DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

DSCI THREAT INTELLIGENCE AND RESEARCH INITIATIVE

THREAT ADVISORY

NOVEMBER 2025

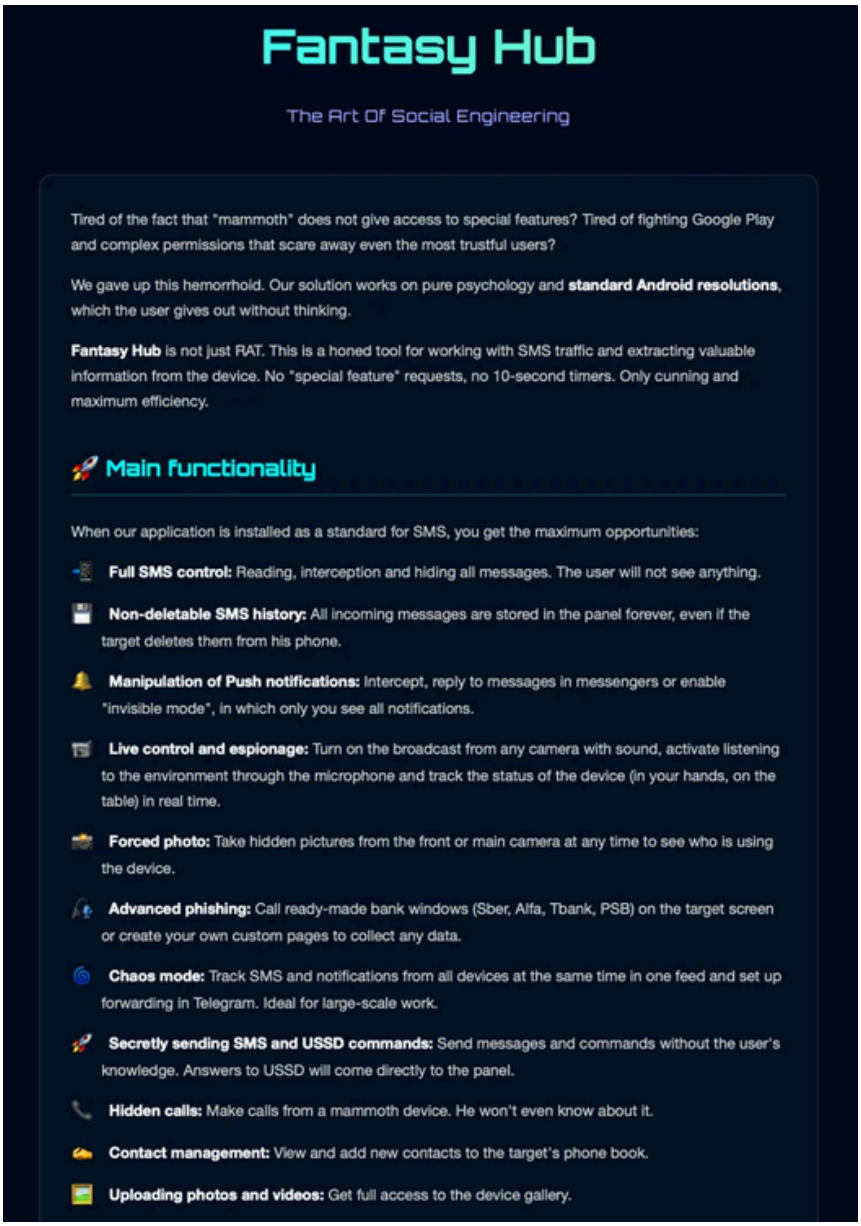
Fantasy Hub Android RAT (MaaS)

Introduction

Fantasy Hub is a commercially sold Android Remote Access Trojan (RAT) being marketed on Russian-language channels as a Malware-as-a-Service (MaaS). It provides buyers with turnkey capabilities like an APK dropper/builder, a Russian-language C2 panel, Telegram alerts, documentation, video instructions etc. lowering the barrier for novice operators. The malware's capabilities include wide data exfiltration such as SMS, contacts, call logs, media, live audio/video streaming via WebRTC, ability to intercept and abuse SMS (including default SMS handler privilege), and the delivery of custom phishing windows to harvest banking credentials.

Who should care

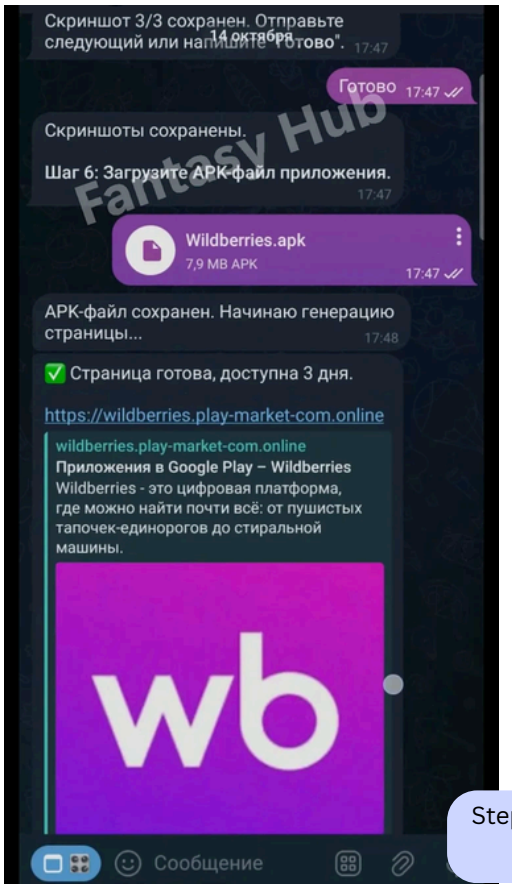
- Enterprise security teams with BYOD policies or unmanaged mobile devices
- Financial institutions (mobile banking and mobile-based 2FA users)
- Mobile app store/review teams and mobile threat detection vendors
- Incident response teams investigating suspicious mobile behavior, unauthorized SMS handling, or credential theft reports



