Symantec by Broadcom

The Jewelbug Dossier

China-based hackers-for-hire group staging espionage attacks alongside a cryptocurrency fraud business.

SYMANTEC THREAT HUNTER TEAM

Symantec by Broadcom

TABLE OF CONTENTS

1. Executive summary 3
2. Who is Jewelbug 4
3. Attribution and operators 6
   - Operator tradecraft 6
4. Tooling and tradecraft 7
   - The XG-Web framework 7
   - “PDF Viewer” browser extension 8
   - The native-messaging shell (`com.microsoft.runedge`) 9
   - The `victim.js` hook and delivery 10
   - Command-and-control: dead drops, reputation self-monitoring, MITM proxy 11
   - The exploit-module library 11
   - Antino backdoor 12
   - ClientKing: Linux and router implant 13
   - Other content 13
   - Planned capabilities (developer roadmap) 13
5. Targeting and victimology 15
   - Espionage campaign roster 15
   - The Middle Eastern shared-hosting compromise 16
   - Reach into internal infrastructure 17
   - Scale 17
6. The financial operation 18
7. Infrastructure 19
8. Attack chains 20
   - Chain A: Government webmail watering-hole 20
   - Chain B: Direct malicious extension distribution 20
   - Chain C: Electron and desktop-application compromise 20
   - Chain D: Cryptocurrency SEO poisoning and phishing 20
9. Campaign results 21
10. Timeline 22
11. Attribution 23
12. Indicators of compromise 24
    - File hashes (SHA-256) 24
    - Network indicators 25
    - Host-based indicators 26
13. Detection and mitigation 28

1. Executive summary

- Jewelbug is a China-based threat actor that runs parallel operations: espionage campaigns against foreign governments and militaries, and a for-profit cryptocurrency fraud business. Both were administered from the same control panel.
- The group operates as a small development-and-operations team, with role-based access controls, a documented feature roadmap and five generations of command-and-control code behind it. Its activities point to a sustained operation rather than an ad-hoc crew.
- Its main payload is the Antino backdoor. It also operates a malicious Chrome/Firefox extension (“PDF Viewer”) backed by a hidden native-messaging shell. It also uses a Linux implant, targeted at servers and routers, which is a custom Rust backdoor (“ClientKing”) containing a kernel rootkit and a credential-stealing authentication module.
- The group recorded more than one million implant check-ins, 580,000+ stolen browser cookies and 2,300+ exfiltrated emails between February and May 2026.
- Espionage attacks targeted government entities in the Middle East, Southeast Asia and South Asia with confirmed executed intrusions.
- We assess with high confidence that Jewelbug operates from within China, most likely as a hackers-for-hire entity. The financially motivated arm is run as a registered Hunan company by a named individual.

2. Who is Jewelbug

- A small Chinese-speaking development-and-operations team, not a lone actor. The group's own documentation uses role-based reading guides, per-operator access controls and a feature schedule.
- Parallel operations, espionage and crypto fraud, are run side-by-side from the same panel by the same operator team.
- The framework is self-named XG-Web (module author string “Xg Team”); the broader actor is tracked by Symantec as Jewelbug.

Jewelbug is an APT group, most likely set up as a “hackers-for-hire” entity, running parallel operations. The espionage operation targets government communications systems and the service providers that host them. The criminal operation runs industrial-scale search-engine-optimization (SEO) poisoning that funnels Chinese-speaking victims to fake cryptocurrency-exchange sites and trojanized apps. The two operations share infrastructure, tooling, page-cloaking techniques and a single operator team, which is the defining characteristic of the group: foreign-government collection conducted alongside commodity fraud, from one panel.

The group's developer documentation drops the “authorized penetration-testing” pretense used in its boilerplate disclaimers and instead describes the system's functions in plain terms: “browser hijacking”, “data theft”, “man-in-the-middle attack”, silent webcam/microphone “ambient listening”, and social-media account hijacking to “bulk-send phishing links”. The same documentation makes clear the project was a port of an earlier NW.js desktop tool, meaning the lineage predates this codebase.

Two Missions, One Control Panel

JEWELBUG

Government espionage and crypto fraud, run by the same small team

XG-WEB • one React panel, one MySQL victim database

ESPIONAGE

Government ministries, police and military networks across the Middle East, Southeast Asia and South Asia

↓

Watering-holes on shared webmail, the Antino backdoor, ClientKing on Linux servers and routers

↓

Builds configured to beacon through the internal proxy of a major U.S. aerospace and industrial manufacturer

↓

Government communications, at national scale

CRYPTO FRAUD

Chinese-speaking cryptocurrency users, with decoys styled after Taiwanese government bodies

↓

SEO poisoning: an AI article generator, more than 40 content-management servers, click-fraud bots

↓

Hundreds of look-alike OKX and Binance domains, cloaked so crawlers saw the phishing content

↓

Profiting from cryptocurrency theft and click fraud

Both missions shared infrastructure, techniques and one panel. That pairing is the signature of a hack-for-hire entity running for-profit crime on the side.

THREAT HUNTER TEAM

3. Attribution and operators

The operators' real-name verification documents, including a business license for a registered information-technology company and a signed, stamped media-platform authorization letter, attribute the cryptocurrency-fraud and SEO arm to a named individual, the sole legal representative of a company. The company, registered in Changsha County, Hunan Province, China, in 2019, openly describes itself as an SEO business.

This individual used the handle "paopaodada" (泡泡大大) and the variant "paopaodada1", advertised on Telegram as the contact for a "website ranking rental" service against a Binance-branded image. The same handle, paired with the password 525xiaoxiao, was reused as the administrative login across a fleet of 44 content management servers and appeared as the registrant of a bulk domain portfolio.

Lure imagery on the phishing pages was generated through a Chinese artificial-intelligence image service whose embedded content-generation identifier ties the imagery back to the operator's account.

The cryptocurrency fraud arm is attributed to the above identity with high confidence. Whether the same individual operated the government espionage campaigns is not established. The two activities shared the same infrastructure, overlapping page-cloaking code and an aligned timeline, and the espionage and fraud campaigns were administered from the same panel. We assess it most likely that the SEO business supplied access, delivery and infrastructure into the espionage operation, rather than that one person performed both roles.

Operator tradecraft

The operators repeatedly test their stealer against their own browsers, with the result that they collect nearly as much information on themselves as on their victims: the cleartext password to a C&C panel, the panel's two-factor-authentication seed, live operator session tokens, bcrypt password hashes, the developer's Windows username and test hostname, and credentials for a Chinese-language hacking forum (t00ls[.]com). Development artifacts in the codebase include the phpStudy WAMP stack path, C:\phpstudy_pro\WWW\, the production path, /data/xg-web/backend/, and a developer LAN address that the implant's own code explicitly excludes from capture. (The operator secrets themselves are not reproduced here.)

