

Threat Hunting and Intelligence Project

Project Title:

Sector-Specific Threat Intelligence and Hunting Using MITRE ATT&CK and SOC Radar

Author: Oghenetega T. Gold

Role: Cybersecurity Analyst

Date: October 2025

Objective:

The objective of this project is to perform sector-based and region-aware threat hunting leveraging Threat Intelligence and MITRE ATT&CK framework, with the goal of identifying and analyzing adversary behaviors, techniques, and mitigations relevant to the Information Services Sector.

1. Background

Threats are increasingly **sector- and region-specific**, making targeted threat intelligence vital for proactive cyber defense. The **Information Services Sector**—which includes organizations handling data storage, processing, and distribution—is often a prime target for cyber espionage, data theft, and sabotage operations by Advanced Persistent Threat (APT) groups.

To ensure structured, compliant, and resilient threat management, this project aligns with established cybersecurity frameworks:

- **NIST Cybersecurity Framework (CSF)**, particularly the **Detect (DE)** and **Respond (RS)** functions, which focus on building detection capabilities, analyzing anomalous activities, and executing coordinated incident response actions.
- **ISO/IEC 27001:2022**, specifically controls **A.8.16–A.8.17** (Event Monitoring and Detection) and **A.5.29–A.5.31** (Incident Response). These guide the development of monitoring processes, timely detection, and effective response procedures.

By aligning the technical threat-hunting process with these frameworks, the project strengthens both the **security operations layer** (through detection engineering and adversary analysis) and the **governance layer** (through framework-driven controls and response readiness).

For this project, Socradar.io (Free Version) was used as the primary **Threat Intelligence source** to identify relevant APT groups affecting this sector. Due to limitations of the free version, the analysis focuses on **industry-specific** threats without filtering by region. Attached below, is an image that shows what socradar looks like.

The screenshot shows the Socradar interface for generating an industry threat landscape report. On the left sidebar, there are links for Dark Web Report, IOC Radar, Threat Reports (with sub-options for Industry Threat Landscape Report, Country Threat Landscape Report, and External Threat Assessment Report), External Attack Surface, Threat Actor (marked as New), CVE Radar, Campaigns, and SOC Tools. The main content area is titled "Industry Threat Landscape Report Result" and includes fields for Industry (Information Services), Report Date (2025-11-13), and Time Period (2025-11-13 - 2024-11-13). It features a large red "Download Free Report" button with a PDF icon. Below this, a section titled "Major Threats to Information Services Industry" displays five categories with corresponding icons and counts: Dark Web Threats (3093), Ransomware Threats (3), Phishing Threats (39577), Target Countries (239), and APT Groups (22).

2. Identified APT Groups

From SOC Radar's threat intelligence for the Information Services sector, 22 APT groups were identified.

22 apt groups found in Information Services

Group Name	Aliases	Country
Ducktail	Ducktail Infostealer Vietnamese Ducktail Group	India , UK ...
Hensi	H3nsi , HensiPanel HensiCrypter	Global
Volatile Cedar	DeftTorero , Lebanese Cedar , Volatile Cedar Dancing Salome ...	Lebanon , USA ...
Earth Lamia	Earth Lamia	China , Philippines ...
Mr Hamza	MrHamza	Belgium , India ...
BRONZE SPRING	UNC302	China , Netherlands ...
InvisiMole	InvisiMole UAC-0035	Philippines , Poland ...
rose87168	-	Pakistan , Australia ...

For the sake of this project, **two** representative APT groups were selected based on their documented global activity and relevance:

i. InvisiMole (UAC-0035)

- **Targeted Regions:** Poland and the Philippines
- **Aliases:** InvisiMole, UAC-0035
- **Primary Motivation:** Cyber espionage
- **Target Types:** Government and information sectors
- **Notable Characteristics:** Modular malware, stealthy persistence, and strong lateral movement techniques.

MITRE | ATT&CK

ATT&CK v18 has been released! Check out the blog post or changelog for more information.

SOFTWARE

- InvisibleFerret
- InvisiMole**
- Invoke-PSImage
- ipconfig
- IPsec Helper
- IronNetInjector
- ISMinjector
- Ixeshe
- J-magic
- Janicab
- Javali
- JCry
- JHUHUGIT
- JPIN
- jRAT
- JSS Loader
- Judy
- JumbledPath
- Kapeka
- KARAE
- Kasidet
- Kazuar
- ..