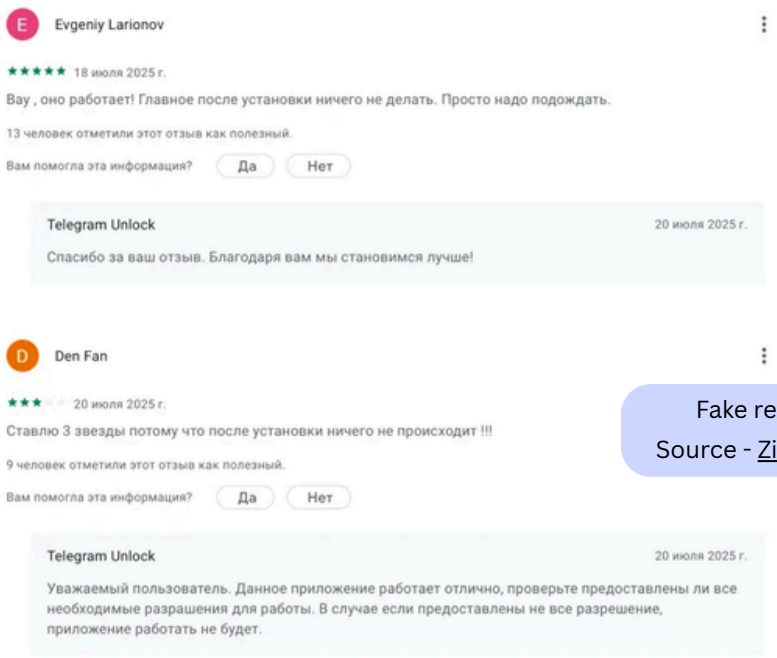
Seller's Advertisement
Source - Zimperium

Distribution Method

These are the instruction shared by seller to create counterfeit Gogle Store page. There are multiple phishing pages including a clone of Telegram with fake reviewsto appear as legitimate reviews.



Steps to create phishing page
Source - Zimperium

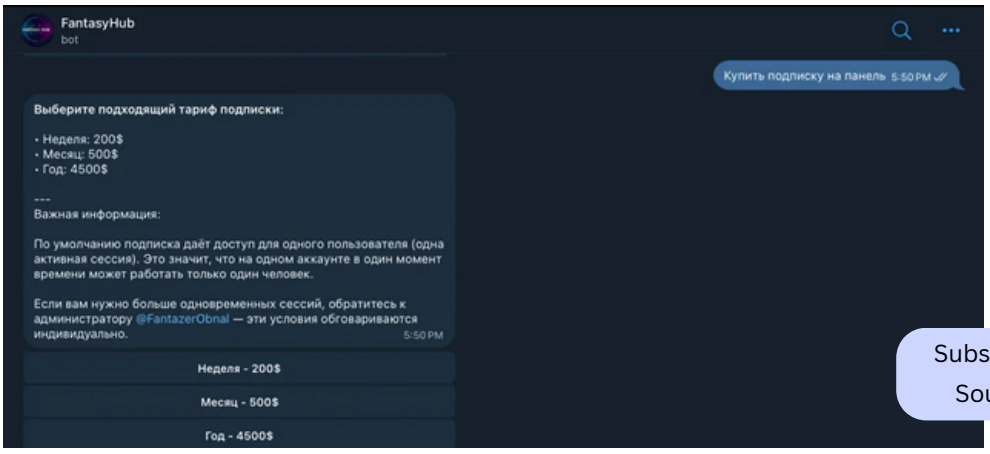


Fake reviews
Source - Zimperium

Fantasy Hub Attack Flow

Threat Actors Prepares Payload (MaaS Model)

Fantasy Hub is sold as subscription-based MaaS. The attackers purchases Fantasy Hub RAT MaaS from Russian-speaking channels. They pay in crypto and then they receive access to the telegram-based APK builder bot to generate a customized malicious APK.



