

Threat Hunting Report (practical documentation).

by: Samsudeen Olapade

1. Introduction

Threat hunting is a proactive cybersecurity practice that involves the systematic search for hidden threats within an organization's IT environment. Unlike traditional security monitoring, which relies primarily on automated alerts and predefined rules, threat hunting focuses on detecting advanced, persistent, and stealthy threats (APTs) that may evade security tools such as firewalls, intrusion detection systems (IDS), or antivirus solutions.

The primary goal of threat hunting is to reduce the *dwell time* of attackers, limit the impact of breaches, and enhance the overall security posture of an organization.

2. Objectives of Threat Hunting

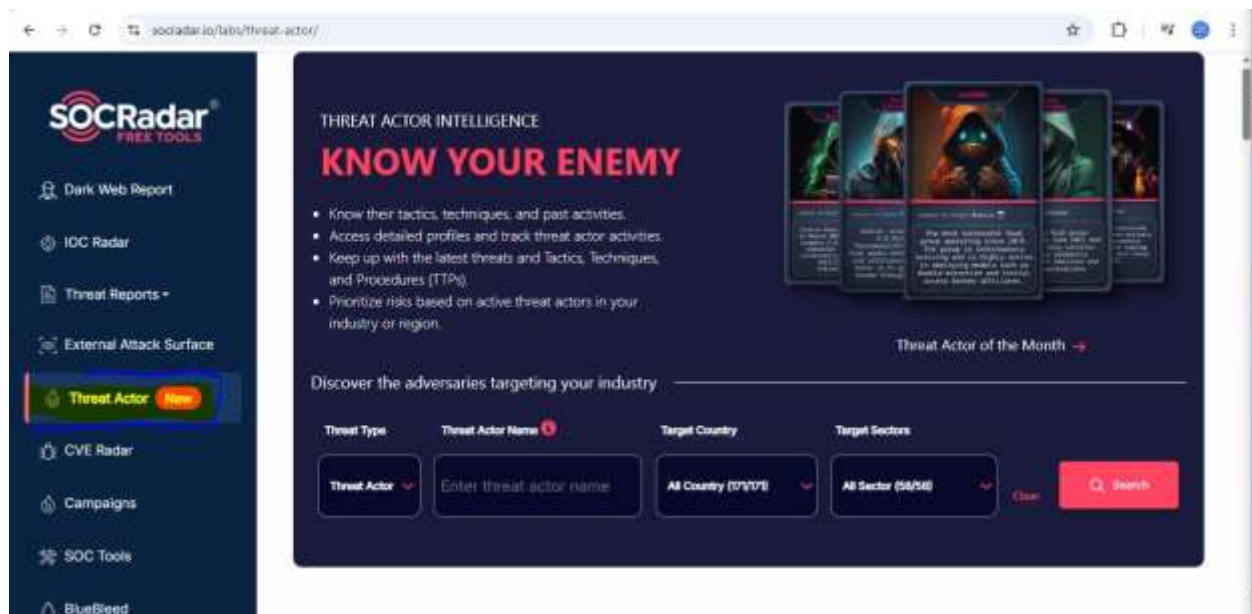
- Identify threats that bypass traditional defenses.
- Detect indicators of compromise (IOCs) and indicators of attack (IOAs).
- Reduce false positives from automated detection systems.
- Enhance incident response capabilities.
- Provide actionable threat intelligence for future defense strategies.


3. Threat Hunting Process

Threat hunting generally follows a structured approach, often based on three key phases:

a. Gathering of Intel

This is the first stage of Threat hunting, in this stage, '**Socradar.io**' is used. Here we want to know what APTs are peculiar to each organisations/country. In the homepage of socradar.io, we will navigate by clicking on 'Free Tools', then 'Threat Actors'(here we will see different threat actors associated with different countries). On the left handside of the page, we wil click on 'Threat Report' then 'Industry Threat Landscape Report'. For the purpose of this report, we will be working on Automotive Industry.





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

Top Threat Actors



TA428

Rank 1

967k

Audience


7k


News


39k


IOC


Target Countries:

 Belarus

 Russia

 Ukraine

 Mongolia


 Afghanistan


+1


Target Sectors:


Industrial plants, design bureaus and research institutes - Government -


Associated Malware/Software:

 win.police

 ET

 asp.bwoface

 win.hypertro



Comment Crew

Rank 2

339k

Audience


5k


News


5k


IOC


Target Countries:

 South Africa

 Canada

 Norway

 India


 France


+12


Target Sectors:


Non-profit organizations - Engineering - Financial - Satellite - IT -


Associated Malware/Software:

 PolSec

 WEBIC2

 win.kurton

 FloutE

 win.webc2.jsle

+18

IOC Radar

Threat Reports +

Industry Threat Landscape Report

Country Threat Landscape Report

External Threat Assessment Report

External Attack Surface

Threat Actor

CVE Radar

Campaigns

SOC Tools

BlueBleed

Get free access to more tools from SOCRadar

Access Now

Company Partners Contact

HealthCare & Social Assistance

Telecommunications

Finance

Insurance

Energy & Utilities

Public Administration

Retail

Delivery Services

Enterprises & Holding

Professional&Technical Services

Transportation&Warehousing

CryptoCurrency & NFT

Automotive

Educational Services

Gaming

Construction




Mining

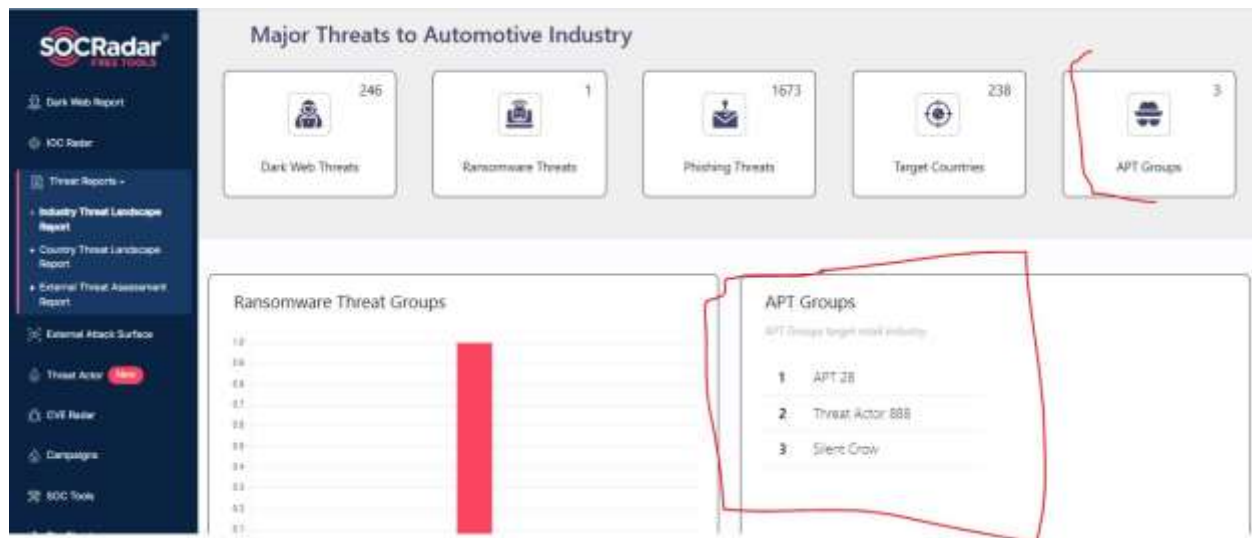
Rental & Leasing

Accommodation&Food Services

Arts & Entertainment

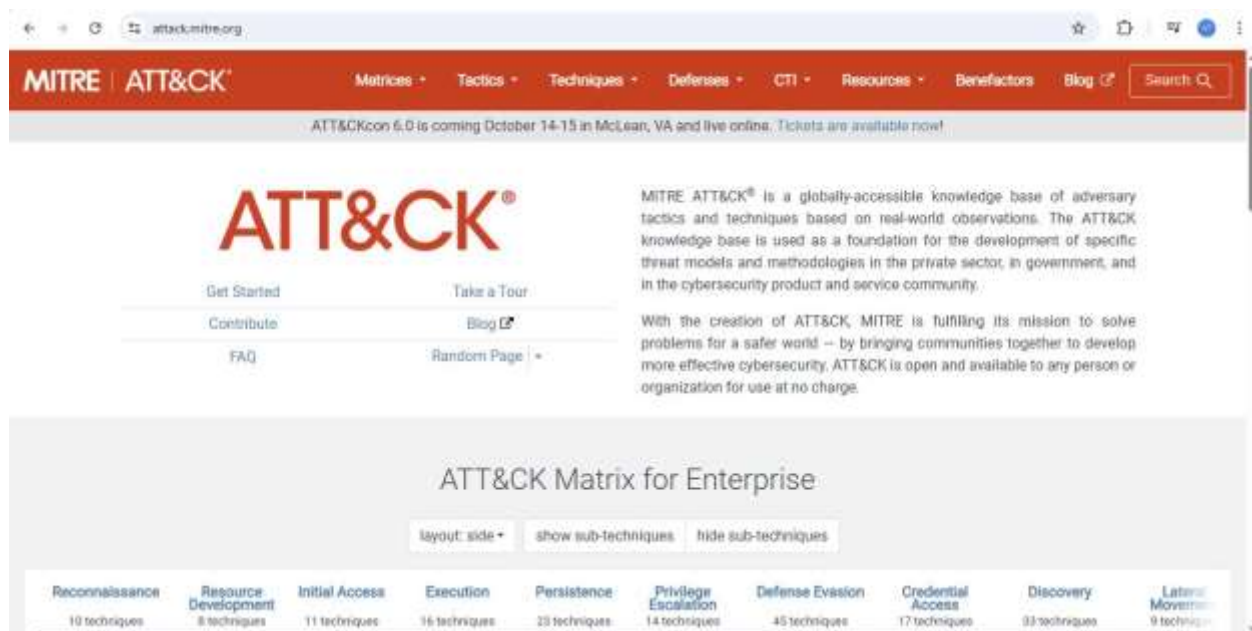
Copyright © 2023 SOCRadar Cyber Intelligence Inc. All rights reserved.
































































































































































































































