

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

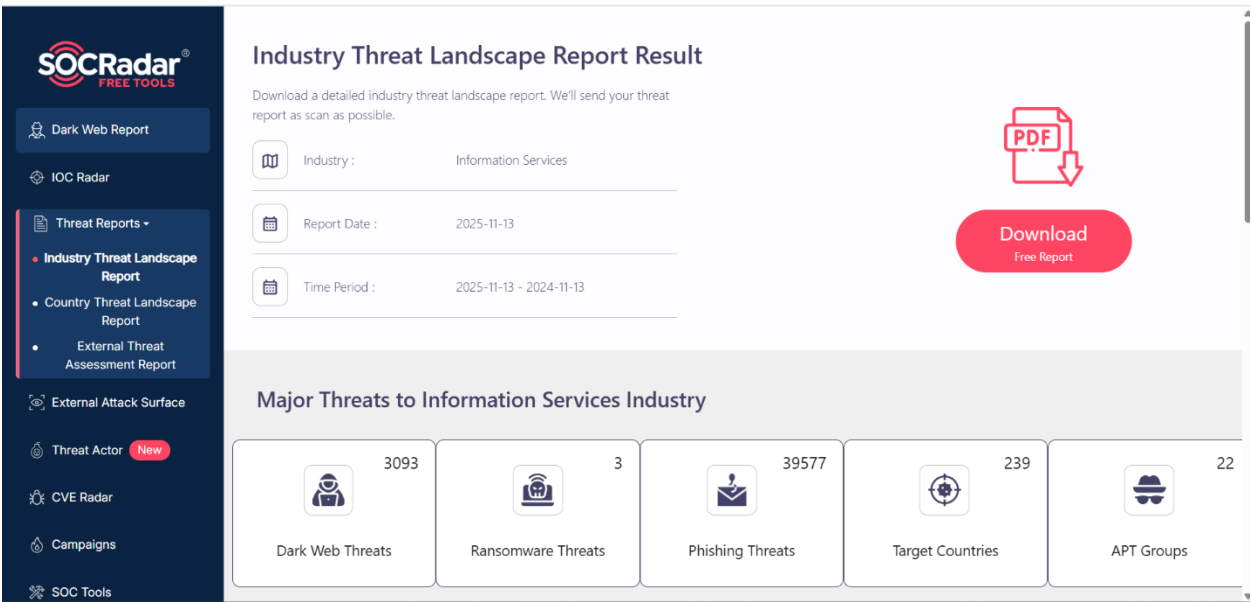
Threats are increasingly **sector- and region-specific**, making targeted threat intelligence vital for proactive cyber defense. The **Information Services Sector**—which includes organizations handling data storage, processing, and distribution—is often a prime target for cyber espionage, data theft,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

APT Groups



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

Matrices
Tactics
Techniques
Defenses
CTI
Resources
Benefactors
Blog

Search Q

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

Kazuair

Home > Software > InvisiMole

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]}

ID: S0260

① Type: MALWARE

① Platforms: Windows

Contributors: ESET

Version: 2.1

Created: 17 October 2018

Last Modified: 25 April 2025

Version Permalink

ATT&CK® Navigator Layers

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]
		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]
		Archive Collected Data: Archive via Library	InvisiMole can use zlib to compress and decompress data. ^{[1][2]}
		Archive Collected Data: Archive via Custom	InvisiMole uses a variation of the VOB stego to compress files before exfiltration. ^[1]

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.

MITRE | ATT&CK

Home > Groups > Volatile Cedar

Volatile Cedar

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.^{[1][2]}

ID: G0123
 ① Associated Groups: Lebanese Cedar
 Version: 1.1
 Created: 08 February 2021
 Last Modified: 16 April 2025

Version Permalink

Associated Group Descriptions

Name	Description
Lebanese Cedar	[2]

Techniques Used

ATT&CK Navigator Layers

Domain	ID	Name	Use
Enterprise	T1595 .002	Active Scanning: Vulnerability Scanning	Volatile Cedar has performed vulnerability scans of the target server. ^{[1][2]}
		Active Scanning: Wordlist Scanning	Volatile Cedar has used DirBuster and GoBuster to brute force web directories and DNS subdomains. ^[2]
Enterprise	T1190	Exploit Public-Facing Application	Volatile Cedar has targeted publicly facing web servers, with both automatic and manual vulnerability discovery. ^{[1] [2]}
Enterprise	T1105	Ingress Tool Transfer	Volatile Cedar can deploy additional tools. ^[2]
Enterprise	T1505 .003	Server Software Component: Web Shell	Volatile Cedar can inject web shell code into a server. ^{[1][2]}

