Threat Hunting Report

Introduction

Threat hunting is a proactive and intelligence-driven cyber security practice focused on detecting malicious activities within an environment before they result in significant damage. Unlike reactive security measures that rely on alerts, threat hunting assumes that adversaries may already be present in the network and uses a systematic process to uncover hidden threats, undetected breaches, or suspicious patterns.

Threat hunting plays a crucial role in modern Security Operations Centers (SOCs), especially as cyber threats grow more sophisticated, persistent, and evasive.

Understanding Threat Hunting

Threat hunting combines **hypothesis-driven investigations**, deep knowledge of adversary behavior, historical data analysis, and advanced security tooling. The primary goals include:

- Identifying unknown threats and indicators that traditional detection mechanisms missed
- Reducing dwell time of attackers
- Strengthening detection capabilities
- Improving organizational resiliency

Threat hunters analyze data from logs, endpoints, cloud infrastructure, network traffic, and threat intelligence sources, correlating this information to find anomalies or suspicious activities.

Advanced Persistent Threats (APTs)

What Are APTs?

Advanced Persistent Threats are highly capable, well-resourced, and often state-sponsored threat actors that infiltrate networks to steal data, disrupt operations, or conduct espionage. Key characteristics include:

- **Advanced**: Use of sophisticated tools, zero-day exploits, and customized malware
- **Persistent**: Long-term presence within the network with stealthy movement
- **Threat**: Skilled actors with defined objectives

APTs often target sectors such as finance, government, energy, healthcare, and critical infrastructure.

Why APTs Matter in Threat Hunting

Threat hunting teams must understand APT behavior because:

- APTs use stealthy techniques that bypass automated defenses
- Their operations follow predictable behavior patterns (TTPs)
- Early detection can prevent significant damage or data compromise

---

Tactics, Techniques, and Procedures (TTPs)

TTPs describe how adversaries plan and execute attacks:

- **Tactics**: High-level goals (e.g., Initial Access, Lateral Movement, Data Exfiltration)
- **Techniques**: Methods used to accomplish a tactic (e.g., phishing, credential dumping)
- **Procedures**: Detailed, step-by-step actions unique to each threat group

TTP-based hunting helps analysts identify malicious activity even when indicators (like IP addresses or file hashes) change, since TTPs are difficult for attackers to mask entirely.

Threat Hunting Tools and Frameworks

MITRE ATT&CK Framework

MITRE ATT&CK is a globally recognized, open-source knowledge base that documents adversary behaviors based on real-world observations.

Uses in Threat Hunting

- Maps adversary TTPs to known threat groups
- Helps build hypotheses based on expected attack paths
- Guides detection engineering and SIEM use case development
- Enhances SOC maturity by providing a common language for threat analysis

Benefits

- Improves visibility across kill-chain stages
- Enhances threat intelligence integration
- Helps validate and strengthen defensive controls

- Supports penetration testing and red team operations

MITRE ATT&CK Navigator

The ATT&CK Navigator is an interactive web tool used to visualize and layer MITRE ATT&CK techniques.

Uses

- Mapping detections and coverage against ATT&CK techniques
- Visualizing APT group behavior
- Prioritizing detection gaps
- Collaborating across SOC, red teams, and threat intel teams

Benefits

- Easy-to-understand heat maps
- Helps in building hunting roadmaps
- Supports strategic security decision-making
- Enables customization for different threat actors or campaigns

---

SOC Radar

SOC Radar is a threat intelligence and attack surface monitoring platform designed to help SOC teams identify and analyze threats in real time.

Uses

- Provides enriched threat intelligence for hypothesis creation
- Monitors external attack surface for vulnerabilities
- Detects exposed credentials, misconfigurations, and dark web threats
- Integrates with SIEM/SOAR platforms for automated alert enrichment

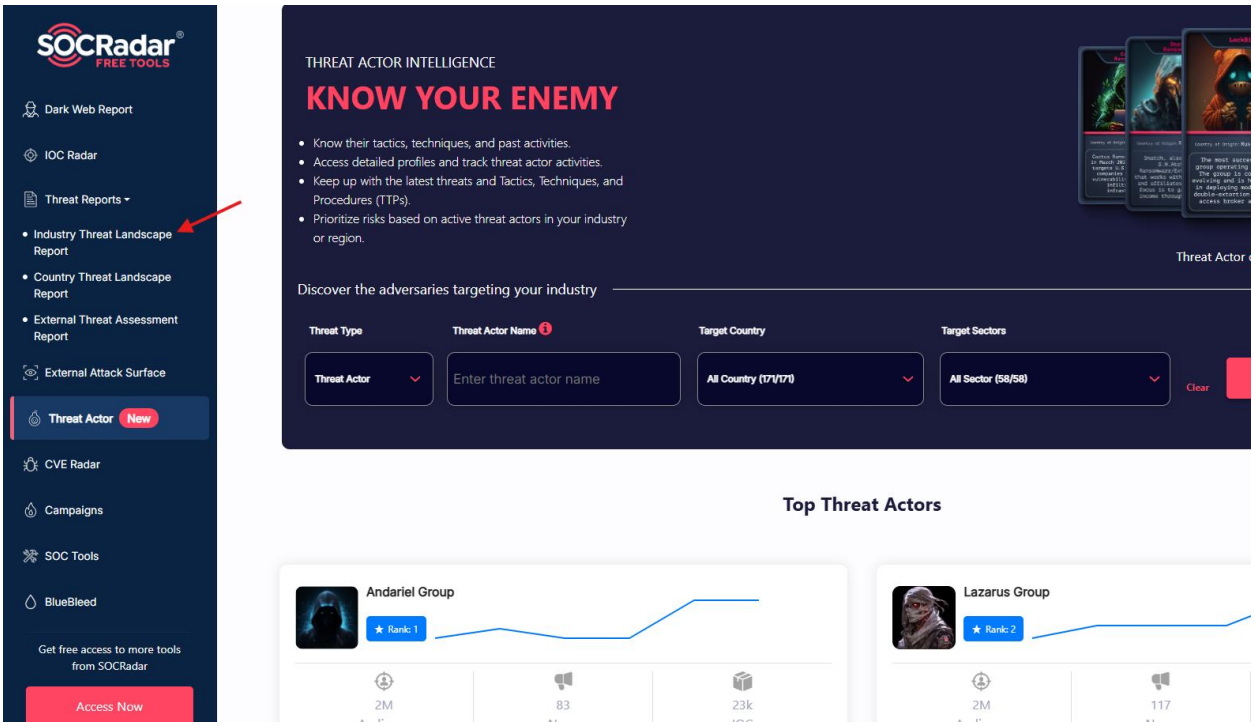
Benefits

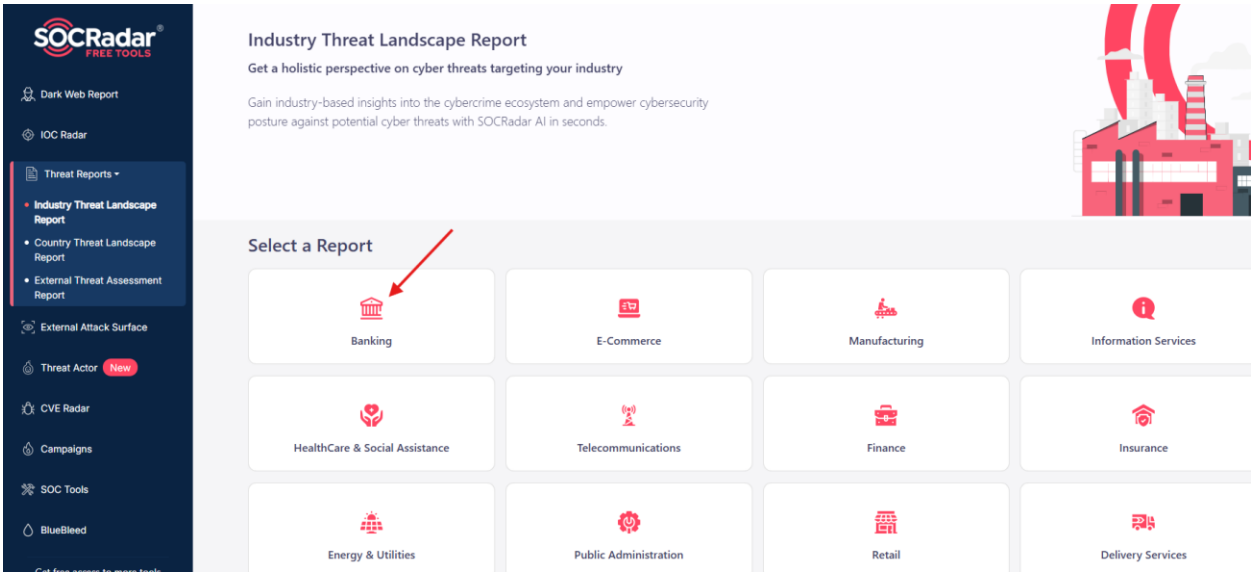
- Fast insights into adversary campaigns and trends
- Helps correlate internal telemetry with external intelligence
- Reduces time spent on manual intelligence gathering
- Offers comprehensive visibility for proactive hunting

The Threat Hunting Process Project

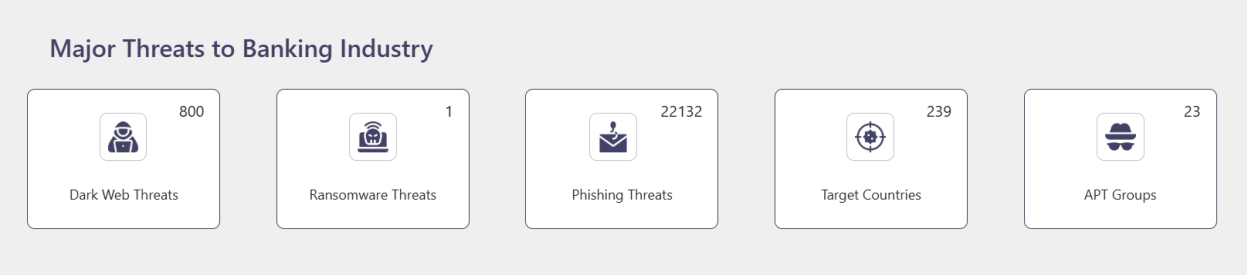
We will be using the banking industry in Canada as a case study for this project.

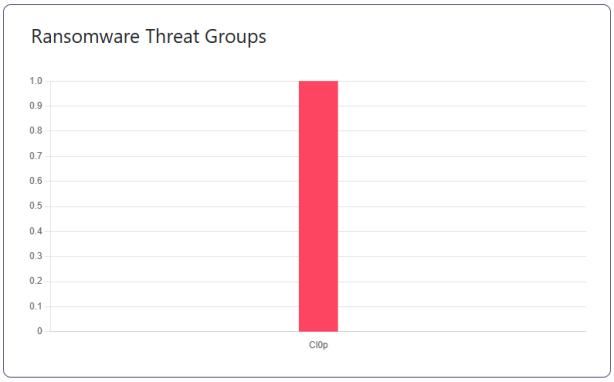
Log onto SOCRadar in your browser (https://socradar.io), navigate to 'threat reports', select a report for the industry you want to evaluate, in this case we will go with Banking.

