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

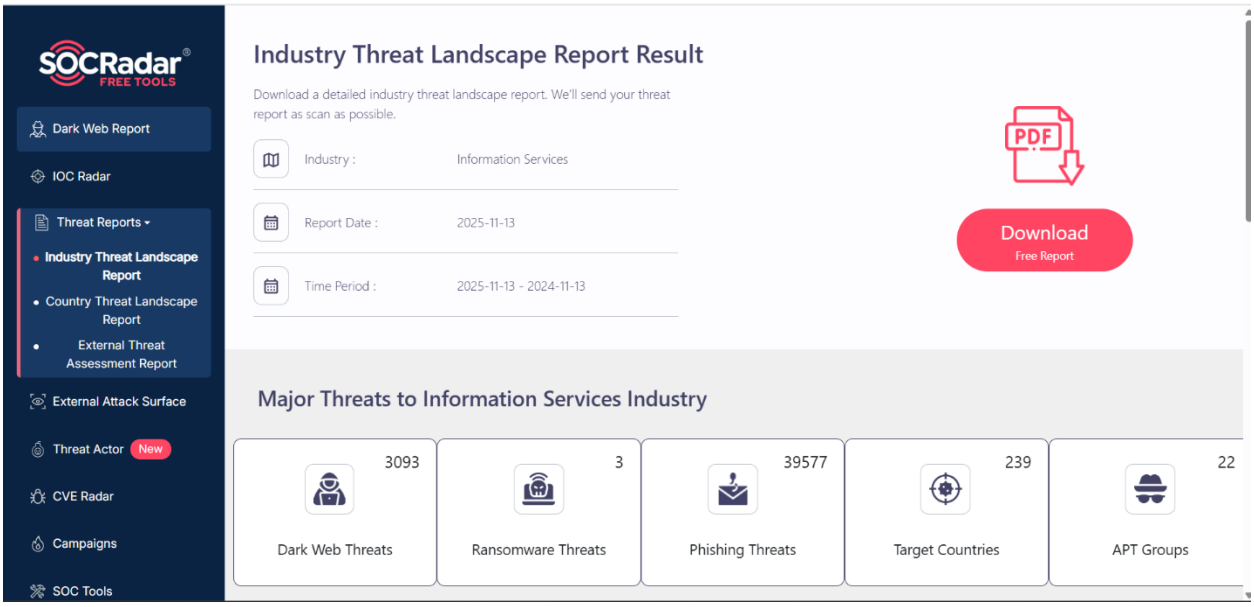
Threats are increasingly **sector- and region-specific**, making targeted threat intelligence vital for proactive cyber defense. The **Information Services Sector**—which includes organizations handling data storage, processing, and distribution—is often a prime target for cyber espionage, data theft,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