The operators' virtual-private-network client is installed locally at D:\工作软件\vpn最新\ on a Windows NT 10.0.26200 host, and its logs show a working pattern concentrated between roughly 13:00–01:00 UTC+8, with the routing profile set to bypass mainland China destinations. This is consistent with an operator physically inside China. Installed software notes referenced Clash and Shadowrocket (Great-Firewall circumvention), AnyDesk/ToDesk, the LDPlayer Android emulator, the 同花顺 stock-trading client, Feishu, Baidu Netdisk and DeepSeek.

Telegram Desktop session data ties one of the operators to the account used to advertise the group's commercial services and, with medium confidence, to an approximate list of group memberships inferred from cached sticker-pack names.

4. Tooling and tradecraft

Key points

- XG-Web: a three-tier browser-centric C&C (React panel, Node.js backend, MySQL), with hybrid RSA-2048/AES-256 transport over WebSocket Secure with HTTP long-poll fallback.
- Antino: the group's Windows backdoor, delivered via fake Flash/Adobe installers and using the Microsoft Graph API for command and control.
- “PDF Viewer” extension: a Manifest V3 Chrome implant (Manifest V2 on Firefox) requesting nearly the entire dangerous extension API, with a CSP-bypassing offscreen sandbox and a generic browser-API remote-procedure bridge.
- `com.microsoft.runedge`: a native-messaging helper giving operators an OS command shell behind the browser.
- ClientKing: a custom Rust Linux/router backdoor (37 builds) with multi-transport C&C including a DNS tunnel, a kernel rootkit, a malicious PAM credential-stealer, and ASUS-router persistence.

The XG-Web framework

XG-Web follows a conventional three-tier C&C design. An operator panel (React 18, TypeScript, Ant Design 5, served by Vite on port 5173 behind an IP allow-list) talks to a Node.js/Express backend on ports 80/443. The backend persists state in MySQL 8 and is the rendezvous point for victim implants. Implants prefer a WebSocket Secure (WSS) channel; older framework variants degrade to 30-second HTTP long-polling (“Comet”) when WSS fails, though the newest analyzed production backend has no Comet fallback at all. All implant traffic is wrapped in an application-layer envelope: the server publishes an RSA-2048 public key, the implant returns a per-session AES-256-CBC key encrypted under it (RSA-OAEP/SHA-256), and subsequent messages are AES-encrypted inside the TLS tunnel. If the browser lacks Web Crypto, the channel silently degrades to Base64 only.

The panel exposes role-based access across three tiers (superadmin, admin and ordinary user operators, though the observed deployment only populated two of the three), with per-campaign access-control lists so junior operators see only their assigned victims. Principal views:

- Client (会话管理): Live victim grid with interactive JS console, screenshot, file manager and shell).
- Attack (攻击任务): Campaign builder that emits the one-line injection snippet.
- Generate Plugin: A button that builds a fresh extension with a non-burned C&C domain baked in
- Browser Management: Cookies, credentials, history, bookmarks, screenshots, clipboard, intercepted requests, header-rewrite rules and a shell executor.
- Gmail / Twitter / Discord / Zalo readers
- Domain (域名管理)
- Settings.

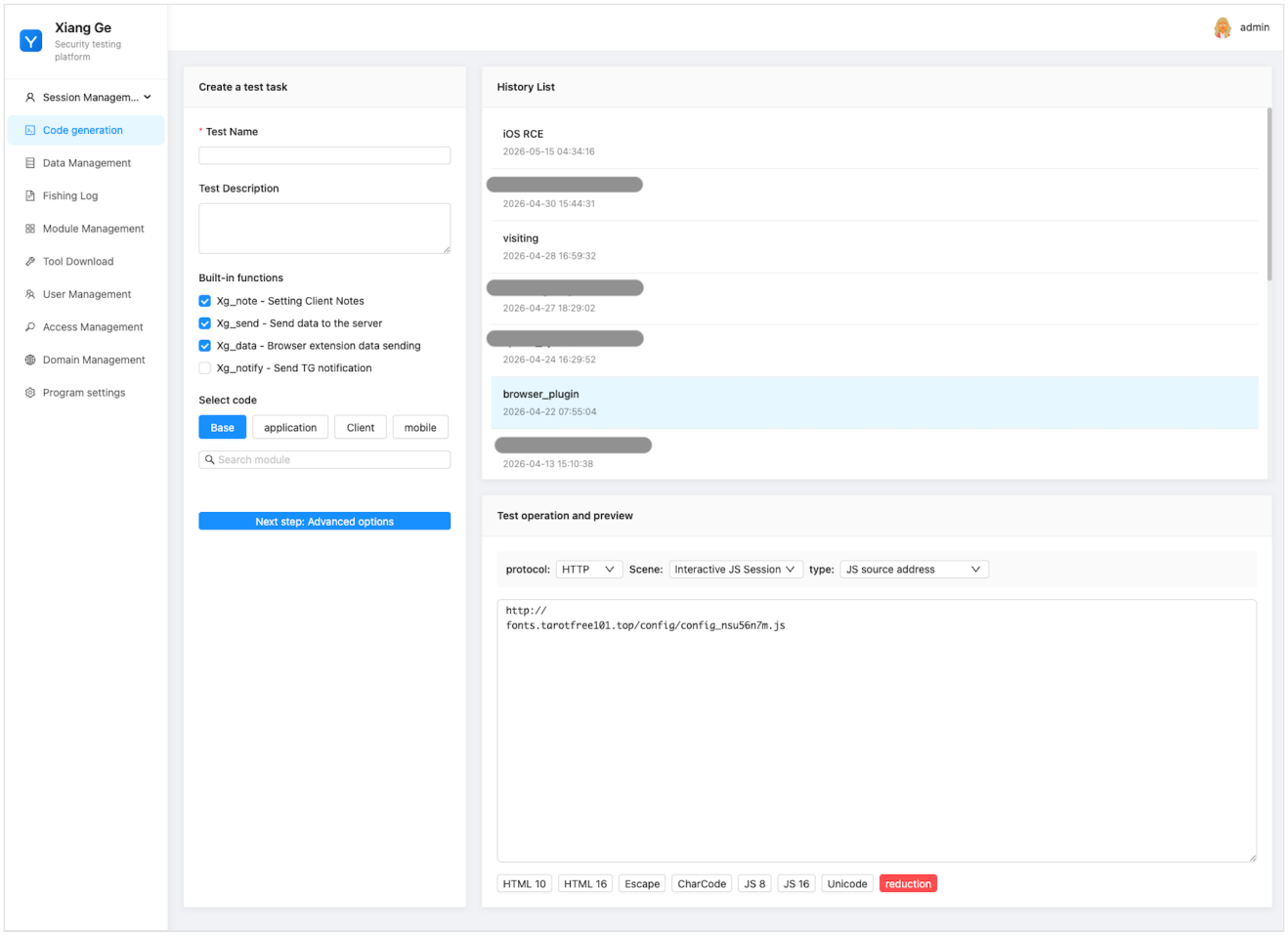

Figure 1. The XG-Web operator panel (self-described as “Xiang Ge — Security Testing Platform”), showing the campaign history list with government targets (redacted) and a live C&C payload URL.