b. Understand their TTPs (Tactics, Techniques, Procedures)



In this stage, we go on 'attack.mitre.org' to understand what TTPs are and what they stand for.



MITRE ATT&CK									
Matrices • Tactics • Techniques • Defenses • CTI • Resources • Benefactors • Blog  Search 									
layout: side • show sub-techniques hide sub-techniques									
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
10 techniques	4 techniques	11 techniques	16 techniques	23 techniques	14 techniques	45 techniques	17 techniques	33 techniques	9 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/Content  Search Victim-Owned Websites 	Acquire Access  Acquire Infrastructure  Compromise Accounts  Compromise Infrastructure  Develop Capabilities  Establish Accounts  Obtain Capabilities  Stage Capabilities  Supply Chain Compromise  Trusted Relationship  Valid Accounts 	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 	Cloud Administration Command  Command and Scripting Interpreter  Container Administration Command  Deploy Container  ESX Administration Command  Exploitation for Client Execution  Input Injection  Inter-Process Communication  Native API  Scheduled Task/job  Serviceless 	Account Manipulation  BITS Jobs  Boot or Logon Autostart Execution  Boot or Logon Initialization Scripts  Cloud Application Integration  Compromise Host Software Binary  Create or Modify System Process  Create Account  Create or Modify System Process  Event Triggered Execution  Event Triggered Execution 	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  Domain or Tenant Policy Modification  Escape to Host  Event Triggered Execution 	Abuse Elevation Control Mechanism  Access Token Manipulation  BITS Jobs  Build Image on Host  Debugger Evasion  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 	Adversary in-the-Middle  Brute Force  Credentials from Password Store  Exploitation for Credential Access  Forced Authentication  Forge Web Credentials  Input Capture  Modify Authentication Process  Multi-Factor Authentication Interception  Multi-Factor 	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 	Exploitation of Remote Services  Internal Spearphishing  Lateral Tool Transfer  Remote Service Session Hijacking  Remote Service Session Hijacking  Remote Service Session Hijacking  Replication Through Removable Media  Software Deployment Tools  Taint Shared Content  Use Alternative Authentication 
https://attack.mitre.org/techniques/T1197									

MITRE ATT&CK									
Matrices • Tactics • Techniques • Defenses • CTI • Resources • Benefactors • Blog  Search 									
layout: side • show sub-techniques hide sub-techniques									
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
10 techniques	4 techniques	11 techniques	16 techniques	23 techniques	14 techniques	45 techniques	17 techniques	33 techniques	9 techniques
Scanning IP Blocks  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/Content 	Acquire Access  Acquire Infrastructure  Compromise Accounts  Compromise Infrastructure  Develop Capabilities  Establish Accounts  Obtain Capabilities  Stage Capabilities  Supply Chain Compromise  Trusted Relationship  Valid Accounts 	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 	Cloud Administration Command  Command and Scripting Interpreter  Container Administration Command  Deploy Container  ESX Administration Command  Exploitation for Client Execution  Input Injection  Inter-Process Communication  Native API  Scheduled Task/job  Serviceless 	Account Manipulation  BITS Jobs  Boot or Logon Autostart Execution  Boot or Logon Initialization Scripts  Cloud Application Integration  Compromise Host Software Binary  Create or Modify System Process  Create Account  Create or Modify System Process  Event Triggered Execution  Event Triggered Execution 	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  Domain or Tenant Policy Modification  Escape to Host  Event Triggered Execution 	Abuse Elevation Control Mechanism  Access Token Manipulation  BITS Jobs  Build Image on Host  Debugger Evasion  Deobfuscate/Decode File or Information  Deploy Container  Direct Volume Access  Domain or Tenant Policy Modification  Email Spoofing  Execution Guardrails  Exploitation for Defense Evasion  File and Directory Permissions 	Adversary in-the-Middle  Brute Force  Credentials from Password Store  Exploitation for Credential Access  Forced Authentication  Forge Web Credentials  Input Capture  Modify Authentication Process  Multi-Factor Authentication Interception  Multi-Factor 	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 	Exploitation of Remote Services  Internal Spearphishing  Lateral Tool Transfer  Remote Service Session Hijacking  Remote Service Session Hijacking  Remote Service Session Hijacking  Replication Through Removable Media  Software Deployment Tools  Taint Shared Content  Use Alternative Authentication 
https://attack.mitre.org/techniques/T1211									

MITRE | ATT&CK

Matrices • Tactics • Techniques • Defenses • CTI • Resources • Benefactors • Blog  Search 

ATT&CKon 6.0 is coming October 14-15 in McLean, VA and live online. Tickets are available now!

