Hackers wiped out thousands of Solana wallets overnight, the error came from the Dev position of Slope wallet

In just one night, hackers hacked into the Solana blockchain platform and wiped out virtual currency in thousands of e-wallets. The stolen virtual currency is worth millions of dollars.

Currently, the platform has started an investigation and is trying to determine how the hacker managed to withdraw the funds.

In a statement, Solana said the attack affected 7,700 wallets, including Slope and Phantom. According to other reports, users of e-wallets such as Solflare and Trust Wallet were also affected.

According to the most recent statistics from blockchain analytics provider Elliptic, the number of affected wallets is close to 7,936 and the loss is 5.2 million USD including various cryptocurrencies (SOL, NFT and more than 300 based tokens. on Solana).

Solana believes that those affected in this attack should be considered compromised and rule out hardware causes as cold wallets appear to be unaffected. The advice for users at this time is not to reuse the security phrase and create a new one for the hardware wallet.

For those who don't have a cold wallet, move all your assets to a trusted centralized exchange. This is the best alternative to protect assets from attackers.

All transactions are signed

Currently, it is not known how the hacker drained the wallets. However, there are many opinions that the software of the e-wallet has vulnerabilities.

'The root cause is still undetermined but it appears there is a vulnerability in the wallet software and not in the Solana blockchain itself,' Elliptics said.

Clues from the attack show that all withdrawals are signed by the rightful owners. This shows that the possibility of the private key being exposed is very high.

This is why revoking a third-party approval method doesn't stop the attack. However, this is still the recommended course of action.

According to blockchain security experts, to access such a large number of private keys, hackers would have to use supply chain attacks, browser zero-day exploits or a compromised random number generator. error used during key generation.

Since hacks like this can happen again and again, users should not keep all their crypto in hot wallets. Instead, just use a hot wallet to store a small amount of money for transactions, most of the remaining assets in a cold wallet where it is disconnected from the internet and 3rd party services.

Updated on August 5: The error originates from the Devs of Slope wallet

According to the latest investigation results, the attack on the Solana platform originated from a security flaw of the Slope wallet. And this flaw comes from the carelessness of the Slope developers.

The Slope wallet application uses Sentry, an open source library to log and exception during the running of the software. This log data will be accessed by the devs to serve patching or fixing problems that arise.

However, it is not clear whether Slope's Dev accidentally or intentionally stored both the private key (private key) and the user's security phrase into the Sentry server. Therefore, when hackers access the sentry server, they have collected all the private keys of the users.

These private keys are used to authenticate the virtual money transfer from the user's Slope wallet to the hacker's wallet. In addition, the hacker also used the security phrase obtained from the Sentry server on other e-wallets and successfully accessed and withdrawn the money of many victims. The reason is because many people often use the same security phrase for many different wallets.

Currently, Slope has deleted all log data to avoid causing more damage. However, users should protect themselves by immediately transferring virtual assets on Slope to decentralized wallets or creating a new wallet on Slope and discarding their current wallet.

You also need to do the same with wallets that are sharing the same security phrase with the Slope wallet.