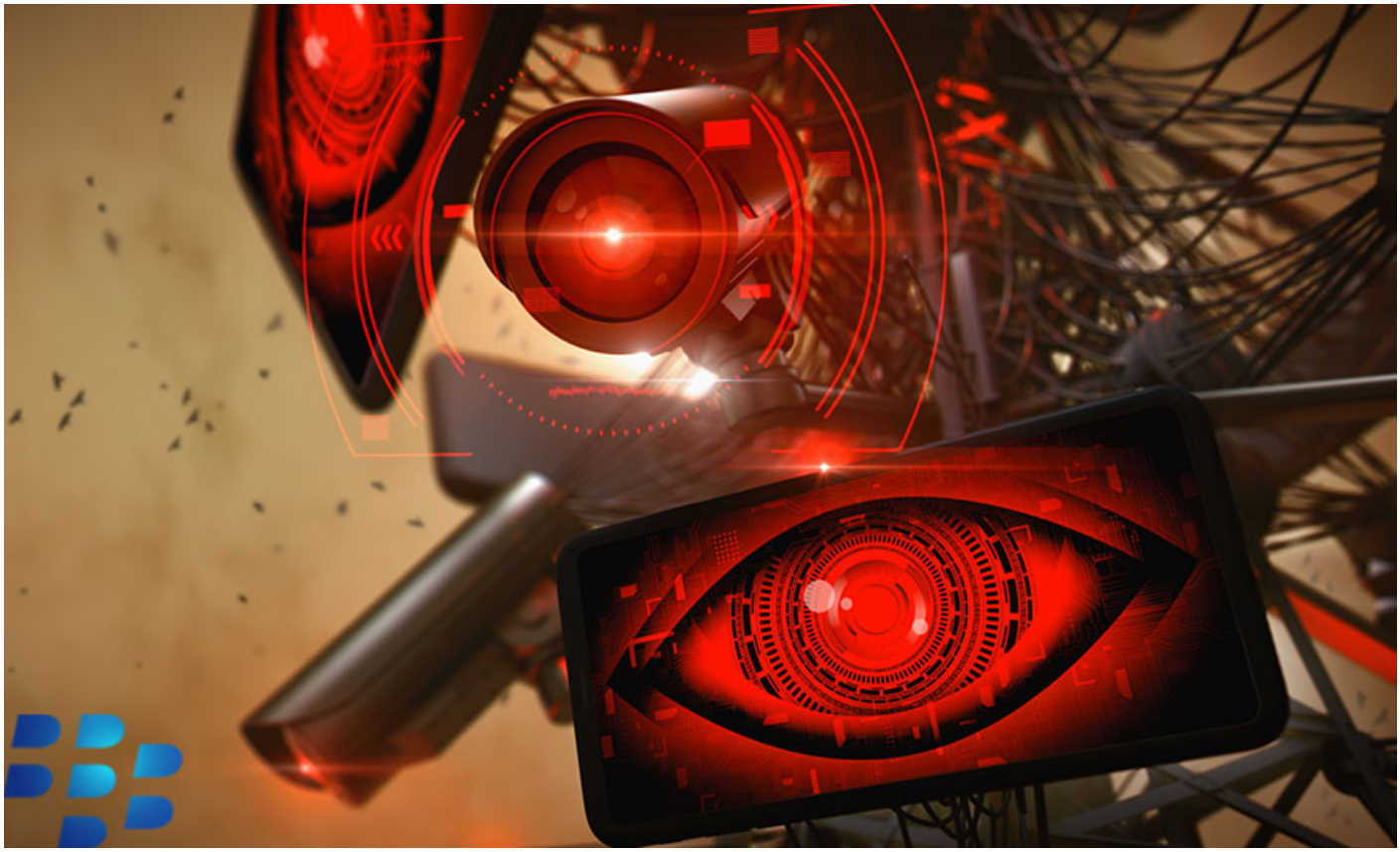
LightSpy Returns: Renewed Espionage Campaign Targets Southern Asia, Possibly India

Dmitry Melikov ⋮⋮ 4/11/2024



Summary

This report details the resurgence of the LightSpy mobile espionage campaign, which focuses on targets in Southern Asia and probably India, potentially indicating a renewed focus on political targets and tensions in the region.

