# MuddyWater Threat Group Deploys New BugSleep Backdoor

By gmcdouga

Published: 2024-07-15 · Archived: 2026-04-08 02:16:52 UTC

Check Point Research (CPR) warns that Iranian threat group MuddyWater has significantly increased its activities against Israel and is deploying a new, previously undocumented backdoor campaign.

**Key Findings**

- MuddyWater, an Iranian threat group affiliated with the Ministry of Intelligence and Security (MOIS), has significantly increased its activities in Israel since the beginning of the Israel-Hamas war in October 2023. This parallels with activities against targets in Saudi Arabia, Turkey, Azerbaijan, India and Portugal
- The threat actors consistently use phishing campaigns sent from compromised organizational email accounts, leading to the deployment of legitimate Remote Management Tools such as Atera Agent and Screen Connect
- Recently, MuddyWater campaigns also led to the deployment of a new, previously undocumented tailor-made backdoor dubbed BugSleep, that is used to target organizations in Israel
- BugSleep is a backdoor designed to execute the threat actors' commands and transfer files between the compromised machine and the C&C server. The backdoor is currently in development, with the threat actors continuously improving its functionality and addressing bugs

**Overview**

CPR has been tracking MuddyWater, the Iranian threat group affiliated with the country's Ministry of Intelligence and Security (MOIS), since 2019. Now, the group has significantly increased its activities in Israel since the beginning of the Israel-Hamas war in October 2023.

In addition to their usual phishing campaigns, with malicious deployment of legitimate Remote Management Tools, MuddyWater has begun deploying a new, previously undocumented backdoor. This backdoor, which Check Point Research has named BugSleep, is being specifically used to target organizations in Israel.

BugSleep is a new malware used in phishing lures since May 2024. Check Point Research discovered several versions of this malware being distributed. The backdoor updates are typically around improvements and bug fixes within the malware itself.

***For a deep dive analysis on the malware, and the latest malicious campaigns of MuddyWater visit the Check Point Research blog.***

**Campaign Targets**

These campaigns are targeting a number of different sectors, from governments to travel agencies and journalists. Most of these emails are targeted at Israeli companies, although others were aimed toward organizations in Turkey, Saudi Arabia, India and Portugal.

Figure 1 – Notable sectors targeted by MuddyWater phishing campaigns.

The usage of BugSleep marks a notable development in MuddyWater's techniques, tactics and procedures (TTPs). Beginning in October 2023, the threat actors have been using phishing campaigns sent from compromised email accounts, leading to the deployment of legitimate Remote Management Tools (RMM) such as Atera Agent and Screen Connect. Since February 2024, CPR has identified over 50 spear phishing emails, targeting more than 10 sectors, including municipalities, journalists and healthcare.

MuddyWater continues to push the deployment of these tools. In fact, a recent phishing email was sent to a Saudi Arabian company and an Israeli company. The payload for the Saudi Arabian company was an RMM; for the Israeli company it was BugSleep.

Figure 2 – Targeted countries for MuddyWater

These campaigns reflect MuddyWater's interests, focusing on specific sectors like airlines and media outlets. The nature of the lures has become simpler over time, and have evolved to introduce custom malware like BugSleep. Additionally, with a shift to generic lures and the increased use of English, the group can focus on higher volumes as opposed to specific targets.

**Check Point Customers Remain Protected Against the Threats Described in this Report**.

**Harmony Email and Collaboration** provides comprehensive inline protection at the highest security level.

**ThreatCloud AI's Threat Emulation engine offers these protections:**

APT.Wins.MuddyWater.ta.X

APT.Wins.MuddyWater.ta.Y

**Harmony Endpoint protections:**
APT.Win.MuddyWater.U

APT.Win.MuddyWater.V

APT.Win.MuddyWater.W

Check Point Research will continue to monitor this group's activities to ensure customers remain protected from their exploits.

---