New LightSpy Spyware Version Targets iPhones with Increased Surveillance Tactics

The Hacker News ⋮ 3-4 minutes

Spyware / Mobile Security

Cybersecurity researchers have discovered an improved version of an Apple iOS spyware called LightSpy that not only expands on its functionality, but also incorporates destructive capabilities to prevent the compromised device from booting up.

"While the iOS implant delivery method closely mirrors that of the macOS version, the post-exploitation and privilege escalation stages differ significantly due to platform differences," ThreatFabric said in an analysis published this week.

LightSpy, first documented in 2020 as targeting users in Hong Kong, is a modular implant that employs a plugin-based architecture to augment its capabilities and allow it to capture a wide range of sensitive information from an infected device.

Attack chains distributing the malware leverage known security flaws in Apple iOS and macOS to trigger a WebKit exploit that drops a file with the extension ".PNG," but is actually a Mach-O binary responsible for retrieving next-stage payloads from a remote server by abusing a memory corruption flaw tracked as CVE-2020-3837.

This includes a component dubbed FrameworkLoader that, in turn, downloads LightSpy's Core module and its assorted plugins, which have gone up significantly from 12 to 28 in the latest version (7.9.0).

"After the Core starts up, it will perform an Internet connectivity check using Baidu.com domain, and then it will check the arguments that were passed from FrameworkLoader as the [command-and-control] data and working directory," the Dutch security company said.

"Using the working directory path /var/containers/Bundle/AppleAppLit/, the Core will create subfolders for logs, database, and exfiltrated data."

The plugins can capture a wide range of data, including Wi-Fi network information, screenshots, location, iCloud Keychain, sound recordings, photos, browser history, contacts, call history, and SMS messages, as well as gather information from apps like Files, LINE, Mail Master, Telegram, Tencent QQ, WeChat, and WhatsApp.

Some of the newly added plugins also boast destructive features that can delete media files, SMS messages, Wi-Fi network configuration profiles, contacts, and browser history, and even freeze the device and prevent it from starting again. Furthermore, LightSpy plugins can generate fake push notifications containing a specific URL.

The exact distribution vehicle for the spyware is unclear, although it's believed to be orchestrated via watering hole attacks. The campaigns have not been attributed to a known threat actor or group to date.

However, there is some evidence that the operators are likely based in China owing to the fact that the location plugin "recalculates location coordinates according to a system used exclusively in China." It's worth noting that Chinese map service providers follow a coordinate system called GCJ-02.

"The LightSpy iOS case highlights the importance of keeping systems up to date," ThreatFabric said. "The threat actors behind LightSpy closely monitor publications from security researchers, reusing newly disclosed exploits to deliver payloads and escalate privileges on affected devices."