

Discover a software stealing Facebook account on the phone developed by Vietnamese hackers

Recently, security experts have discovered a new stream of malicious code called GhostTeam used to steal Facebook login information. Since the code uses Vietnamese, security experts believe that a Vietnamese developer developed GhostTeam and uploaded the Play Store.

Although Google has come up with a number of measures to clean up the Google Play app market, malicious codes still appear regularly and become more and more dangerous.

Recently, security experts have discovered a new stream of malicious code called GhostTeam used to steal Facebook login information and display ads on user devices. This malicious code includes at least 56 Google Play apps such as flashlights, QR code scanners, compasses, enhancing device performance, video downloader .

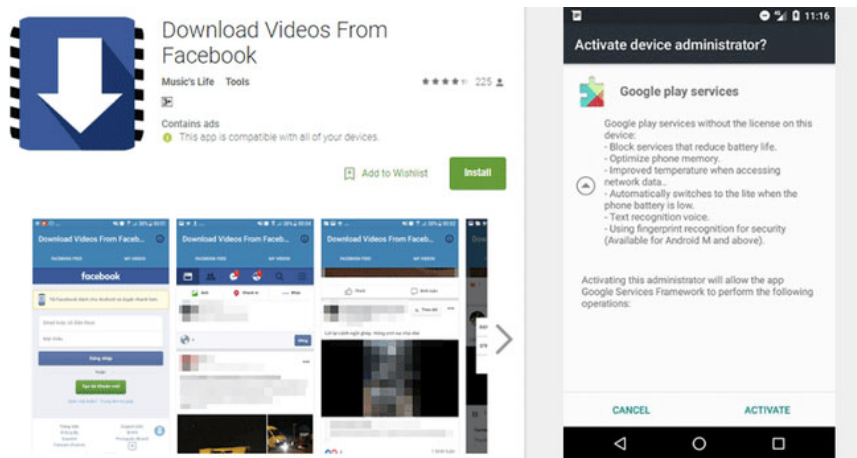
Since the code uses Vietnamese, security experts believe that a Vietnamese developer developed GhostTeam and uploaded the Play Store.

According to malware researchers GhostTeam primarily affects users residing in India, Indonesia, Brazil, Vietnam and Phipippines.



A special feature is that now in Vietnam there is also an organization operating under the name GhostTeam, which was established in 2014 and is now operating underground. It is not yet clear whether this group is the author of the code for GhostTeam.

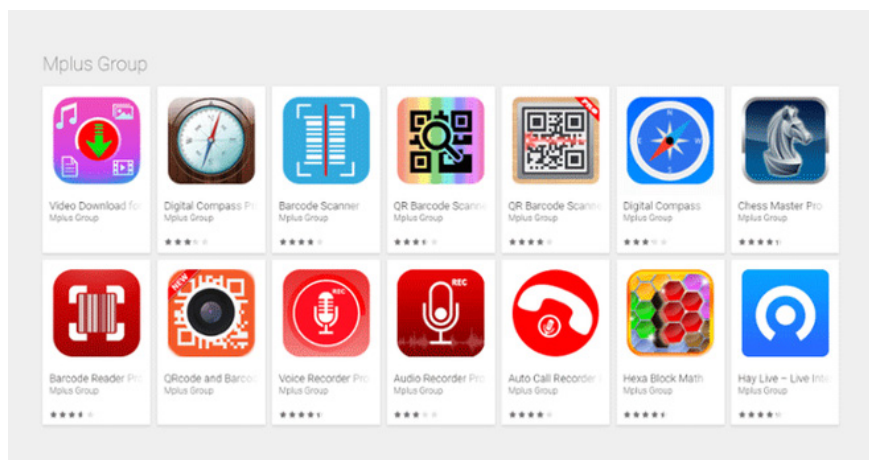
These malware applications are allowed to be distributed on Google Play applications because they do not contain any malicious code. After installation, these applications will test the device environment if they are not virtual environments or simulation environments, then the application will download malicious modules. They will then issue a message prompting the user to approve administrative rights so that the application can stay permanently on the device.



How do malicious users steal Facebook login data?

These malware do not exploit any system or application vulnerabilities, they just need to use a simple phishing program to steal user credentials. Every time a user opens a Facebook application, these malicious code will launch a WebView component with a Facebook-like login page and ask users to re-verify their Facebook account by logging back into Facebook. After obtaining user login information, WebView will send them to the control server of the hackers.

Hackers can use this stolen information to spread malicious code, create malware that exploits virtual money or sell them in black markets because stolen Facebook accounts can reveal lots of financial and personal information of users.



Google has removed the app completely from Google Play as soon as it receives the notice. But to ensure safety, users need to review the device and remove applications of unknown origin, enable the Google Play Protect feature to filter malicious applications. In addition, users need to pay attention to avoid downloading applications from unknown sources and from unreliable developers. In addition, installing anti-virus programs is essential to enhance the security on the device.

See more:

1. Discovered a new line of malicious Android code that steals user data on the electronic application market
2. It turns out this is how hackers attack your computer through the main screen
3. The new vulnerability on Intel allows hackers to take control of your computer within 30 seconds

You finished reading the article "**Discover a software stealing Facebook account on the phone developed by Vietnamese hackers**" 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.