Beyond our findings, the echoes of concern reach further. VirusTotal submissions from India suggest potential victims within its borders, aligning with recent warnings by Apple on detections within the same country.

What is LightSpy?

LightSpy is a sophisticated iOS implant, first reported in 2020 in connection with a watering-hole attack against Apple device users. Specifically, it is a fully-featured modular surveillance toolset that primarily focuses on exfiltrating victims' private information, including hyper-specific location data and sound recording during voice over IP (VOIP) calls. This makes it particularly dangerous to victims, with as many

consequences as can be imagined relating to a threat actor being able to locate their target with near-perfect accuracy.

LightSpy possesses modules designed to exfiltrate device information and saved files, including data from popular messenger applications such as QQ, WeChat, and Telegram. It also has a plugin capable of crawling the payment history of the victim from WeChat Pay (Weixin Pay in China). It can additionally access a user's contacts, SMS messages, phone call history, GPS location, connected WiFi history, and the browser history of Safari and Chrome. This comprehensive set of features can turn a user's infected phone into a potent spying device.

The last campaign attributed to the attacker behind LightSpy was in 2020, amid escalating political tensions in Hong Kong. The malicious implants were distributed through "poisoned" news sites focused on polarizing issues in the Hong Kong region. The threat actor group thought to be behind this LightSpy campaign reportedly had active servers in China, Singapore, and Russia.

Key Findings

- LightSpy is back: After several months of curious inactivity, the advanced mobile spyware has resurfaced, targeting individuals in Southern Asia.
- **Expanded capabilities:** The latest iteration of LightSpy, dubbed "F_Warehouse", boasts a modular framework with extensive spying features, including:
    - **File theft:** LightSpy is capable of stealing files from various popular apps like Telegram, QQ, WeChat, and also targets personal documents and media.
    - **Audio recording:** LightSpy can secretly record audio from the infected device.
    - **Data harvesting:** LightSpy can collect and exfiltrate browser history, WiFi connection lists, installed application details, and even pictures from the device's camera.
    - **System access:** LightSpy can retrieve user KeyChain data and device lists, and execute shell commands for potential full device control.
    - **Chinese origins:** Evidence such as code comments and error messages strongly suggest the attackers behind LightSpy are native Chinese speakers, raising concerns about potential state-sponsored activity.
- **Advanced techniques:** LightSpy employs certificate pinning to prevent detection and interception of communication with its command-and-control (C2) server. Thus, if the victim is on a network where traffic is being analyzed, no connection to the C2 server will be established.

Implications

The reemergence of LightSpy highlights the ongoing threat of sophisticated mobile spyware used for espionage purposes. The targeting of individuals in Southern Asia, coupled with the suspected Chinese origin of the attackers, raises concerns about the potential motives and geopolitical implications of this campaign.

Though typically deployed against a very small percentage of individuals – most usually journalists, activists, politicians and diplomats – hyper-focused spyware attacks are an ongoing and global threat. In recent months, many technology firms have cautioned about the risk of state-sponsored efforts to sway certain electoral outcomes.

“The extreme cost, sophistication and worldwide nature of mercenary spyware attacks makes them some of the most advanced digital threats in existence today,” Apple wrote in its latest advisory.

Technical Details

Infection vector: Based on previous campaigns, initial infection likely occurs through compromised news websites carrying stories related to Hong Kong.

Weaponization: The attack involves a first-stage implant that gathers device information and downloads further stages, including the core LightSpy implant and various plugins for specific spying functions.