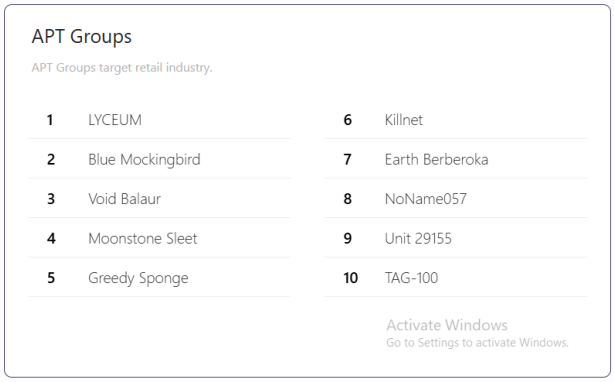




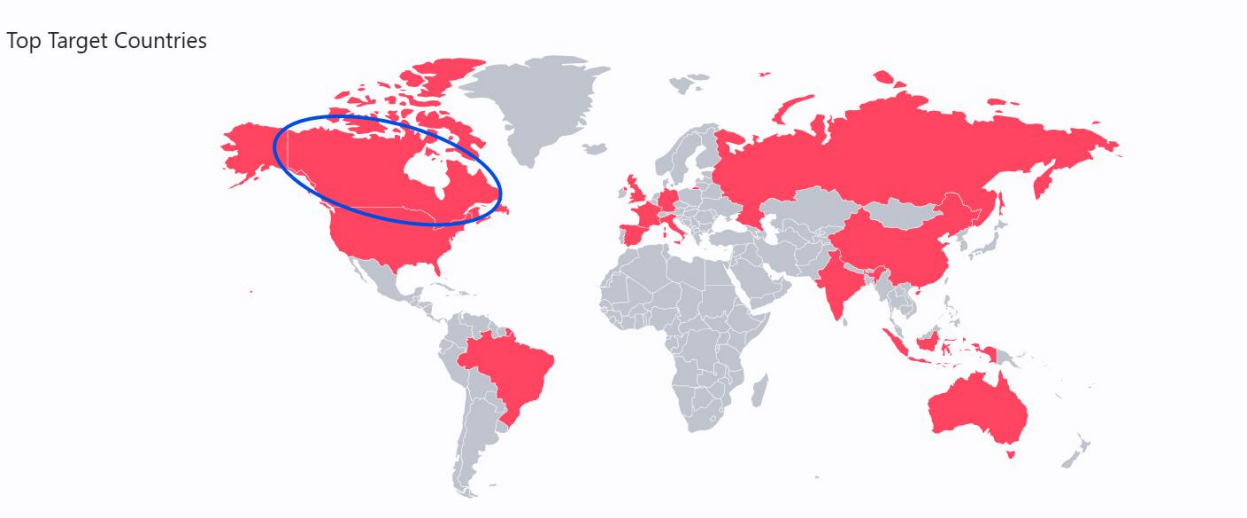
The report highlights some information but our focus is on the APT groups which are currently 23





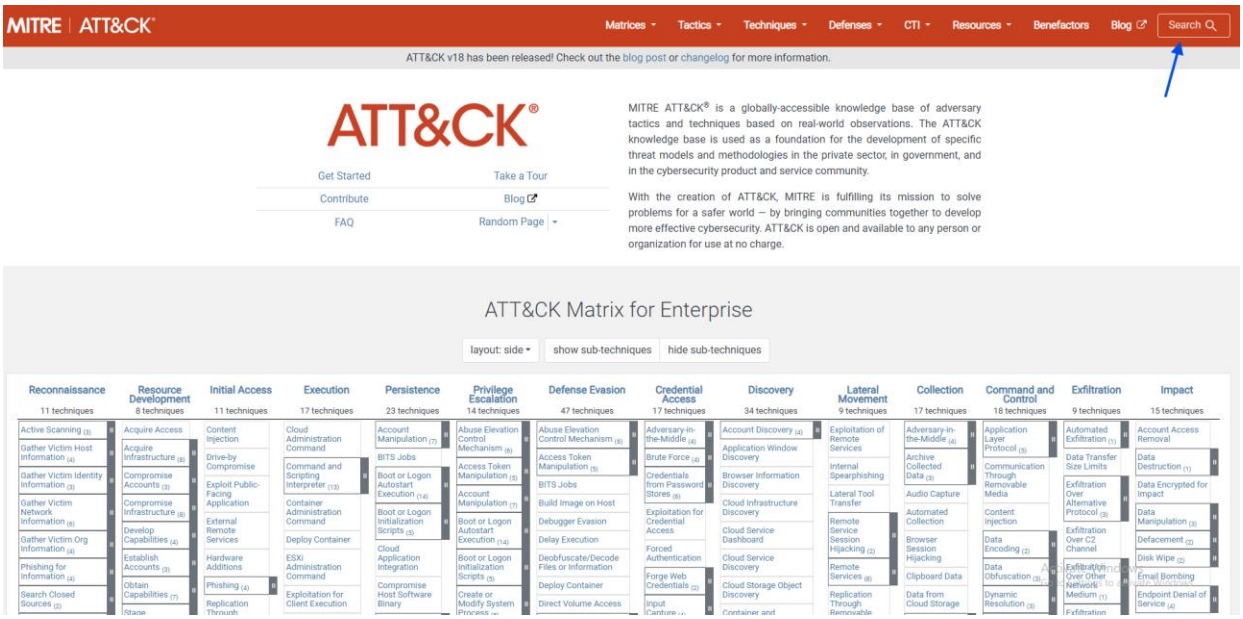


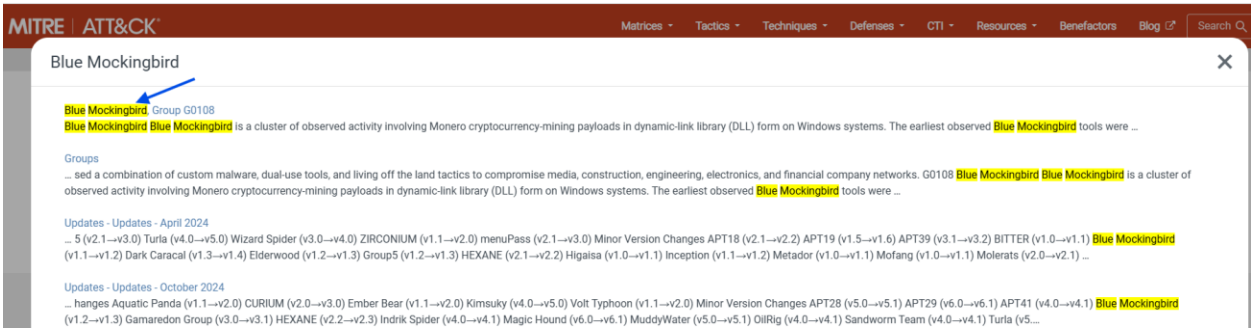
Country of interest is Canada



Now that we have the APT groups, we will use the mitre attack website to research into the TTP of these APT groups.

In your browser, type https://attack.mitre.org/, select one of the AT groups found in the SOCRadar report and search as shown below


MITRE | ATT&CK
Matrices
Tactics
Techniques
Defenses
CTI
Resources
Benefactors
Blog
Search
ATT&CK v18 has been released! Check out the blog post or changelog for more information.
ATT&CK®
Get Started
Take a Tour
Contribute
Blog
FAQ
Random Page
MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.
With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.
ATT&CK Matrix for Enterprise
layout: side
show sub-techniques
hide sub-techniques
Reconnaissance
11 techniques
Resource Development
8 techniques
Initial Access
11 techniques
Execution
17 techniques
Persistence
23 techniques
Privilege Escalation
14 techniques
Defense Evasion
47 techniques
Credential Access
17 techniques
Discovery
34 techniques
Lateral Movement
9 techniques
Collection
17 techniques
Command and Control
18 techniques
Exfiltration
9 techniques
Impact
15 techniques


MITRE | ATT&CK
Matrices
Tactics
Techniques
Defenses
CTI
Resources
Benefactors
Blog
Search
Blue Mockingbird
Blue Mockingbird, Group G0108
Blue Mockingbird Blue Mockingbird is a cluster of observed activity involving Monero cryptocurrency-mining payloads in dynamic-link library (DLL) form on Windows systems. The earliest observed Blue Mockingbird tools were ...
Groups
... sed a combination of custom malware, dual-use tools, and living off the land tactics to compromise media, construction, engineering, electronics, and financial company networks. G0108 Blue Mockingbird Blue Mockingbird is a cluster of observed activity involving Monero cryptocurrency-mining payloads in dynamic-link library (DLL) form on Windows systems. The earliest observed Blue Mockingbird tools were ...
Updates - Updates - April 2024
... 5 (v2.1→v3.0) Turla (v4.0→v5.0) Wizard Spider (v3.0→v4.0) ZIRCONIUM (v1.1→v2.0) menuPass (v2.1→v3.0) Minor Version Changes APT18 (v2.1→v2.2) APT19 (v1.5→v1.6) APT39 (v3.1→v3.2) BITTER (v1.0→v1.1) Blue Mockingbird (v1.1→v1.2) Dark Caracal (v1.3→v1.4) Elderwood (v1.2→v1.3) Group5 (v1.2→v1.3) HEXANE (v2.1→v2.2) Higaisa (v1.0→v1.1) Inception (v1.1→v1.2) Metador (v1.0→v1.1) Mofang (v1.0→v1.1) Molerats (v2.0→v2.1) ...
Updates - Updates - October 2024
... hanges Aquatic Panda (v1.1→v2.0) CURIUM (v2.0→v3.0) Ember Bear (v1.1→v2.0) Kimsuky (v4.0→v5.0) Volt Typhoon (v1.1→v2.0) Minor Version Changes APT28 (v5.0→v5.1) APT29 (v6.0→v6.1) APT41 (v4.0→v4.1) Blue Mockingbird (v1.2→v1.3) Gamaredon Group (v3.0→v3.1) HEXANE (v2.2→v2.3) Indrik Spider (v4.0→v4.1) Magic Hound (v6.0→v6.1) MuddyWater (v5.0→v5.1) OilRig (v4.0→v4.1) Sandworm Team (v4.0→v4.1) Turla (v5....

