SECURITY ADVISORY

CYBER STASH

October, 2025

China-Linked Espionage Threatening Asia-Pacific Critical Communications

Context

The China-linked threat actors are intensifying espionage campaigns across Asia, with telecommunications providers and government networks as prime targets. These operations leverage modernised versions of PlugX, Bookworm, and Turian loaders, all sharing stealthy DLL sideloading and advanced in-memory decryption pipelines. By compromising telecoms and their service providers, adversaries gain access to subscriber data, network management systems, and interconnection gateways—delivering both intelligence and operational leverage.

The tradecraft—spear-phishing, stealth persistence, and credential harvesting—enables long-term footholds that are difficult to detect or eradicate. For enterprises, this represents a sustained risk of data exfiltration, service disruption, and systemic exposure across critical infrastructure. What makes this campaign particularly dangerous is the convergence of multiple malware families into a shared ecosystem of loaders and toolkits, enabling adversaries to scale operations with minimal innovation. This ecosystem approach ensures persistence across borders, sectors, and technologies—posing not just a cybersecurity risk, but a direct challenge to regional resilience and national sovereignty.

Mitigation

Defence measures centre on three immediate priorities: stop DLL abuse, expose in-memory loaders, and contain lateral movement through segmentation and supply-chain controls.

Sideloading Controls — Enforce application allow-listing and restrict writable paths alongside signed binaries to block adversaries from hijacking legitimate executables.

In-Memory Threat Detection — Deploy EDR tuned for reflective loading patterns (VirtualAlloc, WriteProcessMemory, RtlDecompressBuffer) to expose stealth payload injection.

Supply Chain and Telecom Hardening — Monitor vendor and MSP access, apply least-privilege, and restrict egress to known destinations to cut attacker lateral reach.

Technical Details

Overview

The campaign combines a Korplug-style PlugX variant and a modular Bookworm RAT (plus parallel Turian activity). Delivery is via weaponised archives/installers; execution leverages DLL search-order hijacking to load malicious DLLs adjacent to signed binaries. Loaders retrieve an encrypted blob, apply an XOR —> RC4 —> LZNT1 transform, and produce an in-memory PE that is mapped and executed. The end result: minimal on-disk artefacts, high stealth, and easy reuse across victims.

Loader Mechanics

Staging & placement

Attacker drops a malicious helper DLL (or packaged archive) beside a trusted signed EXE (e.g., third-party helper/"Mobile Popup" apps).

- **Detection:** new/unknown DLL filenames in application directories; unexpected writes adjacent to signed binaries; ARP/manifest mismatches.

Blob retrieval (disk/resource)

Loader opens a hardcoded filename (*.dat, *.afx, etc.) or embedded resource and reads an encrypted blob directly into memory (no standalone EXE is written).

- **Detection:** processes opening non-standard blob files in program folders; uncommon file extensions accessed by signed EXEs.

Decryption pipeline (XOR —> RC4 —> LZNT1)

Multi-stage transform: simple XOR pre-pass (single-byte or repeating key) —> RC4 stream cipher (static/semi-static keys observed) —> LZNT1 decompression via `RtlDecompressBuffer`.

- **Detection:** presence of RC4 key-scheduling loops, simple XOR loops, or runtime calls to `RtlDecompressBuffer` immediately followed by memory mapping.

In-memory mapping & injection

Loader resolves APIs dynamically, creates/uses a legitimate host process (suspended), allocates RWX memory (`VirtualAlloc`), writes the decompressed PE (`WriteProcessMemory`), fixes relocations/imports, then resumes execution or spawns a remote thread (`CreateRemoteThread`).

- **Detection:** API call sequences: `VirtualAlloc` —> `WriteProcessMemory` —> `CreateRemoteThread` (or `NtCreateThreadEx`) and high-entropy memory regions shortly after `RtlDecompressBuffer` usage.

Key Families Driving the Campaign

PlugX Variant

- **Config & modularity:** Non-standard config layout (Korplug-style) supporting plugin indices, C2 fallback lists, and plugin stubs (keylogger, credential grabber).

- **Crypto reuse:** RC4/XOR primitives reused across samples—operationally useful as a cross-family indicator. Hunt for RC4 KSA patterns or repeating-byte XOR pre-passes.

- **Post-deployment:** file upload/download, remote shell, plugin loading, process injection, lateral movement via harvested credentials, registry/scheduled-task persistence. C2 uses HTTPS to plausible or compromised domains and dynamic DNS.

Bookworm Internals

- **Leader + Modules:** Small leader DLL fetches modules from C2; core remains lightweight and modules deliver functionality at runtime — complicates static detection.

