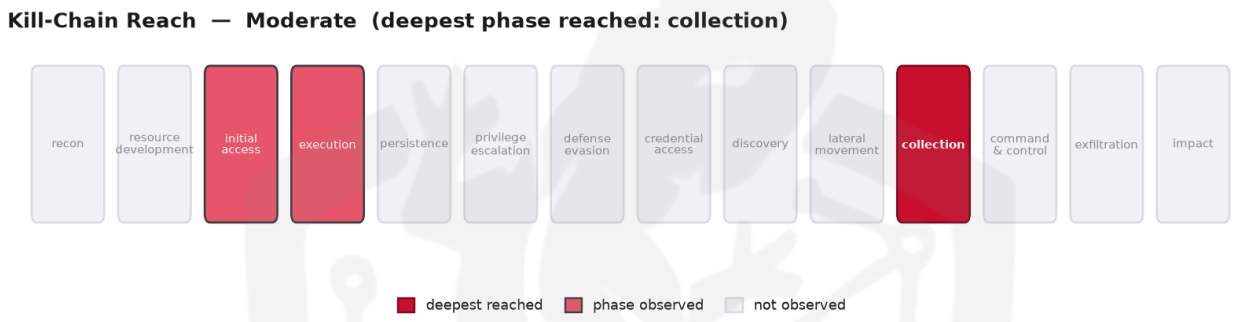
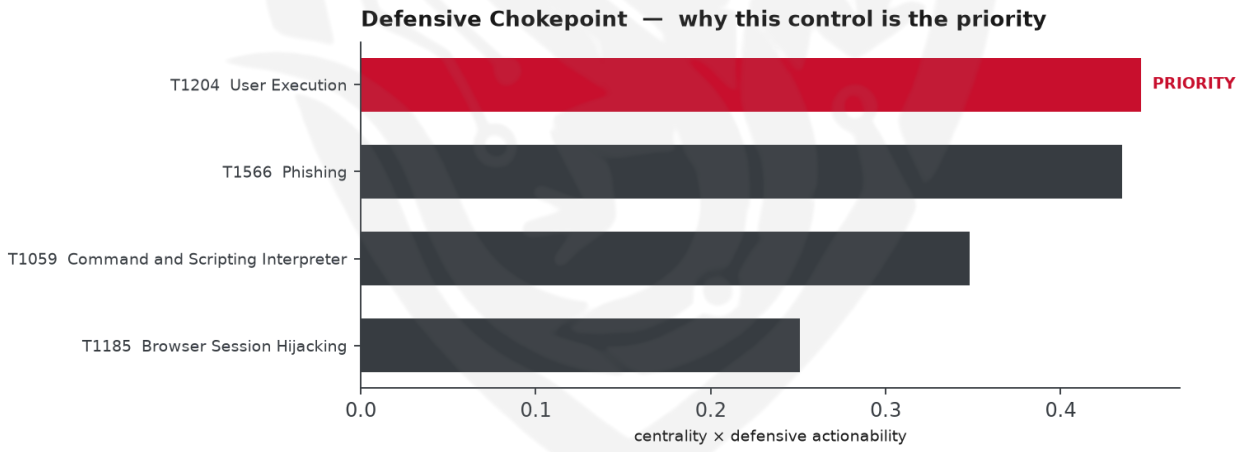
THREAT REPORT: FLYING EAGLE ANDROID RAT TARGETS FINANCE SECTOR IN CHINA AND THAILAND

Visual Summary



How far down the attack chain this campaign reached; deepest phase in crimson.



The control that most disrupts the attack (priority in crimson).

Summary

The observed cluster of activity involves the use of Flying Eagle, Night Dragon, SpyNote, and BTMOB malware families to target the finance sector in China and Thailand. The threat actor's identity is currently insufficient to determine. Priority should be given to blocking the execution of potentially malicious files and enforcing user awareness on phishing lures. The operational risk band is moderate, indicating a potential collection of sensitive information.

Threat Overview

The threat actor, whose identity is currently unknown, is utilizing a range of malware families, including Flying Eagle, Night Dragon, SpyNote, and BTMOB, to target the finance sector in China and Thailand.

Techniques inferred from the report include command and scripting interpreter, browser session hijacking, user execution, and phishing. The central vulnerability exploited is currently insufficient to determine.

Attack Chain and Priority Control

The observed techniques form a chain that starts with phishing and leads to user execution, which is the priority technique (T1204). To mitigate this, the priority control is to block execution of downloaded HTA/JS/LNK; enforce mark-of-the-web; disable Office macros from the internet; and user awareness on lures.

Infrastructure and Corroboration

The malicious infrastructure is hosted on various providers, including Antbox Networks Limited, Zillion Network Inc., Netlab Global, and Closed Joint Stock Company Abkhazmedia. However, there are no malware families corroborated by abuse.ch, and no indicators have an AbuseIPDB confidence of 80% or higher, with the highest confidence seen being 0%.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, machine-extracted from report text — reduced confidence)

The source pulse carried no expert ATT&CK tags, so these techniques were inferred from its narrative by a self-consensus LLM extractor and validated against the ATT&CK catalogue. Treat this technique set, and the chokepoint, kill-chain and risk scores derived from it, as lower-confidence than an expert-tagged brief. - T1059 Command and Scripting Interpreter - T1185 Browser Session Hijacking - T1204 User Execution - T1566 Phishing

Analytical Scores

- Priority technique (graph chokepoint): T1204 User Execution (centrality 0.5573).
- Operational risk: Moderate (score 0.437, reaches collection).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5303; reference threshold tau = 0.6).
- These are behavioural resemblances for defensive playbook cross-referencing, not an identity assessment. Where the source pulse names an actor, that attribution is authoritative; the overlaps below neither confirm nor contest it.

