allot
See. Control. Secure.

Threat Bulletin

Cryptocurrency and Cybercrime

November 2019

Introduction

Today cryptocurrencies have become a global phenomenon known to most people. They are quickly going mainstream and more people are exploring the crypto world. However, investors aren't the only ones interested in cryptocurrency - cybercriminals are thrilled with the idea of unregulated money. It has opened new attack vectors and a new way for cybercriminals to disappear leaving no trace.

Due to their anonymous nature, cryptocurrencies play an essential role in the underground economy. They are used for most criminal-to-criminal (C2C) payments on Darknet forums and marketplaces. Around $76 billion of illegal activity per year involves Bitcoin[1], and by 2021 Cybersecurity Ventures predicts that more than 70 percent of all cryptocurrency transactions will be for illegal activity. Also, many hackers demand payment from victims for attacks, such as ransomware or DDoS extortion, in cryptocurrencies (V2C – victim-to-criminal).

While the rise of cryptocurrency facilitates cybercrime in general, it gave a significant boost to the development of novel types of cyberattacks. Why is cryptocurrency so appealing to cybercriminals? How is it used in the cybercrime ecosystem?

What is Cryptocurrency?

"Cryptocurrency is an internet-based medium of exchange that uses principles of cryptography to conduct and secure transactions. Cryptocurrencies leverage blockchain technology to gain decentralization, transparency, and immutability."

Simply put, cryptocurrency is digital money created using computer programs and computing power. It's unlike fiat (regular) currency — dollars or euros — because it's digital-only, there are no bills or coins to carry around.

The most important feature of a cryptocurrency is that it's completely decentralized and is not controlled by any central authority. Unlike paper currencies controlled by governments, crypto operates independently of central banks – e.g. bitcoins are created in a pre-determined rate regardless of its value and without any economic or political influence. Blockchain technology, which lies at the core of cryptocurrency, lets people and institutions shift funds instantly and without the need for a middleman.

[1] Study by the University of Sydney.

It's called **crypto**currency because it's built on strong cryptography. All transactions are verified cryptographically by all users in the network and are recorded in a decentralized public ledger known as the blockchain. The reason that the blockchain cannot be altered is that the data in the blockchain is validated by millions of participants, or "miners," scattered across the globe.

Bitcoin is the first and most famous cryptocurrency, which serves as a digital "gold standard" for the whole ecosystem. It remains the preferred and most frequently used cryptocurrency among cybercriminals, according to the 2019 Internet Organized Crime Threats Assessment (IOCTA) report by Europol. In 2019, ten years since its initial release, Bitcoin's market cap reached $165.39 billion and transaction volume amounts to more than 300.000 transactions per day[2].

Why Are Cryptocurrencies Appealing to Cybercriminals?

Cryptocurrencies have inherently low levels of regulation and are not governed by a central authority, meaning the transactions can't be closely monitored. This makes them a haven for criminal activity around the globe. Cryptocurrencies can easily carry millions of dollars across borders without detection.

1) **Pseudonymous**: Neither transactions nor accounts are connected to real-world identities, so it's easy for cybercriminals to remain unidentified when they use crypto. Payments are made from "Bitcoin addresses," and individuals can easily create new addresses. While it is usually possible to analyze the transaction flow, it is not an easy task to connect the real-world identity with owners of those addresses.
2) **Fast and global**: Crypto transactions are propagated nearly instantly in the network and are confirmed in a couple of minutes. Since they happen in a global network of computers, they are completely indifferent to physical location. It doesn't matter if you send Bitcoin to your neighbor or to someone on the other side of the world.

Cryptocurrencies have become the most popular means of payment on the dark web because they allow traders and buyers to remain anonymous. Alternative currencies such as Monero and Verge, which are privacy-focused and offer even greater anonymity than Bitcoin, have become favorites for criminal activities on the Darknet.

[2] Numbers are correct as of November 2019.

There’re several types of cyberattacks where cybercriminals are taking advantage of cryptocurrencies. They include **ransomware, DDoS extortion, cryptojacking,** and **cryptocurrency exchange hacks.**

Ransomware

One of the biggest cybersecurity trends in history, ransomware is designed to extort money by encrypting user data. This type of malware typically displays an on-screen message offering to restore access after the victim pays a ransom. Typically, cybercriminals demand payment in the form of Bitcoin or other digital currency. Thus, the attackers are virtually impossible to track down.

2017 was the biggest year for ransomware attacks – global outbreaks of the notorious WannaCry and NotPetya ransomware that brought down many large organizations. 2017 was also the year when the price of Bitcoin skyrocketed from below $1,000 to nearly $20,000, reaching its all-time high of $19,783.21 on Dec. 17[3]. Coincidence? We don’t think so.

DDoS Extortion

DDoS extortion (RDoS or ransom-driven DDoS) campaigns have become very common and are driven, in part, by their ability to use cryptocurrency payments, which make it difficult for investigators to track the money as it flows from victims to criminals.