Hashes (md5, sha-256)	4b973335755bd8d48f34081b6d1bea9ed18ac1f68879d4b0a9211bbab8fa5ff4 2178d673779605ffb9cf7f2fa3ec8e97
File Name	None
File Size	430816 bytes
File Type/Signature	Mach-O64
Additional information	Loader

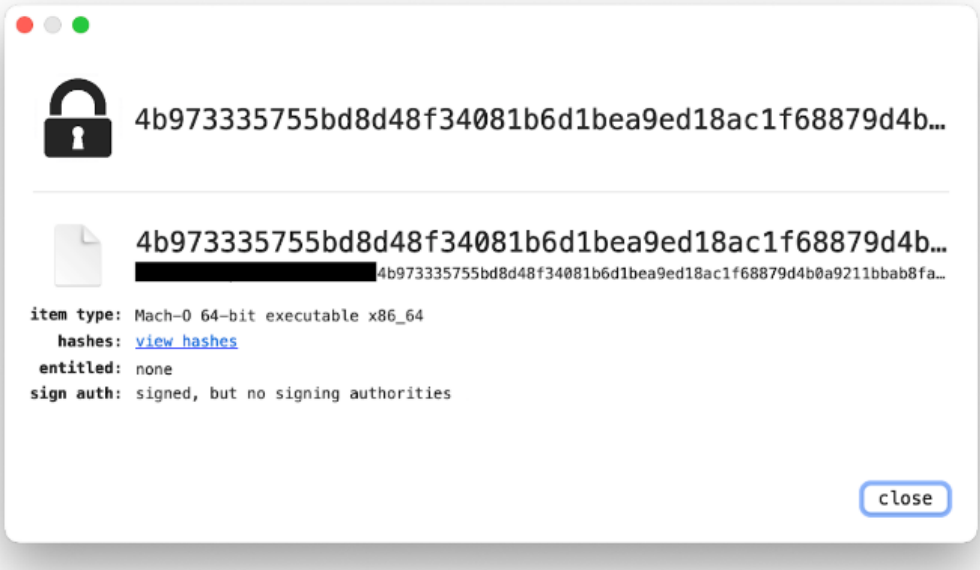


Figure 1. Loader’s signature.

Execution Chain

The Loader initiates the process by loading both the encrypted and subsequently decrypted LightSpy kernel. The core of LightSpy functions as a complex espionage framework, designed to accommodate extensions via a plugin system. The Loader is responsible for loading these plugins, each of which extends the functionality of the main LightSpy implant. Each plugin undergoes a process of secure retrieval from the threat actor’s server in an encrypted format, followed by decryption, before being executed within the system environment.

Hashes (md5,	0f66a4daba647486d2c9d838592cba298df2dbf38f2008b6571af8a562bc306c

sha-256)	59ac7dd41dca19a25a78a242e93a7ded
File Name	C40F0D27
File Size	1252656 bytes
File Type/Signature	Mach-O64
Additional Information	This is the LightSpy core. It supports many different plugins.

The latest LightSpy campaign utilizes a versatile framework known as "F_Warehouse." This framework exhibits a wide range of capabilities, enabling it to:

- **Exfiltrate files:** Systematically search and steal files from the compromised mobile device.
- **Record audio:** Covertly capture audio through the device's microphone.
- **Perform network reconnaissance:** Collect information about WiFi networks the device has connected to.
- **Track user activity:** Harvest browsing history data to monitor online behavior.
- **Application inventory:** Gather details about installed applications on the device.
- **Capture images:** Secretly take pictures using the device's camera.
- **Access credentials**: Retrieve sensitive data stored within the user's KeyChain.
- **Device enumeration:** Identify and list devices connected to the compromised system.

```
v2 = &objc_msgSend;
v3 = +[NSThread currentThread](&OBJC_CLASS___NSThread, "currentThread");
v4 = objc_retainAutoreleasedReturnValue(v3);
+[Utils logDebug:content:](
  &OBJC_CLASS___Utils,
  "logDebug:content:",
  CFSTR("AudioRecorder-Main"),
  CFSTR("env recorder start thread %@"),
  v4);
v5 = &objc_release;
objc_release(v4);
objc_msgSend(*(id *)(a1 + 32), "startAndResume");
v6 = +[NSTimer scheduledTimerWithTimeInterval:target:selector:userInfo:repeats:](
       &OBJC_CLASS___NSTimer,
       "scheduledTimerWithTimeInterval:target:selector:userInfo:repeats:",
       *(_QWORD *)(a1 + 32),
       "startAndResume",
       0LL,
       1LL,
       (double)*(int *)(*(_QWORD *)(a1 + 32) + 60LL));
v7 = objc_retainAutoreleasedReturnValue(v6);
objc_release(v7);
v8 = +[NSTimer scheduledTimerWithTimeInterval:target:selector:userInfo:repeats:](
       &OBJC_CLASS___NSTimer,
```

Figure 2. LightSpy's sound recording plugin.

