Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

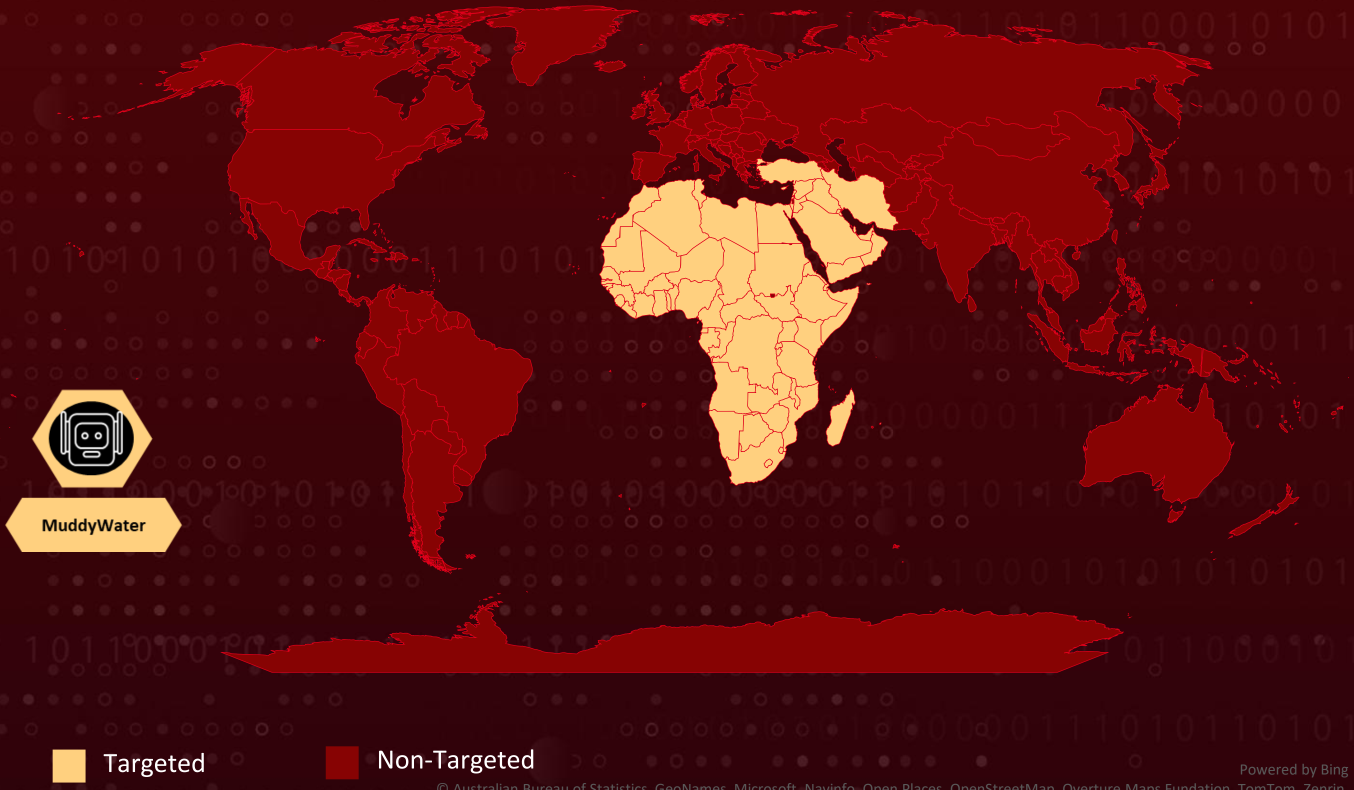
Operation Olalampo: MuddyWater's Expanding Campaign Across MENA

Date of Publication	Admiralty Code	TA Number
February 25, 2026	A1	TA2026054

Summary

First Seen: January 26, 2026
Targeted Regions: Middle East and North Africa (MENA), META (Middle East, Turkey, Africa)
Targeted Platform: Windows
Targeted Products: Microsoft Office (Excel, Word), AnyDesk (abused as RMM tool)
Targeted Industries: Energy, Marine Services, System Integrators, Government
Threat Actor: MuddyWater (aka Earth Vetala, Mango Sandstorm, MUDDYCOAST, Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Boggy Serpens, Yellow Nix)
Malware: GhostFetch, HTTP_VIP, CHAR, GhostBackDoor
Campaign: Operation Olalampo
Attack: The Iranian state-aligned APT group MuddyWater, associated with Iran's Ministry of Intelligence and Security (MOIS), launched Operation Olalampo to target organizations and individuals primarily across the MENA region. The campaign deploys four distinct malware families, such as GhostFetch, GhostBackDoor, HTTP_VIP, and CHAR. Through spear-phishing emails containing weaponized Microsoft Office documents with malicious macro code. The operation uses a diversified command-and-control infrastructure and shows signs of AI-assisted malware development.

Attack Regions



© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Attack Details

#1

The Iranian cyber-espionage group MuddyWater has launched a new campaign, Operation Olalampo, targeting organizations and individuals across the Middle East and North Africa. First observed on January 26, 2026, the operation introduces new malware tools, including the GhostFetch and HTTP_VIP downloaders, a Rust-based backdoor called CHAR, and an advanced implant known as GhostBackDoor.