“PDF Viewer” browser extension

The group's primary persistent endpoint implant is a Chrome Manifest V3 and Firefox WebExtension package it calls “PDF Viewer”. Its manifest requests almost the entire dangerous surface of the extension API, including:

- Cookies
- Debugger
- Scripting
- webRequest
- declarativeNetRequest
- nativeMessaging
- clipboardRead/Write,
- History
- Bookmarks

- The System.* Set
- Host access to <all_urls>

Because Manifest V3 forbids dynamic evaluation in the service worker, the extension creates a hidden offscreen document hosting a sandboxed iframe whose content-security policy permits unsafe-eval, and runs the full victim.js command loop inside it. The background service worker is a generic remote-procedure bridge: any api_call message naming a browser API path, method and arguments is reflected into the corresponding chrome.* call and the result returned, so an operator can invoke any browser function by name. A special case injects and eval()s operator-supplied scripts in the MAIN world of any tab. A 30-second keep-alive alarm defeats Manifest V3 service-worker eviction.

Collection capabilities:

Capability	Mechanism
Credential theft	content-script.js hooks login forms, monitors autofill and reads values on submit/blur/Enter, classifying fields with a multilingual regular expression (>12 languages incl. Simplified/Traditional Chinese).
Full cookie theft	chrome.cookies.getAll plus a live onChanged subscription for near-real-time session-token capture.
Network capture	An injected page hook (analytics-core.js) patches fetch/XMLHttpRequest to capture request/response headers and bodies.
Clipboard clipper	Copy/cut/paste hooks; an operator-set rule can silently substitute a copied cryptocurrency address (Bitcoin-address regex shipped) with the attacker's own.
Download hijack	advancedRouting cancels a matching download and re-issues it from an attacker URL with the same filename.
Header rewriting	A declarativeNetRequest ruleset the operator edits from the panel, to strip security headers or inject authentication headers on any site.
Offline staging	When the C&C is unreachable, the implant silently re-downloads files matching sensitive extensions (.docx .pdf .xlsx .sql .kdbx .ovpn .pem .key .p12 .env .ps1 …) and flushes them on reconnect.
App readers	twitter-dm.js scrapes X direct messages; modules render stolen Gmail, X, Discord and Zalo data in look-alike panels. Gmail harvesting watches for seven Google session cookies, enumerates logged-in accounts via the mailbox Atom feed, and pulls full messages server-side.

The native-messaging shell (`com.microsoft.runedge`)

To escape the browser sandbox, the extension talks to a small Windows helper (compiled from microsoft.hpp, a GUI-subsystem executable) registered as a native-messaging host under the misleading name `com.microsoft.runedge`.

On a {“action”:”execute”,”data”:”<cmd>“} message it runs the command through %ComSpec% /c with a hidden window and returns the output. The panel automates deployment end to end: it renames the chosen executable, uploads it and a host manifest to the OSS bucket, instructs the victim's extension to silently download both into the Downloads folder, then immediately erases the download history; the operator separately writes the enabling registry value. The backend applies per-build source polymorphism so each compiled helper has a unique hash.

The developers' own tooling included the open-source RedExt browser-extension C&C (a likely design influence) and HackBrowserData.

The `victim.js` hook and delivery

For initial access where the extension cannot be installed, the framework serves a polymorphic JavaScript hook (victim.js). It generates a persistent victim identifier (stored under a key mimicking the Baidu Analytics cookie), opens the WSS/Comet channel, completes the crypto handshake, and enters a loop that eval()s any run payload. Every request to the payload endpoint returns a freshly obfuscated copy (XOR'd with a random key, Base64, self-decoding stub with randomized variable names), so no two downloads are byte-identical. Matching template.hta, template.sct and template.wsc wrappers deliver the same hook through mshta.exe, regsvr32.exe and other Windows script-host binaries.

The attack attempts to blend in to normal webpage traffic. The URL paths are made to look like standard Webpack formed URLs (/dist/js/12.<8-hex>.chunk.js) and the C&C hostnames are typosquats of common resources such as Google Fonts (fonts.chrorne[.]com), so an injected <script> reads as a legitimate site asset. Initial-access delivery observed in the originating campaign also used the Antino backdoor and executables disguised as Adobe Flash and Adobe installers, served from attacker-controlled domains.

Command-and-control: dead drops, reputation self-monitoring, MITM proxy

- Google Docs dead-drop resolver (“C3”): Google application credentials and a long-lived refresh token are hard-coded in the source. On campaign activation the backend creates a public Google Document with an innocuous title, writes the obfuscated payload into the body, and records the document identifier. Implants fetch the document's plain-text export URL to execute the payload. Forty-five dead-drop documents span the tool's operational history; 13 were live and mapped to active campaigns at the time of May, 2026.
- VirusTotal self-monitoring. A scheduled job queries the VirusTotal domains API for each of the group's own C&C domains every 12 hours and tags any flagged as possibly malicious. The payload builder then avoids using any burned domains.
- Per-victim man-in-the-middle proxy. On demand, the backend allocates a port (10000–20000) and runs paired HTTP/HTTPS listeners that relay through the victim's browser extension, replaying the victim's own cookies, with leaf certificates minted on the fly by a panel-side certificate authority. The operator can then browse internal web applications exactly as the victim would.

The exploit-module library

The module library comprises close to 40 operator-authored JavaScript modules that are delivered to victims for execution:

- Xg.Basic.Cookie: Baseline collection of cookies, storage and DOM metadata.
- Xg.browser.fake.top: Rewrites the page into a full-viewport same-origin iframe so the hook survives in-application navigation (XSS-persistence).
- Xg.browser.keylogger: Captures committed East Asian input-method text via composition events.
- Xg.browser.webrtc.microphone: Abuses a microphone permission prompt and a relay-less peer connection to leak the victim's genuine internal IP address.
- Flash lure family: Gated fake Adobe Flash / browser update overlays that steer victims to a Windows executable on an attacker-controlled domain. Distinct variants exist per target set (Middle Eastern ministries, Southeast Asian foreign ministry, Southeast Asian army, Southeast Asian police administration, prison-visit system, etc.).
- “Note” auto-labelling family: Scrapes the logged-in username from each target application so new victims appear in the panel pre-labelled with their account identity.
- Xg.Exchange.Automatic.Fishing: An Outlook Web Access lure hard-coded for a list of 90+ South Asian police and government addresses.
- Xg.browser.imitate.fishing_msbuild: A fake browser-update lure for 20+ named Southeast Asian military personnel.
- Xg.Client.Node: File manager and child_process shell for victims running inside Electron/Node contexts.
- Xg.Zalo.Chat: Reads the Zalo client's encrypted SQLCipher databases and uploads them for server-side decryption.
- Xg.client.apifox.rce: An exploit for the Apifox API tool (≤ 2.8.21). By abusing permissive cross-origin settings, the exploit allows a watering-hole page to reach into a developer's running Apifox process and execute code.