Figure 2 above shows the code responsible for the audio recording functionality within LightSpy. This plugin enables the attacker to remotely capture and exfiltrate audio recordings from compromised devices, providing them with a powerful tool for eavesdropping on private conversations and the user's immediate surroundings.

Browser History Tracking:

LightSpy exhibits comprehensive browser history tracking capabilities, targeting both Safari and Google Chrome. The extracted data is structured as follows:

- **ID:** Unique identifier for the history entry.
- **URL:** The specific web addresses the user visits.
- **Title:** The title of the visited web page.
- **Time:** Timestamp indicating the time of the user's last visit to the website.

This granular level of detail allows the attacker to gain a deep understanding of the victim's online activities and interests.

Figure 3. LightSpy's browsing information plugin.

LightSpy operators have exhibited a particular interest in exfiltrating data from popular messaging applications such as Telegram, QQ, and WeChat, likely aiming to intercept private communications and gather sensitive information shared within these platforms. Additionally, the malware searches for documents and media files stored on compromised devices, potentially seeking to acquire confidential documents, personal photos, and videos.

Figure 4. Code working with Telegram's data.

Shell Command Execution:

LightSpy's capabilities extend beyond data exfiltration and surveillance. The malware can also download and run a plugin designed to execute shell commands received from the attacker's malicious server. This functionality grants the threat actor the potential for full control over the victim's device, enabling them to perform numerous actions beyond the core functions of the spyware.

Chinese Code Comments:

Further analysis of the plugin code reveals the presence of comments written in Chinese. This strongly suggests that the developers behind LightSpy are native Chinese speakers, raising concerns about the potential involvement of state-sponsored actors and the geopolitical motivations behind the campaign.

