LightSpy Malware Now Targets Facebook & Instagram Data

Published: 2025-02-20 · Archived: 2026-04-05 13:59:17 UTC

First publicly reported in 2020, **LightSpy is a modular surveillance framework designed for data collection and exfiltration**. Initially observed targeting **mobile devices**, further analysis confirmed its ability to compromise **Windows, macOS, Linux, and routers**. LightSpy has been deployed in **targeted attacks using watering hole techniques and exploit-based delivery**, with its infrastructure frequently shifting to evade detection.

Findings

- Targeting of Facebook and Instagram application database files for data extraction.
- LightSpy deployment date (2021-12-31) is linked to a possibly unreported core version.
- Windows-specific plugins designed for system surveillance and data collection.
- Additional endpoints beyond the admin panel, including a likely testing route that briefly exposes authenticated session behavior.

Tracking LightSpy Infrastructure (Pt. 2)

In June of last year, we published research on **tracking LightSpy servers via their TLS certificates** and integrated a detection query into **Hunt.io** to automate identification. Since then, we have continued monitoring this infrastructure, with Hunt.io currently detecting **eight active IPs**, some of which were previously detailed in **BlackBerry and Volexity's research on the DeepData variant of LightSpy**.

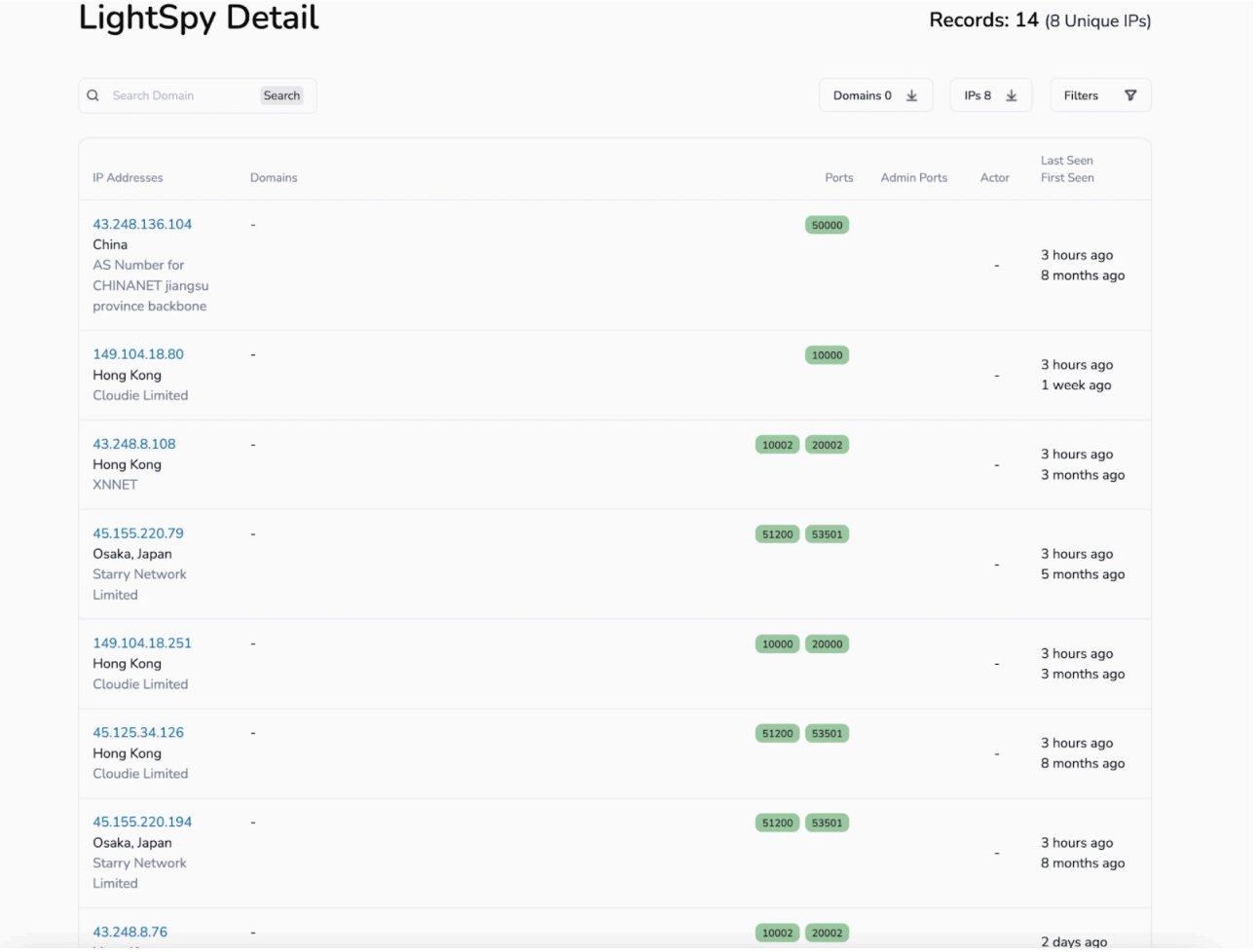

Figure 1: Screenshot of current servers tagged as LightSpy in Hunt.

In October, we posted on X/Twitter about two LightSpy servers---43.248.8[.]108 and 149.104.18[.]251---briefly sharing **SSH keys** with another detected C2, 43.248.8[.]76, as well as an additional IP, 149.104.18[.]80.

Among these, 149.104.18[.]80 is the most recent IP to appear in our scans as LightSpy and its command list modifications and infrastructure details will be the focus of this analysis.

Command List Expansion: What's Different?