Subscription plan rates
Source - Zimperium

Telegram Bot

The bot is used for malware creation. Attacker selects:

- App icon & name
- Fake theme (banking, messaging, etc)
- C2 server link
- Phishing templates
- SMS hijacking capability

The bot generates a malicious APK containing:

- Encrypted payload file (metadata.dat)
- Native loader library (metamask_loader.so)
- Downloader module for adding WebRTC libraries at runtime

It is shared via fake Google Play store pages

Installation and Initial Execution

When the victim launches the APK, it:

- Immediately runs metamask_loader.so and extract metadata.dat from APK assests
- Decrypts it using custom XOR key + gzip decompression
- Load decrypted RAT and downloads additional libraries (WebRTC)

Evasion steps:

- Checks for sandbox
- Obfuscates real functionality
- Removes easy-to-detect strings

```
public static final boolean p(MainActivity mainActivity0, AssetManager assetManager0, String s) {
    return mainActivity0.decryptAndSaveChiken(assetManager0, "metadata.dat", s);
}
```

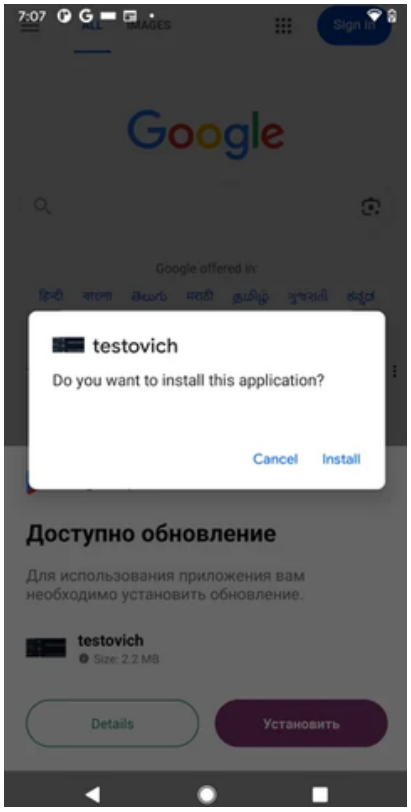
Malware loading encrypted file
Source - Zimperium

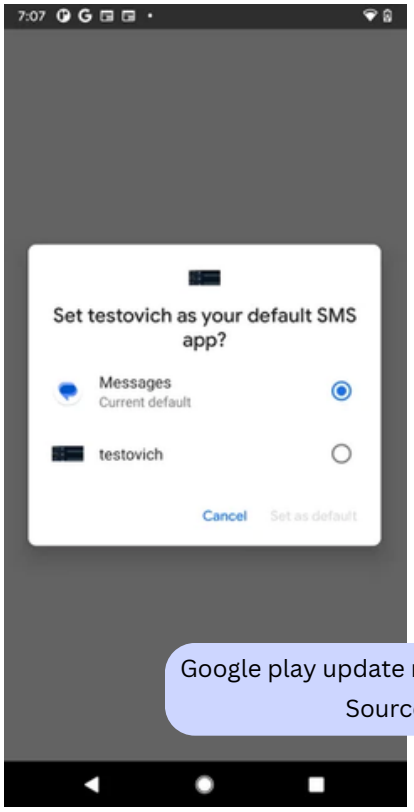
```
        ptr0 = NULL;
    loc_729C4:
        void* ptr10 = NULL;
        void* ptr11 = NULL;
        long v8 = 0L;
        long v9 = 0L;
        long v10 = 0L;
        long v11 = 0L;
        xor_cipher((long)&ptr4, (long)&ptr10);
        long v12 = gzip_decompress((long)&ptr10, (long)&v9);
        if(v12 & 0x1L) {
            sub_72C50((long)&v5, (long)ptr3, 4L);
            if(v3 != 0L) {
                write((long)&v5, v9, v10 - v9);
                long v13 = close((long)&v4);
                if(v13 == 0L) {
                    int* ptr12 = (int*)(*(long*)((long)v5 - 24L) + (long)&v5);
                    clear((long)ptr12, (uint64_t)(*(ptr12 + 8) | 0x4));
                }
            }
            AAsset_close(asset);
```

Decryption routine
Source - Zimperium

Permission Abuse & Role Hijacking

The app requests extremely sensitive permissions like deafult SMS Handler role (it gives full access to read/modify SMS and bypass SMS-based OTP/2FA), camera, microphone, read contacts and storage, etc.

