Threat Hunting in the Energy and Utilities Sector using MITRE ATT&CK

Prepared by: Bamidele Olaleke

Date: 17th November, 2025

Project Overview

This project focuses on **proactive threat hunting** within the **Energy and Utilities industry**, leveraging the **MITRE ATT&CK framework** to identify and analyze Advanced Persistent Threat (APT) groups targeting the sector.

The objective was to:

- Identify **Energy and Utilities**-targeted APTs.
- Analyze their **Tactics, Techniques, and Procedures (TTPs)**.
- Visualize the threat landscape using **MITRE Navigator**.
- Compare APTs to find common attack vectors.

Objectives

1. Understand the MITRE ATT&CK framework and its application to real-world threat hunting.
2. Research APTs targeting the **Energy and Utilities** sector using SOCRadar Labs.
3. Map identified APTs to relevant TTPs in MITRE ATT&CK Navigator.
4. Perform a comparative analysis to highlight overlapping attack patterns.

Tools & Resources

- **SOCRadar Labs** – For retrieving **Energy and Utilities**-specific APT threat intelligence.
- **MITRE ATT&CK Navigator** – For mapping APT TTPs.

- **MITRE ATT&CK Framework** – For structured adversary behavior taxonomy.
- **OSINT Research** – To cross-check TTP details from open sources.

Project Steps

1. Understanding the MITRE ATT&CK Framework

- Studied the MITRE ATT&CK framework structure:
  - **Tactics** – The *why* of an attack (e.g., Initial Access, Persistence, Defense Evasion).
  - **Techniques** – The *how* of an attack (e.g., phishing, credential dumping).
  - **Procedures** – Real-world implementations of techniques.

2. Research APTs Peculiar to the Sector

- I Used SOCRadar Labs to identify **APT groups** targeting **Energy and Utilities Sector**.
- I found the following:

  Volt Typhoon – is a People's Republic of China PRC) state-sponsored actor that has been active since at least 2021 Primarily targetting critical infrastructure of organization in the US and its territories including GUAM. Volt Typhoon's targeting and pattern of behavior have been assessed as pre-positioning to enable lateral movement to operational technology

(OT) assets for potential destructive or disruptive attacks.

LYCEUM (Hexane) – is a cyber espionage threat group that has targeted oil & gas, telecommunications, aviation, and internet service provider organizations since at least 2017.

BITTER – is a suspected South Asian cyber espionage threat group that has been active since at least 2013. BITTER has targeted government, energy, and engineering organizations in Pakistan, China, Bangladesh, and Saudi Arabia

3. Highlight of the TTPs

- For each APT, identified their key TTPs from MITRE:

  1. (Volt Typhoon):
  T1078 – Valid Accounts
  T1589 – Gather Victim Identity Information
  T1190 – Exploit Public-Facing Application

2.LYCEUM (Hexane):
T1078 – Valid Accounts
T1110 – Password Spraying
T1579 – Lateral Tool Transfer