Home > Groups > Blue Mockingbird

Blue Mockingbird

Blue Mockingbird is a cluster of observed activity involving Monero cryptocurrency-mining payloads in dynamic-link library (DLL) form on Windows systems. The earliest observed Blue Mockingbird tools were created in December 2019.[1]

ID: G0108
Contributors: Tony Lambert, Red Canary
Version: 1.3
Created: 26 May 2020
Last Modified: 10 July 2024

Version Permalink

Techniques Used

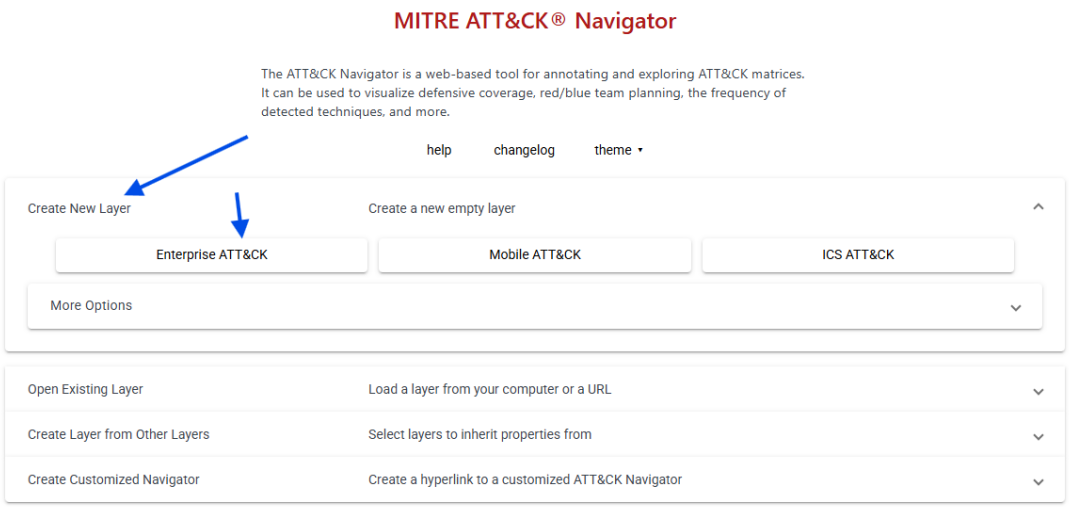
ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1134		Access Token Manipulation	Blue Mockingbird has used JuicyPotato to abuse the `SeImpersonate` token privilege to escalate from web application pool accounts to NT Authority\SYSTEM.[1]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	Blue Mockingbird has used PowerShell reverse TCP shells to issue interactive commands over a network connection.[1]
		.003	Command and Scripting Interpreter: Windows Command Shell	Blue Mockingbird has used batch script files to automate execution and deployment of payloads.[1]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	Blue Mockingbird has made their XMRIG payloads persistent as a Windows Service.[1]
Enterprise	T1546	.003	Event Triggered Execution: Windows Management Instrumentation Event Subscription	Blue Mockingbird has used mofcomp.exe to establish WMI Event Subscription persistence mechanisms configured from a *.mof file.[1]
Enterprise	T1190		Exploit Public-Facing Application	Blue Mockingbird has gained initial access by exploiting CVE-2019-18935, a vulnerability within Telerik UI

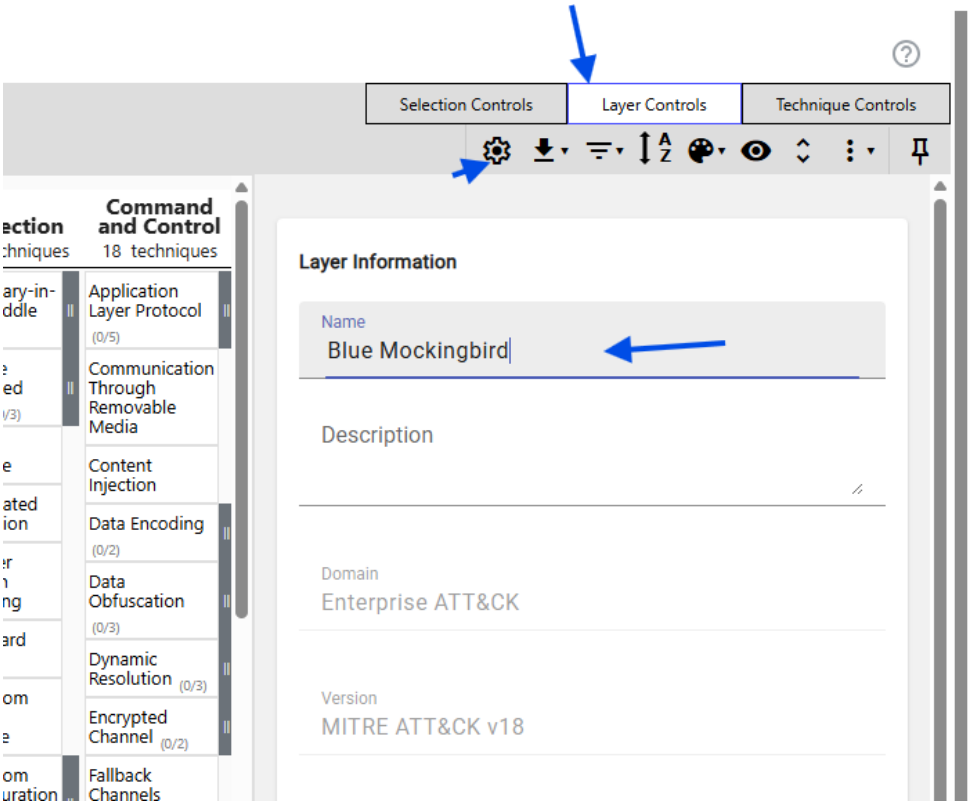
Now we go to Mire attack navigator to visualize and layer the techniques.

SSome APT groups have the same TTP, this will help us to create mitigants for that TP (an overlap) rather than create mitigants for each APT group.

In the browser, got to https://mitre-attack.github.io/attack-navigator/, select new layer, we will be using Enterprice (as we are simulation an enterprice environment)

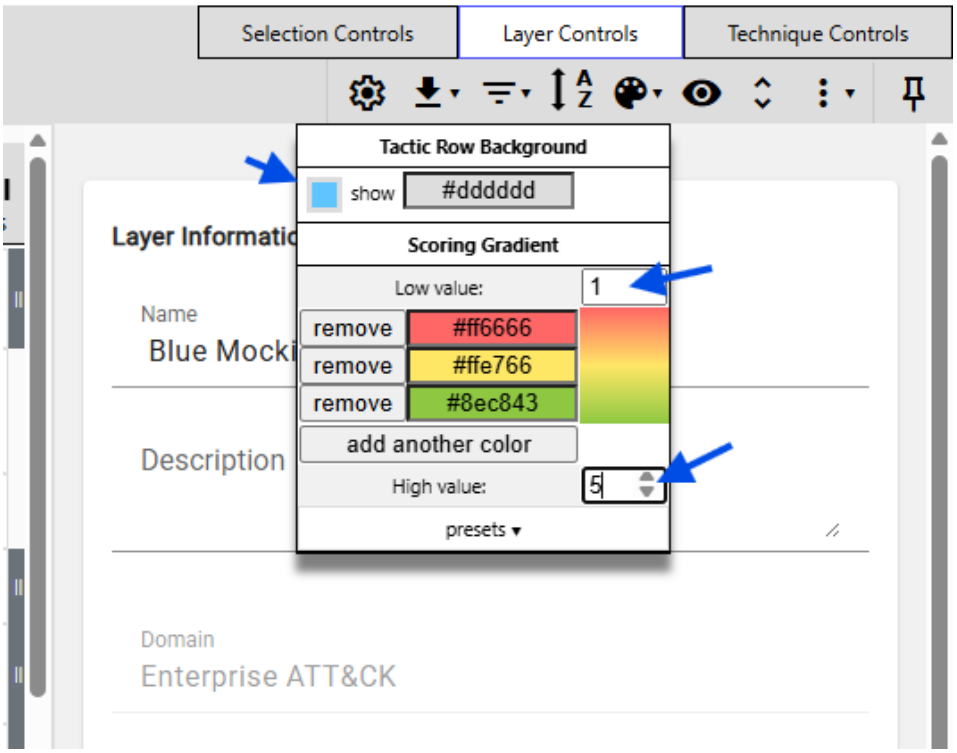


At the top right, select layer controls, clic the gear symbol and type in the name of the APT group under review



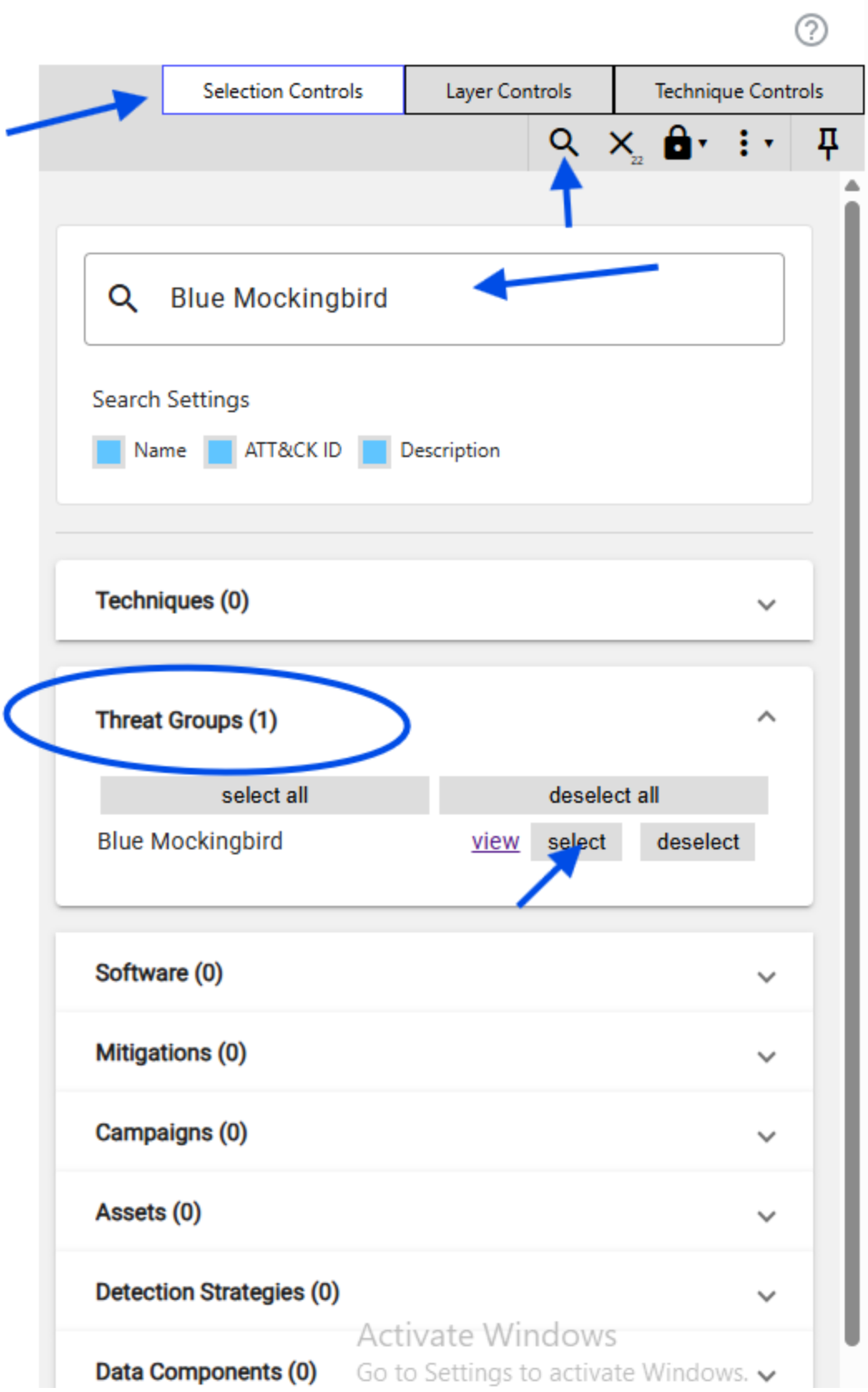
Next select the color palate and input the low and high value numbers, these numbers represent the number of APT groups we will be hunting.

