Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

MuddyWater: Iran's Adaptive Cyber Espionage Machine

Date of Publication	Admiralty Code	TA Number
March 26, 2026	A1	TA2026082

Summary

First Seen: 2017
Targeted Regions: Afghanistan, Armenia, Austria, Azerbaijan, Bahrain, Belarus, Egypt, Georgia, India, Iran, Iraq, Israel, Jordan, Kuwait, Laos, Lebanon, Mali, Netherlands, Oman, Pakistan, Portugal, Qatar, Russia, Saudi Arabia, Sudan, Tajikistan, Tanzania, Thailand, Tunisia, Turkey, UAE, Ukraine, USA, Canada, North Africa
Targeted Industries: Aviation, Defense, Education, Energy, Financial, Food and Agriculture, Gaming, Government, Healthcare, High-Tech, IT, Media, NGOs, Oil and gas, Shipping and Logistics, Telecommunications, Transportation, Software/Technology, Critical Infrastructure
Targeted Platforms: Windows, Linux
Targeted Products: BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA), Ivanti Endpoint Manager Mobile (EPMM), n8n, Meta React Server Components, SmarterTools SmarterMail, Laravel Livewire, N-able N-central, Citrix NetScaler ADC and NetScaler Gateway, Langflow, Fortinet FortiOS and FortiProxy
Threat Actor: MuddyWater (aka Static Kitten, Seedworm, TEMP.Zagros, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Mango Sandstorm, Boggy Serpens, Yellow Nix, Earth Vetala)
Malware: Dindoor, Fakeset, Stagecomp, Darkcomp, LampoRAT, UDPGangster, BlackBeard, Nuso, Phoenix

Actor Map

Actor Details

#1 MuddyWater is an Iranian state-sponsored advanced persistent threat (APT) group active since at least 2017, widely attributed to the Ministry of Intelligence and Security (MOIS). Its operations are primarily centered on cyber espionage, with consistent targeting of government, defense, telecommunications, energy, financial services, and other critical infrastructure sectors across the Middle East, North America, Europe, and Africa. The group's activity aligns closely with Iran's strategic intelligence-gathering objectives, often focusing on organizations of geopolitical and economic significance.

#2 The group is characterized by its agility in adopting new tooling and evolving its tradecraft. MuddyWater frequently develops malware across multiple languages, including PowerShell, Python, JavaScript, and increasingly Rust, while maintaining a strong dependence on social engineering, particularly spear-phishing, for initial access. In parallel, it actively exploits vulnerabilities in public-facing applications to establish footholds, reflecting a hybrid intrusion approach that blends opportunistic exploitation with targeted intrusion techniques.

#3 Recent campaigns highlight a notable shift in both tooling sophistication and operational tempo. Since early February 2026, MuddyWater has deployed the previously undocumented Dindoor backdoor, built on the Deno JavaScript runtime, targeting U.S. entities such as banks, airports, NGOs, and an Israeli defense software affiliate. Alongside this, the group leveraged the Python-based Fakeset backdoor and used Rclone to exfiltrate data to Wasabi cloud storage. This surge in activity coincides with heightened geopolitical tensions, raising concerns that existing intrusions could transition into disruptive or destructive operations.

#4 In parallel, the group conducted **Operation Olalampo** (January–February 2026), targeting organizations across the MENA region with a new malware arsenal including GhostFetch, GhostBackDoor, HTTP_VIP, and the CHAR backdoor written in Rust. Notably, this campaign incorporated Telegram-based command-and-control channels and exhibited indicators of AI-assisted development, signaling an evolution in both development practices and operational flexibility. Additional activity in March 2026 suggests continued targeting of government and telecom sectors across GCC countries, including Saudi Arabia, the UAE, Kuwait, and Bahrain.

#5

MuddyWater has recently strengthened its toolkit with more evasive and persistent capabilities, introducing tools like the UDPGangster backdoor for stealthy communication and LampoRAT, a Rust-based RAT used in targeted attacks. The group is also leveraging AI-assisted development and Rust-based implants such as BlackBeard to rapidly deploy tailored payloads. In a campaign using a malicious Excel lure, it delivered a new payload family, Nuso, highlighting a shift toward more advanced final-stage infections and a modular, adaptive attack approach.

#6

Throughout 2025, MuddyWater sustained large-scale spear-phishing campaigns across the **Middle East**, leveraging compromised legitimate email accounts to enhance credibility. These operations delivered malware such as **RustyWater**, a Rust-based remote access implant featuring asynchronous C2 communication, registry-based persistence, and modular post-exploitation capabilities, as well as the Phoenix backdoor. The group combined custom payloads with legitimate remote management tools to improve stealth and persistence, while using techniques such as icon spoofing and macro-enabled Word documents to increase infection success rates.

