

1. **Introduction.** A new Android spyware "**Skygofree**" has been found that provides hackers full control of infected devices remotely. Skygofree is capable of taking pictures, capturing video, and seizing call records, text messages, geolocation data, calendar events, and business-related information stored in device memory.

2. **Technical analysis**

- a. Spyware is being distributed through fake web pages and social media platforms.
- b. Hackers have the ability to control the spyware via HTTP, XMPP, binary SMS and FirebaseCloudMessaging (or GoogleCloudMessaging in older versions) protocols.
- c. Skygofree - became a sophisticated multi-stage spyware tool that gives attackers full remote control of the infected device using a reverse shell payload and p command and control (C&C) server architecture.
- d. The malware is highly sophisticated having a self-protection feature which is implemented in almost every service.
- e. Skygofree includes multiple exploits to escalate privileges for root access, granting it ability to execute most sophisticated payloads on the infected Android devices. Details of vulnerabilities exploited are as under:-
 - (1) CVE-2013-2094.
 - (2) CVE-2013-2595.
 - (3) CVE-2013-6282.
 - (4) CVE-2014-3153.
 - (5) CVE-2015-3636.
- f. As per analysis there are components that form an entire spyware for the Windows platform too this shows that malware can a/ windows operating system.

3. **Affected Product Versions.** The spyware affects following platforms as under:-

- a. Android
- b. Windows

4. **Mitigation Measures** Following best practices are suggested in this regard:-

- a. Install apps Only from official stores. It's wise to disable installation Of apps from third-party sources, which you can do in your smart phone settings,
- b. If in doubt, don't download. Pay attention to misspelled app names' , small

numbers of downloads, or dubious requests for permissions any of these things should raise flags.

- c. Install a reliable security solution for example, Kaspersky Internet Security for Android: This will protect your device from most malicious apps and files, suspicious websites, and dangerous links.
- d. Be careful while using social media profiles/ pages and don't click or download
- e. Don't open any document received via email or any unknown resource.
- f. Keep all the software's browser and operating system up-to-date.