TECHNIQUES

Enterprise

Reconnaissance

Active Scanning

Scanning IP Blocks

Vulnerability Scanning

Wordlist Scanning

Gather Victim

Active Scanning

Sub-techniques (3)

Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.

Adversaries may perform different forms of active scanning depending on what

ID: T1595

Sub-techniques: T1595.001, T1595.002, T1595.003

Tactic: Reconnaissance

Platforms: PRE

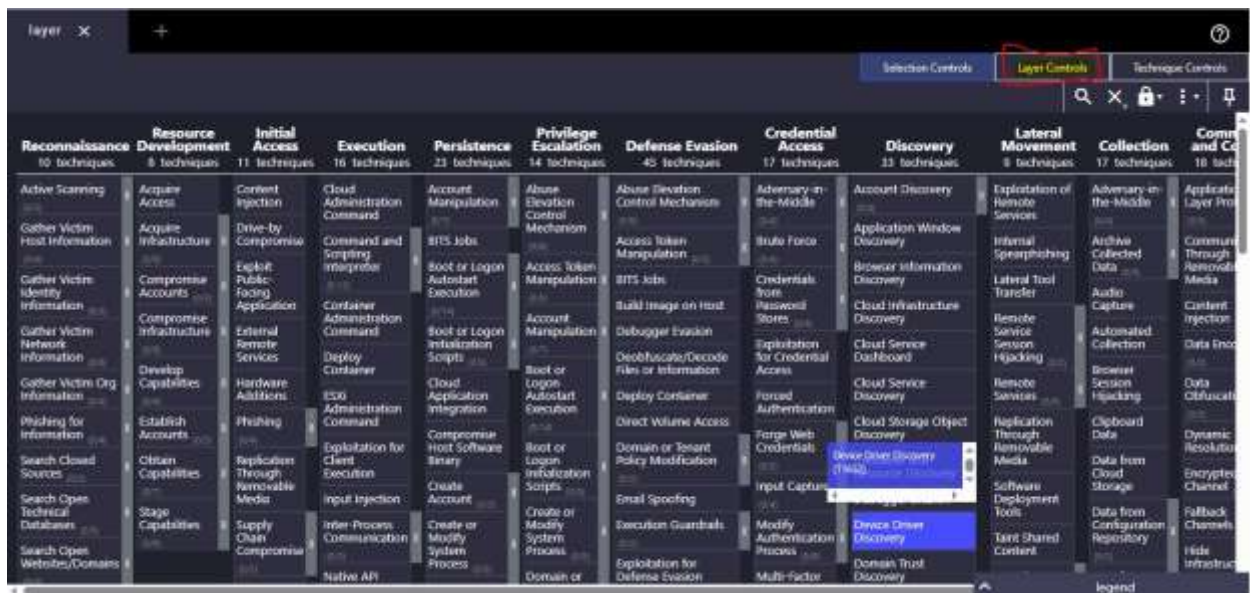
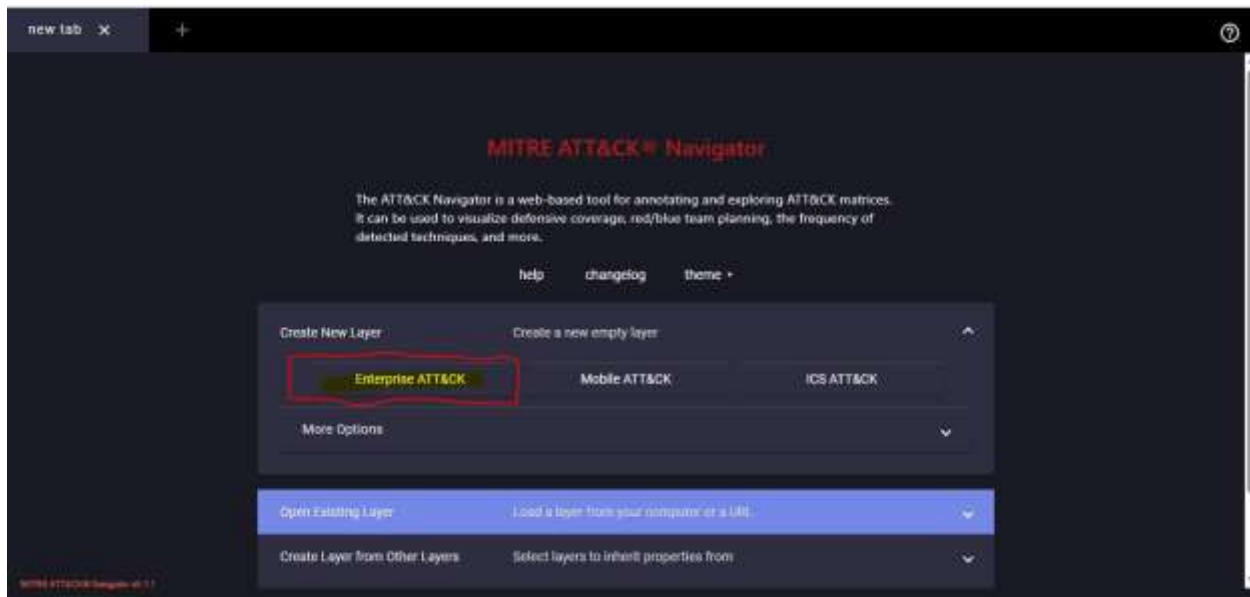
Version: 1.0