The tactic is the following: cybercriminal blackmails organizations by asking them to pay Bitcoin to avoid their site or service being disrupted by a DDoS attack. Many hackers are motivated by the potential for financial gain and the ease at which such attacks can be performed. Extortion is one of the oldest tricks and one of the easiest ways for hackers to profit.

A prominent group that carried out a lot of activity using the 'DDoS-as-an-extortion' technique was DD4BC (short for "DDoS for Bitcoin"), which first emerged in 2014 and was arrested by Europol in 2016. In October 2019, a fake "Fancy Bear"[4] group was sending ransom demands to banks and financial organizations across the word, threatening to launch DDoS attacks. In some cases, the cybercriminals did carry out small DDoS attacks to demonstrate their capabilities and validate the threat, but no serious follow-up attacks have been observed.

Cryptojacking

Cryptojacking shook up the threat landscape in 2017 and 2018, when cryptocurrency prices surged to record levels. It also made a comeback during the summer of 2019. The primary reason for this was the general revival of the cryptocurrency market, which saw trading prices recover after a spectacular crash in late 2018.

The attack consists of hackers using the computing power of a compromised device to generate (“mine”) cryptocurrency without the owner’s knowledge. The types of devices vulnerable to cryptojacking are not limited to smartphones, servers, or computers. IoT devices can be infected as

[3] CoinDesk Bitcoin Price Index (BPI).

[4] The infamous hacking group associated with the Russian government, known for hacking the White House in 2014 and the DNC in 2016.

well. The main effects of cryptojacking for users include: device slowdown; overheating batteries; increased energy consumption; devices becoming unusable; and reduction in productivity.

There're two main types of cryptomining - passive cryptomining through scripts running in a victim's internet browser, and more intrusive cryptojacking malware. Both techniques exploit a victim's processing power, without their permission, to mine cryptocurrencies.

In the beginning, malware operators deployed Bitcoin-based cryptominers, but as Bitcoin became harder to mine on regular computers, they shifted to other altcoins. Due to its anonymity-centric features, Monero slowly became a favorite currency among cybercriminal gangs.

The closure of Coinhive, the most popular mining script, in March 2019 led to a decline in the frequency of browser-based cryptomining. However, attacks against consumers and organizations continue to happen and evolve. There are reports of cryptojacking malware both going 'file-less' and incorporating the Eternal Blue exploit in order to replicate and propagate themselves over a network, like a worm virus.

Cryptocurrency Hacks

Cryptocurrency itself is a very appealing target for cybercriminals. In 2018, over $1 billion in cryptocurrencies was stolen from exchanges and other platforms worldwide. Attacks and fraud, which historically targeted regular payment systems, banks and fiat currencies, have now been adapted to incorporate cryptocurrencies. As such, attacks on various crypto assets like crypto exchanges or personal crypto wallets have now became a routine – an increasing number of malware and phishing activities are targeting crypto-investors and enterprises.

How to protect against ransomware:

In order not to get infected, follow basic security practices in your day-to-day, e.g. do not open suspicious email attachments, do not click on unknown links, make regular offline backups, install software updates when they become available, etc. To get more tips, check out our Ransomware Survival Guide.

Against cryptojacking:

- Avoid installing "free" apps from unofficial sources - other than Google Play Store or App Store.
- Never click on suspicious email links unless you know who sent it to you. Email is the most popular vector for infecting computer systems with malware.
- Use strong passwords for computers, mobile and IoT devices, and Wi-Fi networks.
- Patch operating system and software on a regular basis.

Look for the following symptoms of infection: slowdown of the device, a spike in CPU usage, overheating of the battery up to the point that the phone becomes unresponsive. However, that's not always the case - some malware can be configured to limit the CPU/GPU usage, reducing its impact and thereby avoiding detection by not leaving the phone totally useless. In order to avoid this threat, users should check if their telecom operator offers a security service for cyberprotection of mobile and home devices that can block it.

To protect enterprise assets from cryptojacking and other security threats a multilayer security approach that combines prevention and detection is a best practice. Prevention that blocks unauthorized access is a general requirement, but specifically enterprises should incorporate network visibility and control that is able to detect and block crypto websites, applications and protocols, and other risky apps that can serve as hidden channels for cybercriminal activity.

Against DDoS extortion:

Industry experts don't recommend paying the ransom - there is no guarantee the attack will arrive or that the payment would prevent it. In many cases, such attacks are "empty" threats – their authors are using scare tactics hoping to fool victims into paying, and ransom letters aren't followed by any serious attacks or disruptions to the service. Organizations should consider installing DDoS protection solutions that automatically detect and block even the smallest DDoS attacks.

Conclusion

Cryptocurrencies have been around for already a decade, but it is only since mid-2017 that they have gone mainstream and attracted huge criminal interest. Digital money is here to stay and will probably play a significant role in the future economy. As such, it will always be a lucrative target for cybercrime. Protection for the mass market and for enterprises against crypto-related attacks should be part of everyone's security strategy.

Are you concerned about cyber threats related to crypto?
We can assist.

Contact Allot