#7

Exposure of the group's infrastructure has further revealed a mature and layered operational ecosystem. This includes extensive reconnaissance using tools like Shodan, Nuclei, and Subfinder; custom command-and-control frameworks such as KeyC2, PersianC2, and ArenaC2; and tunneling utilities like Neo-reGeorg and Resocks. Evidence also points to password spraying activity, exploitation attempts across numerous CVEs, and the use of a PowerShell-based loader. Collectively, these capabilities underscore MuddyWater's adaptability and depth in both offensive tooling and infrastructure management.

#8

Overall, MuddyWater remains a high-risk threat actor with a strong likelihood of sustained and potentially escalating activity. Its continued investment in diverse malware development, combined with its alignment to Iranian strategic interests and current geopolitical dynamics, positions it as a persistent and evolving threat to organizations operating in sensitive or high-value sectors.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
MuddyWater (aka Static Kitten, Seedworm, TEMP.Zagros, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Mango Sandstorm, Boggy Serpens, Yellow Nix, Earth Vetala)	Iran **MOTIVE** Cyber Espionage, Intelligence Collection, Pre-positioning for Potential Destructive Operations	Afghanistan, Armenia, Austria, Azerbaijan, Bahrain, Belarus, Egypt, Georgia, India, Iran, Iraq, Israel, Jordan, Kuwait, Laos, Lebanon, Mali, Netherlands, Oman, Pakistan, Portugal, Qatar, Russia, Saudi Arabia, Sudan, Tajikistan, Tanzania, Thailand, Tunisia, Turkey, UAE, Ukraine, USA, Canada, North Africa	Aviation, Defense, Education, Energy, Financial, Food and Agriculture, Gaming, Government, Healthcare, High-Tech, IT, Media, NGOs, Oil and gas, Shipping and Logistics, Telecommunications, Transportation, Software/Technology, Critical Infrastructure

Recommendations

Strengthen Email and Initial Access Defenses: MuddyWater heavily relies on spear-phishing to gain initial access, making email security a critical first line of defense. Organizations should implement advanced email filtering, block malicious attachments, and disable macros by default. Regular security awareness training can help employees identify phishing attempts, especially those that appear to originate from trusted or internal sources. At the same time, all public-facing systems should be regularly updated and patched to prevent exploitation of known vulnerabilities.

Enhance Visibility and Threat Detection: Early detection is key to limiting impact. Security teams should monitor for unusual activity involving scripting environments such as PowerShell, Python, and JavaScript runtimes, as MuddyWater frequently abuses these. The use of tools like Rclone for data exfiltration should also be closely tracked. Deploying endpoint detection and response (EDR) solutions, combined with centralized logging, enables faster identification of suspicious behavior. Enforcing multi-factor authentication (MFA) and limiting administrative privileges further reduces the attack surface.

Adopt Zero Trust and Network Controls: Given the group's tendency to blend malicious activity with legitimate tools and services, organizations should adopt a zero-trust approach, verifying every access request regardless of origin. Network segmentation is equally important, as it helps contain threats and prevents lateral movement within the environment. Monitoring outbound traffic, particularly to cloud storage services, can help detect covert data exfiltration and command-and-control communications.

Prepare for Incident Response and Recovery: Organizations should assume that sophisticated actors like MuddyWater may eventually gain access and plan accordingly. Maintaining regular, secure backups ensures that critical data can be restored if needed. A well-defined and tested incident response plan allows teams to respond quickly, contain threats, and minimize damage. Staying up to date on emerging threat activity and continuously refining defensive measures will help organizations remain resilient against evolving campaigns.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.001: Spear-Phishing Attachment
	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.007: JavaScript
		T1059.006: Python
		T1059.001: PowerShell
	T1204: User Execution	T1204.002: Malicious File
Persistence	T1053: Scheduled Task/Job	
	T1219: Remote Access Software	
Defense Evasion	T1027: Obfuscated Files or Information	
	T1553: Subvert Trust Controls	T1553.002: Code Signing
Credential Access	T1110: Brute Force	T1110.003: Password Spraying
Discovery	T1082: System Information Discovery	
Lateral Movement	T1021: Remote Services	
Collection	T1115: Clipboard Data	

