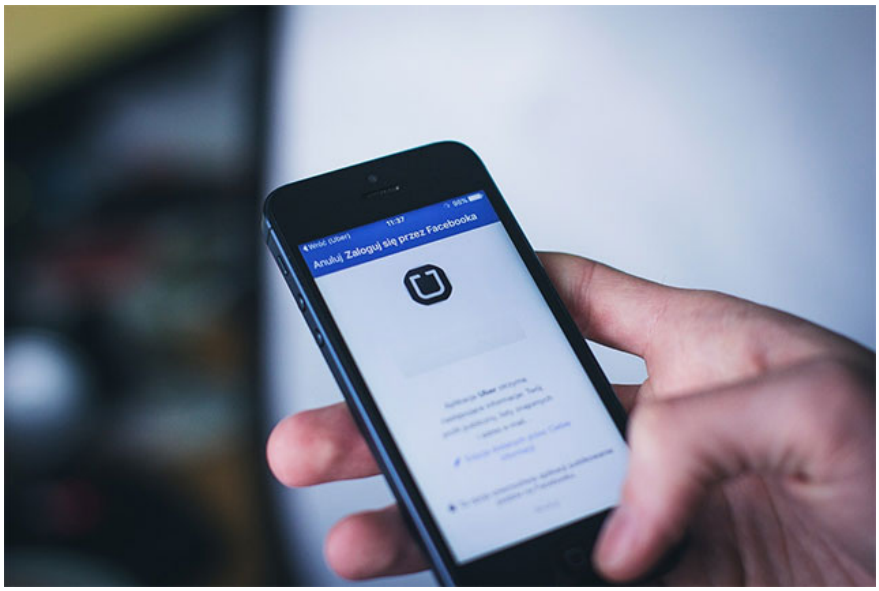
Android apps contain malicious code that uses motion sensors to avoid detection

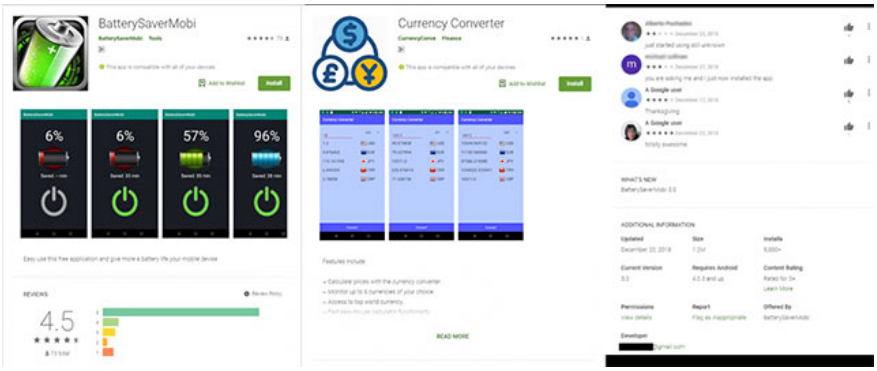
The sad fact is that after many efforts by Google to isolate the Play Store from malware, malicious applications somehow find new ways to deceive measures. malware prevention ...

The sad fact is that after many efforts by Google to isolate the Play Store from malware, malicious applications somehow find new ways to deceive measures. Advanced malware prevention and access to Google services to spread malicious code to Android users.

Recently, two typical malicious applications on Play Store have been debunked by senior security experts of Trend Micro's security research group, and at the same time they discovered that there were thousands Android users have downloaded and installed these two malware, which means the risk of spreading new malicious code on thousands of different devices.



These new malware-containing applications include a currency converter called Currency Converter, and a battery-optimized app called BatterySaverMobi.Worse, these malicious Android apps are trusted by many users to install on their devices because they use a lot of fake five-star reviews.Specifically, the malicious code on these two applications uses the motion sensor of infected Android devices to monitor and hide before automatically installing a dangerous Trojan named Anubis.This clever trick is more dangerous than the traditional stealth techniques commonly found on known types of malicious code in that they can hide in a separate piece of hardware like a motion sensor to avoid being detected when The researchers ran the emulator (using less sensors) to scan those malicious applications.



1. 773 million emails, 21 million passwords were revealed on the Internet, this is the largest personal data leak in history

"When users move, their device often generates a motion sensor data. These malware developers assume that the sandbox used to scan for malware is an emulator. there is no motion sensor and therefore, it is not possible to create such kind of data In this case, security experts can determine whether the application is running in the sandbox environment by examining the data. The sensor " , researchers from security research group Trend Micro explained in a blog post published last Thursday.

Once downloaded and installed, the malicious application will use the device's motion sensor to detect whether the user or device is moving to adjust malicious and malicious behavior. avoid detection from users as well as security applications.

Then, as soon as the sensor data is accessible, the application will run malicious code and try to trick victims into downloading and installing malicious Anubis APKs through bogus system updates. , hide the ball as a "stable update version of Android".

If the user agrees to download a fake system update, the integrated malware spreaders will use requests and responses to legitimate services including Twitter and Telegram . to link connect to its required command and control server (C&C), and automatically download the Anubis Trojan on the infected device.

"One of the ways application developers use to hide malicious servers is to encrypt it in Telegram and Twitter website requests. The malware driver will ask for feedback with Telegram. or Twitter on the device that is running, then it automatically connects to the C&C server and checks the commands with the HTTP POST request.If the server responds to the application with the APK command and attaches the download URL, then Anubis will be 'dropped into' in the device's background launcher, " the researchers explained.

After being spread in the background, Anubis Trojan will obtain the user's bank account login information by using the integrated keylogger or taking a screenshot of the user when they insert any login information. Any banking application.

According to Trend Micro researchers, the latest version of Anubis has been spread to 93 different countries and targeted users of at least 377 financial application variants to extract detailed information. about their bank account.

1. New malware uses Google Drive as a command-and-control server

Not only that, the Trojan also has the ability to access contacts and location lists, send spam messages to contacts, save the number of calls on the device, and record voice calls and change sets. remember outside.

In the latest move, Google removed two malicious applications from Play Store.However, as the Internet has grown, security issues have become much more complicated.So, instead of relying on the behavior of security service providers or experts, the best way to protect yourself against such malicious software is to be vigilant when downloading applications. Even from reputable services such as Google Play Store, and more importantly, be cautious about applications that require you to provide administrative rights by simple means that you have granted Take full control of your device for that application.

See more:

1. Malware and user security bugs are found in top free VPN applications
2. Google paid a fine of 50 million euros after allegedly violating the General Data Protection Act in France
3. MySQL vulnerabilities allow malicious servers to steal data from customers
4. Microsoft shook hands with VirusTotal in resolving malicious code issues that affected MSI files