Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

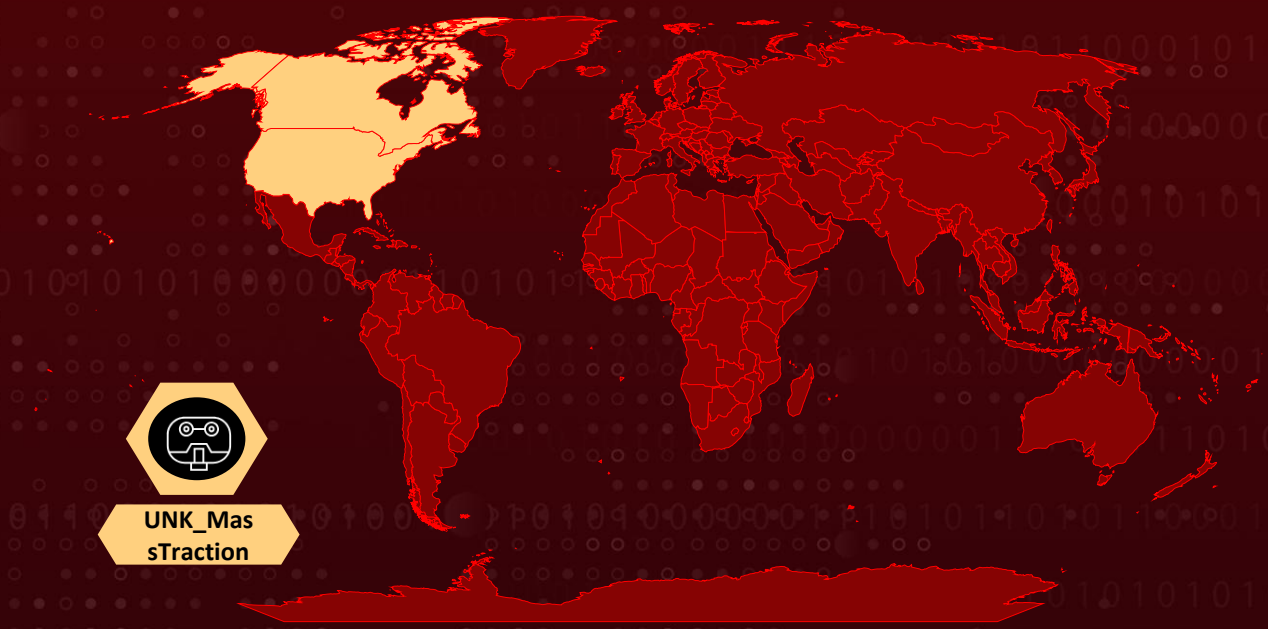
UNK_MassTraction Chains Roundcube N-Days to Pivot into University Networks

Date of Publication	Admiralty Code	TA Number
July 08, 2026	A1	TA2026190

Summary

First Seen: May 2026
Targeted Regions: United States, Canada
Targeted Platforms: Linux mail servers, Web browsers
Targeted Product: Roundcube Webmail
Targeted Industry: Higher Education
Threat Actor: UNK_MassTraction
Malware: VShell, IceCube, SquareShell, SNOWLIGHT
Attack: UNK_MassTraction is a suspected China-aligned espionage cluster that sends phishing emails abusing two n-day Roundcube flaws. An initial cross-site scripting bug (CVE-2024-42009) runs attacker JavaScript the moment a victim opens the email, launching the IceCube stealer to grab webmail credentials, cookies, and two-factor material. IceCube then exploits a deserialization remote code execution flaw (CVE-2025-49113) to plant the SquareShell webshell or load the VShell backdoor in the mail server's memory, turning the compromised server into a springboard into the target's wider network.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-42009	RoundCube Webmail Cross-Site Scripting Vulnerability	Roundcube Webmail	✗	✓	✓
CVE-2025-49113	RoundCube Webmail Deserialization of Untrusted Data Vulnerability	Roundcube Webmail	✗	✓	✓

Attack Details

#1

UNK_MassTraction opens each intrusion with phishing emails aimed at physics and engineering departments at major universities, favoring administrators and professors in groups tied to national security work or astrophysics and particle physics research. The messages use generic lures and are sent from compromised senders and from domains that can be spoofed because of weak DMARC policies. The exploit does not need the recipient to click anything. Simply opening the message in a vulnerable Roundcube webmail client triggers CVE-2024-42009, a cross-site scripting flaw that runs attacker JavaScript through the onanimationstart handler. That JavaScript acts as a loader and pulls the next stage from a remote host.