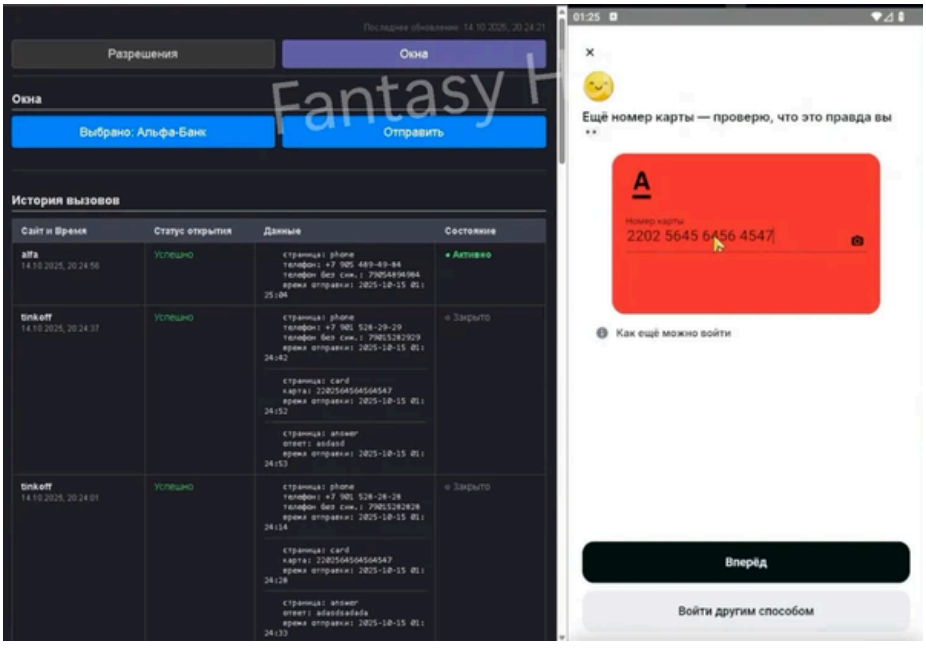




Google play update requesting SMS permissions
Source - Zimperium

Remote Execution

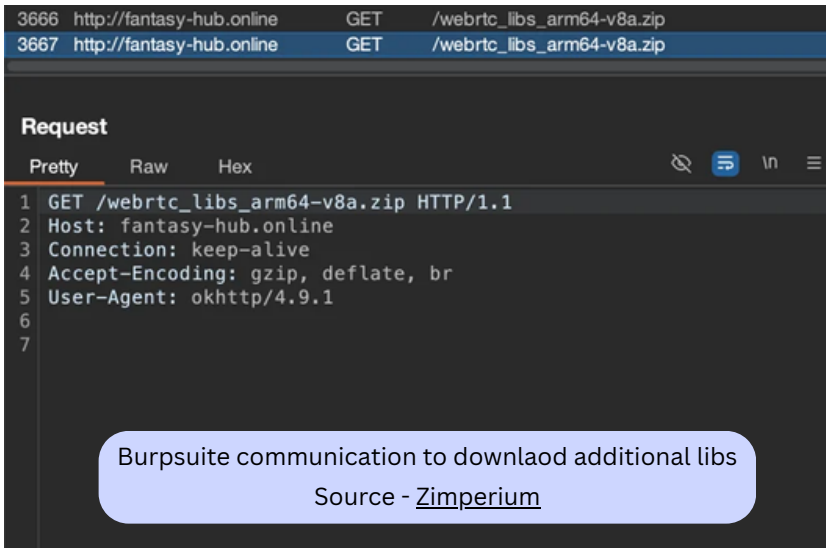
Fantasy Hub provides full RAT functionality which is remotely controlled form C2. It pushes phishing windows (bank overlays) that appear on top of banking apps to capture banking login credentials, MFA codes and session tokens. The malware also uses default SMS handler to read all incoming OTPs, auto-forward them silently and deletes OTP messages.



Alfa-Bank fake window
Source - Zimperium

As it also gets access to communication devices, it can use

- Microphone and front/back camera for real-time recordings using WebRTC
- Call log extraction and content harvesting



Burpsuite communication to downlaod additional libs
Source - Zimperium

List of commands used by Malware

Command	Description
addContact	Add contact to device
getContacts	Capture contacts from victim's device
app_restart	Halts C2 and restars it after 1.2 seconds
createImagesZip	Zip file for images
replyToNotification	Reply to notifications
deleteNotification	Delete notifications
deleteZipArchive	Delete a specific zip file entry
downloadMediaFile	Download media from victim's device
executeCommand	Executes USSD codes or phone calls silently using specific SIM card from victim's device

Command	Description
getCallLogs	Exports calllogs and send it to C2
getDeviceInfo	Capture device info such as brand, IP. etc. and send it to C2
getMediaFiles	Send media files to server
sendSms	Send sms from device
getSystemInfo	Service that receives intents and forwards harvested data to remote dispatcher
getZipArchivesList	Gives the list of stored zip archives
requestSystemAsset	Starts a local service to capture/stream media
webrtc_stream	Creates a WebRTC connection on Android to capture microphone and front/back camera stream
selfDestruct	A kill switch to disable the fake app, cancel alarms and background tasks, stop all running services and wipes app data
sendLocalFile	Captures a local file and sends it to C2
sendUssdWithChoice	Allow app to initiate USSD requests dialing service codes on behalf of user
setInvisibleIntercept	Intercept device activity by saving invisible_intercept_enabled in SharedPreferences
startDeviceStaetMonitoring	Samples sensors (accelerometer, gyro), device posture/state (hand/table/pocket, motion), and broadcasts the updates to server periodically
stopSystemAsset	Stops the device stream

Indicators of Compromise

Full set of IOCs referred in this advisory is available on the **zimperium** blog.

X----X----X----X

Everest Group claims Ransomware Attack on Collins Aerospace

Introduction

In September 2025, Collins Aerospace (RTX) suffered a cyber incident that disrupted check-in and baggage systems at several major European airports. Intelligence indicates the Everest group gained access via legacy/compromised FTP credentials (traced to a 2022 RedLine infostealer compromise), exfiltrated large volumes of passenger and employee data, and sold or claimed the access; ransomware deployed by an affiliated/secondary actor caused operational outages at airports. Multiple aviation authorities and news outlets confirmed operational disruption at Heathrow, Brussels, Berlin, Dublin and Cork.

