Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

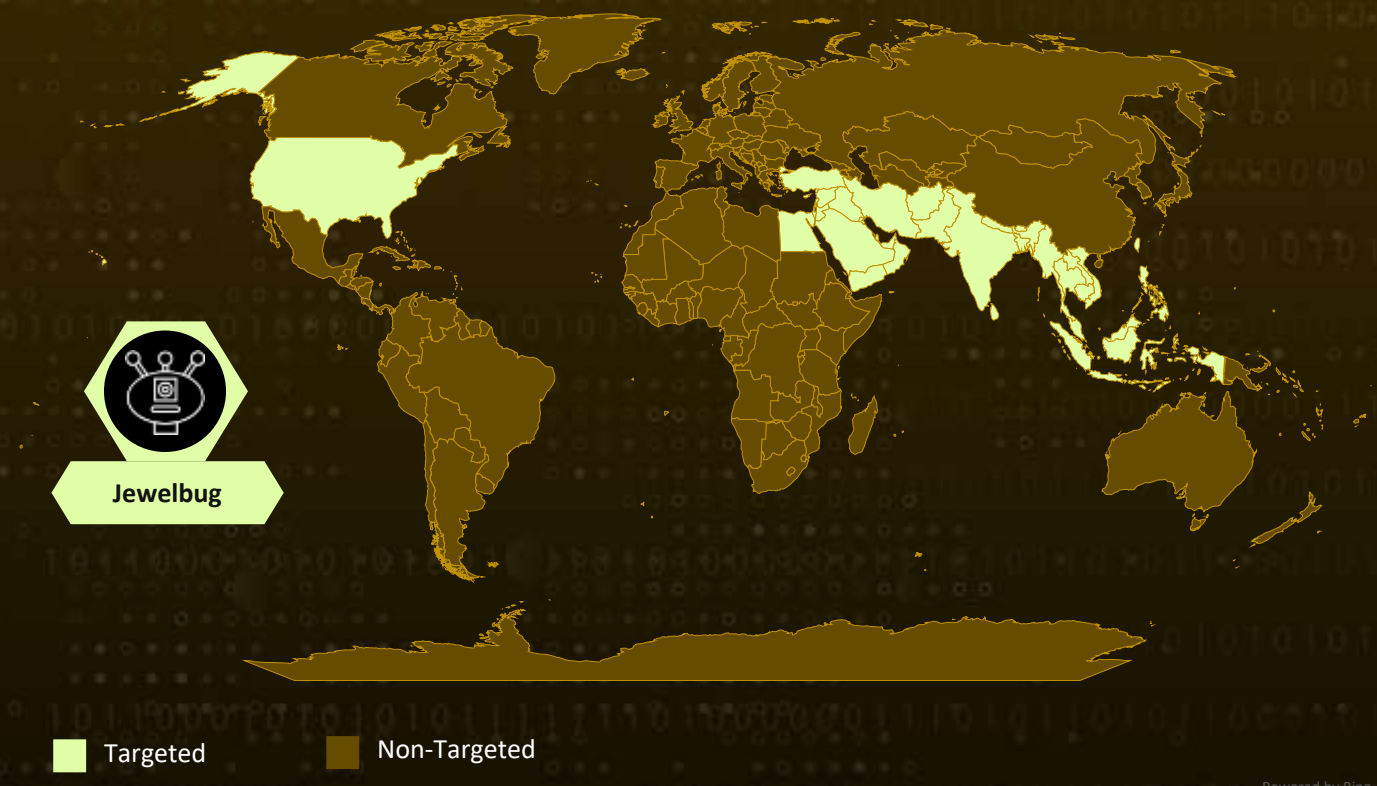
One Team, Two Payrolls: Jewelbug's Parallel Operations