Antino backdoor

Antino is Jewelbug's Windows backdoor. It was distributed through malicious HTML Application (HTA) downloaders whose file names referenced current geopolitical events, and through executables disguised as Adobe Flash and Adobe installers hosted on attacker-controlled domains such as microsoft-flash[.]com, www.wps-cn[.]com and www.f1ash[.]org[.]cn.

Its defining feature is that it uses the Microsoft Graph API as its command-and-control channel, so beacons and tasking ride inside ordinary traffic to Microsoft cloud services and are hard to distinguish from legitimate activity.

Antino samples have been recovered from infected hosts in the Middle East and submitted to public scanners from victims in the Middle East and South Asia, and is delivered by the fake-update lures used in the Middle Eastern government webmail campaign (see Attack chains). A second-stage download chain also retrieves it from a CloudFront URL and a Cloudflare R2 bucket (see Infrastructure).


CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Events

In Person Webcast

Indo-Pacific Forecast 2026

January 14, 2026 • 8:45 am - 12:00 pm EST

Geopolitics and Foreign Policy

This event is invitation only.Attendance is limited to invited guests, and registration is not open to the public.

How will the U.S. alliance network in the Indo-Pacific evolve next year? To what extent will tariff policy and tech competition shape regional economic dynamics? Will the regional balance of power tilt in favor of authoritarian states?

Join CSIS experts to explore these and other questions during our annual preview of political, economic,and security developments across the region.

Agenda

Keynote Address

8:50 am

- **Victor Cha,** President, Geopolitics and Foreign Policy Department and Korea Chair, CSIS

Theme 1: Architectures of Influence: Navigating competitive Order-Building

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

ClientKing: Linux and router implant

Where XG-Web infects victims via their browser, ClientKing targets Linux servers and network devices. The bucket held 37 builds of this Rust implant, compiled from one source tree and differing only in a per-target configuration block (C&C URL, 19-digit “listener” ID, optional egress proxy) stamped into each binary.

- Transports: HTTP, HTTPS, WebSocket, WebSocket Secure, and a custom DNS tunnel. TLS verification is disabled (any certificate accepted); the network protocol uses protobuf and the C2 URL path of /client/api/connection?listenerId=. Later builds front traffic through the AWS API Gateway.
- Anti-forensics: The implant immediately disables shell-history logging and obtains host information derived from /etc/machine-id and DMI identifiers.
- Operator commands: Interactive PTY shell, file operations, recon, SOCKS forward/reverse pivoting, userland (.so) and kernel (.ko) module loading. Later builds load kernel modules directly from memory via the init_module syscall, with one build further refining this to finit_module.
- Companion rootkits: A loadable kernel-module rootkit named `clientking`; a userland rootkit hidden via /etc/ld.so.preload masquerading as libgcc.so/libhandle.so; a malicious PAM module `pam_security.so` hooked into sshd, su and sudo for credential theft; and init persistence at /etc/rc.d/assist with hidden install directory /usr/local/share/.assist and shell-rc marker pq9i75DhW1.
- Targets: x86-64 servers, AArch64 devices, and ASUSWRT consumer/small-office routers (persistence via /jffs/scripts/wan_start and services-start).
- Development timeline: six generations from October 2024 into mid-2025, trackable by listener IDs and compiler versions.
- Recent intrusions: three of the most recent builds were hard-stamped with the internal corporate egress proxy of a major U.S. industrial and aerospace manufacturer, with the operator iterating on egress configuration.

ClientKing's C&C server and the XG-Web C&C server are hosted in the same network range (43.246.208[.]0/24), which ties the browser framework and the Linux/router backdoor to one actor.

Other content

- Off-the-shelf Linux backdoor: A VMProtected Rekoobe/TinySHell derived backdoor (raw-TCP + OpenSSL + PTY shell) first seen in March 2024.
- HTML/JS cloaker (traffic-distribution system): Two near-identical jsjiami.v7-obfuscated landing pages gate visitors against an allow-list of 60 throwaway domains and render the real phishing content inside a full-screen iframe, part of the crypto-phishing arm.
- Android packages: Truncated fragments of the legitimate OKX exchange Android app appear in the group’s staging tooling.

Planned capabilities (developer roadmap)

The group's internal documentation lists features it intended to build next: a full keylogger; real-time screen capture/recording with server-side optical character recognition; geolocation tracking; a clipboard monitor;

network-traffic analysis; silent webcam and microphone capture (“ambient listening”); social-media account hijacking with automated phishing-link distribution; persistence hardening with extension masquerading, and AI-driven triage of stolen data to flag high-value victims (API keys, private keys, payment-card and identity data).

5. Targeting and victimology

- Espionage campaigns, named by the operators themselves, targeted government and military bodies across the Middle East, Southeast Asia and South Asia.
- Confirmed executed intrusions include a Middle Eastern government webmail system, a Southeast Asian foreign ministry system and a senior Southeast Asian justice ministry mailbox.
- Evidence of a separate ClientKing configuration against a major US industrial/aerospace manufacturer
- A parallel stream targeted Chinese-speaking cryptocurrency users; decoy and email artefacts also point to interest in Taiwan.