InvisiMole

InvisiMole is a modular spyware program that has been used by the InvisiMole Group since at least 2013. InvisiMole has two backdoor modules called RC2FM and RC2CL that are used to perform post-exploitation activities. It has been discovered on compromised victims in the Ukraine and Russia. Gamaredon Group infrastructure has been used to download and execute InvisiMole against a small number of victims.^{[1][2]}

Techniques Used

Domain	ID	Name	Use
Enterprise	T1548	.002 Abuse Elevation Control Mechanism: Bypass User Account Control	InvisiMole can use fileless UAC bypass and create an elevated COM object to escalate privileges. ^{[1][2]}
Enterprise	T1087	.001 Account Discovery: Local Account	InvisiMole has a command to list account information on the victim's machine. ^[1]
Enterprise	T1071	.001 Application Layer Protocol: Web Protocols	InvisiMole uses HTTP for C2 communications. ^[1]
		.004 Application Layer Protocol: DNS	InvisiMole has used a custom implementation of DNS tunneling to embed C2 communications in DNS requests and replies. ^[2]
Enterprise	T1010	Application Window Discovery	InvisiMole can enumerate windows and child windows on a compromised host. ^{[1][2]}
Enterprise	T1560	.001 Archive Collected Data: Archive via Utility	InvisiMole uses WinRAR to compress data that is intended to be exfiltrated. ^[1]
		.002 Archive Collected Data: Archive via Library	InvisiMole can use zlib to compress and decompress data. ^{[1][2]}

ATT&CK® Navigator Layers •

ii. Volatile Cedar (a.k.a. DeftTorero, Lebanese Cedar, Dancing Salome)

- **Targeted Regions:** Middle East and the United States
- **Primary Motivation:** Espionage and surveillance
- **Target Types:** Telecommunications, IT service providers, and critical infrastructure
- **Notable Characteristics:** Long-term infiltration, webshells, and command-and-control obfuscation.

The screenshot shows the MITRE ATT&CK Navigator interface. On the left, there's a sidebar with a tree view of threat groups, where 'Volatile Cedar' is selected. The main content area shows the details for 'Volatile Cedar'. At the top, it says 'Volatile Cedar is a Lebanese threat group that has targeted individuals, companies, and institutions worldwide. Volatile Cedar has been operating since 2012 and is motivated by political and ideological interests.' Below this is a box with ID: G0123, Associated Groups: Lebanese Cedar, Version: 1.1, Created: 08 February 2021, and Last Modified: 16 April 2025. There are links for 'Version' and 'Permalink'. Under 'Associated Group Descriptions', there's a table with one row for 'Lebanese Cedar'. Under 'Techniques Used', there's a table listing various techniques with their domains, IDs, names, and descriptions.

3. Methodology

3.1 Tools and Frameworks Used

- **SOC Radar (Free Version)** (socradar.io) – for sector threat intelligence collection
- **MITRE ATT&CK Framework** (attack.mitre.org) – for mapping adversary tactics and techniques
- **MITRE ATT&CK Navigator** (<https://mitre-attack.github.io/attack-navigator/>) – for visualization and overlap analysis of APT behaviors

3.2 Approach

1. Query APT profiles (Volatile Cedar & InvisiMole) on attack.mitre.org.
2. Extract techniques mapped to **MITRE ATT&CK for Enterprise** (14 tactic categories).
3. Upload both APT technique sets into **ATT&CK Navigator**.

4. Overlay the two APT profiles to identify:
 - o Common techniques (Purple overlap)
 - o Unique techniques per group
5. Identify mitigations and defensive recommendations for overlapping and critical unique techniques.