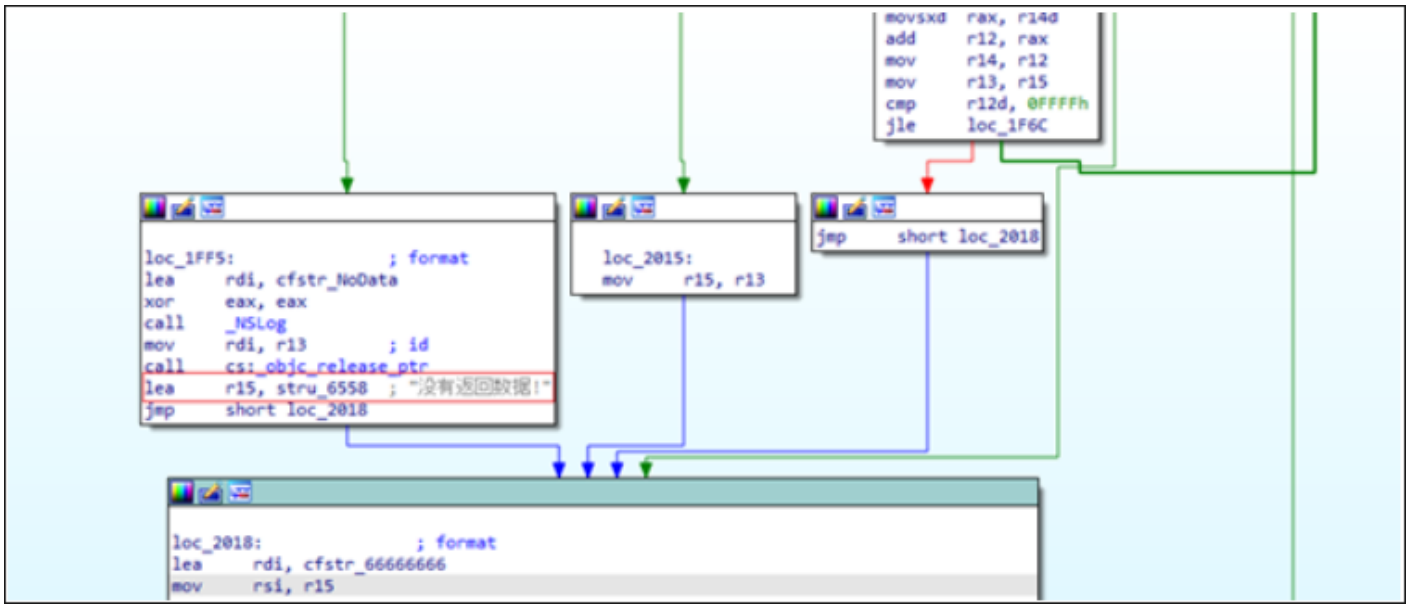


Figure 5. Code's comments in Chinese language (Translation: "Data is not returned").

Command-and-control: LightSpy communicates with a server located at hxxps://103.27[.]109[.]217:52202, which also hosts an administrator panel accessible on port 3458.

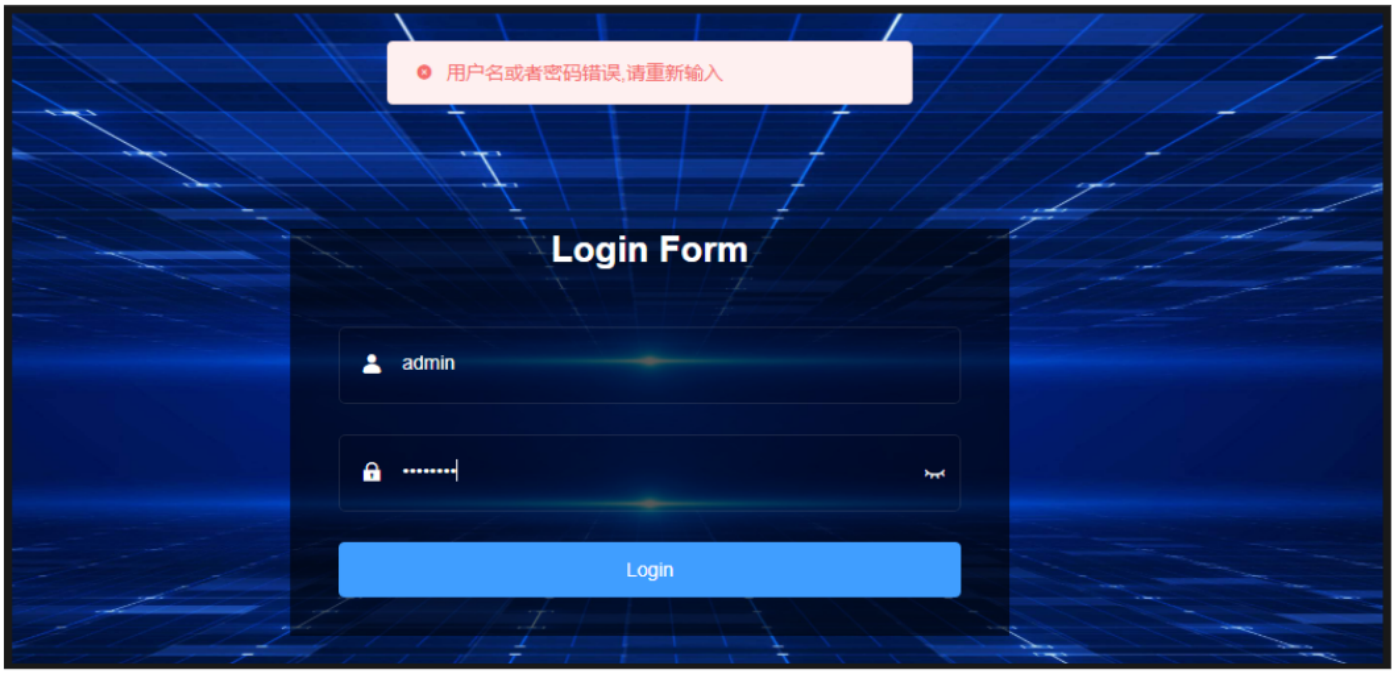


Figure 6. LightSpy's admin panel. (Translation: In the Chinese language, this message says the username or password is incorrect; try again.)

