مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

LightSpy Mobile Espionage Campaign

Tracking #:432315765

Date:16-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed resurgence of a sophisticated mobile espionage campaign known as LightSpy targeting iPhone users.

TECHNICAL DETAILS:

The LightSpy mobile espionage campaign has resurfaced, targeting iPhone users. This campaign is a renewed cyber espionage effort that delivers an Apple iOS spyware implant called LightSpy.

Target Platform: Apple iOS
Delivery Method: Watering hole attacks compromising legitimate news websites.
Capabilities:

- Modular framework allowing for potential expansion of functionalities
- Data exfiltration of MS messages, phone call history, connected WiFi history, and the browser history of Safari and Chrome.
- System access: LightSpy can retrieve user KeyChain data and device lists, and execute shell commands for potential full device control
- Highly precise location data: This includes not only GPS coordinates but potentially even building floor information.
- Audio recordings: LightSpy can capture audio during Voice over IP (VoIP) calls.
- Payment information: The malware exhibits the ability to steal data from popular mobile payment platforms.

INDICATORS OF COMPROMISE(IoCs):

Attached File

RECOMMENDATIONS:

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Update Apple Devices: Ensure all iPhones and iPads are updated to the latest iOS version to patch potential vulnerabilities exploited by LightSpy.

- Be Wary of Unfamiliar Links: Exercise caution when clicking on links, particularly from unexpected sources or emails. Malicious actors often use compromised websites to distribute malware.
- Consider using a mobile device management (MDM) solution or mobile threat defense (MTD) solution to detect and mitigate potential threats.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings (e.g. IOCs, TTPs...etc).

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

1. https://blogs.blackberry.com/en/2024/04/lightspy-returns-renewed-espionage-campaign-targets-southern-asia-possibly-india