Created: 02 October 2020

c. Using Mitre Navigator to map the TTPs to APTs

Here, we go on "mitre-attack.github.io/attack-navigator/" , on the homepage, we navigate by clicking on 'Create New Layer', then 'Enterprise ATT&CK' to map out the three APT groups associated to the Automotive Industry. 1. Click on Layer, setting icon to search for the APT group, click on the color icon to set the color from 1-3 because we only have three groups associated to this industry. 2. Click on Selection Controls to select the APT group. 3. Click on Technique Controls to give a score like 1, being number one on the group.







APT 28 mapping (wine color- 1)

APT 28 X Tg 888/3390 X Silent Crow/ Silent Librarian X layer by operation X +

Selection Controls Layer Controls Technique Controls

Reconnaissance 10 techniques Resource Development 8 techniques Initial Access 11 techniques Execution 16 techniques Persistence 23 techniques Privilege Escalation 14 techniques Defense Evasion 45 techniques Credential Access 17 techniques Discovery 23 techniques Lateral Movement 9 techniques Collection 17 techniques Command and Control 18 techniques Exfiltration 9 techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
Active Scanning (1/10)	Acquire Access (1/8)	Context Injection (1/11)	Cloud Administration Command (1/16)	Account Manipulation (1/23)	Abuse Elevation Control Mechanism (1/14)	Abuse Elevation Control Mechanism (1/45)	Adversary in the Middle (1/17)	Account Discovery (1/23)	Exploitation of Remote Services (1/9)	Adversary in the Middle (1/17)	Application Layer Protocol (1/18)	Automated Exfiltration (1/9)
Gather Victim Host Information (1/10)	Acquire Infrastructure (1/8)	Drive-by Compromise (1/11)	Command and Scripting Interpreter (1/16)	BITS Jobs (1/23)	Access Token Manipulation (1/14)	Access Token Manipulation (1/45)	Brute Force (1/17)	Application Window Discovery (1/23)	Internal Spearphishing (1/9)	Archive Collected Data (1/17)	Communication Through Removable Media (1/18)	Data Transfer Out Links (1/9)
Gather Victim Identity Information (1/10)	Compromise Accounts (1/8)	Exploit Public-Facing Application (1/11)	Container Administration Command (1/16)	Boot or Logon Autostart Execution (1/23)	Account Manipulation (1/14)	Build Image on Host (1/45)	Credentials from Password Stores (1/17)	Browser Information Discovery (1/23)	Lateral Tool Transfer (1/9)	Audio Capture (1/17)	Content Injection (1/18)	Exfiltration Over Alternative Protocol (1/9)
Gather Victim Network Information (1/10)	Compromise Infrastructure (1/8)	External Remote Services (1/11)	Deploy Container (1/16)	Boot or Logon Initialization Scripts (1/23)	Root or Logon Initialization Scripts (1/14)	Debugger Evasion (1/45)	Exploitation for Credential Access (1/17)	Cloud Infrastructure Discovery (1/23)	Remote Service Session Hijacking (1/9)	Automated Collection (1/17)	Data Encoding (1/18)	Exfiltration Over C2 Channel (1/9)
Gather Victim Org Information (1/10)	Develop Capabilities (1/8)	Hardware Additions (1/11)	ESXi Administration Command (1/16)	Cloud Application Integration (1/23)	Boot or Logon Initialization Scripts (1/14)	Deploy Container (1/45)	Forced Authentication (1/17)	Cloud Service Dashboard (1/23)	Remote Session Hijacking (1/9)	Browser Session Hijacking (1/17)	Data Obfuscation (1/18)	Exfiltration Over Physical Medium (1/9)
Pushing for Information (1/10)	Establish Accounts (1/8)	Phishing (1/11)	Exploitation for Client Execution (1/16)	Input Injection (1/23)	Compromise Host Software Binary (1/14)	Domain or Tenant Policy Modification (1/45)	Forge Web Credentials (1/17)	Cloud Storage Object Discovery (1/23)	Application Through Removable Media (1/9)	Clipboard Data (1/17)	Dynamic Resolution (1/18)	Exfiltration Over Other Network Medium (1/9)
Search Cloud Sources (1/10)	Obtain Capabilities (1/8)	Replication Through Removable Media (1/11)	Inter-Process Communication (1/16)	Create Account (1/23)	Create or Modify System Process (1/14)	Email Spoofing (1/45)	Input Capture (1/17)	Container and Resource Discovery (1/23)	Software Deployment Tools (1/9)	Data from Cloud Storage (1/17)	Encrypted Channel (1/18)	Exfiltration Over Physical Medium (1/9)
Search Open Technical Databases (1/10)	Stage Capabilities (1/8)	Supply Chain Compromise (1/11)	Inter-Process Communication (1/16)	Create or Modify System Process (1/23)	Create or Modify System Process (1/14)	Execution Guardrails (1/45)	Modify Authentication Process (1/17)	Device Driver Discovery (1/23)	Task Shared Content (1/9)	Data from Configuration Repository (1/17)	Fallback Channels (1/18)	Exfiltration Over Physical Medium (1/9)
Search Open Websites/Domains (1/10)	Trusted Relationships (1/8)	Scheduled Task/Job (1/11)	Scheduled Task/Job (1/16)	Event Triggered Execution (1/23)	Domain or Tenant Policy Modification (1/14)	File and Directory Permissions Modification (1/45)	Multi-Factor Authentication Interception (1/17)	Domain Trust Discovery (1/23)	Use Alternate Authentication Material (1/9)	Data from Information Repositories (1/17)	Ingress Tool Transfer (1/18)	Exfiltration Over Web Service (1/9)
Search Victim-Owned Websites (1/10)	Valid Accounts (1/8)	Serverless (1/11)	Serverless (1/16)	Escape to (1/23)	Escape to (1/14)	Escape to (1/45)	Multi-Factor Authentication (1/17)	Group Policy (1/23)	Out (1/9)	Multi-Stage (1/17)	Scheduled (1/18)	Scheduled (1/9)

Legend

TG 888/3390 mapping (yellow color- 2)

APT 28 X Tg 888/3390 X Silent Crow/ Silent Librarian X layer by operation X +

Selection Controls Layer Controls Technique Controls

Reconnaissance 10 techniques Resource Development 8 techniques Initial Access 11 techniques Execution 16 techniques Persistence 23 techniques Privilege Escalation 14 techniques Defense Evasion 45 techniques Credential Access 17 techniques Discovery 23 techniques Lateral Movement 9 techniques Collection 17 techniques Command and Control 18 techniques Exfiltration 9 techniques

