A crypto influencer is under a sweeper bot attack. How can Beosin help recover his funds?

Have you ever had the experience of sending your crypto assets to your wallet and then finding it disappear?

If your private key is compromised, the attacker will usually run a sweeper bot to monitor your wallet and then wait for an opportunity to transfer the assets in your wallet. No matter whether you deposit $ETH or other tokens or received an airdrop in this wallet, the tokens will be transferred by the sweeper.

Recently, a crypto influencer's wallet was compromised and monitored by sweeper bots. He immediately sought help from Beosin to deal with it.

What is a sweeper bot?

A sweeper bot is a script used to monitor data on a blockchain, which monitors transactions and mempool(transaction pool) that stores pending transactions. Once these sweeper bots identify a transaction related to a compromised wallet, they will frontrun a new transaction before the original transaction is completed.

To put it simply, as long as you send ETH, other tokens, or airdrops to the wallet whose private key is stolen, it will be monitored by a sweeper bot. Since it has the private key of the address, it will immediately send a transaction to transfer the assets out before the user. Users usually send a transaction manually, which is much slower than a sweeper bot.

Therefore, when the private key of a wallet is stolen, how to transfer the assets in the wallet has become a difficult problem for many users.

● Scripts send a transaction faster than humans, how should users save their assets?

● Users don't immediately realize they've been hacked. If a user performs a transaction, he/she might first think that the transaction is pending, or the wallet fails.

How did the crypto influencer suffer a sweeper bot attack?

On April 16, 2023, Beosin's friend Lanxing (Twitter: @lanxing4) was under a sweeper bot attack.

Lanxing was attacked by phishing and the attacker obtained the private key of his wallet. The attacker wrote a sweeper bot and then allowed the script to sign any transaction without the user's permission, which made the bot completely control the wallet.

It can be seen that when Lanxing transferred a small number of $ETH to pay the gas fee to the compromised address, the $ETH were transferred to other addresses immediately. It proved to be a sweeper bot attack.

0x2e070c526238e5...	Transfer	17059641	1 day 16 hrs ago	0x79CFDd...D1A679f7	OUT	0xe432d6...6dd29FE6	0.00186243 ETH	0.00113756
0x6e27ec27f873ad...	Transfer	17059640	1 day 16 hrs ago	bluestarpin.eth	IN	0x79CFDd...D1A679f7	0.003 ETH	0.00049483
0x7cf4f1da672060a...	Transfer	15865535	169 days 1 hr ago	0x79CFDd...D1A679f7	OUT	0xF520c0...AC8DB754	0.00483786 ETH	0.00023092
0x6e57f774e796e0f...	Transfer	15865533	169 days 1 hr ago	bluestarpin.eth	IN	0x79CFDd...D1A679f7	0.005 ETH	0.00025939

The bot continuously monitors the transactions of this wallet. At that time, Lanxing still had some assets in this wallet and some tokens staked in contracts. How to transfer the assets out has become a headache for Lanxing.

The bot continuously monitors the transactions of this wallet. At that time, Lanxing still had some assets in this wallet and some tokens staked in contracts. How to transfer the assets out has become a headache for Lanxing.

How did Beosin save the funds?

After communicating with Lanxing, Beosin security team found that he had about $1,000 assets on the X2Y2 trading platform. The assets were not transferred out by hackers. If Lanxing needs to withdraw it and transfer it to other safe addresses, then the

gas needs to be transferred to the compromised address. According to what we mentioned above, the gas will be transferred to the hacker addresses immediately.

Beosin security team immediately rescued Lanxing's funds. We transferred the gas fee to the compromised address, withdrew the assets and finally transferred the assets to a safe address in the same block.