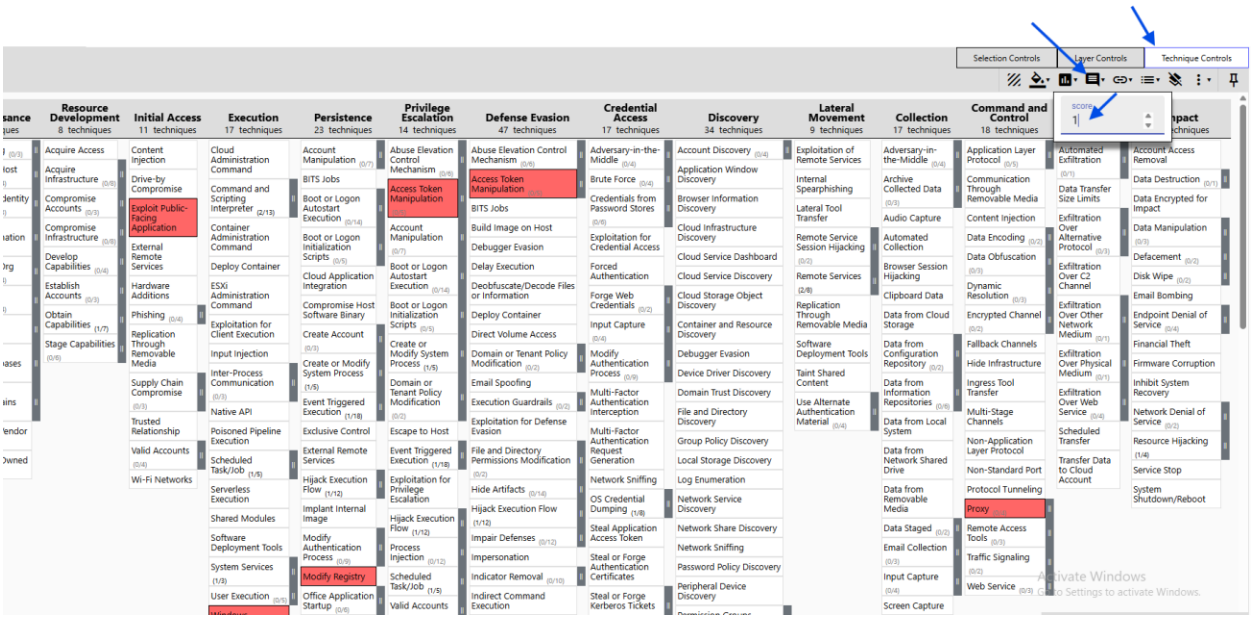
In this example we will review 5 APT groups of the banking industry. So low value will be 1 and high value will be 5



In the Selection controls, click on the search icon and paste the name of an APT group name, under the threat groups, click ‘select’. It will high light the TPP used by this APT group.

Next, in the technical controls, select score and assign a number (in this case 1, as we will be adding 4 more), it will assign this group a color

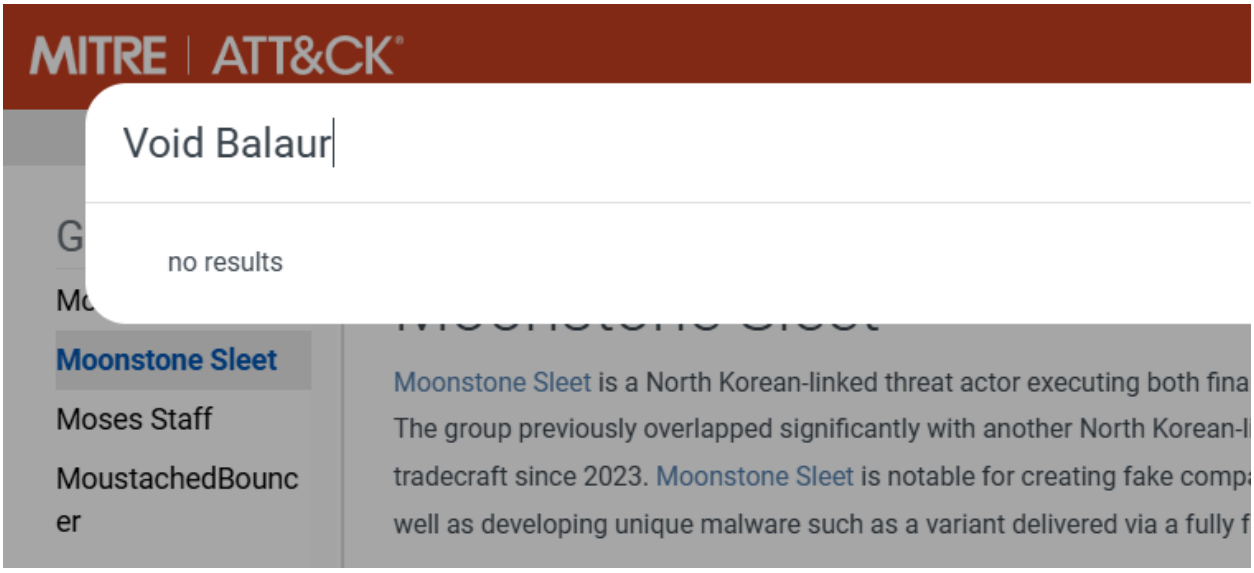

Selection Controls
Layer Controls
Technique Controls
Blue Mockingbird
Search Settings
Name
ATT&CK ID
Description
Techniques (0)
Threat Groups (1)
select all
deselect all
Blue Mockingbird
view
select
deselect
Software (0)
Mitigations (0)
Campaigns (0)
Assets (0)
Detection Strategies (0)
Data Components (0)
Activate Windows
Go to Settings to activate Windows.

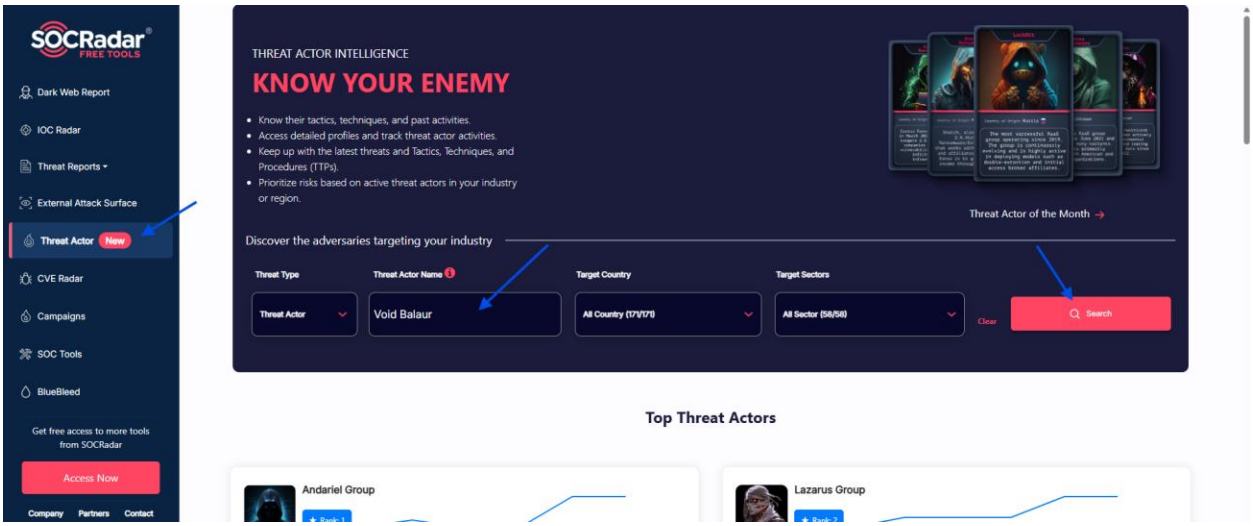


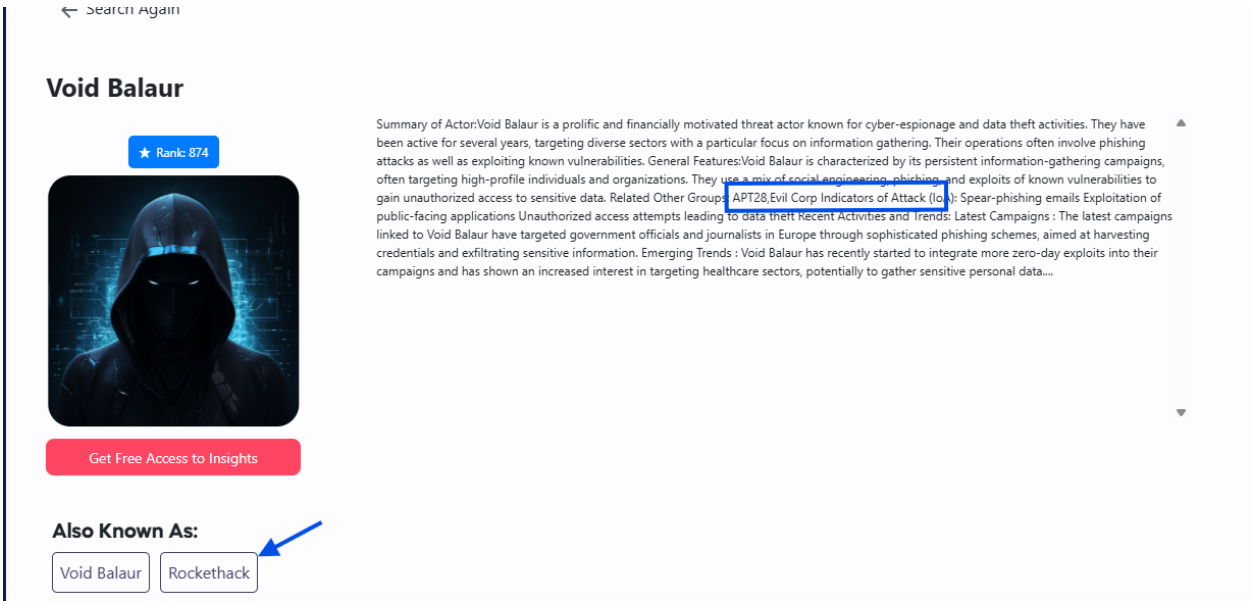
Now repeat this for other APT groups you want to review.

