Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

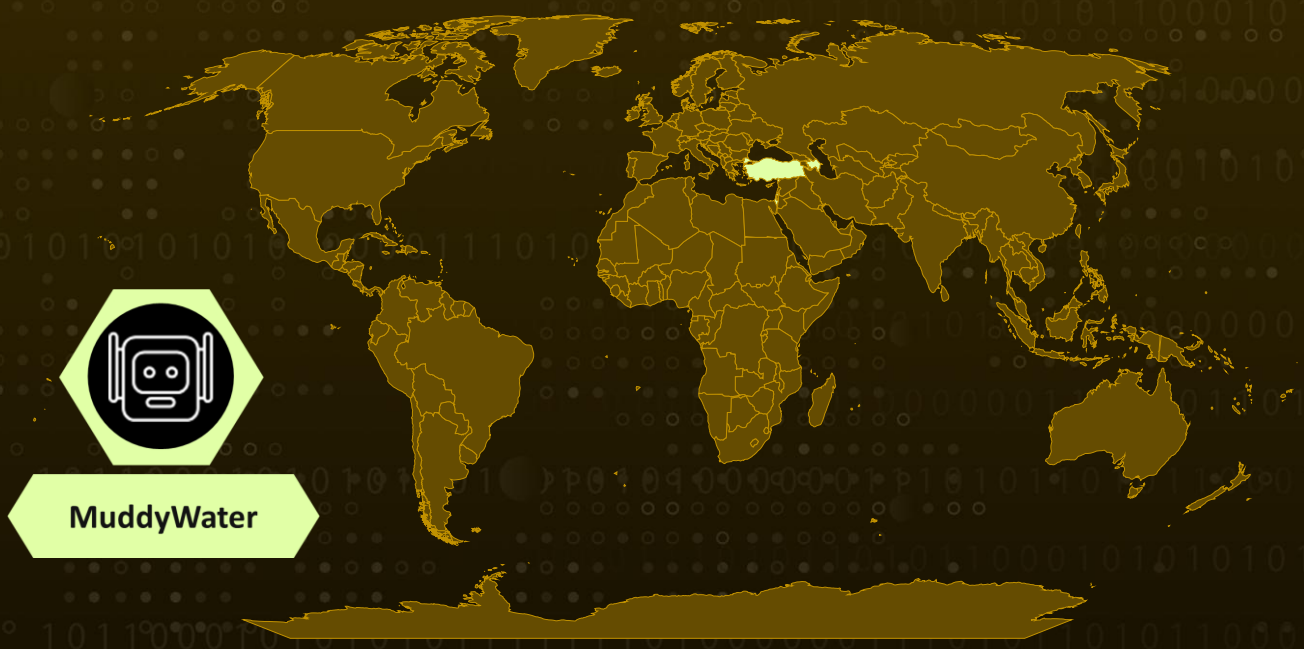
Echoes Over UDP: MuddyWater's Covert Backdoor Strikes

Date of Publication	Admiralty Code	TA Number
December 9, 2025	A1	TA2025373

Summary

Attack Discovered: 2025
Targeted Countries: Turkey, Israel, Azerbaijan
Affected Platforms: Microsoft Windows
Malware: UDPGangster
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: UDPGangster is a stealthy UDP-based backdoor used in MuddyWater's latest espionage campaigns, distributed through convincing phishing emails and malicious Word documents that trick users into enabling macros. Once activated, it quietly deploys itself, evades virtual analysis, and gathers system details while hiding behind distraction images and layered obfuscation. The malware establishes persistence, communicates with its C2 server over UDP, and supports commands for file theft, remote execution, and payload delivery. Linked campaigns targeting Turkey, Israel, and Azerbaijan share infrastructure, decoys, and code patterns, painting a clear picture of a coordinated operation. Overall, the campaign blends social engineering, anti-analysis techniques, and custom tooling to infiltrate regional targets with precision and stealth.

Attack Regions



Attack Details

#1 UDPGangster is a UDP-based backdoor tied to the MuddyWater threat group. This malware gives attackers quiet but powerful control over compromised machines, letting them run remote commands, steal files, and deploy additional payloads, all while blending into network traffic through UDP channels that often slip past conventional defenses. Recently, multiple campaigns distributing UDPGangster through malicious Microsoft Word documents laced with VBA macros were uncovered. These operations have primarily targeted users in Turkey, Israel, and Azerbaijan.