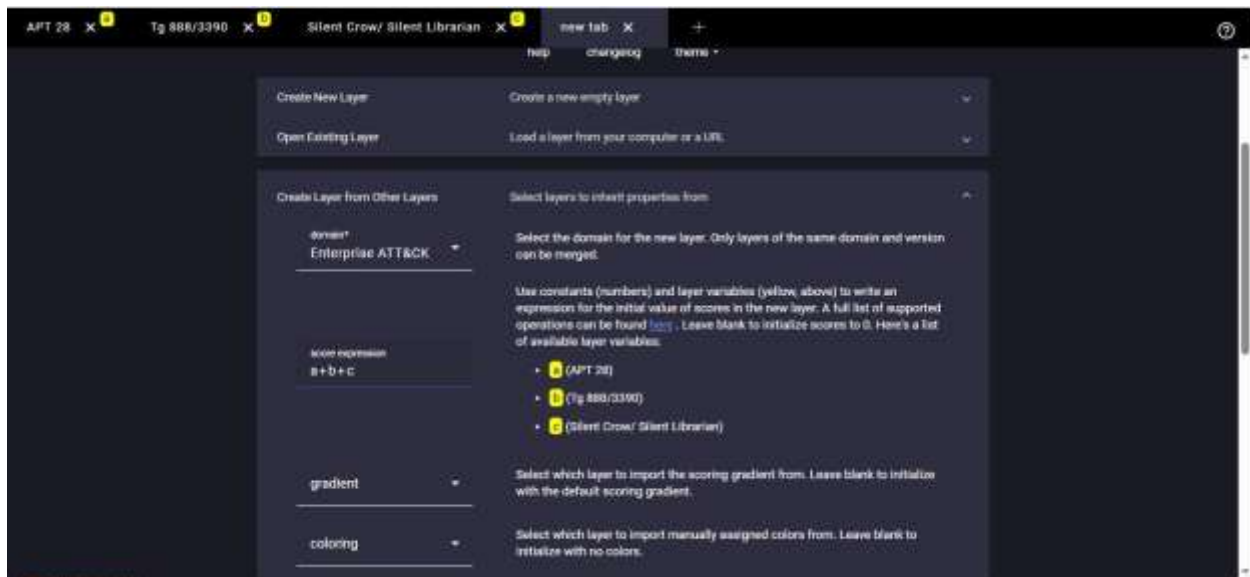
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
Active Scanning (1/10)	Acquire Access (1/8)	Context Injection (1/11)	Cloud Administration Command (1/16)	Account Manipulation (1/23)	Abuse Elevation Control Mechanism (1/14)	Abuse Elevation Control Mechanism (1/45)	Adversary in the Middle (1/17)	Account Discovery (1/23)	Exploitation of Remote Services (1/9)	Adversary in the Middle (1/17)	Application Layer Protocol (1/18)	Automated Exfiltration (1/9)
Gather Victim Host Information (1/10)	Acquire Infrastructure (1/8)	Drive-by Compromise (1/11)	Command and Scripting Interpreter (1/16)	BITS Jobs (1/23)	Access Token Manipulation (1/14)	Access Token Manipulation (1/45)	Brute Force (1/17)	Application Window Discovery (1/23)	Internal Spearphishing (1/9)	Archive Collected Data (1/17)	Communication Through Removable Media (1/18)	Data Transfer Out Links (1/9)
Gather Victim Identity Information (1/10)	Compromise Accounts (1/8)	Exploit Public-Facing Application (1/11)	Container Administration Command (1/16)	Boot or Logon Autostart Execution (1/23)	Account Manipulation (1/14)	Build Image on Host (1/45)	Credentials from Password Stores (1/17)	Browser Information Discovery (1/23)	Lateral Tool Transfer (1/9)	Audio Capture (1/17)	Content Injection (1/18)	Exfiltration Over Alternative Protocol (1/9)
Gather Victim Network Information (1/10)	Compromise Infrastructure (1/8)	External Remote Services (1/11)	Deploy Container (1/16)	Boot or Logon Initialization Scripts (1/23)	Root or Logon Initialization Scripts (1/14)	Debugger Evasion (1/45)	Exploitation for Credential Access (1/17)	Cloud Infrastructure Discovery (1/23)	Remote Service Session Hijacking (1/9)	Automated Collection (1/17)	Data Encoding (1/18)	Exfiltration Over C2 Channel (1/9)
Gather Victim Org Information (1/10)	Develop Capabilities (1/8)	Hardware Additions (1/11)	ESXi Administration Command (1/16)	Cloud Application Integration (1/23)	Boot or Logon Initialization Scripts (1/14)	Deploy Container (1/45)	Forced Authentication (1/17)	Cloud Service Dashboard (1/23)	Remote Session Hijacking (1/9)	Browser Session Hijacking (1/17)	Data Obfuscation (1/18)	Exfiltration Over Other Network Medium (1/9)
