MUDDY WATER

[/ ˈmʌd.i ˈwɔː.tər /]

MuddyWater, an Iran-linked APT active since 2015, conducts espionage and influence operations. High risk, it uses phishing and credential theft with open-source tools, mainly targeting government, telecom, defense, and NGOs in the Middle East, Europe, and North America.

IDENTITY

Attribution : Iran-aligned APT group, publicly tracked by multiple cybersecurity vendors.

Active Since : At least 2015.

Aliases : Earth Vetala, ATK51, Seedworm, COBALT ULSTER, TA450, Static Kitten, Mango Sandstorm, MERCURY, G0069, Boggy Serpens, TEMP.Zagros.

Motivation : Strategic cyber espionage and regional influence operations in line with Iranian geopolitical interests.

TTPs

Initial Access : Phishing and spear-phishing campaigns delivering malicious documents; exploitation of public-facing applications.

Persistence : Use of legitimate administrative tools, registry modifications, and long-term compromised accounts.

Command & Control (C2) : Relies on open-source tools, publicly available malware, and custom scripts for communication and control.

Malware & Tools : POWERSTATS, PowGoop, Small Sieve, MuddyC3, malicious PowerShell scripts, and repurposed open-source frameworks.

Techniques : Credential theft, lateral movement using stolen admin credentials, use of living-off-the-land binaries (LOLBins), and data exfiltration via encrypted channels.

TARGET PROFILE

Target Sectors : Government, telecom, defense, academia, NGOs, and energy infrastructure.

Geographies Targeted : Middle East (notably Israel, Saudi Arabia, and regional rivals), Europe, and North America.

THREAT ASSESSMENT

Risk Level : High – persistent and adaptive despite modest sophistication.

Most Recent Activity : Active through 2024–2025 with phishing and credential theft campaigns, often leveraging open-source frameworks and legitimate tools.

Evolution : Transitioned from basic spear-phishing operations to more stealthy intrusions involving custom malware and broader regional and global targeting.

NOTABLE OPERATIONS

- **2017–2018:** Conducted phishing attacks against telecom and government organizations in the Middle East.
- **2019:** Expanded targeting to include academia and NGOs in Europe.
- **2020:** Deployed malicious PowerShell scripts and open-source frameworks for espionage campaigns.
- **2021:** U.S. Cyber Command issued warnings about MuddyWater's use of open-source tools for credential theft.
- **2022:** Increased focus on defense and energy sectors in Israel and Saudi Arabia.
- **2023:** Expanded targeting to North American research institutions and European government entities.
- **2024–2025:** Active phishing and espionage campaigns using repurposed open-source malware and custom tools across Europe, North America, and the Middle East.