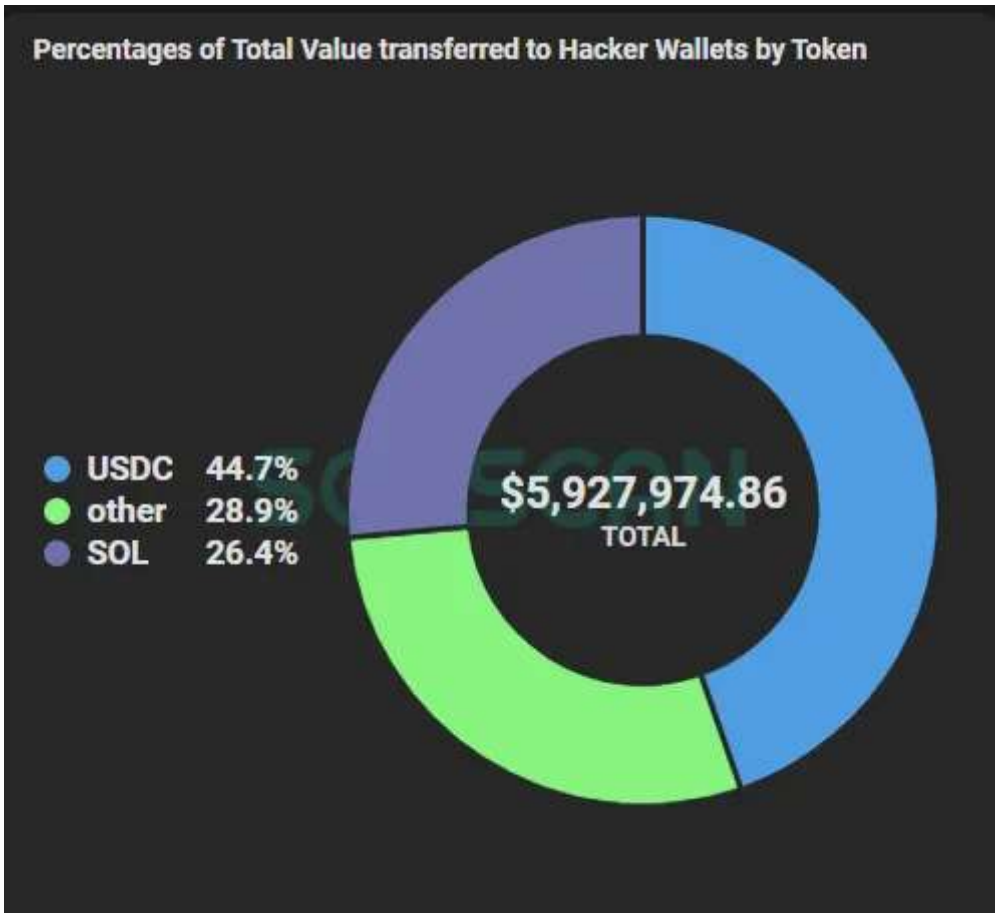
Beosin’s Detailed Analysis of Solana Attack