#2

The next stage is a full-featured stealer called IceCube. It escapes Roundcube's iFrame through DOM traversal, giving it reach across the whole browser and the authenticated webmail session. From there it collects stored usernames and passwords, two-factor authentication material, and cookies, and it fingerprints the browser by reading the language in use, screen size, and form field values. The harvested data is sent to the command-and-control server over an HTTP POST. IceCube then uses the session's CSRF token to weaponize a second flaw, CVE-2025-49113, a PHP object deserialization bug in Roundcube's Crypt_GPG_Engine parsing. It sends serialized PHP data containing a gadget that executes commands when deserialized, dropping a lightweight webshell named SquareShell at the endpoint plugins/newmail_notifier/mail_preview.php. The webshell is timestomped with the modified time of a legitimate plugin so it blends into the environment.

#3

The chain is built to keep moving even when a step fails. If the webshell does not install, a fallback introduced in June 2026 downloads a shell script that stages an architecture-specific ELF loader tracked as SNOWLIGHT, fetches the matching payload from the C&C, and runs it with nohup. IceCube also sets up what it calls deferred triggers that watch for the user closing the page, switching tabs, moving the mouse out of the browser window, or clicking logout. When any of those happen, IceCube re-attempts the CVE-2025-49113 exploit and beacons that the user has left the session. Once its work is done or a timeout is reached, it destroys the user and malware sessions on the server, logging the victim out and wiping forensic evidence from the Roundcube host.

#4

Stolen credentials and reconnaissance data leave the environment over the same HTTP channel back to the C&C. On the server side, the SNOWLIGHT loader first checks for a lock file at /tmp/log_de.log to avoid running twice, spoofs the process name [kworker/0:2] to look like a kernel worker, beacons over a socket, and loads the VShell backdoor entirely in memory using fexecve(). VShell is a publicly available Go implant with capabilities comparable to Cobalt Strike; its interactive shell and port-forwarding features are the most likely tools the operators would use to pivot from the compromised mail server deeper into the university network. Infrastructure overlaps, the reuse of SNOWLIGHT and VShell, and Chinese-language artifacts in earlier emails point to a China-aligned, espionage-motivated actor treating the mail server as an edge device for network access rather than as the end target.

Recommendations

Patch Roundcube to a Fixed Release: Upgrade every Roundcube instance to 1.6.11 or 1.5.10 (or later), which close both CVE-2024-42009 and CVE-2025-49113, and treat any server below these versions as exposed.

Block Known Command-and-Control Infrastructure: Add the listed IceCube and VShell IPs, delivery URLs, and sslip.io endpoints to network blocklists and alert on any outbound connections to them.

Reset Exposed Credentials and Sessions: Force password resets, invalidate active Roundcube sessions, and rotate two-factor secrets for any account on a potentially compromised server, since IceCube harvests credentials, cookies, and 2FA material.

Tighten Email Authentication: Enforce a strict DMARC policy (p=reject) with validated SPF and DKIM to blunt the sender spoofing this actor relies on for delivery.

Scan Linux Hosts for the VShell Loader: Look for the lock file /tmp/log_de.log, processes masquerading as [kworker/0:2], and in-memory execution via fexecve(), which indicate the SNOWLIGHT loader and the VShell backdoor.

Treat Mail Servers as Edge Devices: Monitor, log, and harden internet-facing webmail with the same rigor applied to VPN concentrators and other remote-access nodes.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	
	T1190: Exploit Public-Facing Application	
Execution	T1203: Exploitation for Client Execution	
	T1059: Command and Scripting Interpreter	T1059.007: JavaScript
		T1059.004: Unix Shell
Credential Access	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
	T1539: Steal Web Session Cookie	
	T1111: Multi-Factor Authentication Interception	
Persistence	T1505: Server Software Component	T1505.003: Web Shell
Defense Evasion	T1070: Indicator Removal	T1070.006: Timestomp
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1620: Reflective Code Loading	

Tactic	Technique	Sub-technique
Command-and-Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1105: Ingress Tool Transfer	
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
Email	jpcontreras[@]newfield[.]cl
IPv4	45[.]150[.]109[.]151, 194[.]213[.]18[.]133, 45[.]86[.]229[.]111
URLs	hxxps[:]//45[.]150[.]109[.]151[.]sslip[.]io[:]23088/app/js/jquery[.]min[.]js, hxxps[:]//194[.]213[.]18[.]133[.]sslip[.]io[:]23088/app/js/jquery[.]min[.]js, hxxps[:]//45[.]150[.]109[.]151[.]sslip[.]io[:]23088, hxxps[:]//194[.]213[.]18[.]133[.]sslip[.]io[:]23088, hxxp[:]//45[.]86[.]229[.]111/slw[:]8080
SHA256	a02f124c5ce4180bd130a62ee03262f399c33491de3aed36e0b15155ae4926c0

Patch Link

https://github.com/roundcube/roundcubemail/releases

References

https://www.proofpoint.com/us/blog/threat-insight/one-email-closer-edge-unkmasstraction-physics-exploitation

https://hivepro.com/threat-advisory/a-decade-old-roundcube-glitch-comes-back-to-bite/

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 08, 2026 • 08:00 AM

More at www.hivepro.com