Hackers can spy on Samsung users with pre-installed apps

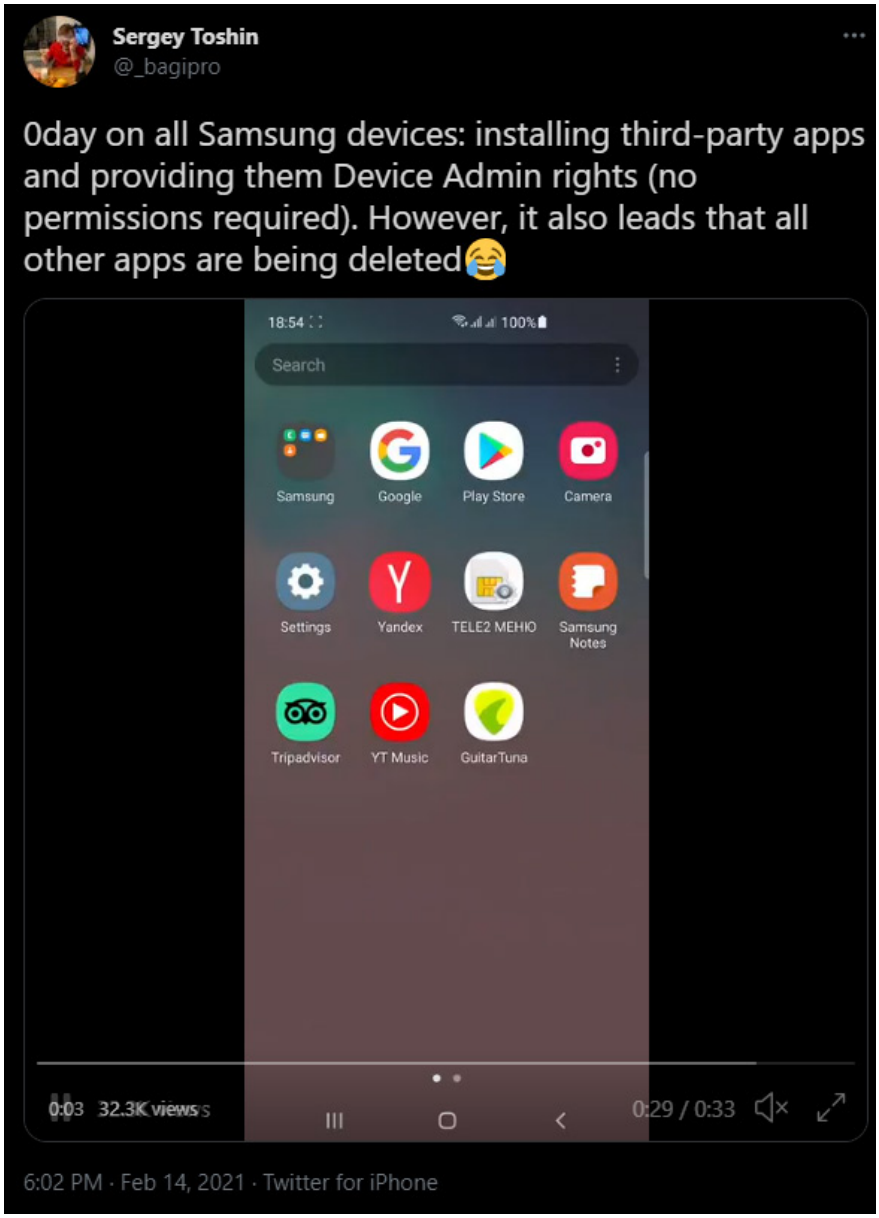
Sergey Toshin - founder of Oversecure company specializing in mobile application security, has found more than a dozen vulnerabilities affecting Samsung devices, allowing hackers to steal information and track users.

Samsung is working on patching multiple vulnerabilities affecting mobile devices, which can be used for spying or for total system control. The bugs discovered are part of a larger set of bugs that were discovered and reported by Sergey Toshin, founder of Oversecured, a company specializing in mobile application security.

Security expert Toshin has found more than a dozen vulnerabilities affecting Samsung devices.

Currently, the details of the three vulnerabilities are still unclear because they affect users too much. Without going into specifics, BleepingComputer quoted Toshin as saying that the least serious of these bugs is that the flaw could help attackers steal the content of text messages if they trick victims. .

However, there are two other vulnerabilities that are more serious because they do not 'show' but operate stealthily. Exploiting them requires no action by the user of the Samsung device. An attacker could exploit those two vulnerabilities to read and/or write arbitrary files with higher permissions.



It is not clear when the fixes will be shipped to users, as the process usually takes about two months due to various tests of the patch to ensure that it does not cause other problems.

In Samsung alone, hackers have made nearly $30,000 since the beginning of the year when they revealed 14 problems. The remaining three vulnerabilities are currently waiting to be patched. In addition, seven of the bugs patched cost Samsung $20,690.

The hacker discovered the bugs in pre-installed apps on Samsung devices using the Oversecure scanner he created specifically for the task.

In February, the hacker reported the vulnerabilities and also published a video demonstrating how a third-party app gained device admin rights. The exploit - a zero-day vulnerability at the time - had an unexpected side effect: during the process of getting elevated privileges, all other apps on the Android phone were deleted.

This bug (CVE-2021-25356) was patched in April. It affected the Managed Provisioning application. Hacker received $7,000 for reporting this bug.

Additionally, Toshin received another hefty bounty ($5,460) for sharing details with Samsung about an issue (CVE-2021-25393) in the Settings app. This bug would allow a hacker to gain read/write access to arbitrary files with system user privileges.

In February, another bug that cost Samsung $4,850 also allowed hackers to write arbitrary files as a Telephony user, with access to call details and SMS/MMS messages.

In May, Samsung patched most of the above bugs. However, according to Toshin, Samsung has also patched seven other bugs that he disclosed.

These risks create opportunities for hackers to gain read/write access to users' contacts, access to SD cards, and leak personal information such as phone numbers, addresses, and emails.

Users are advised to get the latest firmware updates from the manufacturer to avoid potential security risks.

Toshin has reported more than 550 vulnerabilities in his career, earning over 1 million USD in bounty through HackerOne platform and various bounty programs.

You finished reading the article "**Hackers can spy on Samsung users with pre-installed apps**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com