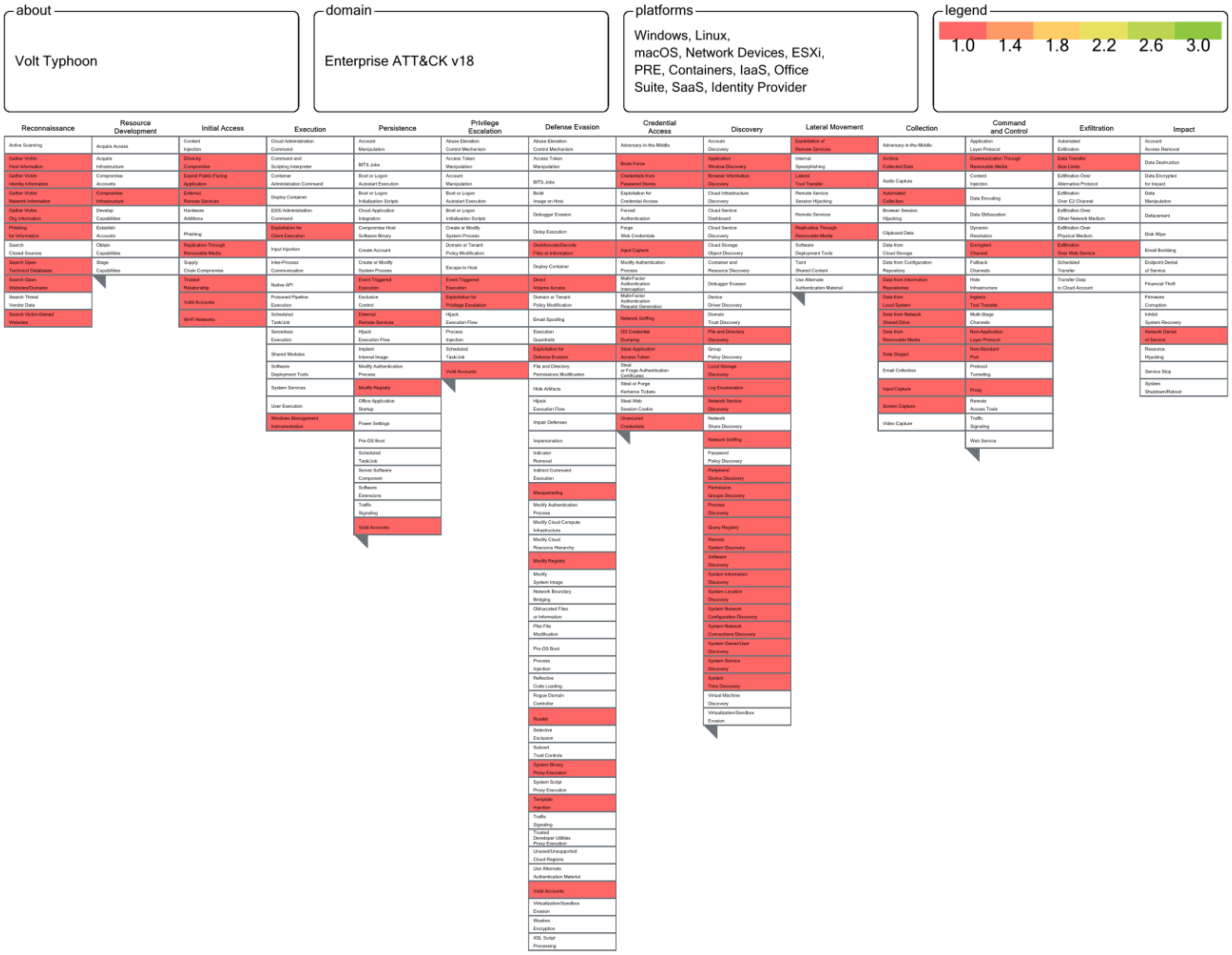
3. BITTER:
T1568 – Dynamics Resolution
T1573 – Encrypted Channel
T1203 – Exploitation for Client Execution

4. Map APTs to TTPs using MITRE Navigator

- I created an **Invidual layers** in MITRE navigator for each APT group
- Color-coded:
    - Red – Techniques confirmed in public reports.
    - Orange – Techniques suspected but unconfirmed.
    - Green – Techniques with existing detection measures.

I conducted an in-depth research on the threat group APTs (Advance Persistent group) common to a particular region and sectors to understand their TTPs (Tactics, Techniques and Procedure) activities and how they carry out their attack on the victims.
The screenshot below show main tactics and techniques

Volt Typhoon threat group tactics and techniques mapping.



about

Volt Typhoon

domain

Enterprise ATT&CK v18

platforms

Windows, Linux,
macOS, Network Devices, ESXi,
PRE, Containers, IaaS, Office
Suite, SaaS, Identity Provider

legend

1.0 1.4 1.8 2.2 2.6 3.0

Reconnaissance

- Active Scanning
- Gather Victim Host Information
- Gather Victim Identity Information
- Gather Victim Network Information
- Gather Victim Org Information
- Phishing for Information
- Search Closed Sources
- Search Open Technical Databases
- Search Open Websites/Domains
- Search Threat Vendor Data
- Search Victim-Owned Websites

Resource Development

- Acquire Access
- Acquire Infrastructure
- Compromise Accounts
- Compromise Infrastructure
- Develop Capabilities
- Establish Accounts
- Obtain Capabilities
- Stage Capabilities

Initial Access

- Content Injection
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing
- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts
- Wi-Fi Networks