#2

The attacks begin with carefully crafted spear-phishing emails carrying malicious Microsoft Office documents. Each document is tailored to regional themes to appear legitimate. In one variant, a fake Excel file posing as an energy and marine services company triggers hidden code once macros are enabled, installing the CHAR backdoor. Another Excel-based lure deploys the GhostFetch downloader instead. A third variant uses Word documents themed around flight tickets and reports to deliver HTTP_VIP, often targeting specific individuals and system integrators.

#3

Once activated, the malware follows different paths. GhostFetch first analyzes the infected system, checking for virtual machines, security software, and user activity to avoid detection. It loads additional payloads directly into memory and installs GhostBackDoor, which adapts to system privileges and enables remote control, file access, and reinfection if needed. In the CHAR variant, attackers control compromised systems through a Telegram bot named “Olalampo,” issuing commands through PowerShell or the Windows command interface.

#4

Post-compromise activity shows a focus on credential theft and long-term access. Using CHAR, operators deploy a SOCKS5 reverse proxy, additional backdoors such as Kalim, and tools designed to extract browser data. Some components reveal signs of AI-assisted development and share structural similarities with earlier MuddyWater malware such as BlackBeard, also known as Archer RAT or RUSTRIC.

#5

The HTTP_VIP variant performs system reconnaissance, connects to a command server, and installs AnyDesk to gain full remote access. A newer version expands its capabilities to include file transfer, clipboard capture, interactive shell access, and system profiling. Beyond phishing, the group also exploits newly disclosed server vulnerabilities to enter networks, maintaining multiple access routes and a layered command structure to support sustained cyber-espionage operations.

Recommendations

Disable Office Macros by Default: Enforce Group Policy Objects (GPO) to restrict macro execution from untrusted sources across all endpoints. Only permit digitally signed macros where business-critical operations require them, and log all macro execution events for audit purposes.

Deploy Endpoint Detection for Rust-Based Implants: Update EDR signatures and behavioral detection rules to identify CHAR, GhostFetch, GhostBackDoor, and HTTP_VIP payloads. Integrate the YARA rules and EDR detection rules published in Group-IB's report into existing security tooling.

Monitor for In-Memory Payload Execution: Since GhostFetch retrieves and executes payloads directly in memory to evade disk-based detection, implement memory scanning capabilities and behavioral analysis rules that detect fileless execution techniques such as process hollowing and reflective DLL injection.

Implement Multi-Factor Authentication: Enforce MFA on all critical accounts, VPN gateways, and remote access platforms to mitigate credential theft risk from browser data exfiltration observed in MuddyWater's post-exploitation activities.

Monitor Suspicious PowerShell and cmd.exe Activity: Deploy behavioral detection rules for PowerShell-based SOCKS5 reverse proxy execution, unusual cmd.exe invocations, and unexpected Telegram API communications from endpoints, as these are key indicators of CHAR backdoor activity.

Hunt for Post-Exploitation Artifacts: Proactively search for the presence of executables named "sh.exe" and "gshdoc_release_X64_GUI.exe," suspicious directory creation under the Public user folder, and anomalous outbound traffic patterns consistent with SOCKS5 proxy or Telegram bot beaconing.

Implement Network Segmentation: Segment critical assets and limit lateral movement potential by enforcing strict network access controls between trust zones. Monitor east-west traffic for anomalous patterns indicative of network enumeration or credential harvesting activities.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1587: Develop Capabilities	T1587.001: Malware
Initial Access	T1566: Phishing	T1566.001: Spear-phishing Attachment
	T1190: Exploit Public-Facing Application	
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
	T1106: Native API	
Persistence	T1547: Boot or Logon Autostart Execution	
Defense Evasion	T1140: Deobfuscate/Decode Files or Information	
	T1620: Reflective Code Loading	
	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1036: Masquerading	
Discovery	T1082: System Information Discovery	
	T1033: System Owner/User Discovery	
Credential Access	T1555: Credentials from Password Stores	

Tactic	Technique	Sub-technique
Collection	T1115: Clipboard Data	
	T1005: Data from Local System	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1102: Web Service	
	T1219: Remote Access Software	
	T1573: Encrypted Channel	
	T1029: Scheduled Transfer	
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	codefusiontech[.]org, Promoverse[.]org, miniquest[.]org, jerusalemsolutions[.]com
IPv4	162[.]0[.]230[.]185, 209[.]74[.]87[.]100, 143[.]198[.]5[.]41, 209[.]74[.]87[.]67
SHA1	f4e0f4449dc50e33e912403082e093dd8e4bc55d, 3441306816018d08dd03a97ac306fac0200e9152, 9ca11fcbd75420bd7a578e8bf6ef855e7bd0fb8e, 06f3b55f0d66913cd53d2f0e76a5e2d67ff8ed04, 7bd04218276fc8f375c0ce3be43a710f6a2b4d09, 2f5166086da5a57d7e59a767a54ed6fe9a6db444, 8c592d9ab58264e68dfe029ea90f80862c526670, f779a3b1dcc0c3aacacf7ebfa4ed57d53af7e26c, 2993b0ab9786ddc29eb9cf1ace4a28c6e34ea4fb,