LightSpy has been previously documented targeting messaging applications such as Telegram, QQ, WeChat, WhatsApp, and Line across multiple operating systems. ThreatFabric's reporting highlighted the framework's ability to exfiltrate payment data from WeChat, delete contacts, and clear messaging history, among other functions.

The servers analyzed in this research share similarities with prior malicious infrastructure but introduce notable differences in the command list. As previously observed, the cmd_list endpoint is at /ujmfanncy76211/front_api. Another endpoint, command_list, also exists but requires authentication, preventing direct analysis.

A comparison of command lists between the previously reported 45.125.34[.]126:49000 and the recently observed 149.104.18[.]80:10000 reveals a significant expansion:

- **Previous reported C2**: 55 supported commands.
- **Recently observed C2**: Over **100** commands spanning Android, iOS, Windows, macOS, routers, and Linux.

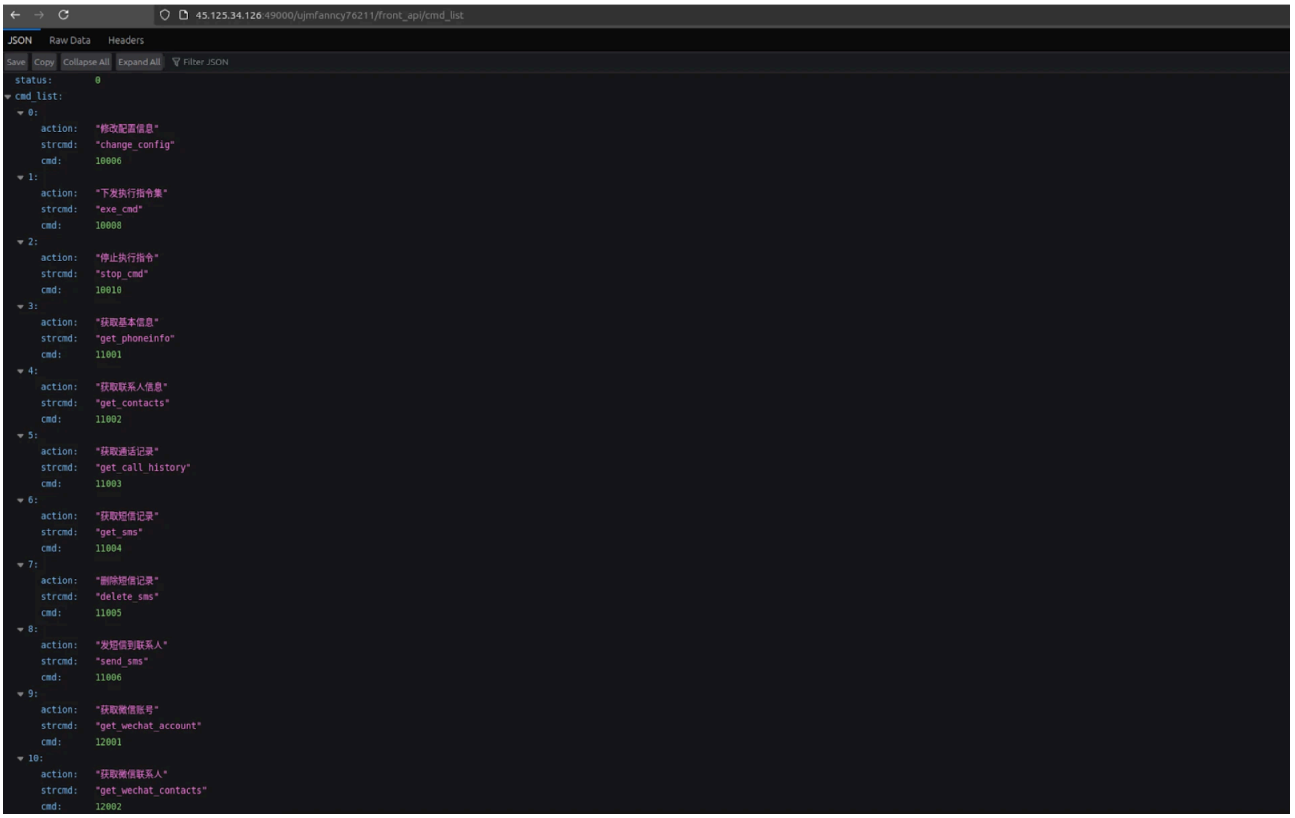

Figure 2: Snippet of C2 command list at IP 45.125.34[.]126.

The new command list shifts focus from direct data collection to broader operational control, including **transmission management** ("传输控制") and **plugin version tracking** ("上传插件版本详细信息"). These additions suggest a more flexible and adaptable framework, allowing LightSpy operators to manage deployments more efficiently across multiple platforms.