Tactic	Technique	Sub-technique
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1102: Web Service	
	T1105: Ingress Tool Transfer	
	T1572: Protocol Tunneling	
Exfiltration	T1567: Exfiltration Over Web Service	T1567.002: Exfiltration to Cloud Storage
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	0f9cf1cf8d641562053ce533aaa413754db88e60404cab6bbaa11f2b2491d542, 1d984d4b2b508b56a77c9a567fb7a50c858e672d56e8cf7677a1fca5c98c95d1, 2a00705cfd3c15cf8913e9eb4e23968efd06f1feceaef9987d26c5518887d043, 2a09bbb3d1ddb729ea7591f197b5955453aa3769c6fb98a5ef60c6e4b7df23a5, 42a5db2a020155b2adb77c00cbe6c6ad27c2285d8c6114679d9d34137e870b3f, 7467f326677a4a2c8576e71a832e297e794ea00e9b67c4fcbe78b5aec697cec4, 7c30c16e7a311dc0cdb1cdfd9ea6e502f44c027328dbe7d960b9bcd85ccf5eef, b0af82de672d81f3c2f153977923b3884a8a9e7045b182c2379b19a1996931a0, bd8203ab88983bc081545ff325f39e9c5cd5eb6a99d04ae2a6cf862535c9829a, c7cf1575336e78946f4fe4b0e7416b6ebe6813a1a040c54fb6ad82e72673478e, 077ab28d66abdafad9f5411e18d26e87fe43da1410ee8fe846bd721ab0cb52de, 15061036c702ad92b56b35e42cf5dc334597e7311e98d2fdd3815a69ac3b1d84, 2b7d8a519f44d3105e9fde2770c75efb933994c658855dca7d48c8b4897f81e6, 4aef998e3b3f6ca21c78ed71732c9d2bdcc8a4e0284f51d7462c79d446fbc7be,

TYPE	VALUE
SHA256	64263640a6fdeb2388bca2e9094a17065308cf8dcb0032454c0a71d9b78327eb, 64cf334716f15da1db7981fad6c81a640d94aa1d65391ef879f4b7b6edf6e7f1, 74db1f653da6de134bdc526412a517a30b6856de9c3e5d0c742cb5fe9959ad0d, 94f05495eb1b2ebe592481e01d3900615040aa02bd1807b705a50e45d7c53444, a4bd1371fe644d7e6898045cc8e7b5e1562bdfd0e4871d46034e29a22dec6377, a5d4d6be3bfe0cba23fe6b44984b5fc9c7c7e10030be96120bb30da0f2545d4c, ddceade244c636435f2444cd4c4d3dc161981f3af1f622c03442747ecef50888, 24857fe82f454719cd18bcbe19b0cfa5387bee1022008b7f5f3a8be9f05e4d14, A92d28f1d32e3a9ab7c3691f8bfca8f7586bb0666adbba47eab3e1a8faf7ecc0, 3df9dcc45d2a3b1f639e40d47eceeafb229f6d9e7f0adcd8f1731af1563ffb90, 1319d474d19eb386841732c728acf0c5fe64aa135101c6ceee1bd0369ecf97b6, c3afd5ce1ca50a38438bb5026cca27bfbf2d8e786e03f323adceb8ad17517eca, 52d8fb9a11920f27b9a3b43f27c275767a57cdffc95af94b7b66433506287314, b2c52fde1301a3624a9ceb995f2de4112d57fcbc6a4695799aec15af4fa0a122, 1c16b271c0c4e277eb3d1a7795d4746ce80152f04827a4f3c5798aaf4d51f6a1, 4db3645f678fb519b9f529dde41f77944754f574f16a9a845c22d3703da5bed0, 2c92c7bf2d6574f9240032ec6adee738edddc2ba8d3207eb102eddf4ab963db0, 23f3a98befdff13c802eed32eea754018b8b525ec0dd3afce8459a0287df74ec, 69e038b9f3a228f09059bc1ce92b1c5c49396bb70987a38df0fdb39eed380b22, 84e665a0dfbff74b4c356bfa282c7c253ae3411a8f4d58bfe121c8411c52552c, 6f079c1e2655ed391fb8f0b6bfafa126acf905732b5554f38a9d32d0b9ca407d, 7ea4b307e84c8b32c0220eca13155a4cf66617241f96b8af26ce2db8115e3d53, f38a56b8dc0e8a581999621eef65ef497f0ac0d35e953bd94335926f00e9464f,

