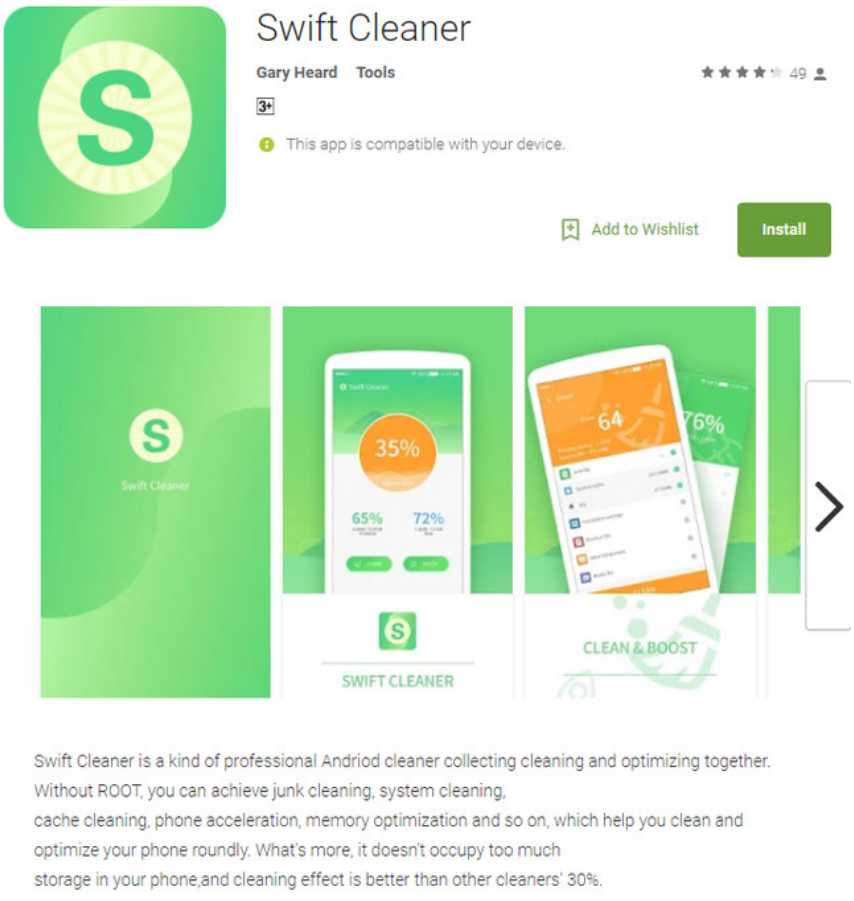
Discovered a new line of malicious Android code that steals user data on the electronic application market

Recently a security expert at Trend Micro discovered a new line of malicious code first written in Kotlin, a kind of static language for Android programmers.

Recently, security expert at Trend Micro discovered a new line of malicious code first written in Kotlin, a kind of static language for Android programmers, spread on Googplay electronic application market. The new malicious code belongs to Androidos_bkotklind.Hrx line hidden in the form of utility called 'Swift Cleaner'.



According to the description, this application has the ability to clean up and optimize Android devices. But if users download Swift Cleaner and install it, the malicious code will send device configuration information to the

control server and start performing tasks including sending messages, collecting Wifi data as well as injections. Malicious Javascript code to secretly steal device's data. In addition, this malicious code also performs many other malicious behaviors such as sending SMS, URL forwarding, clicking ads and without the request or the permission of the user can still automatically register the news service. Paid message.

What is KOTLIN?

Kotlin is a new open source programming language for cross-platform applications. This is the first language used to program Android apps and it is the language used to write applications like Netflix, Pinterest, and Twitter.

Since its publication, this is the first case of a malicious code on Android written in Kotlin.

How to remove malicious code

Google Play has removed Swift Cleanerra application from the electronic market right after receiving Trend Micro's notification. But before that there were several tens of thousands of downloads of this application. If you accidentally downloaded and installed this application on devices, then quickly uninstall the application like any other normal application.

To ensure the safety of your devices from malicious applications, users should only download applications from reputable developers and use AntiVirus applications.

See more:

1. The Chrome gadget secretly exploits virtual money, making it slow
2. Warning: a new variant of the virus that fills virtual money via Facebook Messenger will appear every 10 minutes
3. How to remove the code as a video format on Facebook Messenger