- **UUID-encoded shellcode:** Shellcode sometimes encoded as UUID/GUID ASCII strings inside archives/artifacts. Loader decodes hyphenated UUIDs into raw bytes, concatenates, optional RC4/XOR decode, then LZNT1/reflective load.

- **Detection:** search artifacts and memory for long sequences of hex UUIDs (regex below) and processes that parse/convert UUID strings into binary buffers.

- **Delivery:** spear-phish/weaponised downloads; small stager decodes UUID shellcode and pulls modules.

Turian

- **Loader:** Mirrors PlugX loader patterns (DLL sideloading + XOR —> RC4 —> LZNT1) and loads from encrypted .dat-style files adjacent to signed binaries.

- **Capabilities:** remote command exec, file transfer, credential theft — but crucially, shows code reuse with PlugX/RainyDay loaders, indicating a shared loader ecosystem rather than isolated development.

- **Detection:** Flag new DLLs beside signed EXEs and processes that open *.dat/.afx blobs in program folders. Hunt for the API sequence RtlDecompressBuffer —> VirtualAlloc —> WriteProcessMemory/CreateRemoteThread, and for repeated RC4/XOR primitives in memory.

Tactics, Techniques and Procedures

The following TTPs have are observed in the campaign:

Tactic	Technique	MITRE ID	Details
Initial Access	Spear-phishing (malicious attachments)	T1566.001	Weaponized Office/ZIP used for PlugX/Bookworm delivery.
Execution	DLL search-order hijacking / sideloading	T1574.001 / T1218	Abuses signed/legitimate binaries (Mobile Popup App, etc.) to load
Execution	In-memory execution / Script	T1059 / T1055	XOR→RC4→LZNT1 in-memory unpacking and process injection / reflective loading.
Persistence	Registry Run Keys / Services / Scheduled Tasks	T1547 / T1543	Disguised service names and scheduled tasks used to maintain
Defense Evasion	Obfuscation / Encrypted payloads	T1027	RC4/AES encryption, UUID-encoded shellcode, dynamic API resolution.
C2	Encrypted web protocols / dynamic DNS	T1071.001	HTTPS beaconing to legitimate-looking domains / dynamic DNS providers.
Exfiltration	Exfiltration over C2 channel	T1041	Encrypted, compressed exfiltration (screenshots, credentials prioritized).

Strategic Recommendations

- ### Assume Compromise — Don’t Rely on Awareness or EDR Alone

User training and EDR reduce risk but won’t stop DLL sideloading, UUID-encoded shellcode, or in-memory loaders. Adopt a defence-in-depth posture that assumes initial compromise: combine allow-listing, immutable application paths, runtime process containment, and rapid memory-capture playbooks so detection leads to immediate containment rather than hopeful prevention.

- ### Hunt Persistence and DLL Hygiene Continuously

These families weaponise legitimate binaries by planting malicious DLLs and abusing startup artifacts (services, run keys, scheduled tasks). Make persistence hunting routine: baseline expected DLLs next to signed EXEs, alert on new DLL writes in program folders, and automate drift detection for services/scheduled tasks so disguised entries are flagged and rolled back before escalation.

- ### Shift Detection Toward Memory, Network, and Identity Signals

Reflective loads and compressed/encrypted payloads bypass static controls. Prioritise telemetry that reveals behaviour: RWX allocations, RtlDecompressBuffer + VirtualAlloc sequences, high-entropy memory regions, and anomalous TLS/DNS patterns. Correlate these with identity anomalies (privileged logins, sudden token use) to detect lateral movement and C2 activity earlier.

Cyber Threat Intelligence

The re-emergence of PlugX and Bookworm alongside Turian underscores the continued evolution of China-linked espionage tooling. By layering shared loaders, modular RATs, and overlapping decryption pipelines, these clusters ensure persistence, scalability, and redundancy across multiple campaigns. This convergence reflects a deliberate strategy: to maintain long-term espionage access even if individual toolsets are exposed or neutralised.

Motivation

Operations attributed to these clusters are consistently aligned with China's state-driven intelligence priorities:

- **Espionage:** Telecommunications and government networks provide adversaries with sensitive diplomatic, commercial, and subscriber data. Persistent access offers Beijing visibility into regional decision-making, trade flows, and diplomatic communications.
- **Strategic Leverage:** Compromise of telecom infrastructure and service providers delivers operational options — from covert surveillance to potential disruption during periods of geopolitical tension.
- **Operational Continuity:** By reusing and modernising existing families, threat actors reduce development overhead while ensuring their arsenal remains stealthy and resilient.

Target Profile

Current targeting reflects a strategic focus on sectors that amplify intelligence advantage:

- **Telecommunications Providers:** Access to subscriber databases, core routing infrastructure, and interconnection gateways enables surveillance at scale and potential manipulation of traffic flows.
- **Government Ministries:** Espionage against ASEAN and Asia-Pacific governments provides diplomatic intelligence and supports statecraft objectives.
- **Critical Infrastructure Supply Chains:** Compromised vendors and managed service providers act as multipliers, extending intrusions into downstream enterprises and critical sectors.

