

Mitre Threat Hunting Report

Overview

Cyber threats differ across industries, regions and sectors. Modern adversaries, whether they are hacker groups, threat groups, adversary groups, or Advanced Persistent Threats (APTs), conduct highly organized campaigns targeting specific environments.

These groups often specialize in particular regions (e.g., North America, Western Europe, Middle East) or industries (e.g., Telecommunication, finance, healthcare, energy, government).

To understand and anticipate their behavior, the cybersecurity community uses a globally recognized framework known as MITRE ATT&CK, which documents how real world threat actors operate.

All APT groups are analyzed through something called TTPs:

TTPs (Tactics, Techniques and Procedures)

1. Tactics (The Why)

Tactics represent the adversary's goals or objectives, why they are performing an action during an attack.

The MITRE ATT&CK framework organizes these tactics in a structured matrix.

You can view them at: '<https://attack.mitre.org/>'

In the ATT&CK Enterprise Matrix, tactics form the columns at the top, starting from:

- Reconnaissance,
- Resource Development,
- Initial Access,
...all the way to
- Impact.

Every known threat group's behavior fits somewhere across these tactics.

2. Techniques (The How)

Techniques describe how adversaries achieve their objectives under each tactic.

Each tactic contains anywhere from **8 to 47 techniques**, depending on its complexity.

Techniques show the practical methods attackers use during an operation.

3. Procedures (The Step-by-Step Actions)

Procedures detail the specific actions, commands, or sequences used by a threat actor to execute a technique.

This is the most granular level ,what the attacker actually did.

Procedures represent the real world implementation seen in logs, alerts and incidents.

This is where threat hunting becomes actionable.

MITRE ATT&CK											
Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾ CTI ▾ Resources ▾ Benefactors Blog 🔍 Search Q											
layout: side ▾ show sub-techniques hide sub-techniques											
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Communication
11 techniques	8 techniques	11 techniques	17 techniques	23 techniques	14 techniques	47 techniques	17 techniques	34 techniques	9 techniques	17 techniques	11 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	App Layer Protection
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (13)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Control Plane Protocol Manipulation
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	Build Image on Host	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Control Plane Protocol Manipulation
Gather Victim Network Information (8)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (3)	Boot or Logon Autostart Execution (14)	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Control Plane Protocol Manipulation
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Initialization Scripts (3)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data from Cloud Storage
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Exploitation for Client Execution	Compromise Host Software Binary	Create or Modify System Process (5)	Deploy Container	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Data from Cloud Storage
Search Closed Sources (2)	Obtain Capabilities (7)	Stage Capabilities (6)	Input Injection	Create Account (3)	Domain or Tenant Policy Modification (2)	Direct Volume Access	Multi-Factor Authentication Process (9)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Configuration Repository (2)	Data from Configuration Repository (2)
Search Open Technical Databases (5)	Trusted Relationship	Supply Chain Compromise (3)	Inter-Process Communication (3)	Create or Modify System Process (5)	Event Triggered Execution (16)	Email Spoofing	Multi-Factor Authentication Request Generation	Container and Resource Discovery	Taint Shared Content	Data from Information Repositories (8)	Data from Information Repositories (8)
Search Open Websites/Domains (3)	Valid Accounts (4)	Wi-Fi Networks	Poisoned Pipeline Execution	Exclusive Control	Exploitation for Privilege Escalation	Execution Guardrails (2)	Network Sniffing	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Local System	Data from Local System
Search Threat Vendor Data			Scheduled Task/Job (5)	External Remote Services	Hijack Execution	File and Directory Permissions Modification (2)		Device Driver Discovery		Data from Network Shared Drive	Data from Network Shared Drive
Search Victim-Owned Websites			Serverless Execution	Shared Modules		Hide Artifacts (14)		Domain Trust Discovery		Data from Removable	Data from Removable

Why TTPs Matter in Threat Hunting

Threat hunters focus on TTPs because:

- Tactics→ Help identify what stage of an attack is occurring
- Techniques→ Help identify how the attacker is operating
- Procedures → Help identify exact log artifacts, commands and indicators.

Instead of chasing malware or IP addresses (which change constantly), hunters track behaviors, because behavior does not change even when tools do.

MITRE ATT&CK provides the blueprint.

Threat Hunting Methodology

When reviewing APT behavior, we often notice that different adversary groups share similar tactics and techniques. For example, one APT group might use the technique ‘Hardware Additions’ under the ‘Initial Access tactic’. If **APT27** uses ‘Hardware Additions’ for ‘Initial Access’, and **APT39** also uses ‘Hardware Additions’ in addition to ‘Trusted Relationship’ their behaviors overlap on that shared technique.

