BankBot is back on Play Store - an uninterrupted story about malware on Android

After Google's efforts to block malware from Play Store, malicious applications still find ways to trick Android anti-malware and poisoning tools.

After Google's efforts to block malware from Play Store, malicious applications still find ways to trick Android anti-malware and poisoning tools.

A group of researchers has discovered two new malware campaigns targeting Google Play Store, one of which spreads a new version of BankBot. This is a bank trojan that mimics real banking applications to steal credit card login information by displaying overlapping banking applications, including Citibank, WellsFargo, Chase and DiBa.

With the ability to display fake overlay, BankBot also performs many other tasks such as sending and interfering with SMS, making calls, tracking devices that infect and steal contacts. Google deleted at least four previous versions of the trojan, but it still found a way to get into Play Store.

The second campaign not only spreads BankBot but also Mazar and Red Alert, described in detail on ESET's blog.*https://www.welivesecurity.com/2017/11/15/multi-stage-malware-sneaks-google-play/*

According to an analysis of the mobile threat research group at Avast in partnership with ESET and SfyLabs, BankBot's latest variant hidden in the Android app looks credible.

First discovered on October 13, BankBot uses special technology to bypass Google's automatic check, such as after 2 hours of operation after receiving admin rights and issuing applications under another developer name. .

After tricking the victim to download the device, it will check the applications installed on the device in the list of 160 banking applications. If found, it will download and install the BankBot APK from the C&C server, tricking the victim into giving admin rights by pretending to be Play Store or updating the system.

Once it has taken over, it will overwrite the real application, thereby stealing the user's account information. Because many banks use 2-factor authentication, BankBot is also capable of interfering with SMS messages.

The latest BankBot version does not use the Accessibility Service feature because Google has blocked this feature for almost every application. Applications that have BankBot have also been removed from the Store by Google.

Since BankBot needs to download external payloads, go to **Settings** > **Security** > turn off **Allow Installation Of Apps From Sources Other Than The Play Store** to prevent 3rd party APKs from being installed on the phone.

See also: Trojan banks surpass the malware defense of Google Play