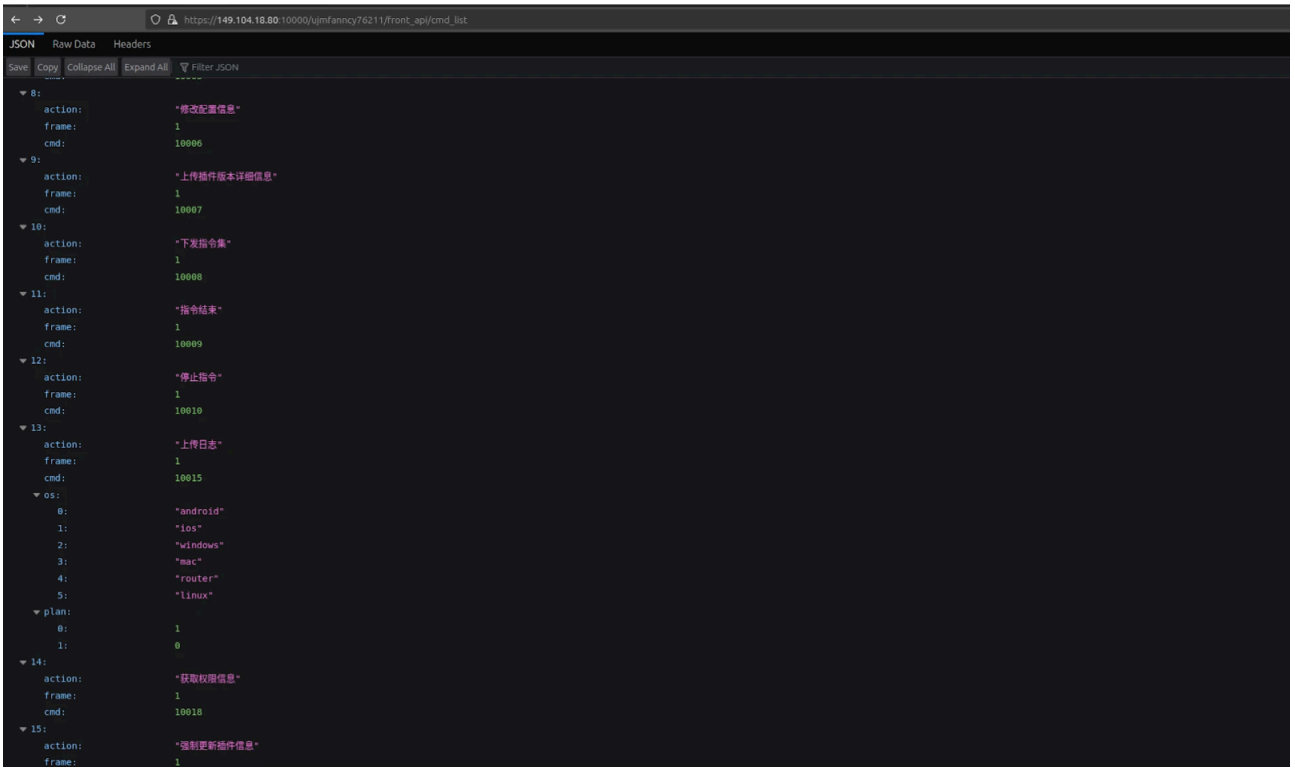

Figure 3: Snippet of the more recent C2 command list at 149.104.18[.]80

Among the newly introduced Android commands are:

- **获取Facebook数据库文件** ("Get Facebook Database Files")
    - Command ID: 83001
- **获取Instagram数据库文件** ("Get Instagram Database Files")
    - Command ID: 83002

This is the first reference we are aware of **Facebook and Instagram database targeting** within LightSpy's command structure. Additionally, the list references **"Enigma,"** which may correspond to the secure messaging platform of the same name.

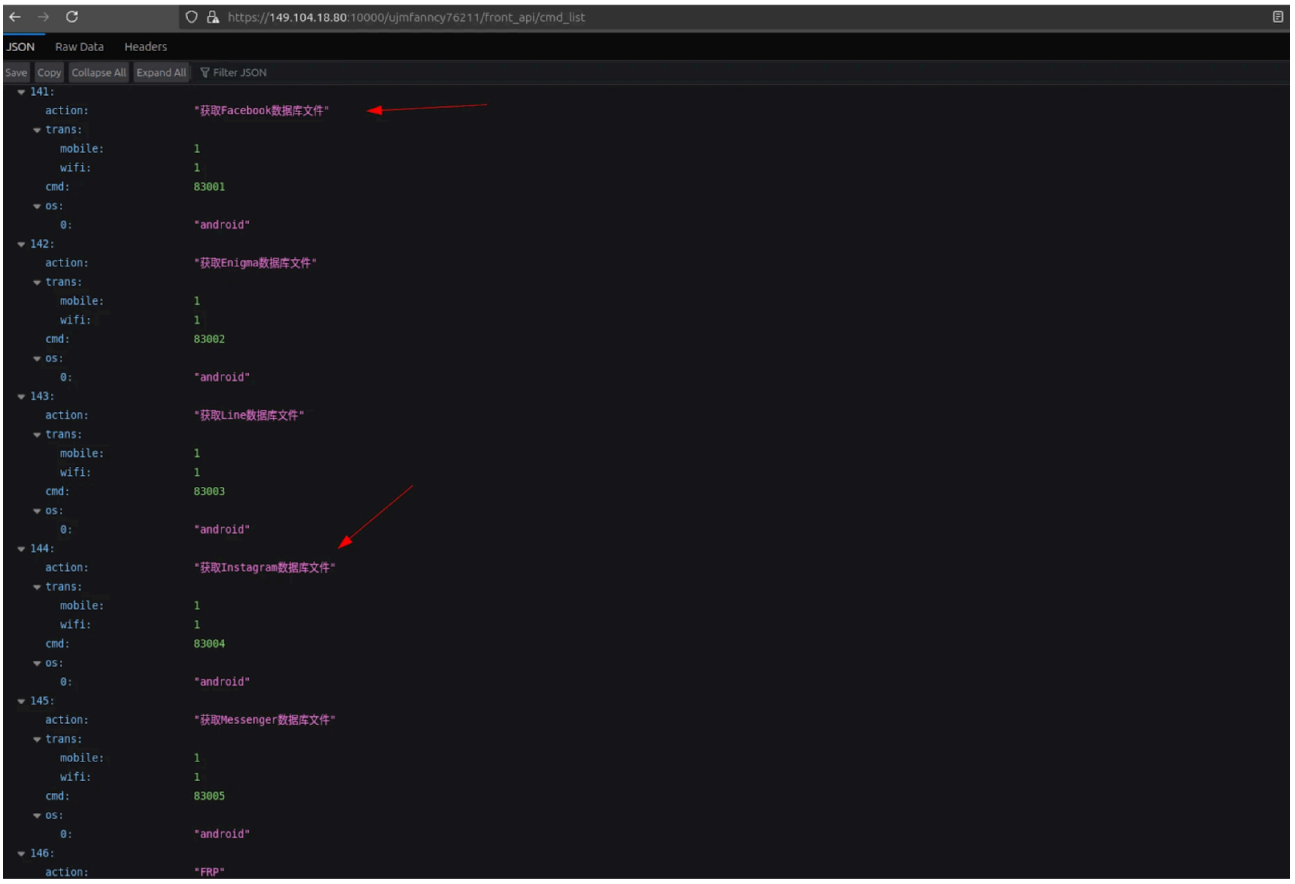

Figure 4: Command list showing targeting of Facebook and Instagram database files.