In this case, instead of creating separate detection rules for each group (**APT27** and **APT39**), we create one unified detection rule for the overlapping technique.

This increases efficiency and ensures consistent alerting across similar threat behaviors. As a Security Analyst, beyond producing a standard threat report, we also create an overlap analysis and a comparison across multiple APT groups and their TTPs.

The MITRE ATT&CK Navigator (<https://mitre-attack.github.io/attack-navigator/>) is used to visualize this. It allows us to load multiple APT profiles and highlight where their techniques intersect.

This overlap map helps identify the most commonly used TTPs for a particular industry, enabling more accurate detection engineering, prioritization, and threat-hunting activities.

We will be using three tools;

- Soc Radar (socradar.io)
- Mitre Att&ck Framework (<https://attack.mitre.org/>)
- Mitre Att&ck Navigator (<https://mitre-attack.github.io/attack-navigator/>)


1. SOCRADAR

SOCRadar can be used to research APT groups by filtering them based on region, industry, or sector.

It provides the latest threat intelligence reports for each category.

STEPS ON SOCRADAR→

- After selecting Threat Reports Industry Threat Landscape Report for ‘Telecommunications’.
- SOC Radar displays all relevant APT groups.
- I selected the group ‘**APT31**’, copied its name, and then pasted it into the MITRE ATT&CK Navigator to analyze its associated TTPs.



FREE TOOLS

Dark Web Report

IOC Radar

Threat Reports ▾

- Industry Threat Landscape Report
- Country Threat Landscape Report
- External Threat Assessment Report

External Attack Surface

Select a Report

Banking

E-Commerce

Manufacturing

Information Services

HealthCare & Social Assistance

Telecommunications

Finance


Insurance

Energy & Utilities

Public Administration

Retail

Delivery Services



FREE TOOLS

Dark Web Report

IOC Radar

Threat Reports ▾

- Industry Threat Landscape Report
- Country Threat Landscape Report
- External Threat Assessment Report

External Attack Surface

Threat Actor New

CVE Radar

Campaigns

823

Dark Web Threats

129

Ransomware Threats

11202

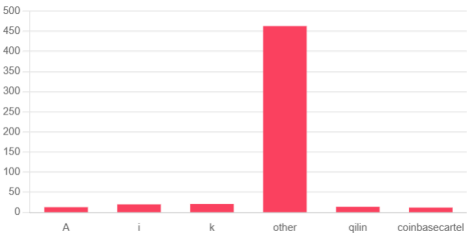
Phishing Threats

239

Target Countries

APT Groups

Ransomware Threat Groups



Category	Count
A	~10
i	~20
k	~20
other	~450
qlin	~10
coinbasecartel	~10

APT Groups

APT Groups target retail industry.

1	Mirage	6	Sandman
2	AjaxTM	7	BrazenBamboo
3	Earth Estries	8	APT31
4	APT 29	9	FamousSparrow
5	MuddyWater	10	Syrian Electronic Army (SEA)

