Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

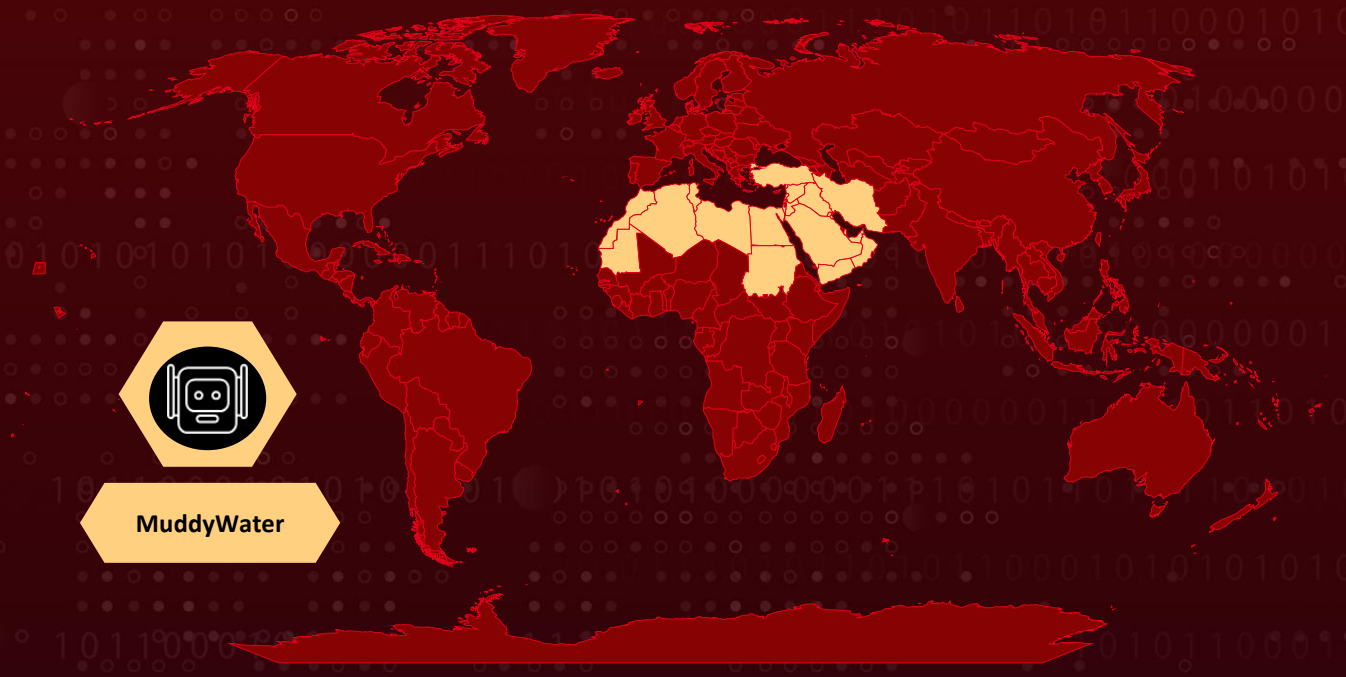
MuddyWater Deploys Phoenix Backdoor in Targeted Espionage Campaign

Date of Publication	Admiralty Code	TA Number
October 23, 2025	A1	TA2025322

Summary

First Seen: August 17, 2025
Targeted Region: Middle East and North Africa (MENA)
Targeted Platform: Windows
Malware: Phoenix Backdoor v4, FakeUpdate Loader, Chromium_Stealer
Targeted Industries: Government, Diplomatic, Foreign Affairs Ministries and Consulates, Telecommunications, International Organizations
Threat Actor: MuddyWater (aka Seedworm, TEMP.Zagros, Static Kitten, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17, Mango Sandstorm, Boggy Serpens, Yellow Nix)
Attack: MuddyWater, an Iran-linked APT group, launched a phishing campaign targeting over 100 government and critical infrastructure across the Middle East and North Africa. Using compromised emails and malicious Word files, it deployed the Phoenix backdoor and other tools for espionage. By blending custom malware with legitimate RMM utilities, the group enhanced stealth and persistence, underscoring the need for stronger email and endpoint defenses.

