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.

---

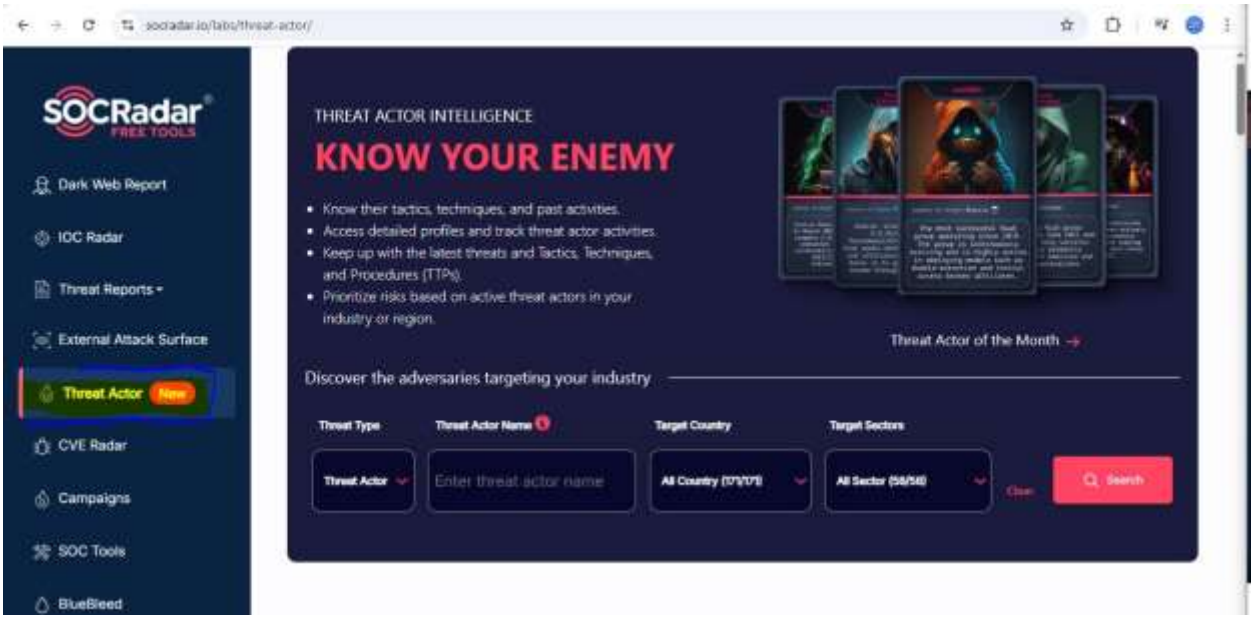
3. Threat Hunting Process

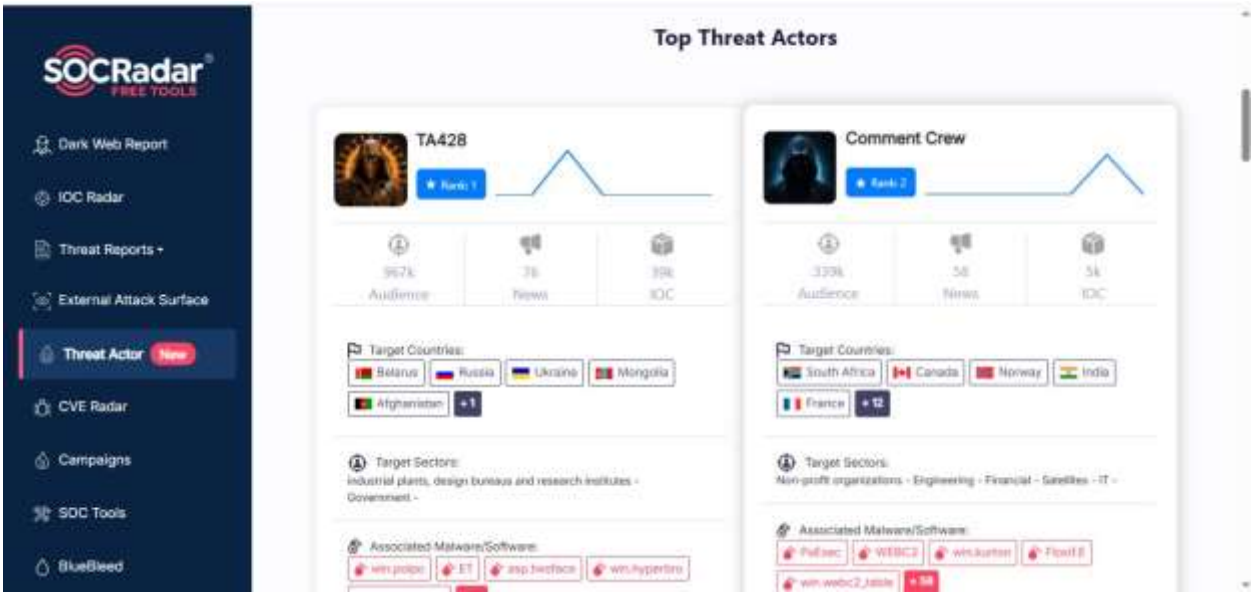
Threat hunting generally follows a structured approach, often based on three key phases:

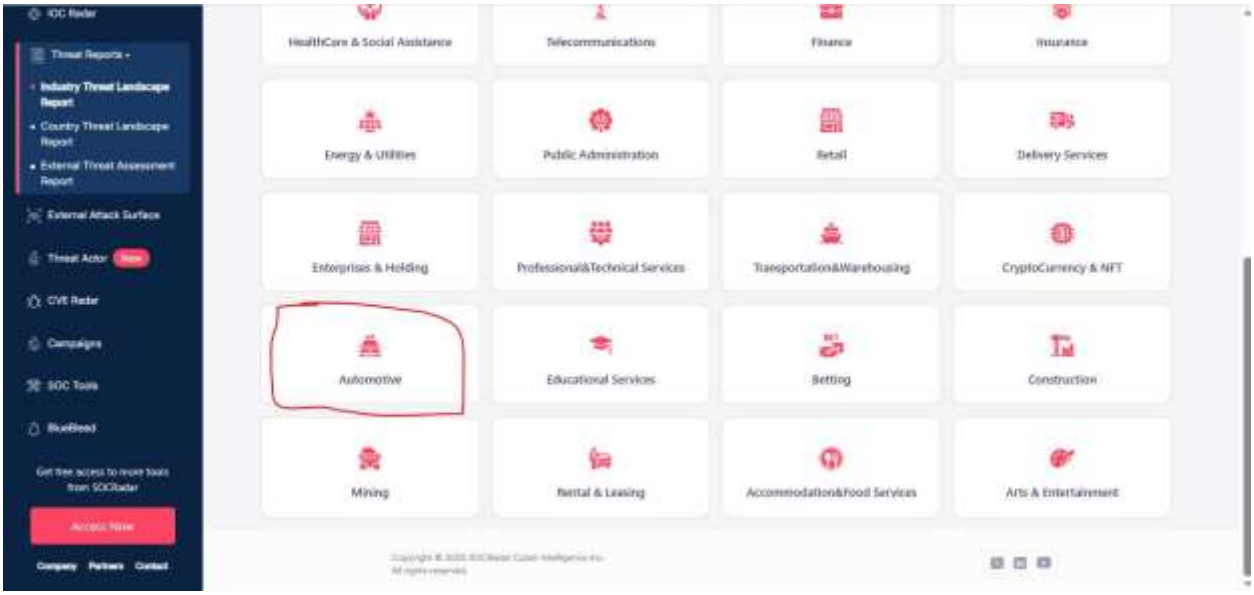
a. Gathering of Intel

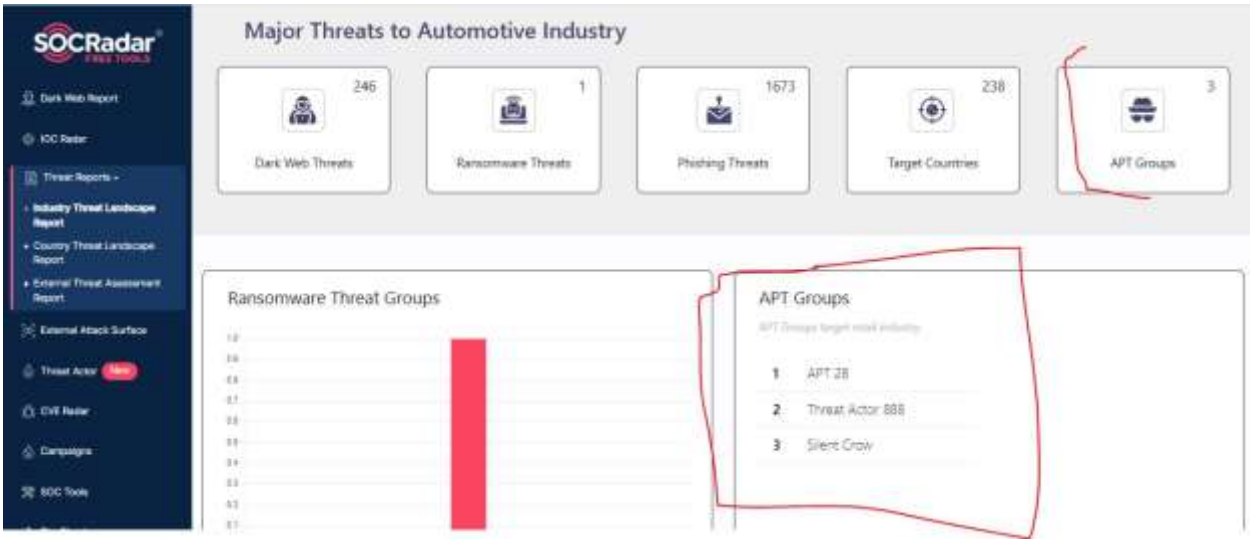
This is the first stage of Threat hunting, in this stage, '**Socradar.io'** is used. Here we want to know what APTs are peculiar to each organisations/country. In the homepage of socradar.io, we will navigate by clicking on 'Free Tools', then 'Threat Actors'(here we will see different threat actors associated 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.


socradar.io
Blog
Trainings
Start Free Trial
Login
SOCRadar
Products
Solutions
Plans & Pricing
Resources
Free Tools
Company
Get a Personalized Demo
Get Your Free Report
Your Early Warning System Against Hackers.
Get real-time visibility into vulnerabilities, leaked data, and threat actor activity targeting your organization.
Start Free Trial
Advanced Dark Web Monitoring
Cyber Threat Intelligence
Attack Surface Management
Brand Protection
Supply Chain Intelligence


socradar.io/labs/threat-actor/
SOCRadar
FREE TOOLS
Dark Web Report
IOC Radar
Threat Reports
External Attack Surface
Threat Actor
New
CVE Radar
Campaigns
SOC Tools
BlueBleed
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 Name
Target Country
Target Sectors
Threat Actor
Enter threat actor name
Clear
Search