Espionage campaign roster

The attacks table in the control panel is the most direct statement of intent, because each row is a campaign the operators created and named. Fifteen campaigns (plus two later deleted) mapped to:

Operator's campaign name	Target	Location
[REMOVED]	Ministry of Defence webmail	Middle East
[REMOVED]	Ministry of Interior webmail	Middle East
[REMOVED]	Ministry of Foreign Affairs	Middle East
[REMOVED]	National networking services agency	Middle East
[REMOVED]	Government correspondence portal	Middle East
[REMOVED] hosting panel	Middle Eastern state telecoms hosting control panel	Middle East
visiting	Ministry visitor-pass / prison-visit system	Middle East
[REMOVED]	Corrections Ministry	Southeast Asia
[REMOVED]	Southeast Asian army intelligence	Southeast Asia
[REMOVED]	Southeast Asian police electronic-correspondence system	Southeast Asia
[REMOVED]	Ministry of Foreign Affairs document-tracking system	Southeast Asia
[REMOVED]	Navy	Southeast Asia
案件 (“case”)	Mixed / crypto-fraud back-ends	China
传销案件 (“pyramid-scheme case”)	Fraud-related	Domestic
browser_plugin	Generic malicious-extension distribution	—
ios rce / iOS 钓鱼案件	iOS phishing	—

Two further target sets appear only in exploit-module allow-lists: 90+ South Asian police and government addresses, and 20+ named Southeast Asian military personnel. Victim records additionally confirmed an

executed compromise of a senior Southeast Asian justice ministry office, including full access to their Google mailbox, internal bookmarks and an internal document tracker.

The Middle Eastern shared-hosting compromise

The largest Middle Eastern campaign did not breach each government ministry separately. The group compromised the shared web-hosting platform operated by a state telecommunications provider and national network-services agency, obtained write access to the common webmail installation, and inserted a single script, planting a watering-hole on every government, university and foundation tenant on the platform at once.

Victim records for the campaign span 15+ government webmail tenants (covering Defence, Finance, Interior, Foreign Affairs, the Central Bank, Higher Education, Local Administration, Agriculture, Transport, Energy, Post and several regional councils) plus universities and private foundations. Two companion campaigns hooked the hosting control panel used by the telecoms provider's own administrators and the agency that runs the country's government infrastructure, i.e., the group also hooked the provider's staff to harvest the credentials that granted write access in the first place.

Reach into internal infrastructure

On at least one victim, a hosting administrator at the national network-services agency, the deployed implant was the “PDF Viewer” extension and its com.microsoft.runedge native shell, not only the lighter watering-hole hook. The extension's own telemetry tables record it being used to reach internal systems: authenticated traffic to a virtualization-management cluster inside the Middle Eastern government network, complete with anti-forgery tokens and captured by the extension's request hook, and credentials the administrator pasted into internal firewall and appliance login pages, captured by its clipboard sniffer. This extension-only telemetry from the host is direct evidence that the “PDF Viewer” extension, not merely the victim.js hook, was deployed in the Middle Eastern campaign, and shows hands-on enumeration of internal infrastructure from that foothold.

Scale

Runtime server logs recorded approximately 1.1 million connection-geolocation events against roughly 4,300 distinct source IPs across the March to May 2026 active period.

Traffic clustered heavily in government and military network ranges: approximately 87,200 connections from a Southeast Asian country (2,451 distinct IPs, predominantly state-telecom and military-network ranges), approximately 53,100 from a Middle Eastern country (1,015 distinct IPs within the national telecommunications carrier, spanning all regions including Starlink-connected addresses in the capital suggesting diplomatic or high-value targets), and approximately 15,148 from a second Southeast Asian country (14 distinct IPs including addresses registered to a government telecommunications ministry).

Among non-victim infrastructure connections, a ProtonVPN Singapore exit node accounted for approximately 3,900 panel-access sessions, consistent with routine operator VPN use for C&C monitoring.

6. The financial operation

- Run as a registered SEO company advertising a “search-ranking rental” service, monetized through fake OKX and Binance portals and trojanized apps.
- Automated attack pipeline: scrape keywords → AI-generate thousands of fake download pages → publish across a 44-server content-management fleet and hundreds of lookalike domains → click-fraud bots manipulate rankings → cloaking shows crawlers the ‘high-quality’ webpage content while users are redirected.
- Evolved from earlier black-hat SEO spam (medical/surrogacy themes) done in 2024 into cryptocurrency phishing before becoming entangled with the espionage toolkit.

The financially motivated arm is run as a commercial business in its own right. The pipeline used the Shuimiao (水淼) keyword-and-URL harvester to collect cryptocurrency search terms, an AI article generator (365jz and related tools) to produce thousands of plausible fake “OKX/Binance download” pages, and a content-management fleet of 44 servers run under a single credential set (paopaodada / 525xiaoxiao). Beyond cryptocurrency, the operator runs additional active lure verticals: sports betting and football (足球) templates, pirated livestream portals (直播/JRS), private detective service scams (侦探), and a donation/charity fraud set (捐). One live deployment, the self-branded “XXFSEO” PHP site-cluster engine at haoxizhiye[.]com, confirmed one of the operators maintained active web infrastructure separate from the primary cryptocurrency phishing domains. Seven-plus Selenium-driven click-fraud bots (“必应多线程” / Bing fast-rank, plus a Baidu equivalent) searched target keywords from rotating Chinese residential proxies, moving the mouse along randomized Bézier curves, typing with human-like delays, and rewriting the top organic result's link to point at the group's lure domains before clicking. The residential-proxy service used was a commercial provider (juliangip[.]com).

The group registered hundreds of lookalike `.com.cn` domains impersonating OKX (欧易) and Binance by combining the exchange names with popular Chinese platform names (iQiyi, Youku, Douyin, Zhihu, etc.), supported by a link farm of 2,300+ throwaway subdomains. Phishing pages were cloaked with a PHP snippet that redirects search engine crawlers to the live bait content domains while ordinary users were sent elsewhere, the same cloaking technique used in the espionage panel. Lure imagery was produced with a Chinese AI image-generation service. Fake-Binance clone sites and disguised Android packages rounded out the kit. The same files show the business evolved from earlier black-hat SEO spam (surrogacy/medical-aesthetic themes around 2024) into cryptocurrency phishing.

7. Infrastructure

Category	Detail
XG-Web C&C / panel domains	fonts.tarotfree101[.]top (primary), fonts.chrorne[.]com, robot.avbliud[.]com
XG-Web C&C server	43.246.208[.]236
Payload / phishing-log domains	microsoft-flash[.]com (also the phishing-hit logger), www.wps-cn[.]com, www.f1ash[.]org[.]cn, browser-update.pages[.]dev, eastus2.wac-azure[.]com, mailbycloud[.]com
Antino payload URLs	hxxp://d2nq35tel3ucuo.cloudfront[.]net/LtVGUSsyUTDA.log; hxxps://pub-abfa7742e315485a98a5fafd6dbfb68e.r2[.]dev/hjgzBskgslc.dll.iwq
ClientKing C&C	www.jkskhei[.]com (:80/:443), ns1.jkskhei[.]com (DNS tunnel), dns.wizkidblogger[.]com, r6fi2yvqql.execute-api.ap-southeast-2.amazonaws[.]com; IPs 43.246.208[.]179, 47.84.37[.]113; build-distribution panel 47.84.51[.]173:1880
Other observed C&C	SOCKS proxy (cherry-ai.exe): 167.71.195[.]255, 38.12.1[.]47, 129.212.237[.]224
Operator login addresses	Panel allow-list 47.87.71[.]167, 47.250.208[.]35 (Alibaba Cloud), 219.76.254[.]184 (PCCW Hong Kong); dev whitelist 192.168.73[.]129, dev LAN 192.168.1[.]171
Operator egress (attribution)	Self-hosted VLESS/REALITY nodes on tkstream123[.]com (node names prefixed xgzz/zz), plus 195.172.120[.]227 and 103.27.77[.]10; China firewall bypass via sttlink[.]com subscription using nodes on bieqiang[.]xyz / badns[.]help / aws.baidupi[.]top
Residential proxy accounts	juliangip[.]com
SEO/phishing infrastructure	365jz content-management system, 44 servers under paopaodada/525xiaoxiao; hundreds of OKX/Binance look-alike .com.cn domains; 2,300+ subdomain link farm; DNS via dm1.longmingdns[.]com / dm2.longmingdns[.]com; fake-Binance clones usnbweb[.]mobi, eoycqqcyix[.]com