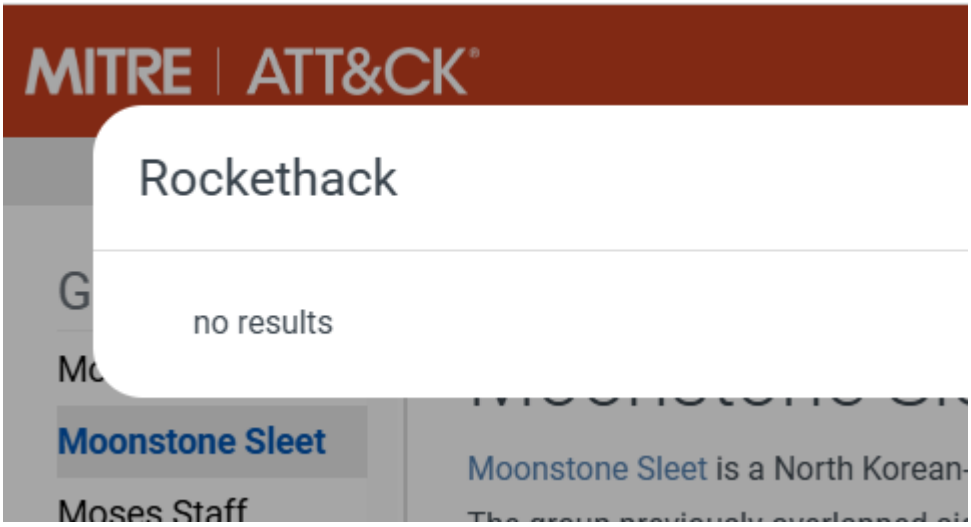
There are instances where we will not be able to find an APT group name. We then go to SOCRadar to see what other names or alias they have or groups they are associated with.

An example is seen below

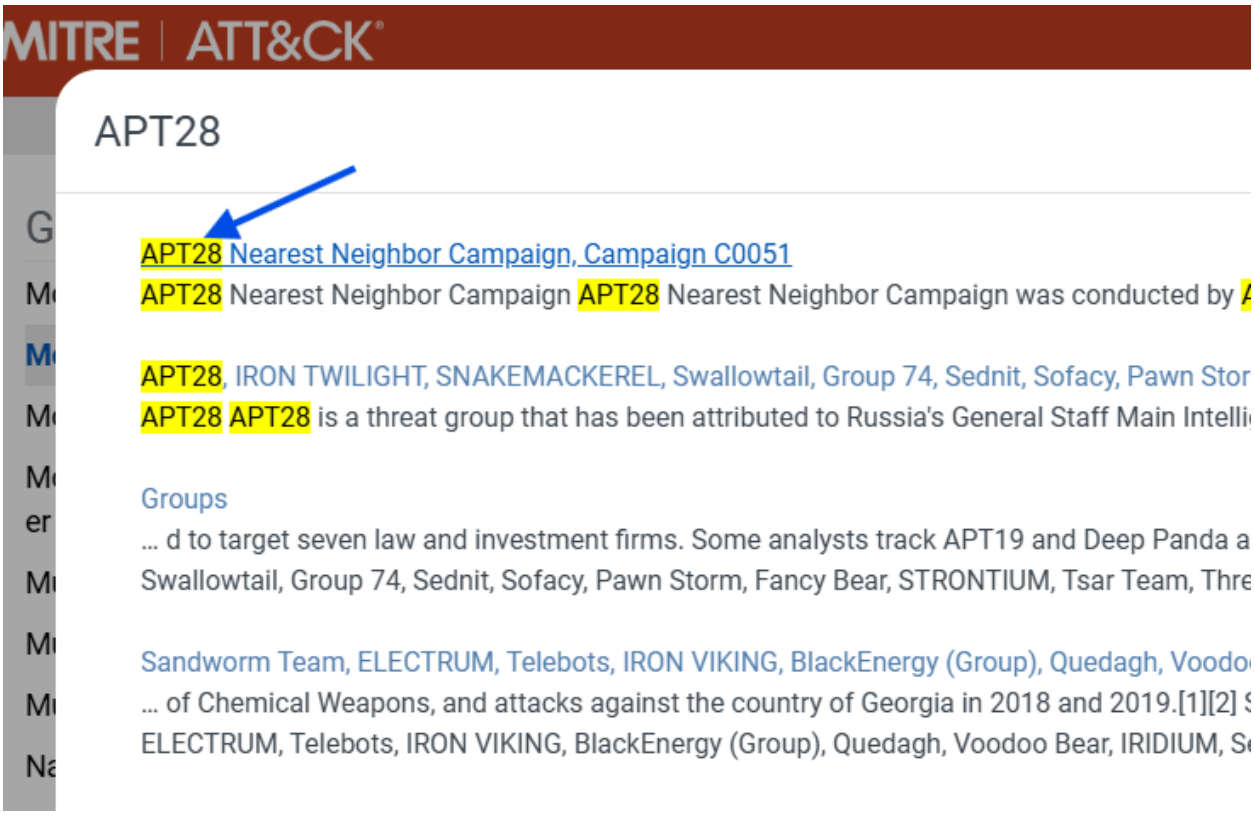


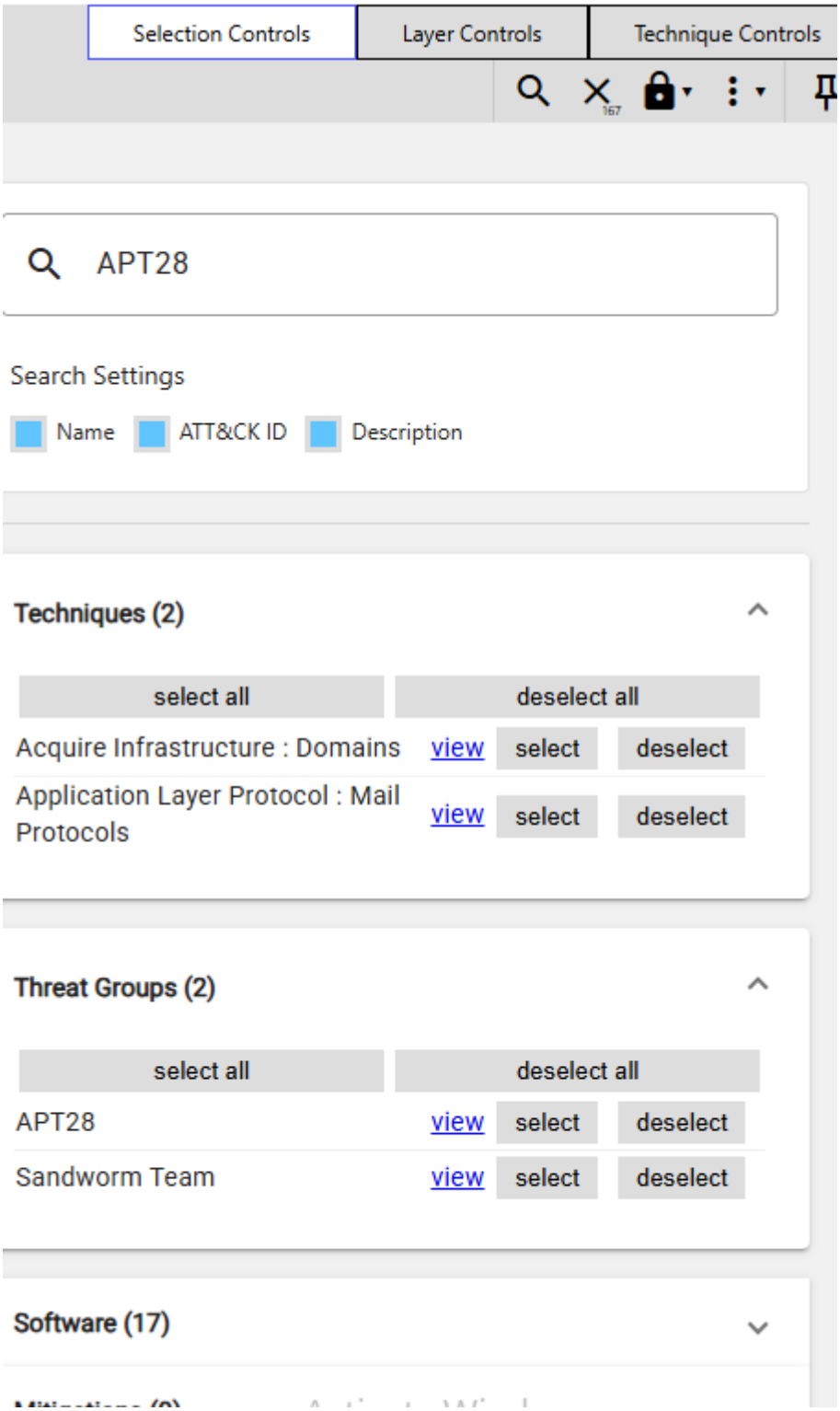

SOCRadar
FREE TOOLS
Dark Web Report
IOC Radar
Threat Reports
External Attack Surface
Threat Actor New
CVE Radar
Campaigns
SOC Tools
BlueBleed
Get free access to more tools from SOCRadar
Access Now
Company Partners Contact
THREAT ACTOR INTELLIGENCE
KNOW YOUR ENEMY
Know their tactics, techniques, and past activities.
Access detailed profiles and track threat actor activities.
Keep up with the latest threats and Tactics, Techniques, and Procedures (TTPs).
Prioritize risks based on active threat actors in your industry or region.
Threat Actor of the Month
Discover the adversaries targeting your industry
Threat Type
Threat Actor
Threat Actor Name
Void Balaur
Target Country
All Country (171/171)
Target Sectors
All Sector (58/58)
Clear
Search
Top Threat Actors
Andariel Group
Lazarus Group