Operational Flexibility

The design of these malware families demonstrates their ability to support both enduring espionage operations and adaptable campaign structures:

- Long-term Persistence: DLL sideloading, reflective in-memory loading, and stealth persistence techniques allow dwell time measured in months or years without detection.
- Adaptive Modularity: Toolkits such as Bookworm's leader+modules design enable functionality to be extended on demand, ensuring campaigns can pivot between intelligence collection, credential theft, and lateral movement as required.

Strategic Implication

The convergence of PlugX, Bookworm, and Turian illustrates not just technical overlap but the existence of a shared development ecosystem supporting multiple China-aligned groups. For defenders, this convergence means attribution is blurred, but the threat is constant: a persistent, scalable espionage capability designed to erode regional resilience, sovereignty, and trust in critical communications infrastructure.

References

Indicators of Compromise (IOCs):

Type	Values
Domains	www.fjke5oe[.]com, update.fjke5oe[.]com, www.i5y3dl[.]com, www.hbsanews[.]com, www.b8pjmgd6[.]com, www.zimbra[.]page, www.ggrdl4[.]com, www.gm4rys[.]com
File Hash (SHA256)	cf61b7a9bdde2a39156d88f309f230a7d44e9feaf0359947e1f96e069eca4e86 fbc67446daaa0a0264ed7a252ab42413d6a43c2e5ab43437c2b3272daec85e81 5064b2a8fcfc58c18f53773411f41824b7f6c2675c1d531ffa109dc4f842119b 243b92959cd9aa03482f3398fbe81b4874c50a5945fe6b0c0abb432a33db853f a0887fa90f88dd002b025a97b3a57e4fdb7f5fdd725490d96776f8626f528ef2 a2452456eb3a1a51116d9c2991aae3b0982acc1a9b30efee92a4f102dc4d2927 3e137da41cb509412ee230c6d7aac3d69361358b28c3a09ec851d3c0f3853326 ab54af1dbe6a82488db161a7f57cd74f2dd282a9522587f18313b4e9835dc558 43de1831368e6420b90210e15f72cea9171478391e15efdd608ad22fe916cea8 2bae8b07f5098e1ca8fb5a5776eb874072ace4e19734cba4af4450eeccde7f89 a229a2943cf8d1b073574f0c050ca06392d0525b2028f4b4b04d1e4b40110c66 9192a1c1ab42186a46e08b914d66253440af2d2be6b497c34fe4b1770c3b5e01 4a92fa725adc57d7b501f33e87230a8291cf8ad22d4d3a830293abcc0ac10d12 da8ef50fe5e571d0143a758c7c66bb55653f1f2d04f16464fc857226441d79b2 f0df09513dcf292264b336269952c7e9ff685df8180a2035bee9f3143b36609 fdad627a21a95ea2a6136c264c6a6cc2f0910a24881118b6eabc2d6509dc8dd7 8ec37dac2beaa494dcefec62f0bf4ae30a6ce44b27a588169d8f0476bbc94115 e72e49dc1d95efabc2c12c46df373173f2e20dab715caf58b1be9ca41ec0e172 0e9071714a4af0be1f96cffc3b0e58520b827d9e58297cb0e02d97551eca3799 39280139735145ba6f0918b684ab664a3de7f93b1e3ebcdd071a5300486b8d20 41a0407371124bcad7cab56227078ccd635ba6e6b4374b973754af96b7f58119 02aa5b52137410de7cc26747f26e07b65c936d019ee2e1afae268a00e78a1f7f 2a07877cb53404888e1b6f81bb07a35bc804daa1439317bccde9c498a521644c 5d98d1193fcbb2479668a24697023829fc9dc1f7d31833c3c42b8380ef859ff1 3cef0b5f069cc1d15d36aa83d54d2a7be79b29b02081b6592dd4714639ad0a66
IP Addresses	123.253.32[.]15, 123.253.35[.]231

Public Intelligence:

1. https://thehackernews.com/2025/09/china-linked-plugx-and-bookworm-malware.html
2. https://unit42.paloaltonetworks.com/plugx-variants-in-usbs/
3. https://www.justice.gov/archives/opa/pr/justice-department-and-fbi-conduct-international-operation-delete-malware-used-china-backed
4. https://therecord.media/plugx-malware-infections-more-than-170-countries
5. https://rodtrent.substack.com/p/security-check-in-quick-hits-cisco-d80

Stay Ahead

Access Emerging Threat Reports

Scan to Subscribe

cyberstash.com