مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

UDPGangster Campaign Targeting Middle East Countries

Tracking #:432318104
Date:08-12-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Security researchers identified an ongoing campaign distributing the UDPGangster (HORSESHOE) backdoor, attributed to the MuddyWater threat group (aka Static Kitten, TA450).

TECHNICAL DETAILS:

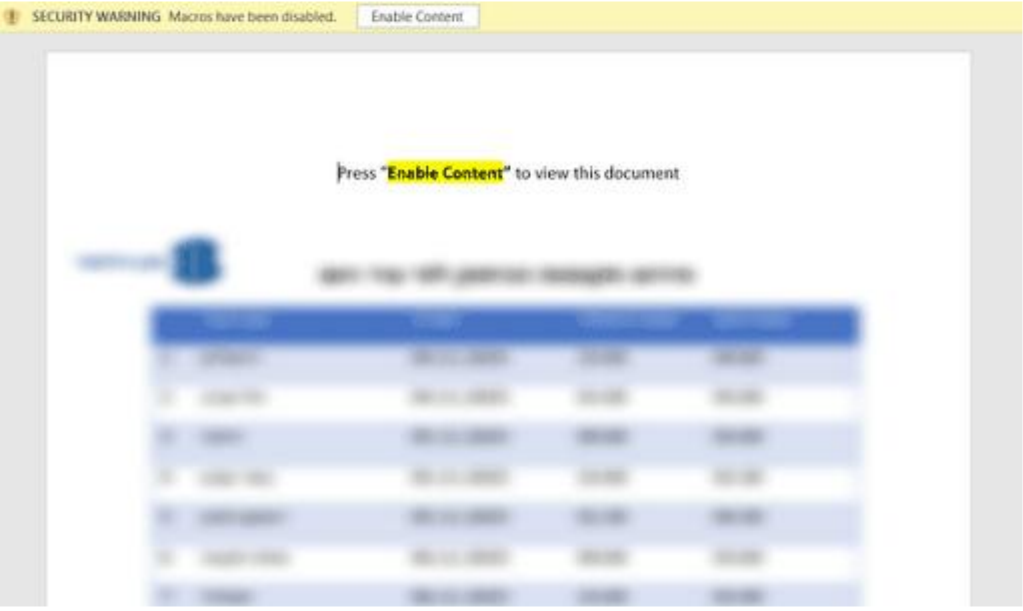
Security researchers identified an ongoing campaign distributing the UDPGangster (HORSESHOE) backdoor, attributed to the MuddyWater threat group (aka Static Kitten, TA450). Across all reporting, MuddyWater consistently used malicious Microsoft Word documents embedded with VBA macros as the initial infection vector. These phishing emails impersonated legitimate government entities and employed decoy content—such as seminar invitations and outage schedules—to trick victims into enabling macros. Once activated, the malware installs the UDPGangster backdoor, providing remote command execution, file exfiltration, and the ability to deploy additional payloads.

TECHNICAL ANALYSIS

All intelligence indicates these incidents represent multiple clusters within a single MuddyWater campaign. Tactics, techniques, and procedures (TTPs) remained consistent:

Initial Infection

- Delivery via phishing emails spoofing government ministries.
- Attachments such as seminer.doc/seminer.zip contained VBA-based droppers.
- Macros used Document_Open() to decode a Base64 payload from hidden form data and drop it to C:\Users\Public\ui.txt.



SECURITY WARNING Macros have been disabled. Enable Content

Press "Enable Content" to view this document

Document with VBA script

Behavior of UDPGangster

Once executed, UDPGangster:

- Establishes persistence by installing itself as SystemProc.exe under

%AppData%\RoamingLow and modifying:
  - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell
- Creates a mutex: xhxhxhxhxhxpp
- Communicates via UDP port 1269 with C2 servers
- Supports operational commands including:
  - Heartbeats
  - Remote cmd.exe execution
  - File exfiltration
  - Deployment of follow-on malware
  - Updating the C2 address

Anti-Analysis Capabilities

UDPGangster employs extensive evasion techniques:

- Debugger checks
- CPU core count and memory size checks
- VM detection via MAC prefixes, WMI hardware checks, and driver/service enumeration
- Sandbox/analysis tool detection (dll scanning, filename checks)
- Registry-based virtualization checks (16+ system paths)

Infrastructure & Campaign Linkage

- Decoy themes and code artifacts (e.g., mutexes, PDB paths) align closely across samples.
- Telemetry links UDPGangster with MuddyWater's Phoenix Backdoor, confirming shared operators.

INDICATORS OF COMPROMISE:

Domain
157.20.182[.]75 64.7.198[.]12
URL
hxxps://reminders[.]trahum[.]org/Scheduled_Internet_Outages.doc
Email
d177cf65a17bffcd152c5397600950fc0f81f00990ab8a43d352f9a7238428a1 3d3fbd586f61043ff04ab0369b913a161c0159425fb269d52b7d8d8a14838ece 232e979493da5329012022d3121300a4b00f813d5b0ecc98fdc3278d8f4e5a48 e84a5878ea14aa7e2c39d04ea7259d7a4ed7f666c67453a93b28358ccce57bc5 fc4a7eed5cb18c52265622ac39a5cef31eec101c898b4016874458d2722ec430 44deab99e22340fc654494cc4af2b2c27ef1942c6fea6eace9fb94ce7855c0ca 13d36f3011ed372ad4ec4ace41a6dee52361f221161192cb49c08974c86d160e b7276cad88103bdb3666025cf9e206b9fb3e66a6d934b66923150d7f23573b60 b552e1ca3482ad4b37b1a50717ac577e1961d0be368b49fa1e4e462761ae6eeb bca7d23b072a2799d124977fdb8384325b30bb1d731741d84a1dfc5e3cf6ac26 01b1073cb0480af3bde735f559898774e1a563e06f9fe56ec3845ea960da0f3c
Document
7ea4b307e84c8b32c0220eca13155a4cf66617241f96b8af26ce2db8115e3d53

RECOMMENDATIONS:

- Block macros from untrusted documents.
- Enforce advanced email filtering.

- Monitor for UDP traffic on port 1269.
- Implement behavioral EDR with antitamper protection.
- Conduct threat hunting for related registry keys, mutex presence, and suspicious VBA activity

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