Iranian APT MuddyWater Uses Dindoor Malware to Target U.S. Networks

By Ameer Owda

Published: 2026-03-09 · Archived: 2026-04-29 02:05:19 UTC

Mar 09, 2026

6 Mins Read

A recently uncovered cyber espionage campaign attributed to the **Iranian** state-linked threat group **MuddyWater** has drawn attention from security researchers after several organizations in the United States were compromised using newly observed malware. The attacks reportedly targeted sectors including aviation, financial services, and software development, highlighting how geopolitical tensions can extend into cyberspace.

Researchers discovered that the attackers deployed a previously undocumented backdoor known as **Dindoor**, along with additional malware tools, to maintain access within victim networks. The campaign appears to have started in early 2026 and involved organizations such as a U.S. airport, a bank, a non-profit organization, and a software supplier connected to the defense and aerospace industry.

The activity is attributed to MuddyWater (also tracked as Seedworm), a threat actor believed to operate under Iran's Ministry of Intelligence and Security.

Who Is the MuddyWater Threat Group?

MuddyWater is a state-aligned Advanced Persistent Threat (APT) group that has been active for several years and is widely associated with Iranian intelligence operations. Security agencies, including the FBI, CISA, and the UK's National Cyber Security Centre, have linked the group to the Iranian Ministry of Intelligence and Security.

SOCRadar Threat Actor Intelligence profile showing MuddyWater's activity

The group primarily conducts cyber espionage campaigns aimed at government entities, telecommunications providers, financial organizations, and critical infrastructure. Its operations typically involve long-term access to victim environments rather than quick disruption attacks.

MuddyWater has previously used spear-phishing, malicious documents, and custom backdoors to gain footholds inside targeted networks.

What Is the Dindoor Malware?

One of the key discoveries in the recent campaign is **Dindoor**, a previously unknown backdoor used to execute commands on compromised systems.

Dindoor is notable because it uses the **Deno runtime environment**, which allows JavaScript or TypeScript code to run outside a web browser. This design enables attackers to execute commands and maintain control over infected machines while blending into legitimate software processes.

Because the malware had not been publicly documented before, traditional signature-based security tools may struggle to detect it immediately.

Researchers also identified another backdoor called **Fakeset**, which is written in Python and used for similar remote access purposes.

Which Organizations Were Targeted?

The campaign affected several organizations across different sectors, including:

- A **U.S. airport**
- A **U.S. bank**
- A **Canadian non-profit organization**
- A **software company connected to the defense and aerospace industries**

Security researchers believe the Israeli operations of the software company may have been a primary target.

The targeting pattern suggests a focus on sectors with strategic or geopolitical importance, particularly organizations that handle sensitive operational or financial information.

How Did the Attackers Operate Inside the Networks?

Investigators found evidence that the attackers had already gained access to several networks before the campaign was publicly identified. In some cases, the threat actors had maintained access for weeks before the discovery of the malware.

Once inside the environment, the attackers deployed backdoors to establish persistent access and potentially collect sensitive data. Researchers also observed an attempt to exfiltrate data from one victim organization using **Rclone**, an open-source file synchronization tool, to transfer files to a cloud storage bucket hosted by Wasabi.

This type of tool abuse is common in advanced cyber espionage campaigns because legitimate utilities can help attackers avoid detection.

Why Is This Campaign Significant?

One important aspect of this campaign is its timing. Researchers noted that MuddyWater had already gained access to some networks before tensions in the region increased. Having this type of access allows attackers to gather intelligence or prepare for future operations.

Because MuddyWater is linked to Iranian state interests and some of the targets are connected to aviation, finance, and defense-related sectors, the activity may also be connected to the wider cyber activity surrounding the ongoing tensions between the U.S., Israel, and Iran.

For more context on how cyber operations have appeared alongside this conflict, see SOCRadar's analysis: https://socradar.io/blog/cyber-reflections-us-israel-iran-war/

What Indicators of Compromise Are Associated With the Campaign?

Security researchers and threat intelligence analysts have also shared **indicators of compromise (IoCs)** linked to the MuddyWater activity. These indicators can support threat hunting and help organizations identify potential communication with attacker infrastructure.

The following domains have been observed in connection with the campaign:

- gitempire.s3.us-east-005.backblazeb2[.]com
- elvenforest.s3.us-east-005.backblazeb2[.]com
- uppdatefile[.]com
- serialmenot[.]com
- moonzonet[.]com

Security teams should investigate environments for connections to these domains and monitor for unusual outbound traffic to cloud storage services, especially when combined with tools such as **Rclone** or unexpected **Deno runtime processes** on enterprise systems.

What Should Security Teams Watch For?

Security teams can reduce risk by focusing on behaviors associated with the campaign rather than relying solely on malware signatures.

Key defensive measures include:

- Monitoring unusual use of tools like **Rclone** for potential data exfiltration
- Investigating unexpected execution of **Deno runtime processes**
- Reviewing certificate usage associated with suspicious binaries
- Strengthening monitoring for persistence mechanisms and backdoor activity
- Hunting for indicators of compromise associated with MuddyWater campaigns

Threat actors associated with nation-state operations often maintain access for long periods before taking action. Early detection of unusual behavior can significantly reduce potential damage.

Tracking the Cyber Dimension of the Iran–Israel Conflict

Cyber activity linked to the Iran–Israel conflict continues to evolve alongside geopolitical developments. Campaigns involving groups like MuddyWater highlight how cyber operations can appear as part of broader regional tensions.

To help security teams monitor these developments, **SOCRadar provides a live Iran–Israel Cyber Conflict Dashboard**, which tracks cyber incidents, threat actor activity, and attack claims related to the conflict. The dashboard brings together intelligence on APT operations, hacktivist campaigns, DDoS attacks, data leaks, and regional targeting patterns in one place.

SOCRadar Iran–Israel Cyber Conflict Dashboard mapping cyber operations, threat actors, and regional targets linked to the conflict

By combining verified intelligence with real-time updates, the dashboard helps analysts and organizations better understand how cyber operations are evolving during the conflict.
