BLACKSWAN CYBERSECURITY

THREAT ADVISORY
Russian APT "Laundry Bear" Exploiting OWA XSS for Persistent Mailbox Access

August 5, 2026

Threat Actor: Laundry Bear (aka TA488, CL-STA-1114, UNK_PitStop, Void Blizzard)
Vulnerability: CVE-2026-42897 (CVSS 8.1) – Cross-Site Scripting in Microsoft Outlook Web Access (OWA)
Malware: OWAReaper (JavaScript browser-based implant)
Activity Start: July 22, 2026 (infrastructure prepared as early as March 2026)
Targets: U.S. & European government entities, telecommunications, financial services, hospitality, and aerospace sectors

Summary

Russian threat actors previously linked to Zimbra XSS exploitation (CVE-2025-66376 / ZimReaper) have shifted focus to Microsoft OWA. They are delivering "half-click" phishing emails that trigger CVE-2026-42897 simply by viewing the message in a vulnerable OWA instance (no clicks, attachments, or links required).

The payload deploys **OWAReaper**, a sophisticated JavaScript implant that:

- Executes in the OWA reading pane
- Removes exploit evidence from the server-side email
- Captures credentials via browser autofill
- Achieves dual persistence (browser localStorage + offline IndexedDB cache)
- Grants Owner-level permissions on mail folders
- Maintains access even after credential rotation or full device re-imaging
- Uses GitHub commit search API or inbound emails for C2
- Exfiltrates data via encrypted HTTPS or DNS tunneling

This is a significant evolution of their earlier Zimbra campaign and demonstrates improved tradecraft focused on stealthy, server-side persistence.

Key Technical Details

Delivery: Vague, legitimate-looking emails (supply chain updates, research notes, market metrics) sent from compromised or adversary-controlled accounts (including Proton Mail).

Exploit trigger: JavaScript loaded via social media icons in the message HTML; payload assembled from Base64 fragments.

Persistence mechanisms:

1. Encrypted implant + decryption wrapper written to browser localStorage (auto-runs on OWA tab open)
2. Hidden iframe injected into offline message cache (re-infects even after re-imaging)

Privilege escalation: Leverages Outlook add-ins with ReadWriteMailbox permissions to steal OAuth tokens and grant broad mailbox access across the organization.

THREAT ADVISORY
Russian APT "Laundry Bear" Exploiting OWA XSS for Persistent Mailbox Access

August 5, 2026

C2 & Exfiltration: GitHub API polling (every 24h) or email-based commands; primary exfil over AES-CTR encrypted HTTPS, fallback DNS tunneling.

Why This Matters

Credential resets and endpoint re-imaging **do not** remove the actor. Persistence lives on the Exchange server and in the browser environment. Organizations relying solely on password rotation or device hygiene remain at risk.

Recommended Actions

1. **Patch immediately** – Apply Microsoft's fix for CVE-2026-42897 if not already done.
2. **Hunt for indicators:**
    - Unusual OWA localStorage entries
    - Hidden iframes or anomalous IndexedDB activity related to OWA
    - Unexpected Owner permissions on mail folders
    - Suspicious GitHub API queries or DNS activity matching known patterns
3. **Review OWA/Exchange configurations** – Restrict or audit add-ins with ReadWriteMailbox permissions.
4. **Monitor for half-click style phishing** – Especially generic informational emails with no links or attachments.
5. **Assume breach mindset** – Investigate for lateral movement if any account in the organization was previously compromised.