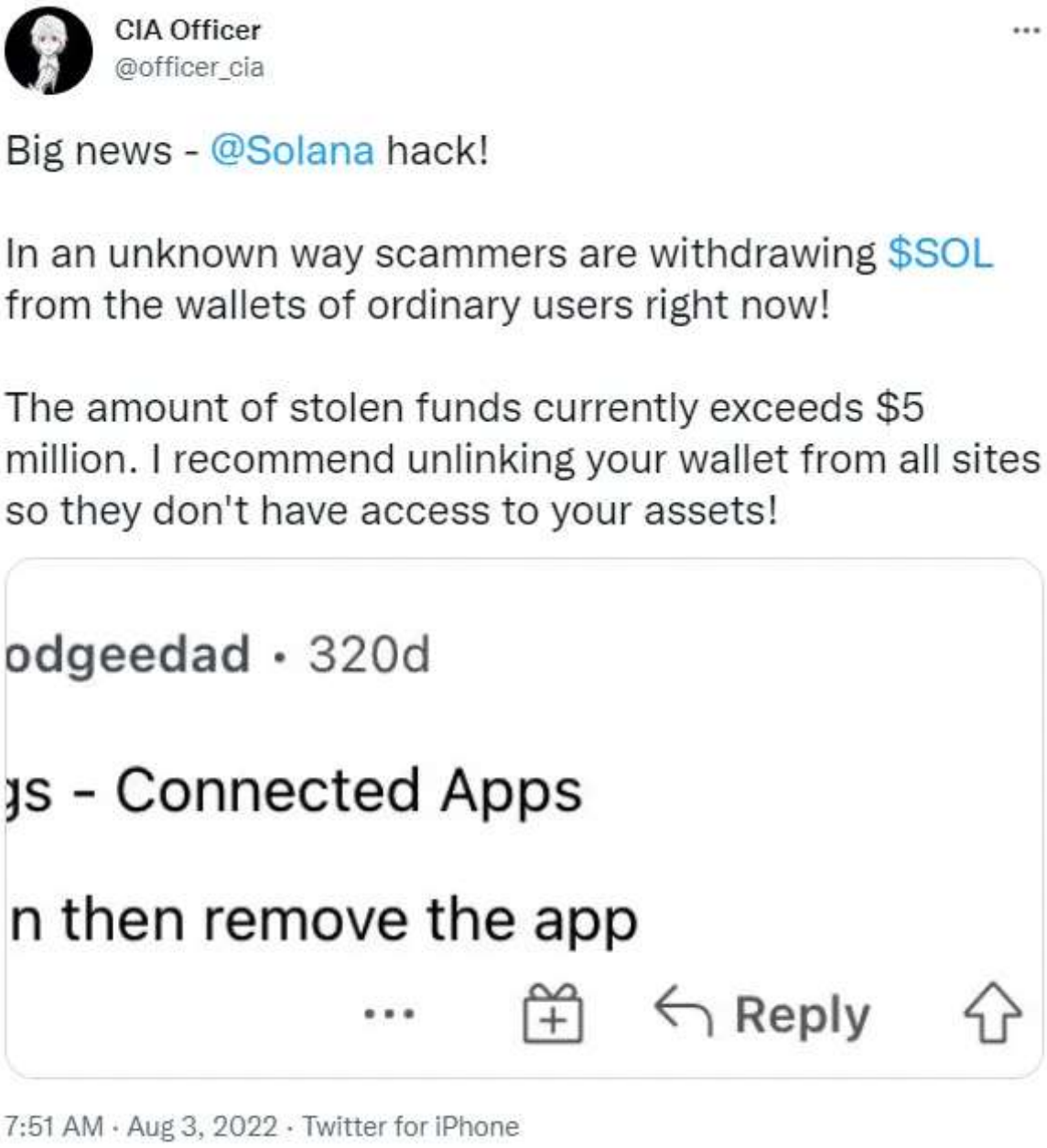
On August 3, according to Beosin EagleEye, a massive coin robbery occurred at Solana, and as of press time, nearly 10,000+ Solana wallet addresses have been attacked, and about $6 million worth of SOL, SPL, USDC, USDT, BTC, ETH, etc. have been stolen. In yesterday’s alert, we first advised Solana wallet users to transfer their crypto assets to CEX or hardware wallets as soon as possible.



ONE Wallet attack on Solana, how more than 10,000 wallets were stolen

On August 3, first the official tweet from MagicEden, Solana's ecological NFT marketplace, stated that there was a suspected SOL vulnerability that could steal assets from the Phantom wallet.

Then, independent security researcher CIA Officer, hackers are now extracting $SOL from ordinary users' wallets in an unknown way , with the amount of stolen funds currently exceeding $5 million.



A well-known developer @0xfoobar tweeted that in addition to Phantom, Slope wallet users have also reported the theft.

Immediately afterwards, more and more users' wallets were compromised and everyone realized that the situation had become serious!

The Beosin technical team was the first to track and analyze the attack, and now we share the analysis progress of this attack as follows.

