Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

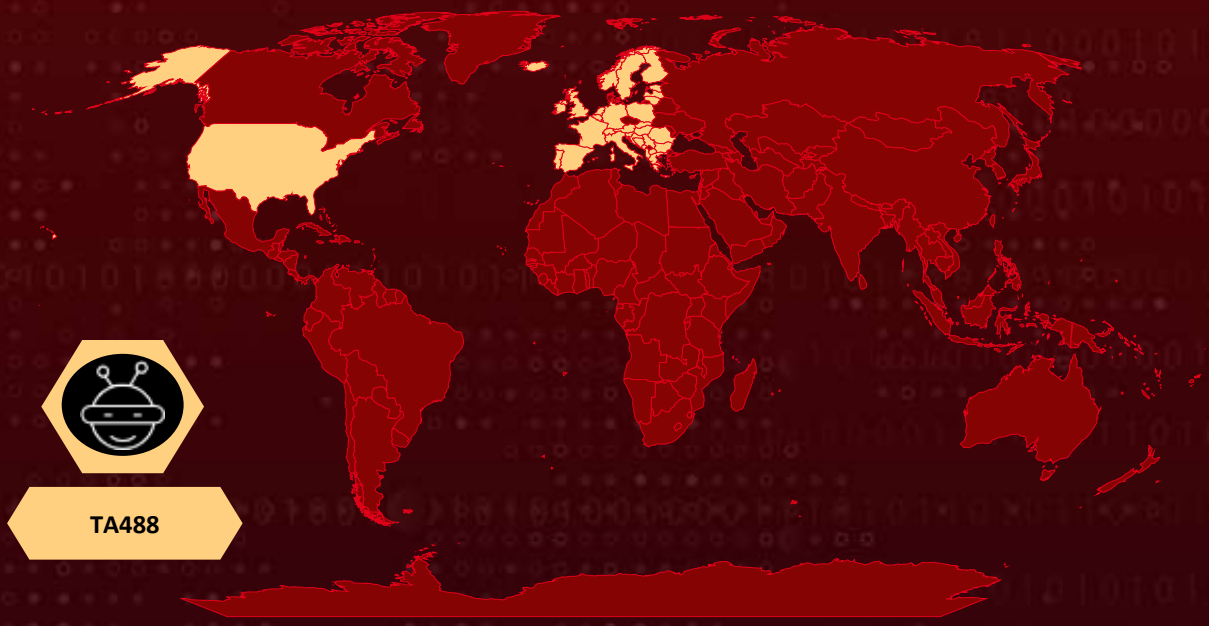
TA488 Unleashes OWAReaper: A Half-Click Backdoor for Outlook Web Access

Date of Publication	Admiralty Code	TA Number
July 30, 2026	A1	TA2026216

Summary

First Seen: March 2026 (earliest infrastructure); campaign activity from July 22, 2026
Targeted Regions: United States and Europe
Targeted Platforms: Microsoft Exchange Server (Outlook Web Access)
Targeted Industries: Government, Telecommunications, Financial, Hospitality, Aerospace
Threat Actor: TA488 (aka Void Blizzard, Laundry Bear)
Malware: OWAReaper
Attack: TA488 ran a broad email campaign that exploits CVE-2026-42897, a cross-site scripting flaw in Outlook Web Access. Merely opening a booby-trapped email in OWA runs attacker JavaScript that deploys OWAReaper, a browser-based backdoor with no host footprint. OWAReaper harvests saved credentials and OAuth tokens, quietly grants itself server-side mailbox permissions, and hides persistence inside the browser's own storage, letting the actor keep reading a victim's mail even after passwords are rotated or the device is fully re-imaged.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-42897	Microsoft Exchange Server Cross-Site Scripting Vulnerability	Microsoft Exchange Server	✓	✓	✓

Attack Details

#1

TA488 opened the campaign on July 22, 2026, sending a high volume of emails from a series of compromised accounts to organizations across the government, telecommunications, financial, hospitality, and aerospace sectors in the United States and Europe. The goal was for a recipient to open and skim the message, then dismiss it as junk without reporting it. The email body itself is the weapon: it exploits CVE-2026-42897, a flaw in which the Exchange server fails to sanitize HTML in the message body properly. A small JavaScript loader uses an onload event handler to parse the rest of the body, reassemble a Base64 fragment hidden in social-media icon URLs after a "#" character, and execute it. Because opening the email in OWA is enough to trigger everything, this is classified as a "half-click" exploit.

#2

Execution happens entirely inside the OWA reading pane. Once the decoded payload runs, it deploys OWAReaper, a JavaScript implant that is an evolution of the actor's earlier ZimReaper malware. OWAReaper immediately uses Outlook APIs to rewrite the malicious email on the Exchange server and strip out the exploit content, while disabling OWA pop-ups and right-click functionality so its activity is harder to notice. It generates a per-target session key and collects the account's email address, username, and Outlook settings. For persistence, it writes an encrypted copy of itself and a decryption wrapper into the browser's localStorage under a legitimate OWA settings field. OWA's normal page-sync flow then re-executes the implant automatically every time the user opens an OWA tab, and the malware leaves no file on the host.