Attack Regions



Attack Details

#1

MuddyWater, an Iranian-aligned Advanced Persistent Threat (APT) group linked to Iran's Ministry of Intelligence and Security (MOIS), has recently executed a sophisticated cyber-espionage campaign targeting over 100 organizations, primarily in the Middle East and North Africa (MENA) region. Their targets include embassies, diplomatic missions, foreign ministries, international organizations, and critical infrastructure entities. The campaign is focused on intelligence collection rather than disruption, reflecting the group's strategic espionage objectives.

#2

The attack begins with highly convincing phishing emails sent from a compromised mailbox accessed via NordVPN, increasing trust and bypassing conventional email defenses. Emails include Microsoft Word attachments that prompt recipients to enable macros. When enabled, embedded Visual Basic for Applications (VBA) code executes, initiating the first stage of the infection chain.

#3

The infection proceeds through a multi-stage payload deployment. The VBA macro installs a custom loader, FakeUpdate, which decrypts and injects the second-stage payload into its process. This final payload is the Phoenix backdoor version 4, which establishes persistence, registers the host with a Command-and-Control (C2) server, and continuously beacon for remote commands. This enables ongoing data collection, credential harvesting, and post-exploitation operations.

#4

In addition to Phoenix, MuddyWater deploys a custom credential-stealing tool, Chromium_Stealer, disguised as a benign application to exfiltrate login credentials from popular browsers such as Chrome, Edge, Opera, and Brave. The group also integrates commercial Remote Monitoring and Management (RMM) tools, including PDQ RMM and Action1, blending legitimate software with custom malware to enhance stealth, maintain persistent access, and complicate detection and forensic analysis.

#5

Since at least 2017, MuddyWater has evolved its tradecraft, using spear-phishing, exploitation of Microsoft Exchange and SharePoint, and living-off-the-land techniques. Organizations should disable macros, deploy EDR, monitor networks, and block known C2s like screenai[.]online. Threat intelligence sharing and preparedness are essential to mitigate this persistent state-sponsored threat.

Recommendations

Disable Macros by Default: Configure Microsoft Office to disable macros by default to prevent execution of malicious scripts. Only allow macros from trusted and verified sources to minimize risk. Educate users on the dangers of enabling macros in unsolicited emails.

Deploy Endpoint Detection and Response (EDR): Use advanced EDR solutions capable of detecting abnormal script executions and unauthorized registry changes. Monitor for known malware behaviors, including Phoenix backdoor and Chromium_Stealer activity. Ensure centralized logging for efficient detection and incident response.

Conduct Phishing Awareness Training: Regularly train employees to identify sophisticated spear-phishing attempts and suspicious attachments or links. Emphasize verifying sender legitimacy before opening embedded content. Simulated phishing exercises can reinforce learning and improve vigilance.

Enforce Multi-Factor Authentication (MFA): Require MFA on all critical access points including VPN, remote management tools, and cloud services. This limits unauthorized access even if credentials are compromised. Regularly review permissions and revoke unnecessary or outdated access rights.

Browser Credential Defense: Implement a policy to prohibit saving corporate credentials in web browsers to nullify the effectiveness of the custom Chromium_Stealer tool.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0007 Discovery
TA0005 Defense Evasion	TA0040 Impact	TA0010 Exfiltration	TA0009 Collection

TA0006 Credential Access	T1566.001 Spearphishing Attachment	T1566 Phishing	T1204 User Execution
T1059.003 Windows Command Shell	T1059 Command and Scripting Interpreter	T1547.001 Registry Run Keys / Startup Folder	T1204.002 Malicious File
T1547 Boot or Logon Autostart Execution	T1219 Remote Access Software	T1027 Obfuscated Files or Information	T1586 Compromise Accounts
T1564.001 Hidden Files and Directories	T1564 Hide Artifacts	T1555 Credentials from Password Stores	T1082 System Information Discovery
T1071.001 Web Protocols	T1071 Application Layer Protocol	T1555.003 Credentials from Web Browsers	T1090.002 External Proxy
T1090 Proxy	T1041 Exfiltration Over C2 Channel	T1565 Data Manipulation	T1059.005 Visual Basic
T1059.001 PowerShell	T1547.004 Winlogon Helper DLL	T1546.015 Component Object Model Hijacking	T1546 Event Triggered Execution
T1055 Process Injection	T1055.002 Portable Executable Injection	T1140 Deobfuscate/Decode Files or Information	T1027.007 Dynamic API Resolution
T1027.009 Embedded Payloads	T1112 Modify Registry	T1027.002 Software Packing	T1105 Ingress Tool Transfer

