Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

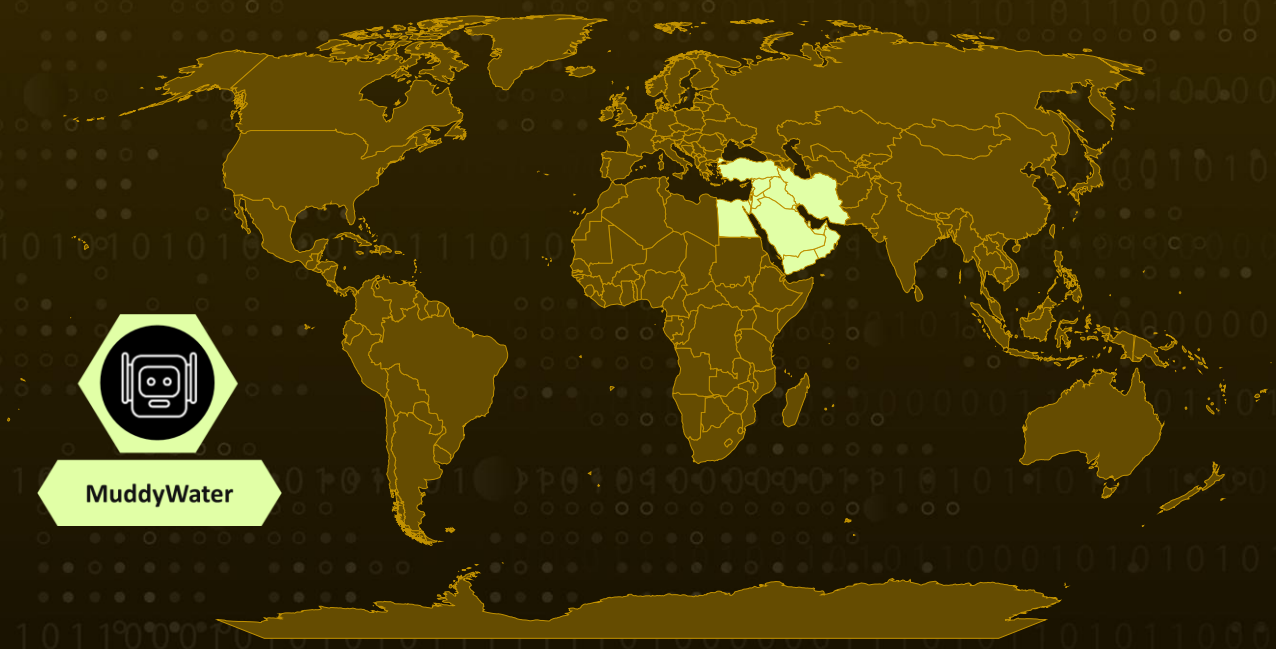
MuddyWater’s Rust Implants Target the Middle East

Date of Publication	Admiralty Code	TA Number
January 12, 2026	A1	TA2026010

Summary

First Seen: 2025
Targeted Region: Middle East
Targeted Industries: Diplomatic, Maritime, Financial, and Telecom Entities
Malware: RustyWater
Actor: MuddyWater (aka Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Mango Sandstorm, Boggy Serpens, Yellow Nix, G0069)
Attack: A recently identified spear-phishing campaign attributed to the MuddyWater APT group targeting multiple sectors across the Middle East. The campaign employs icon spoofing and malicious Microsoft Word documents containing VBA macros to deliver RustyWater, a Rust-based remote access implant. This represents a significant tooling evolution for MuddyWater, historically reliant on PowerShell and VBS loaders. The implant features asynchronous C2 communication, anti-analysis capabilities, registry persistence, and modular post-compromise capability expansion. The threat actor leveraged compromised legitimate email accounts from organizations, including TMCell (Turkmenistan's primary mobile operator) and government entities, to send spear-phishing emails masquerading as cybersecurity guidelines.

