

comments

links

metadata

states

filters

legend

Create layer

Select layers to inherit properties from

Select the domain for the new layer. Only layers of the same domain and version can be merged.

Use constants (numbers) and layer variables (yellow, above) to write an expression for the initial value of scores in the new layer. A full list of supported operations can be found [here](#). Leave blank to initialize scores to 0. Here's a list of available layer variables:

- (Night Dragon (C0002))
- (Operation Dust Storm (C0016))
- (C0021 (C0021))

Select which layer to import the scoring gradient from. Leave blank to initialize with the default scoring gradient.

Select which layer to import manually assigned colors from. Leave blank to initialize with no colors.

Select which layer to import comments from. Leave blank to initialize with no comments.

Select which layer to import technique links from. Leave blank to initialize without links.

Select which layer to import technique metadata from. Leave blank to initialize without metadata.

Select which layer to import enabled/disabled states from. Leave blank to initialize all to enabled.

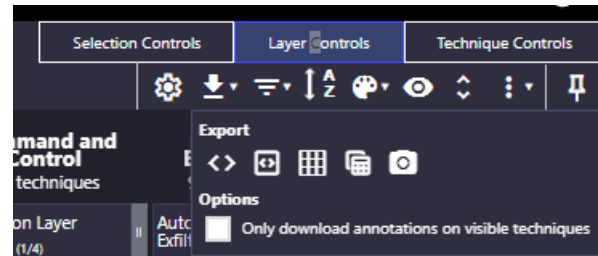
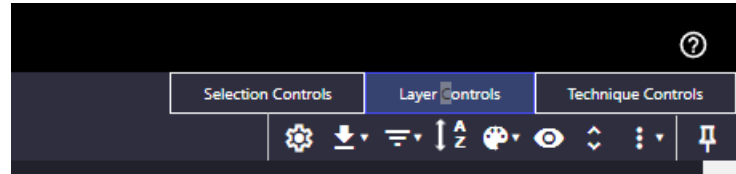
Select which layer to import filters from. Leave blank to initialize with no filters.

Select which layer to import the legend from. Leave blank to initialize with an empty legend.

Comprehensive threat model of scenarios based on known campaigns of threat actors targeting the Petroleum Industries... VERY EASY...to see, not to say.