The shift from targeting messaging applications to Facebook and Instagram expands LightSpy's ability to collect private messages, contact lists, and account metadata from widely used social platforms. Extracting these database files could provide attackers with stored conversations, user connections, and potentially session-related data, increasing surveillance capabilities and opportunities for further exploitation.

LightSpy Core, iOS & Windows Plugins

While we were unable to recover any first-stage implants for LightSpy, we examined the server for files of interest that were accessible for download. The server `149.104.18[.]80`, hosted on Cloudie Limited in Hong Kong, was observed with open ports 80, 443, 10000, 30000, and 40002.

LightSpy's configurations frequently use `/963852741` as a recurring endpoint pattern. A GET request to `http[:]//149.104.18[.]80:30000/963852741/ios/version.json` returned metadata on LightSpy's core, including its deployment date, file name, and MD5 hash. The date listed was 2020-12-21, reportedly associated with version 7.7.1.

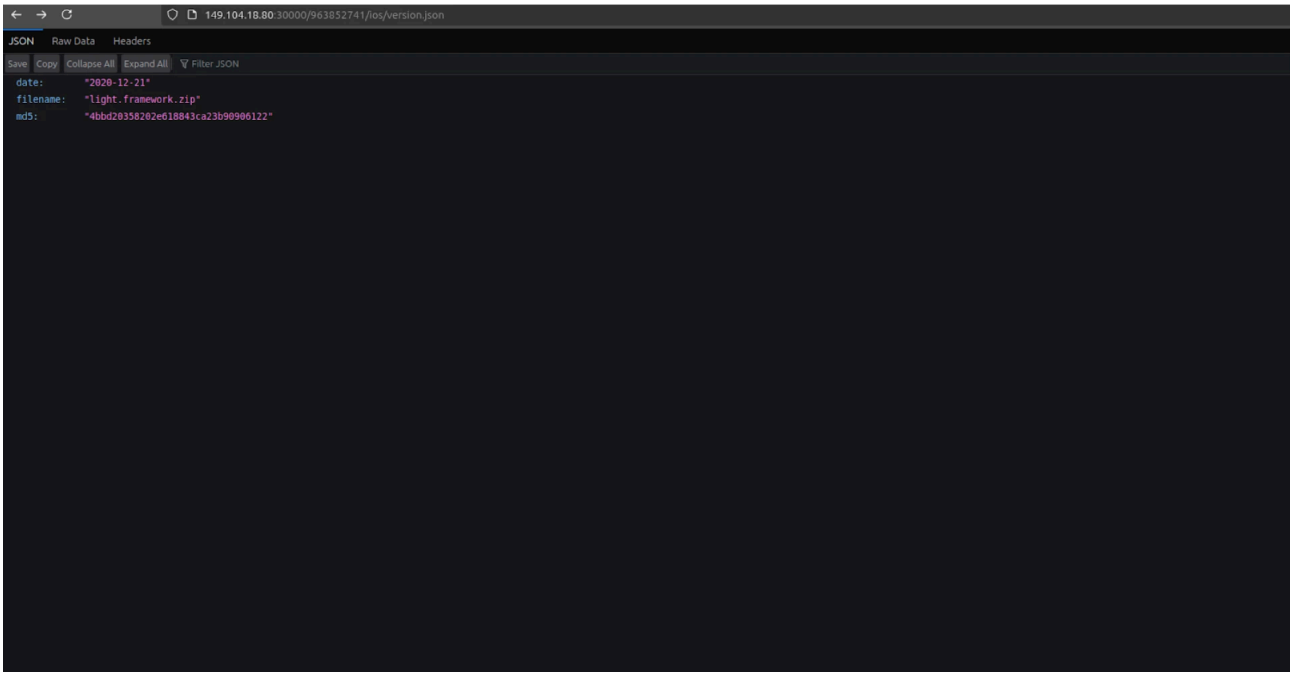

Figure 5: JSON response when requesting /ios/version.json on port 30000.

Querying the same endpoint on port 40002 returned a deployment date of **2021-12-31**, with the MD5 hash **81d2bd4781e3753b508ff6d966dbf160**. To our knowledge, this date/version has not been publicly reported.