2.)MITRE ATT&CK FRAMEWORK

The MITRE ATT&CK(<https://attack.mitre.org/>) framework maintains an extensive database of known APT groups and maps each group to the specific Tactics, Techniques, and Procedures (TTPs) they use during real-world attacks.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Communication
11 techniques	8 techniques	11 techniques	17 techniques	23 techniques	14 techniques	47 techniques	17 techniques	34 techniques	9 techniques	17 techniques	10 techniques
Active Scanning (3) Gather Victim Host Information (4) Gather Victim Identity Information (3) Gather Victim Network Information (3) Gather Victim Org Information (4) Phishing for Information (4) Search Closed Sources (2) Search Open Technical Databases (5) Search Open Websites/Domains (3) Search Threat Vendor Data Search Victim-Owned Websites	Acquire Access Acquire Infrastructure (8) Compromise Accounts (3) Compromise Infrastructure (8) Develop Capabilities (4) Establish Accounts (3) Obtain Capabilities (7) Stage Capabilities (6) Supply Chain Compromise (3) Trusted Relationship Valid Accounts (4) Wi-Fi Networks	Content Injection Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (4) Replication Through Removable Media Supply Chain Compromise (3) Trusted Relationship Valid Accounts (4) Wi-Fi Networks	Cloud Administration Command Command and Scripting Interpreter (13) Container Administration Command Deploy Container ESXi Administration Command Exploitation for Client Execution Input Injection Inter-Process Communication (3) Native API Poisoned Pipeline Execution Scheduled Task/Job (5) Serverless Execution Shared Modules	Account Manipulation (7) BITS Jobs Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (3) Cloud Application Integration Compromise Host Software Binary Create Account (3) Create or Modify System Process (5) Domain or Tenant Policy Modification (2) Escape to Host Event Triggered Execution (18) Exclusive Control External Remote Services Hijack Execution	Abuse Elevation Control Mechanism (6) Access Token Manipulation (5) 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 (2) Email Spoofing Execution Guardrails (2) Exploitation for Defense Evasion File and Directory Permissions Modification (2) Hide Artifacts (14) Network Sniffing	Abuse Elevation Control Mechanism (6) Access Token Manipulation (5) 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 (2) Email Spoofing Execution Guardrails (2) Exploitation for Defense Evasion File and Directory Permissions Modification (2) Hide Artifacts (14) Network Sniffing	Adversary-in-the-Middle (4) Brute Force (4) Credentials from Password Stores (6) Exploitation for Credential Access Forced Authentication Forge Web Credentials (2) Input Capture (4) Modify Authentication Process (9) Multi-Factor Authentication Interception Multi-Factor Authentication Request Generation Network Sniffing	Account Discovery (4) 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	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (2) Remote Services (8) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (4)	Adversary-in-the-Middle (4) Archive Collected Data (3) Automated Collection Browser Session Hijacking Clipboard Data Data from Cloud Storage Data from Configuration Repository (2) Data from Information Repositories (9) Data from Local System Data from Network Shared Drive Data from Removable	App Layer Protection Command and Control Data Exfiltration Data Infiltration Data Obfuscation Data Resilience Data Retention Data Theft Data Wiping Device Control Device Wiping File and Directory Permissions Modification (2) File and Directory Discovery Group Policy Discovery Local Storage

3.)MITRE ATT&CK NAVIGATOR.

In MITRE ATT&CK Navigator, begin by selecting ‘Create a New Layer’ and choose either the Enterprise ATT&CK or ICS matrix depending on your analysis. I will be selecting ‘Enterprise’.

Once the layer is created, rename it to match the APT group you are analyzing.

Navigate to Layer Controls → Layer Settings, and under Layer Information, change the title to ‘APT31’ to reflect the group you are working on.

Next, configure the visualization by selecting Color Setup. If you are comparing multiple APTs (e.g., three groups), set the Low value to 1 and the High value to 3 so the overlap intensity is displayed accurately.

After adjusting the settings, click Save or simply close the settings menu to apply the changes.

The screenshot displays the MITRE ATT&CK Navigator web application. At the top, a red banner reads "ATT&CK v18 has been released! Check out the [blog post](#) or [changelog](#) for more information." The main header shows "MITRE ATT&CK® Navigator" and a description: "The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more." Below this is a navigation bar with "help", "changelog", and "theme" links.

The "Create New Layer" dialog is open, showing options to "Create a new empty layer" or select a pre-defined layer. The "Enterprise ATT&CK" layer is selected. Below this are "More Options" and "Mobile ATT&CK" and "ICS ATT&CK" buttons.