4. MITRE ATT&CK Mapping

4.1 Tactics in Scope

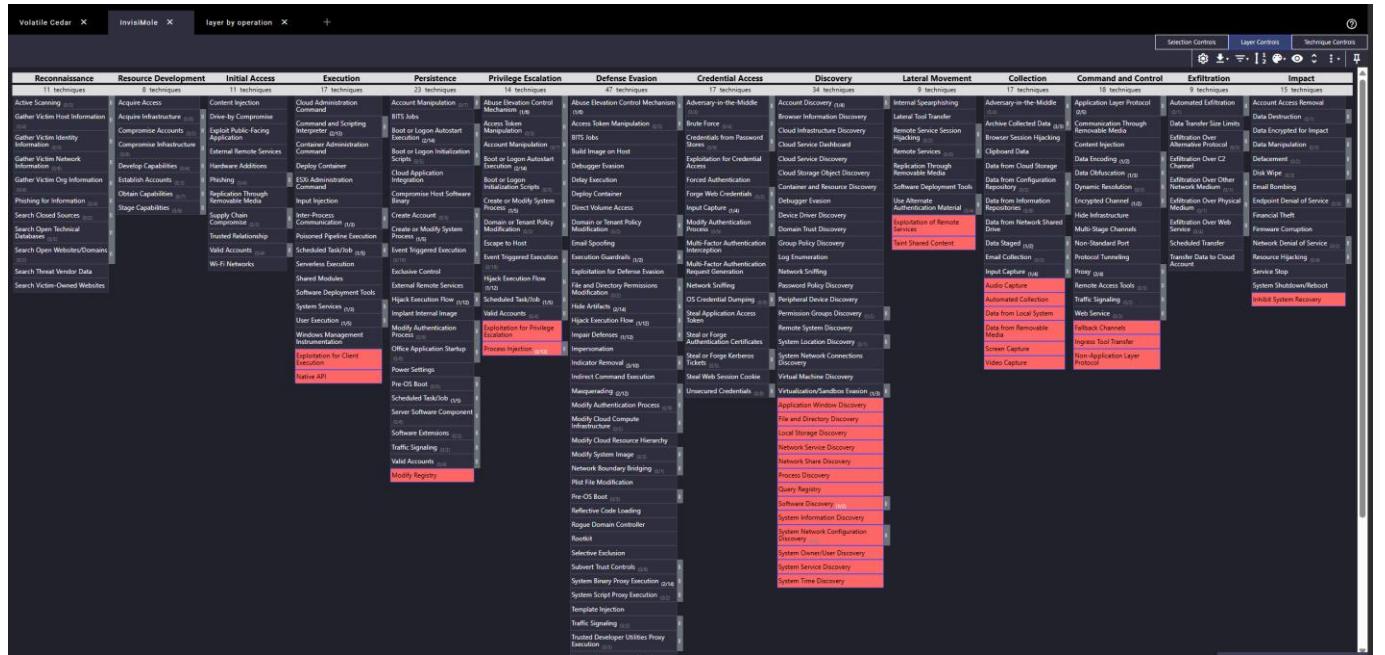
The analysis covered all **14 ATT&CK Tactics**:

- | | |
|-------------------------|-------------------------|
| 1. Reconnaissance | 8. Credential Access |
| 2. Resource Development | 9. Discovery |
| 3. Initial Access | 10. Lateral Movement |
| 4. Execution | 11. Collection |
| 5. Persistence | 12. Command and Control |
| 6. Privilege Escalation | 13. Exfiltration |
| 7. Defense Evasion | 14. Impact |