Night Dragon (C0002) × Operation Dust Storm (C0016) × C0021 (C0021) × layer by operation ×													
Selection Controls Layer Controls Technique Controls													
Reconnaissance 10 techniques Resource Development 8 techniques Initial Access 10 techniques Execution 14 techniques Persistence 20 techniques Privilege Escalation 14 techniques Defense Evasion 43 techniques Credential Access 17 techniques Discovery 32 techniques Lateral Movement 9 techniques Collection 17 techniques Command and Control 18 techniques Exfiltration 9 techniques Impact 14 techniques													
Active Scanning (0/2)	Acquire Access (2/8)	Content Injection (0/2)	Cloud Administration Command (4/10)	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/3)	Abuse Elevation Control Mechanism (0/5)	Adversary-in-the-Middle (0/3)	Account Discovery (0/8)	Exploitation of Remote Services (0/2)	Adversary-in-the-Middle (0/3)	Application Layer Protocol (1/4)	Automated Exfiltration (0/1)	Account Access Removal (0/2)
Gather Victim Host Information (0/4)	Acquire Infrastructure (2/8)	Drive-by Compromise (0/2)	Command and Scripting Interpreter (4/10)	BITS Jobs (0/5)	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (1/4)	Application Window Discovery (0/2)	Internal Spearphishing (0/2)	Archive Collected Data (0/2)	Communication Through Removable Media (0/2)	Data Transfer Size Limits (0/2)	Data Destruction (0/2)
Gather Victim Identity Information (0/3)	Compromise Accounts (0/2)	Exploit Public-Facing Application (0/2)	Container Administration Command (0/2)	Boot or Logon Autostart Execution (0/14)	Account Manipulation (0/5)	Account Manipulation (0/5)	Credentials from Password Stores (0/2)	Browser Information Discovery (0/2)	Remote Service Session Hijacking (0/2)	Audio Capture (0/2)	Content Injection (0/2)	Exfiltration Over Alternative Protocol (0/2)	Data Encrypted for Impact (0/2)
Gather Victim Network Information (0/6)	Compromise Infrastructure (2/8)	External Remote Services (0/2)	Deploy Container (0/2)	Boot or Logon Autostart Execution (0/2)	Boot or Logon Autostart Execution (0/2)	Boot or Logon Autostart Execution (0/2)	Exploitation for Credential Access (0/2)	Cloud Infrastructure Discovery (0/2)	Remote Services (0/2)	Automated Collection (0/2)	Data Encoding (0/2)	Exfiltration Over C2 Channel (0/2)	Data Manipulation (0/2)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Additions (0/2)	Phishing (2/4)	Browser Extensions (0/14)	Build Image on Host (0/14)	Build Image on Host (0/14)	Forward Authentication (0/2)	Cloud Service Dashboard (0/2)	Replication Through Removable Media (0/2)	Browser Session Hijacking (0/2)	Data Obfuscation (0/2)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (1/8)	Establish Accounts (1/8)	Replication Through Removable Media (0/2)	Exploitation for Client Execution (0/2)	Compromise Host Software Binary (0/5)	Debugger Evasion (0/2)	Debugger Evasion (0/2)	Deobfuscate/Decode Files or Information (1/14) (1/2) Score: 2	Cloud Service Discovery (0/2)	Software Deployment Tools (0/2)	Clipboard Data (0/2)	Dynamic Resolution (0/2)	Exfiltration Over Physical Medium (0/2)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Obtain Capabilities (2/7)	Supply Chain Compromise (0/2)	Inter-Process Communication (0/2)	Create Account (0/3)	Direct Volume Access (0/2)	Direct Volume Access (0/2)	Multi-Factor Authentication Process (0/2)	Container and Resource Discovery (0/2)	Taint Shared Content (0/2)	Data from Cloud Storage (0/2)	Encrypted Channel (1/2)	Exfiltration Over Web Service (0/4)	Endpoint Denial of Service (0/2)
Search Open Technical Databases (0/3)	Stage Capabilities (1/6)	Trusted Relationship (0/5)	Native API (0/5)	Create or Modify System Process (0/5)	Domain or Tenant Policy Modification (0/2)	Domain or Tenant Policy Modification (0/2)	Multi-Factor Authentication Interception (0/2)	Debugger Evasion (0/2)	Use Alternate Authentication Material (1/4)	Data from Configuration Repository (0/2)	Failback Channels (0/2)	Exfiltration Over Physical Medium (0/2)	Financial Theft (0/2)
Search Open Websites/Domains (0/3)	Valid Accounts (1/4)	Valid Accounts (1/4)	Scheduled Task/Job (0/5)	Create or Modify System Process (0/5)	Event Triggered Execution (0/16)	Event Triggered Execution (0/16)	Multi-Factor Authentication Request Generation (0/2)	Device Driver Discovery (0/2)		Data from Information Repositories (0/3)	Ingress Tool Transfer (0/2)	Exfiltration Over Web Service (0/4)	Firmware Corruption (0/2)
Search Victim-Owned Websites (0/3)			Serverless Execution (0/2)	Event Triggered Execution (0/16)	Escape to Host (0/2)	Escape to Host (0/2)	Network Sniffing (0/12)	Domain Trust Discovery (0/2)		Data from Local System (0/2)	Non-Application Layer Protocol (0/2)	Scheduled Transfer (0/2)	Inhibit System Recovery (0/2)
			Software Deployment Tools (0/2)	Hijack Execution Flow (0/13)	Exploitation for Defense Evasion (0/2)	Exploitation for Defense Evasion (0/2)	OS Credential Dumping (1/8)	Group Policy Discovery (0/2)		Data from Network Shared Drive (0/2)	Multi-Stage Channels (0/2)	Transfer Data to Cloud Account (0/2)	Resource Hijacking (0/2)
			System Services (0/2)	Implant Internal Image (0/13)	File and Directory Permissions Modification (0/2)	File and Directory Permissions Modification (0/2)	Steal Application Access Token (0/2)	Log Enumeration (0/2)		Data from Removable Media (0/2)	Non-Standard Port (0/2)	Service Stop (0/2)	System Shutdown/Reboot (0/2)
			User Execution (2/3)	Hijack Execution Flow (0/13)	Hide Artifacts (0/12)	Hide Artifacts (0/12)	Steal or Forge Kerberos Tickets (0/4)	Network Service Discovery (0/2)		Data Staged (1/2)	Protocol Tunneling (0/2)		
			Windows Management Instrumentation (0/2)	Modify Authentication Process (0/13)	Hijack Execution Flow (0/13)	Hijack Execution Flow (0/13)	Steal Web Session Cookie (0/2)	Network Share Discovery (0/2)		Email Collection (1/3)	Proxy (0/4)		
				Office Application Startup (0/12)	Impersonation (0/11)	Impersonation (0/11)	Unsecured Credentials (0/8)	Network Sniffing (0/2)		Input Capture (0/4)	Remote Access Software (0/2)		
				Power Settings (0/5)	Indicator Removal (0/9)	Indicator Removal (0/9)	Modify Authentication Process (0/5)	Password Policy Discovery (0/2)		Screen Capture (0/2)	Traffic Signaling (0/2)		
				Pre-OS Boot (0/5)	Scheduled Task/Job (0/5)	Scheduled Task/Job (0/5)	Modify Cloud Compute Infrastructure (0/5)	Peripheral Device Discovery (0/3)		Video Capture (0/2)	Web Service (0/2)		
				Scheduled Task/Job (0/5)	Valid Accounts (1/4)	Valid Accounts (1/4)	Modify Registry (0/2)	Permission Groups Discovery (0/3)					
				Server Software Component (0/2)			Modify System Image (0/2)	Process Discovery (0/2)					
				Traffic Signaling (0/2)			Network Boundary Bridging (0/1)	Query Registry (0/2)					
				Valid Accounts (1/4)			Obfuscated Files or Information (0/2)	Remote System Discovery (0/2)					
								Software Discovery (0/2)					
								System Information Discovery (0/2)					
								System Location Discovery (0/2)					
								System Network Configuration Discovery (0/2)					

