Android.Clipper.2.origin — Dr.Web Malware description library

Published: 2018-08-09 · Archived: 2026-04-05 16:40:03 UTC

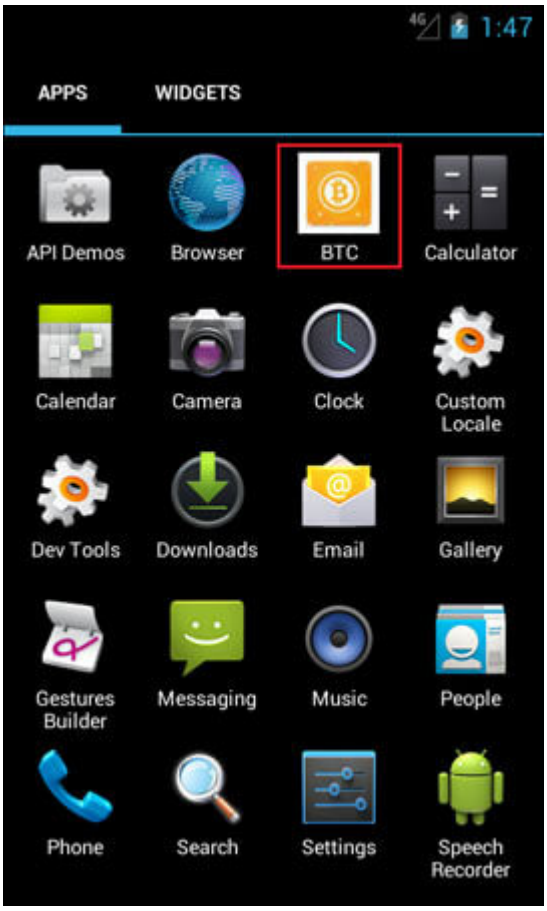
Added to the Dr.Web virus database: 2018-08-08

Virus description added: 2018-08-09

SHA1:

- a2f50f63ae8c4ba7e96a5b3bf30321ac125c715b

A malicious program for Android mobile devices. It can be distributed under the guise of popular harmless applications, such as software for the Bitcoin cryptocurrency:



When **Android.Clipper.2.origin** launches for the first time, it makes its main activity clipper.abcchannelmc.ru.clipperreborn.MainActivity inaccessible by changing the access settings. As a result, the malicious application's icon disappears from the list of programs on the Android home screen.

In the OnPrimaryClipChangedListener interface, the Trojan then adds a listener that tracks changes in the clipboard content and waits for a user to copy a number of one of the targeted digital wallets.

Once the corresponding number is found in the clipboard, **Android.Clipper.2.origin** sends the number information to the http://fastfrmt.*****.tech command and control server. The malware then reconnects to the server and waits for the cybercriminals' wallet number that belongs to the same payment system as the intercepted number.

The Trojan tracks and replaces wallet numbers of the following payment systems and cryptocurrencies:

- QIWI
- WebMoney R
- WebMoney Z
- Yandex.Money
- Bitcoin
- Monero
- zCash
- DOGE
- DASH
- Etherium
- Blackcoin
- Litecoin

To provide the autostart every time the infected mobile device is turned on, **Android.Clipper.2.origin** tracks the following system events:

- android.intent.action.BOOT_COMPLETED;
- android.intent.action.QUICKBOOT_POWERON;
- com.htc.intent.action.QUICKBOOT_POWERON.

News about the Trojan