Execution

- Cloud Administration Command
- Command and Scripting Interpreter
- Container Administration Command
- Deploy Container
- ESXi Administration Command
- Exploitation for Client Execution
- Input Injection
- Inter-Process Communication
- Native API
- Poisoned Pipeline Execution
- Scheduled Task/Job
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services
- User Execution
- Windows Management Instrumentation

Persistence

- Account Manipulation
- BITS Jobs
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Cloud Application Integration
- Compromise Host Software Binary
- Create Account
- Create or Modify System Process
- Event Triggered Execution
- Exclusive Control
- External Remote Services
- Hijack Execution Flow
- Implant Internal Image
- Modify Authentication Process
- Modify Registry
- Office Application Startup
- Power Settings
- Pre-OS Boot
- Scheduled Task/Job
- Server Software Component
- Software Extensions
- Traffic Signaling
- Valid Accounts

Privilege Escalation

- Abuse Elevation Control Mechanism
- Access Token Manipulation
- Account Manipulation
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Create or Modify System Process
- Domain or Tenant Policy Modification
- Escape to Host
- Event Triggered Execution
- Exploitation for Privilege Escalation
- Hijack Execution Flow
- Process Injection
- Scheduled Task/Job
- Valid Accounts

Defense Evasion

- Abuse Elevation Control Mechanism
- Access Token Manipulation
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Delay Execution
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain or Tenant Policy Modification
- Email Spoofing
- Execution Guardrails
- Exploitation for Defense Evasion
- File and Directory Permissions Modification
- Hide Artifacts
- Hijack Execution Flow
- Impair Defenses
- Impersonation
- Indicator Removal
- Indirect Command Execution
- Masquerading
- Modify Authentication Process
- Modify Cloud Compute Infrastructure
- Modify Cloud Resource Hierarchy
- Modify Registry
- Modify System Image
- Network Boundary Bridging
- Obfuscated Files or Information
- Plist File Modification
- Pre-OS Boot
- Process Injection
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- Selective Exclusion
- Subvert Trust Controls
- System Binary Proxy Execution
- System Script Proxy Execution
- Template Injection
- Traffic Signaling
- Trusted Developer Utilities Proxy Execution
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material
- Valid Accounts
- Virtualization/Sandbox Evasion
- Weaken Encryption
- XSL Script Processing

Credential Access

- Adversary-in-the-Middle
- Brute Force
- Credentials from Password Stores
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials
- Input Capture
- Modify Authentication Process
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets
- Steal Web Session Cookie
- Unsecured Credentials

Discovery

- Account Discovery
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Local Storage Discovery
- Log Enumeration
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery
- System Information Discovery
- System Location Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtual Machine Discovery
- Virtualization/Sandbox Evasion

Lateral Movement

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking
- Remote Services
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material

Collection

- Adversary-in-the-Middle
- Archive Collected Data
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Screen Capture
- Video Capture

Command and Control

- Application Layer Protocol
- Communication Through Removable Media
- Content Injection
- Data Encoding
- Data Obfuscation
- Dynamic Resolution
- Encrypted Channel
- Fallback Channels
- Hide Infrastructure
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy
- Remote Access Tools
- Traffic Signaling
- Web Service

