JOINT ADVISORY BY SINGAPORE POLICE FORCE AND THE CYBER SECURITY AGENCY OF SINGAPORE

PROTECTING YOURSELF FROM CRYPTO DRAINERS

Cybercriminals are increasingly leveraging crypto drainers to target owners of cryptocurrency wallets ("crypto wallets") as the use of cryptocurrencies become increasingly popular with their dollar values correspondingly increasing.

2 A Crypto drainer is a type of malware that targets crypto wallets. These drainers are often deployed as part of phishing attacks, where the victim is tricked into clicking a malicious link or opening a malicious attachment. By doing so, the victims are tricked into consenting to a malicious transaction that allows the drainer to steal cryptocurrencies stored in their wallets.

How Scammers Make Use of Crypto Drainers to Facilitate Cryptocurrency Theft

3 While such cases have not been observed in Singapore, members of the public should remain alert to such cyber attacks that are happening globally.

4 There are cybercriminal groups that develop "commercial" crypto draining kits and provide services to other cybercriminals with limited technical expertise based upon a Drainer-as-a-Service (DaaS) model. Under this model, a percentage of the stolen amount are charged by these groups in exchange for the provision of wallet draining scripts, phishing kits, instruction sets etc.

[1] Crypto airdrops involve the distribution of free tokens (e.g., cryptocurrencies) en masse as part of a broader initiative.

[2] A seed phrase is a sequence of random words that provide the information required to recover a lost crypto wallet.

[3] Smart contracts are programs stored on a blockchain that run when predetermined conditions are met.

5 The modus operandi of these crypto drainers can be distilled into the following steps:

a) Launch a Phishing Campaign: Cybercriminals will promote a fake crypto airdrop[1] by publicising the campaign through social media platforms or emails. These cybercriminals have also been observed to compromise verified X (formerly known as Twitter) accounts to increase the reach and credibility of their campaigns.

b) Direct Victims to a Phishing Website: A phishing link will then be provided to direct unsuspecting victims attempting to claim the allegedly free tokens to a phishing website that resembles a token distribution platform. The website will prompt them to provide their crypto wallet details to receive the tokens.

c) Wallet Connection: When unsuspecting victims connect their crypto wallets to the website, they will be requested to authenticate their accounts using their private keys or seed phrases[2]. Once a connection has been established with their crypto wallets, the foundation is now laid for cybercriminals to begin exfiltrating cryptocurrencies out from the victims' wallets.

d) Malicious Smart Contract Interaction: The victims will then be induced to interact with a malicious smart contract[3] under the pretext that it is a necessary step to claim the airdrop or incentives. However, the contract contains embedded malicious functionalities such as manipulating 'approve' or 'permit' allowances for cybercriminals. Once executed, it enables cybercriminals to drain the victims' cryptocurrency wallet without further interactions (or authorisations) required from the victims.

e) Asset Transfer and Obfuscation: Upon successfully infiltrating and attaining the necessary controls over the victims' crypto wallet, cybercriminals will begin to swiftly drain the wallet. The cybercriminals will also leverage sophisticated

[1] Crypto airdrops involve the distribution of free tokens (e.g., cryptocurrencies) en masse as part of a broader initiative.

[2] A seed phrase is a sequence of random words that provide the information required to recover a lost crypto wallet.

[3] Smart contracts are programs stored on a blockchain that run when predetermined conditions are met.

techniques such as cryptocurrency mixers or orchestrate a series of transfers to obfuscate the stolen assets trails, making it difficult to trace and attempt recoveries.

Safeguarding Yourself from Crypto Drainers

6 Despite the sophistication and possible scale of crypto drainer-related campaigns, there are measures that owners of crypto wallets can take to safeguard themselves from such scams.

These measures (non-exhaustive) include:

a) Using a hardware wallet for enhanced security.
b) Being wary of attractive offers such as free crypto airdrops that appear too good to be true.
c) Verifying the legitimacy and functions of smart contracts before interacting with them.
d) Limiting the use of high allowances and regularly reviewing and revoking them by using blockchain explorers or wallet interfaces.
e) Understanding the implications of approving or signing transactions before doing so.
f) Researching the background/history of a project or cryptocurrency before connecting your wallet and ensuring that any connections are performed after verifying the validity of the website.
g) Connecting a newly created or empty crypto wallet when uncertain about a project or token.
h) Not divulging seed phrases[3] to anyone.

What to do if you fall Victim to a Crypto Scam

7 If you are, or suspect that you are, a victim of a crypto scam involving crypto drainers or otherwise, you are advised to perform the following immediately:

a) Contact your cryptocurrency exchange immediately to halt further transactions or freeze your account, if possible.

[1] Crypto airdrops involve the distribution of free tokens (e.g., cryptocurrencies) en masse as part of a broader initiative.

[2] A seed phrase is a sequence of random words that provide the information required to recover a lost crypto wallet.

[3] Smart contracts are programs stored on a blockchain that run when predetermined conditions are met.

b) Report the incident to the police and CSA’s SingCERT.

c) Review and revoke any suspicious token approvals using applicable wallet interfaces.

d) If a wallet’s seed phrase is compromised, transfer all remaining cryptocurrencies in the compromised wallet to another wallet immediately.

SINGAPORE POLICE FORCE
CYBER SECURITY AGENCY
31 JANUARY 2024 @ 9.00AM

[1] Crypto airdrops involve the distribution of free tokens (e.g., cryptocurrencies) en masse as part of a broader initiative.

[2] A seed phrase is a sequence of random words that provide the information required to recover a lost crypto wallet.

[3] Smart contracts are programs stored on a blockchain that run when predetermined conditions are met.