How do hackers turn thousands of bitcoin virtual currencies after stealing into cash?

With extortion code, hackers earn millions of dollars in virtual money, but how do they convert them into real money to use?

Digital money has gradually become a favorite tool for hackers and cyber criminals because transactions are done almost anonymously, allowing them to use in the underground market for illegal transactions, taking thousands dollars in blackmail attacks, such as WannaCry, Petya, LeakerLocker, Locky and Cerber .

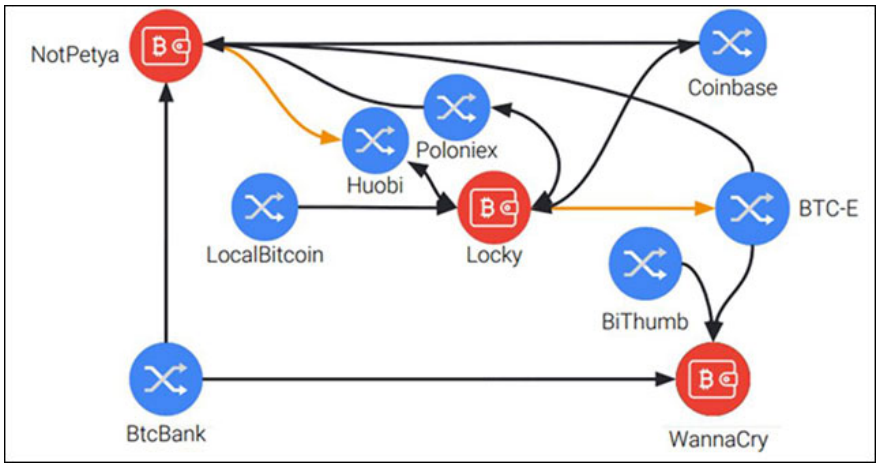
Every day, we still hear about hacking virtual currency trading floors or electronic wallets, so hackers can steal millions of dollars in Bitcoin or Ethereum.

The most recent example is the theft of Ethereum - one of the increasingly popular and very popular virtual currencies - whereby about half a billion dollars have been stolen.

Obviously, after stealing hundreds of thousands of dollars from virtual exchanges, e-wallets or victims of blackmail, cyber criminals will not keep them in virtual form but must transfer them to money. face to use in the real world.

How can hackers turn virtual money into cash without being detected?

You may not know, some virtual money trading floors have money laundering activities, illegal activists, help hackers and cyber criminals easily transfer virtual money into cash without being detected.



Track payment via blockchain

According to a recent study by three Google researchers, more than 95% of bitcoin payments taken from victims of extortion money have been converted into cash through Russia's virtual currency trading platform. BTC-e name, since 2014.

Interestingly, just two days before Google announced, one of BTC-e's founders, Alexander Vinnik, was arrested by Greek police by washing more than $ 4 billion bitcoin for criminals.

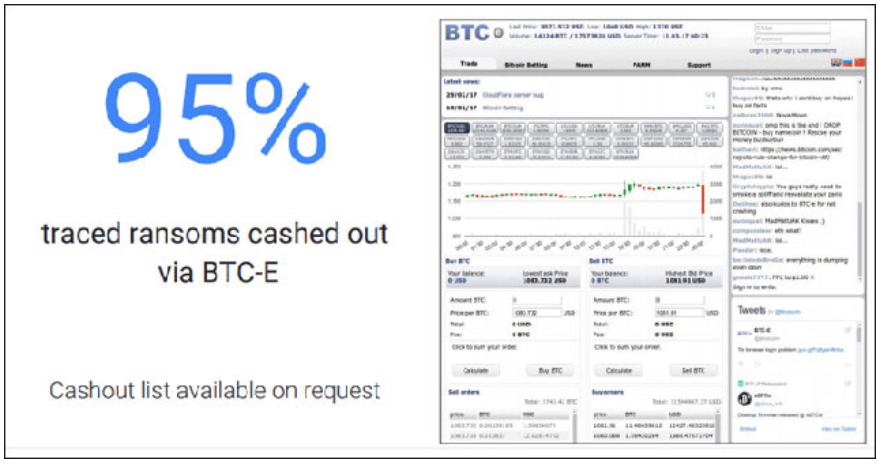
'We discovered the secret money transfer points, monitored the money out of Bitcoin system, allowed the authorities to track money by traditional financial monitoring methods', 3 researchers Luca Invernizza, Kylie McRoberts and Elie Bursztein said.

Track extortion payments

The researchers tracked the amount of money step by step, studying the ever-changing ecosystem of extortion code variants (which helped cyber criminals earn at least $ 25 million over the past two years.

1. Ransomware families cause the most damage: according to research, two families of extortion money give hackers the most money, Locky and Cerber, while the variants are still appearing.
2. Crime earns millions: Locky is the most earned name for hackers with 7.8 million dollars and is the first ransomware to earn more than 1 million dollars a month so far. Meanwhile Cerber has earned $ 6.9 million so far and still earns more than $ 200,000 per month.
3. Where victims like to buy bitcoins: obviously the victim also needs BTC to pay the attacker, most victims choose LocalBitcoins, Bithumb and CoinBase to buy BTC. In it, 90% of victims pay in a transaction.
4. How the attacker turns virtual money into real money: according to research, more than 95% of bitcoin payments for extortion are transferred to cash through BTC-e, a service that was launched in 2011.
5. Botnet crimes: criminals behind Dridex, Locky and Cerber have hired Necurs botnets to distribute large-scale ransomware.

Google conducts research with researchers from New York University, University of California San Diego and Chainalysis blockchain analysis company.



95% of bitcoin is converted into cash via BTC

Talking about BTC-e, the virtual money trading platform is said to be related to the cash conversion of stealing bitcoin from the Japanese trading platform, which is very popular with Mt. Gox. This floor was collapsed in 2014 after performing many mysterious robberies.