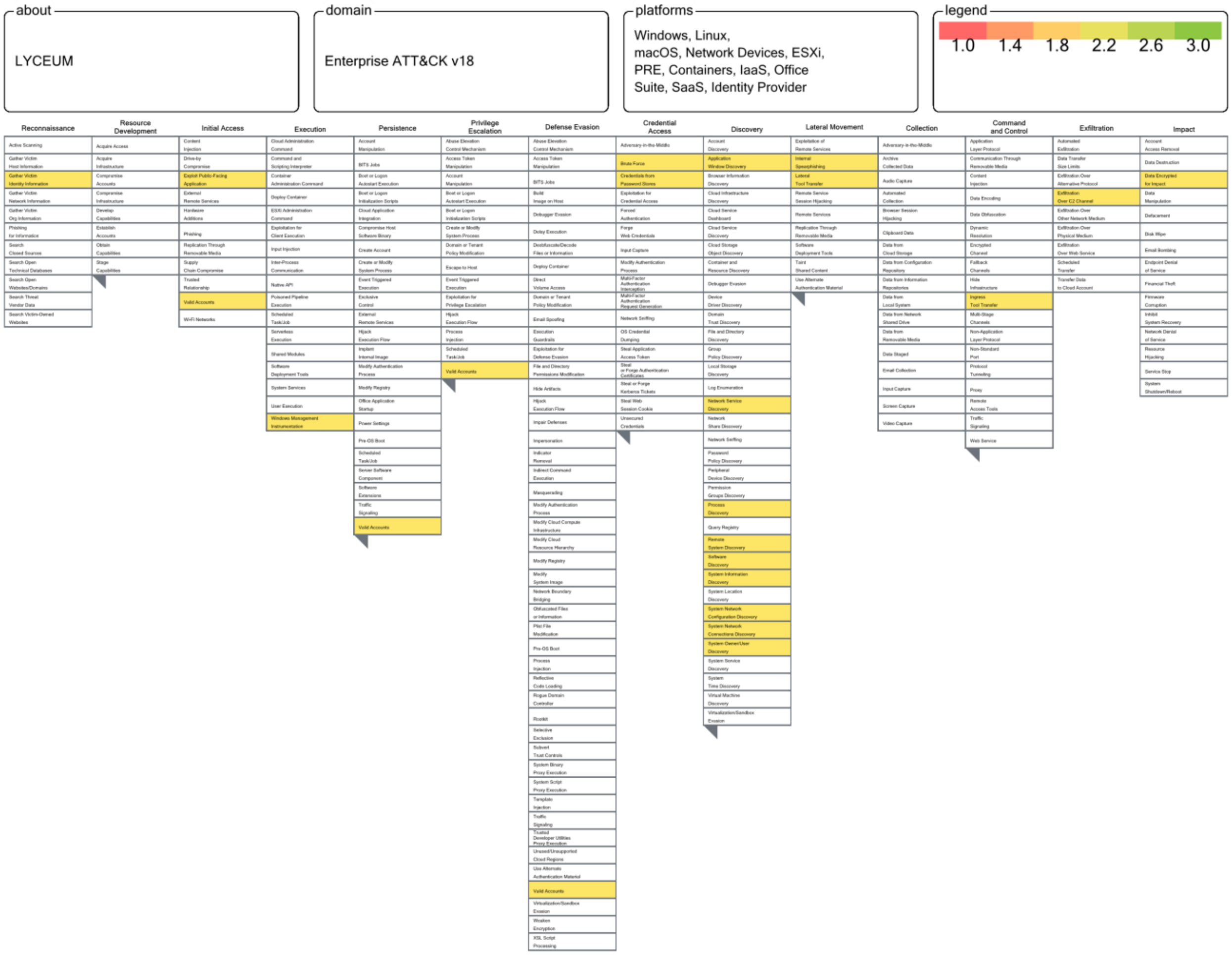
Exfiltration

- Automated Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Exfiltration Over Web Service
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation
- Defacement
- Disk Wipe
- Email Bombing
- Endpoint Denial of Service
- Financial Theft
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

LYCEUM threat group tactics and techniques mapping.



about
LYCEUM

domain
Enterprise ATT&CK v18

platforms
Windows, Linux,
macOS, Network Devices, ESXi,
PRE, Containers, IaaS, Office
Suite, SaaS, Identity Provider

legend
1.0 1.4 1.8 2.2 2.6 3.0

Reconnaissance
- Active Scanning
- Gather Victim Host Information
- Gather Victim Identity Information
- Gather Victim Network Information
- Gather Victim Org Information
- Phishing for Information
- Search Closed Sources
- Search Open Technical Databases
- Search Open Websites/Domains
- Search Threat Vendor Data
- Search Victim-Owned Websites

Resource Development
- Acquire Access
- Acquire Infrastructure
- Compromise Accounts
- Compromise Infrastructure
- Develop Capabilities
- Establish Accounts
- Obtain Capabilities
- Stage Capabilities

Initial Access
- Content Injection
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing
- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts
- Wi-Fi Networks

Execution
- Cloud Administration Command
- Command and Scripting Interpreter
- Container Administration Command
- Deploy Container
- ESXi Administration Command
- Exploitation for Client Execution
- Input Injection
- Inter-Process Communication
- Native API
- Poisoned Pipeline Execution
- Scheduled Task/Job
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services
- User Execution
- Windows Management Instrumentation

