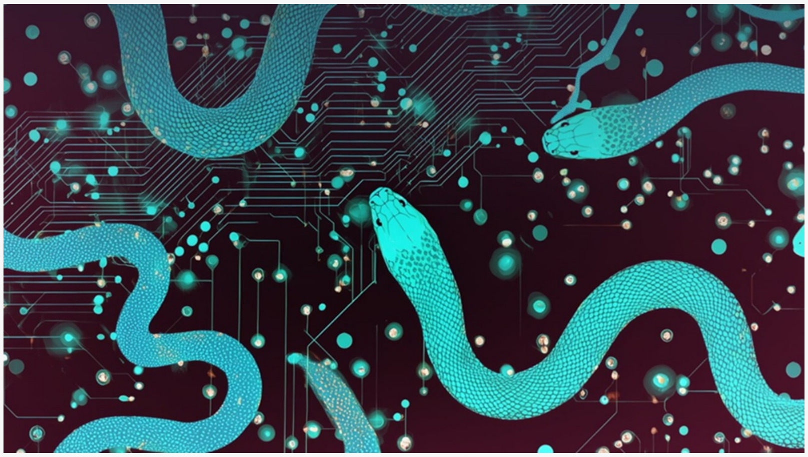
EINPRESSWIRE

Iran’s MuddyWater targets critical infrastructure in Israel and Egypt, masquerades as Snake game–ESET Research discovers



DUBAI , DUBAI, UNITED ARAB EMIRATES, December 8, 2025 /EINPresswire.com/ -- ESET researchers have identified new MuddyWater activity primarily targeting organizations in Israel, with one confirmed target in Egypt. The victims in Israel were in the technology, engineering, manufacturing, local government, and educational sectors. MuddyWater, also referred to as Mango Sandstorm or TA450, is an Iran-aligned cyberespionage group known for its persistent targeting of government and critical infrastructure sectors, often leveraging custom malware and publicly available tools, and has links to the Ministry of Intelligence and National Security of Iran. In this campaign, the attackers deployed a set of previously undocumented, custom tools with the objective of improving defense evasion and persistence. New backdoor MuddyViper enables the attackers to collect system information, execute files and shell commands, transfer files, and exfiltrate Windows login credentials and browser data. The campaign leverages additional credential stealers. Among these tools is Fooder, a custom loader that masquerades as the classic Snake game.

In this campaign, initial access is typically achieved through spearphishing emails, often containing PDF attachments that link to installers for remote monitoring and management (RMM) software hosted on free file-sharing platforms such as OneHub, Egnyte, or Mega. These links lead to the download of tools including Atera, Level, PDQ, and SimpleHelp. Among the tools deployed by MuddyWater operators is also the VAX One backdoor, named after the legitimate software which it impersonates: Veeam, AnyDesk, Xerox, and the OneDrive updater service.

The group’s continued reliance on this familiar playbook makes its activity relatively easy to detect and block. However, in this case, the group also used more advanced techniques to deploy MuddyViper, a new backdoor, by using a loader (Fooder) that reflectively loads MuddyViper into memory and executes it. Several versions of Fooder masquerade as the classic Snake game, hence the designation, MuddyViper. Another notable characteristic of Fooder is its frequent use of a custom delay function that implements the core logic of the Snake game, combined with "Sleep" API calls. These features are intended to delay execution in an attempt to hide malicious behavior from automated analysis systems. Additionally, MuddyWater developers adopted CNG, the next-generation Windows cryptographic API, which is unique for Iran-aligned groups and somewhat atypical across the broader threat landscape. During this campaign, the operators deliberately avoided hands-on-keyboard interactive sessions, which is a historically noisy technique often characterized by mistyped commands. Thus, while some components remain noisy and easily detected, as is typical for MuddyWater, overall this campaign shows signs of technical evolution – increased precision, strategic targeting, and a more advanced toolset.

The post-compromise toolset also includes multiple credential stealers: CE-Notes, which targets Chromium-based browsers; LP-Notes, which stages and verifies stolen credentials; and Blub, which steals login data from Chrome, Edge, Firefox, and Opera browsers.

MuddyWater was first introduced to the public in 2017 by Unit 42, whose description of the group's activity is consistent with ESET's profiling – a focus on cyberespionage, the use of malicious documents as attachments designed to prompt users to enable macros and bypass security controls, and primarily targeting entities located in the Middle East.

Notable past activities include Operation Quicksand (2020), a cyberespionage campaign targeting Israeli government entities and telecommunications organizations, which exemplifies the group's evolution from basic phishing tactics to more advanced, multistage operations; and a campaign targeting political groups and organizations in Türkiye, demonstrating the group's geopolitical focus, its ability to adapt social engineering tactics to local contexts, and reliance on modular malware and flexible C&C infrastructure.

ESET has documented multiple campaigns attributed to MuddyWater that highlight the group's evolving toolset and shifting operational focus. In March and April 2023, MuddyWater targeted an unidentified victim in Saudi Arabia, and the group conducted a campaign in January and February 2025 that was notable for its operational overlap with Lyceum (an OilRig subgroup). This cooperation suggests that MuddyWater may be acting as an initial access broker for other Iran-aligned groups.

For a more detailed analysis of the latest MuddyWater campaign, check out the latest ESET Research blogpost "MuddyWater: Snakes by the riverbank" on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X), BlueSky, and Mastodon for the latest news from ESET Research.

About ESET

ESET® provides cutting-edge cybersecurity to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of emerging global cyberthreats, both known and unknown—securing businesses, critical infrastructure, and individuals. Whether it’s endpoint, cloud, or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. The ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit ESET Middle East or follow us on LinkedIn, Facebook & X.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here