Timeline

September 10, 2025
The Everest ransomware group gains access to Collins Aerospace's vMUSE backend via compromised FTP credentials

September 11, 2025
The ransomware group exfiltrate data before their activity is detected and blocked

September 15, 2025
The group informs RTX about the stolen data through vulnerability reporting portal

September 16-18, 2025
Conversations and negotiations between Everest and Collins Aerospace

September 19, 2025
The Aerospace reports about the "disruption" to aviation authorities; many European airports starts facing check-in and baggage system outage

September 20-22, 2025
Airports like Heathrow, Brussels, Berlin, Dublin and Cork confirms disruptions, switches to manual operations, warn passengers about delays

September 24 2025
UK authorities arrest and release a suspect; investigation continues

September 29, 2025
Replacement systems are rolled out at affected airports

Affected Airports

Airport	Country	Imapct
Heathrow Airport	UK	Check-in, baggage delays
Brussels Airport	Belgium	Check-in, delays
Berlin Brandenburg Airport	Germany	Check-in, delays
Dublin Airport	Ireland	Check-in, delays
Cork Airport	Ireland	Check-in, delays

Manual operation began as automated check-in and baggage system were disabled. Thousands of passengers were affected due to delays and cancellations. The issue remained up to a week in some airports.

Attack Details

Initial access

The ransomware group compromised legacy FTP credentials like aiscustomers, muse-insecure, etc. on 'ftp.arinc.com', likely stemming from a 2022 RedLine infostealer infection on an employee endpoint from Collins Aerospace.

Data Exfiltration

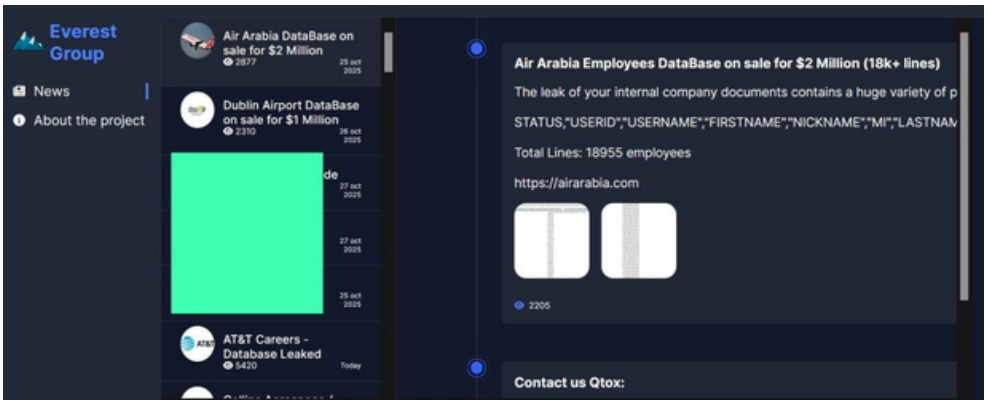
FTP server - 'ftp.arinc.com' was the main exfiltration point. The credentials were not rotated after the prior infosteaker compromise. The Everest ransomware group didn't deployed any ransomware rather acted as initial access broker and conducted data exfiltration. A separate ransomware group deployed ransomware on Collins Aerospace's MUSE system that caused shutdown of operations and airport disruptions.

Everest claimed theft of:

- 1,533,900 passengers records like flyer details, travel data, seat number, passengers IDs, etc. were leaked
- 3637 airline employee records like names, usernames, aliases, emails, login status, audit metadata were leaked
- 50+ GB data of internal topology/audit and application files were leaked

Everest claimed AT&T Carrier Database Leak

The group claimed leak of personal details of 1.5 million Dublin Airport passengers and asked for ransom amount of $1 million and 18,000 data of Air Arabia employees and a ransom amount of $2 million.



Screenshot from ransomware group's dark web leak site
Source - Hackread

It was reported on October 21, 2025, that personal information has been stolen from AT&T Carrier database and they were given a time of 6 days for communication. The data was released online and it includes two CSV files, one titled '*user_list*' and other titled *'customer_list'*.

The *'user_list'* file contains personal data such as email address, full names and phone numbers of 429,103 individuals.

The *'customer_list'* file contains email addresses, phone numbers and last name of 147,621 individuals.

