Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

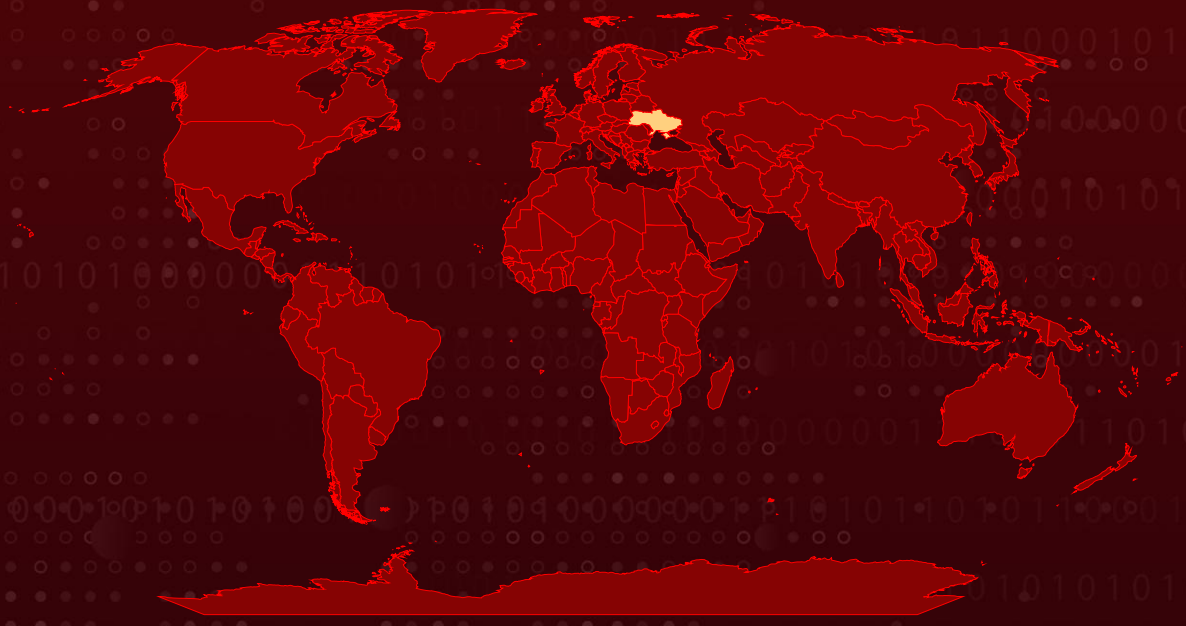
Operation GhostMail: The Invisible Inbox Breach

Date of Publication	Admiralty Code	TA Number
March 20, 2026	A1	TA2026078

Summary

First Seen: January 22, 2026
Targeted Region: Ukraine
Targeted Products: Synacor Zimbra Collaboration Suite (ZCS)
Targeted Industry: Government
Campaign: Operation GhostMail
Attack: Operation GhostMail turns a simple email into a stealthy intrusion vector, requiring no links or attachments to compromise a target. Disguised as a routine internship request, the phishing email quietly exploited a Zimbra webmail flaw to execute hidden scripts directly in the victim's browser, hijacking their authenticated session without leaving a trace on disk. From there, the attackers moved swiftly, harvesting credentials, generating persistent access, and siphoning sensitive mailbox data, including full email archives, while blending seamlessly with legitimate activity. The operation highlights a sharp evolution in tradecraft, where trusted platforms and browser sessions themselves become the attack surface, enabling silent, fileless espionage.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-66376	Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting Vulnerability	Synacor Zimbra Collaboration Suite	✗	✓	✓

Attack Details

#1

What looked like a harmless internship inquiry quietly unfolded into a full-scale compromise. On January 22, 2026, attackers launched Operation GhostMail with a carefully crafted spear-phishing email sent from a compromised student account at Ukraine's National Academy of Internal Affairs. Written in fluent Ukrainian, the message posed as a polite outreach from a fourth-year student seeking internship opportunities, complete with an apologetic tone to build credibility. The target was an employee at the Ukrainian State Hydrology Agency, part of the country's critical infrastructure. Notably, the email carried no attachments or links, eliminating common red flags and relying entirely on subtlety.

#2

Instead of delivering malware in the traditional sense, the attackers embedded their payload directly within the HTML body of the email. Hidden inside a div element was code exploiting CVE-2025-66376, a stored XSS flaw in Zimbra Classic UI caused by improper sanitization of CSS @import directives. When the victim opened the email in an authenticated Zimbra session, the exploit triggered silently. By bypassing the AntiSamy sanitizer through fragmented token injection, the attackers reconstructed executable SVG elements, allowing JavaScript to run within the trusted browser context, effectively inheriting session cookies, local storage, and API access.

#3 The initial script acted as a stealthy loader, ensuring it executed only once before decoding a Base64 payload and applying an XOR routine using the key "twichcba5e." This process deployed a second-stage browser stealer directly into the top-level document, sidestepping iframe restrictions and gaining full visibility into the session. From there, the operation escalated rapidly. The malware executed multiple tasks in parallel, harvesting sensitive data such as user identities, server configurations, and even backup 2FA recovery codes. It also created a persistent app-specific password labeled "ZimbraWeb," effectively granting the attackers long-term access without raising suspicion.

#4 Beyond credential theft, the attackers expanded their foothold by enumerating connected mobile devices, listing authorized OAuth applications, and enabling IMAP access to facilitate ongoing data collection. By leveraging legitimate SOAP API requests authenticated with stolen CSRF tokens, all malicious activity blended seamlessly with normal webmail operations. This approach made detection significantly more difficult, as the traffic appeared indistinguishable from legitimate user behavior.