Persistence
- Account Manipulation
- BITS Jobs
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Cloud Application Integration
- Compromise Host Software Binary
- Create Account
- Create or Modify System Process
- Event Triggered Execution
- Exclusive Control
- External Remote Services
- Hijack Execution Flow
- Implant Internal Image
- Modify Authentication Process
- Modify Registry
- Office Application Startup
- Power Settings
- Pre-OS Boot
- Scheduled Task/Job
- Server Software Component
- Software Extensions
- Traffic Signaling
- Valid Accounts

Privilege Escalation
- Abuse Elevation Control Mechanism
- Access Token Manipulation
- Account Manipulation
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Create or Modify System Process
- Domain or Tenant Policy Modification
- Escape to Host
- Event Triggered Execution
- Exploitation for Privilege Escalation
- Hijack Execution Flow
- Process Injection
- Scheduled Task/Job
- Valid Accounts

Defense Evasion
- Abuse Elevation Control Mechanism
- Access Token Manipulation
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Delay Execution
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain or Tenant Policy Modification
- Email Spoofing
- Execution Guardrails
- Exploitation for Defense Evasion
- File and Directory Permissions Modification
- Hide Artifacts
- Hijack Execution Flow
- Impair Defenses
- Impersonation
- Indicator Removal
- Indirect Command Execution
- Masquerading
- Modify Authentication Process
- Modify Cloud Compute Infrastructure
- Modify Cloud Resource Hierarchy
- Modify Registry
- Modify System Image
- Network Boundary Bridging
- Obfuscated Files or Information
- Plist File Modification
- Pre-OS Boot
- Process Injection
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- Selective Exclusion
- Subvert Trust Controls
- System Binary Proxy Execution
- System Script Proxy Execution
- Template Injection
- Traffic Signaling
- Trusted Developer Utilities Proxy Execution
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material
- Valid Accounts
- Virtualization/Sandbox Evasion
- Weaken Encryption
- XSL Script Processing

Credential Access
- Adversary-in-the-Middle
- Brute Force
- Credentials from Password Stores
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials
- Input Capture
- Modify Authentication Process
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets
- Steal Web Session Cookie
- Unsecured Credentials

Discovery
- Account Discovery
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Local Storage Discovery
- Log Enumeration
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery
- System Information Discovery
- System Location Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtual Machine Discovery
- Virtualization/Sandbox Evasion

Lateral Movement
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking
- Remote Services
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material

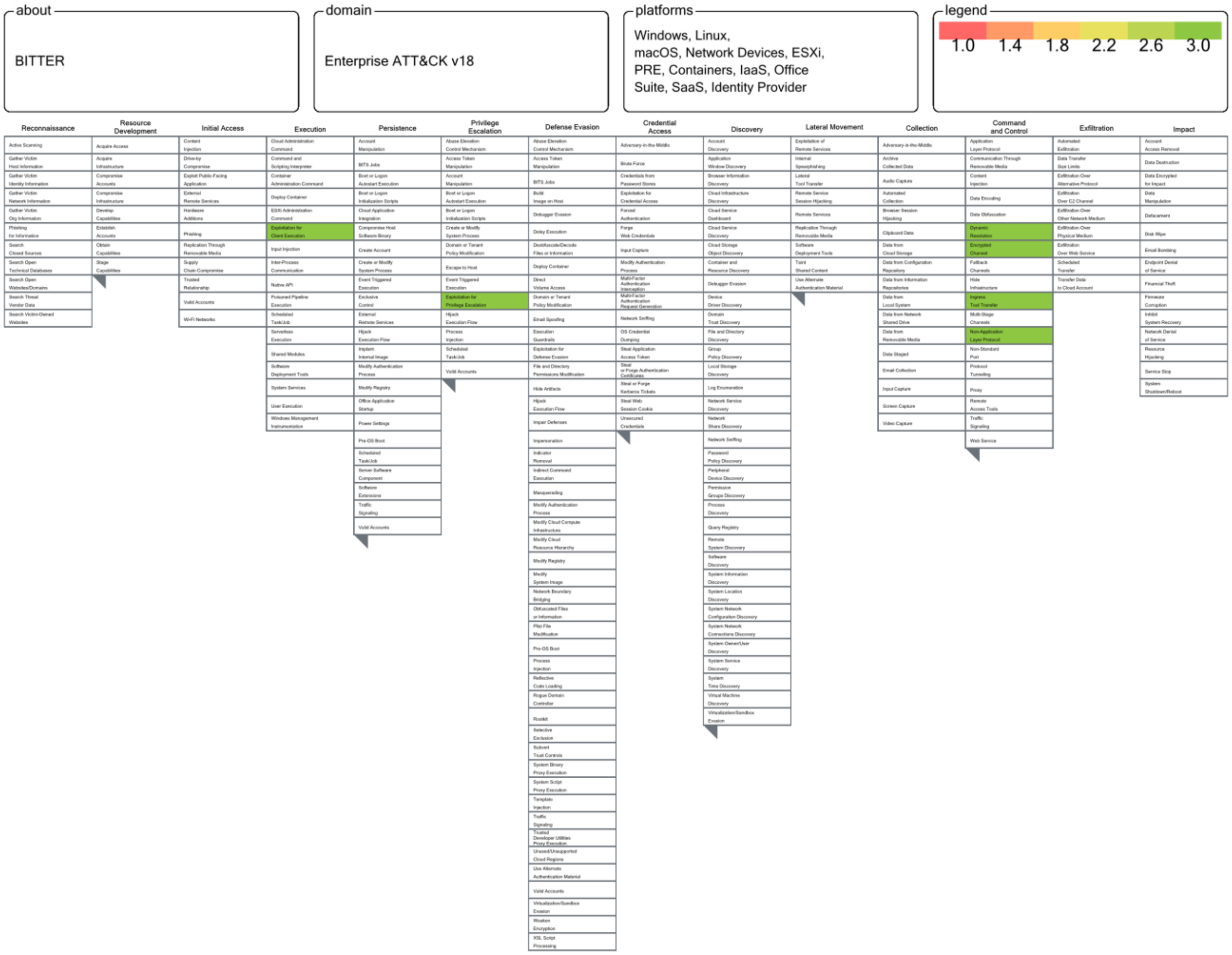
Collection
- Adversary-in-the-Middle
- Archive Collected Data
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Screen Capture
- Video Capture

