Cybercriminals increasingly target cryptocurrency

Even though the value of cryptocurrencies is dropping, they have become a lucrative target for thieves.

By ROHMA SADAQAT

AS cryptocurrencies and non-fungible tokens (NFTs) become more mainstream, cybercriminals are increasingly turning to them as a new method of financial extraction, security experts have warned.

Researchers have observed multiple objectives demonstrated by cybercriminals relating to digital tokens and finance, such as traditional fraud leveraging business email compromise (BEC) to scam individuals, as well as activity targeting decentralised finance (DeFi) organisations that facilitate cryptocurrency storage and transactions for possible follow-on activity.

Studies by Proofpoint have found that both of these threat types contributed to around US$14bil (RM62bil) in cryptocurrency losses in 2021.

In fact, BEC topped the list of types of attacks chief information security officers (CISOs) in the UAE expect to face in the coming months, with 35% of CISOs concerned about potential BEC attacks.

Sherrod DeGrippo, vice president of Threat Research and Detection at Proofpoint, explained that the financially motivated attacks targeting cryptocurrencies have largely coalesced under pre-existing attack patterns observed in the phishing landscape prior to the rise of blockchain based currency.

"Common techniques observed when targeting cryptocurrency over email include credential harvesting, the use of basic malware stealers that target cryptocurrency credentials and cryptocurrency transfer solicitation like BEC," she revealed.

"These techniques are viable methods of capturing sensitive values, which facilitate the transfer and spending of cryptocurrency."

There are multiple DeFi applications and platforms – such as cryptocurrency exchanges – that people can use to manage their cryptocurrency, she added.

"These platforms often require usernames and passwords, which are potential targets for financially motivated threat actors.

"Despite public keys being safe to share, researchers are seeing actors solicit the transfer of cryptocurrency funds via BEC-type emails that include threat actor controlled public keys and cryptocurrency addresses.

"These email campaigns rely on social engineering to secure the transfer of funds from targeted victims," she said.

Users, she stressed, should be aware of common social engineering and exploitation mechanisms used by threat actors aiming to steal cryptocurrencies.

In 2022, Proofpoint observed regular attempts to compromise users' cryptocurrency wallets using credential harvesting.

This method often relies on the delivery of a URL within an email body or formatted object that redirects to a credential harvesting landing page.

Notably, these landing pages have begun to solicit values utilised in the transfer and conversion of cryptocurrencies.

Proofpoint researchers have also observed multiple examples of phishing threat actors creating and deploying phishing kits to harvest both login credentials to cryptocurrency related sites and cryptocurrency wallet credentials or passphrases.

Phishing kits give threat actors the ability to deploy an effective phishing page regardless of their skill level.

They are pre-packaged sets of files that contain all the code, graphics, and configuration files to be deployed to make a credential capture webpage.

DeGrippo explained that these are designed to be easy to deploy as well as reusable.

They are usually sold as a zip file and are ready to be unzipped and deployed without a lot of "behind the scenes" knowledge or technical skill.

She added that 2022 also saw an increase in BEC specifically for cryptos.

Primarily, these requests are observed in the context of employee targeting, using impersonation as a deception, and often leveraging advanced fee fraud, extortion, payroll redirect, or invoicing as themes.

The initial BEC email often contains the safe for public consumption values, including public keys and cryptocurrency addresses.

"By impersonating an entity known to the user and listing an actor-controlled public key or address, actors are attempting to deceive users into transferring funds from their account willingly based on social-engineering content.

"This is like the way actors use routing and bank account numbers during BEC phishing campaigns," DeGrippo said. – Khaleej Times/Tribune News Service