Screenshot of AT&T data leak
Source - Hackread

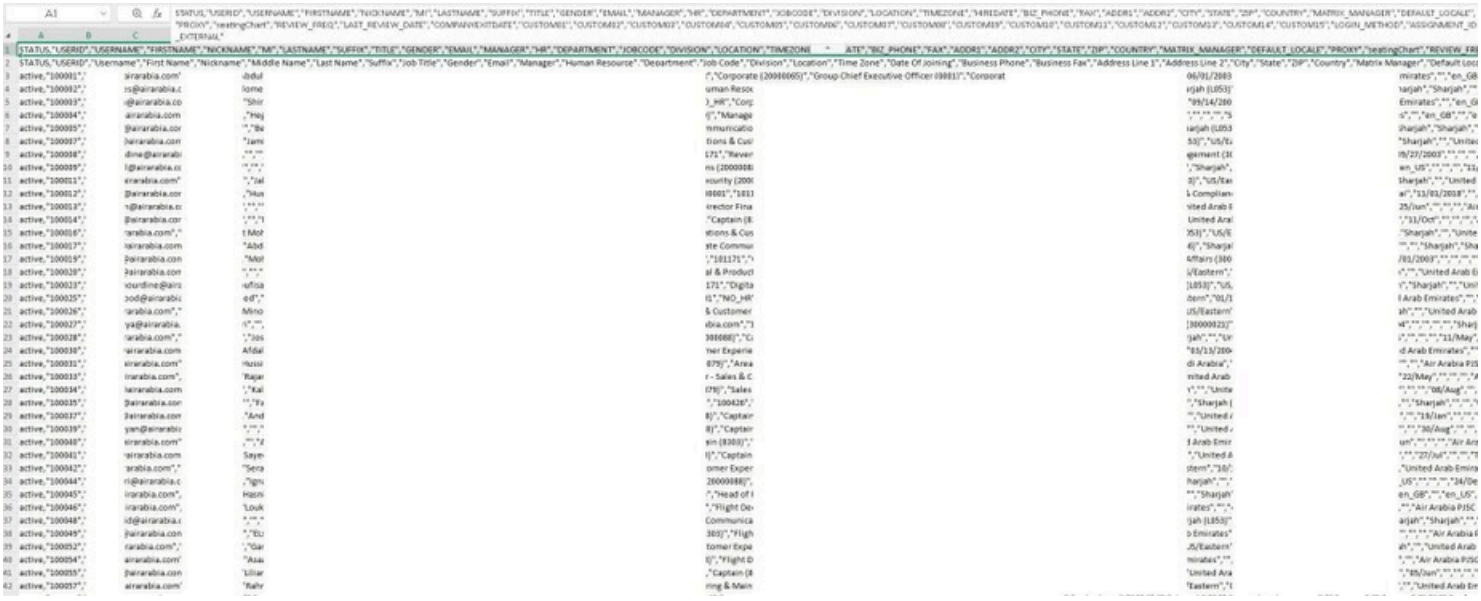
Dublin Airport Passenger Data Leaked

Dublin ransomware group was listed as a victim by the Everest ransomware group on their dark web site on October 25, 2025. They claimed to possess data of around 1.5 million passengers and a time period of 6 days were given but the group shortened its deadline and started offering entire dataset for $1 million.

Air Arabia Emloyee Data Leaked

liThey also claimed to have stolen 18,000 employees data of Air Arabia. It contains both personal and corporate employee details. The data contains

- Status of employee (active/terminated/on leave)
- User ID/Username
- First/middle/last name, any suffix or nickname
- Emails, location and timezone
- Manager, HR contact details



Screenshot of Air Arabia data leak
Source - Hackread

It is not confirmed if the data leak is genuine or not, but if it is true, it can heavily impact the passengers and employees of both the company. Also, AT&T and Air Arabia have not confirmed the data leak also.

X----X----X----X

First Ai-orchestrated cyber-espionage campaign

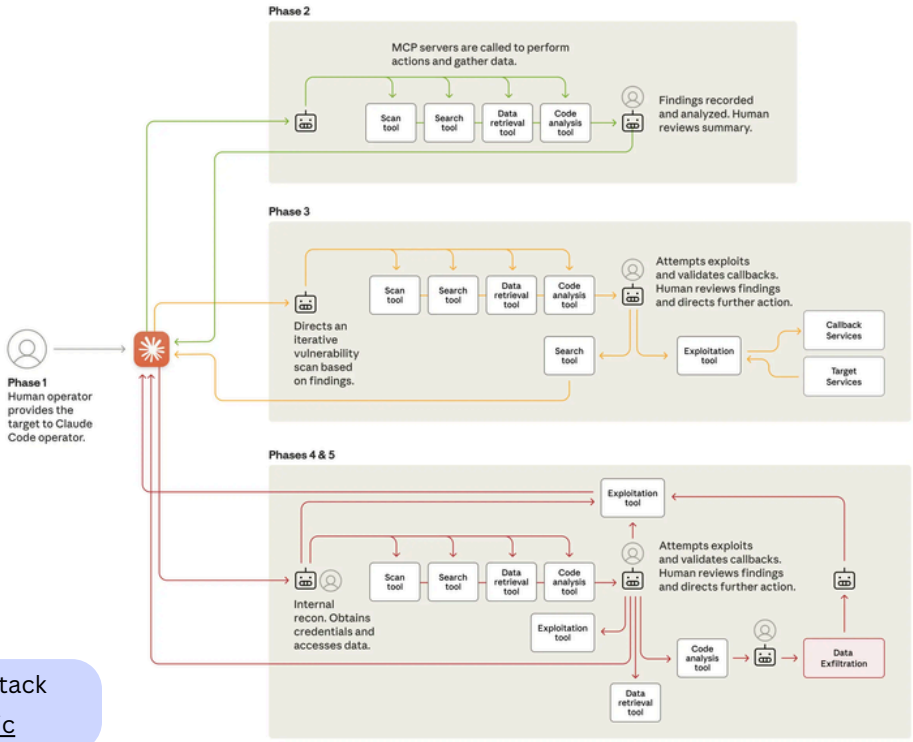
Introduction

In mid-September 2025, a suspicious activity was detected which later turned out to be a large-scale cyber-espionage campaign that leveraged AI as a core component. The attackers are believed to be a Chinese state-sponsored group (designated “GTG-1002”) that used the AI model Claude Code not merely as a support tool, but as an autonomous agent to execute the majority of the attack lifecycle.