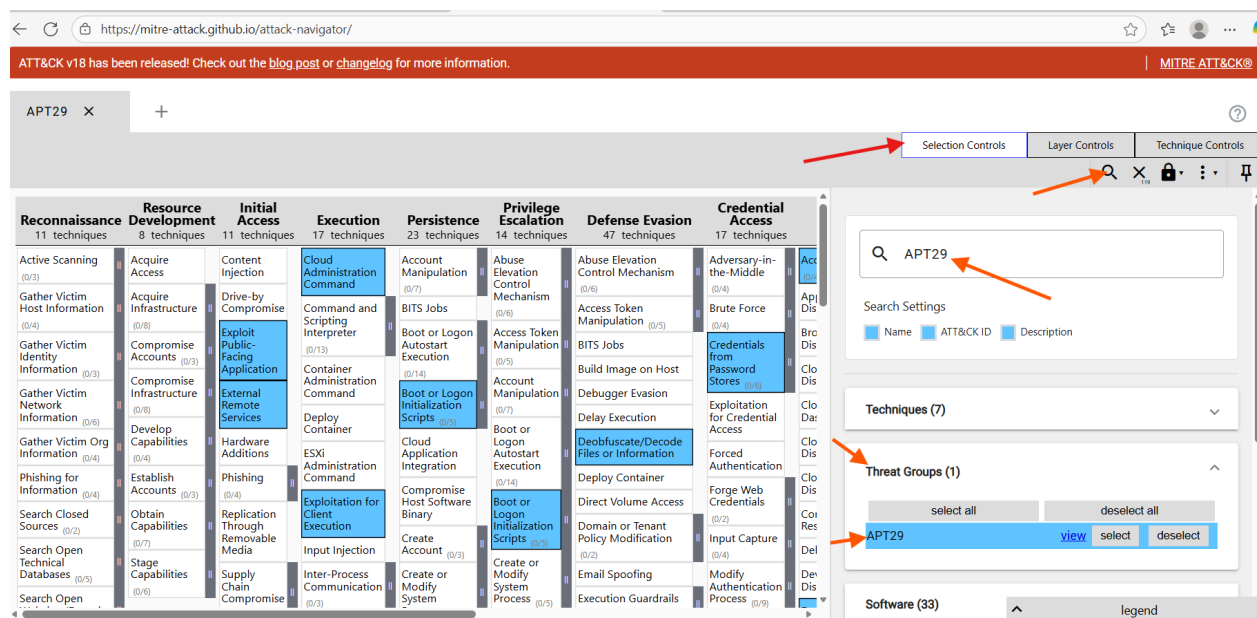
The main interface shows a grid of ATT&CK techniques categorized into Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, and Discovery. The "APT31" layer is selected, and the "Color Setup" dialog is open for this layer. The "Color Setup" dialog shows a "Scoring Gradient" with a low value of 1 and a high value of 3. The gradient is currently set to a red-to-yellow color scheme. The "Layer Information" panel on the right shows the layer name "APT31" and its description "Enterprise ATT&CK".

Next,

Navigate to 'Selection Controls' → click the Search icon. Search for the APT group (e.g., APT29) and scroll to the Threat Group section.

Select the group, then click 'Select'.

MITRE Navigator will automatically highlight all techniques associated with APT29 within the layer.

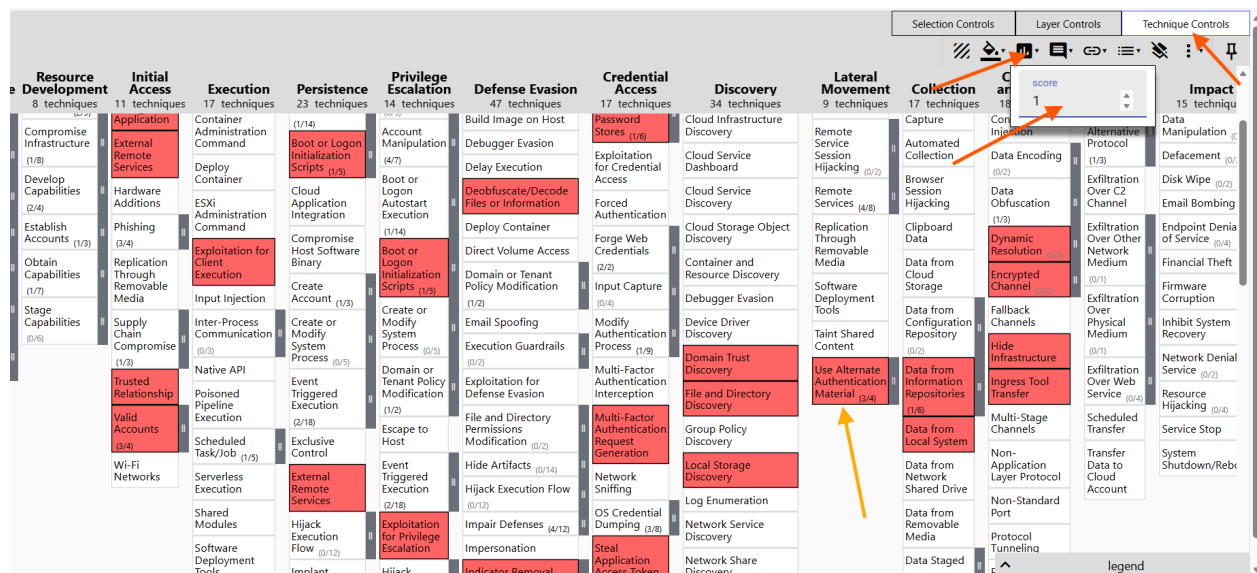


NEXT,

Navigate to ‘**Technique Controls**’ and select Scoring.

Assign a score (e.g., 1–3) to apply a color gradient typically green, yellow, and red to distinguish multiple APT groups.

This visual scoring of ‘1’ highlights all TTPs associated with APT29, making it easier to see which tactics and techniques the group commonly uses.