Pushing for Information (1/10)	Establish Accounts (1/8)	Phishing (1/11)	Exploitation for Client Execution (1/16)	Input Injection (1/23)	Compromise Host Software Binary (1/14)	Domain or Tenant Policy Modification (1/45)	Forge Web Credentials (1/17)	Cloud Storage Object Discovery (1/23)	Application Through Removable Media (1/9)	Clipboard Data (1/17)	Dynamic Resolution (1/18)	Exfiltration Over Other Network Medium (1/9)
Search Cloud Sources (1/10)	Obtain Capabilities (1/8)	Replication Through Removable Media (1/11)	Inter-Process Communication (1/16)	Create Account (1/23)	Create or Modify System Process (1/14)	Email Spoofing (1/45)	Input Capture (1/17)	Container and Resource Discovery (1/23)	Software Deployment Tools (1/9)	Data from Cloud Storage (1/17)	Encrypted Channel (1/18)	Exfiltration Over Physical Medium (1/9)
Search Open Technical Databases (1/10)	Stage Capabilities (1/8)	Supply Chain Compromise (1/11)	Inter-Process Communication (1/16)	Create or Modify System Process (1/23)	Create or Modify System Process (1/14)	Execution Guardrails (1/45)	Modify Authentication Process (1/17)	Device Driver Discovery (1/23)	Task Shared Content (1/9)	Data from Configuration Repository (1/17)	Fallback Channels (1/18)	Exfiltration Over Physical Medium (1/9)
Search Open Websites/Domains (1/10)	Trusted Relationships (1/8)	Scheduled Task/Job (1/11)	Scheduled Task/Job (1/16)	Event Triggered Execution (1/23)	Domain or Tenant Policy Modification (1/14)	File and Directory Permissions Modification (1/45)	Multi-Factor Authentication Interception (1/17)	Domain Trust Discovery (1/23)	Use Alternate Authentication Material (1/9)	Data from Information Repositories (1/17)	Ingress Tool Transfer (1/18)	Exfiltration Over Web Service (1/9)
Search Victim-Owned Websites (1/10)	Valid Accounts (1/8)	Serverless (1/11)	Serverless (1/16)	Escape to (1/23)	Escape to (1/14)	Escape to (1/45)	Multi-Factor Authentication (1/17)	Group Policy (1/23)	Out (1/9)	Multi-Stage (1/17)	Scheduled (1/18)	Scheduled (1/9)