5. Results and Analysis

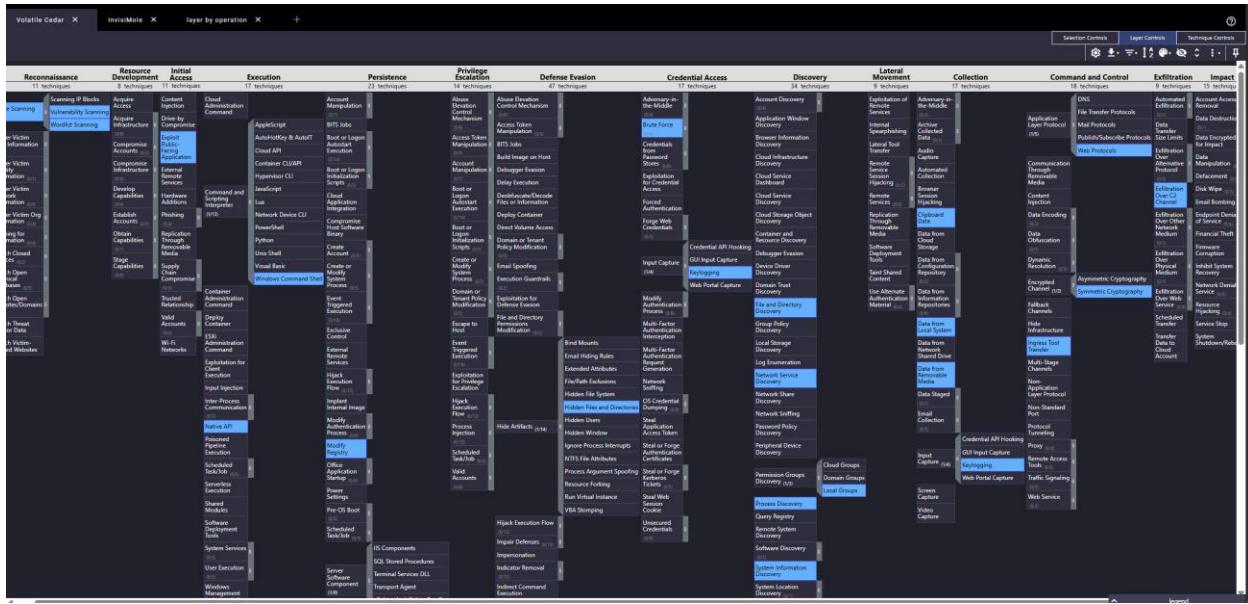
5.1 Individual APT Profiles

InvisiMole (Red Layer)



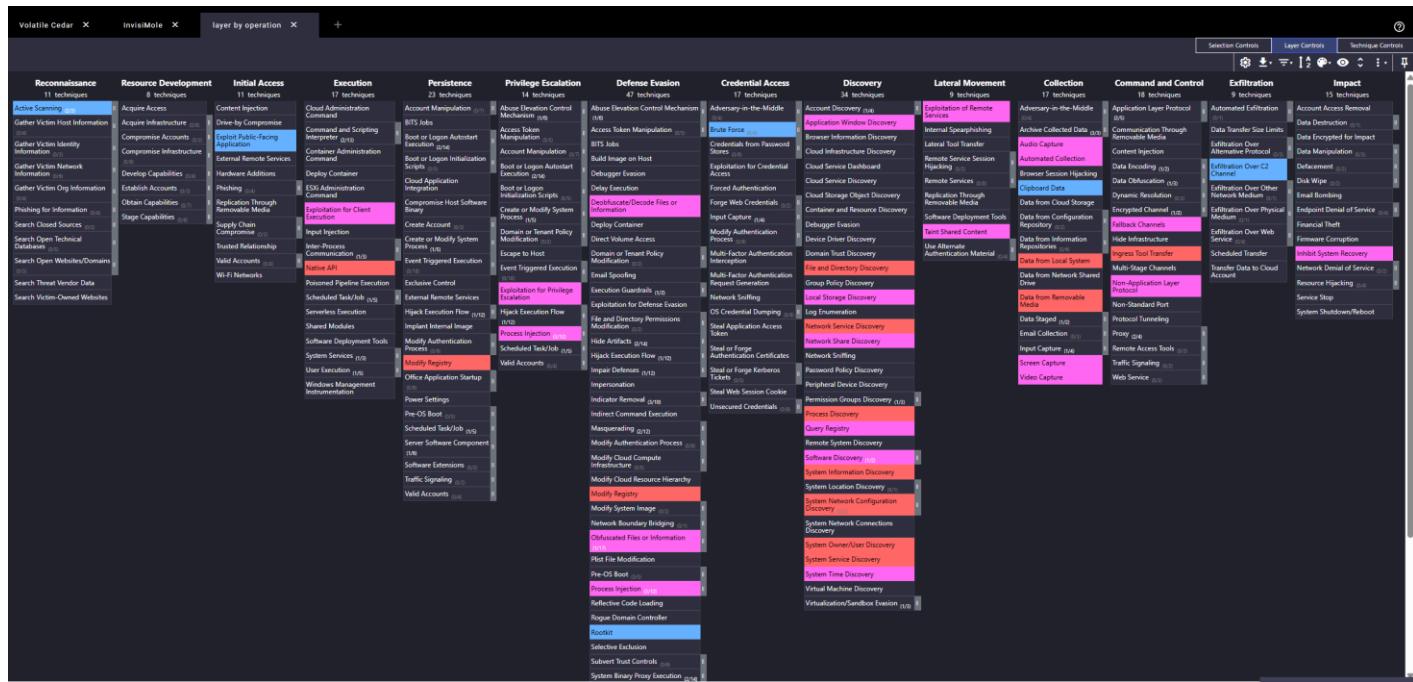
- Strong emphasis on **Execution, Persistence, and Defense Evasion.**
- Techniques include:
 - **Native API, Exploitation for Client Execution, Modify Registry, and Process Injection.**
 - **Automated Collection, Video Capture, and Data from Removable Media** under *Collection.*
 - **Fallback Channels, Ingress Tool Transfer, and Non-Application Layer Protocol** under *C2.*
- High use of **Discovery** techniques: *System Information Discovery, File and Directory Discovery, Process Discovery*.

