CRYPTO CRIME INVESTIGATION

Crypto Crime Typologies, Modus Operandi

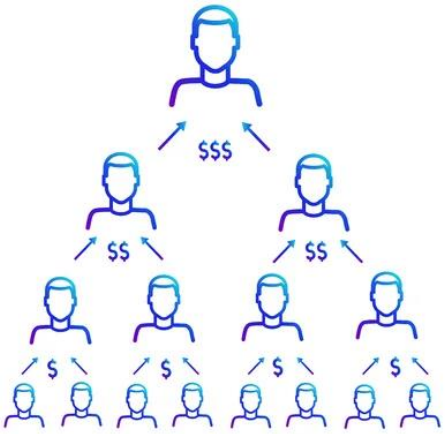
JANUARY 1, 2023

PRAVIN MANDLOI [DATA SCIENTIST]
Superintendent of Police, Central Bureau of Investigation, New Delhi

Fraud related to Bitcoin and other cryptocurrencies can take many forms, and the specific modus operandi can vary significantly depending on the type of fraud being perpetrated. Some common types of Bitcoin fraud and their associated modi operandi include:

Ponzi Schemes:

These are investment schemes in which returns are paid to earlier investors using the investments of more recent investors. The modus operandi for a Ponzi scheme involving Bitcoin may involve promoting an investment opportunity that promises high returns, and using the proceeds from new investors to pay returns to earlier investors.



Phishing Attacks:

These are attempts to obtain sensitive information, such as login credentials, by disguising oneself as a trustworthy entity. The modus operandi for a phishing attack involving Bitcoin may involve sending a fraudulent email or message that appears to be from a legitimate Bitcoin exchange or wallet, and asking the recipient to enter their login details.

Ransomware Attacks:

These are attacks in which the attacker demands a ransom in exchange for releasing control of a victim's computer or data. The modus operandi for a ransomware attack involving Bitcoin may involve infecting a victim's computer with malware that

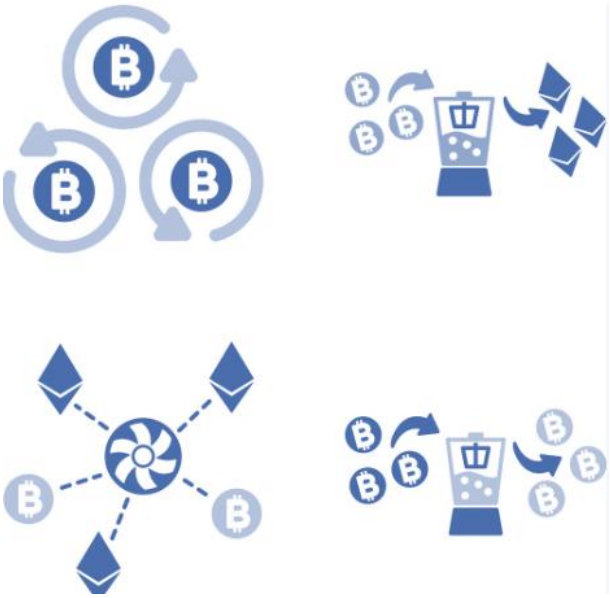
encrypts their data, and then demanding payment in Bitcoin in exchange for the decryption key.

Malware Attacks:

These are attacks in which malware is used to gain unauthorized access to a victim's computer or steal sensitive information. The modus operandi for a malware attack involving Bitcoin may involve distributing malware that is designed to steal Bitcoin or other cryptocurrency from a victim's wallet or exchange account.

Bitcoin Tumbler:

A Bitcoin tumbler, also known as a Bitcoin mixing service, is a service that is designed to help users conceal the origin of their Bitcoin transactions. Bitcoin transactions are recorded on the public blockchain, which means that they can be traced back to the original source. A Bitcoin tumbler is intended to obscure this trail by mixing the user's Bitcoin with the Bitcoin of other users, making it more difficult to trace the origin of the transaction.



Bitcoin tumbler fraud is a type of cybercrime in which the perpetrator operates a fake Bitcoin tumbler service, also known as a Bitcoin mixing service. A Bitcoin tumbler is a legitimate service that is used to obscure the origin of Bitcoin transactions by mixing the coins with those of other users, making it difficult to trace the origin of the funds. However, some fraudsters have set up fake tumbler services in order to steal Bitcoin from unsuspecting users.

The modus operandi for a Bitcoin tumbler fraud typically involves the perpetrator promoting their fake tumbling service and offering attractive terms,

such as low fees or fast turnaround times. When a user sends their Bitcoin to the tumbler, the fraudster keeps the coins and does not return them to the user.

Blackmail Scam:

A Bitcoin blackmail scam is a type of cybercrime in which the perpetrator threatens to reveal embarrassing or damaging information about the victim unless they receive a payment in Bitcoin or some other cryptocurrency. These scams can take many forms, but they typically involve the attacker claiming to have evidence of the victim's involvement in some sort of illegal or illicit activity, or threatening to release sensitive personal information about the victim unless they receive a payment.

These scams are often delivered through email or social media, and they may be designed to appear as though they are from a government agency or other legitimate organization. The perpetrators may use tactics such as social engineering or psychological manipulation to coerce the victim into making a payment.

Ransomware:

Ransomware is a type of malware that encrypts a victim's files and demands a ransom from the victim to restore access to the files. Ransomware attacks are often financially motivated, and the perpetrators may demand payment in Bitcoin or another cryptocurrency as a way to facilitate the transaction and make it more difficult to trace the payment.

Bitcoin and other cryptocurrencies can be attractive payment methods for ransomware attacks because they can be sent and received anonymously, and they do not require the use of a traditional financial institution. However, paying the ransom does not guarantee that the victim will regain access to their files, and there is a risk that the perpetrator may not hold up their end of the bargain.

Sextortion:

Sextortion is a type of cybercrime in which the perpetrator threatens to reveal embarrassing or sensitive information about the victim, or to take some other action, unless the victim pays them a ransom. Sextortion scams may involve threats to release explicit or embarrassing photos or videos, or to reveal sensitive personal information, unless the victim pays the perpetrator a sum of money. The ransom is often demanded in Bitcoin or another cryptocurrency because it allows the perpetrator to remain anonymous and makes it more difficult to trace the payment.

Sextortion scams are often delivered through email or social media, and they may be designed to appear as though they are from a government agency or other legitimate organization. The perpetrators may use tactics such as social engineering or psychological manipulation to coerce the victim into making a payment.

Darknet Market:

The darknet is a part of the internet that is not indexed by search engines and can only be accessed using specialized software, such as the TOR browser. The darknet is often associated with illegal activities, such as the sale of illicit goods or the distribution of illegal content.

Bitcoin and other cryptocurrencies are often used on the darknet because they allow for anonymous transactions, making it more difficult to trace the parties involved and the origins of the funds. As a result, Bitcoin and other cryptocurrencies have been used in a variety of frauds and scams on the darknet, including:

The sale of fake or counterfeit goods: Some darknet vendors may sell fake or counterfeit goods and accept payment in Bitcoin or other cryptocurrencies. These goods may be of poor quality or may not be delivered at all.

Investment scams: Some darknet vendors may operate investment scams, such as Ponzi schemes or HYIPs (high-yield investment programs), and accept payment in Bitcoin or other cryptocurrencies. These scams may promise high returns but ultimately result in the loss of the victim's funds.