Stealing, electronic money scams in 2019 may hit a record of $ 4.3 billion

Fraud, theft, and electronic money scams can cost mankind $ 4.3 billion in 2019.

According to the latest report by CextTrace, one of the most trusted security intelligence companies operating in the world's most prestigious electronic currency, fraud, theft, and possible cryptocurrency scams humanity costs $ 4.3 billion in 2019.

This number may even be higher because in the first quarter of this year, the world lost more than 1.2 billion dollars in electronic money because of fraudulent activities, sophisticated ransom attacks, while the peak season of online phishing activities (the last months of the year) have not really started yet.

1. 32 million dollars 'evaporated' in the hack of Bitpoint electronic money trading floor

Fraud, theft, and electronic money scams can cause $ 4.3 billion in losses in 2019

CextTrace has now released the Electronic Anti-Money Laundering Report (Cryptocurrency Anti-Money Laundering) for the second quarter of 2019, including the latest overview statistics on theft, fraud and large electronic money laundering. , attracting a lot of interest worldwide.

Electronic money theft is still on the rise

Although information on electronic money theft tactics has become more and more dense, along with advanced prevention measures have also been introduced, the number of electronic money theft is not only not decline, but

on the contrary, there are signs of rapid increase in both quantity, scale, and complexity.

In fact, digital exchanges, electronic wallets and electronic depository services in the world mostly try to strengthen defensive measures. But hackers are also masters of cyber security, they are constantly innovating, creating sophisticated new tricks and even surpassing the current defensive capabilities of online facilities. That is why the damage from fraudulent acts, electronic money theft is constantly increasing.

Even Binance, the world's No. 1 electronic money trading platform, has lost tens of millions of dollars of electronic money after sophisticated violations, caused by a variety of complicated methods like phishing and spread cocktails. malicious code, as well as many other types of attack vectors.

1. Hacker earned $ 32,000 in 7 weeks by fixing a series of gaps in e-money projects

The number of electronic money theft incidents this year has shown signs of rapid increase in both quantity, size, and complexity.

So in the second quarter of this year alone, cybercriminals pocketed $ 125 million Bitcoin, Ethereum and many other digital assets from a wide range of large and small exchanges around the globe. This figure was calculated by CipherTrace based on the value of electronic currencies at the time they were stolen, with the exchange rate of Bitcoin and many other currencies continuously increasing in the last few months, the value of the number The stolen virtual money will be much larger, maybe 3 times - according to experts' calculations.

In addition, many cases are still in the process of investigation, inventory losses, and after completion can push the total damage significantly higher.

1. The Cuban government considered using electronic money to overcome US sanctions

2019 may be the year of Exit Scam

It is not exaggerating to say that Exit Scam is one of the most painful issues in the internet age, especially in the area of ??electronic money investment.

If you do not know, Exit Scam is a fraud by creating trust, tricking a victim into transferring money, then hugging money or not doing it as a contract. For example: If you buy product A from a certain online shop, you paid but the other shop failed to deliver, deliver, or deliver the wrong product.

Not only exists in traditional purchases, reports of CipherTrace also pointed out that Exit Scam is currently emerging as a new phishing trend in the field of electronic money, while the damage they cause can obscure losses from normal network attacks.

1. Selling $ 2 million of Bitcoin illegally, the American man is at risk of peeling five calendars

Exit Scam is currently emerging as a new phishing trend in the field of electronic money

Indeed, while hacking / cyber attacks only brought hackers $ 277 million in the first half of 2019, the total number of Exit Scam cases under investigation could cost up to $ 3.1 billion. And, 874 million dollars of electronic money among them has certainly been appropriated - many times more than the traditional form of cyber attack.

The report of CipherTrace also mentioned some shocking new information from the Canadian federal court regarding the electronic money scam that occurred in the first quarter of this year by QuadrigaCX - the name that was once the largest online trading floor. Canada. According to experts' estimates, continuous frauds and theft of electricity have caused investors in QuadrigaCX to lose more than $ 200 million in electronic money.

At the end of the second quarter of this year, there was also a bizarre fraud-related story in the form of Exit Scam (not specifically confirmed) targeting PlusToken, one of the major Korean exchanges, and allegations related to pyramid scam model (a fraud model mainly appears in the business sector, in which members are promised profits or rewards by joining the model and introduce new people to join.) The fraud could affect tens of thousands of electronic money investors, with estimated losses of up to $ 2.9 billion.

The second quarter also recorded the collapse of many major Darknet markets after aggressive suppression campaigns from intergovernmental law enforcement organizations. The most prominent of these are the cases of:

1. Wall Street Market: The name is considered the second largest web transaction market in the world, was destroyed and confiscated by the German Federal Police Investigation Agency (with the help of Europol forces). set of servers and more than 550,000 Euro (about 615,000 USD) in cash, along with a large amount of Bitcoin and Monero (all at 6 digits).
2. DeepDotWeb: Requested by the FBI to close under arrest warrants by the Office of the US Attorney General of the Western District of Pennsylvania, Department of Intellectual Property and Crime of the US Department of Justice (DoJ). Earlier, another large darknet market, Silkkitie, was forced to close down for investigation.

Statistics have shown that despite the popularity of private currencies, Bitcoin is still the preferred name, often found in every black trading market and cybercrime.

Global regulatory operations

With an alarming increase in the number of online fraudulent acts, as more countries become a haven for cybercrime, international regulators have maximized potential to monitor your virtual assets. It can be mentioned as an 'iron hand' style transaction management measure proposed by the Financial Action Task Force (FATF) - an organization backed by G20 nations at the level of The highest, which requires that all transactions between online virtual currency exchanges must include personal information about senders and recipients, similar to international bank transfer and SWIFT transfers. of mainstream monetary funds today.

1. Facebook's Libra electronic currency has not yet set a launch date but scam tricks are ready

Libra, Facebook's electronic currency has sparked many debates across the globe

Electronic money regulations are now considered mandatory globally and politicians are increasingly expressing concerns about the potential for financial disruption of activities related to blockchain. It can be said that the decision to penetrate the world of Facebook's electronic money with the Libra project has caused fierce debates at major global economic forums, involving risks and benefits. of this new type of financial instrument.

The electronic money market is holding more issues than ever before.

1. President Trump: 'I'm not a fan of Bitcoin or any other electronic money'

can search for similar articles on tips and guides. Thank you for reading and for following us regularly.