Attack Details

They used Claude Code tool and attempted infiltrating roughly 30 global targets, including large tech firms, financial institutions, chemical manufacturers, government agencies, etc. and they suceeded in some of the cases. It is believed to be the first large-scale cyberattack executed without substancial human intervention.

AI handled almost 80-90% of the “tactical operations” (reconnaissance, exploit development, credential harvesting, lateral movement, data exfiltration and analysis) and humans intervened only for some strategic decisions. Upon detection, attacker’s account were banned, notified some affected entities, coordinated with authorities and expanded its safeguards.



Lifecycle of Cyberattack
Source - Anthropic

Phase 1

In the first phase, humans chose the relevant targets which they want to infiltrate which mainly includes business or government organizations. Then they created an attack framework which is a system that is designed to compromise a selected target on its own with minimal assistance from humans. They used Claude Code in their framework for the automation process and carry out the desired operations.

They started persuading Claude, which is trained to avoid performing or taking part in any harmful act. They used jailbreak techniques so that it an bypass its barriers. They divided their attacks into small innocent tasks that Claude can easily carry out without knowing its full malicious purpose. They also informed that attacker is an employee of a cybersecurity firm and is being used for defensive training.

Phase 2

In the second phase, Claude Code started examining the infrastructure and systems of the targeted company to identify the databasTransparentTribe APT Lifecycle Source - Cyble es with the highest value. This reconnaissance was completed by Claude in a fraction of the time that ma yrequire a group of human hackers to do the same work. After that, it sent a summary of its results back to the human operators.

Phase 3

Then Claude started conducting research adn wrote its own exploit codes to find security flaws and vulnerabilities in the target's system. After that, the framework used Claude to gather credentials like passwords and usernames due to which they gained further access and extracted a large amount of sensitive data. Highest privilege accounts were identified, backdoors were created and with minimal human intervention data was exfiltrated.

Phase 4&5

In the final phase, attackers guided Claude to create a detailed documentation of the attack, containing credentials and system details that was further used by the framework to plan their next stage of attack. These threat actors used AI for 80-90% of their campaign requiring minimal intervention of humans in some 4-6 crucial decision parts of the campaign.

Comparing this work, a human attacker team would take a large amount of time to complete the work done by AI. AI generated thousands of requests (multiple requests per second), a speed which is impossible for humans to match.

Implications

- The use of AI significantly lowers the skill barrier. Now, attackers don’t need deep human expertise for every stage as AI can automate reconnaissance, exploit development, and data exfiltration.

- Detection and defense mechanisms need to evolve as traditional intrusion-detection, human-led pen-testing, and signature-based SOC workflows may be inadequate. Organizations must consider AI-aware monitoring, behavior analytics, and anomaly detection.

- For cloud / SaaS / AI-providers strong guardrails, misuse resistance, AI-model auditing, red-teaming against misuse are no longer optional.

This demonstrates that AI-orchestrated cyber-espionage is no longer theoretical, it's a real, operational threat.

X----X----X----X

Scattered Spider / LAPSUS$ Hunters Supply Chain Breach

Introduction

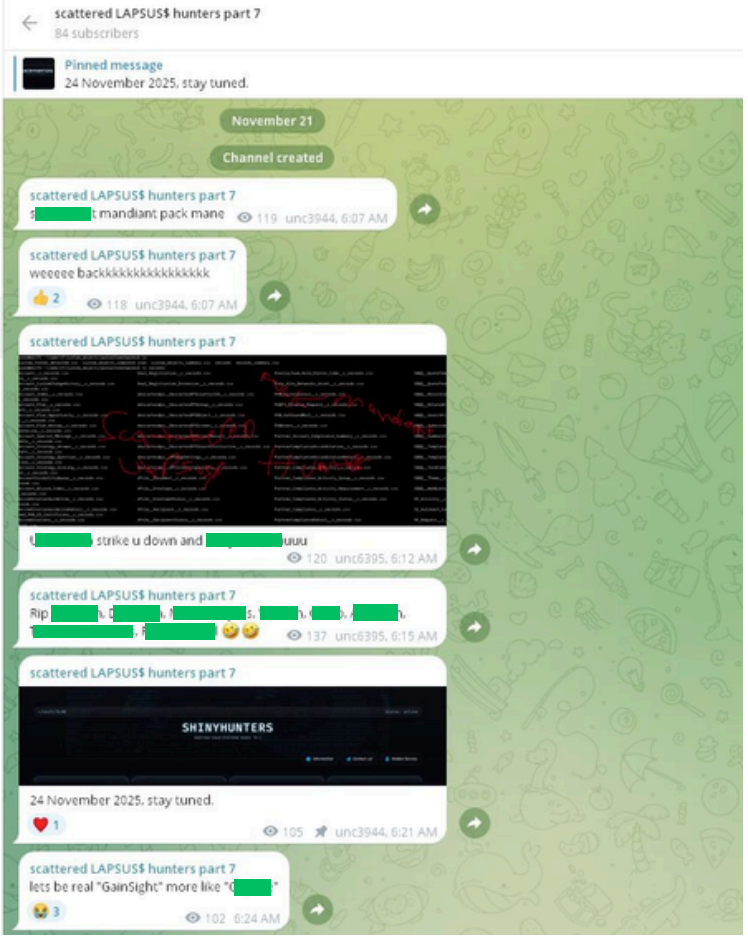
The threat group branding itself as “Scattered LAPSUS$ Hunters” has resurfaced on Telegram, announcing a major supply chain compromise affecting an estimated 284 companies through a breach of Gainsight, a Customer Success and data-integration platform used across global enterprises.