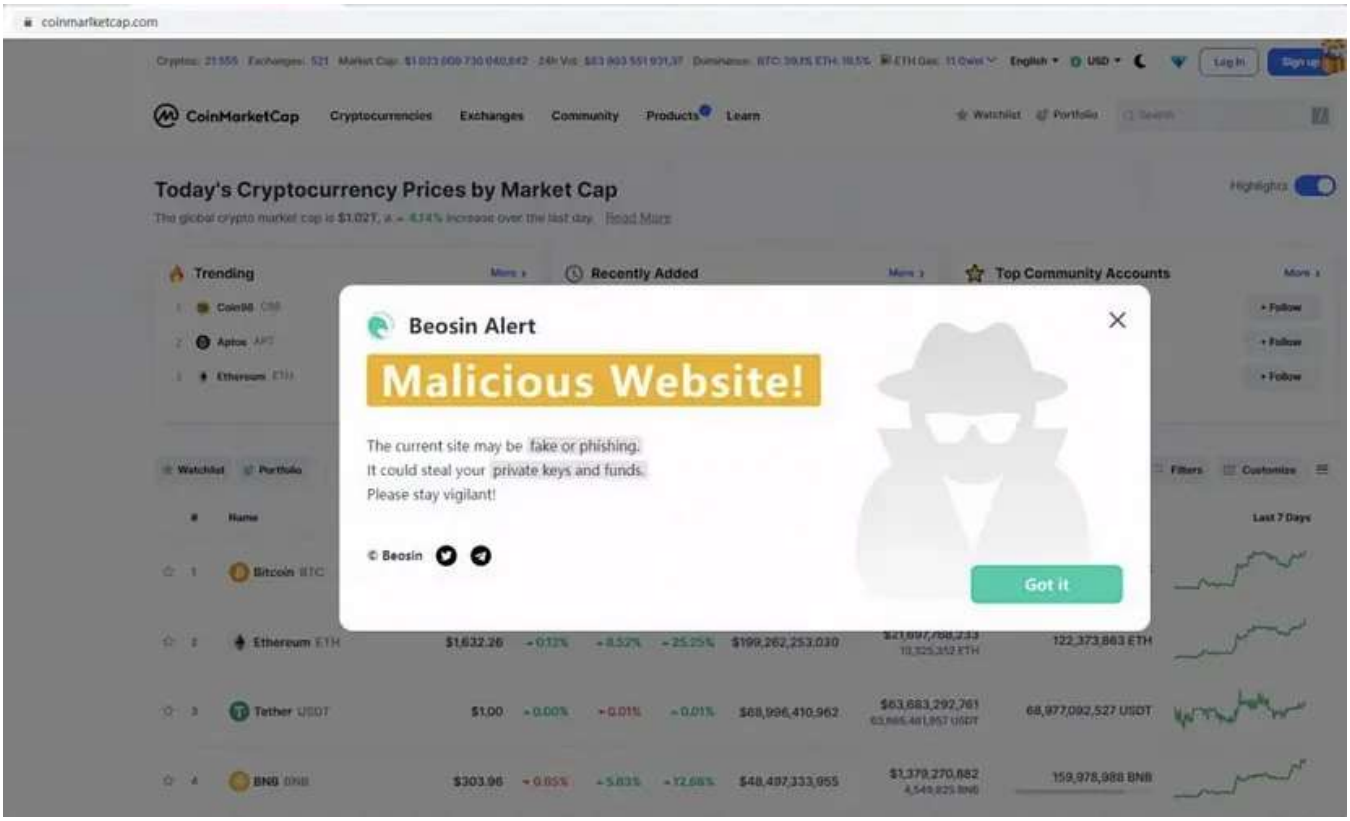
To put it simply, by packaging multiple transactions and cooperating with block validators, the transactions are directly sent to a block producer, which prevents hackers from monitoring the mempool and launching a sweeper bot attack to steal the user's assets.

0x135f7457d51da2...	Transfer	17064918	1 day ago	0x79CFDd...D1A679f7	OUT	X2Y2: X2Y2 Token	0 ETH	0.00163996
0x84c0bb42939b26...	Transfer	17064918	1 day ago	0x79CFDd...D1A679f7	OUT	Wrapped Ether	0 ETH	0.00104013
0xe8d70a91aae6dfe...	Withdraw	17064918	1 day ago	0x79CFDd...D1A679f7	OUT	X2Y2: Presale	0 ETH	0.00422866
0x4093971a073df7...	Transfer	17064918	1 day ago	0xE8EDc3...A965B3e3	IN	0x79CFDd...D1A679f7	0.0095 ETH	0.000735

How to fight against sweeper bots?

If you notice unauthorized transactions in your wallet, it is a sign that your wallet may have been hacked and if your wallet is hacked, there is a 95% chance that a sweeper bot is added.

Keeping your private keys safe is the best way to avoid a sweeper bot attack. Thus it's important to fight against phishing attacks. In any situation that requires you to enter your private keys or seed phrases, you can first assume that it is a phishing attack. You can use Beosin Alert anti-phishing extension to help you identify phishing websites. The following picture shows Beosin Alert identifying a fake Coinmarketcap website.



Beosin Alert Download link: https://chrome.google.com/webstore/detail/beosin-alert/lgbhcpagiobjacpmcgckfgodjeogceji?hl=en

Fighting against sweeper bots is difficult, but not impossible. Assuming you have funds (staking tokens, LP and NFT) in your wallet and the hacker somehow didn't notice it or wait for the unlocking process, you have to try to transfer the remaining funds. If you suffer a sweeper bot attack, you can seek help from Beosin immediately.

Beosin is a leading global blockchain security company co-founded by several professors from world-renowned universities and there are 40+ PhDs in the team. It has offices in 10+ countries. With the mission of "Securing Blockchain Ecosystem", Beosin provides "All-in-one" blockchain security solution covering Smart Contract Audit, Risk Monitoring & Alert, KYT/AML, and Crypto Tracing. Beosin has already audited more than 3000 smart contracts and protected more than $500 billion funds of our clients. You are welcome to contact us.