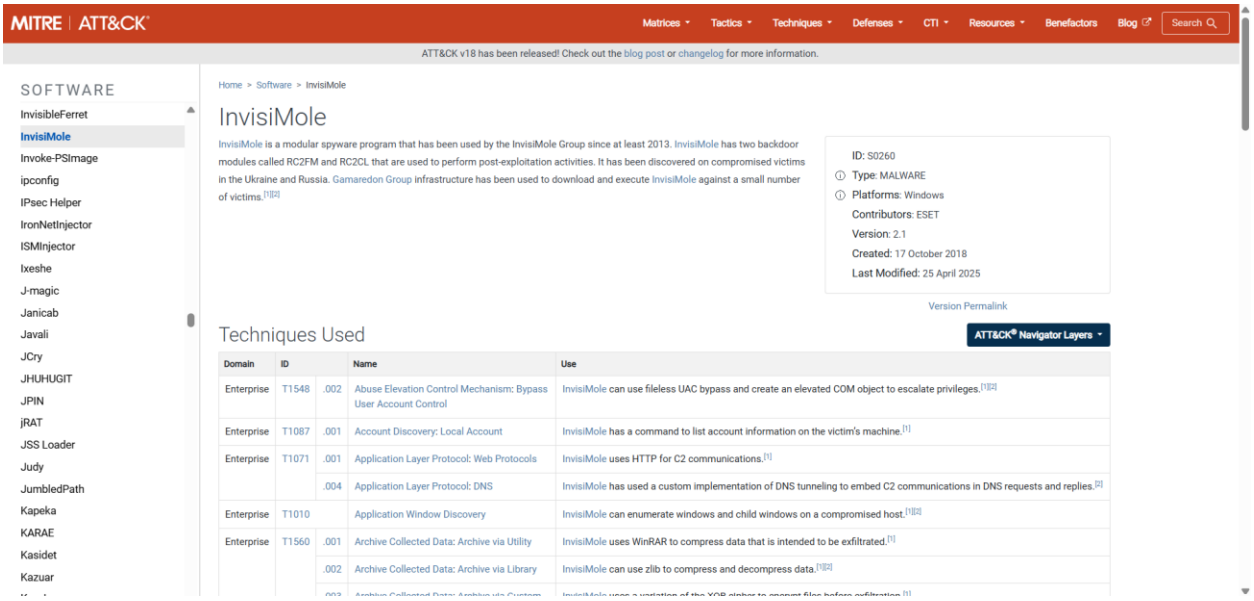
2. Identified APT Groups

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

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

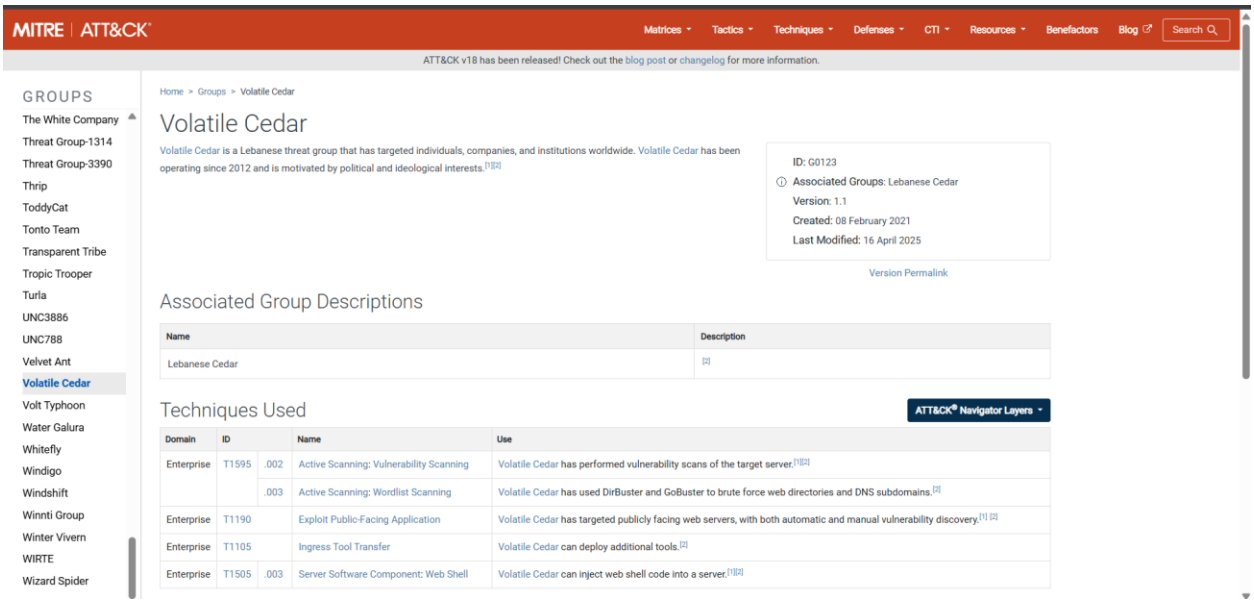
i. **InvisiMole (UAC-0035)**

- **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.



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.



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:
    - Common techniques (Purple overlap)
    - 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

