TIR-20260325 Iranian Threat Actor MuddyWater

3/25/2026

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

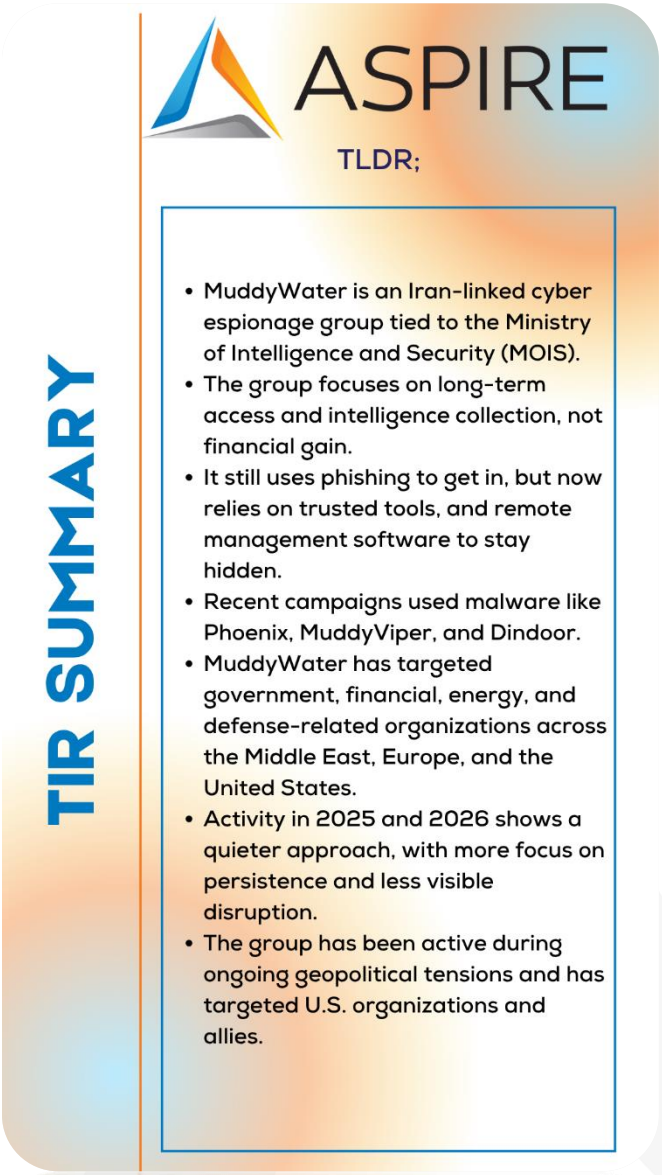
TABLE OF CONTENTS

Executive Summary

MuddyWater is an Iranian state-aligned cyber espionage group that has been active since at least 2017. The group is widely linked to Iran's Ministry of Intelligence and Security (MOIS) and focuses on long-term intelligence collection rather than financial gain. MuddyWater targets government agencies, critical infrastructure, and organizations tied to geopolitical interests. Over time, MuddyWater has built a reputation for persistence, often maintaining access to victim environments for weeks or months before taking action.

MuddyWater has evolved its operations. It still uses phishing to get in but now relies on remote tools and legitimate services to stay hidden. It also continues to expand its malware toolkit, including the Phoenix backdoor, MuddyViper, and Deno-based payloads like Dindoor.

MuddyWater is active in ongoing geopolitical tensions, including activity tied to operations surrounding Operation Epic Fury. The group has also been observed targeting organizations in the United States and allied countries. Let's look at MuddyWater and how the group's activity is shifting.



MuddyWater

MuddyWater is an Advanced Persistent Threat (APT) group believed to originate from Iran. Security agencies including the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the United Kingdom's National Cyber Security Centre (NCSC) have linked the group to Iran's Ministry of Intelligence and Security. The group has been active since at least 2017 and has conducted cyber espionage campaigns across multiple regions. Its operations focus on collecting intelligence rather than demanding ransoms, which separates it from financially motivated threat actors.

The group is known by several names, including Seedworm, TA450, TEMP.Zagros, Mango Sandstorm, Static Kitten, and Earth Vetala. These aliases reflect how different vendors and researchers track the same activity. MuddyWater targets a wide range of industries, including government, financial services, healthcare, telecommunications, software, and energy. The group has had victims in the Middle East, Africa, Europe, Asia, and North America. Countries frequently targeted include Israel, Turkey, Saudi Arabia, the United Arab Emirates, India, and the United States.

MuddyWater knows how to stay in a network without being noticed. It reuses the same infrastructure and blends into normal activity, which makes it harder to catch. The group is still active in 2026 and hasn't slowed down. In several cases, it has targeted organizations connected to foreign policy or regional conflict. Its operations are designed to remain low-key. Rather than disrupt systems immediately, the group collects data and maps networks over time.