REPEAT THE SAME PROCESS FOR OTHER APTs (Volt Typhoon, APT33)

Volt Typhoon,

ATT&CK v18 has been released! Check out the [blog post](#) or [changelog](#) for more information. MITRE ATT&CK®

APT29 × Volt Typhoon × +

Selection Controls Layer Controls Technique Controls

Source Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Impact
Active Scanning (0/3)	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism (0/6)	Adversary-in-the-Middle (0/4)	Account Discovery (2/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/4)	Application Layer Protocol (1/5)	Automated Exfiltration (0/1)
Drive-by Compromise (0/3)	Drive-by Compromise	Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (1/3)	Communication Through Removable Media	Data Transfer Size Limits (0/1)
Exploit Public-Facing Application (0/13)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (0/7)	Build Image on Host	Credentials from Password Stores (1/6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Data Encrypted for Impact (0/3)
External Remote Services (0/3)	External Remote Services	Deploy Container	Cloud Application Integration	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)	Exfiltration Over Alternative Protocol (0/2)
Hardware Additions (0/4)	Phishing	ESXi Administration Command	Compromise Host Software Binary	Boot or Logon Initialization Scripts (0/5)	Delay Execution	Forge Web Credentials	Cloud Service Dashboard	Remote Services (1/8)	Browser Session Hijacking	Data Obfuscation (0/3)	Exfiltration Over C2 Channel (0/1)
Replication Through Removable Media (0/3)	Replication Through Removable Media	Input Injection	Create Account	Create or Modify System Process (0/5)	Domain or Tenant Policy Modification (0/2)	Input Capture (1/4)	Container and Resource Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)
Supply Chain Compromise (0/3)	Supply Chain Compromise	Inter-Process Communication	Create or Modify System	Create or Modify System Process (0/5)	Email Spoofing	Modify Authentication Process (0/9)	Device Driver Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2/2)	Firmware Corruption (0/1)

Legend

APT33

ATT&CK v18 has been released! Check out the [blog post](#) or [changelog](#) for more information. MITRE ATT&CK®

APT29 × Volt Typhoon × APT33 × +

Selection Controls Layer Controls Technique Controls

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Command and Control	Exfiltration
Active Scanning (0/3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism (0/6)	Adversary-in-the-Middle (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Application Layer Protocol (0/1)	Automated Exfiltration (0/1)
Gather Victim Host Information (0/4)	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Communication Through Removable Media	Data Transfer Size Limits (0/1)
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (0/7)	Build Image on Host	Credentials from Password Stores (0/6)	Browser Information Discovery	Audio Capture	Content Injection	Data Encrypted for Impact (0/3)
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/14)	Debugger Evasion	Delay Execution	Exploitation for Credential Access	Cloud Infrastructure Discovery	Automated Collection	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/2)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Autostart Execution (0/14)	Deobfuscate/Decode Files or Information	Forge Web Credentials	Cloud Service Dashboard	Remote Service Session Hijacking (0/2)	Data Obfuscation (0/3)	Exfiltration Over C2 Channel (0/1)
Phishing for Information (0/4)	Establish Accounts (0/3)	Phishing	Exploitation for Client Execution	Compromise Host Software Binary	Boot or Logon Initialization Scripts (0/5)	Direct Volume Access	Container and Resource Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)
Search Closed Sources (0/2)	Obtain Capabilities (0/7)	Replication Through Removable Media	Input Injection	Create Account	Create or Modify System Process (0/5)	Domain or Tenant Policy Modification (0/2)	Debugger Evasion	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (0/2)	Firmware Corruption (0/1)
Search Open Technical Databases (0/6)	Stage Capabilities	Supply	Inter-Process Communication	Create or Modify System Process (0/5)	Email Spoofing	Modify Authentication Process (0/9)	Device Driver Discovery	Taint Shared Content	Data from Configuration Repository	Fallback Channels	Inhibit System Recovery (0/1)

Legend

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

ATT&CK v18 has been released! Check out the [blog post](#) or [changelog](#) for more information. MITRE ATT&CK®