Command and Control
- Application Layer Protocol
- Communication Through Removable Media
- Content Injection
- Data Encoding
- Data Obfuscation
- Dynamic Resolution
- Encrypted Channel
- Fallback Channels
- Hide Infrastructure
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy
- Remote Access Tools
- Traffic Signaling
- Web Service

Exfiltration
- Automated Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Exfiltration Over Web Service
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation
- Defacement
- Disk Wipe
- Email Bombing
- Endpoint Denial of Service
- Financial Theft
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

BITTER threat group tactics and techniques mapping.



about

BITTER

domain

Enterprise ATT&CK v18

platforms

Windows, Linux,
macOS, Network Devices, ESXi,
PRE, Containers, IaaS, Office
Suite, SaaS, Identity Provider

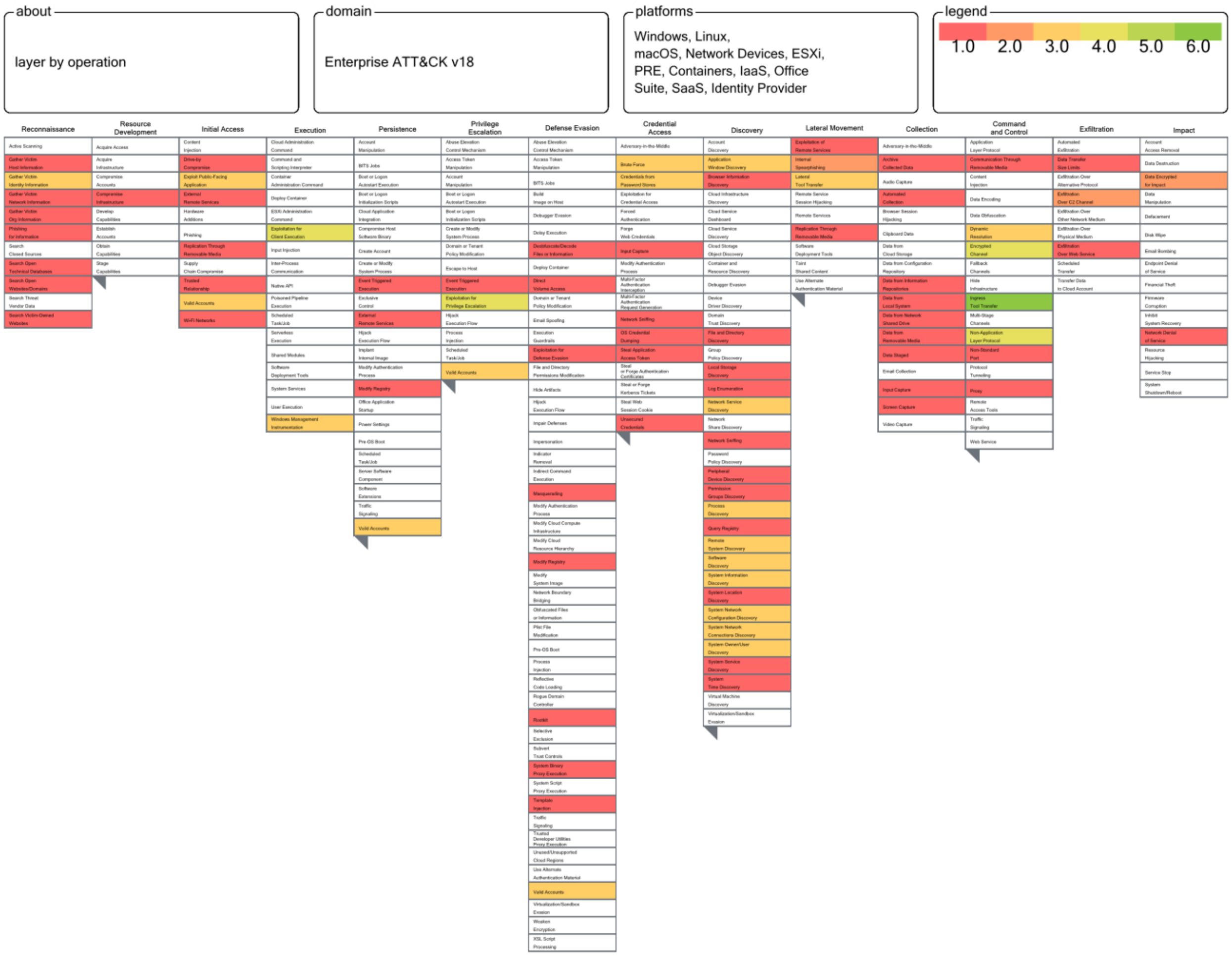
legend

1.0 1.4 1.8 2.2 2.6 3.0

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

5. Compare the APTs

- Imported all Three APT layers into a **combined Navigator view**.
- Noted **common techniques** across multiple APTs, such as:
  - T1573 – Encrypted Channel: Symmetric Cryptography
  - T1078 – Valid Accounts
  - T1068 – Exploitation for Privilege Escalation



about

layer by operation

domain

Enterprise ATT&CK v18

platforms

Windows, Linux,
macOS, Network Devices, ESXi,
PRE, Containers, IaaS, Office
Suite, SaaS, Identity Provider

legend

1.0 2.0 3.0 4.0 5.0 6.0

Reconnaissance