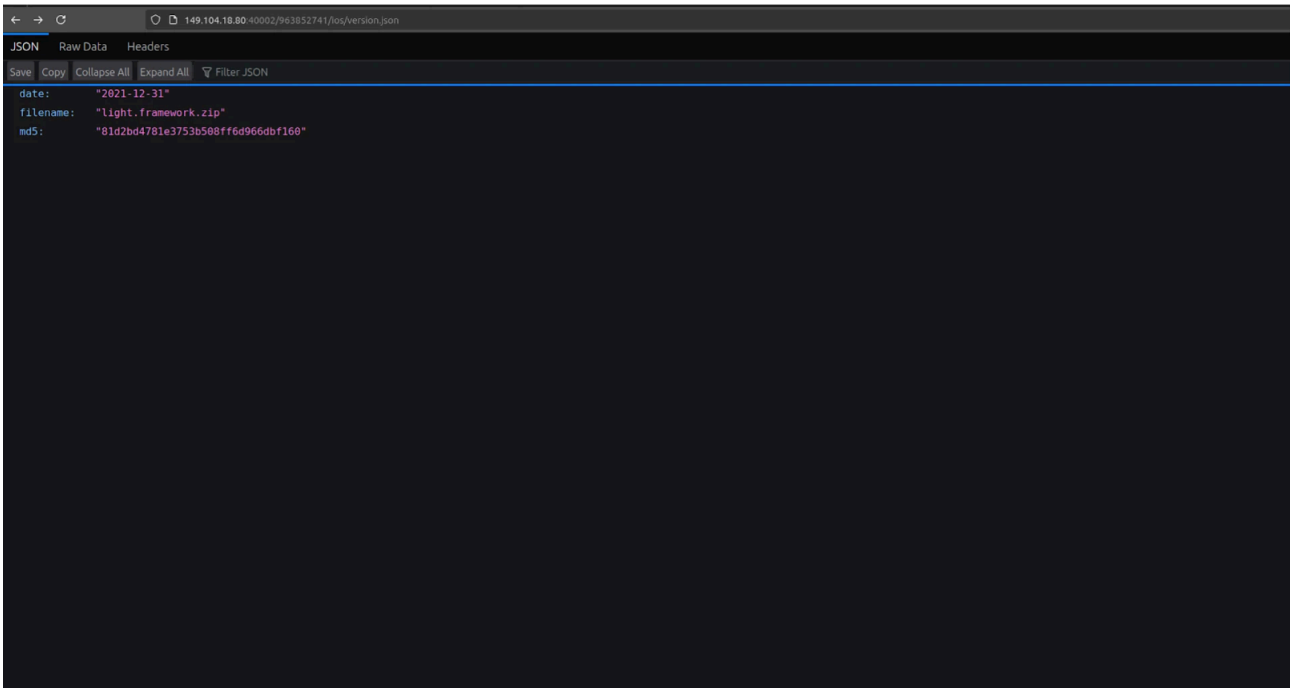

Figure 6: Screenshot of LightSpy core information dated 2021-12-31.

The hashes for both light.framework.zip files can be found at the end of this post.

iOS Plugins

Alongside version.json, the server also hosts manifest.json, which contains version numbers, class paths, MD5 hashes for integrity verification, file names, and download URLs. The response listed **17** different plugins, all

matching the versions and capabilities described in ThreatFabric's most recent analysis. Notably, the operator removed plugins associated with destructive actions on the victim host.

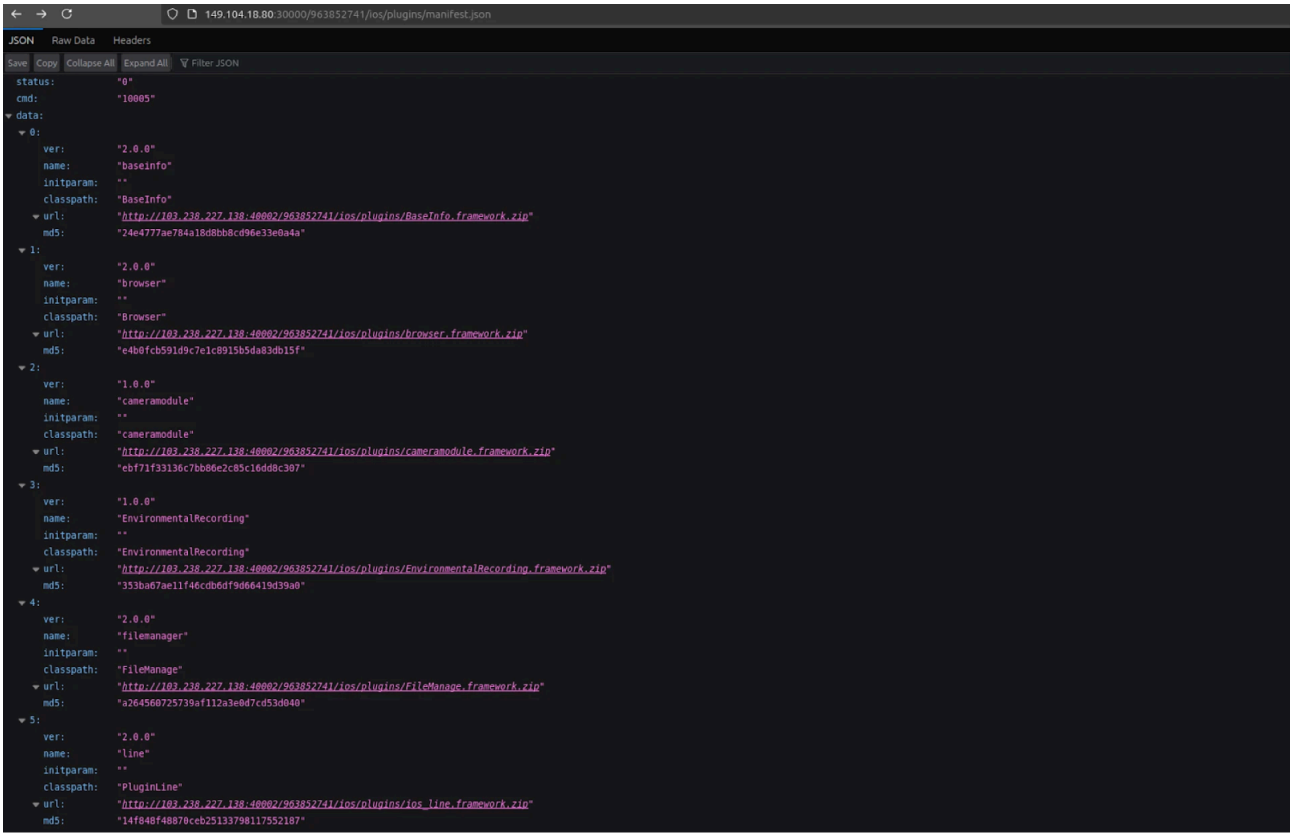

Figure 7: Snippet of iOS plugins targeting several apps and functionalities.

