

# Doctor Web anticipates increase in number of banking Trojan attacks on Android users

Published: 2017-01-20 · Archived: 2026-04-06 00:28:04 UTC

By continuing to use this website, you are consenting to Doctor Web’s use of cookies and other technologies related to the collection of visitor statistics.

[Learn more](#)

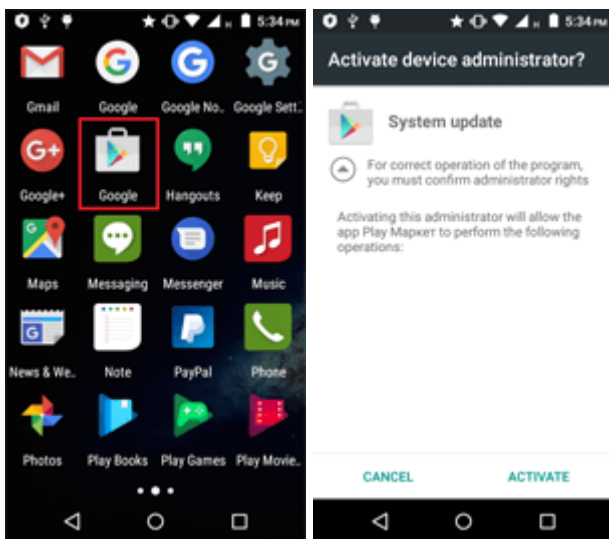
20.01.2017

Hot news | Threats to mobile devices | All the news | Virus alerts

January 20, 2017

**Modern Android banking Trojans are created by virus writers and sold for serious sums as commercial products via underground Internet platforms. However, the source code of one such malicious application was recently made public on a hacker forum, along with instructions on how to use it. Doctor Web security researchers believe that this may lead to a significant increase in the number of attacks involving Android banking Trojans.**

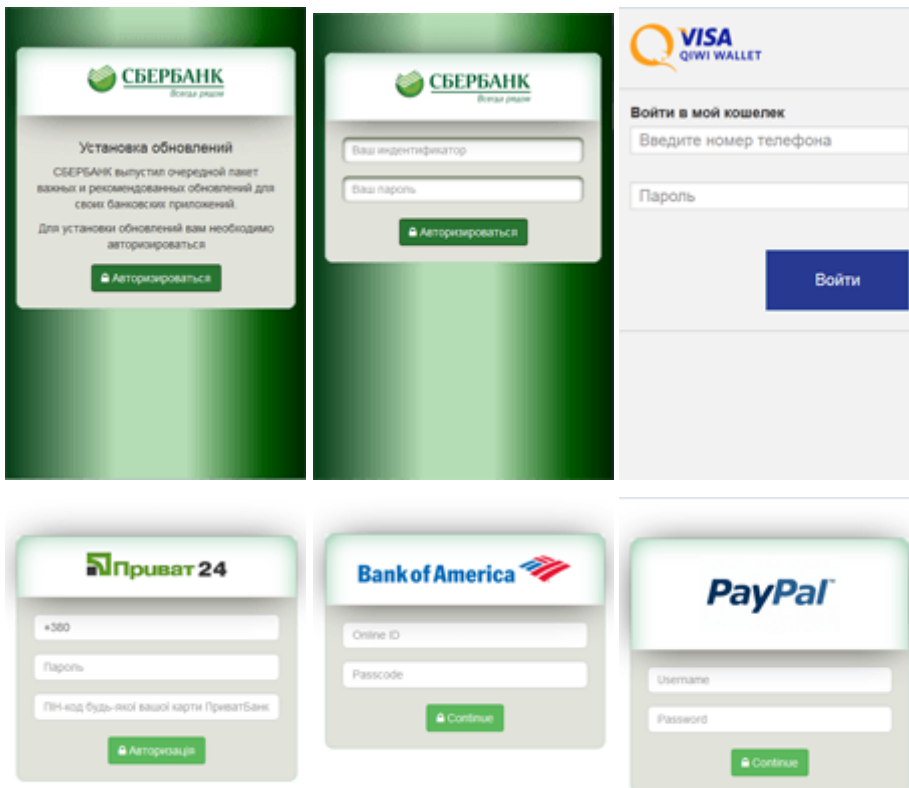
The virus writers published the source code of the new malicious application just one month ago, but Doctor Web security researchers have already detected an Android Banker that has been created using the information published by the cybercriminals. This Trojan, dubbed [Android.BankBot.149.origin](#), is distributed under the guise of benign programs. When a smartphone or tablet user installs and runs [Android.BankBot.149.origin](#), the banker prompts the user to grant it administrative privileges to hinder its removal from the system. After that it hides itself from the user by removing its shortcut from the home screen.



Then [Android.BankBot.149.origin](#) connects to the command and control (C&C) server and awaits instructions. The Trojan can execute the following actions:

- send SMS messages;
- intercept SMS messages;
- request administrator privileges;
- send USSD requests;
- obtain all contact list phone numbers;
- send SMS messages containing the text specified in a command to all contact list numbers;
- track device geolocation via GPS satellites;
- request additional permission on devices using the most recent Android versions to send SMS messages, make calls, and access the contact list and GPS receiver;
- receive an executable file containing a list of attacked banking applications;
- show phishing dialogs.

Like many other Android bankers, [Android.BankBot.149.origin](#) steals confidential user information by tracking the launch of online banking applications and payment system software. One sample examined by Doctor Web security researchers controls over three dozen such programs. Once [Android.BankBot.149.origin](#) detects that any of the aforementioned applications have been launched, it loads the relevant phishing input form to access user bank account login and password information and displays it on top of the attacked application.



The Trojan not only steals mobile banking login credentials but also bank card information belonging to the owner of the compromised device. For this purpose, [Android.BankBot.149.origin](#) tracks the launch of such popular



will appear. Dr.Web for Android successfully detects [Android.BankBot.149.origin](#); therefore, this malicious program poses no threat to our users.

[More about this Trojan](#)

11104 en 5

0

## **Doctor Web's Q1 2026 review of virus activity on mobile devices**

01.04.2026

Virus reviews

[Read](#)

## **Doctor Web's Q1 2026 virus activity review**

01.04.2026

Virus reviews

[Read](#)

## **Dr.Web for personal computers receives SKD AWARDS product excellence distinction**

24.03.2026

Corporate news | Dr.Web products

[Read](#)

---

Source: <https://news.drweb.com/show/?i=11104&lng=en>