Active Scanning
Gather Victim Host Information
Gather Victim Identity Information
Gather Victim Network Information
Gather Victim Org Information
Phishing for Information
Search Closed Sources
Search Open Technical Databases
Search Open Websites/Domains
Search Threat Vendor Data
Search Victim-Owned Websites

Resource Development

Acquire Access
Acquire Infrastructure
Compromise Accounts
Compromise Infrastructure
Develop Capabilities
Establish Accounts
Obtain Capabilities
Stage Capabilities

Initial Access

Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Wi-Fi Networks

Execution

Cloud Administration Command
Command and Scripting Interpreter
Container Administration Command
Deploy Container
ESXi Administration Command
Exploitation for Client Execution
Input Injection
Inter-Process Communication
Native API
Poisoned Pipeline Execution
Scheduled Task/Job
Serverless Execution
Shared Modules
Software Deployment Tools
System Services
User Execution
Windows Management Instrumentation

Persistence

Account Manipulation
BITS Jobs
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Cloud Application Integration
Compromise Host Software Binary
Create Account
Create or Modify System Process
Event Triggered Execution
Exclusive Control
External Remote Services
Hijack Execution Flow
Implant Internal Image
Modify Authentication Process
Modify Registry
Office Application Startup
Power Settings
Pre-OS Boot
Scheduled Task/Job
Server Software Component
Software Extensions
Traffic Signaling
Valid Accounts