APT29 × Volt Typhoon × **APT33 ×** +

Selection Controls Layer Controls Technique Controls

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact	Exfiltration
Active Scanning (0/3)	Acquire Access (2/8)	Content Injection (0/13)	Cloud Administration Command (0/17)	Account Manipulation (1/7)	Abuse Elevation Control Mechanism (0/6)	Abuse Elevation Control Mechanism (0/6)	Adversary-in-the-Middle (0/4)	Account Discovery (1/4)	Exploitation of Remote Services (0/4)	Adversary-in-the-Middle (0/4)	Automated Exfiltration (0/1)
Gather Victim Host Information (0/4)	Acquire Infrastructure (2/8)	Drive-by Compromise (0/13)	Command and Scripting Interpreter (0/17)	BITS Jobs (0/5)	Access Token Manipulation (1/5)	Access Token Manipulation (1/5)	Brute Force (1/4)	Application Window Discovery (0/4)	Internal Spearphishing (0/3)	Archive Collected Data (0/3)	Data Transfer Size Limit (0/1)
Gather Victim Identity Information (1/2)	Compromise Accounts (1/3)	Exploit Public-Facing Application (0/13)	Container Administration Command (0/17)	Boot or Logon Autostart Execution (0/14)	Access Token Manipulation (1/5)	Build Image on Host (0/5)	Credentials from Password Stores (1/8)	Browser Information Discovery (0/4)	Lateral Tool Transfer (0/3)	Audio Capture (0/3)	Exfiltrate Over Alternative Protocol (0/1)
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/3)	External Remote Services (0/13)	Deploy Container (0/17)	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (1/7)	Debugger Evasion (0/5)	Exploitation for Credential Access (0/2)	Cloud Infrastructure Discovery (0/4)	Remote Service Session Hijacking (0/2)	Automated Collection (0/3)	Exfiltrate Over Network Medium (0/1)
Gather Victim Org Information (1/4)	Develop Capabilities (0/4)	Hardware Additions (0/4)	ESXi Administration Command (0/17)	Cloud Application Integration (0/14)	Boot or Logon Autostart Execution (0/14)	Deobfuscate/Decode Files or Information (0/2)	Forced Authentication (0/2)	Cloud Service Dashboard (0/2)	Remote Services (0/8)	Data Encoding (0/3)	Exfiltrate Over Other Network Medium (0/1)
Phishing for Information (0/4)	Establish Accounts (2/3)	Phishing (0/4)	Exploitation for Client Execution (0/17)	Compromise Host Software Binary (0/3)	Boot or Logon Initialization Scripts (0/5)	Deploy Container (0/2)	Forge Web Credentials (0/2)	Cloud Storage Object Discovery (0/2)	Replication Through Removable Media (0/2)	Data Obfuscation (0/3)	Exfiltrate Over Physical Medium (0/1)
Search Closed Sources (0/2)	Obtain Capabilities (2/7)	Replication Through Removable Media (0/4)	Input Injection (0/17)	Create Account (0/3)	Create or Modify System Process (0/5)	Direct Volume Access (0/2)	Input Capture (1/4)	Container and Resource Discovery (0/2)	Software Deployment Tools (0/2)	Clipboard Data (0/3)	Exfiltrate Over Physical Medium (0/1)
Search Open Technical Databases (0/3)	Stage Capabilities (1/6)	Supply Chain Compromise (0/4)	Inter-Process Communication (0/17)	Create or Modify System (0/3)	Create or Modify Process (0/5)	Domain or Tenant Policy Modification (0/2)	Modify Authentication Process (0/4)	Debugger Evasion (0/2)	Taint Shared Content (0/2)	Dynamic Resolution (0/3)	Exfiltrate Over Physical Medium (0/1)
Search Open (0/3)						Execution Guardrails (0/2)				Encrypted Channel (0/2)	Exfiltrate Over Physical Medium (0/1)

NEXT,

Create a consolidated **‘overlap layer’** to visualize which techniques are shared across all selected APT groups (for example, common overlaps in Initial Access or Credential Access).

Steps to Generate an Overlap Layer;

1. Click the ‘+’ icon to open a new tab.
2. Select **‘Create Layer from Other Layers.’**
3. Change the domain to **‘Enterprise v18.’**
4. In the Score Expression field, add all APT group layers using an expression such as: **a + b + c** (where each letter corresponds to a different 3 APT layer)
5. Scroll down and click **‘Create Layer.’**
6. Rename the layer to something descriptive, such as **‘Layer of operation Overlap.’**

Click **‘Export’** → Choose **‘Export All Layers to Excel’** to download a consolidated spreadsheet of all TTP overlaps.

ATT&CK v18 has been released! Check out the [blog post](#) or [changelog](#) for more information.

APT29 x ^a Volt Typhoon x ^b APT33 x ^c new tab x +

Create New Layer Create a new empty layer

Open Existing Layer Load a layer from your computer or a URL

Create Layer from Other Layers Select layers to inherit properties from

domain*
Enterprise ATT&CK ...

score expression
a+b+c

gradient

coloring

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 (APT29)
- ^b (Volt Typhoon)
- ^c (APT33)

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.