The URL field within the response referenced an additional IP, 103.238.227[.]138, serving plugins at the same port and path. This server, also hosted on Cloudie Limited, had ports 22 and 7000 open. A single domain, hk.cdn[.]cat resolves to this IP, though we found no indication that it is associated with LightSpy activity.

Windows Plugins

In addition to the iOS plugin page, we identified a separate page for Windows plugins. No references to Linux, Android, or macOS plugins were found on this server, suggesting that iOS and Windows were the primary targets for this campaign.

The Windows JSON file followed the same structure as its iOS counterpart. There are **15** plugins with DLL files targeting x86 and x64 architectures. The observed version numbers were either 0.0.0.0 or 0.0.0.2, indicating the files were recent or the developer opted not to track version changes.

Below is a list of the Windows plugins, their version numbers, and the affected platforms:

Filename	Version	Platform
vxx64m.dll	0.0.0.2	x64
vxx86m.dll	0.0.0.2	x86

Filename	Version	Platform
Terminalx86m.dll	0.0.0.2	x86
Terminalx64m.dll	0.0.0.2	x64
KeyLogLib32m.dll	0.0.0.2	x86
KeyLogLib64m.dll	0.0.0.2	x64
audiox64m	0.0.0.0	x64
audiom.dll	0.0.0.0	x86
Capx64m.dll	0.0.0.0	x64
Capm.dll	0.0.0.0	x86
srvx64m.dll	0.0.0.0	x64
srvm.dll	0.0.0.0	x86
usbx64m.dll	0.0.0.0	x64
usbm.dll	0.0.0.0	x86
video64m.dll	0.0.0.0	x64
videom.dll	0.0.0.0	x86

Table 1: Windows plugin DLLs.

The DLL files share one of the following PDB paths, indicating the directory structure used during development:

- `W:\yk\Bigfoot\bin\*.pdb`
- `W:\yk\Darwin\Bin\*.pdb`

The Windows plugins indicate a focus on **keylogging** ("KeyLogLib"), **audio recording** ("audio"), video capture ("video"), and **USB interaction** ("usb"), typical for surveillanceware. "Terminal*" DLLs suggest potential remote command execution or user activity monitoring, while "Cap" plugins are related to screenshot or screen recording capabilities.

Admin Panel/Infrastructure

The two other IPs associated with this activity, `43.248.8[.]108` and `149.104.18[.]251`, host admin panels on ports 10000 or 10002. The login page, built on the Vue framework, is titled "Console Login" and is located at `/ujmfanncy76211/login`.

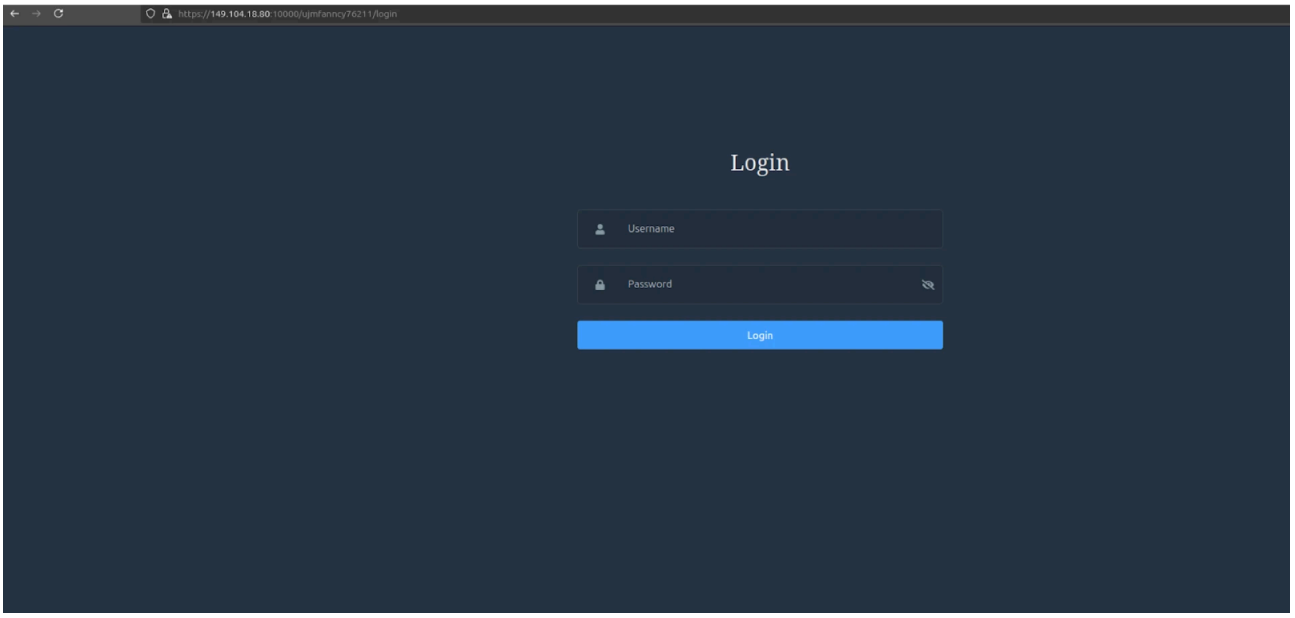

Figure 8: Screenshot of login panel at 149.104.18[.]80.