But Brad You *Charismatic Gentleman*, Do I Have to Do This *Every Time*? **No...**



This Can Be Exported to the Following Formats:

- JSON
- Excel
- SVG

Reconnaissance											
A	B	C	D	E	F	G	H	I	J	K	L
1	Reconnaissance	Resource Development	Initial Access		Execution		Persistence		Privilege Escalation		Defense Evasion
2	Active Scanning	Acquire Access	Content Injection		Cloud Administration Command		Account Manipulation		Abuse Elevation Control Mechanism		Abuse Elevation Control Mechanism
3	Gather Victim Host Information	Acquire Infrastructure	Drive-by Compromise		Command and Scripting Interface		BITS Jobs		Access Token Manipulation		Access Token Manipulation
4	Gather Victim Identity Information	Bonnet	Exploit Public-Facing Application		AutoHotKey & AutoIT		Boot or Logon Autostart Execution		Account Manipulation		BITS Jobs
5	Gather Victim Network Information	Domains	External Remote Services		Cloud API		Boot or Logon Initialization Scripts		Boot or Logon Autostart Execution		Build Image on Host
6	Gather Victim Org Information	Malvertising	Hardware Additions		JavaScript		Browser Extensions		Boot or Logon Initialization Scripts		Debugger Evasion
7	Phishing for Information	Server	Phishing	Spearghishing Attachment		Network Device CLI	Compromise Host Software Binary		Create or Modify System Process		Deobfuscate/Decode Files or Information
8	Search Closed Sources	Services		Spearghishing Link		PowerShell	Create Account		Domain or Tenant Policy Modification		Deploy Container
9	Search Open Technical Database	Virtual Private Server		Spearghishing Voice		Python	Create or Modify System Process		Escape to Host		Direct Volume Access
10	Search Open Websites/Domain	Web Services				Unix Shell	Event Triggered Execution		Event Triggered Execution		Domain or Tenant Policy Modification
11	Search Victim-Owned Websites	Compromise Accounts	Replication Through Removable Media		Visual Basic		Visual Basic		Exploitation for Privilege Escalation		Execution Guards
12		Compromise Infrastructure	Supply Chain Compromise		Windows Command Shell		Windows Command Shell		Exploitation for Privilege Escalation		Exploitation for Privilege Escalation
13		Bonnet	Trusted Relationship		Container Administration Command		Implant Internal Image		Process Injection		File and Directory Permissions Modification
14		DNS Server	Valid Accounts	Cloud Accounts	Deploy Container		Modify Authentication Process		Scheduled Task/Job		Hide Artifacts
15		Domains		Default Accounts	Exploitation for Client Execution		Office Application Startup		Valid Accounts	Cloud Accounts	Impair Defenses
16		Network Devices		Domain Accounts	Inter-Process Communication		Power Settings		Default Accounts	Default Accounts	Disable or Modify Windows Firewall
17		Server		Local Accounts	Main API		Pre-OS Boot		Domain Accounts	Domain Accounts	Disable or Modify Windows Firewall
18		Services			Scheduled Task/Job		Scheduled Task/Job		Local Accounts	Local Accounts	Disable or Modify Windows Firewall
19		Virtual Private Server			Serverless Execution		Server Software Component				Disable Windows Defender
20		Web Services			Shared Modules		Windows Management Instrumentation				Downgrade Attack
21	Develop Capabilities				Software Deployment Tools						Impersonation
22	Establish Accounts	Artificial Intelligence			System Services						Indicator Removal
23	Obtain Capabilities	Code Signing Certificates			User Execution	Malicious File					Indirect Command Execution
24		Digital Certificates				Malicious Image					Masking
25		Exploits				Malicious Link					Modify Authentication Process
26		Malware									Modify Cloud Compute Infrastructure
27		Tool									Modify Registry
28		Vulnerabilities									Modify System Image
29		Drive-by Target									Network Boundary Bridging
30		Install Digital Certificate									Obfuscate Files or Information
31		Link Target									Binary Padding
32		SEO Poisoning									Command Obfuscation
33		Upload Malware									Compile After De
34		Upload Tool									Dynamic API Re
35											Embedded Pack
36											Encapsulate
37											Fileless Storage
38											HTML Smuggling
39											Indicator Removal
40											Link Icon Smugg
41											Software Packag
42											Stealthy Network
43											Stripped Payload
44											
45											
46											
47											
48											
49											
50											
51											
52											
53											
54											



Ok I Have The Data Now What?

- **This is how you Embark on a Journey....**
- Build scenarios to test and validate for your assets security posture
- Determine gaps in security controls
- Integrate this function into design of security controls
- Train your team
- Impress your friends!



www.VictimOfTechnology.com



Questions? Come up
front and see me!

Thanks for connecting with me!

- <https://linktr.ee/bradvoris>
- <https://www.linkedin.com/in/brad-voris/>
- <https://github.com/bvoris>
- <https://x.com/HMInfoSecViking>