MuddyWater has gotten better over time. Early campaigns were simple and relied on phishing and basic scripts. Now the group uses loaders, encrypted payloads, and better persistence. It also blends in with normal tools, which makes it harder to detect once it's inside.

Links to Other Threat Actors

MuddyWater has been linked to other Iranian threat groups through shared infrastructure and targeting patterns. There is overlap between MuddyWater and groups such as OilRig and Void Manticore. In some cases, one group appears to gain access

while another carries out follow-on activity. This suggests coordination within Iran's broader cyber operations.

There is also ongoing debate about whether MuddyWater operates as a single group. Some analysts believe it functions as a collection of operators working under a shared mission. This would explain variations in skill level and tooling across campaigns. Others assess that the group uses contracted operators or partners within the cybercriminal ecosystem.

Tactics, Techniques, and Procedures (TTPs)

MuddyWater has consistently relied on phishing as its primary entry point. The group sends emails that appear to come from trusted sources. In many cases, these emails come from compromised accounts, which increases the chance that the recipient will trust the message. Attachments often contain Microsoft Word documents that prompt users to enable macros. Once enabled, these macros execute code that installs a loader and deploys a backdoor. This method has remained a core part of the group's operations for years.

MuddyWater still uses phishing to get in, but what happens after that has changed. The group now relies on remote management tools and normal system activity to stay inside a network. It avoids dropping obvious malware when it can and uses tools that look legitimate. At the same time, its malware has improved. Newer payloads are harder to spot and built to keep access for longer periods.

MuddyWater 2026

- Uses remote management tools like Atera, Action1, PDQ, and ScreenConnect for access and control
- Creates SSH tunnels and uses cloud storage to move data out of the network
- Shifts away from basic scripts to tools like Phoenix v4, MuddyViper, UDPGangster, and Dindoor
- Runs payloads in memory and uses encryption to reduce visibility
- Focuses on staying in the network longer instead of moving fast

MuddyWater continues to exploit vulnerabilities when possible. The group has targeted public-facing applications, including Microsoft Exchange vulnerabilities and CVE-2017-0199. It has also used credential harvesting tools such as Mimikatz and LaZagne to expand access. Social engineering is also central to its operations. The group often uses themes tied to geopolitical events to increase the success of phishing campaigns.

In early 2026, MuddyWater targeted exposed Exchange and IIS servers using phishing emails that dropped backdoors like PowGoop and Small Sieve. This shows the group is not just getting in but coming back. The goal is to regain access and stay inside without being noticed.

Common MITRE Techniques Observed

- Initial Access, Spearphishing Attachment [T1566.001] – The attacker delivers malicious Word documents with embedded macros to gain access.
- Initial Access, Spearphishing Link [T1566.002] – The attacker sends links to file-sharing platforms hosting malicious payloads.
- Execution, Command and Scripting Interpreter: PowerShell [T1059.001] – The attacker uses PowerShell to execute payloads and manage activity.
- Persistence, Scheduled Task/Job: Scheduled Task [T1053.005] – The attacker creates scheduled tasks to maintain access.
- Execution, Windows Management Instrumentation [T1047] – The attacker uses WMI to execute commands and gather system data.
- Credential Access, OS Credential Dumping [T1003] – The attacker dumps credentials from system memory or registry hives.

Recent Attacks

Israeli and Egyptian Organizations

In late 2024 through early 2025, MuddyWater targeted Israeli and Egyptian organizations. The group deployed a new loader known as Fooder, which delivered the

MuddyViper backdoor. Victims included organizations in engineering, government, and utilities sectors. The attack relied on phishing and custom malware. The group maintained access while collecting credentials and system data.

The Middle East and North Africa

In October 2025, MuddyWater launched a large phishing campaign targeting more than 100 organizations across the Middle East and North Africa. The group used a compromised email account to send malicious Word documents. These documents deployed the Phoenix v4 backdoor through a loader called FakeUpdate. Targets included embassies and international organizations. The campaign focused on intelligence collection and used shared infrastructure across multiple operations.

The United States and Canada

In early 2026, MuddyWater targeted organizations in the United States and Canada using Dindoor malware. Victims included a U.S. airport, a financial institution, and a software company tied to the defense sector. The group maintained access for weeks before detection. It used Rclone to move data to cloud storage and relied on Deno-based payloads to blend into legitimate processes.

Why MuddyWater is Still a Threat

MuddyWater is still active because it continues to adapt. The group has not abandoned older methods but has layered new techniques on top of them. This includes the use of remote management tools, cloud services, and new malware families. These changes allow it to operate quietly inside networks. Once inside, it can move slowly and avoid detection.

The group's involvement in geopolitical activity also raises concern. MuddyWater has been linked to operations tied to regional tensions, including activity surrounding Operation Epic Fury. These campaigns often focus on intelligence collection before or during periods of conflict. This suggests that cyber operations are being used to support broader strategic goals.