Upon entering incorrect login credentials into the LightSpy operator panel, a warning message is displayed in the Chinese language, further reinforcing the suspected origin and potential attribution of the malware's developers.

Indicators of Compromise (IoCs):

This report includes a comprehensive list of IoCs, including file hashes, URLs, and IP addresses associated with the LightSpy campaign. This information can be used by security teams to detect and mitigate potential infections.

Hashes	Filename
Sha256 - 4511567b33915a4c8972ef16e5d7de89de5c6dffe18231528a1d93bfc9acc59f Md5 - 54570441e91d8e65ea81bb265ba71c8c	libLanDevices
Sha256 -5fb67d42575151dd2a04d7dda7bd9331651c270d0f4426acd422b26a711156b5 Md5 - 480da467b4687549b38eeea4d4ced293	libFileManage
Sha256 - 0f662991dbd0568fc073b592f46e60b081eedf0c18313f2c3789e8e3f7cb8144 Md5 - 6371a942334444029f73b2faa2b76cf6	libAudioRecorder
Sha256 - 65aa91d8ae68e64607652cad89dab3273cf5cd3551c2c1fda2a7b90aed2b3883 Md5 - 32076ae7b19f2669fd7c36e48425acd6	libKeyChains
Sha256 - ac6d34f09fcac49c203e860da00bbbe97290d5466295ab0650265be242d692a6 Md5 - ef92e192d09269628e65145070a01f97	libShellCommand

Sha256 - d2ccbf41552299b24f186f905c846fb20b9f76ed94773677703f75189b838f63 Md5 - cad4de220316eebc9980fab812b9ed43	libProcessAndApp
Sha256 - fc7e77a56772d5ff644da143718ee7dbaf7a1da37cceb446580cd5efb96a9835 Md5 - a2fee8cfdabe4fdeeeb8faa921a3d158	libWifiList
Sha256 - 3d6ef4d88d3d132b1e479cf211c9f8422997bfcaa72e55e9cc5d985fd2939e6d Md5 - f162b87ad9466381711ebb4fe3337815	libBrowserHistory
Sha256 - 18bad57109ac9be968280ea27ae3112858e8bc18c3aec02565f4c199a7295f3a Md5 - 564235b40d78f9c763b5022954ee9aae	libCameraShot
Sha256 - 4b973335755bd8d48f34081b6d1bea9ed18ac1f68879d4b0a9211bbab8fa5ff4 Md5 - 2178d673779605ffb9cf7f2fa3ec8e97	Loader
Sha256 - 0f66a4daba647486d2c9d838592cba298df2dbf38f2008b6571af8a562bc306c MD5 - 59ac7dd41dca19a25a78a242e93a7ded	Core Implant
hxxp://103[.]27[.]109[.]217:52202/963852741/mac/plugins/2e351c7b4de4d3b1 hxxp://103[.]27[.]109[.]217:52202/963852741/mac/plugins/0c377d6b6b074d16 hxxp://103[.]27[.]109[.]217:52202/963852741/mac/plugins/0408ece5a667ec06 hxxp://103[.]27[.]109[.]217:52202/963852741/mac/C40F0D27 hxxp://103[.]27[.]109[.]217:52202/963852741/mac/plugins/f99fcea4aba03364 hxxp://103[.]27[.]109[.]217:52202/963852741/mac/plugins/6a0e40740cb52a1c hxxp://103[.]27[.]109[.]217:52202/963852741/mac/plugins/484c8be6af1675b7 hxxp://103[.]27[.]109[.]217:52202/963852741/mac/plugins/7e3211e5a00d2783 hxxp://103[.]27[.]109[.]217:52202/963852741/mac/plugins/70a5ecc118536683 hxxp://103[.]27[.]109[.]217:52202/963852741/mac/macversion[.]json hxxp://103[.]27[.]109[.]217:52202/963852741/mac/plugins/4d29ee714380cd29 hxxp://103[.]27[.]109[.]217:52202/963852741/mac/plugins/26f7d6b449f01571	