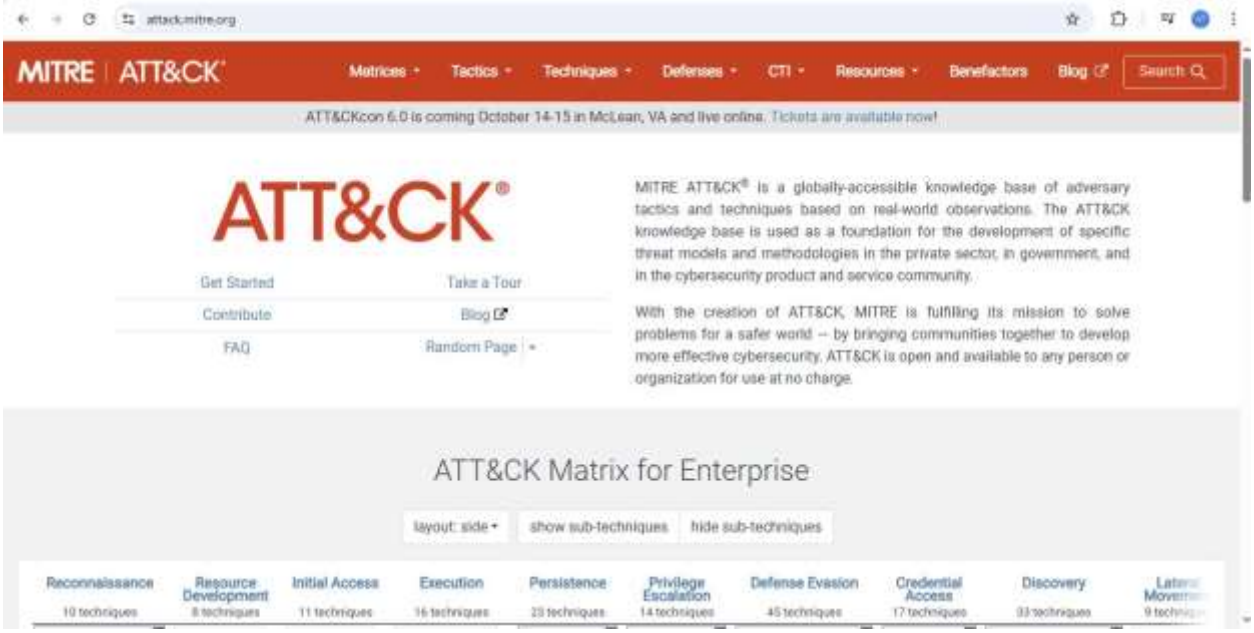

SOCRadar
FREE TOOLS
Dark Web Report
IOC Radar
Threat Reports
External Attack Surface
Threat Actor New
CVE Radar
Campaigns
SOC Tools
BlueBleed
Top Threat Actors
TA428
Rank 1
967k
Audience
News
IOC
Target Countries:
Belarus
Russia
Ukraine
Mongolia
Afghanistan
+1
Target Sectors:
Industrial plants, design bureaus and research institutes - Government -
Associated Malware/Software:
Comment Crew
Rank 2
339k
Audience
58
News
5k
IOC
Target Countries:
South Africa
Canada
Norway
India
France
+12
Target Sectors:
Non-profit organizations - Engineering - Financial - Satellites - IT -
Associated Malware/Software:
PsExec
WEBC2
Flash8
+58