Privilege Escalation

Abuse Elevation Control Mechanism
Access Token Manipulation
Account Manipulation
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Create or Modify System Process
Domain or Tenant Policy Modification
Escape to Host
Event Triggered Execution
Exploitation for Privilege Escalation
Hijack Execution Flow
Process Injection
Scheduled Task/Job
Valid Accounts

Defense Evasion

Abuse Elevation Control Mechanism
Access Token Manipulation
BITS Jobs
Build Image on Host
Debugger Evasion
Delay Execution
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain or Tenant Policy Modification
Email Spoofing
Execution Guardrails
Exploitation for Defense Evasion
File and Directory Permissions Modification
Hide Artifacts
Hijack Execution Flow
Impair Defenses
Impersonation
Indicator Removal
Indirect Command Execution
Masquerading
Modify Authentication Process
Modify Cloud Compute Infrastructure
Modify Cloud Resource Hierarchy
Modify Registry
Modify System Image
Network Boundary Bridging
Obfuscated Files or Information
Plist File Modification
Pre-OS Boot
Process Injection
Reflective Code Loading
Rogue Domain Controller
Rootkit
Selective Exclusion
Subvert Trust Controls
System Binary Proxy Execution
System Script Proxy Execution
Template Injection
Traffic Signaling
Trusted Developer Utilities Proxy Execution
Unused/Unsupported Cloud Regions
Use Alternate Authentication Material
Valid Accounts
Virtualization/Sandbox Evasion
Weaken Encryption
XSL Script Processing

Credential Access

Adversary-in-the-Middle
Brute Force
Credentials from Password Stores
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials
Input Capture
Modify Authentication Process
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets
Steal Web Session Cookie
Unsecured Credentials

Discovery

Account Discovery
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Local Storage Discovery
Log Enumeration
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Software Discovery
System Information Discovery
System Location Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtual Machine Discovery
Virtualization/Sandbox Evasion

Lateral Movement

Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking
Remote Services
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material

Collection

Adversary-in-the-Middle
Archive Collected Data
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Screen Capture
Video Capture

Command and Control

Application Layer Protocol
Communication Through Removable Media
Content Injection
Data Encoding
Data Obfuscation
Dynamic Resolution
Encrypted Channel
Fallback Channels
Hide Infrastructure
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy
Remote Access Tools
Traffic Signaling
Web Service

Exfiltration

Automated Exfiltration
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Exfiltration Over Web Service
Scheduled Transfer
Transfer Data to Cloud Account

Impact

Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation
Defacement
Disk Wipe
Email Bombing
Endpoint Denial of Service
Financial Theft
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Service Stop
System Shutdown/Reboot

Findings

- Many **Energy and Utilities** -targeted APTs rely on **phishing** and **valid accounts** for initial access.
- Credential dumping and obfuscation are commonly used across groups to escalate access.
- Persistent techniques like **scheduled tasks** and **remote services** are frequently used.

Recommendations

1. **Strengthen Email Security & Phishing Defenses**
   - Implement advanced email filtering and sandboxing to detect malicious attachments and URLs.
   - Enforce multi-factor authentication (MFA) across all user accounts to reduce the effectiveness of compromised credentials.
   - Conduct regular phishing simulations and user awareness training to reduce susceptibility to social engineering attacks.
2. **Enhance Credential Security & Access Management**
   - Deploy endpoint detection solutions capable of identifying credential dumping tools and abnormal authentication patterns.
   - Implement strict privileged access management (PAM), including just-in-time (JIT) access and credential vaulting.
   - Regularly audit account permissions and remove unused or dormant accounts to limit lateral movement opportunities.
3. **Improve Persistence Detection & System Hardening**
   - Monitor for suspicious scheduled tasks, service modifications, or remote service creations using SIEM and EDR alerts.
   - Enforce application whitelisting and restrict administrative tools to authorized personnel only.

- Apply timely patching and system hardening guidelines to minimize exploitable weaknesses.

4. **Increase Network Visibility & Threat Hunting Capabilities**

    - Establish continuous threat hunting cycles focused on phishing-led intrusions, credential theft patterns, and persistence mechanisms.

    - Use MITRE ATT&CK mapping to identify gaps in defensive controls and continuously improve detection rules.

    - Implement network segmentation to limit the spread of APT activity and protect critical operational technology (OT) assets.