8. Attack chains

Chain A: Government webmail watering-hole

- Preparation: The operators register C&C domains, create a campaign, and attach a cookie module and an auto-labelling module. Saving the campaign triggers the C3 subsystem to create a public Google Doc holding the obfuscated payload; in parallel the operators stand up a file-hosting server on a group domain and upload the second-stage executable.
- Initial access: The group compromises the shared hosting platform's webmail template and inserts a single disguised script tag (<script src="https://fonts.chrorne[.]com/dist/js/12.qgfvjzvs.chunk.js">), watering-holing every tenant.
- Foothold: A ministry staff member logs in; the hook reports in, exfiltrates cookies, and labels the new victim with their government email address.
- Escalation lure: The "flash" module overlays a fake Adobe Flash update prompt for in-scope targets and steers the victim to https://microsoft-flash[.]com/download/Adobeinstall.exe.
- Persistent implant: The downloaded executable is the Antino backdoor, a fake Flash or Adobe installer that beacons to the Microsoft Graph API and was recovered from infected Middle Eastern hosts. On this chain it also side-loads the "PDF Viewer" extension, drops the native-messaging helper and writes the enabling registry value (HKCU\SOFTWARE\Google\Chrome\NativeMessagingHosts\com.microsoft.runedge).
- Actions on objective: Operators gain full browser access and, via native messaging, host command execution; in at least one case they reached an internal virtualization management cluster.

Chain B: Direct malicious extension distribution

The operator clicks "Generate Plugin", which builds a fresh extension with a non-burned domain, and distributes it through social engineering (or, for the financial campaigns, the fake-exchange download network). The extension grant alone yields complete browser visibility; operators can escalate to the native shell using the OSS-staged deployment.

Chain C: Electron and desktop-application compromise

For victims running Node-enabled desktop apps (most prominently the Zalo client), the Xg.Client.Node.* and Xg.Zalo.Chat.* modules provide a file manager, command shell, and theft of Zalo's encrypted message databases for server-side decryption.

The Apifox module reaches from a watering-hole page into a developer's locally running Apifox process to achieve drive-by code execution.

Chain D: Cryptocurrency SEO poisoning and phishing

The SEO pipeline causes search engines to list fake cryptocurrency exchange pages; a Chinese-speaking user searching for OKX or Binance lands on a lure page and downloads either a trojanized desktop client (Chain C delivery) or the "PDF Viewer" extension (Chain B). Either way, the operators harvest exchange session cookies and credentials.

9. Campaign results

We collected the following stats, which reveal some interesting details about the scale and nature of the campaign's data collection.

Data store	Approx. rows	Contents
clients	1,018,930	Implant beacon log (≈ several thousand distinct victims)
gmail_cookies	833,778	Harvested Google session cookies
browser_cookies	580,488	Full victim cookie jars
offline_history	38,330	Buffered browsing history
browser_downloads	17,014	Download logs
browser_requests	6,926	Captured request/response pairs (incl. internal-network traffic)
offline_passwords	3,428	Form-grabbed credentials (offline queue)
gmail_attachments	3,172	Exfiltrated attachments
datas	2,958	Generic exfil store
gmail_emails	2,332	Full exfiltrated email bodies
browser_credentials	1,694	Captured username/password pairs
browser_proxy_logs	940	Requests relayed through victims
twitter_cookies	595	X session cookies
browser_extensions	220	Victim extension inventories
exploits / attacks / c3_google_docs / domains	37 / 15 / 13 / 3	Module library, campaigns, dead drops, C&C pool

10. Timeline

Date	Event
~2024	SEO-fraud business active (medical/surrogacy black-SEO themes, per work-file timestamps)
2024-10 → mid-2025	ClientKing development across six generations (Linux → static builds → AWS API Gateway fronting → ARM64/ASUS routers → per-victim proxy stamping, incl. the manufacturer intrusion)
2026-02-11	Earliest dated XG-Web artefact (“xg-lite” initial port from NW.js desktop)
2026-03-16 → 2026-03-31	Documented XG-Web feature sprints: Gmail and X hijack, download/clipboard hooks, code obfuscation, VirusTotal domain rotation, per-operator access controls
2026-02 → 2026-05	Espionage and fraud campaigns active (campaign creation dates span Feb–May 2026)
2026-05-17	Database backup

11. Attribution

We assess with high confidence that Jewelbug is a China-based hackers-for-hire entity. The attribution is supported by government-issued documents belonging to the operators that map to a registered Hunan company by a named individual.