Attack Regions



Attack Details

#1 A recently uncovered spear-phishing campaign attributed to the MuddyWater APT group highlights a clear evolution in the actor's tooling and tradecraft. The operation targets a broad range of organizations across the Middle East, including diplomatic missions, maritime operators, financial institutions, and telecommunications providers. Unlike MuddyWater's earlier campaigns that leaned heavily on PowerShell and VBS loaders, this activity introduces Rust-based implants with more mature remote access Trojan (RAT) capabilities. These implants support asynchronous command-and-control, anti-analysis safeguards, registry-based persistence, and modular post-compromise functionality, signaling a deliberate shift toward stealthier and more resilient malware.

#2 The attack chain begins with a carefully crafted spear-phishing email titled "Cybersecurity Guidelines," sent from the legitimate domain of TMCell (Altyn Asyr CJSC). The message includes a malicious attachment, Cybersecurity.doc, which serves as the entry point for the infection. By leveraging a trusted sender and a thematically relevant lure, the attackers increase the likelihood of user interaction, allowing the document to act as the foundation for subsequent exploitation stages.

#3 Analysis of the weaponized document reveals embedded VBA macros designed to conceal their true purpose. A hex-encoded payload is hidden within the document and reconstructed using the WriteHexToFile function, which strips formatting and writes the resulting file as CertificationKit.ini to the ProgramData directory. An obfuscated execution wrapper, dynamically builds a WScript.Shell object and invokes cmd.exe to execute the dropped file. The payload's legitimacy is superficially reinforced by a valid PE header, masking its malicious nature during initial inspection.

#4 Once executed, CertificationKit.ini masquerades as a benign executable but ultimately deploys a Rust-based malware family linked to MuddyWater, referred to here as RustyWater. This implant incorporates multiple defensive features, including anti-debugging and anti-tampering checks, while harvesting key system details such as user identity, host name, and domain information. Critical strings and operational paths are obfuscated through position-independent XOR encryption, complicating static analysis and hindering detection efforts.

#5 RustyWater demonstrates a strong focus on evasion and operational longevity. It scans for more than two dozen antivirus and EDR products, attempts persistence through Windows startup registry keys, and maintains encrypted communications with its command-and-control servers using Rust's reqwest and tokio frameworks. Data is protected through layered encoding and encryption, while randomized sleep intervals and asynchronous execution reduce behavioral patterns. The malware also employs classic yet effective techniques such as process injection into explorer.exe, ensuring in-memory execution and minimizing its on-disk footprint. Collectively, these characteristics align closely with MuddyWater's known tactics and reinforce attribution, especially given the reuse of distinctive VBA macro patterns and the targeting of government, financial, educational, and maritime entities across the Middle East.

Recommendations

- **Strengthen Email Awareness and Handling:** Train employees to treat unexpected emails with caution, even when they appear to come from trusted or official domains. Users should be encouraged to verify the sender through a secondary channel before opening attachments, especially documents related to policies, guidelines, or security updates.
- **Monitor Network Traffic And C2 Behavior:** Implement network monitoring to detect irregular outbound connections, long sleep intervals, and encrypted traffic to unfamiliar servers. Pay close attention to systems that repeatedly attempt to communicate with external infrastructure, as this may indicate command-and-control activity.
- **Limit Impact Through Access Control and Patching:** Apply the principle of least privilege to user accounts so that a single compromised user cannot lead to widespread access. Regularly patch operating systems and applications, and review startup registry entries to identify and remove unauthorized persistence mechanisms.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	T1566 Phishing	T1566.001 Spearphishing Attachment
T1204 User Execution	T1204.002 Malicious File	T1059 Command and Scripting Interpreter	T1059.005 Visual Basic
T1106 Native API	T1047 Windows Management Instrumentation	T1620 Reflective Code Loading	T1547 Boot or Logon Autostart Execution