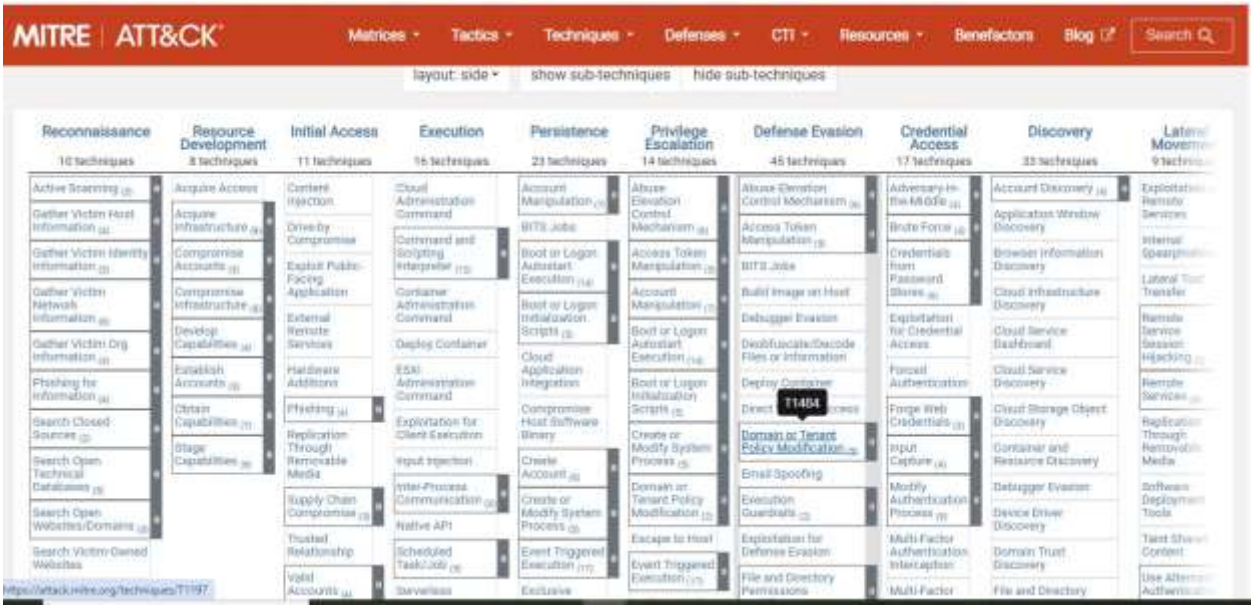

IOC Radar
Threat Reports
Industry Threat Landscape Report
Country Threat Landscape Report
External Threat Assessment Report
External Attack Surface
Threat Actor New
CVE Radar
Campaigns
SOC Tools
BlueBleed
Get free access to more tools from SOCRadar
Access Now
Company
Partners
Contact
HealthCare & Social Assistance
Telecommunications
Finance
Insurance
Energy & Utilities