12. Indicators of compromise

File hashes (SHA-256)

```
e6ff096a0562c0042b09d250bd60272ffcd8d72bd95c563842acf765a8dc8bcf  Resolution on the Updated Chart
of Bajo de Masinloc.hta (HTA downloader)
01b5c6acb20e41799a0e96d9d1d6e1c44791883706b6285e874fcb15cc93b31a  HTA downloader (Russia/Venezuela/
Ukraine lure)
e809da86bd81463347fa7f922d3e088755a94a331889d32acb55aa8f57778a34  CSIS Indo-Pacific Forecast
2026(Event Details) (1).hta
f1ef5fe4c0cdcff13cc750c867728b89719f81437bdc49041edd1ae1f3edb4e8  TEST.hta (Antino downloader)
e2eb7703047b37b28dc34e6990205d758a2454b39bc655b460606745fadcb530  slc.dll (Antino)
e7e3b0bcd6798634adf8b49d305f3a7b7682e4b76db549682a183c5a186df4bb  Vb0c44dfslc.dll.wxb (Antino)
09ef7c736bccfafefc44d9910d499173b88063b73b221fc0dc9e9105107e5cff  Antino sample
c11714f9fe2df1ca906585c81498cd77f5ec05b132aab73fa3a71d71d71e42cc  Antino sample
b90a4e770869c28fd2140acb3ebdc50c113bb6f096b4bbdb9ac87c349c70e85e  flashcenter_pp_ax_install_en.exe
(fake Flash / Antino, Middle East)
0c39264337a1186b2e765e24073399cbdcba118306614eb411e315887af578bd  Antino (Microsoft Graph C&C, from
microsoft-flash[.]com)
9b7df409c9a89f7536d3ba7b6d43fb6dbac618c8bb52615ba34cc971ad71bbf3  Adobe_installer (1).exe (Antino,
South Asia)
153d077bcb58e00f5746573cba25f6b0788b809bf7b2a52fca0dc22d3bb5c94e  Antino-related (infected Middle
Eastern host)
297413a3e49e7353bf484a3eb15ec647de729211059df8fc68678d2378b6f561  Antino-related (infected Middle
Eastern host)
30f5122cc199b9c2e524503b343a9ee13a6f9773dcbc1df82c8b25ad20bca61d  Antino-related (infected Middle
Eastern host)
430f12970f8d58f12edccee9019a1aa90fa232c961449bdcc69c8d348a52cf55  Antino-related (infected Middle
Eastern host)
5ccdf53881f6c758af8d94fe67066af209b4bc0a3cb80b6a4c724fad86eb97ef  Antino-related (infected Middle
Eastern host)
5edb8d1023b8babf302871b68fa2b26d5ca57633f64951922998e8f1d6c8f7ac  Antino-related (infected Middle
Eastern host)
6d5fe6b6a34eeb470798b970b70f41a07ccf59b22f49ad9b3dfff7aa3256f3c2  Antino-related (infected Middle
Eastern host)
97c3a6be1711c5340d8806e4a54f7297f3f763d0aa4240b667f1e4e1f98f2aad  Antino-related (infected Middle
Eastern host)
ac3d453d3c9b0310ebb8a67cef35e2ac954d4acdf70cf497fe43a02c7a510813  Antino-related (infected Middle
Eastern host)
e782a6d4919f194d41e524ebd6df5894197043cf772fcf60455127b246f302c0  Antino-related (infected Middle
Eastern host)
ea893abf20b00d9bfc042a88fbf7b4bd42e68ce07c116d3e3b002e5b4a853877  Antino-related (infected Middle
Eastern host)
ed96e7f1085a50251eb8967ac53777272a617831084f0edad8a769c583a18869  Antino-related (infected Middle
Eastern host)
```

Network indicators

```
fonts.tarotfree101[.]top                      XG-Web C&C / panel (primary)
fonts.chrorne[.]com                           XG-Web C&C (Google Fonts typosquat)
robot.avbliud[.]com                           XG-Web C&C
43.246.208[.]236                              XG-Web C&C server
microsoft-flash[.]com  (103.87.9[.]62)        Payload delivery + phishing-hit logger
www.wps-cn[.]com                              Fake-Flash delivery
www.f1ash[.]org[.]cn                          Fake-Flash delivery
browser-update.pages[.]dev                    Fake browser-update lure
eastus2.wac-azure[.]com  (152.42.174[.]151)   Malicious C&C (Cloudflare-fronted)
mailbycloud[.]com                             Operator-controlled domain
www.jkskhei[.]com  (:80/:443)                 ClientKing C&C
ns1.jkskhei[.]com                             ClientKing DNS-tunnel C&C
dns.wizkidblogger[.]com                       ClientKing DNS-tunnel C&C
r6fi2yvqql.execute-api.ap-southeast-2.amazonaws[.]com   ClientKing C&C (AWS API Gateway)
43.246.208[.]179                              ClientKing C&C server
47.84.37[.]113:8080                           ClientKing C&C server
47.84.51[.]173:1880                           ClientKing build-distribution panel
167.71.195[.]255 / 38.12.1[.]47 / 129.212.237[.]224   SOCKS proxy C&C (cherry-ai.exe)
47.87.71[.]167 / 47.250.208[.]35 / 219.76.254[.]184   Operator login addresses (panel allow-list)
hxxp://d2nq35tel3ucuo.cloudfront[.]net/LtVGUSsyUTDA.log                          Antino payload
hxxps://pub-abfa7742e315485a98a5fafd6dbfb68e.r2[.]dev/hjgzBskgslc.dll.iwq       Antino payload
```

```
Google Docs dead-drop document identifiers
```

```
Payload at docs.google[.]com/document/d/<id>/export?format=txt
```

```
1--R8Dz3UNLVYrs6nRpxxhzC2nZ6I1nLsB4VSokVttqw
1A-zCyFokpUjyEfC47-TDzIsQYSG7lv7EO-Q0oCFO0zo
10G_ngLhLP0g0-ebVLHXvYt5C8vi67SXKPD_p4fRoUQU
1a859lrBUdj5evji0DJ21juaD9g7MJEfji-HvHkJ0EQ8
13dLhDfazg-l-EW3rtMYtcbG60RN505LiTRvxsS41kIk
1A8Ej5yCSRodKT9pD4mpsIuVvH361yByueAzMQzgYr4o
14-W65hspkAAAgaHr54M9Ccw2RiRM38RsZipAp87EpM4
1BbrdCQiLZ6xBe4ID0V9SyQJtVPbXwVIqoRNaC54tuGU
14fYTVMMkMps4kRFxffXU86k5-2hD8N8aVUwxVVGu7AE
1cJPHqKsOTZFHMEMzUTCVDE3KC0Q1c0quj6bQhRRSju0
14ghr2xR8rNiaq5M8Cw7ee_SzfxHA_DBabgS841YYcV8
1DkOHxHSPpnLAK7uyUeAuXeTurSzxC3UfPWKnC5Wf3MA
16vPxwILnG3zhDGKcCVY9QfwNSNuLytj9HpovmiCGW_8
1DRkLv-RNR-ojoBc47WDMg5giWJ8rtlfvea5Ec0j68_o
1enhBG7zJsymlK5bG7jaxqKbbx6WhZ01CtwKLb6cUaKo
1EsJfm4K_68rffWbpQdkX9LR_px7ntQbqDe5C0r8Wl6o
1ExIJXpL55CJ7-3UjY3FJW7O-3Nx8sNMlHUsrcNzH2ds
1g65-1ScmWFa0U3Gkbbo52SXG2Mq54OIQDQfqlllolno
1g_J-DE4xUxV1a5B-tRPwFoK165gJyXGpPSmtITWO1uQ
1Ga3WLSIPaKSoELw0Q0ToiOCu5oiiDh3u_A0St4vtCNk
1gy7WRu3ZnkKmbKLgXfovhXQ2qJ0DQNDmwsGgfsfgUiU
1j1nz6WwEQWFyTcIGRv2tcLjuQlaqiYccivYa4YTY6nk
1kMJcSDVCk-HD1hDtby9zAvneBUCx0oEVXm2eBK-PfaI
1lb9MmSufzyv09AjvfTrtBy51kbXHENe7np_qlv2Tk8k
1mSgQsJR1hkwXhjw6jE4OnbWYlRahqRh2k71A2eHcD5E
1NzZfi-oPhAQt7Qt38jPyG3ipj5tK7W-e75Plbihnci4
1oTrKoOmP9nP4LPiCMrsOLyF9N0vlFk2C-bH3m89zbgA
1pFT79JyBFxJDmzBRhiHCC2RuFZuTxZq6zB2YaFI8Ofo
1pGgRx3oPkEk79GkSFd27n6KSwsBcc_x8Gxco3eTMios
1pp9BAl6jpeVERhSstUqPmznGHRPBYJoE2WF4qMgvqvQ
1q3iiJ5t4DQabysux4QBW7_tG9aJZ5Cz2ftY8DkF7wJE
1qb5oczfzdRMlOUWgb0F00FBsx4hY6LBvbauvA5w9vnc
1SbSWICXt9LkBZ69eyHFEW8b6ONo-d4f6GrtjLutH1m4
1st_o_H9w1lRFa14rWuIFTR46obNOuBep9eB5UvtVZRM
1uAHADCl1TsHSLmJOhFg9zTKLQftTUyO0Y3l5_GtyiTQ
1wAHfVom6f9ChGqEuxZt5Rg811w-z71loZ9cFQWl50yA
1Wh_Kr7nqeTNKPbagYOe2v7Gcx8dLD44B1ldZKZ5VUSg
1wmCCusolwzf814P5pqHVsjK6E0I_7hDNWRB7vAwA7JI
1XiqV4o0v1XKJF95LexyHtZTDnnBiqdj3NYEFlAR9s1U
1xPBH9aAFlRz6RUFbnhIKQWam1L-GBmr0tTLdt8LGbWw
1YzEruVOR9K-rIByqbl70wBHPKhvM3TcixRKoA2weL5s
1Z0OsZFxVBz4ESHG009pkecS9KyOMHH7sGEU7bPiarb0
1ZCss0wm6AEuGATv7prydk_3Lk2fzcfrIbiH513vZSLs
1zLdzKunW-IRWziFGHegVSXohnTc6ugSF9pWeZj7Qzj4
1ZPxwFyDhbhW2hJpoZYiWRtK3pkxkNjdb8Ii4NI0MpmY
```