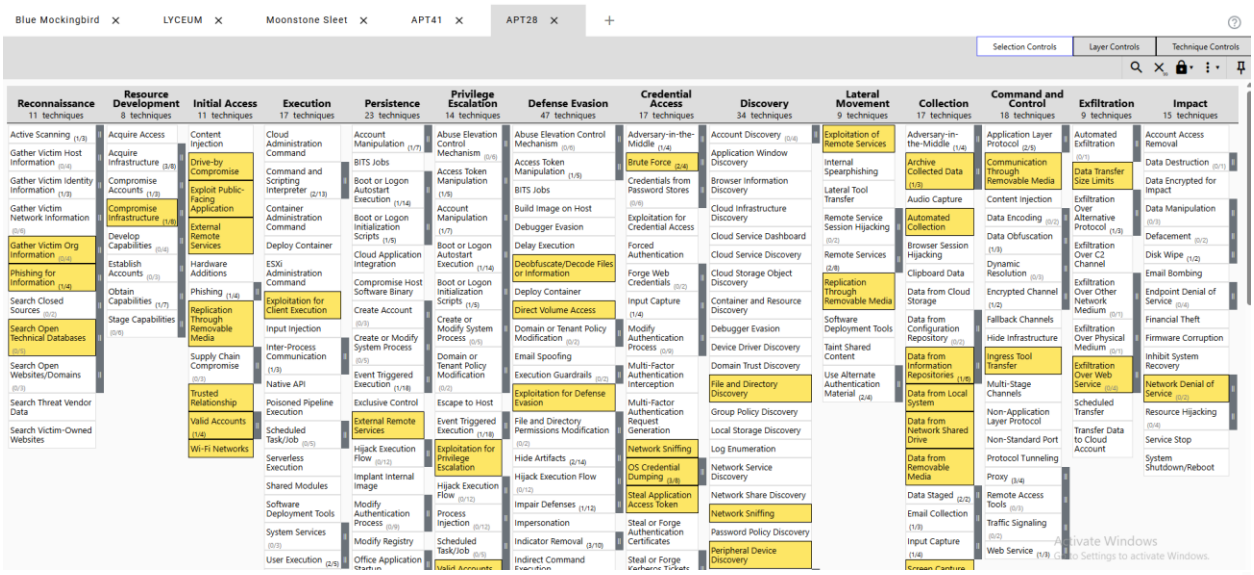

Search Again
Void Balaur
Rank: 874
Summary of Actor:Void Balaur is a prolific and financially motivated threat actor known for cyber-espionage and data theft activities. They have been active for several years, targeting diverse sectors with a particular focus on information gathering. Their operations often involve phishing attacks as well as exploiting known vulnerabilities. General Features:Void Balaur is characterized by its persistent information-gathering campaigns, often targeting high-profile individuals and organizations. They use a mix of social engineering, phishing, and exploits of known vulnerabilities to gain unauthorized access to sensitive data. Related Other Groups: APT28,Evil Corp Indicators of Attack (IoA): Spear-phishing emails Exploitation of public-facing applications Unauthorized access attempts leading to data theft Recent Activities and Trends: Latest Campaigns : The latest campaigns linked to Void Balaur have targeted government officials and journalists in Europe through sophisticated phishing schemes, aimed at harvesting credentials and exfiltrating sensitive information. Emerging Trends : Void Balaur has recently started to integrate more zero-day exploits into their campaigns and has shown an increased interest in targeting healthcare sectors, potentially to gather sensitive personal data....
Get Free Access to Insights
Also Known As:
Void Balaur
Rockethack

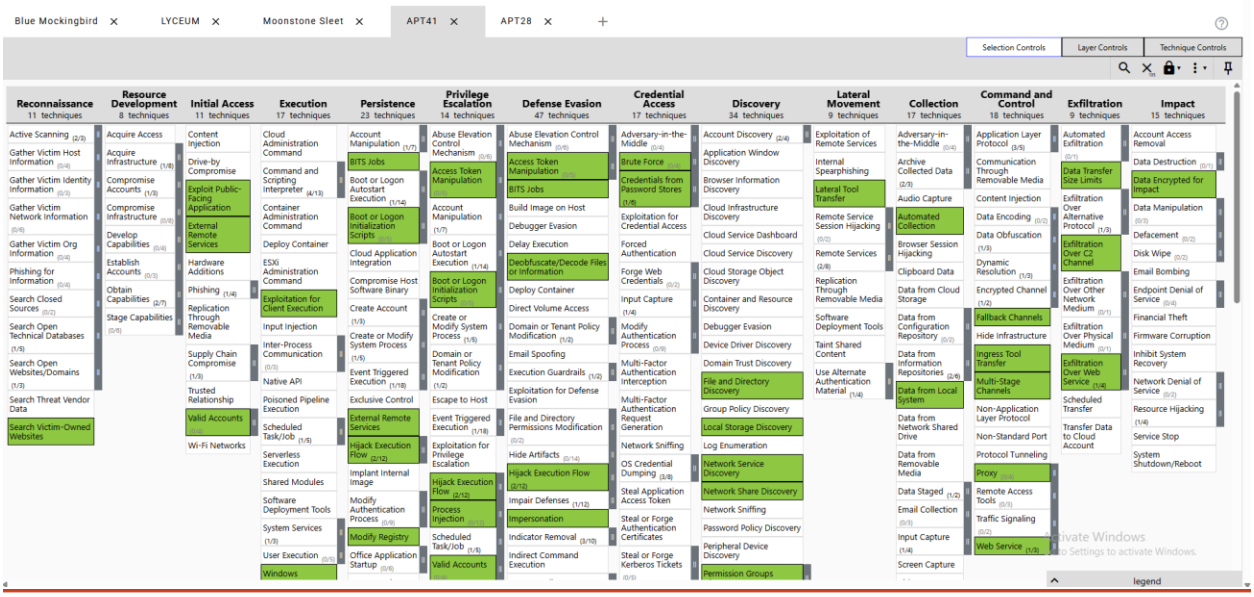

MITRE | ATT&CK
Rockethack
no results
Moonstone Sleet
Moonstone Sleet is a North Korean-
Moses Staff

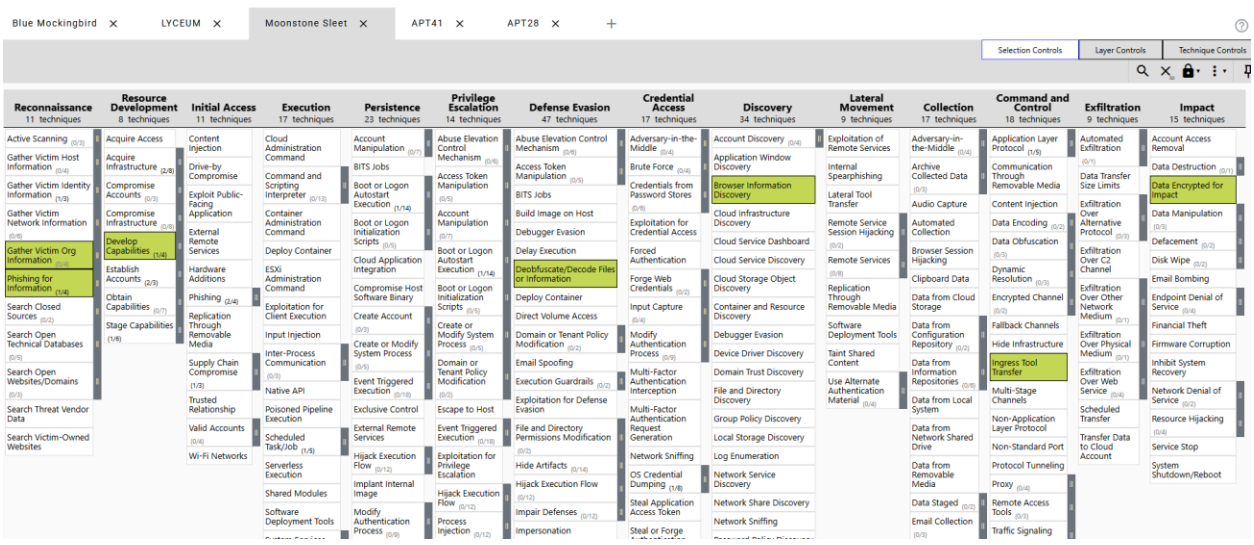
The name Rockethack is also not found in the mitre attack website, but its highlighted in SOCRadar they are associated with the name APT28

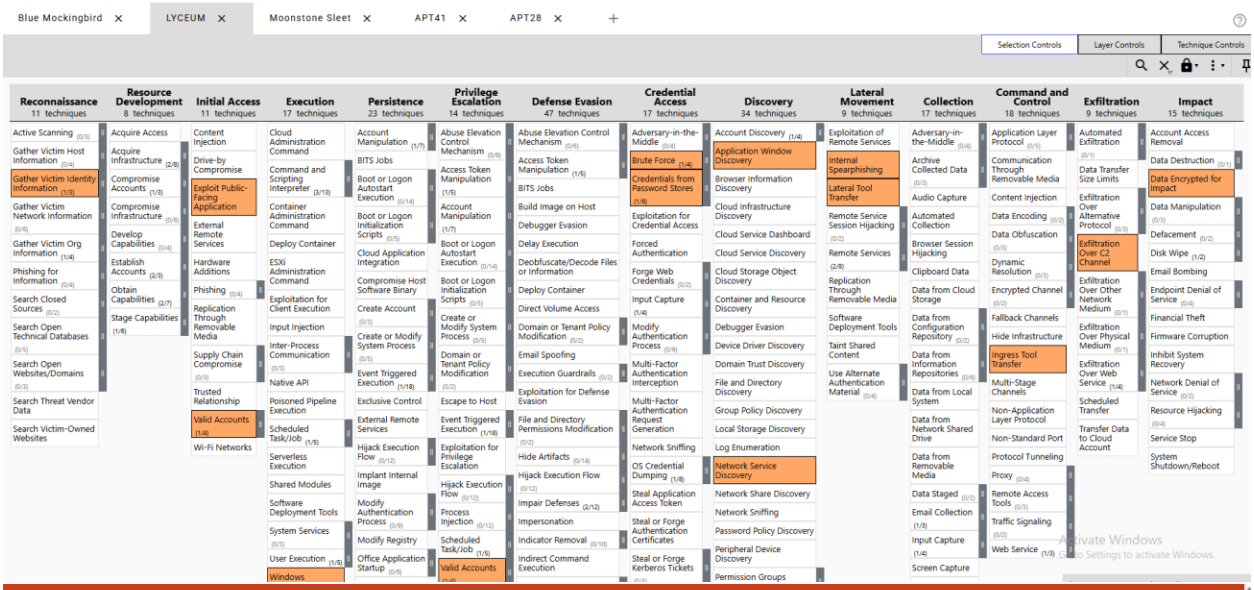


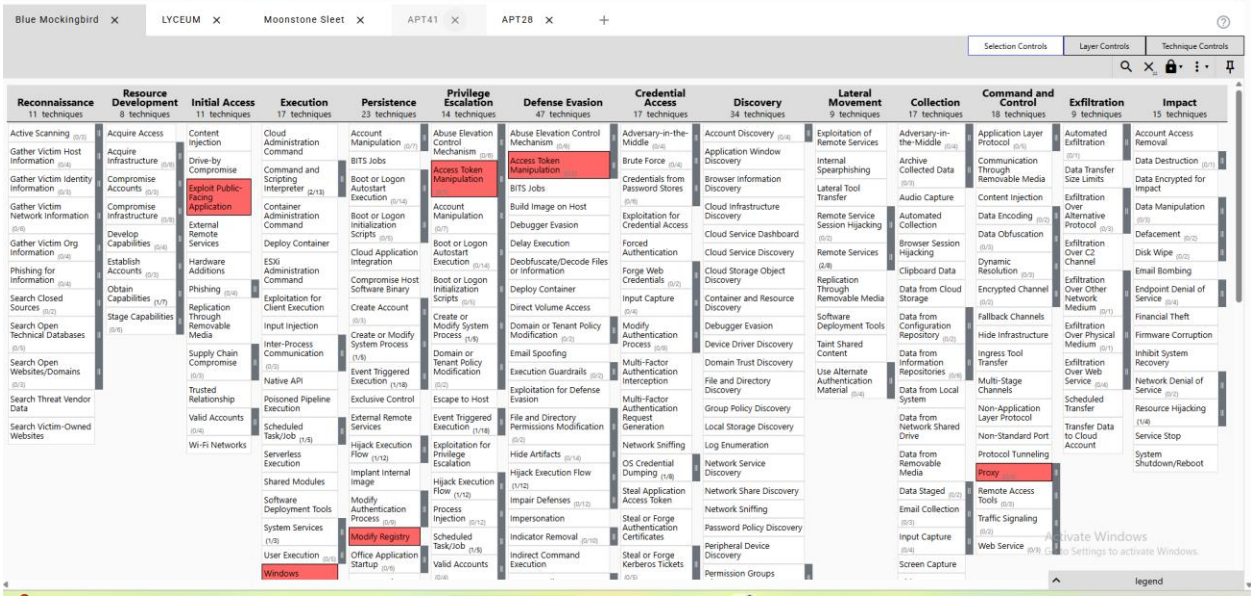

Selection Controls
Layer Controls
Technique Controls
APT28
Search Settings
Name
ATT&CK ID
Description
Techniques (2)
select all
deselect all
Acquire Infrastructure : Domains
view
select
deselect
Application Layer Protocol : Mail Protocols
view
select
deselect
Threat Groups (2)
select all
deselect all
APT28
view
select
deselect
Sandworm Team
view
select
deselect
Software (17)