TYPE	VALUE
SHA1	e3cc95ca6e271ddf04cd88c85051b2cc9ce04e8e, 270dbaedfbeef9333e0780f3c4e74c01392ce381, d3fa50a9eba93a7fbc79e7ad0c4889d762718a5f, 392a36717fa948f7e00d35711e8598108fbe2f72, 62ed16701a14ce26314f2436d9532fe606c15407, ceb9b7dfb8a36ee8fe223063a6e3f730f2dcefd1, 88cb6169fd7dd21e6d6aa3a8df0a78938e698028, d0d7d0c816753639b5c577aacf14fd2e994b64b0, b55e063607e8f56c9b398b289ba04ddca11398fe, 5c1500296857ed0b0bb7230a1cb17993d25ab69b, f449b95830c584cef72dfb60fb78ee3d6c69ecb4, 3c47eab6ebe5b48097c0099ff18f2a8bc13c12f7, 324918c73b985875d5f974da3471f2a0a4874687, e21564fd0fc3103c1d18b1e1525a0b40e9077d40, feb4318a90057d92ea5ab6420ed6164dd9605013, 0365daf83e37d2c6daaae6c28b4c8343288ef2f9, 777040bed9d26f5da97e8977c6efc0586beae064, f5a129ba4141361ca266950dc4adcb2c548aa949, f77499a8fc6e615e21bf111a88c658ba3d5f0f81, dc785be0c4430bfc5b507255f892bf30134a02b6, e79ccc3f6517c911d6c1df79c94e88896f574e64, 2eea39dbe11889e5713cbca020f7ede653bc48ec, 975c763e050d0a9a46f0aafdde66d3e7f0626c5b, d97d21536c061e7a7151a453242d36f3ab196a14, 56380a652471962387693f4bcc893fd21f0fc324, 9defffba933fc44f8e3b6e25b31508bc17d29077, efb18cf7cf227037e034c0b525f502e642815f94, 0588cf26b6e9210f86a266ac0366af1fd29f135c, 80cea18e19665c5a57e7b9ca0bf36aad06096e93, 7d3757d5165e2e95b0b89e33316025a4b9301e2d, ac982b7b46e085e0bb51cba2edb61bff5910b6a8, 8632b62fa14fd679fa97cfe50e6c25696b846129, ea80deaed00c8b71aa0033b00fe0ef5b63840b99, 92e2f826804d762679b13283102f3560078eb4cb

References

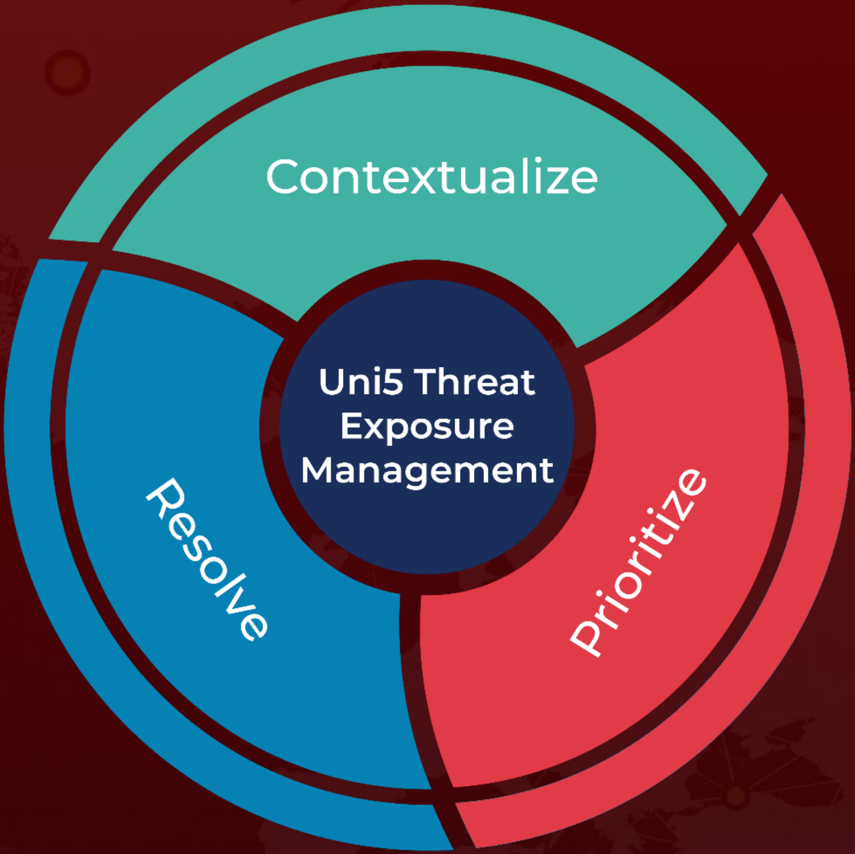
https://www.group-ib.com/blog/muddywater-operation-olalampo/

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

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

February 25, 2026 • 4:00 AM

More at www.hivepro.com