No images? Click here

Block the Chain -Supervising the Crypto Criminal

by Brian J. Kelly - Supervisory Cyber Analyst

"Crypto-assets are a type of private sector digital asset that depends primarily on cryptography and distributed ledger or similar technology. The different segments of crypto-asset markets – including unbacked crypto-assets (such as Bitcoin), so-called "stablecoins", and decentralized finance (DeFi) – are closely interrelated in a complex and constantly evolving ecosystem, and need to be considered holistically when assessing related financial stability risks." (Financial Stability Board www.fsb.org). While most of us have heard of cryptocurrency such as Bitcoin, also included under the crypto-asset umbrella are lesser

known assets like non-fungible tokens (NFTs). NFTs are blockchain-based tokens that each represent a unique asset like a piece of art, digital content, or media. The common denominator is the decentralized and often unregulated design of the blockchain. This design means no single person, group, entity or government has control. Unfortunately, this can lead to instability and an area ripe for fraudulent activity.

According to BankRate.com, as of January 2023, the value of all existing cryptocurrency is $804 billion. And due to this large amount of value, there are many scams and illegal activities funded by and/or targeting cryptocurrency. These schemes include investments scams, romance scams, impersonation scams, and blackmail. For more information and descriptions, please visit the Federal Trade Commission - What To Know About Cryptocurrency and Scams https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams#know

Arrests and prosecutions of cases involving crypto-assets have made their way into the courts in recent years, and as a result, individuals involved in these cases have come under community supervision. Cases include prosecutions of NFT “rug pull” schemes ("A rug pull is a scam where a cryptocurrency or NFT developer hypes a project to attract investor money, only to suddenly shut down or disappear, taking investor assets with them. The name comes from the idiom “to pull the rug out” from under someone, leaving the victim off-balance and scrambling." bankrate.com),

cryptojacking ("Cryptojacking involves malware installed on devices, or small bits of code injected into browsers, that surreptitiously steal computer processing resources to mine cryptocurrency. This attack does not damage computers or victims' data, though targets might notice lagging performance."https://duo.com/decipher/cybercriminals-still-want-to-cash-in-on-crypojacking), shadow banking (https://corporatefinanceinstitute.com/resources/cryptocurrency/shadow-banking-and-cryptocurrencies/), scam crypto recovery sites (https://manhattanda.org/manhattan-d-a-s-office-seizes-scam-cryptocurrency-recovery-site/), etc. You can also find numerous civil and criminal filings related to crypto-assets at the U.S. Securities and Exchange Commission (SEC) website under https://www.sec.gov/spotlight/cybersecurity-enforcement-actions and https://www.sec.gov/litigation/litreleases.htm. These filings are extremely useful when developing language for use in conditions of supervision, which can be constructed similar to existing financial conditions. For an example, see the link to the action and language below:

https://www.sec.gov/litigation/litreleases/2023/lr25729.htm

"permanently restrained and enjoined from participating, directly or indirectly, including, but not limited to, through any entity they control, in any offering of crypto asset securities; provided, however, that such injunction shall not prevent them from purchasing or selling any crypto asset security for their own personal accounts."

What should you look for if you are monitoring the computer & Internet activity of a person under supervision (PUS) for a crypto-asset related offense? It is important to realize that if a PUS owns crypto-assets, it is not an automatic red flag. It can be treated as any other financial asset when assessing a PUS's financial status. Important questions to ask: Do you have a crypto wallet? What exchange do you use? Is your exchange account linked to a traditional financial institution? What's your public key/address? A "Crypto-Asset Financial Statement" can be used to collect information on all digital assets such as cryptocurrency, non-fungible tokens, etc. With the PUS's public key/address, historical transactions can be verified via a blockchain ledger, such as Block Chain Explorer https://www.blockchain.com/explorer.

An excellent resource for those starting to familiarize themselves with crypto-asset investigations is the Cryptocurrency Investigations Handbook, available for free (with registration) from the Blockchain Intelligence Group (BIG) https://blockchaingroup.io/cryptocurrency-investigations-handbook/. BIG's training section is run by William (Bill) J. Callahan III, CCI, Director of Government & Strategic Affairs, who spent 20+ years with the Drug Enforcement Administration (DEA), including as the Special Agent In Charge (ret.) for the St. Louis division. Bill is an expert in financial crimes investigations and also active in providing training resources for the Anti-Human Trafficking Intelligence Initiative (ATII) https://followmoneyfightslavery.org/. The

Cryptocurrency Investigations Handbook cites important information to obtain when collecting evidence relating to a crypto-asset investigation including:

-The public key or address.

-The hash/ID of the transaction.

-The quantity of cryptocurrency transferred.

-The associated fees.

-Any change addresses that were generated from the transaction.

-Fiat currency conversion for each value at the time of the transfer.

Other issues to be aware of during investigations and supervision include the following: common payment apps like CashApp allow users to send/receive cryptocurrency like Bitcoin. The account holder will have a Bitcoin address for this purpose and would be different from the payment app username. The Bitcoin Abuse Database https://www.bitcoinabuse.com/ tracks bitcoin addresses used by ransomware, blackmailers, fraudsters, etc. Users can report Bitcoin addresses used by criminals and hackers, as well as check if an address has been linked to a cyber attack.

On June 29, 2023, Blockchain Intelligence Group and Bluestone Analytics, in conjunction with the Nassau County Police Department, will sponsor a free training for law enforcement entitled "Decrypting the Digital Underworld: Unraveling Cryptocurrency, Darkweb, and AI

Investigations" Register here (law enforcement personnel only): https://blockchaingroup.io/decrypting-the-digital-underworld/

IPPC Technologies continues to strive towards predictive and proactive solutions so officers can intervene early, address areas of concern and change behavior. For more information on IPPC's services such as Spotlight, please call IPPC at (888) WEB-IPPC. For any questions/feedback on this or previous article topics, feel free to contact me directly at bkelly@ippctech.net or by calling (516)341-4201. Links to past articles can be found on my personal website.

Existing customers using Spotlight can give feedback on the service by taking the Spotlight Performance Survey by clicking here.

IPPC TECHNOLOGIES
PO BOX 60144
KING OF PRUSSIA, PA 19406
TEL: 888-WEB-IPPC (932-4772)
INFO@IPPCTECH.NET
WWW.IPPCTECH.NET