TWO Analysis of the progress of this attack

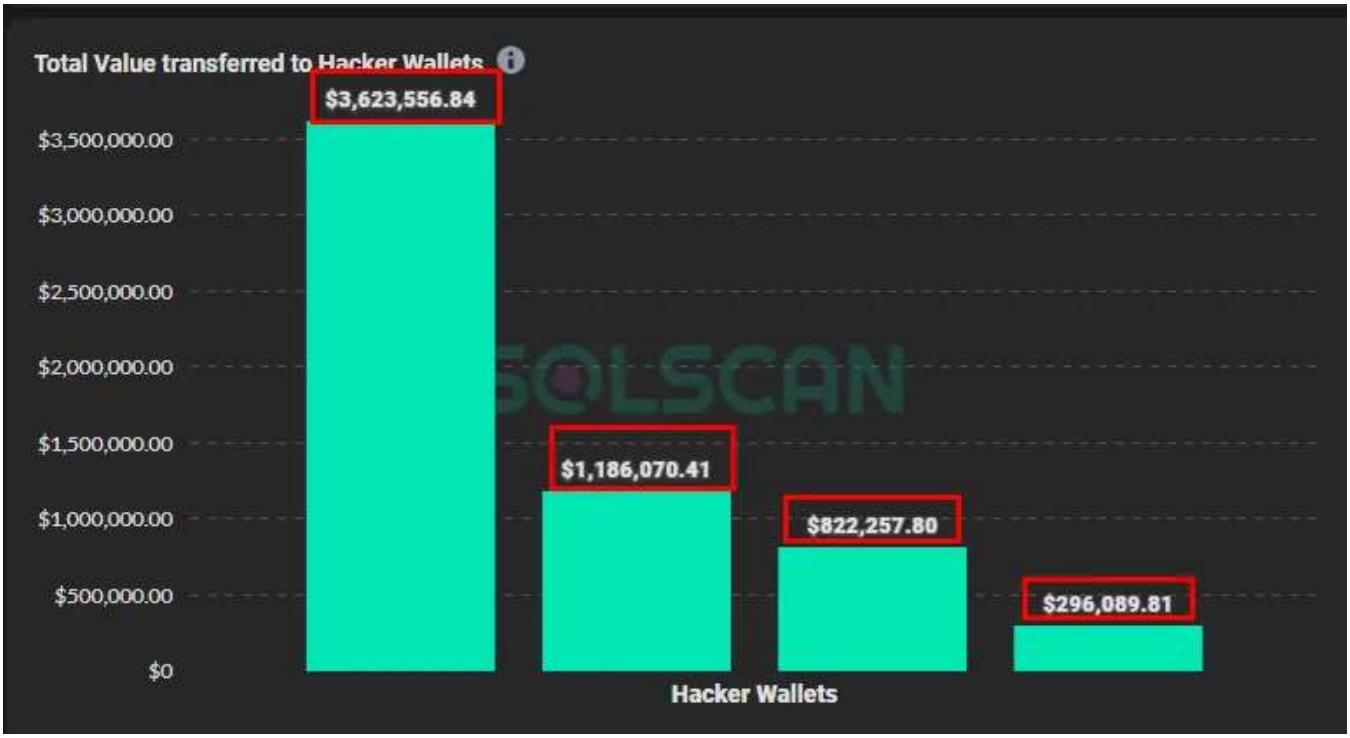
Yesterday we have announced that the stolen funds have entered these wallet addresses and the amount of each address is as follows.