Volatile Cedar (Blue Layer)



- Heavy use of **Execution** and **Command & Control** stages.
- Techniques include:
 - **Windows Command Shell**, **PowerShell**, and **Network Device CLI**.
 - **Hidden Files and Directories**, **Rootkit**, and **Credential Dumping** under *Defense Evasion*.
 - **Keylogging**, **Web Portal Capture**, and **GUI Input Capture** for *Credential Access*.
 - **Symmetric Cryptography** and **Encrypted Channel** for *Exfiltration*.
- Emphasis on **Persistence** through **Create or Modify System Process** and **Boot/Logon Initialization Scripts**.

5.2 Overlap Analysis (Purple Layer)



The overlap layer highlights techniques common to both APT groups. These represent shared tradecraft that defenders in the Information Services sector should prioritize detecting and mitigating.

Common Techniques Identified

ATT&CK Tactic	Common Techniques	Potential Defensive Focus
Execution	Native API, PowerShell	Endpoint execution monitoring, API abuse detection
Persistence	Modify Registry, Scheduled Task/Job	Registry integrity monitoring, Scheduled task auditing

Privilege Escalation	Process Injection	Memory and behavioral analysis for process injection
Defense Evasion	Modify System Image, Obfuscated Files or Information	File integrity monitoring, obfuscation pattern detection
Discovery	File and Directory Discovery, System Information Discovery, Process Discovery	Endpoint visibility, asset inventory correlation
Collection	Automated Collection, Clipboard Data	Data exfiltration behavior analysis
Command & Control	Non-Application Layer Protocol, Ingress Tool Transfer	Network segmentation, traffic anomaly detection
Impact	Inhibit System Recovery	System backup monitoring, ransomware resilience planning

6. Mitigation Recommendations

Based on MITRE ATT&CK's mitigation mapping, the following defensive strategies are recommended:

1. Implement Endpoint Detection and Response (EDR):

Detect behaviors such as process injection, registry modification, and unusual persistence mechanisms.

2. Adopt Strong Network Segmentation and Traffic Inspection:

Detect command-and-control traffic using non-standard or encrypted protocols.

3. Regular Patch Management and Hardening:

Limit exploitation opportunities through timely software updates.

4. Registry and Task Monitoring:

Track unauthorized registry changes and newly created scheduled tasks.

5. Behavior-Based Threat Hunting:

Hunt for cross-APT commonalities (identified purple techniques) as priority indicators of compromise (IOCs).

6. User Awareness and Access Control:

Prevent phishing-based initial access and enforce least privilege.

7. Conclusion

This project demonstrates the importance of **sector-specific threat intelligence** combined with **MITRE ATT&CK analytical tools** to understand and defend against real-world APTs.

The overlap between **InvisiMole** and **Volatile Cedar** reveals recurring techniques across different regions and campaigns, indicating adversarial convergence in TTPs.

By continuously enriching threat intelligence (via SOC Radar) and correlating with MITRE ATT&CK, defenders in the Information Services sector can:

- Improve detection coverage,
- Prioritize mitigations, and

- Enhance resilience against multi-regional APT threats.

Supporting Documents

The following supporting materials are attached to the project repository for reference and validation:

1. InvisiMole MITRE Navigator Layer – InvisiMole_navigator.png
2. Volatile Cedar MITRE Navigator Layer – Volatile_Cedar_navigator.png
3. Overlapping Techniques (Combined Layer) – overlap of a_b.png
4. Raw Intelligence Notes and Data Sources – from SOC Radar and MITRE ATT&CK
5. Excel export of overlapping techniques

These documents collectively support the findings and visual mappings described in this report.

References

- SOC Radar Threat Intelligence Portal: <https://socradar.io>
- MITRE ATT&CK Framework: <https://attack.mitre.org>
- MITRE ATT&CK Navigator: <https://mitre-attack.github.io/attack-navigator/>
- APT Profiles: InvisiMole & Volatile Cedar (MITRE Database)