#5 Data exfiltration was equally methodical and resilient. The attackers used a dual-channel strategy, encoding smaller data chunks into DNS queries while transmitting larger datasets over HTTPS. Their most impactful move was systematically downloading a 90-day archive of the victim's emails via Zimbra's export functionality, packaging each day into compressed files and exfiltrating them incrementally. Progress tracking via localStorage ensured the operation could resume if interrupted. With infrastructure registered just days prior and tactics aligned with known tradecraft, the campaign has been attributed to APT28 with medium confidence, highlighting a shift toward fileless, browser-native intrusion techniques that evade traditional defenses.

Recommendations

Patch Zimbra Collaboration Suite Immediately: Upgrade all Zimbra instances to version 10.1.13 or 10.0.18 (minimum) to remediate CVE-2025-66376. Organizations still running Zimbra 8.8.15 should migrate immediately to a supported release or an alternative platform, as this version is end-of-life and lacks security patches.

Migrate Off Zimbra 10.0 Branch: Zimbra version 10.0 reached End of Life on December 31, 2025. While 10.0.18 patches this specific CVE, organizations should accelerate migration to the 10.1 series to maintain access to ongoing security updates.

Deploy Email Content Inspection: Implement enhanced email filtering that inspects HTML email bodies for obfuscated JavaScript payloads, particularly those using Base64-encoded scripts within hidden div elements and CSS @import-based bypasses. Standard attachment and link scanning alone is insufficient against this attack vector.

Audit App-Specific Passwords: Review all Zimbra accounts for app-specific passwords named "ZimbraWeb" or any passwords created around the time of suspicious email activity. Revoke unauthorized app-specific passwords immediately, as these survive standard password resets and provide persistent access.

Audit IMAP Configuration Changes: Check account settings for unexpected zimbraPrefImapEnabled: TRUE changes, particularly on accounts that do not have a legitimate business need for IMAP access. Disable unused mail protocols (IMAP, POP3) at the administrative level to remove persistence vectors.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
	T1586: Compromise Accounts	T1586.002: Email Accounts
Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
Execution	T1059: Command and Scripting Interpreter	T1059.007: JavaScript
	T1203: Exploitation for Client Execution	
Persistence	T1098: Account Manipulation	T1098.001: Additional Cloud Credentials

Tactic	Technique	Sub-technique
Credential Access	T1528: Steal Application Access Token	
	T1539: Steal Web Session Cookie	
	T1111: Multi-Factor Authentication Interception	
	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
Discovery	T1082: System Information Discovery	
	T1087: Account Discovery	T1087.003: Email Account
	T1069: Permission Groups Discovery	
	T1120: Peripheral Device Discovery	
Collection	T1114: Email Collection	T1114.002: Remote Email Collection
	T1185: Browser Session Hijacking	
	T1213: Data from Information Repositories	
Exfiltration	T1041: Exfiltration Over C2 Channel	
	T1071: Application Layer Protocol	T1071.004: DNS

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	c010f64080b0b0997b362a8e6b9c618e
Domains	zimbrasoft[.]com[.]ua, js-[a-z0-9]{12}[.]i[.]zimbrasoft[.]com[.]ua

Patch Link

https://wiki.zimbra.com/wiki/Zimbra_Releases

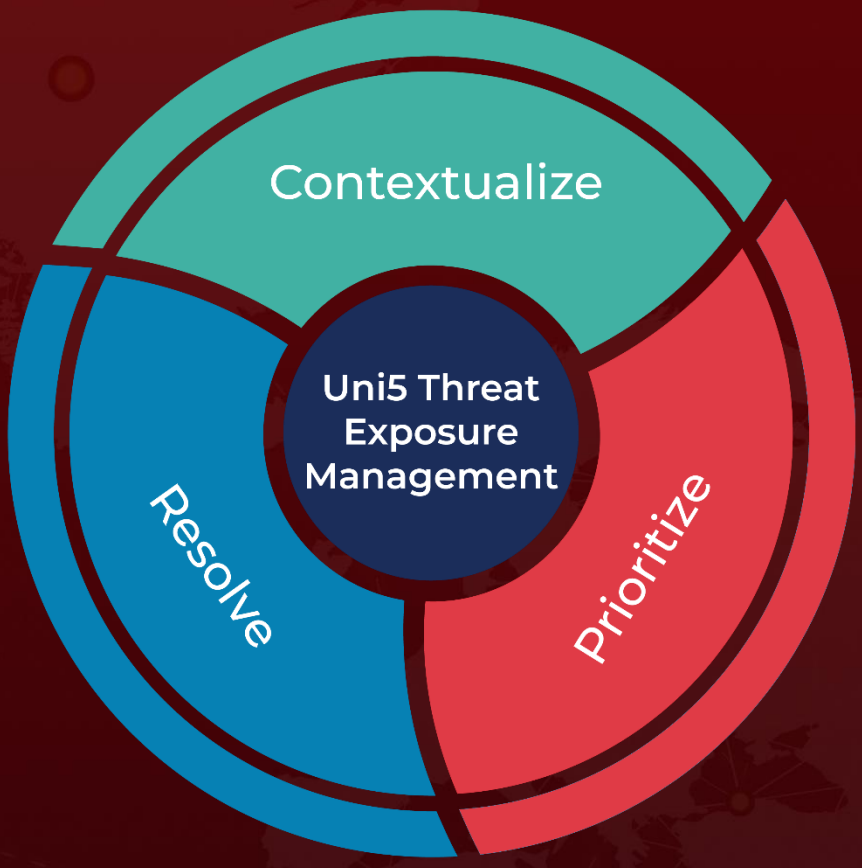
References

https://www.seqrite.com/blog/operation-ghostmail-zimbra-xss-russian-apt-ukraine/

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

March 20, 2026 • 8:30 AM

More at www.hivepro.com