مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

MuddyWater's New Malware Toolkit Driving International Espionage

Tracking #:432317850

Date:23-10-2025

TLP: WHITE

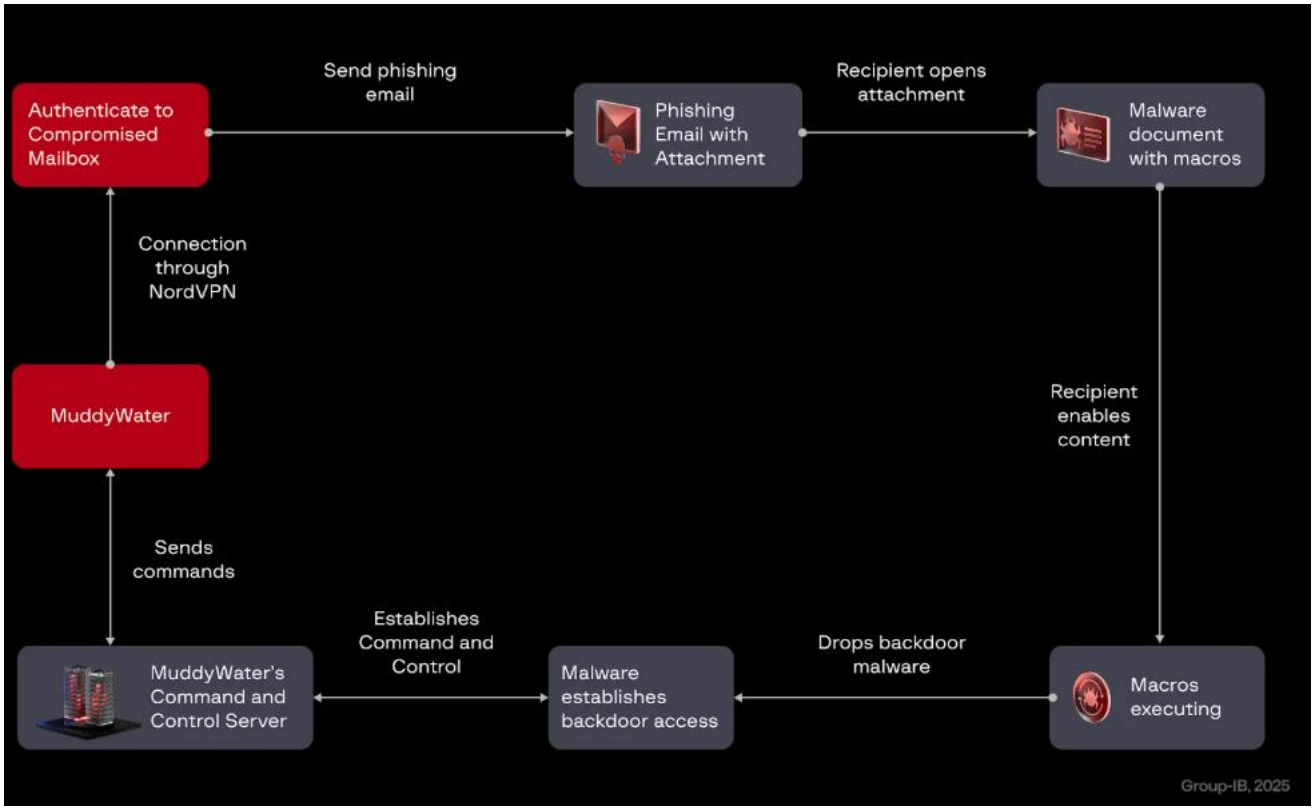
EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that security researchers have identified a highly targeted espionage campaign attributed to MuddyWater (also known as Seedworm, APT34) Advanced Persistent Threat (APT) group.

TECHNICAL DETAILS:

Security researchers has identified a highly targeted espionage campaign attributed to MuddyWater (also known as Seedworm, APT34) Advanced Persistent Threat (APT) group. The campaign targeted across the whole Middle East and North Africa region, targeting more than 100 government entities.

The campaign leverages compromised legitimate mailboxes and abused VPN services (NordVPN) to distribute malicious Microsoft Word attachments that deploy Phoenix Backdoor version 4 via the FakeUpdate injector.



Overview of the execution killchain

Threat Element	Details
Actor	MuddyWater APT
Motivation	Cyber espionage and intelligence gathering
Infection Vector	Phishing emails sent from compromised legitimate mailboxes
Primary Payload	Phoenix Backdoor v4 (delivered via FakeUpdate injector)
Secondary Tools	Action1, PDQ RMM, Chromium_Stealer
Persistence Mechanisms	Winlogon registry modification, COM-based persistence DLL
C2 Domain	screenai[.]online

C2 Real IP	159[.]198[.]36[.]115 (NameCheap ASN)
Malware Families Observed	Phoenix v4, FakeUpdate, Mononoke.exe, coreglobconfig.dll
Target Geography	Middle East, North Africa, Europe, North America
Notable Tactics	Abuse of NordVPN, use of legitimate RMM tools, credential theft from Chromium-based browsers

Indicators of Compromise (IOCs):

Backdoor	mononoke.exe	668dd5b6fb06fe30a98dd59dd802258b45394ccd7cd610f0aaab43d801bf1a1e
Backdoor	mononoke.exe	5ec5a2adaa82a983fcc42ed9f720f4e894652bd7bd1f366826a16ac98bb91839
Backdoor	sysProcUpdate	1883db6de22d98ed00f8719b11de5bf1d02fc206b89fedd6dd0df0e8d40c4c56
Backdoor	sysProcUpdate	3ac8283916547c50501eed8e7c3a77f0ae8b009c7b72275be8726a5b6ae255e3
Backdoor	sysProcUpdate	76fa8dca768b64aefedd85f7d0a33c2693b94bdb55f40ced7830561e48e39c75
Backdoor	sysProcUpdate	3d6f69cc0330b302ddf4701bbc956b8fca683d1c1b3146768dcbce4a1a3932ca
C2 Domain	Creation date 2025-08-17	screenai[.]online
C2 IP	real IP address behind CloudFlare	159[.]198[.]36[.]115

RECOMMENDATIONS:

1. Strengthen Threat Intelligence and Monitoring

- Integrate IOCs and YARA rules related to Phoenix, FakeUpdate, and screenai[.]online into SIEM and EDR platforms.
- Continuously hunt for registry modifications involving Winlogon and anomalous COM object registrations.
- Subscribe to Threat Intelligence feeds for updated TTPs on MuddyWater.

2. Enhance Email Security

- Enforce attachment sandboxing and macro scanning for Office files.
- Block or quarantine emails with external macros or unexpected attachments.
- Conduct phishing simulation exercises and reinforce user awareness around "Enable Content" prompts.

3. Harden Endpoints and Access

- Disable Office macros by default via Group Policy; permit only digitally signed macros.
- Deploy and monitor EDR/XDR solutions for process injection and PowerShell-based activity.
- Enforce Multi-Factor Authentication (MFA) for all accounts, particularly administrative and email access.

4. Network and Infrastructure Protection

- Monitor outbound HTTP(S) traffic for patterns matching MuddyWater's C2 beacons.
- Restrict or whitelist use of RMM tools (Action1, PDQ, ScreenConnect).
- Implement DNS filtering and block known malicious domains.

5. Strategic and Operational Defense

- Maintain asset visibility and apply least-privilege principles.
- Use behavioral analytics to detect abnormal login behavior, especially from VPN or foreign IPs.
- Review and test incident response playbooks for phishing and credential theft scenarios.
- Conduct periodic malware simulations to test detection and containment capabilities.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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