Date of Publication	Admiralty Code	TA Number
August 19, 2026	A1	TA2026237

Summary

First Seen: 2023
Targeted Regions: Middle East, Southeast Asia, South Asia, Taiwan, United States
Targeted Platforms: Windows, Linux, Google Chrome, Mozilla Firefox, x86-64 servers, ARM64 devices, consumer routers
Targeted Products: Google Chrome, Mozilla Firefox, ASUS consumer routers
Targeted Industries: Government, Military, Defense, Law Enforcement, Telecommunications, Aerospace, Industrial Manufacturing, Web Hosting Services, Cryptocurrency
Threat Actor: Jewelbug (Earth Alux, REF7707, CL-STA-0049, Ink Dragon)
Malware: Antino, ClientKing, XG-Web (command-and-control framework)

Actor Map



Attack Details

#1

Jewelbug is a China-based hacker-for-hire group tracked variously as **Earth Alux**, REF7707, CL-STA-0049, and Ink Dragon. The group conducts two concurrent operations: cyber espionage against government and military organizations across the Middle East, Southeast Asia, and South Asia, and a for-profit cryptocurrency fraud business directed at Chinese-speaking victims. Both operations are run by the same small team on shared infrastructure and from a single control panel. That panel, XG-Web, is a browser-centric remote-access and information-stealing framework that converts a compromised browser into a remote-control channel and extends access from the browser into the host and the internal network behind it. Its developers document the platform as a penetration-testing tool, although internal function names recorded within it, including browser hijacking, data theft, and man-in-the-middle attack, are inconsistent with that description.

#2

The group has developed five generations of command-and-control code supporting implants across browsers, Windows endpoints, Linux servers and network devices, all reporting into a single victim database. Observed initial access methods include watering-hole compromise of shared web-hosting infrastructure, malicious HTML Application downloaders themed on current geopolitical events, counterfeit Adobe installers hosted on actor-controlled domains, and search-engine-optimization poisoning that directs cryptocurrency users to fraudulent exchange-download portals.

#3

The group's largest reported espionage operation illustrates its methodology. Rather than compromising government ministries individually, Jewelbug compromised the shared web-hosting platform operated by a Middle Eastern state telecommunications provider and national network-services agency, harvested administrator credentials from the provider itself, and inserted a single script tag into the common webmail template. This modification established a watering hole across more than 15 government webmail tenants simultaneously, executing on the login page and on every mailbox view.

#4

On victim authentication, the injected script exfiltrated session cookies over a WebSocket channel and labeled each victim according to the government email address read from the webmail interface. Operators subsequently delivered a lure module that validated the target before presenting a counterfeit Adobe Flash update prompt. Victims who accepted the prompt received Antino, the group's primary Windows backdoor, which additionally sideloaded a malicious browser extension named PDF Viewer along with a native-messaging helper that provided operators with command execution on the host. For Linux servers and network devices the group deploys ClientKing, a Rust implant supporting five command-and-control transports including a custom DNS tunnel, accompanied by a kernel-module rootkit and a malicious authentication module hooked into su and sudo for credential theft.

#5

Collection is conducted primarily through the browser extension, which hooks login forms, exfiltrates the full cookie store, subscribes to cookie-change events to capture newly issued session tokens, and collects browsing history, screenshots, clipboard contents and intercepted traffic. Command-and-control activity relies on trusted services to reduce the likelihood of detection, with obfuscated payloads staged in public Google Documents, Antino beaconing through the Microsoft Graph API, and a scheduled task querying VirusTotal every twelve hours so that flagged domains could be rotated before access was lost.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Jewelbug (Earth Alux, REF7707, CL-STA-0049, Ink Dragon)	China **MOTIVE** Espionage and Financial Gains	Middle East, Southeast Asia, South Asia, Taiwan, United States	Government, Military, Defense, Law Enforcement, Telecommunications, Aerospace, Industrial Manufacturing, Web Hosting Services, Cryptocurrency

Recommendations

Enforce Extension Allowlisting: Move browsers to an enterprise-managed allowlist so only approved extension IDs can install, and block sideloading from local profile directories. Jewelbug's backdoor writes the extension into the browser profile directly rather than going through a store, so store-level policy alone will not stop it.