·Htp9MGP8Tig923ZFY7Qf2zzbMUmYneFRAhSp7vSg4wxV

·CEzN7mqP9xoxn2HdyW6fjEJ73t7qaX9Rp2zyS6hb3iEu

·5WwBYgQG6BdErM2nNNyUmQXfcUnB68b6kesxBywh1J3n

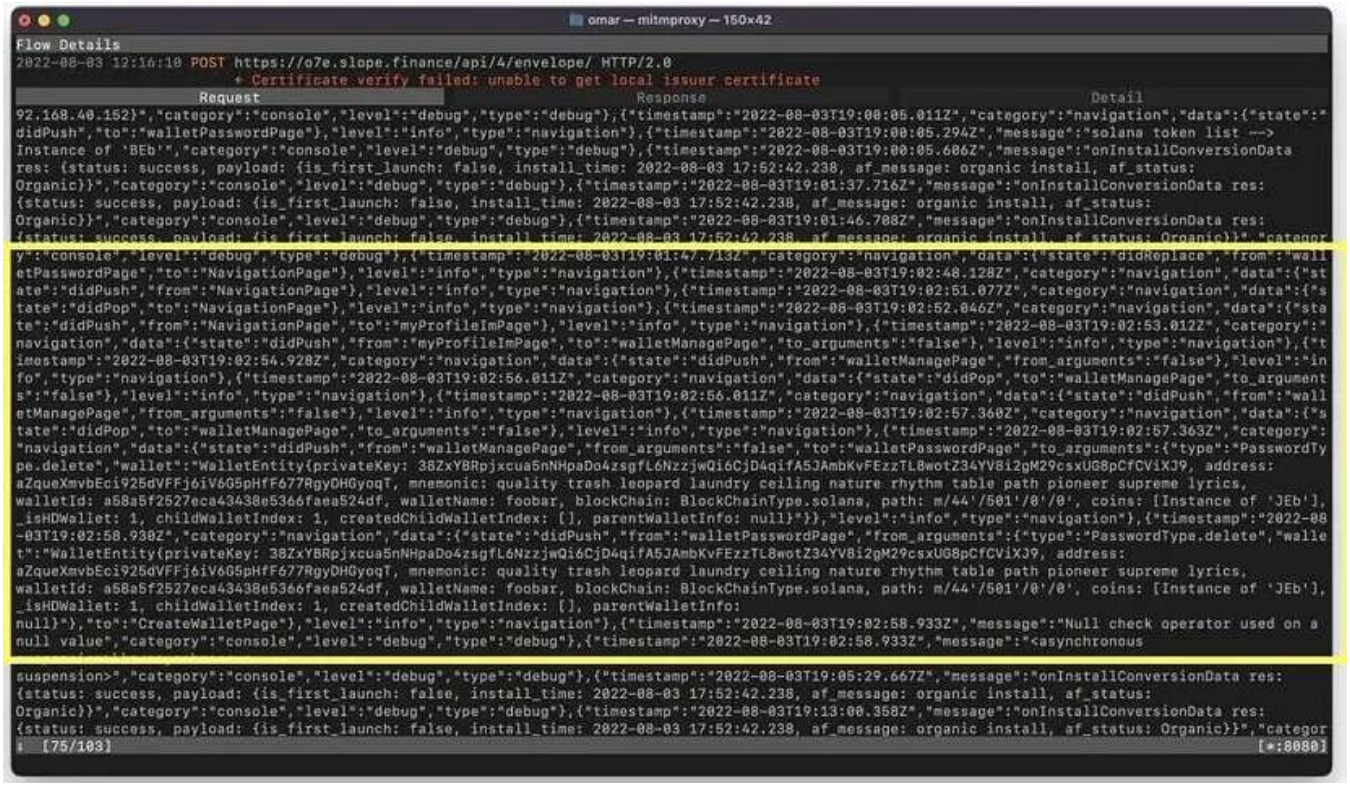
·GeEccGJ9BEzVbVor1njkBCCiqXJbXVeDHaXDCrBDbmuy



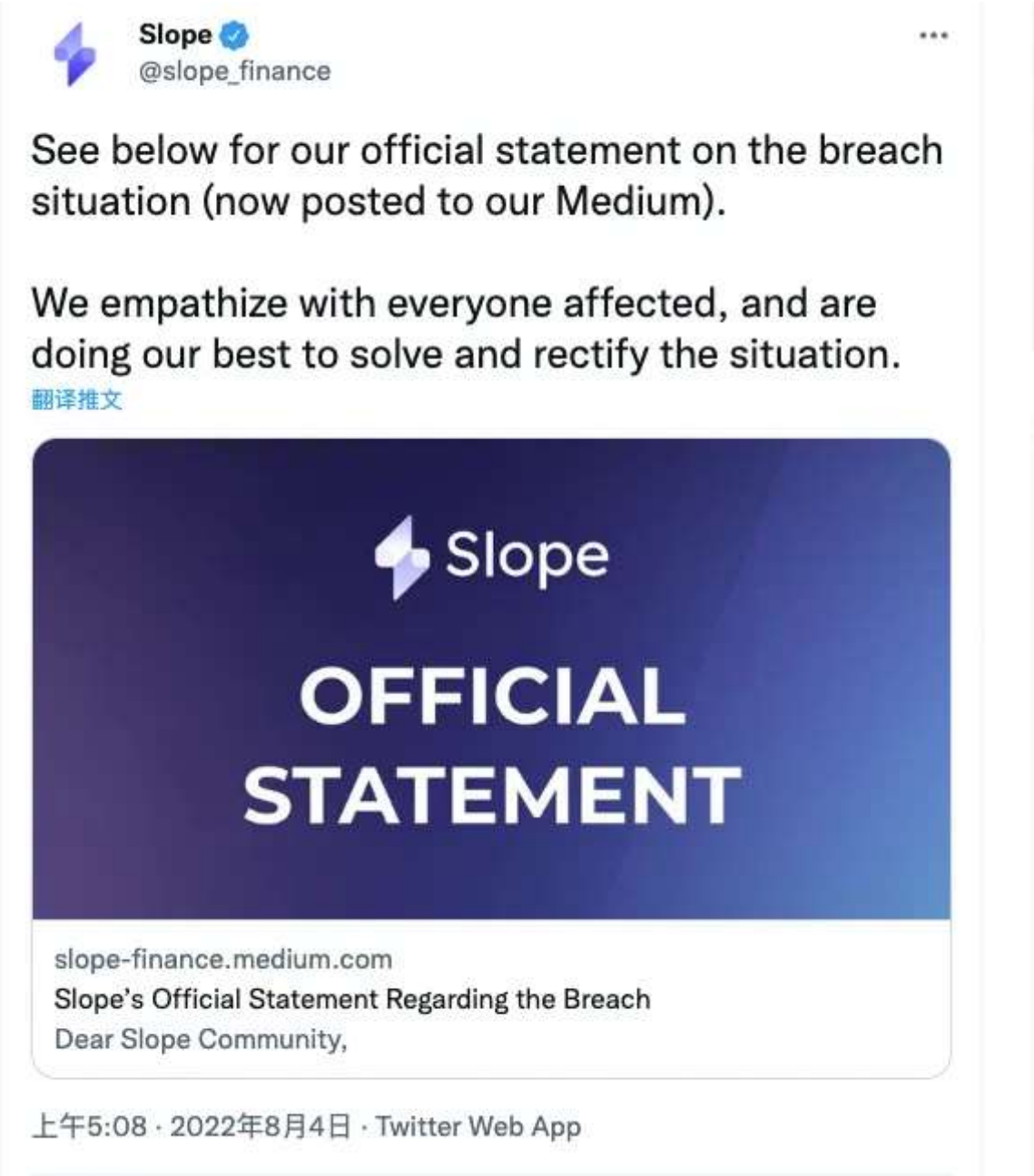
One:

According to user feedback, the wallets affected so far are mainly Phantom wallet and Slope wallet.

When Beosin security team analyzed the Sentry service used by Slope wallet, it was found through packet capture that this service sends sensitive data such as helper and private key to Slope's server o7e.slope.finance when the user creates a wallet, causing the helper or private key to be leaked.



Slope officials have now issued a document and are working to resolve the issue.



The analysis of the Phantom wallet, reverse code found that it also contains the sentry library, but through packet analysis, for the time being, no sensitive data such as helper words and private keys were found to be sent to the server when the user created the wallet.

In addition, according to public opinion, NEAR's wallet was found to have similar issues to Slope Wallet in June. When Near wallet users selected "email" as the booster recovery method, the booster was leaked to a third-party site.

Two:

According to the public opinion, previously Ava Labs' head of engineering patrickogrady tweeted, "I wonder if there is a nonce reuse vulnerability in some of the ed25519 signature libraries being used by the Solana project. I think this would allow any attacker viewing Solana to obtain the private key regardless of where it was generated." In response to this speculation, the Beosin security team is currently continuing to follow up on the research.

THREE What do users and projects need to pay attention to in terms of wallet security?

This massive wallet hacking has likewise given us a lot of insight into the ecological world of Web 3.0, and we have the following suggestions for wallet security.

For users

Users can usually divide their wallets into two categories based on their usage. The first category is for storing assets, including some large assets, etc. Such assets can be stored using cold wallets to improve security.

The second category is used for asset transactions, and some temporary wallets can be used. Temporary wallets include: using a wallet like MetaMask to recreate an address inside which very little money is stored; or some web wallets such as Burner Wallet, which can generate a temporary QR code for small transactions by simply setting the parameters of the transfer on the webpage, such as: transfer address, amount, etc.

Also, the user can use a different PC, browser, etc., when making some potentially dangerous transactions, or use a different browser.

For projects

Wallets should also be careful not to upload users' private keys and helper words to the server, and project parties would do well to find a professional third-party security company to conduct a professional security audit before the product goes live.

FOUR Last words

After this stolen incident, Beosin issued a warning at the first time and advised Solana wallet users to transfer their crypto assets to CEX or hardware wallets as soon as possible to avoid expanding losses. At the same time, Beosin security team is using ChainBuilder — the intelligent research and analysis platform for virtual currency cases to monitor and track the addresses of the stolen funds.

Contact

If you have need any blockchain security services, please contact us:

Website Email Official Twitter Alert Telegram LinkedIn