Android “System Update” malware steals photos, videos, GPS location

First spotted by the research team at Zimperium zLabs, the newly found malware is already detected by Malwarebytes for Android. It does not have a catchy name, but because of its capabilities and its method for going unnoticed, we are calling it Android/Trojan. FakeSysUpdate is not available on the Google Play store, and it is currently unclear how it is being delivered to Android devices. Even more obscured is the visibility of the app to victims.

Once FakeSysUpdate is implanted on a device, it disguises itself to its victims by masquerading as a generic «System Update» application. In fact, when a threat actor uses FakeSysUpdate to steal targeted information from an infected, asleep device, FakeSysUpdate will also send a fraudulent notification posing as a «System Update» that is «Searching for update». Beneath the surface, FakeSysUpdate can let a malicious actor steal highly sensitive information while also granting them dangerous control of a victim’s device. According to Zimperium zLabs, the malware can allow a threat actor to monitor GPS locations, record phone calls, record ambient audio, take photos from the front-facing and rear-facing cameras on a device, observe the device’s installed applications, inspect bookmark and search history from Google Chrome, Mozilla Firefox, and Samsung Internet Browser, and steal SMS messages, phone contacts, and call logs.

If you’ve read our coverage on these types of capabilities in the past, you might think that FakeSysUpdate is just the latest stalkerware-type app on the market. That’s contrary to many of the stalkerware-type apps that we see, which are, for lack of a better word, «user-friendly.» They do not require a high-tech proficiency to use or understand. Instead, these apps have familiar layouts, intuitive designs, and easy-to-use commands. For many apps, it’s as simple as logging into a web platform, clicking a menu item, and browsing through private photos without any consent.

Stalkerware-type apps do not hide in the shadows. They flood Google results for anyone searching how to spy on their romantic partners. We thank Zimperium zLabs for discovering this malware and for bringing it to the public’s attention.

What can the malware do?

The mobile application poses a threat to Android devices by functioning as a Remote Access Trojan (RAT) that receives and executes commands to collect and exfiltrate a wide range of data and perform a wide range of malicious actions, such as:

- Stealing instant messenger messages;
- Stealing instant messenger database files (if root is available);
- Inspecting the default browser’s bookmarks and searches;
- Inspecting the bookmark and search history from Google Chrome, Mozilla Firefox, and Samsung Internet Browser;
- Searching for files with specific extensions (including .pdf, .doc, .docx, and .xls, .xlsx);
- Inspecting the clipboard data;
- Inspecting the content of the notifications;
- Recording audio;
- Recording phone calls;
- Periodically take pictures (either through the front or back cameras);
- Listing of the installed applications;
- Stealing images and videos;
- Monitoring the GPS location;
- Stealing SMS messages;
- Stealing phone contacts;
- Stealing call logs;
- Exfiltrating device information (e.g., installed applications, device name, storage stats); and
- Concealing its presence by hiding the icon from the device’s drawer/menu.

How prevent:

- Avoid downloading apps from third-party app stores if you are not sure, also, only download updated to apps from Google Play store only.
- Remember all system updates are published by OEM (Original Equipment Manufacturer) and can be found under the Updates section inside the Settings menu.

- Invest in a good antivirus app and set regular scans.
- It would also be good to limit your app downloads and the storage access permissions.

References:

- https://blog.malwarebytes.com/cybercrime/mobile/2021/04/android-system-update-malware-steals-photos-videos-gps-location/?web_view=true
- https://www.news18.com/news/tech/android-system-update-spyware-can-steal-your-photos-money-record-calls-and-track-you-too-3603692.html
- https://blog.zimperium.com/new-advanced-android-malware-posing-as-system-update/