T1547.001 Registry Run Keys / Startup Folder	**T1027** Obfuscated Files or Information	**T1036** Masquerading	**T1055** Process Injection
T1082 System Information Discovery	**T1518** Software Discovery	**T1518.001** Security Software Discovery	**T1071** Application Layer Protocol
T1071.001 Web Protocols	**T1573** Encrypted Channel	**T1140** Deobfuscate/Decode Files or Information	**T1083** File and Directory Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	76aad2a7fa2657785203984113245 22c57bfd7d2ff30a5cfe6460960491bc552, f38a56b8dc0e8a581999621eef65ef497f0ac0d35e953bd94335926f00e9464f, 7523e53c979692f9eecff6ec760ac3df5b47f172114286e570b6bba3b2133f58, e61b2ed360052a256b3c8761f09d185dad15c67595599da3e587c2c553e83108, a2001892410e9f34ff0d02c8bc9e7c53b0bd10da58461e1e9eab26bdbf410c79, c23bac59d70661bb9a99573cf098d668e9395a636dc6f6c20f92c41013c30be8, 42ad0c70e997a268286654b792c7833fd7c6a2a6a80d9f30d3f462518036d04c, e081bc408f73158c7338823f01455e4f5185a4365c8aad1d60d777e29166abbd, 3d1e43682c4d306e41127ca91993c7befd6db626ddbe3c1ee4b2cf44c0d2fb43, ddc6e6c76ac325d89799a50dffd11ec69ed3b5341740619b8e595b8068220914
IPv4	159[.]198[.]68[.]25, 161[.]35[.]228[.]250, 159[.]198[.]66[.]153

References

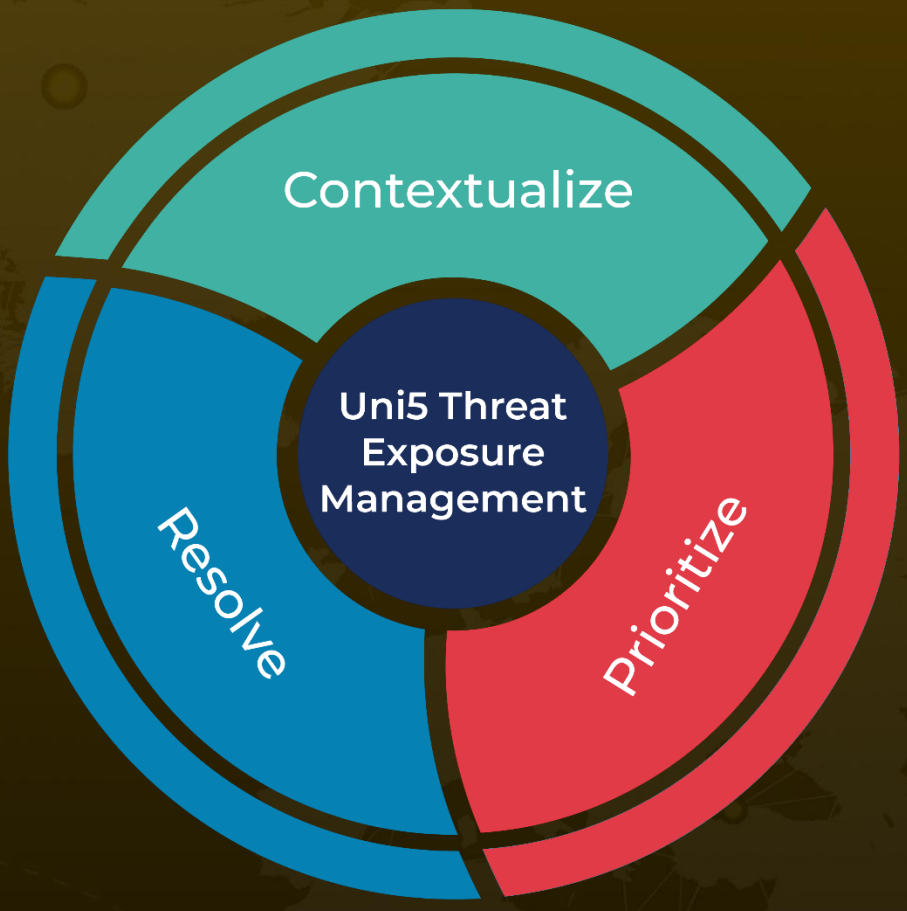
https://www.cloudsek.com/blog/reborn-in-rust-muddywater-evolves-tooling-with-rustywater-implant

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

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

January 12, 2026 • 8:00 AM

More at www.hivepro.com