Further investigation revealed multiple endpoints under `/ujmfanncy76211`, each returning different behaviors:

Endpoint	Behavior
/at	Captures requesting host information, including browser, GPU, and User-Agent. (Screenshot included below)
/remote_csm	Likely for remote access; it redirects back to /login.
/963852oiu/login	Displays a loading spinner and attempts to connect to 192.168.1[.]208
/963852tgb/login	Returns a token error.
/963852iuy/login	Redirects to /login.
/third_login/:username	May allow persistent access or automated login attempts.
thd/login	Responds with "login with thd_tk is not permission" (Screenshot included below).

Table 2: Additional endpoints found under the admin panel.

Figure 9: Result of querying /at which captures requestor information.

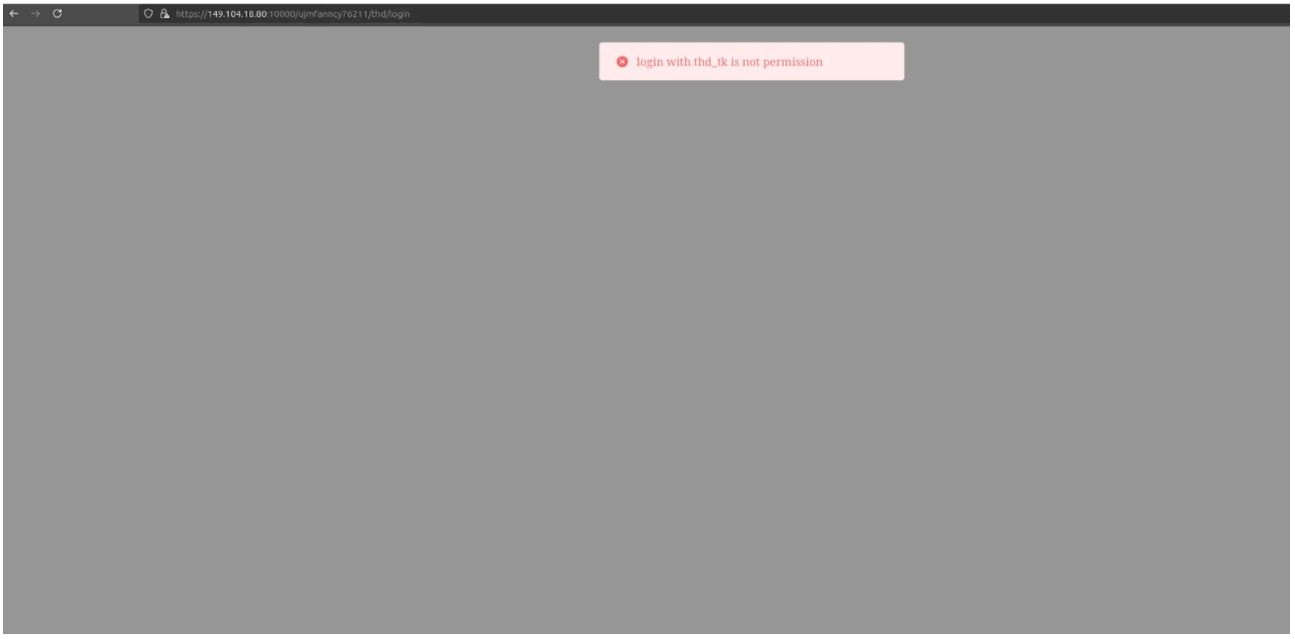

Figure 10: Error message when requesting /thd/login.

Due to a misconfiguration in the server, the `/third_login/:username` endpoint provides a brief glimpse into the inner workings of the framework as an authenticated user. When loaded, the below page is visible and hosted at `/phone/phoneinfo`, of which we were able to capture a screenshot.

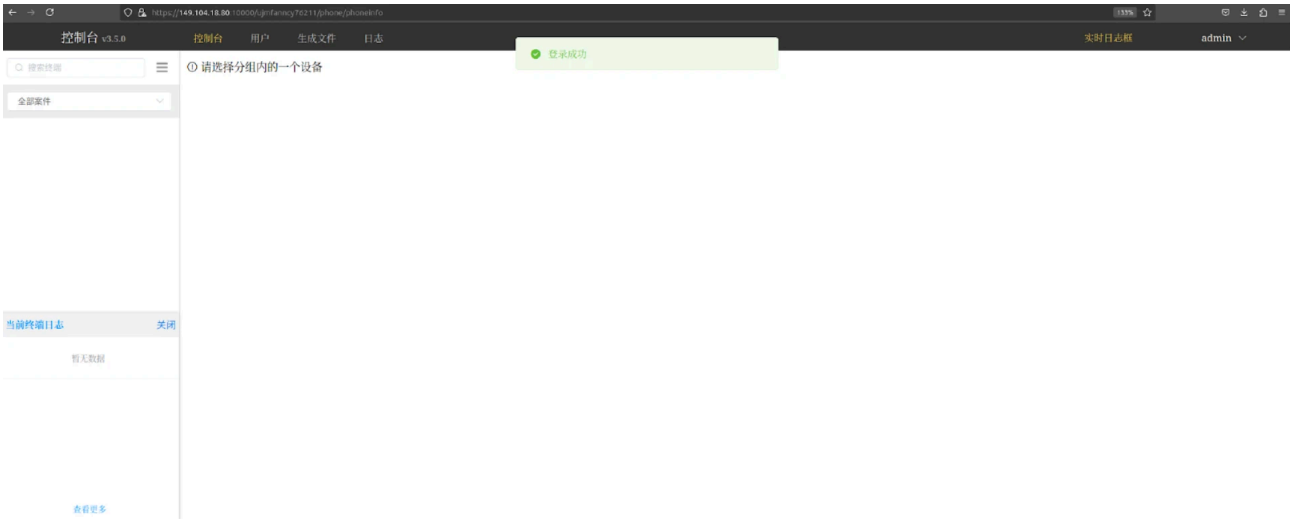

Figure 11: View of the phone info page in LightSpy when accessing the /third_login/:username endpoint.