Yara Rule

```
rule LightSpy_Plugins {
        meta:
        description = "Rule to detect LightSpy iOS implant"
        last_modified = "2024-04-11"
```

```
        author = "BlackBerry Threat Research & Intelligence Team"
        version = "1.0"

        strings:
        $a1 = "/Users/air/work/F_Warehouse/mac/new_plugins"
        $a2 = "/Users/air/work/znf_ios/mac/frame/macircloader/macircloader"
        $a3 = "/Users/air/work/F_Warehouse"

        condition:
        (
        (uint32be(0) == 0x3C3F786D) or
        (uint32be(0) == 0x6465780A) or
        (uint32(0) == 0x464c457f) or
        (uint32(0) == 0xfeedfacf) or
        (uint32(0) == 0xcffaedfe) or
        (uint32(0) == 0xfeedface) or
        (uint32(0) == 0xcefaedfe)

        ) and
        ((filesize < 3MB) and any of ($a*))
}
```

Conclusion

The return of LightSpy, now equipped with the versatile “F_Warehouse” framework, signals an escalation in mobile espionage threats. **The expanded capabilities of the malware, including extensive data exfiltration, audio surveillance, and potential full device control, pose a severe risk to targeted individuals and organizations in Southern Asia.**

The evidence pointing towards Chinese-speaking developers, coupled with the precise targeting of individuals potentially involved in political activism and sensitive activities, raises concerns about the potential involvement of state-sponsored actors and the geopolitical motivations behind the campaign. This highlights the need for increased vigilance and robust security measures, particularly for individuals and organizations operating in the targeted region.

The modular nature of LightSpy suggests that its capabilities could evolve further, making it crucial to stay informed about the latest developments and indicators of compromise. By understanding the tactics and techniques employed by this advanced spyware, we can work towards mitigating its impact and safeguarding sensitive information.

Recommendations:

- **Exercise heightened vigilance:** Individuals and organizations in Southern Asia, especially those involved in sensitive activities or political activism, should be particularly cautious about potentially being targeted by LightSpy.
- **Use of Lockdown mode:** Apple recommends individuals who may be targeted by this type of spyware to enable Lockdown Mode to reduce their attack surface. When Lockdown Mode is enabled, certain apps, websites, and features are strictly limited for security and some experiences might not be available at all.

- **Use highly secure voice and messaging solutions:** BlackBerry customers can use SecuSUITE® to encrypt the conversations of its technology and cyber leaders wherever they communicate – in the workplace, at home or travelling abroad.
- **Review the latest threat intelligence:** Stay informed about the latest threats and vulnerabilities via reports offered by reliable security researchers and organizations.
- **Create an incident response plan:** Develop a comprehensive incident response plan to effectively address potential cyberattacks.

In addition, it is recommended that individuals follow security best practices for mobile devices, which include:

- **Update your devices:** Ensure you install the latest software, because that will include the latest security fixes.
- **Use a passcode:** Protect devices by setting a passcode that will prevent unauthorized physical usage.
- **Enable 2FA:** Use two-factor authentication and a strong password for your Apple ID.
- **Beware of unofficial software:** Install apps from the App Store only; don't be tempted by "free" software offered elsewhere on the web.
- **Password hygiene:** Use strong and unique passwords online, and don't reuse the same password across multiple sites. Better yet, we strongly encourage the use of passwordless (e.g. FIDO2) authentication whenever possible.
- **Think before you click**: Don't click on links or attachments from unknown senders. Remember; this now applies just as much on your mobile device as it does on your personal computer.
- **Restart your phone often**: In some cases, restarting your mobile device can help you remove or disable some types of malware.

The BlackBerry Research and Intelligence team would like to thank Dmitry Bestuzhev for his contributions to this report.

Read More:

LightSpy Group is back on VT:
📱 MD5: 2178d673779605ffb9cf7f2fa3ec8e97, 59ac7dd41dca19a25a78a242e93a7ded
C2: 103[.]27[.]109[.]217 🌐 (Hong Kong) #LightSpy #LightRiver #iOS #znf_ios #F_Warehouse

— Dmitry Bestuzhev (@dimitribest) April 10, 2024