Jewelbug: government mailboxes and fake crypto exchanges

Symantec has published the inside of a Chinese operation running two businesses from one control panel: stealing from government mailboxes across Asia and the Middle East, and running hundreds of fake cryptocurrency exchange sites.

INCIDENT DETAILS · 5WH

Who A group Symantec calls Jewelbug, also tracked as Earth Alux and REF7707. Symantec ties an operator to a registered Hunan company and assesses the espionage as state-directed.
What One team, two missions, one control panel. A compromise of a shared webmail platform exposed more than fifteen government tenants at once.
Where Government and military targets in the Middle East, South Asia and Southeast Asia. The fraud targets Chinese-speaking users.
When Published by Symantec's Threat Hunter Team on 13 Aug 2026.
Why Intelligence collection and money; the scale of the fraud sets this apart from a state actor earning on the side.
How A watering-hole compromise of shared webmail, a permission-greedy browser extension, and session-token theft that defeats multi-factor authentication.

IMPACT

- Government email: more than fifteen tenants compromised through one shared platform, reaching correspondence, contacts and password-reset links.
- Authentication: a stolen session token is proof the user already logged in, so replaying it passes both password and second factor.
- Single point of failure: shared hosting concentrated fifteen departments' exposure into one platform.
- Attribution: espionage and commodity crime from one set of hands muddies classification and complicates response.

SEQUENCE OF EVENTS

Mid-2023 Jewelbug first active
13 Aug 2026 Symantec publishes the research

1. Write access to a shared webmail template
2. The script takes cookies and checks the address
3. Valuable users get a fake Flash update prompt
4. A PDF Viewer extension takes tokens and traffic
5. The same panel runs fake OKX and Binance pages
6. Symantec gets inside: 1m check-ins, 580,000 cookies

ASSESSMENT, LESSONS, AND RECOMMENDATIONS

- The shared platform is the finding, not the malware - the exposure existed before any attacker arrived.
- Session-token theft defeats multi-factor authentication without attacking it.
- Espionage and crime in one organisation degrades attribution for every defender.
- The attribution is a vendor assessment, unusually well evidenced, and still short of establishing state direction.