Public Administration
Retail
Delivery Services
Enterprises & Holding
Professional&Technical Services
Transportation&Warehousing
CryptoCurrency & NFT
Automotive
Educational Services
Betting
Construction
Mining
Rental & Leasing
Accommodation&Food Services
Arts & Entertainment

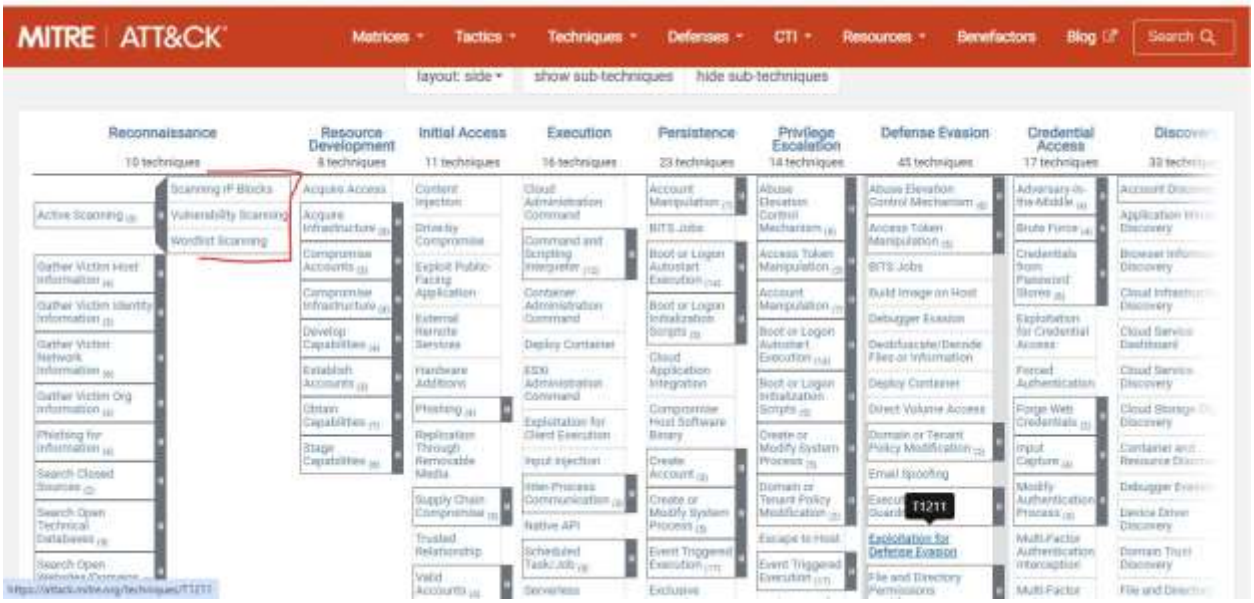


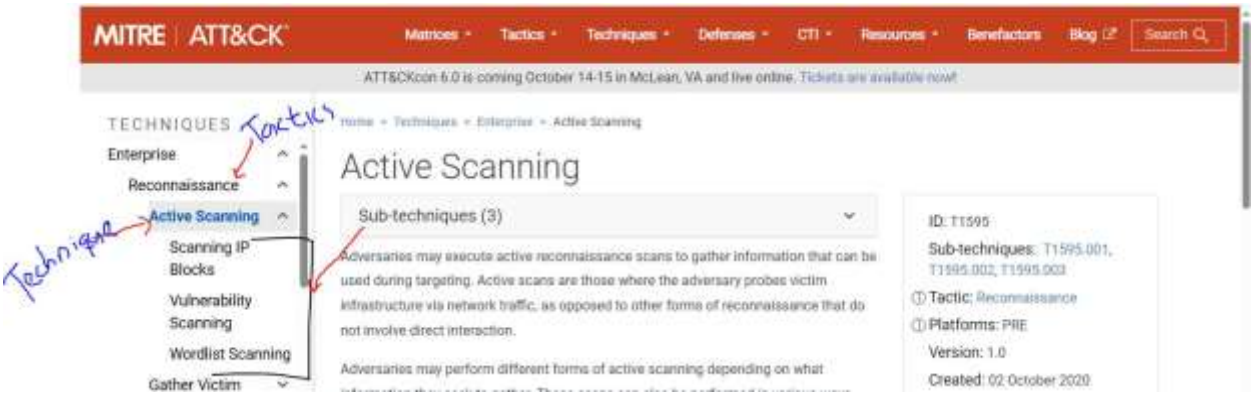
b. Understand their TTPs (Tactics, Techniques, Procedures)