#2 The phishing email at the center of this activity imitates an official communication from the Turkish Republic of Northern Cyprus Ministry of Foreign Affairs. Written in formal Turkish and crafted to resemble legitimate government correspondence, it invites recipients to an online seminar. Attached to the message are two files, seminar.doc and seminar.zip, both intended to lure victims into enabling malicious macro content. The ZIP archive contains the same document as the standalone Word file, and once opened, it prompts users to "Enable Content," a classic social engineering tactic used to trigger hidden malicious code embedded in the document.

#3 Once macros are enabled, the VBA script embedded in the document acts as a dropper. Through the Document_Open() event, it decodes Base64 content stored in a concealed form field and writes the resulting output to C:\Users\Public\ui.txt. The malware then uses the CreateProcessA API to run this file, activating the UDPGangster payload. The script also includes a subroutine called SmartToggle(), which flips between two overlay images to distract the user with harmless-looking content while malicious operations execute in the background. Interestingly, despite the email's Turkish theme, the displayed decoy image referenced internet outages in Israel, an odd mismatch that hints at broader targeting beyond the immediate phishing audience.

#4 Once deployed, UDPGangster establishes persistence by copying itself to the %AppData%\RoamingLow directory as SystemProc.exe and adding its path to a registry key, ensuring it runs at startup. It creates a mutex to avoid multiple instances and then launches a series of anti-analysis checks. These routines inspect CPU cores, RAM size, MAC address prefixes, workgroup configuration, disk and baseboard hardware identifiers, registry signatures, and even filenames, each meant to detect virtualization or sandbox environments. If the system passes these checks, the malware collects host details such as computer name, OS version, username, and domain/workgroup information. This data is encoded using an ROR transformation and sent to its command-and-control server at UDP port 1269.

#5 Further investigation connected this phishing activity to additional documents used in campaigns against Israel and Azerbaijan, which shared infrastructure, mutex values, and PDB paths with the Turkish lure. One of the associated IP addresses also appeared in previous attacks involving the Phoenix Backdoor, reinforcing the link to MuddyWater. More recently, we observed the actor targeting Israel and Egypt to deliver another custom backdoor known as MuddyViper.

Recommendations

- **Be Suspicious of Unexpected Documents:** If an email you weren't expecting asks you to open a file, especially a Word document, and "Enable Content," treat it as a red flag. Most legitimate organizations don't require macros to open simple documents.
- **Turn Off Macros Unless Absolutely Needed:** Macros are one of the most common entry points for malware like UDPGangster. Keep them disabled by default, and only enable them for trusted, verified files.
- **Use Strong Email Filtering:** Invest in email security tools that can spot spoofed addresses, malicious attachments, and phishing wording. Stopping these emails before they reach inboxes makes a huge difference.
- **Monitor Unusual Network Traffic:** Since UDPGangster communicates over UDP to its C2 server, keep an eye on unusual outbound UDP traffic. Alerts on strange IPs or non-standard ports can catch hidden backdoors early.
- **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	**TA0010** Exfiltration	**TA0011** Command and Control	**T1566** Phishing
T1566.001 Spearphishing Attachment	**T1059** Command and Scripting Interpreter	**T1059.003** Windows Command Shell	**T1204** User Execution
T1204.002 Malicious File	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1497** Virtualization/Sandbox Evasion

