Cyber Snapshot

Exploring and Assessing Current Topics

MICHIGAN CYBER COMMAND CENTER (MC3)

March 01, 2024
CS-03-2024

CRYPTOCURRENCY & CYBERCRIME

OVERVIEW:

Cryptocurrencies like Bitcoin, Ethereum, and Monero have exploded in popularity in recent years. However, along with increased mainstream adoption, cryptocurrencies have also seen a rise in use by cybercriminals. The presumed anonymity and global, decentralized nature of most cryptocurrencies make them appealing tools for illegal online activities. This snapshot examines how features inherent in cryptocurrency technology have instigated different types of cybercrimes.

Ransomware Attacks

One of the most lucrative forms of cybercrime utilizing cryptocurrency is ransomware attacks. These attacks involve malware that encrypts a victim's computer files until a ransom payment is made and a decryption key is provided. In early ransomware campaigns, payments were demanded through untraceable methods like prepaid cards or wire transfers. However, most ransomware cybercriminals shifted to requiring payment in Bitcoin and other cryptocurrencies.

Several characteristics make cryptocurrency the ideal form of ransom payment. Transactions in Bitcoin and other can be difficult to trace compared to traditional financial systems. The pseudonymous nature of cryptocurrency wallets can also allow criminals to evade identification. Since transactions cannot be reversed, once ransom payments are sent, cybercriminals easily abscond with the funds. The popularity of ransomware has surged since cybercriminals shifted to relying on cryptocurrency payments. Recent estimates show victims paid out close to $1 Billion worth of cryptocurrency to ransomware attackers in 2023 alone.

Illegal Darknet Commerce

Beyond ransomware, cryptocurrencies have also been widely adopted to facilitate trade in illegal goods or services on darknet marketplaces. The dark web allows anonymity through networks like Tor and cryptocurrencies provide similarly anonymous payment options difficult to block or shut down. Early dark web markets like The Silk Road popularized the model of using Bitcoin to buy and sell illicit drugs, stolen financials like credit cards or personal data, weapons, and more with minimal traceability.

This document is the property of the Michigan Cyber Command Center (MC3) and is prepared for the limited purpose of information sharing. The information is designated UNCLASSIFIED – TLP: CLEAR Information found within this document can be shared without restriction. This document must not be reclassified in any way, in whole or in part. Violation of this restriction will be cause for removal from MC3 distribution lists.

Although darknet markets sporadically get taken down by law enforcement and scammed by admins, new ones quickly emerge to sell or auction off similar illegal offerings, almost universally transacted through cryptocurrencies. The growth of these underground crypto-fueled bazaars continues to expand cybercriminal enterprise and profits built on abuse of cryptocurrency infrastructure.

Other Cyber Threats

Beyond funding ransomware and dark web marketplaces, cryptocurrency also underpins other cybersecurity threats. Cryptocurrency scams are abundant, often involving thousands of dollars worth of stolen cryptocurrency from victims. Stolen cryptocurrency scammed from individuals is also frequently sold on darknet markets. Additionally, cryptojacking attacks have emerged in which hackers exploit vulnerabilities or employ malware to secretly use a computer's processing power to mine new cryptocurrency. While free money for hackers, cryptojacking hijacks system resources, slows down devices, and can potentially damage hardware not designed for such resource-intensive mining. Though the techniques vary, cybercriminals continue pivoting to cryptocurrencies as transactional mechanisms to propel wider threat campaigns.

Recap

In closing, major characteristics of cryptocurrencies – most notably their anonymity, difficulty to trace, and irreversibility – provide affordable operational benefits to hackers and scammers. Ransomware, dark web commerce, crypto fraud, and cryptojacking are only a few of the most prominent examples to date. As long as most cryptocurrency systems retain these traits in some form, their inherent privacy and complexities will likely continue inviting criminal abuse at scale unless mitigated. It is important to maintain good cybersecurity hygiene to prevent becoming a victim of cybercrime.

ADDITIONAL RESOURCES:

(U) https://www.chainalysis.com/blog/ransomware-2024/

For more information and additional resources, please visit www.michigan.gov/mc3.

To report a cyber incident to the MC3, please contact 1-877-MI-CYBER or mc3@michigan.gov.

This document is the property of the Michigan Cyber Command Center (MC3) and is prepared for the limited purpose of information sharing. The information is designated UNCLASSIFIED – TLP: CLEAR Information found within this document can be shared without restriction. This document must not be reclassified in any way, in whole or in part. Violation of this restriction will be cause for removal from MC3 distribution lists.