Doctor Web discovered a clipper Trojan for Android

Published: 2018-08-07 · Archived: 2026-04-06 00:23:50 UTC

07.08.2018

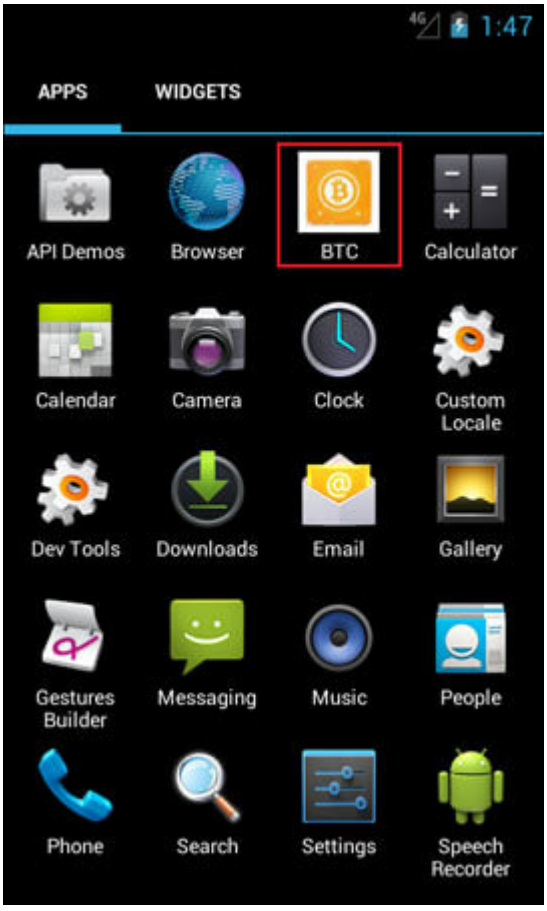
Real-time threat news | Hot news | All the news | Virus alerts

August 7, 2018

Trojans for Microsoft Windows that replace wallet numbers in the clipboard during operations involving digital money and cryptocurrencies are widespread and well known for both computer users and information security specialists. In August 2018, Doctor Web virus analysts examined several malicious programs with similar functions designed for the Android mobile platform.

Trojans capable of replacing digital wallet numbers in the clipboard in order to send money to cybercriminals instead of recipients are commonly referred to as “clippers”. Until recently, such malicious programs bothered Windows users only. Trojans for Android with similar functions are rarely seen in the wild. In August 2018, records of two modifications of a clipper Trojan **Android.Clipper** were added to the Dr.Web virus databases. They were dubbed **Android.Clipper.1.origin** and **Android.Clipper.2.origin**. These malicious programs pose a threat to Android users.

Android.Clipper is capable of replacing the digital wallet numbers of the QIWI, WebMoney (R and Z), and Yandex.Money payment systems, as well as the Bitcoin, Monero, zCash, DOGE, DASH, Etherium, Blackcoin and Litecoin cryptocurrencies. One of the examined modifications of **Android.Clipper** is guised as an application for Bitcoin digital wallets:



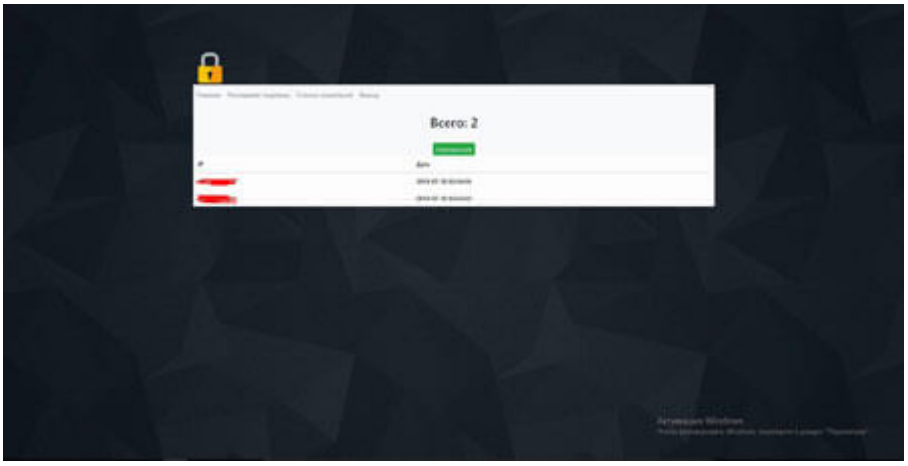
Once the Trojan is launched on an infected device, it displays a fake error message and continues to operate in hidden mode. The Trojan hides its icon from the list of applications on the Android home screen. From now on, the malware can be found in the apps management section of the system preferences only. Both modifications of **Android.Clipper** are then launched automatically every time an infected smartphone or tablet is turned on.

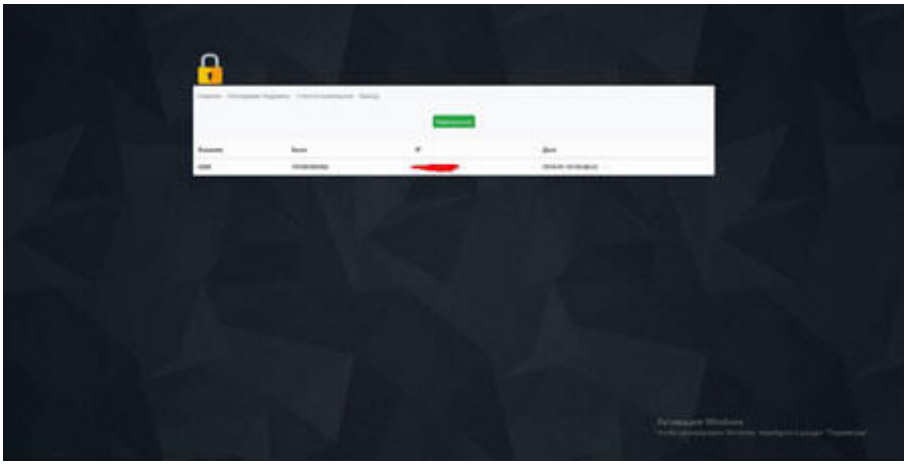
After a successful infection, the Trojan starts to track changes in the clipboard content. Once the user copies the digital wallet number to the clipboard, **Android.Clipper** sends the number to the command and control server. The malware then makes another server request waiting for the cybercriminals' wallet number that needs to be added to the clipboard instead of the original one.

The author of **Android.Clipper** actively sells Trojans of this family in hacking forums. At that, cybercriminals' clients are free to use any application icon and name for every purchased copy of the malicious program. Thus, we can soon expect many modifications of these Trojans that will be spread by cybercriminals under the guise of harmless useful software.


Android Clipper Reborn


Android Clipper Reborn
ПРЕИМУЩЕСТВА


Всего: 2



The virus writer claims in his advertisements that the malware's functions include sending a report on the program operation to the Telegram app and a quick change of wallet numbers embedded into the clipboard using the FTP protocol. However, these features are not implemented in the Trojan itself. All the specified functions are provided for cybercriminals by the command and control center.

Dr.Web for Android has successfully detected and deleted all the known modifications of the **Android.Clipper** Trojan family, so they do not pose any threat to our users.

More information on Android.Clipper.1.origin

More information on Android.Clipper.2.origin

#Android #bitcoin #cryptocurrencies

12739 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