In this stage, we go on ‘attack.mitre.org’ to understand what TTPs are and whatthey stand for.



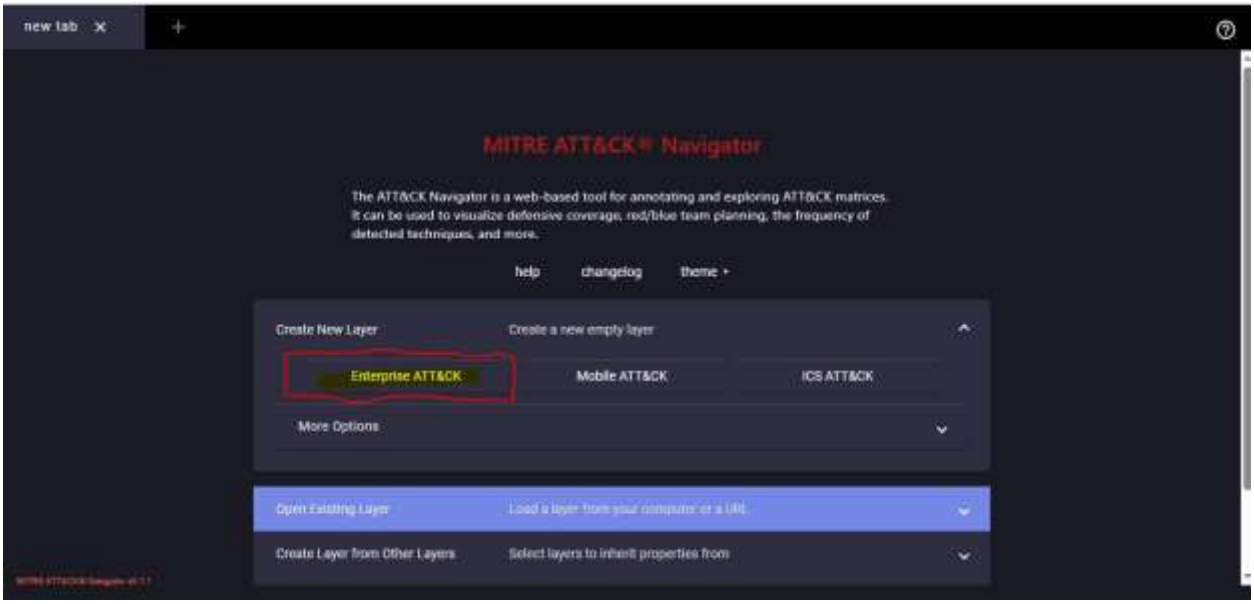

MITRE | ATT&CK
Matrices
Tactics
Techniques
Defenses
CTI
Resources
Benefactors
Blog
Search
layout: side
show sub-techniques
hide sub-techniques
Reconnaissance
10 techniques
Resource Development
8 techniques
Initial Access
11 techniques
Execution
16 techniques
Persistence
23 techniques
Privilege Escalation
14 techniques
Defense Evasion
45 techniques
Credential Access
17 techniques
Discovery
33 techniques
T1484
Domain or Tenant Policy Modification

