US $ 1.7 billion of electronic money was beaten by hackers in 2018

The cyber criminals 'working' in the e-money market must have had a successful 2018 pocket-sized electronic money worth $ 1.7 billion.

The cyber criminals 'working' in the e-money market must have had a massive $ 1.7 billion pocket-sized electronic money worth $ 1.7 billion from exchange services, users or even Only investors.In particular, various forms of fraud, extortion, hacking and malware are the main methods used by hackers to get money.

According to a report shared with BleepingComputer, the related electronic and infrastructure exchanges in the past year cost about $ 950 million to hackers.In particular, Korea and Japan are believed to be the shelters of most of these high-tech thieves.

1. 1.6 million computers in Vietnam were erased by the virus, losing nearly 15,000 billion in 2018

Exit Scam is the crux of the problem

Exit Scam is the trick used by hackers in the 2018 electronic money market, according to a report from security experts from CextTrace, a company that provides anti-money laundering and blockchain solutions. by.If you do not know, Exit Scam is a trick to create trust, then take the victim's money and then run away or not perform the services as contracted.An example of Exit Scam is that you buy product A from an online store, you paid but did not receive delivery.

One of the biggest virtual money scams last year occurred in April, when a Vietnamese electronic money company called Modern Tech launched the service Initial Coin Offering (ICO) and collected $ 660 million from about 32,000 individuals.After a while, all the activities abruptly stopped and 'boom' everything disappeared with questions of no one calling for those who were light-hearted.

Another noteworthy scam in 2018 also involved a Vietnamese money-mining company named Sky Mining.Accordingly, the founder and CEO of this company suddenly disappeared along with assets of self-operators and rigs worth up to 35 million USD.

Tragedy lies in the fact that in many countries in the world including Vietnam, electronic money is still a relatively new field and the state does not accept transactions related to this currency.Therefore, the management mechanisms as well as sanctions for violations in the field of e-money are completely unavailable, so the victims cannot do anything but blame themselves.

1. Ham hacked the game, the boy made the computer infected with virtual money and ruined it

Hack and steal SIM for the purpose of stealing electronic money

Also according to the report, the gaps in the management of exchanges are another cause of users becoming victims of scams.Attacks are often aimed at exchanging services or focusing directly on high-value users.

For example, in the case of Japan, hackers made trot one of the biggest electronic money theft cases in history, pocketing a large electronic money trading floor, worth up to 530 million dollars. la.Shortly thereafter, at the beginning of October, a trading floor in Osaka was lost over 70 million dollars by a thief.

In addition, some cyber criminals have switched to SIM swap technology to steal the victim's phone number and gain access to sensitive information used in two-factor authentication, or in the body. Two steps to access the victim's trading account or e-wallet.

One of the simplest ways to achieve this is to bribe or trick someone responsible for managing the mobile service provider's SIM problems, then link the phone number of the victim. Multiply with another SIM card.For example, hackers can call your service provider (too easy to find the operator's phone number), use the information they know about the victim to get through the sentences. ask security and ask your service provider to transfer your phone number to a new SIM card.With a bit of other social knowledge, hackers can completely trick the tech support representatives into sending their phones to their phones.

By swapping SIM, a hacker last year was accused of stealing $ 23.8 million from an electronic money investor.In addition, hackers have used the same technique against the CrowdMachine startup in California and stole the organization's entire $ 14 million virtual money stockpile.Later, two men were arrested for suspected crime.

While the above cases are examples of big burglaries, the actual SIM swap method is often used in smaller operations.

1. Hack SIM: Things to know and how to avoid

CodesTrace has created a list of the top 10 threats that tend to target electronic money in the year 2018, and will most likely be widely used throughout 2019:

1. SIM Swap: Identity theft technique, hijacking victim's mobile device to steal login information and break into e-wallets, or trading accounts to steal electronic money.
2. Scan electronic money: A new form of blockchain spam, which erodes the reputation of recipients by sending electronic money from known money mixers.
3. Electronic taxation: The model of countries using electronic money has been promoted by the governments of Iran and Venezuela.
4. New generation electronic money mixers: Promising money laundering services can exchange poisoned tokens for newly-exploited electronic money, but in fact, it's electronic money laundering through deal.

5. Business fraud: Hackers lurk under the name of unlicensed electronic money service (MSBs) businesses, without financial knowledge, nor approved by law, and therefore causing investors to risk without knowing who to call.
6. Exploiting electronic money according to data center scale: The attacks of appropriating operating rights to exploit large-scale electronic money have been discovered in data centers, including AWS.
7. Lightning online transactions: Allow anonymous bitcoin transactions by "offline conversion" and can now scale up to $ 2,150,000.
8. Decentralized electronic money: Stable tokens can be designed to be used as private coins.
9. Email extortion and terrorist threats: Internet extortionists promote the spread of phishing emails customized to specific areas and objects.This type of scams tend to skyrocket from the second half of 2018 to the present.
10. Crypto Robning Ransomware: Internet extortionists began distributing new malware, emptied e-wallet and stole victim's private keys, while using hostage data.

In addition, CodesTrace also stated that the value of the digital money stolen in 2018 is 3.6 times higher than the average of previous years.In particular, a quarterly comparison shows that the dollar value of electronic money theft is lower in the fourth quarter of 2018 than in the third quarter. Without precautions and lifting Highly understanding the trading floor managers and investors, it is likely that 2019 will still be a "fertile" year for these sophisticated scammers.

See more:

1. Azorult Trojan steals user passwords while running in the background like Google Update
2. Android apps contain malicious code that uses motion sensors to avoid detection
3. MySQL vulnerabilities allow malicious servers to steal data from customers
4. Malware and user security bugs are found in top free VPN applications