Blue Mockingbird
LYCEUM
Moonstone Sleet
APT41
APT28
Selection Controls
Layer Controls
Technique Controls
Reconnaissance 11 techniques
Resource Development 8 techniques
Initial Access 11 techniques
Execution 17 techniques
Persistence 23 techniques
Privilege Escalation 14 techniques
Defense Evasion 47 techniques
Credential Access 17 techniques
Discovery 34 techniques
Lateral Movement 9 techniques
Collection 17 techniques
Command and Control 18 techniques
Exfiltration 9 techniques
Impact 15 techniques

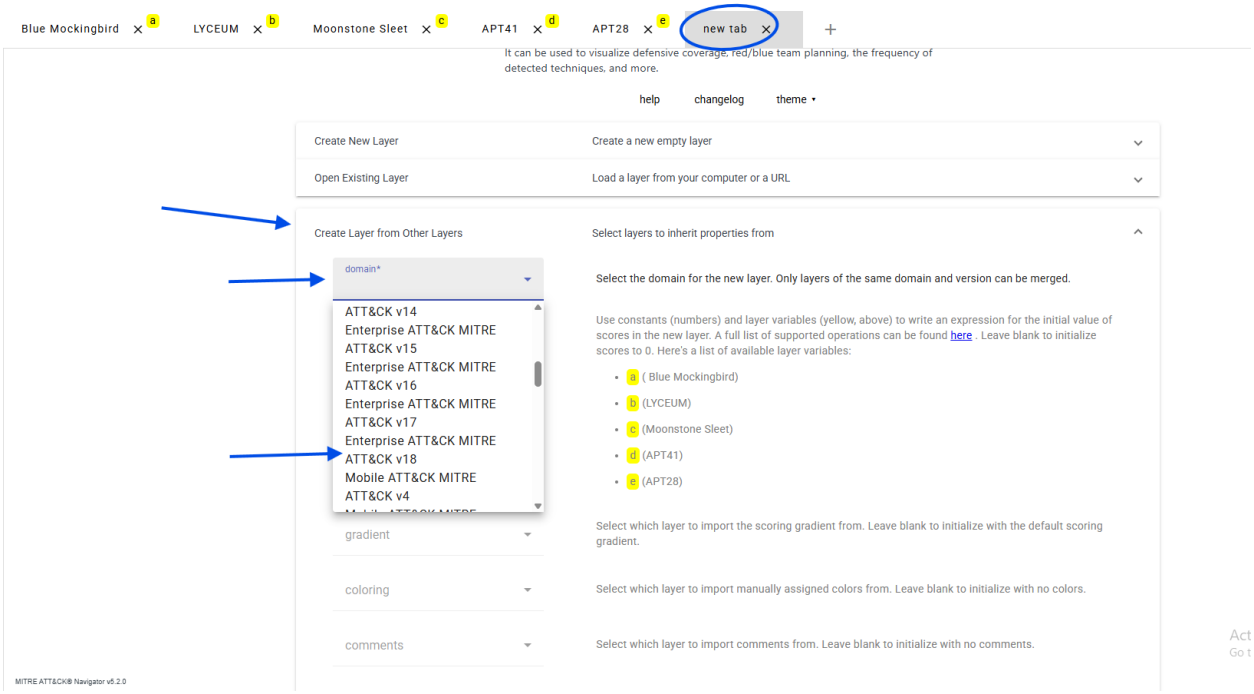

Blue Mockingbird
LYCEUM
Moonstone Sleet
APT41
APT28
Selection Controls
Layer Controls
Technique Controls
Reconnaissance 11 techniques
Resource Development 8 techniques
Initial Access 11 techniques
Execution 17 techniques
Persistence 23 techniques
Privilege Escalation 14 techniques
Defense Evasion 47 techniques
Credential Access 17 techniques
Discovery 34 techniques
Lateral Movement 9 techniques
Collection 17 techniques
Command and Control 18 techniques
Exfiltration 9 techniques
Impact 15 techniques
legend

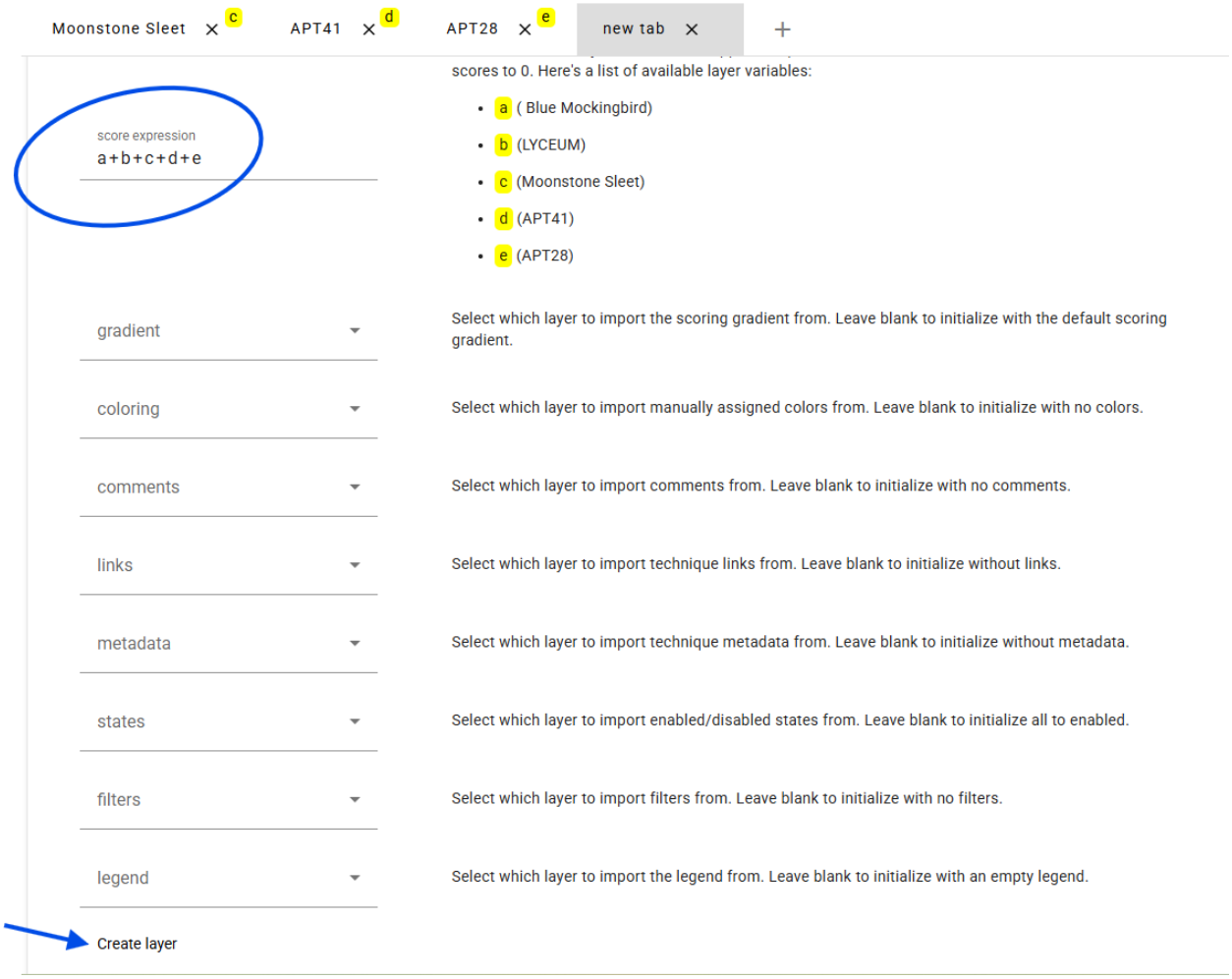

Blue Mockingbird
LYCEUM
Moonstone Sleet
APT41
APT28
Selection Controls
Layer Controls
Technique Controls
Reconnaissance 11 techniques
Resource Development 8 techniques
Initial Access 11 techniques
Execution 17 techniques
Persistence 23 techniques
Privilege Escalation 14 techniques
Defense Evasion 47 techniques
Credential Access 17 techniques
Discovery 34 techniques
Lateral Movement 9 techniques
Collection 17 techniques
Command and Control 18 techniques
Exfiltration 9 techniques
Impact 15 techniques

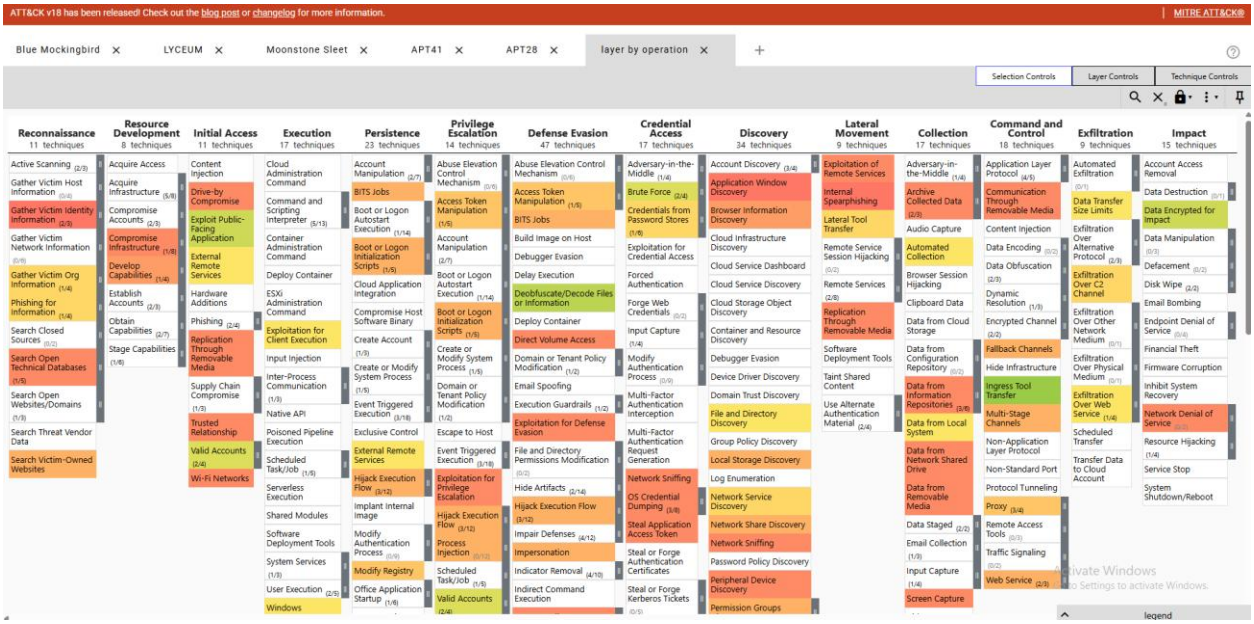

Blue Mockingbird
LYCEUM
Moonstone Sleet
APT41
APT28
Selection Controls
Layer Controls
Technique Controls
Reconnaissance 11 techniques
Resource Development 8 techniques
Initial Access 11 techniques
Execution 17 techniques
Persistence 23 techniques
Privilege Escalation 14 techniques
Defense Evasion 47 techniques
Credential Access 17 techniques
Discovery 34 techniques
Lateral Movement 9 techniques
Collection 17 techniques
Command and Control 18 techniques
Exfiltration 9 techniques
Impact 15 techniques
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
Acquire Access
Acquire Infrastructure
Compromise Accounts
Compromise Infrastructure
Develop Capabilities
Establish Accounts
Obtain Capabilities
Stage Capabilities
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
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
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
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
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
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
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
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
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
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
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
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
ATT&CK v18 has been released! Check out the blog post or changelog for more information.
MITRE ATT&CK®
Activate Windows
Go to Settings to activate Windows.