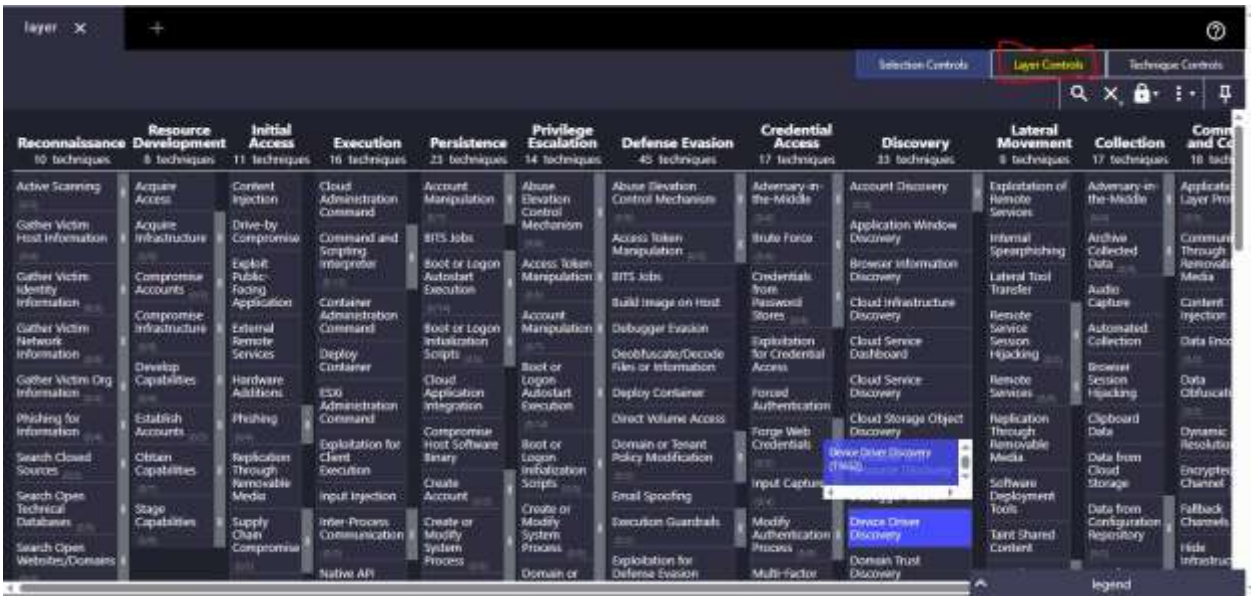

MITRE | ATT&CK
Matrices
Tactics
Techniques
Defenses
CTI
Resources
Benefactors
Blog
Search
layout: side
show sub-techniques
hide sub-techniques
Reconnaissance
10 techniques
Resource Development
8 techniques
Initial Access
11 techniques
Execution
16 techniques
Persistence
23 techniques
Privilege Escalation
14 techniques
Defense Evasion
45 techniques
Credential Access
17 techniques
Scanning IP Blocks
Vulnerability Scanning
Wordlist Scanning
Active Scanning
T1211
Exploitation for Defense Evasion


MITRE | ATT&CK
Matrices
Tactics
Techniques
Defenses
CTI
Resources
Benefactors
Blog
Search
ATT&CKcon 6.0 is coming October 14-15 in McLean, VA and live online. Tickets are available now!
TECHNIQUES
Tactics
Home > Techniques > Enterprise > Active Scanning
Enterprise
Reconnaissance
Active Scanning
Technique
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.


new tab
MITRE ATT&CK® Navigator
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.
help
changelog
theme
Create New Layer
Create a new empty layer
Enterprise ATT&CK
Mobile ATT&CK
ICS ATT&CK
More Options
Open Existing Layer
Load a layer from your computer or a URL
Create Layer from Other Layers
Select layers to inherit properties from


layer
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
33 techniques
Lateral Movement
9 techniques
Collection
17 techniques
legend

