AWARENESS

Malicious System Update App Targets Android Users With Malware

Malware Steals Data, Messages, Images; Takes Control of Phones

Android users are now facing a new malware threatening their personal information. The new Android malware poses as a System Update app that actually delivers spyware on the target devices.

New 'System Update' Android Malware
Researchers from Zimperium Labs zLabs have shared details about a new malware targeting Android users. As observed, this new malware is basically spyware that poses as a 'System Update' app to trick Android users.

Briefly, this remote access trojan (RAT) reaches a device once the victim user downloads the malicious app. Once installed, the malware then stealthily executes to take control of the device and steal data.

Regarding the data it accesses, this includes messages, database files of messenger apps, clipboard data, notifications, contacts, call logs and other device data. It also records audios and calls, takes pictures through device cameras, lists the apps installed on the device, and accesses GPS location.

It then transmits the exfiltrated data to its Firebase Command and Control (C&C) where it first registered the infected device. Whereas, at the time of device registration, it transmits certain details to the C&C such as the existence of WhatsApp on the device, battery status, internet connection, storage status, and Firebase messaging service token.

Tactics To Stay Undetected
Unlike most other Android malware, this spyware doesn't continuously exfiltrate data in bulk. Rather it activates every time a change in the data is made, for instance, the addition of a new contact or new photos. It then only steals the most recent data.

Also, in the case of videos or large image files, the malware prefers stealing the thumbnails instead. Since they are small in size, stealing thumbnails won't impact the bandwidth, thus keeping the malware hidden.

Besides, the malware also ensures not to transmit more stolen details over the mobile data connection. It waits for the device to connect to WiFi to transmit data stolen from all folders.

Moreover, the malware also hides the app icon from the menu to remain hidden. More details about this malware are available in Zimperium's blog post.

Malware Not On Google Play Store
The researchers have confirmed that this malicious System Update application doesn't exist on Google Play Store. Hence, this scam particularly threatens the Android users who frequently use third-party app stores.

Thus, to prevent oneself from becoming a victim, all users must avoid interacting with third-party app stores.

Source: LHN. Abeerah Hashim March 29, 2021

Focus Audits, LLC
11301 N. US Hwy. 301
Ste. 105
Thonotosassa, FL 33592
(813) 638-8565
www.FocusAudits.com