Unveiling Void Manticore: Structured Collaboration Between Espionage and Destruction in MOIS

By gmcdouga

Published: 2024-05-20 · Archived: 2026-04-05 23:48:59 UTC

Check Point Research (CPR) has been actively monitoring the activities of Void Manticore, an Iranian threat actor affiliated with the Ministry of Intelligence and Security (MOIS). This threat actor has garnered attention for its involvement in destructive wiping attacks, often coupled with influence operations. Notably, Void Manticore has adopted various online personas to carry out its operations, with the most prominent ones being "Homeland Justice" for attacks in Albania and "Karma" for operations targeting Israel.

Key Highlights:

- *Void Manticore, linked to the Iranian Ministry of Intelligence and Security (MOIS), executes destructive wiping attacks alongside influence operations.*
- *Operating under various online personas, notably Homeland Justice for Albania and Karma for Israel, Void Manticore targets different regions with tailored attacks.*
- *Overlaps exist between Void Manticore and Scarred Manticore targets, suggesting coordinated efforts and a systematic handoff of victims in MOIS.*
- *Utilizing five distinct methods, including custom wipers for Windows and Linux, Void Manticore disrupts operations through file deletion and shared drive manipulation.*

Void Manticore's Collaborative Cyber Offensive

In recent years, the landscape of cyber security threats has evolved dramatically, with state-sponsored actors increasingly utilizing sophisticated tactics to target organizations and nations. Among these actors, Void Manticore has emerged as a significant threat to anyone who opposes to Iranian interests. With a reputation for conducting destructive wiping attacks coupled with sophisticated influence operations, Void Manticore's operations are characterized by their dual approach, combining psychological warfare with actual data destruction.

In this report, CPR has shed light on the intricate tactics employed by this threat actor, uncovering a complex web of online personas, strategic collaborations, and sophisticated attack methodologies. In this blog, we delve into the intricate details of Void Manticore's operations, dissecting its modus operandi and shedding light on the evolving landscape of state-sponsored cyber threats.

Understanding Void Manticore

Void Manticore is an Iranian threat actor affiliated with the Ministry of Intelligence and Security (MOIS). Their modus operandi involves carrying out destructive wiping attacks combined with influence operations. Operating under various online personas, such as "Karma" for attacks in Israel and "Homeland Justice" for attacks in Albania, Void Manticore has demonstrated a capacity for coordinated and targeted cyber assaults.

Collaboration with Scarred Manticore

A significant aspect of Void Manticore's operations is their collaboration with another Iranian MOIS affiliated threat group, Scarred Manticore. Analysis reveals a systematic handoff of targets between the two groups, indicating a coordinated effort to conduct destructive activities against selected victims. The handoff process involves Scarred Manticore initially accessing and exfiltrating data from targeted networks, followed by a transition of control to Void Manticore, which then executes the destructive phase of the operation. This strategic partnership not only amplifies the scale and impact of their attacks but also poses a formidable challenge for cybersecurity defenders.

By leveraging the resources and expertise of multiple threat actors, Void Manticore and its collaborators can execute sophisticated cyber campaigns with far-reaching consequences. This collaboration not only extends the reach of Void Manticore, but also suggests a level of sophistication beyond their individual capabilities.

Figure 1 – A high-level timeline of the Void-Scarred Manticores Connection.

This handoff procedure is not unprecedented and is highly correlated with Microsoft's reporting on the destructive attacks against Albania in 2022.

A comparison of the process that happened in Albania and in Israel is summarized in the table below:

	Albania (2022)	**Israel** (2023-2024)
Actor #1	**Storm-0861 ~ Scarred Manticore**	
Actor #1 Initial Access	CVE-2019-0604	CVE-2019-0604
Actor #1 Tools	Foxshell	Liontail
Actor #1 Access Time	Over a year	Over a year
Actor #1 Objective	Email Exfiltration	Email Exfiltration (LionHead)
Actor #2	**Storm-0842 ~ Void Manticore**	
Actor #2 Initial Access	Provided by Actor #1	Provided by Actor #1

	Albania (2022)	**Israel** (2023-2024)
Actor #1 Objective	Wiper (CL Wiper) + Ransomware	Wiper (BiBi Wiper)
Leaking Persona	Homeland Justice	Karma

The overlaps in techniques employed in attacks against Israel and Albania, including the coordination between the two different actors, suggest this process has become routine.

The ties between the events in Israel and Albania have strengthened with the latest attacks against Albania (late 2023 and early 2024), during which Void Manticore dropped partition wipers similar to those used in Israel as part of the BiBi wiper attacks.

Techniques, Tactics, and Procedures

Void Manticore's tactics are relatively straightforward yet effective. They often utilize basic, publicly available tools to establish access to target networks. Once inside, they deploy custom wipers for both Windows and Linux systems, targeting critical files and partition tables to render data inaccessible. Additionally, the group engages in manual data destruction activities, further amplifying the impact of their attacks.

The Wipers

Void Manticore employs a range of custom wipers to execute its destructive operations effectively. These wipers serve varying purposes, with some targeting specific files or file types within infected systems, enabling selective erasure of critical information and causing targeted damage to applications, user data, and system functionality. Others focus on attacking the system's partition table, obliterating it to render all data on the disk inaccessible, despite remaining unaltered on the storage medium.

Notably, the group utilizes the CI Wiper, which was first deployed in an attack against Albania in July 2022, alongside Partition Wipers like the LowEraser, used in attacks against entities such as INSTAT in Albania and multiple Israeli entities.

Their most recent attacks saw the deployment of the BiBi Wiper, named after Israel's Prime Minister Benjamin Netanyahu, which exists in both Linux and Windows variants, employing sophisticated techniques to corrupt files and disrupt system functionality.

Conclusion

Void Manticore's ability to conduct coordinated, destructive attacks highlights the growing sophistication of state-sponsored cyber operations. As organizations and nations continue to grapple with cyber threats, understanding and mitigating the risks posed by groups like Void Manticore are paramount to safeguarding digital infrastructure and national security.

In the ever-evolving landscape of cybersecurity, staying vigilant and proactive is key to defending against emerging threats. As Void Manticore and other threat actors continue to adapt and evolve, ongoing collaboration

between cybersecurity researchers, government agencies, and private sector organizations will be essential in countering the challenges posed by state-sponsored cyber aggression.