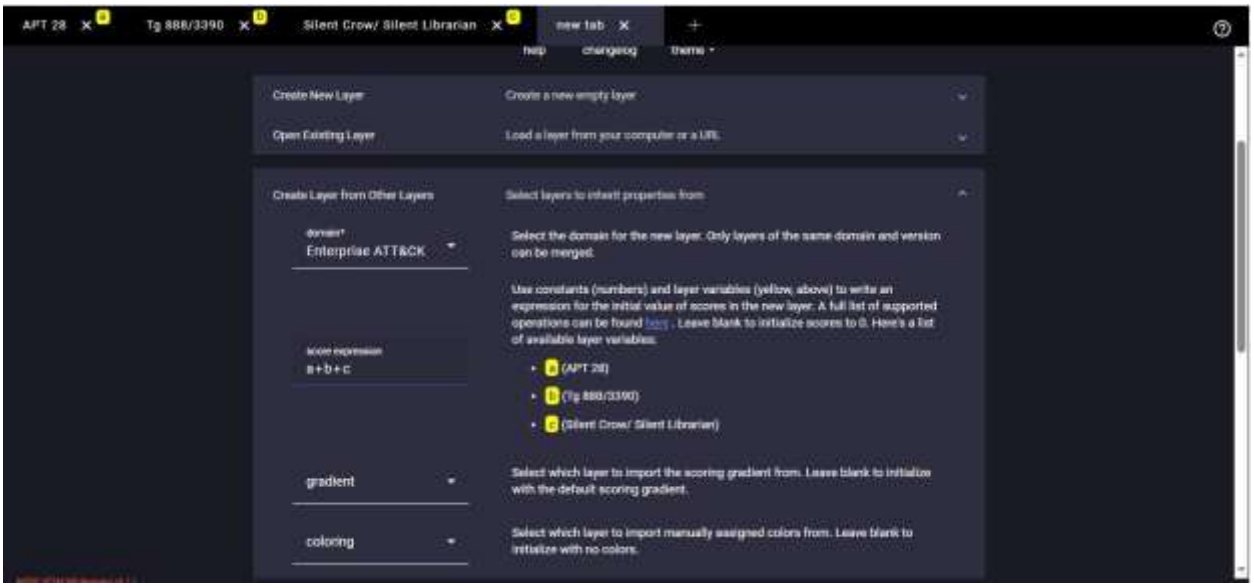
APT 28 mapping (wine color- 1)

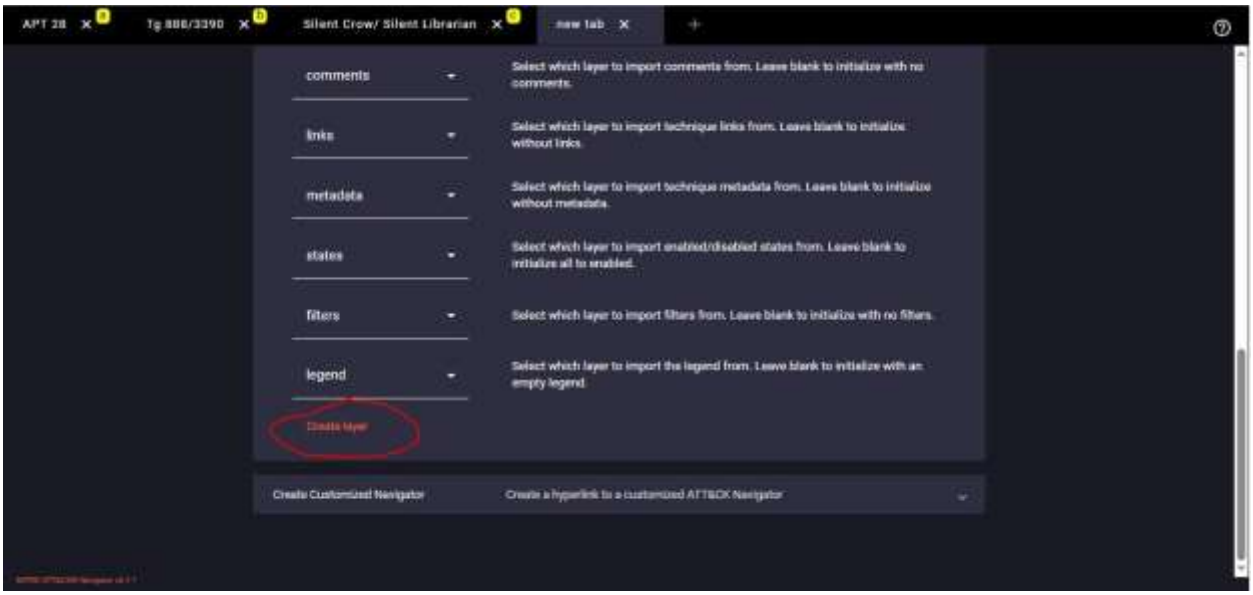
TG 888/3390 mapping (yellow color- 2)

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.