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 | 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)

Volatile Cedar														InvisiMale	layer by operation	+															Selection Controls	Layer Controls	Technique Controls																																																																																																																																																																																														
Reconnaissance														Resource Development														Initial Access														Execution														Persistence														Privilege Escalation														Defense Evasion														Credential Access														Discovery														Lateral Movement														Collection														Command and Control														Exfiltration														Impact																																									
11 techniques														8 techniques														11 techniques														17 techniques														23 techniques														14 techniques														47 techniques														17 techniques														34 techniques														8 techniques														17 techniques														14 techniques														9 techniques														17 techniques														14 techniques														12 techniques													
Active Scanning														Acquire Access														Content Injection														Cloud Administration Command														Account Manipulation														Abuse Elevation Control Mechanism														Adversary-in-the-Middle														Account Discovery														Internal Spearphishing														Adversary-in-the-Middle														Application Layer Protocol														Automated Exfiltration														Account Access Removal																																																							
Gather Victim Host Information														Acquire Infrastructure														Drive-by Compromise														Command and Scripting Interpreter														BITS Jobs														Access Token Manipulation														Backdoor														Browser Information Discovery														Lateral Tool Transfer														Archive Collected Data														Communication Through Removable Media														Data Destruction																																																																					
Gather Victim Identity Information														Compromise Accounts														Exploit Public-Facing Application														Container Administration Command														Boot or Logon Autostart Execution														BITS Jobs														Credentials from Password Store														Cloud Service Dashboard														Remote Service Session Hijacking														Browser Session Hijacking														Content Injection														Exfiltration Over Alternative Protocol														Data Manipulation																																																							
Gather Victim Network Information														Compromise Infrastructure														External Remote Services														Deploy Container														Boot or Logon Initialization Scripts														Build Image on Host														Cloud Service Discovery														Remote Services														Clipboard Data														Data Encoding														Exfiltration Over C2 Channel														Deauthentication																																																																					
Develop Capabilities														Hardware Additions														Phishing														EDR Administration Command														Delay Execution														Forge Web Credentials														Cloud Storage Object Discovery														Replication Through Removable Media														Data from Cloud Storage														Data Exfiltration														Exfiltration Over Other Network Medium														Denial of Service																																																																					
Establish Accounts														Obtain Capabilities														Stage Capabilities														Input Injection														Create or Modify System Process														Direct Volume Access														Debugger Evasion														Software Deployment Tools														Data from Configuration Repository														Dynamic Resolution														Email Bombing																																																																																			
Phishing for Information														Supply Chain Compromise														Inter-Process Communication														Domain or Tenant Policy Modification														Domain Trust Discovery														Device Driver Discovery														Data from Information Respositories														Encrypted Channel														Exfiltration Over Physical Medium														Endgame																																																																																																	
Search Cloud Sources														Trusted Relationship														Scheduled Task/Job														Event Triggered Execution														Email Spoofing														Multi-Factor Authentication Interception														Group Policy Discovery														Exploitation of Remote Services														Data from Network Shared Drive														Multi-Stage Channels														Exfiltration Over Web Service														Forward Corruption																																																																					
Search Open Technical Databases														Wi-Fi Networks														Shared Modules														Exclusive Control														Hijack Execution Flow														Exploitation for Defense Evasion														Network Sniffing														Data Staged														Non-Standard Port														Network Denial of Service														Resource Hijacking																																																																																			
Search Open Websites/Domains														Serverside Execution														External Remote Services														Hijack Execution Flow														File and Directory Permissions Modification														Password Policy Discovery														Email Collection														Protocol Tunneling														Transfer Data to Cloud Account														Service Stop																																																																																																	
Search Threat Vendor Data														System Services														Implant Internal Image														Scheduled Task/Job														OS Configuration Dumping														Peripheral Device Discovery														Input Capture														Proxy														Service Step														System Shutdown/Reboot																																																																																																	
Search Victim-Owned Websites														User Execution														Windows Management Instrumentation														Valid Accounts														Steal Application Access Token														Permissions Groups Discovery														Automated Collection														Traffic Signaling														Wield System Recovery																																																																																																															
														Exploitation for Client Injection														Office Application Startup														Process Injection														Steal or Forge Remote Authentication Certificates														Remote System Discovery														Data from Local System														Web Service																																																																																																																													
														Native API														Power Settings														Host File Modification														Unsecured Credentials														System Network Connections Discovery														Screen Capture														Ingress Tool Transfer																																																																																																																													