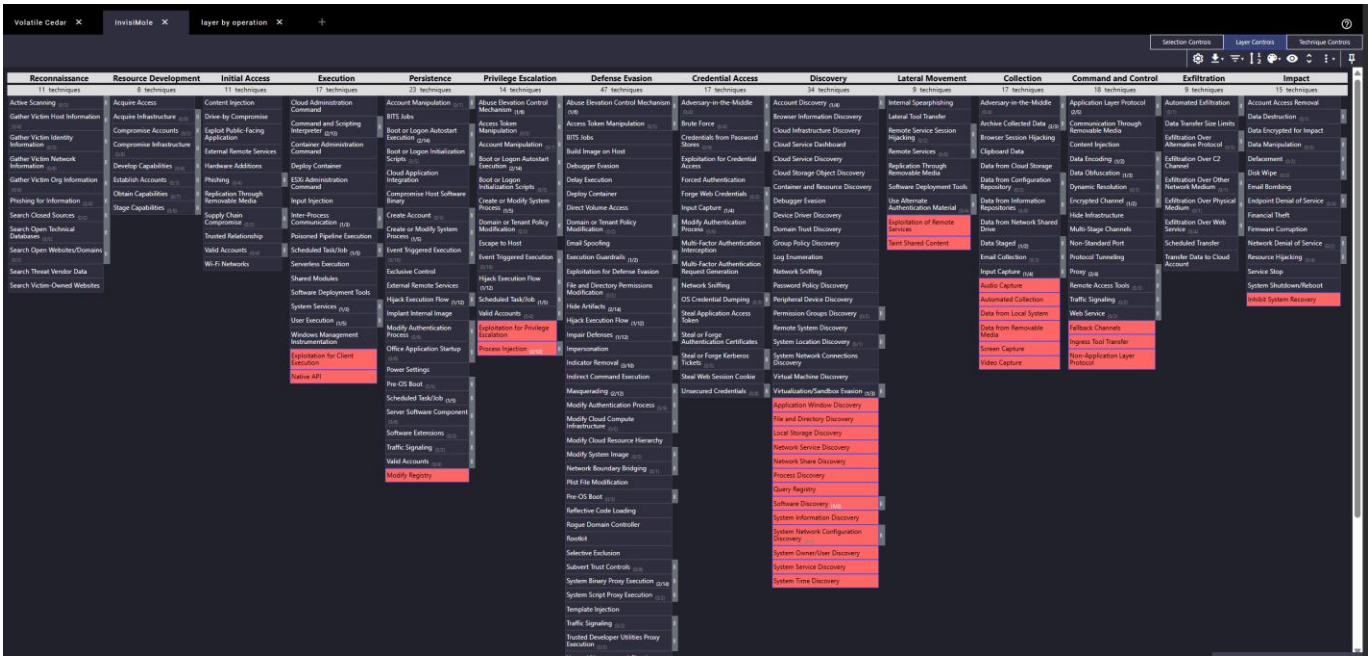
The analysis covered all **14 ATT&CK Tactics**:

