BIZCOMMUNITY

# Cybercriminals on the hunt for cryptocurrency

With the cryptocurrency boom continuing across the world, it is fast becoming an attractive target for cybercriminals, who are targeting popular cryptocurrencies such as Bitcoin, Ethereum, Zcash, Dash, Monero and others. Indeed, criminals have already succeeded with bitcoin wallets, earning almost $140,000 overall.

123rf.com

Kaspersky Lab researchers have discovered a new malware which steals cryptocurrencies from a user's wallet by replacing their address with its own in the device's clipboard. According to the research, cryptocurrency stealers - which have been increasing in prevalence since 2014, are again putting users' crypto savings at risk.

## CryptoShuffler

Clipboard hijacking attacks have been known for years, redirecting users to malicious websites and targetting online payments systems. However, cases involving a cryptocurrency host address are rare. There is a new CryptoShuffler Trojan is designed to change the addresses of users' cryptocurrency wallets in the infected device's clipboard (a software facility used for short-term data storage).

In most cryptocurrencies, if the user wants to transfer crypto coins to another user, they need to know the recipient's wallet ID – a unique multi-digit number. Here is how the CryptoShuffler exploits the system's need to operate with these numbers.

After initialising, the malware starts to monitor the device's clipboard, utilised by users when making a payment. This involves copying wallets' numbers and pasting them into the "destination address" line of the software that is used to carry out a transaction. The Trojan replaces the user's wallet with one owned by the malware creator, meaning when the user pastes the wallet ID to the destination address line, it is not the address they originally intended to send money to. As a result, the victim transfers his or her money directly to the criminals, unless an attentive user spots the sudden replacement.

The latter is usually not the case, since multi-digit numbers and the wallets' addresses in blockchain are typically very difficult to remember. Therefore, it's hard to define any distinctive features in the transaction line, even if it is directly in front of the user's eyes.

Destination replacement in the clipboard occurs instantly, thanks to the simplicity of searching for wallet addresses: the majority of cryptocurrency wallets have a constant position in the transaction line and always use a certain number of characters. Thus, intruders can easily create regular codes to replace them.

So far, based on observations from Kaspersky Lab researchers, the criminals behind the CryptoShuffler Trojan have mostly succeeded in attacks against Bitcoin wallets - they were able to steal 23 BTC, which is equivalent to almost $140,000. The total amounts in other wallets ranges from a few dollars to several thousand dollars.

## Not a far-off technology

"Cryptocurrency is not a far-off technology anymore. It is getting into our daily lives and actively spreading around the world, becoming more available for users, as well as a more appealing target for criminals. Lately we've observed an increase in malware attacks targeting different types of cryptocurrencies, and we expect this trend to continue. So, users considering cryptocurrency investments at this time need to think about ensuring they have proper protection", says Sergey Yunakovsky, malware analyst at Kaspersky Lab.

Experts have also found another Trojan targeting the Monero cryptocurrency – DiscordiaMiner, which is designed to upload and run files from a remote server. According to the research, there are some performance similarities with the NukeBot Trojan, discovered earlier this year. As in the NukeBot case, the Trojan's source codes have been shared on underground hacking forums.