MuddyWater has also expanded its reach. Recent campaigns show activity in the United States and allied countries. Targets include critical infrastructure, financial systems, and defense-related organizations. This places the group in a position to gather sensitive information that could be used in future operations. United States agencies have warned that Iranian cyber actors, including MuddyWater, continue to target domestic organizations.

There is concern because of the group's persistence. MuddyWater does not rely on a single method or tool. It reuses what works and improves over time. Its use of compromised accounts, legitimate software, and short-lived infrastructure makes it difficult to track. Even when one campaign is disrupted, the group often returns using a slightly different approach.

Why Organizations Should Care

- MuddyWater maintains access for long periods, increasing the risk of data exposure.
- The group targets sectors tied to national security and economic stability.
- Its use of legitimate tools makes detection harder for traditional defenses.
- Campaigns often align with geopolitical events, increasing risk during periods of conflict.

CONCLUSION

MuddyWater's activity has expanded far past its original regional attacks, and the group now operates across multiple regions. The group shows a steady refinement in how they work rather than major shifts in strategy. Their focus on intelligence collection is consistent, and they continue to adjust their tactics to stay effective. Based on their current targeting, there is no sign that their operations will slow in the near future.

ASPIRE'S RECOMMENDATIONS

Organizations should take steps now to reduce the risk of compromise from MuddyWater activity. These campaigns rely on a mix of phishing, legitimate tools, and stealthy malware. Defenses should focus on both prevention and detection.

- Disable Office macros by default and watch for any attempt to turn them back on. MuddyWater still relies on this step to kick off its infection chain.
- Lock down remote management tools like Atera, PDQ, and Action1. Only allow what is needed and alert on anything outside normal use.
- Enforce multi-factor authentication across all email and remote access points. This cuts off one of their most effective entry points, which is compromised accounts.
- Monitor outbound traffic for connections to cloud storage services and unknown domains. MuddyWater uses these paths to move data out quietly.
- Use behavior-based detection to catch unusual PowerShell use, command-line activity, and registry changes tied to persistence. These are common signs the group is active inside a system.

MITRE MAP

Reconnaissance	T1598 – Phishing for Information T1593 – Search Open Websites/Domains
Initial Access	T1566.001 – Phishing: Spearphishing Attachment T1566.002 – Phishing: Spearphishing Link T1078 – Valid Accounts
Execution	T1204 – User Execution T1059.001 – Command and Scripting Interpreter: PowerShell T1059.003 – Command and Scripting Interpreter: Windows Command Shell

Persistence	T1053.005 – Scheduled Task/Job: Scheduled Task
Privilege Escalation	T1548.002 – Abuse Elevation Control Mechanism: Bypass User Account Control
Defense Evasion	T1055 – Process Injection
Credential Access	T1003 – OS Credential Dumping
Lateral Movement	T1534 – Internal Spearphishing
Command and Control	T1071 – Application Layer Protocol T1090 – Proxy
Exfiltration	T1567 – Exfiltration Over Web Services

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.
  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.
- **Aspire Incident Response**

- The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
- Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Indicators of Compromise (IoCs)

Domains

- screenai[.]online
- uppdatefile[.]com
- serialmenot[.]com
- moonzonet[.]com

IP Addresses

- 159[.]198[.]36[.]115

File Hashes

- 6de859a27ccc784689e8748cef536e32780e498a
- bed6506f8f5281888f89781cf6fbc750545292fc

URLs

- hxxp://159[.]198[.]36[.]115:4444/chromium_stealer_user.exe

Supporting Documentation

MuddyWater Targets MENA Organizations with GhostFetch, CHAR, and HTTP_VIP

Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks | CISA

U.S. says Iranian 'MuddyWater' cyber actors targeting various sectors worldwide | Reuters

Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: Iranian APT MuddyWater targets Turkish users via malicious PDFs, executables

Cyber Insights 2022: Nation-States | SecurityWeek.Com

Statement by President Joe Biden on Cybersecurity Awareness Month | The White House

Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks | CISA

MuddyWater APT Group | Iranian Cyber Espionage Profile

Iranian APT: New Methods to Target Turkey, Arabian Peninsula (bankinfosecurity.com)

Unmasking an Attack Chain of MuddyWater | Huntress

FBI Disrupts Cyclops Blink Botnet Used by Russian Intelligence Directorate (hackread.com)

MuddyWater targets Middle Eastern and Asian countries in phishing attacks | TechRepublic

Iranian MOIS Actors & the Cyber Crime Connection - Check Point Research

MuddyWater strikes Israel with advanced MuddyViper malware

Sophos MDR blocks and tracks activity from probable Iranian state actor “MuddyWater” | SOPHOS

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

Iran-Linked MuddyWater Targets 100+ Organizations in Global Espionage Campaign

MuddyWater APT Profile: Tactics, Malware, And MITRE ATT&CK

Unmasking MuddyWater’s New Malware Toolkit Driving International Espionage | Group-IB Blog

Boggy Serpens Threat Assessment

Appendix II: Disclaimer

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.