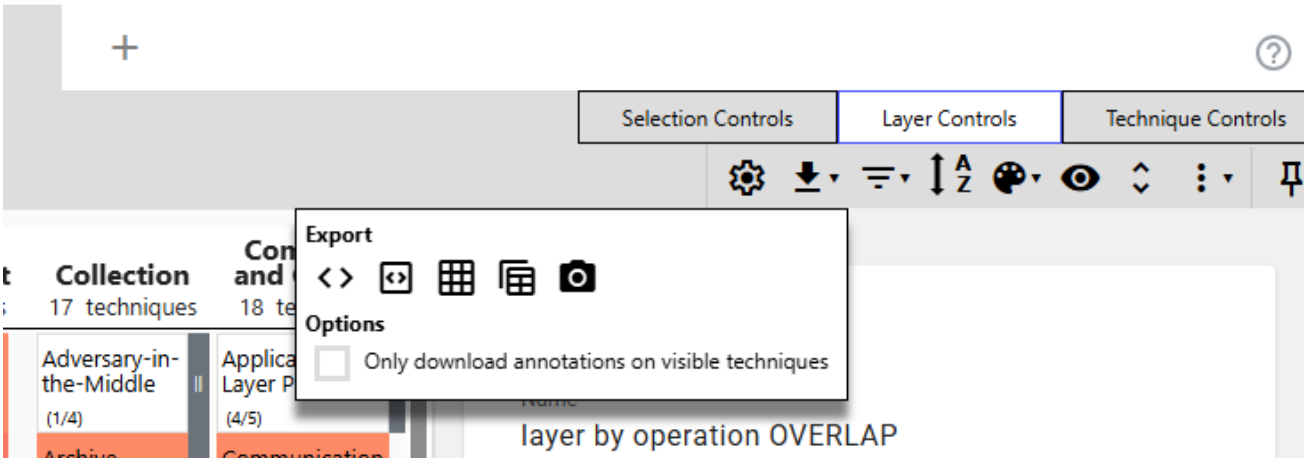

Blue Mockingbird
LYCEUM
Moonstone Sleet
APT41
APT28
Selection Controls
Layer Controls
Technique Controls
Reconnaissance 11 techniques
Resource Development 8 techniques
Initial Access 11 techniques
Execution 17 techniques
Persistence 23 techniques
Privilege Escalation 14 techniques
Defense Evasion 47 techniques
Credential Access 17 techniques
Discovery 34 techniques
Lateral Movement 9 techniques
Collection 17 techniques
Command and Control 18 techniques
Exfiltration 9 techniques
Impact 15 techniques
Windows
Proxy
Modify Registry
Access Token Manipulation
Activate Windows
Go to Settings to activate Windows.
legend

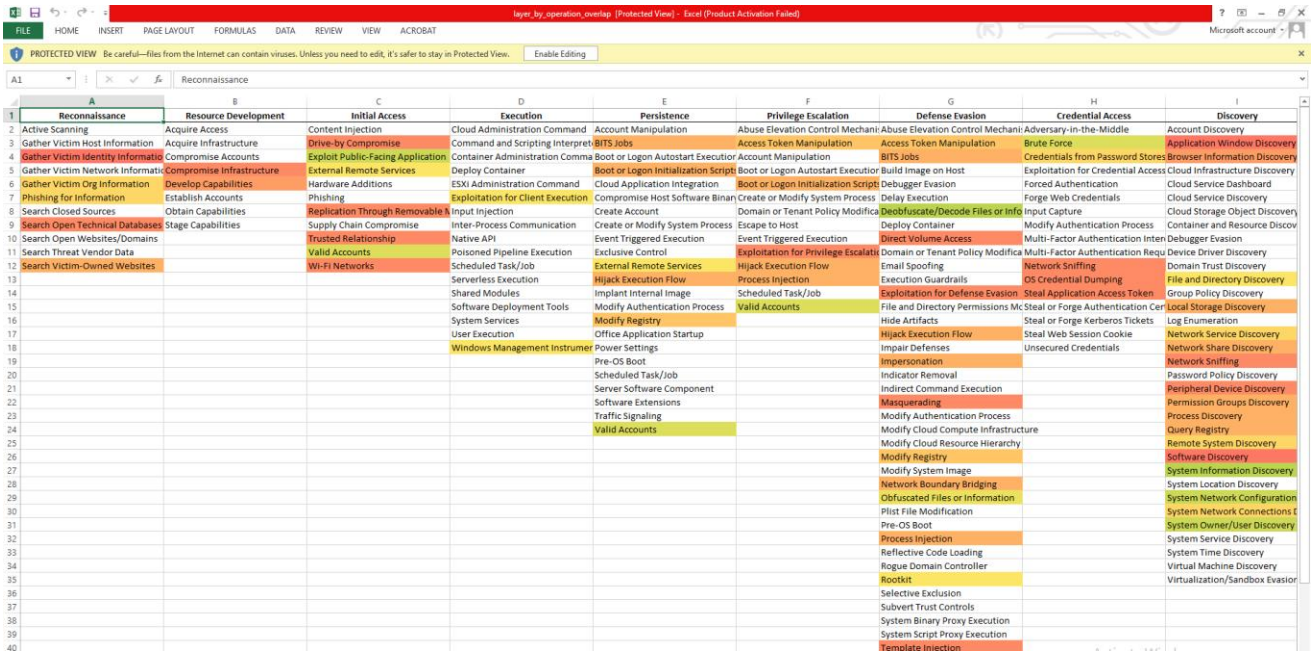
Once all 5 layers have been created, we then create a layer overlap and export






ATT&CK v18 has been released! Check out the blog post or changelog for more information.
MITRE ATT&CK®
Blue Mockingbird
LYCEUM
Moonstone Sleet
APT41
APT28
layer by operation
Selection Controls
Layer Controls
Technique Controls
Reconnaissance
11 techniques
Resource Development
8 techniques
Initial Access
11 techniques
Execution
17 techniques
Persistence
23 techniques
Privilege Escalation
14 techniques
Defense Evasion
47 techniques
Credential Access
17 techniques
Discovery
34 techniques
Lateral Movement
9 techniques
Collection
17 techniques
Command and Control
18 techniques
Exfiltration
9 techniques
Impact
15 techniques
legend


Selection Controls
Layer Controls
Technique Controls
Export
Options
Only download annotations on visible techniques
Collection
17 techniques
Adversary-in-the-Middle
(1/4)
(4/5)
layer by operation OVERLAP



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
Active Scanning	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechani	Abuse Elevation Control Mechani	Adversary-in-the-Middle	Account Discovery
Gather Victim Host Information	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpret	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery
Gather Victim Identity Informatio	Compromise Accounts	Exploit Public-Facing Application	Container Administration Comma	Boot or Logon Autostart Executior	Account Manipulation	BITS Jobs	Credentials from Password Stores	Browser Information Discovery
Gather Victim Network Informatio	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Initialization Script	Boot or Logon Autostart Executior	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery
Gather Victim Org Information	Develop Capabilities	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Initialization Script	Debugger Evasion	Forced Authentication	Cloud Service Dashboard
Phishing for Information	Establish Accounts	Phishing	Exploitation for Client Execution	Compromise Host Software Binar	Create or Modify System Process	Delay Execution	Forge Web Credentials	Cloud Service Discovery
Search Closed Sources	Obtain Capabilities	Replication Through Removable M	Input Injection	Create Account	Domain or Tenant Policy Modifica	Deobfuscate/Decode Files or Info	Input Capture	Cloud Storage Object Discovery
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 Discov
Search Open Websites/Domains		Trusted Relationship	Native API	Event Triggered Execution	Event Triggered Execution	Direct Volume Access	Multi-Factor Authentication Inter	Debugger Evasion
Search Threat Vendor Data		Valid Accounts	Poisoned Pipeline Execution	Exclusive Control	Exploitation for Privilege Escalatio	Domain or Tenant Policy Modifica	Multi-Factor Authentication Requ	Device Driver Discovery
Search Victim-Owned Websites		Wi-Fi Networks	Scheduled Task/Job	External Remote Services	Hijack Execution Flow	Email Spoofing	Network Sniffing	Domain Trust Discovery
			Serverless Execution	Hijack Execution Flow	Process Injection	Execution Guardrails	OS Credential Dumping	File and Directory Discovery
			Shared Modules	Implant Internal Image	Scheduled Task/Job	Exploitation for Defense Evasion	Steal Application Access Token	Group Policy Discovery
			Software Deployment Tools	Modify Authentication Process	Valid Accounts	File and Directory Permissions Mc	Steal or Forge Authentication Cer	Local Storage Discovery
			System Services	Modify Registry		Hide Artifacts	Steal or Forge Kerberos Tickets	Log Enumeration
			User Execution	Office Application Startup		Hijack Execution Flow	Steal Web Session Cookie	Network Service Discovery
			Windows Management Instrumer	Power Settings		Impair Defenses	Unsecured Credentials	Network Share Discovery
				Pre-OS Boot		Impersonation		Network Sniffing
				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
						Plist File Modification		System Network Connections D
						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 Evasior
						Selective Exclusion		
						Subvert Trust Controls		
						System Binary Proxy Execution		
						System Script Proxy Execution		
						Template Injection		

Conclusion

Threat hunting is a vital component of modern cyber security operations, especially given the rise of APTs and sophisticated threat actors. By leveraging intelligence-driven methodologies, understanding TTPs, and utilizing powerful tools like MITRE ATT&CK, ATT&CK Navigator, and SOC Radar, organizations can significantly enhance their detection and response capabilities.

Effective threat hunting transforms an organization from being reactive to proactive—staying ahead of adversaries and ensuring a more resilient security posture.