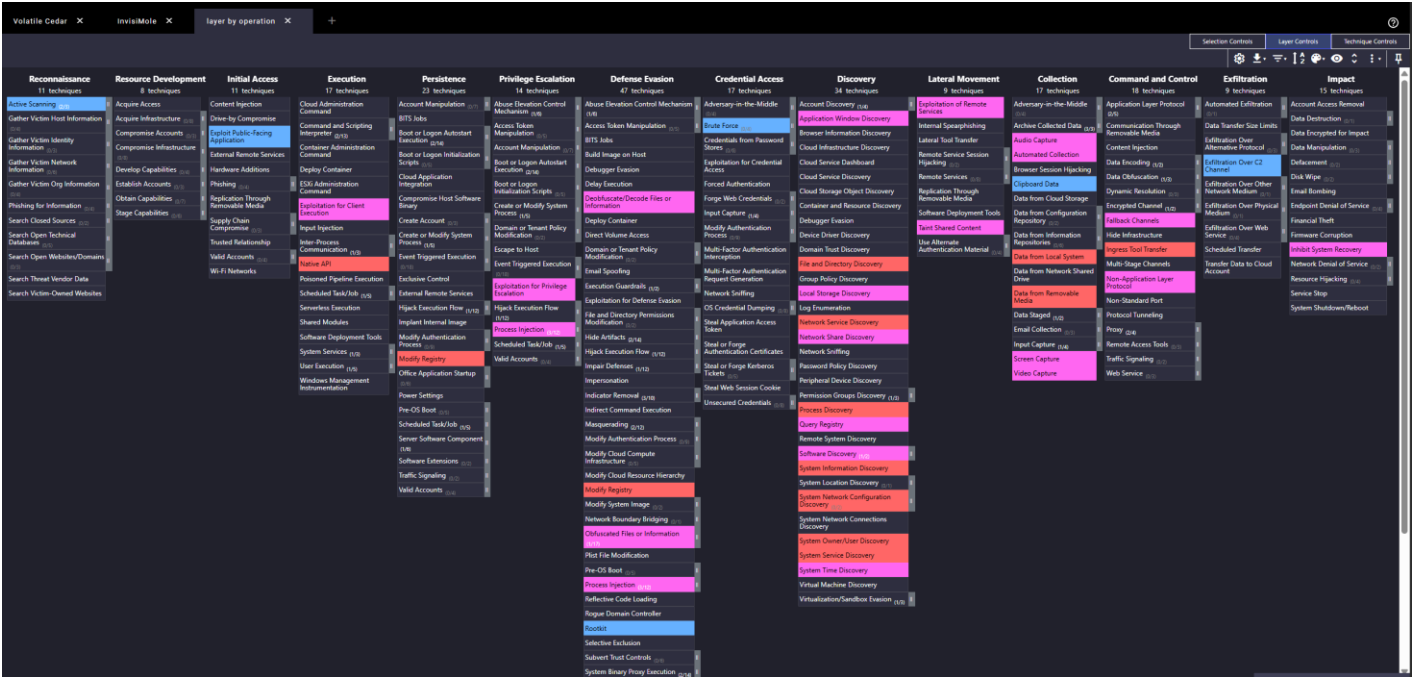
- Strong emphasis on **Execution, Persistence, and Defense Evasion**.
- Techniques include:
 - **Native API, Exploitation for Client Execution, Modify Registry, and Process Injection.**
 - **Automated Collection, Video Capture, and Data from Removable Media** under *Collection*.
 - **Fallback Channels,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

[illegible]

- 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	Common Techniques	Potential Defensive Focus
Tactic		
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)