Hunt for Malicious Native Messaging Hosts: Search the registry for native-messaging host registrations under Chrome and Firefox, specifically the value HKCU\SOFTWARE\Google\Chrome\NativeMessagingHosts\com.microsoft.runedge, and validate every remaining host manifest against its signing publisher. This registration is what lets the extension break out of the browser sandbox and run commands on the host.

Revoke Sessions and Rotate Credentials for Exposed Webmail Users: For any user whose browser is suspect, invalidate all active web sessions server-side, force a password reset and re-enroll multi-factor authentication. Stolen cookies and live session tokens let operators reuse authenticated sessions without ever needing the password, so a password change alone leaves access intact.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.006: Web Services
	T1584: Compromise Infrastructure	T1584.004: Server
	T1587: Develop Capabilities	T1587.001: Malware
	T1608: Stage Capabilities	T1608.001: Upload Malware
		T1608.004: Drive-by Target
		T1608.006: SEO Poisoning
Initial Access	T1189: Drive-by Compromise	
	T1566: Phishing	T1566.002: Spearphishing Link
	T1078: Valid Accounts	
Execution	T1204: User Execution	T1204.002: Malicious File
		T1204.001: Malicious Link
	T1059: Command and Scripting Interpreter	T1059.007: JavaScript
		T1059.003: Windows Command Shell
Persistence	T1176: Software Extensions	T1176.001: Browser Extensions
	T1556: Modify Authentication Process	T1556.003: Pluggable Authentication Modules
	T1547: Boot or Logon Autostart Execution	T1547.006: Kernel Modules and Extensions

Tactic	Technique	Sub-technique
Defense Evasion	T1112: Modify Registry	
	T1014: Rootkit	
	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1036: Masquerading	T1036.005: Match Legitimate Resource Name or Location
	T1218: System Binary Proxy Execution	T1218.005: Mshta
Credential Access	T1539: Steal Web Session Cookie	
	T1056: Input Capture	T1056.003: Web Portal Capture
	T1185: Browser Session Hijacking	
Discovery	T1217: Browser Information Discovery	
	T1082: System Information Discovery	
Lateral Movement	T1550: Use Alternate Authentication Material	T1550.004: Web Session Cookie
Collection	T1114: Email Collection	T1114.002: Remote Email Collection
	T1113: Screen Capture	
	T1115: Clipboard Data	
	T1557: Adversary-in-the-Middle	
	T1074: Data Staged	T1074.002: Remote Data Staging
Command and Control	T1102: Web Service	T1102.001: Dead Drop Resolver
		T1102.002: Bidirectional Communication

Tactic	Technique	Sub-technique
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
		T1071.004: DNS
	T1572: Protocol Tunneling	
	T1090: Proxy	T1090.001: Internal Proxy
	T1105: Ingress Tool Transfer	
Exfiltration	T1041: Exfiltration Over C2 Channel	
Impact	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	e6ff096a0562c0042b09d250bd60272ffcd8d72bd95c563842acf765a8dc8bcf, 01b5c6acb20e41799a0e96d9d1d6e1c44791883706b6285e874fcb15cc93b31a, e809da86bd81463347fa7f922d3e088755a94a331889d32acb55aa8f57778a34, f1ef5fe4c0cdcff13cc750c867728b89719f81437bdc49041edd1ae1f3edb4e8, e2eb7703047b37b28dc34e6990205d758a2454b39bc655b460606745fadcb530, e7e3b0bcd6798634adf8b49d305f3a7b7682e4b76db549682a183c5a186df4bb, 09ef7c736bccfafefc44d9910d499173b88063b73b221fc0dc9e9105107e5cff, c11714f9fe2df1ca906585c81498cd77f5ec05b132aab73fa3a71d71d71e42cc, b90a4e770869c28fd2140acb3ebdc50c113bb6f096b4bbdb9ac87c349c70e85e, 0c39264337a1186b2e765e24073399cbdcba118306614eb411e315887af578bd,

