Mphasis
The Next Applied

LightSpy Malware

Date: 30th May 2024 | Severity: High

Summary

- LightSpy is a modular iOS and Android surveillance framework used to steal a wide variety of data from people's mobile devices, including files, screenshots, location data, voice recordings during WeChat calls, and payment information from WeChat Pay, and data exfiltration from Telegram and QQ Messenger.
- LightSpy's control panel by exploiting a misconfiguration that allowed unauthorized access to the authenticated interface, gaining insights into the functionality, infrastructure, and infected devices.
- The Android version of this malware on the same C2 as the macOS version, it doesn't appear the iOS version is also present. In this article, we'll only be focusing on the macOS implant. For more information of the Android version.

Attack Vectors

- The threat actors use WebKit flaws CVE-2018-4233 and CVE-2018-4404 to trigger code execution within Safari, targeting macOS 10.13.3 and earlier. Initially, a 64-bit MachO binary disguised as a PNG image file is delivered on the device, decrypting and executing embedded scripts that fetch the second stage.
- The second stage payload downloads a privilege escalation exploit ("ssudo"), an encryption/decryption utility ("ddss"), and a ZIP archive ("mac.zip") containing two executables ("update" and "update.plist").
- LightSpy core can also execute shell commands on the device, update its network configuration, and set an activity timetable to evade detection.
- Though the malware uses 14 plugins on Android and 16 plugins on its iOS implant, the macOS version uses the following ten soundrecord, browser , cameramodule, FileManage , keychain, LanDevices, softlist, ScreenRecorder , ShellCommand, wifi.
- These plugins enable LightSpy to perform comprehensive data exfiltration from infected macOS systems, while its modular design gives it operational flexibility.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• afd03337d1500d6af9bc447bd900df26786ea4a4 • 0f66a4daba647486d2c9d838592cba298df2dbf38f2008b6571af8a562bc306c • fd49866245721acc6e7431ec61b066696b72a1e1 • 0563225dcc2767357748d9f1f6ac2db9825d3cf9 • 476c726b58409a8e3e6cf8fb6bb7d46596917e24 • 33c39728a0393d4271f27cc1d85cf3c1610be333 • 9a00f6ca0d9140316f9ae03f79c7511cec32849f • 8f390335b571297a9eb605576745876666ee7f6a • 7aceb8db03b8b8c7899982b5befcaf455a86fe0b • c65817a55b003462d48189875f18fa8bdb57b402 • 30e33f1188ca4cffc997260c9929738594e7488c • 8e7e8d896ed61bea7a49271e2e6ffc982942e5c7
IP	• 103[.]27[.]109[.]217 • 46[.]17[.]43[.]74 • 45[.]134[.]1[.]180 • 45[.]83[.]137[.]83
Domain	• spaceskd[.]com • messager[.]cloud • news.hkrevolution[.]club • appledaily.googlephoto[.]vip • www.facebooktoday[.]cc
URL	• http[:]//103.27.109.217:52202/963852741/mac/plugins/f99fcea4aba03364

Recommendation

- Keep Your System Updated: Regularly update your macOS to the latest version. Security patches often address vulnerabilities that could be exploited by malware like LightSpy.
- Be Cautious with Downloads and Installations: Only download software from trusted sources (such as the Mac App Store or official developer websites) and avoid downloading cracked or pirated software, as these may contain hidden malware.
- Use Security Software: Install reputable security software that can detect and prevent malicious activity. Consider using antivirus solutions specifically designed for macOS.
- Monitor for Suspicious Activity: Keep an eye on any unusual behavior on your system, such as unexpected network connections or high CPU usage. Investigate any unknown processes running in the background.
- Network Traffic Analysis: Monitor network traffic using tools like Wireshark or Little Snitch. Look for any suspicious connections to known LightSpy-related domains or IP addresses.
- Review Installed Applications: Regularly review the list of installed applications on your Mac. Uninstall any software that you no longer use or trust.
- Backup Your Data: Regularly back up your important files to an external drive or cloud storage. In case of a malware infection, having backups ensures you can restore your data.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https[:]//www.bleepingcomputer.com/news/security/macos-version-of-elusive-lightspy-spyware-tool-discovered/
- https[:]//www.huntress.com/blog/lightspy-malware-variant-targeting-macos
- https://dashboard.ti.insight.rapid7.com/#/tip/cyber-term/661d542007cd9a98ad21d8af