TYPE	VALUE
SHA256	0ce54a5a6f061b158e3891aadd03773d0bae220b0316e84fc042a741924b3525, 167d5ab70f55c100e51833fbfea44048095889c162e1330df0631423fc547409, 4d2958d93d4650fc4a70f70663fe6943e8c11d61b2824512da296e8fd84e5bb9, 156b325231742a73ded4104fbde1c55ad3913d2eaf09b5194ef74c81ee3ba393, cc2ec568f978f328b6de112670a1b35ca1f9db377ff32cb9d313a5b2ac3c127b, 7523e53c979692f9eecff6ec760ac3df5b47f172114286e570b6bba3b2133f58, 0be499354dc498248d27f6d186eb3bb75a607ae4a2c0a6734c76f1a1b7b1d316, 81a6e6416eb7ab6ce6367c6102c031e2ae2730c3c50ab9ce0b8668fec3487848, 47bb271c34210f52e3e08339a0c83688d9e9aa5c7cfc45b3e4bdffd1753f6cb2, 1b9e6fe4b03285b2e768c57e320d84323ac9167598395918d56a12e568b0009a, 9c207c51c448f96eaae91241a39c8bb85e2307f2d2a99244763a53176cf4c02f, c91413ad7c94c0e2694862b9d671d1204873bf65576ba2cb91fbd562a4ccf79b, 668dd5b6fb06fe30a98dd59dd802258b45394ccd7cd610f0aaab43d801bf1a1e, 5ec5a2adaa82a983fcc42ed9f720f4e894652bd7bd1f366826a16ac98bb91839, a2001892410e9f34ff0d02c8bc9e7c53b0bd10da58461e1e9eab26bdbf410c79, 1bcd8d7dc7bed5873bbdd2822e84e19773a33d659b16587ca9dc6db204447a86, fc4a7eed5cb18c52265622ac39a5cef31eec101c898b4016874458d2722ec430, 8d2227f2c53d7e22a57e12c45cecdd43dbec08dbc3ab93e74e6df52cdf80548b, 1bcd8d7dc7bed5873bbdd2822e84e19773a33d659b16587ca9dc6db204447a86, 5323a573e3f423b69ef965dadb3c059879d718b1c9052038ef749868cf361891
Telegram Bot ID	8398566164:AAEJbk6EOirZ_ybm4PJ-q8mOpr1RkZx1H7Q

TYPE	VALUE
Domains	gitempire[.]s3[.]us-east-005[.]backblazeb2[.]com, elvenforest[.]s3[.]us-east-005[.]backblazeb2[.]com, uppdatefile[.]com, serialmenot[.]com, moonzonet[.]com, bootcamptg[.]org, codefusiontech[.]org, maxisteq[.]org, miniquest[.]org, Netivtech[.]org, nomercys.it[.]com, promoverse[.]org, reminders[.]trahum[.]org, screenai[.]online, stratioai[.]org
IPv4	157[.]20[.]182[.]75, 64[.]7[.]198[.]12, 46[.]101[.]36[.]39, 159[.]198[.]68[.]25, 159[.]198[.]66[.]153
PDB Path	C:\Users\win10\Desktop\phonix\phoenix\x64\Release\phoenix.pdb, Char.pdb, C:\Users\nuso\source\repos\http_vip\http_vip\f*ckAnalyzor.pdb, C:\Users\nuso\source\repos\http_last_ver\http_last_ver\f*ckAnalyser.pdb, D:\phonix\phoenixV3\phoenixV3\phoenixV2\x64\Release\phoenix.pdb, C:\Users\win10\Desktop\phoenixV4\phoenixV3\phoenixV2\x64\Release\phoenix.pdb, C:\Users\win10\Desktop\phoenixV4\phoenixV3\phoenixV2\x64\Debug\phoenix.pdb, C:\Users\piper\source\repos\udp_3.0 - Copy\x64\release_86\udp_3.0.pdb, C:\Users\gangster\source\repos\udp_3.0 - Copy - Copy\x64\release_86\udp_3.0.pdb, C:\Users\SURGE\source\repos\udp_3.0 - Copy\x64\release_86\udp_3.0.pdb

References

https://www.security.com/threat-intelligence/iran-cyber-threat-activity-us

https://securityaffairs.com/189060/apt/iran-linked-muddywater-deploys-dindoor-malware-against-u-s-organizations.html

https://www.darkreading.com/threat-intelligence/iran-muddywater-new-malware-tensions-mount

https://www.esentire.com/security-advisories/iranian-apt-muddywater-exposed

https://www.rescana.com/post/muddywater-s-dindoor-backdoor-iranian-apt-targets-u-s-organizations-via-deno-runtime-and-cloud-sto

https://hivepro.com/threat-advisory/muddywaters-rust-implants-target-the-middle-east/

https://hivepro.com/threat-advisory/operation-olalampo-muddywater-expanding-campaign-across-mena/

https://hivepro.com/threat-advisory/echoes-over-udp-muddywaters-covert-backdoor-strikes/