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	668dd5b6fb06fe30a98dd59dd802258b45394ccd7cd610f0aaab43d801bf1a1e,

TYPE	VALUE
SHA256	5ec5a2adaa82a983fcc42ed9f720f4e894652bd7bd1f366826a16ac98bb91839, 1883db6de22d98ed00f8719b11de5bf1d02fc206b89fedd6dd0df0e8d40c4c56, 3ac8283916547c50501eed8e7c3a77f0ae8b009c7b72275be8726a5b6ae255e3, 76fa8dca768b64aefedd85f7d0a33c2693b94bdb55f40ced7830561e48e39c75, 3d6f69cc0330b302ddf4701bbc956b8fca683d1c1b3146768dcbce4a1a3932ca
IPv4	159[.]198[.]36[.]115
Domain	screenai[.]online

References

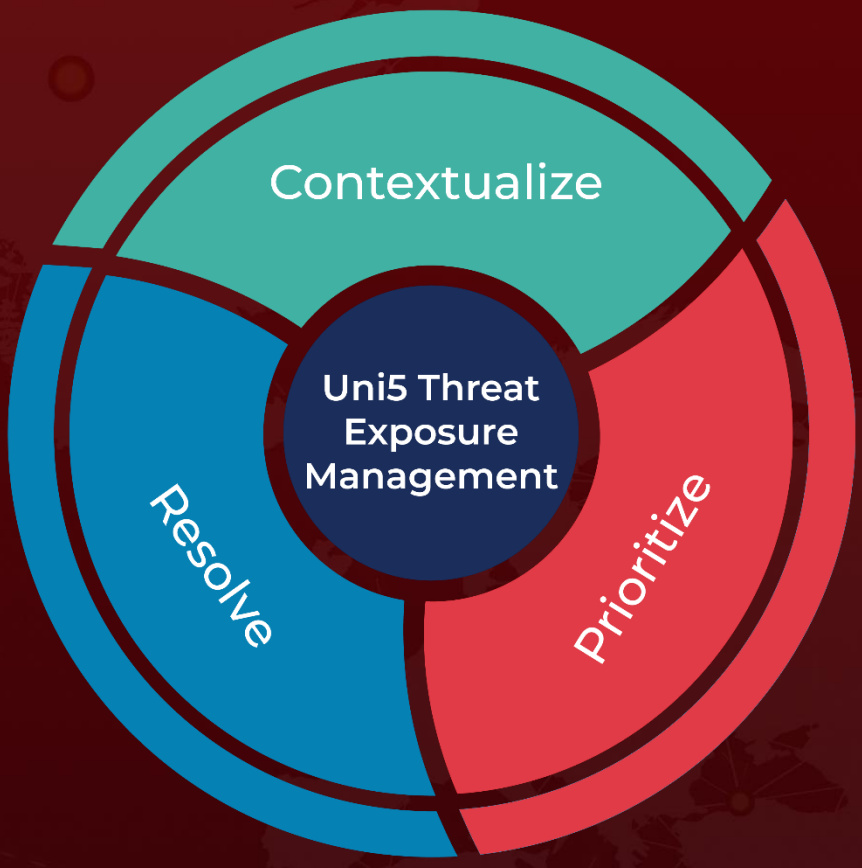
https://www.group-ib.com/blog/muddywater-espionage/

https://hivepro.com/threat-advisory/muddywater-expands-its-arsenal-with-bugsleep-malware/

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

October 23, 2025 . 9:30 PM

More at www.hivepro.com