TYPE	VALUE
SHA256	9b7df409c9a89f7536d3ba7b6d43fb6dbac618c8bb52615ba34cc971ad71bbf3, 153d077bcb58e00f5746573cba25f6b0788b809bf7b2a52fca0dc22d3bb5c94e, 297413a3e49e7353bf484a3eb15ec647de729211059df8fc68678d2378b6f561, 30f5122cc199b9c2e524503b343a9ee13a6f9773dcbc1df82c8b25ad20bca61d, 430f12970f8d58f12edccee9019a1aa90fa232c961449bdcc69c8d348a52cf55, 5ccdf53881f6c758af8d94fe67066af209b4bc0a3cb80b6a4c724fad86eb97ef, 5edb8d1023b8babf302871b68fa2b26d5ca57633f64951922998e8f1d6c8f7ac, 6d5fe6b6a34eeb470798b970b70f41a07ccf59b22f49ad9b3dfff7aa3256f3c2, 97c3a6be1711c5340d8806e4a54f7297f3f763d0aa4240b667f1e4e1f98f2aad, ac3d453d3c9b0310ebb8a67cef35e2ac954d4acdf70cf497fe43a02c7a510813, e782a6d4919f194d41e524ebd6df5894197043cf772fcf60455127b246f302c0, ea893abf20b00d9bfc042a88fbf7b4bd42e68ce07c116d3e3b002e5b4a853877, ed96e7f1085a50251eb8967ac53777272a617831084f0edad8a769c583a18869
Domains	fonts[.]tarotfree101[.]top, fonts[.]chrorne[.]com, robot[.]avbliud[.]com, microsoft-flash[.]com, www[.]wps-cn[.]com, www[.]f1ash[.]org[.]cn, browser-update[.]pages[.]dev, eastus2[.]wac-azure[.]com, mailbycloud[.]com, www[.]jkskhei[.]com, ns1[.]jkskhei[.]com, dns[.]wizkidblogger[.]com, r6fi2yvqql[.]execute-api[.]ap-southeast-2[.]amazonaws[.]com

TYPE	VALUE
IPv4	103[.]87[.]9[.]62, 152[.]42[.]174[.]151, 43[.]246[.]208[.]236, 43[.]246[.]208[.]179, 47[.]84[.]37[.]113, 47[.]84[.]51[.]173, 167[.]71[.]195[.]255, 38[.]12[.]1[.]47, 129[.]212[.]237[.]224, 47[.]87[.]71[.]167, 47[.]250[.]208[.]35, 219[.]76[.]254[.]184
URLs	hxxp[:]//d2nq35tel3ucuo[.]cloudfront[.]net/LtVGUSsyUTDA[.]log, hxxps[:]//pub-abfa7742e315485a98a5fafd6dbfb68e[.]r2[.]dev/hjgzBskgslc[.]dll[.]iwq, hxxps[:]//microsoft-flash[.]com/download/flashcenter_pp_ax_install_en[.]exe, hxxps[:]//www[.]f1ash[.]org[.]cn/flashcenter_pp_ax_install_cn[.]exe, hxxps[:]//microsoft-flash[.]com/download/Adobeinstall[.]exe, hxxps[:]//fonts[.]chrorne[.]com/dist/js/12[.]qgfvjzvs[.]chunk[.]js
Filename	flashcenter_pp_ax_install_en.exe, flashcenter_pp_ax_install_cn.exe, Adobeinstall.exe, Adobe_installer (1).exe, TEST.hta, slc.dll, Vb0c44dfslc.dll.wxb
Registry Key	HKCU\SOFTWARE\Google\Chrome\NativeMessagingHosts\com.microsoft.runedge

References

https://www.security.com/threat-intelligence/jewelbug-crypto-fraud-espionage

https://www.hivepro.com/threat-advisory/earth-alux-the-cyber-threat-hiding-in-plain-sight

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

August 19, 2026 • 04:00 AM

More at www.hivepro.com