The actors claim that access enabled them to pivot into Salesforce instances, leading to potential theft of customer datasets, marketing pipelines, support data, and internal operational insights of large enterprise customers.

The campaign is visibly similar to the Salesloft–Drift compromise, which Scattered Spider previously weaponized to obtain internal tokens and support-case credentials.

Key Findings

On November 19-20, 2025, Salesforce publically acknowledged an incident that certain customers’ data may have been exposed following “unusual activity” involving third-party applications published by Gainsight. As a result, Salesforce revoked access tokens for all Gainsight-connected applications and temporarily removed those apps from its AppExchange.



Security firms like Google Threat Intelligence Group estimated that more than 200 customer Salesforce instances may have been impacted. Also, Scattered LAPSUS$ Hunters publicly claimed the responsibility via a Telegram channel, naming dozens of alleged high-profile victims such as Fortune-500, large enterprises, etc. asserting the breach has affected 284 companies.

Attack Vector

Initial Breach - Attackers exploit OAuth tokens / secret credentials tied to third-party integrations. In this case, Gainsight apps are connected to Salesforce.

Supply-chain pivot - As many enterprises rely on Gainsight to manage CRM, support and customer-success workflows, compromising Gainsight enables downstream Salesforce data access across multiple clients.

Data exfiltration - Once inside Salesforce instances, attackers can dump CRM records, contact lists, support case notes, business data, access tokens, etc. anything accessible with the permissions granted via the compromised integration.

Claims & extortion posture - The group publicly claims large-scale theft, pobably hundreds of companies and threaten them to release their data via dedicated leak site if ransom demands aren't met. They also hinted at a RaaS platform launch.

Claim vs Confirmed Facts

Claim (by Actors / Media)	Verified ?	Status
284-company breach via Gainsight	Partially: >200 Salesforce instances possibly affected, confirmed by Google	Ongoing Investigations, exact number unconfirmed
1,000 downstream organizations impacted (Gainsight + Salesloft/Drift)	Actor claim - not verified	Unconfirmed
Insider leaks at CrowdStrike leading to breach	Insider sharing screenshots confirmed; but CrowdStrike denies system compromise	Verified insider leak; no breach confirmation
RaaS launched (ShinySp1d3r)	Logistics and group announcements observed	Ongoing / speculations until verified leak

Conclusion

The supply-chain attack via Gainsight → Salesforce has credible foundation and is being treated seriously by multiple vendors and security firms. The large list of victim names and scale (hundreds to nearly a thousand) remains unverified (hyped by attackers), but it must be taken seriously by any firm using Gainsight or similar SaaS integrations.

References

- **Zimperium** - Fantasy Hub: Another Russian Based RAT as M-a-a-S - https://zimperium.com/blog/fantasy-hub-another-russian-based-rat-as-m-a-a-s

- **Protos Labs** - Deep Dive Analysis: Collins Aerospace Ransomware Attack Claimed by Everest Group - https://www.protoslabs.io/resources/deep-dive-analysis-collins-aerospace-ransomware-attack-claimed-by-everest-group

- **Hack Read** - Everest Leaks AT&T Records, Demands $1M for Dublin Airport Passenger Data - https://hackread.com/everest-att-leak-dublin-airport-data/

- **Anthropic** - Disrupting the first reported AI-orchestrated cyber espionage campaign - https://www.anthropic.com/news/disrupting-AI-espionage

- **Cyderes** - The First Verified AI-Orchestrated Cyber Espionage Campaign Signals a New Era of Attack and Defense - https://www.cyderes.com/howler-cell/first-ai-driven-cyber-espionage-campaign-anthropic-analysis

- **Tech Crunch** - Salesforce says some of its customers' data was accessed after Gainsight breach - https://techcrunch.com/2025/11/20/salesforce-says-some-of-its-customers-data-was-accessed-after-gainsight-breach/?utm_source=chatgpt.com

- **Zerofox** - Flash Report: Scattered Lapsus$ Hunters Announce Return - https://www.zerofox.com/intelligence/flash-report-scattered-lapsus-hunters-announce-return/?utm_source=chatgpt.com

- **Rankiteo** - Gainsight - https://blog.rankiteo.com/gai1832518112125-gainsight-cyber-attack-november-2025/?utm_source=chatgpt.com

- **Bleeping Computer** - CrowdStrike catches insider feeding information to hackers - https://www.bleepingcomputer.com/news/security/crowdstrike-catches-insider-feeding-information-to-hackers/?utm_source=chatgpt.com

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

ABOUT DSCI

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, set up by Nasscom, committed to making cyberspace safe, secure, and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

Data Security Council of India
4th Floor, Nasscom Campus, Plot No. 7-10, Sector 126, Noida, UP-201303

data-security-council-of-india/ DSCI_Connect dsci.connect

dsci.connect dscivideo security chips