MITRE ATT&CK® Navigator v5.2.0

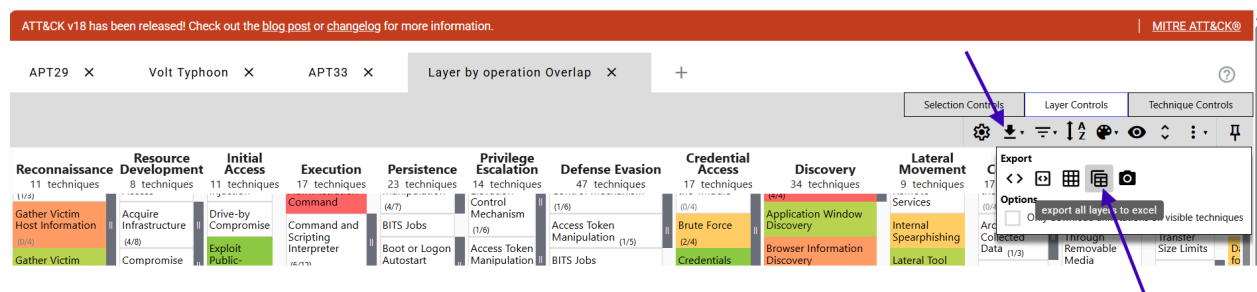
ATT&CK v18 has been released! Check out the [blog post](#) or [changelog](#) for more information.

MITRE ATT&CK®

APT29 x Volt Typhoon x APT33 x Layer by operation Overlap x +

Selection Controls Layer Controls Technique Controls

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
11 techniques	8 techniques	11 techniques	17 techniques	23 techniques	14 techniques	47 techniques	17 techniques	34 techniques	9 techniques	17 techniques	18 techniques	9 techniques
Gather Victim Host Information (0/4)	Acquire Infrastructure (4/8)	Drive-by Compromise (0/2)	Command and Scripting Interpreter (6/13)	BITS Jobs (4/7)	Control Mechanism (1/8)	Access Token Manipulation (1/5)	Brute Force (2/4)	Application Window Discovery (0/4)	Internal Spearphishing (0/4)	Archive Collected Data (1/3)	Communication Through Removable Media (0/1)	Data Transfer Size Limits (0/1)
Gather Victim Identity Information (2/3)	Compromise Accounts (2/3)	Exploit Public-Facing Application (0/8)	Container Administration Command (0/1)	Boot or Logon Autostart Execution (1/5)	Access Token Manipulation (1/5)	BITS Jobs (1/5)	Credentials from Password Stores (1/6)	Browser Information Discovery (0/4)	Lateral Tool Transfer (0/4)	Audio Capture (0/2)	Content Injection (1/3)	Exfiltration Over Alternative Protocol (0/1)
Gather Victim Network Information (2/6)	Compromise Infrastructure (0/8)	External Remote Services (0/8)	Deploy Container (0/1)	Boot or Logon Initialization Scripts (1/3)	Account Manipulation (4/7)	Debugger Evasion (0/4)	Exploitation for Credential Access (0/2)	Cloud Infrastructure Discovery (0/2)	Remote Service Hijacking (0/2)	Automated Collection (0/2)	Data Encoding (0/2)	Data Mar (0/1)
Gather Victim Org Information (1/4)	Develop Capabilities (0/4)	Hardware Additions (0/4)	ESXi Administration Command (0/3)	Cloud Application Integration (0/5)	Boot or Logon Autostart Execution (1/14)	Delay Execution (0/2)	Forced Authentication (0/2)	Cloud Service Dashboard (0/2)	Remote Services (4/8)	Browser Session Hijacking (0/2)	Data Obfuscation (1/3)	Exfiltration Over C2 Channel (0/1)
Phishing for Information (0/4)	Establish Accounts (2/3)	Phishing (0/4)	Exploitation for Client Execution (0/3)	Compromise Host Software Binary (0/3)	Boot or Logon Initialization Scripts (1/3)	Deploy Container (0/2)	Forge Web Credentials (2/2)	Cloud Storage Object Discovery (0/2)	Replication Through Removable Media (0/2)	Clipboard Data (0/2)	Dynamic Resolution (0/2)	Exfiltration Over Other Network Medium (0/1)
Search Closed Sources (0/2)	Obtain Capabilities (0/7)	Replication Through Removable Media (0/3)	Input Injection (0/3)	Create Account (1/3)	Boot or Logon Initialization Scripts (1/3)	Domain or Tenant Policy Modification (1/2)	Input Capture (1/4)	Container and Resource Discovery (0/2)	Software Deployment Tools (0/2)	Data from Cloud Storage (0/2)	Encrypted Channel (2/2)	Exfiltration Over Physical Medium (0/1)
Search Open Technical Databases (1/3)	Stage Capabilities (1/6)	Supply Chain Compromise (1/3)	Inter-Process Communication (0/3)	Create or Modify System Process (0/5)	Create or Modify System Process (0/5)	Email Spoofing (0/2)	Modify Authentication Process (1/8)	Debugger Evasion (0/2)	Taint Shared Content (0/2)	Data from Configuration Repository (0/2)	Fallback Channels (0/1)	Exfiltration Over Web Service (1/4)
Search Open Websites/Domains (0/3)	Search Threat Vendor Data (0/3)	Trusted Relationship (1/3)	Native API (0/3)	Event Triggered Execution (2/18)	Domain or Tenant Policy Modification (1/2)	Execution Guardrails (0/2)	Multi-Factor Authentication Interception (0/2)	Domain Trust Discovery (0/2)	Use Alternate Authentication Material (3/4)	Data from Information Repositories (1/6)	Hide Infrastructure (0/1)	Scheduled Transfer (0/1)
Search Victim-Owned Websites (0/4)	Valid Accounts (4/4)	Poisoned Pipeline Execution (0/4)	Scheduled Task/Job (0/4)	Exclusive Control (0/4)	Escape to Host (0/4)	File and Directory Permissions Modification (1/2)	Multi-Factor Authentication Request (0/4)	File and Directory Discovery (0/4)	Multi-Stage Channels (0/4)	Data from Local System (0/4)	Ingress Tool Transfer (0/4)	Exfiltration Over Web Service (1/4)



