A tool capable of tracking cybercrime financial transactions in Bitcoin

December 13 2022

Credit: Unsplash/CC0 Public Domain

IMDEA Software researchers Gibran Gómez, Pedro Moreno-Sánchez and Juan Caballero have created an open-source automated tool to track the financial relationships of malicious entities that abuse Bitcoin

technology, tested on 30 malware families.

The study "Watch Your Back: Identifying Cybercrime Financial Relationships in Bitcoin through Back-and-Forth Exploration," in which they present their research and the tool, was published as part of the *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* as well as being presented at the conference.

Cybercrime is the plague of the digital environment. Scams, phishing, identity theft, personal data theft, phishing or computer fraud are just a few examples of illicit activities on the network. Blockchain technology and cryptocurrencies, such as Bitcoin, have consistently attracted the attention of cybercriminals, who have frequently used them as a means of payment and even as a means of storing data for illicit purposes.

Aware of this problem, Gibran, Pedro and Juan have analyzed more than 7,500 Bitcoin addresses belonging to 30 malware families, including ransomware families, clippers, sextorsion, crypto-jackers or info stealers.

The main advantage provided by the back-and-forth exploration method, used in the study, is that it allows tracking all transactions produced by a Bitcoin address recursively. This means that, if a Bitcoin address receives cryptocurrencies from another address, and this in turn sends them to a third address, the complete path of the cryptocurrencies could be traced starting from the first address, or from the last one.

As Gibran Gómez points out, "one of the main advantages of the tool is that the user can replicate the whole process in a transparent way, which allows the results to be corroborated."

The tool, in addition to serving Bitcoin users themselves, could be especially useful for law enforcement agencies, as it would allow them to

identify paths between malicious addresses and deposit addresses used by operators of illicit activities that belong to financial entities regulated by KYC policies, such as exchanges (cryptocurrency exchanges).

This means that the National Police, for example, could use such paths as evidence to obtain a court order to require from an exchange the personal identification data associated with the addresses involved, and get to know who the final recipients of the illicit money are.

In addition, Gómez advises users to take certain precautionary measures before carrying out transactions to avoid being the target of cybercrime: "Paying close attention when including the destination address in a transaction is essential. It is necessary to check several times that the destination address is correct to avoid clippers."

To prevent malware, he suggests always using antivirus software and running frequent computer scans and, lastly, performing constant back-ups to avoid the loss of important data that can result from a ransomware attack.

More information: Gibran Gomez et al, Watch Your Back, *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (2022). DOI: 10.1145/3548606.3560587

Conference: www.sigsac.org/ccs/CCS2022/

Provided by IMDEA Software Institute