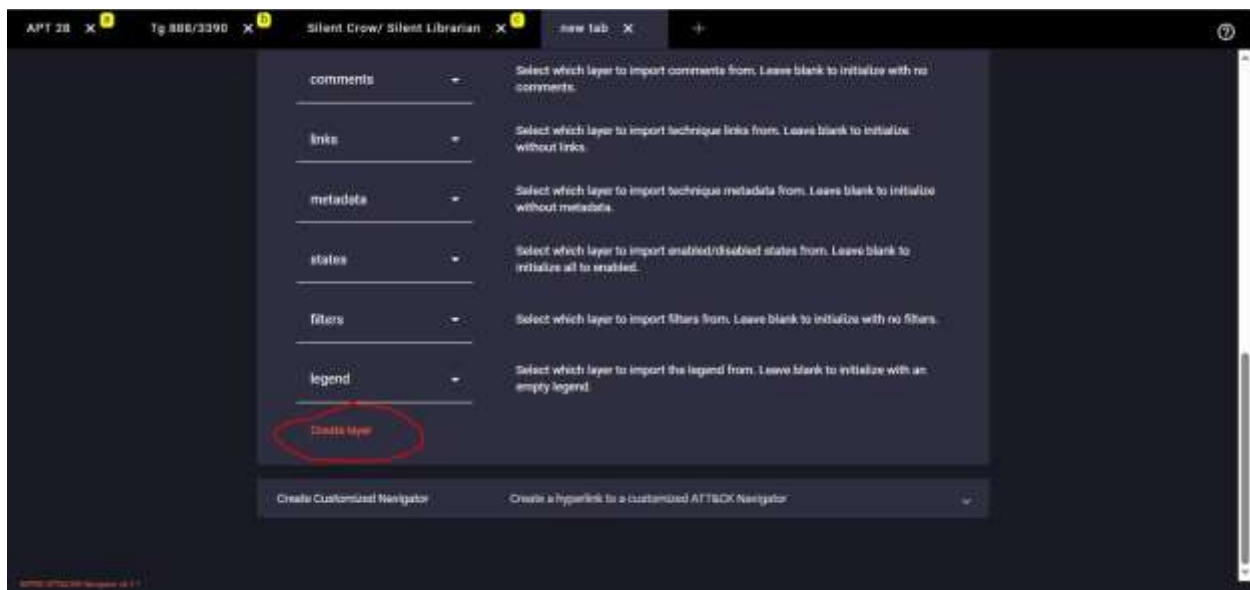
Silent crow/ Silent Librarian mapping (Green color- 3)



4. Overlap the TTps of the APTs

Here we compare the TTps of the APTs by creating a new tab, selecting newer version of 'Enterprise ATT&CK' adding the score expression and clicking on creating layer.





Overlapping of APT28, Silent Crow, TG 888.



5. Benefits of Threat Hunting

- **Early Detection:** Uncovers threats before they cause significant damage.
- **Improved Resilience:** Strengthens security posture by closing gaps.
- **Reduced Attack Dwell Time:** Minimizes the time attackers remain undetected.
- **Enhanced Incident Response:** Provides context and insights that improve response efficiency.
- **Continuous Improvement:** Builds organizational knowledge and refines detection rules.

6. Conclusion

Threat hunting is an essential component of modern cybersecurity. By proactively searching for hidden adversaries, organizations can identify advanced threats that bypass traditional defenses, minimize risk exposure, and strengthen their resilience against cyberattacks. Successful threat hunting requires skilled analysts, robust tools, and a well-structured process that integrates intelligence, detection, and response.

As cyber threats continue to evolve, organizations that adopt and mature their threat hunting capabilities will be better positioned to defend against sophisticated adversaries and maintain trust in their digital infrastructure.