https://hivepro.com/threat-advisory/serpents-in-disguise-muddywaters-hidden-toolset-exposed/

https://hivepro.com/threat-advisory/muddywater-deploys-phoenix-backdoor-in-targeted-espionage-campaign/

https://attack.mitre.org/groups/G0069/

https://unit42.paloaltonetworks.com/boggy-serpens-threat-assessment/

Appendix

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-1731	BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) OS Command Injection Vulnerability	BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA)	✗	✓	✓
CVE-2026-1281	Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability	Ivanti Endpoint Manager Mobile (EPMM)	✓	✓	✓
CVE-2025-68613	n8n Improper Control of Dynamically-Managed Code Resources Vulnerability	n8n	✗	✓	✓
CVE-2025-55182	Meta React Server Components Remote Code Execution Vulnerability	Meta React Server Components	✗	✓	✓
CVE-2025-52691	SmarterTools SmarterMail Unrestricted Upload of File with Dangerous Type Vulnerability	SmarterTools SmarterMail	✗	✓	✓
CVE-2025-54068	Laravel Livewire Code Injection Vulnerability	Laravel Livewire	✗	✓	✓
CVE-2025-9316	N-able N-central Unauthenticated SessionID Generation Vulnerability	N-able N-central	✗	✗	✓
CVE-2025-5777	Citrix NetScaler ADC and Gateway Out-of-Bounds Read Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✗	✓	✓
CVE-2025-34291	Langflow Remote Code Execution Vulnerability	Langflow	✗	✗	✓

Note: Vulnerabilities exploited by MuddyWater. The Patch links are hyperlinked to the patch icon.

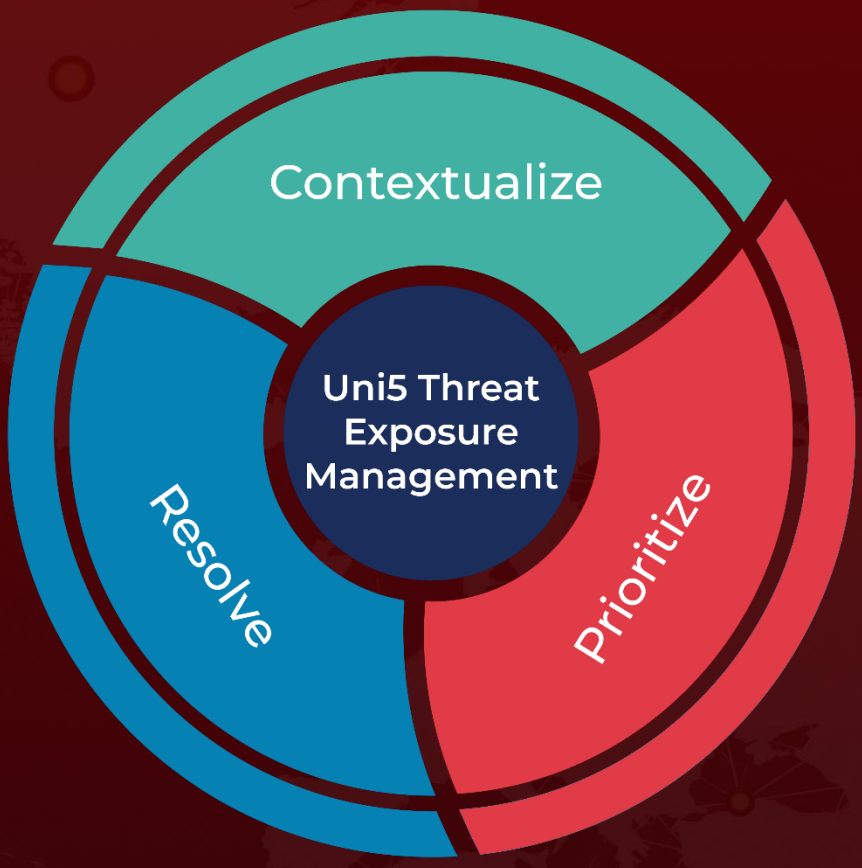
CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-55591	Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability	Fortinet FortiOS and FortiProxy	✓	✓	✓
CVE-2024-23113	Fortinet Multiple Products Format String Vulnerability	Fortinet Multiple Products	✗	✓	✓
CVE-2022-42475	Fortinet FortiOS Heap-Based Buffer Overflow Vulnerability	Fortinet FortiOS	✓	✓	✓

Note: Vulnerabilities exploited by MuddyWater. The Patch links are hyperlinked to the patch icon.

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 26, 2026 • 5:30 AM

More at www.hivepro.com