Host-based indicators

```
Windows (browser implant / native shell)
```

```
Browser extension:  “PDF Viewer”  v2026.5.13.1  (desc “Portable Document Format”; Firefox ID pdf-viewer@example.com)
Native host:        com.microsoft.runedge
Registry:           HKCU\SOFTWARE\Google\Chrome\NativeMessagingHosts\com.microsoft.runedge
                    HKCU\SOFTWARE\Mozilla\NativeMessagingHosts\com.microsoft.runedge
Files:              %USERPROFILE%\Downloads\microsoft.json
                    %USERPROFILE%\Downloads\microsoft_setup_<epoch>.exe
                    %USERPROFILE%\Downloads\microsoft_config_<epoch>.json
Storage keys:       localStorage Hm_lvt_$, _domain_google_mark; cookie Hm_lvt__<32-char>
Observed extension IDs:  kijgcnllicmahabnlhpomdlgnjnhnloe, kcadidgfgpkkogolajeofgbfnoadiccj, popoijcenfhnkdfeppmjfbmjankcpojl
Second-stage filenames:  Adobeinstall.exe, Adobe_install.exe, Adobe-install.exe, Adobe_installer.exe,
                         flashcenter_pp_ax_install_en.exe, flashcenter_pp_ax_install_cn.exe,
                         Browser_installation.exe, shellcode_load.exe, cab.exe
```

```
Linux (ClientKing and companions)
```

```
Process name (set via prctl):  client-king
LKM rootkit:                   clientking
ld.so.preload entries:         libgcc.so, libhandle.so
Malicious PAM module:          pam_security.so   (in /etc/pam.d/{sshd,su,sudo})
Persistence:                   /etc/rc.d/assist ; /usr/local/share/.assist
Markers:                       pq9i75DhW1 (in ~/.bashrc, ~/.zshrc) ; /tmp/.tmp.pq9i75DhW1
Router persistence (ASUSWRT):  /jffs/scripts/wan_start ; /jffs/scripts/services-start
```

13. Detection and mitigation

Key points

- Hunt for the “PDF Viewer” extension and the `com.microsoft.runedge` native host; alert on a browser process spawning `cmd.exe` over anonymous pipes.
- On servers, hunt for the ClientKing host artefacts and the `pam_security.so` / ld.so.preload rootkit footprint; review ASUS routers for /jffs/scripts persistence.
- Block the network indicators; alert on extension-initiated fetches of Google Docs export URLs and outbound PUT to the OSS bucket.
- Targeted organisations should audit webmail and intranet front-end templates for unauthorized script injection and deploy a content-security policy that would block external loaders.

Browser fleet. Enumerate installed extensions across managed Chrome, Edge and Firefox and alert on any extension (especially one named “PDF Viewer”) holding nativeMessaging, debugger, cookies and <all_urls> together. Alert on creation of the com.microsoft.runedge native-messaging host keys and on any native-host manifest path resolving into a user's Downloads folder. A cmd.exe process whose parent is a browser and whose handles are anonymous pipes is a high-fidelity native-shell indicator.

Servers and network devices. Hunt for the ClientKing process name, persistence paths and markers above; for the pam_security.so PAM hook on sshd/su/sudo; and for the libgcc.so/libhandle.so entries in /etc/ld.so.preload. Review ASUS routers for unexpected /jffs/scripts/wan_start and services-start entries. Treat any host beaconing to the ClientKing domains/IPs, including via DNS to *.jkskhei[.]com, as compromised.

Network. Block the indicators listed above. Alert on requests to docs.google[.]com/document/d/<id>/export?format=txt initiated by a service worker or extension rather than a user navigation, and on outbound PUT requests to *.oss-cn-hongkong.aliyuncs[.]com from user workstations.

Targeted organizations. Audit webmail and intranet front ends for unauthorized template modifications, rotate hosting-control-panel, firewall and virtualization credentials where the browser foothold reached internal systems, and deploy a content-security policy whose script-src directive would block external loaders such as the typosquatted font domains and Google-Docs payloads. Apifox users should upgrade beyond 2.8.21 and restrict the local mock server on port 4523.

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