T1027 Obfuscated Files or Information	**T1036** Masquerading	**T1082** System Information Discovery	**T1033** System Owner/User Discovery
T1095 Non-Application Layer Protocol	**T1105** Ingress Tool Transfer	**T1005** Data from Local System	**T1041** Exfiltration Over C2 Channel
T1083 File and Directory Discovery			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	157[.]20[.]182[.]75, 64[.]7[.]198[.]12
URL	hxxps[:]//reminders[.]trahum[.]org/Scheduled_Internet_Outages[.]doc
SHA256	d177cf65a17bffcd152c5397600950fc0f81f00990ab8a43d352f9a7238428a1, 3d3fbd586f61043ff04ab0369b913a161c0159425fb269d52b7d8d8a14838ece, 232e979493da5329012022d3121300a4b00f813d5b0ecc98fdc3278d8f4e5a48, e84a5878ea14aa7e2c39d04ea7259d7a4ed7f666c67453a93b28358ccce57bc5, fc4a7eed5cb18c52265622ac39a5cef31eec101c898b4016874458d2722ec430, 44deab99e22340fc654494cc4af2b2c27ef1942c6fea6eace9fb94ce7855c0ca, 13d36f3011ed372ad4ec4ace41a6dee52361f221161192cb49c08974c86d160e, b7276cad88103bdb3666025cf9e206b9fb3e66a6d934b66923150d7f23573b60, b552e1ca3482ad4b37b1a50717ac577e1961d0be368b49fa1e4e462761ae6eeb, bca7d23b072a2799d124977fdb8384325b30bb1d731741d84a1dfc5e3cf6ac26, 01b1073cb0480af3bde735f559898774e1a563e06f9fe56ec3845ea960da0f3c, 7ea4b307e84c8b32c0220eca13155a4cf66617241f96b8af26ce2db8115e3d53

References

https://www.fortinet.com/blog/threat-research/udpgangster-campaigns-target-multiple-countries

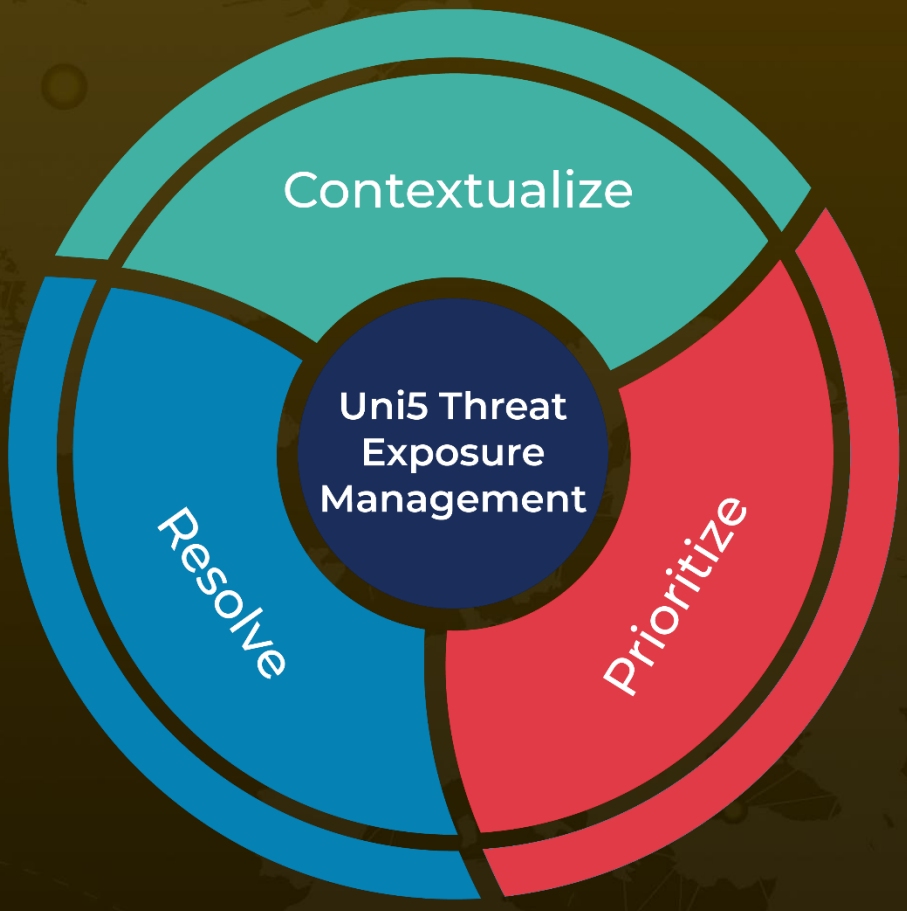
https://hivepro.com/threat-advisory/muddywater-deploys-phoenix-backdoor-in-targeted-espionage-campaign/

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

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

December 9, 2025 • 9:00 AM

More at www.hivepro.com