Nearest historical profiles by behavioural overlap (resemblance only):

Historical Profile	Behavioural Overlap
TA459	0.5303
APT30	0.5
TA577	0.4523
Nomadic Octopus	0.4523
Gallmaker	0.4523

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator	Context
IP	108[.]187[.]7[.]66	AbuseIPDB 0% (HK) · AS138995 Antbox Networks Limited
IP	108[.]187[.]7[.]71	AbuseIPDB 0% (HK) · AS138995 Antbox Networks Limited
IP	154[.]44[.]25[.]12	AbuseIPDB 0% (HK) · AS979 Netlab Global
IP	207[.]56[.]30[.]188	AbuseIPDB 0% (HK) · AS54801 Zillion Network Inc.
IP	207[.]56[.]30[.]194	AbuseIPDB 0% (HK) · AS54801 Zillion Network Inc.
IP	77[.]105[.]161[.]235	AbuseIPDB 0% (FI) · AS216300 Closed Joint Stock Company Abkhazmedia
IP	85[.]137[.]253[.]48	AbuseIPDB 0% (DE) · AS215428 Mykyta Skorobohatko
Domain	110gongan[.]com	
Domain	fusu666[.]cc	
Domain	xyttkx[.]cc	

Type	Indicator	Context
Domain	alcs[.]xyttkx[.]cc	
Domain	h5[.]xyttkx[.]cc	
Domain	ls[.]j2x8a[.]top	
Domain	s[.]orove[.]cn	
Domain	txl[.]xyttkx[.]cc	
Hash	18827998ad05c58da1d218066374fe16	
Hash	645ee92d197441684919c0b1ad5cfd15	
Hash	81694f8296ea8e589acc68382add4311	
Hash	b5f64311ffe3c6f1eb13b769663702c6	
Hash	d23e2d0c71cbf0a5d67e17e7b3c690e0	
Hash	5d95ddf7cd857acaaa3447e710a3ee596262b4e2	
Hash	68389a8ae359c2e730e33ab60e9fa6ad71120983	
Hash	d767524b3b288f09840f3d7196718e4187515f6b	
Hash	e02955f78fca6c758d760c36474ae0d4f546efb4	
Hash	e9c71b51de94d6ef1f1090a36754d987374f6f70	
Hash	0376db397807c1f1e32a99a9db622f35f4fe5597bd0 5b4fd5e93117062e0131f	
Hash	1456f31bf6b5d4ade90fe080006478133296080353b f69c1819fa9b766e7f57a	
Hash	4395db6ad53a415532673b16f5b64207d53cecc5b1 5a736c038cf3890368a164	
Hash	5dee5cde6f2874c582effe302960b21569ee007e9e0 cd4f7499d418cceb9095b	
Hash	773c77494d6321e4e449c9558c7915166bcb6c05e3 c42a9d30e5eac4db8ee0df	

Type	Indicator	Context
Hash	7fe8d14e7a9cda92c79d5ae836ed95d772bcc85307 9c4020c5213c3894c7f7af	
Hash	82520e6aa6194b2de0b1c404805a5da7d3693acab 8f7ae2dd5104f14baf82cd7	
Hash	b803cd5032dc1abd7aabc45c8cadc471c8a59872a9 5d48807f13e230c58230f3	
Hash	c692ad120cc90548d48dbe57d006f2403c49833b89 93af3c38fe031eb39999bd	
Hash	d8a82d7b4457352774772bfac094127d7f67526ae7 011d838cc3f7ccc15fd86e	

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.

Flame Cell // Adversary Pivot [BETA]

BETA. A hypothetical tabletop projection, anchored to documented ATT&CK behaviour and technique co-occurrence across 170 tracked groups. It is not a prediction; treat it as a war-game prompt and review before acting. Spot a pivot that looks wrong? norbert@salacti.com

- **Control applied:** T1204 User Execution (execution)
- **Observed here:** T1204 User Execution was the only execution technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1203 Exploitation for Client Execution (execution)
- **Basis:** of the 36+ groups that use User Execution, this pairing runs 1.5x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1203 Exploitation for Client Execution to maintain their objective by leveraging vulnerabilities in client applications, such as browsers or Office software, which may be exposed through user interactions like opening malicious files or clicking on links. This technique in particular could be appealing as it allows the actor to execute malicious code on the client-side, potentially bypassing some of the restrictions imposed by the blocked T1204 User Execution technique. The defensive countermeasure to mitigate this potential pivot would be to patch client applications, enable exploit mitigations such as ASLR, DEP, and CFG, and implement application isolation.

Also plausible (same tactic): T1053 Scheduled Task/Job (n=42, lift 1.2), T1106 Native API (n=17, lift 1.5)

Detection and hardening for the pivot (T1203 Exploitation for Client Execution)

- **Telemetry:** EDR process + memory telemetry; Office/browser/reader child-process telemetry; Windows Error Reporting (application crashes)
- **Detect:**

    - Office, browser or PDF-reader processes (winword/excel/outlook/acrobat/chrome) spawning shells or LOLBINs
    - Sysmon 1 anomalous children of document/browser apps; unbacked-memory execution right after a client crash
    - WER application-crash events for client apps immediately followed by a new child process
- **Harden:**
    - Patch client software fast (browsers, Office, PDF, Java); retire end-of-life plugins
    - ASR rules blocking Office child processes; exploit protection (DEP/ASLR/CFG) and browser sandboxing
- **MITRE:** M1048 Application Isolation and Sandboxing, M1050 Exploit Protection, M1051 Update Software, M1040 Behavior Prevention on Endpoint · DS0009 Process, DS0011 Module, DS0015 Application Log