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

5. Results and Analysis

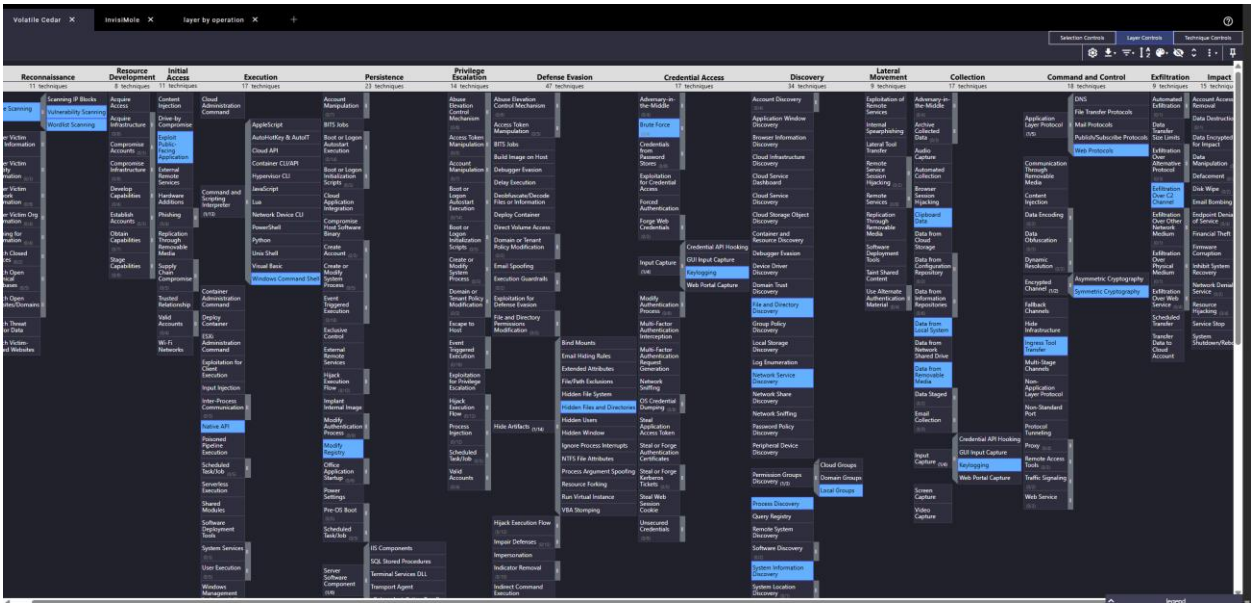
5.1 Individual APT Profiles

InvisiMole (Red Layer)



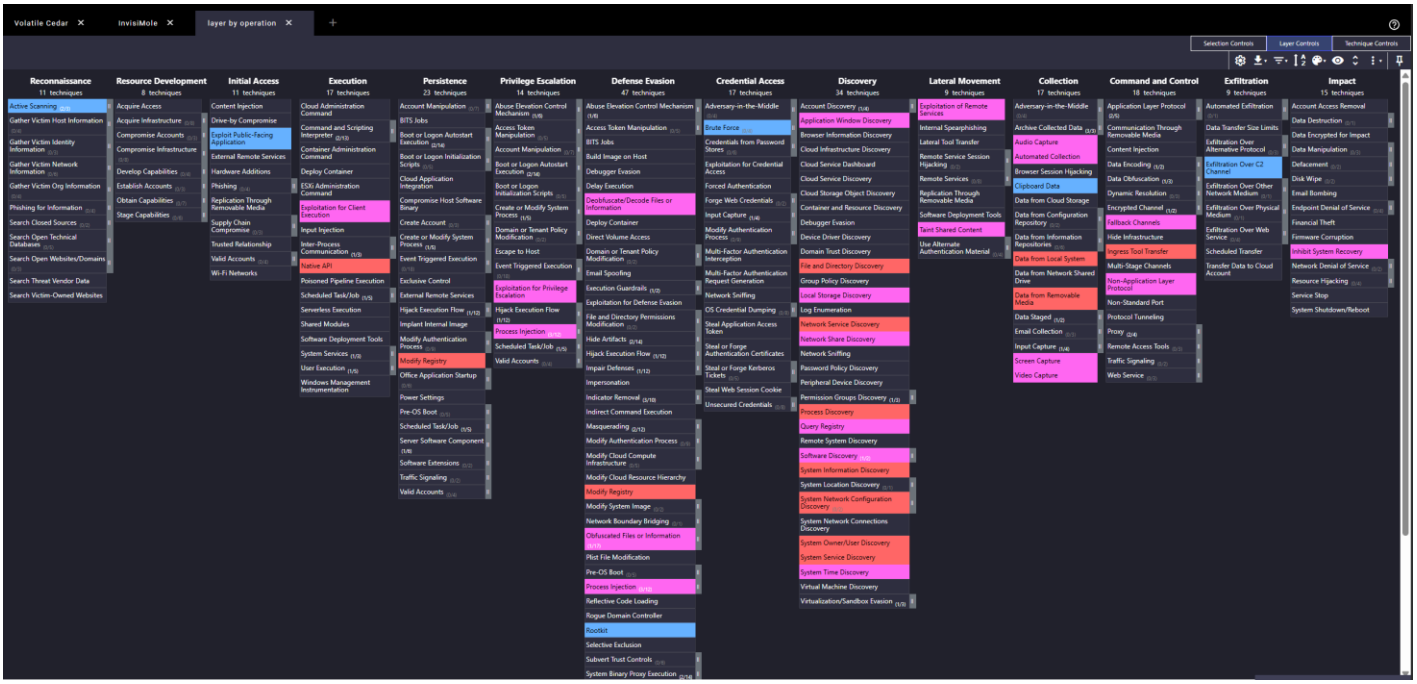
- Strong emphasis on **Execution**, **Persistence**, and **Defense Evasion**.
- Techniques include:
    - **Native API**, **Exploitation for Client Execution**, **Modify Registry**, and **Process Injection**.
    - **Automated Collection**, **Video Capture**, and **Data from Removable Media** under *Collection*.
    - **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)