#3

To deepen its foothold, OWAReaper creates two invisible input elements in the DOM and waits for the browser's autofill to populate them, capturing the user's saved OWA username and password. It then looks for installed Outlook add-ins that hold ReadWriteMailbox permissions and abuses them, calling GetClientAccessToken to steal OAuth tokens. Next, it calls UpdateFolder to grant Owner-level permissions on every mail folder to the "Default" user, a low-permission alias present in all Exchange tenants. This effectively hands mailbox access to any authenticated account in the same organization. Because the permission change lives on the Exchange server, rotating the victim's credentials or even fully re-imaging their device does not remove the actor's access, which must be deliberately stripped from the server. As a further fallback, OWAReaper injects a hidden iframe into messages cached in OWA's offline IndexedDB store, so the implant re-infects the target whenever a poisoned cached email is reopened.

#4

OWAReaper supports two command-and-control channels and two exfiltration paths. For commands, it queries GitHub's Commit Search API every 24 hours for specially crafted commit messages keyed to the target's email address, decrypting them with AES-CTR using a hardcoded key plus a per-session key; the command types observed are code, domn, and cmnd. Alternatively, it parses inbound attacker emails from IndexedDB every five minutes, matching a specific message structure. For exfiltration, the primary route is HTTPS with AES-CTR-encrypted URI paths, relayed through legitimate image CDN services and ultimately fetched from the actor domain; if that fails it beacons directly to the C&C. When the HTTPS route fails entirely, OWAReaper falls back to DNS tunneling, AES-CTR-encrypting the data, Base32-encoding it, and splitting it across the subdomain labels of an actor-controlled domain. Unlike ZimReaper, it does not mass-exfiltrate the mailbox, likely to reduce noise and improve operational security.

Recommendations

Patch Exchange Server for CVE-2026-42897: Apply Microsoft's out-of-band update for CVE-2026-42897 across all Exchange Server and Outlook Web Access deployments, prioritizing internet-facing OWA instances.

Revoke and Audit EWS Tokens for Outlook Add-ins: Revoke and review Exchange Web Services (EWS) tokens for installed add-ins, focusing on any that hold ReadWriteMailbox permissions, since OWAReaper abuses these to steal OAuth tokens.

Remove Malicious Mailbox Permissions: Audit Exchange mailbox folder permissions and remove any Owner-level grants made to the "Default" user, which the implant uses to give itself organization-wide mailbox access.

Clear Poisoned Browser Artifacts: On affected endpoints, clear OWA's IndexedDB message cache (owa_offline_db) and delete the PageDataPayload.OwaUserDefaultSettings localStorage key to strip the implant's browser-resident persistence and iframe re-infection.

Rotate Credentials, Then Verify Eviction: Reset compromised passwords and invalidate active sessions, but treat this as insufficient on its own. Because access persists server-side, confirm the malicious folder permissions and tokens have been removed before considering an account clean.

Raise Awareness of Half-Click Threats: Educate users that with these webmail exploits, opening or previewing a bland, link-free email can be enough to trigger compromise, and encourage reporting of unusual messages even when they appear harmless.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1586: Compromise Accounts	T1586.002: Email Accounts
	T1583: Acquire Infrastructure	T1583.001: Domains
Initial Access	T1566: Phishing	

Tactic	Technique	Sub-technique
Execution	T1203: Exploitation for Client Execution	
	T1059: Command and Scripting Interpreter	T1059.007: JavaScript
Defense Evasion	T1027: Obfuscated Files or Information	
	T1140: Deobfuscate/Decode Files or Information	
	T1070: Indicator Removal	T1070.008: Clear Mailbox Data
Persistence	T1098: Account Manipulation	T1098.002: Additional Email Delegate Permissions
Credential Access	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
	T1528: Steal Application Access Token	
Collection	T1114: Email Collection	
Command and Control	T1102: Web Service	T1102.002: Bidirectional Communication
Exfiltration	T1041: Exfiltration Over C2 Channel	
	T1048: Exfiltration Over Alternative Protocol	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	asecdns[.]com, acocdn[.]com, dnsrecursive[.]eu, tdndns[.]com
SHA256	6897b649f29e54d8910459963bbf94ed5c7a4fe66a56bc5962540b226b8e48c4

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42897

References

https://www.proofpoint.com/us/blog/threat-insight/cleaning-out-inboxes-ta488-comes-outlook-another-half-click-exploit

https://hivepro.com/threat-advisory/active-exploitation-of-cve-2026-42897-targets-microsoft-exchange-servers/

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 Demo of **HivePro**.

REPORT GENERATED ON

July 30, 2026 • 08:30 AM

More at www.hivepro.com