	A	B	C	D	E	F	G
	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
1	Active Scanning	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism
2	Gather Victim Host Information	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation	Access Token Manipulation
3	Gather Victim Identity Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution	Account Manipulation	BITS Jobs
4	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
5	Gather Victim Org Information	Develop Capabilities	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Initialization Scripts	Debugger Evasion
6	Phishing for Information	Establish Accounts	Phishing	Exploitation for Client Execution	Compromise Host Software Binary	Create or Modify System Process	Delay Execution
7	Search Closed Sources	Obtain Capabilities	Replication Through Removable Media	Input Injection	Create Account	Domain or Tenant Policy Modification	Deobfuscate/Decode Files or Information
8	Search Open Technical Databases	Stage Capabilities	Supply Chain Compromise	Inter-Process Communication	Create or Modify System Process	Escape to Host	Deploy Container
9	Search Open Websites/Domains		Trusted Relationship	Native API	Event Triggered Execution	Event Triggered Execution	Direct Volume Access
10	Search Threat Vendor Data		Valid Accounts	Poisoned Pipeline Execution	Exclusive Control	Exploitation for Privilege Escalation	Domain or Tenant Policy Modification
11	Search Victim-Owned Websites		Wi-Fi Networks	Scheduled Task/Job	External Remote Services	Hijack Execution Flow	Email Spoofing
12				Serverless Execution	Hijack Execution Flow	Process Injection	Execution Guardrails
13				Shared Modules	Implant Internal Image	Scheduled Task/Job	Exploitation for Defense Evasion
14				Software Deployment Tools	Modify Authentication Process	Valid Accounts	File and Directory Permissions Manipulation
15				System Services	Modify Registry		Hide Artifacts
16				User Execution	Office Application Startup		Hijack Execution Flow
17				Windows Management Instrumentation	Power Settings		Impair Defenses
18					Pre-OS Boot		Impersonation
19					Scheduled Task/Job		Indicator Removal
20					Server Software Component		Indirect Command Execution
21					Software Extensions		Masquerading
22					Traffic Signaling		Modify Authentication Process
23					Valid Accounts		Modify Cloud Compute Infrastructure
24							Modify Cloud Resource Hierarchy
25							Modify Registry
26							Modify System Image
27							

Conclusion

This project demonstrates how MITRE ATT&CK, threat intelligence platforms, and overlap analysis can be combined to strengthen detection engineering and threat hunting. By mapping multiple APT groups and identifying shared tactics and techniques, we can prioritize high-risk behaviors, develop more efficient detection rules, and reduce alert fatigue.

The use of SOC Radar, MITRE Navigator, and TTP scoring provides a structured, repeatable methodology for analyzing adversary behavior across industries.

This approach aligns with modern threat-informed defense practices and supports proactive hunting by focusing on adversary behavior rather than isolated indicators.