The interface, named Console v3.5.0, serves as a remote management panel for compromised mobile devices. Upon accessing the page, a "Login Successful" message is displayed, granting the operator access to device controls. The top menu options include:

- 控制台 → Console
- 产生文件 → Generate Files
- 日志 → Logs

The main content window prompts the user to "Please select a device from the group," while the side panel provides access to terminal logs and additional device data.

The presence of admin panel endpoints such as `/third_login/:username` and `/remote_csm provides` an opportunity to track LightSpy infrastructure through distinctive authentication requests and operator activity. Analyzing server responses, panel access patterns, and command execution behavior can offer further insight into the malware's operational framework.

Conclusion

LightSpy's infrastructure reveals previously unreported components and administrative functionality, though it remains unclear whether these represent new developments or older versions not publicly documented. Command set modifications and Windows-targeted plugins suggest that operators continue to refine their data collection and surveillance approach across multiple platforms.

The exposure of admin panel authentication endpoints provides insight into how operators manage compromised systems and suggests that aspects of LightSpy's infrastructure may be monitored or tracked through behavioral analysis of authentication flows. Understanding how these endpoints function helps profile operational patterns and uncover related infrastructure. As LightSpy's operators adapt, we will do the same and continue refining our tracking methods to identify new C2 servers as they appear.

To mitigate risks, defenders/users should:

- Restrict app permissions to prevent unnecessary access to sensitive data. On Android, use Privacy Dashboard to review and revoke permissions, and on iOS, enable App Privacy Reports to monitor background data access.
- Enable advanced device security features that limit the exploitability of devices. iOS users can turn on Lockdown Mode, which restricts attack surfaces, while Android users can enable Enhanced Google Play Protect and exploit protection settings to detect and block malicious activity.
- Examine historical system logs and forensic artifacts to determine whether the 2021-12-31 core version or related LightSpy components were present in previously undetected infections.

LightSpy Network Observables and Indicators of Compromise (IOCs)

IP Address	ASN	Domains	Location	Last Seen
149.104.18[.]80	Cloudie Limited	N/A	HK	16 February 2025
149.104.18[.]251	Cloudie Limited	N/A	HK	16 February 2025
43.248.8[.]108	XNNET LLC	N/A	HK	16 February 2025
43.248.8[.]76	XNNET LLC	N/A	HK	17 February 2025
103.238.227[.]138	Cloudie Limited	hk.cdn[.]cat	HK	17 December 2024

LightSpy Host Observables and Indicators of Compromise (IOCs)

Filename	SHA-256
light.framework.zip (2021-12-31)	890712c46e6629a59d1d82840256530f1cd3f1eda5c1e7f7f459ca786e120ba7
light.framework.zip (2020-12-21)	9e4e2c92037f43441376685af7f30c6df602ed9706715073e696a6a178a4b5d7
smallmload.jar	bd6ec04d41a5da66d23533e586c939eece483e9b105bd378053e6073df50ba99
bbbb.jar	9da5c381c28e0b2c0c0ff9a6ffcd9208f060537c3b6c1a086abe2903e85f6fdd
vxx64m.dll	1b47cd2595d0f3468dbb609f5dcedfc90e2ee7c291d84bd6bd7d6a311a5f6bd
vxx86m.dll	f05b8387f808a598338ce2258014b2c259a4297a5593779e46029b3c5539ea4e
Terminalx86m.dll	98a5275997acab23c26165980f221eaf2aab90b779af162c06e8823b4d19c7a3
KeyLogLib32m.dll	72eff7f7f928f54db67d9b3aeee9a6c2b0af89edc0a71ce09715489ac7644a68
KeyLogLib64m.dll	250e2aefc5a31019da9afeb22b1c704c6fd4db2da1ff6b5a0be4c63d23a32090

Filename	SHA-256
audiox64m.dll	10c43f9dfaf94777f89248720555d17ac275b21ca726291989672b34f3991bc3
audiom.dll	2e86456358046e347e05dce6ef6e30af92560901c145b95329fecaf6e64bd898
Capx64m.dll	1d9293814fa3ce62fa67c1cbb8661660ffe1caa848142ba7f58dbbb60bc491ba
Capm.dll	7147672b45832714c8b3d075665345d0860e9ebb672c4b5cbbe17243270ca41d
srvx64m.dll	7dbc26526fa32e1c91767d8b18abd3f4367f1b55b0f9ccf338fe5b9f74a36e48
srvm.dll	e7b9e5e3bd6f72c39ef687ae59b2380815e827ea479ad142f278f295d706c5ec
usbx64m.dll	29e090acf7aa1296fa5d22b0df92a830e7a58467f966dd0f78bd1560dc0bad45
usbm.dll	74ce9f196c930c50811e4640283779ddd971e6a5ad6771c0577a80147c12bd35
videox64m.dll	aee8ca6bcfff02ae0f931b76f48e39576477af289385cbcde27d3ac3e7fae35e
videom.dll	0258edc8c3efe8b3d8ccfce790c9192994e54a81dded1c0e116093d638506a01

PDB Paths

- W:\yk\Bigfoot\bin\filename.pdb
- W:\yk\Darwin\Bin\filename.pdb
