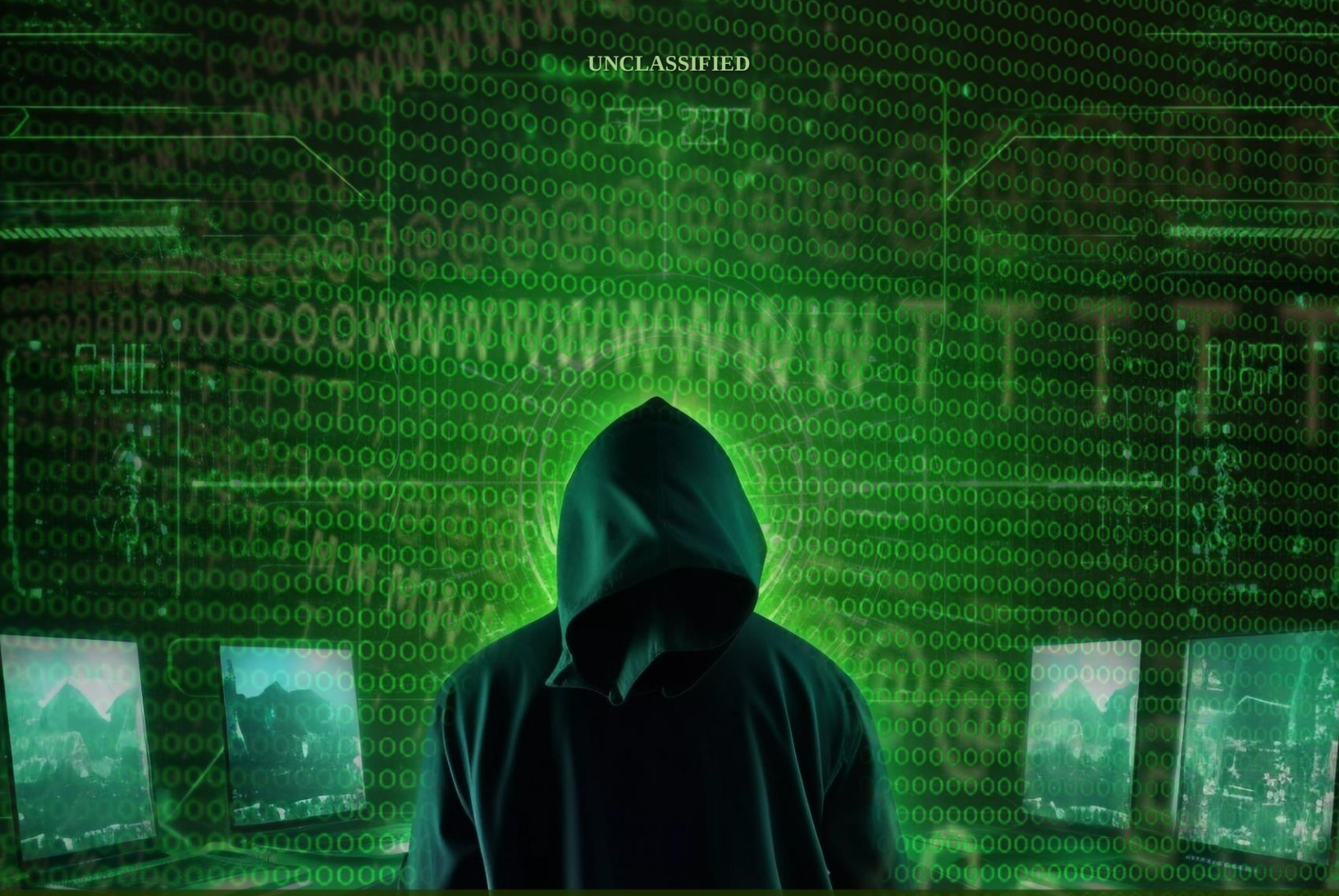
UNCLASSIFIED



THE USE OF NON-STATE-SPONSORED

CRYPTOCURRENCIES

BY CRIMINAL ORGANIZATIONS

EXECUTIVE SUMMARY

INTELLIGENCE OPERATIONS COMMAND CENTER
DEPARTMENT OF INTELLIGENCE AND SECURITY STUDIES AT COASTAL CAROLINA UNIVERSITY

DECEMBER 2023

ABOUT THIS PROJECT

This unclassified report contains the executive summary of a semester-long, open-source research project led by the student analysts of the **Chanticleer Intelligence Brief (CIB)**, a pre-professional initiative of the **Department of Intelligence and Security Studies (ISS)** at **Coastal Carolina University (CCU)**. The CIB operates as an ancillary practicum for students in the ISS program, who wish to cultivate and refine their ability to gather, analyze, and present information in accordance with methods and techniques used in the intelligence profession. The project was inspired by an invitation extended to the CIB by United States Secret Service Special Agent **Gabriel Cazares**, of the Washington Field Office. Funding for this project was provided by the **Thomas W. and Robin W. Edwards College of Humanities and Fine Arts** at CCU, and disbursed by CCU's **Intelligence Operations Command Center (IOCC)**.

The ISS Department at CCU wishes to thank Special Agent **Gabriel Cazares** and the **Washington Field Office** of the **United States Secret Service** for this opportunity. We are grateful for the assistance of CCU Edwards College Dean Dr. **Claudia Bornholdt** and CCU ISS Chair Dr. **Jonathan Smith**. Thank you also to Federal Bureau of Investigation Supervisory Special Agent **Michael Connelly**, CCU ISS Professor of Practice **Mark S. Chandler**, Mr. **Alex Fowler**, and IOCC Senior Intelligence Advisory Board Chair **Robert J. Vipperman**. Our thanks also go to CIB Executive Director **Tessa Bentley**, CIB Records Officer **McKenzie Tsiantoulas**, and CIB Senior Analyst **Kristian Nesheim** for their time and useful feedback.

For more about the ISS Department: *www.coastal.edu/intelligence/*
For more about the CIB: *www.cibrief.org/*
For more about the IOCC: *www.coastal.edu/app/academic/iocc/services.html*
For more about the Edwards College: *www.coastal.edu/humanities/*

THE USE OF NON-STATE-SPONSORED

CRYPTOCURRENCIES

BY CRIMINAL ORGANIZATIONS

EXECUTIVE SUMMARY – UNCLASSIFIED

Authored by
Hannah L. Albert, Brandon W. Macallair, and Alejandro A. Olivares

Technical Overview Authored by
Nathan A. Wynkoop

Edited by
Dr. Joseph G. Fitsanakis

December 2023

Intelligence Operations Command Center
Department of Intelligence and Security Studies
Coastal Carolina University


COASTAL CAROLINA UNIVERSITY
INTELLIGENCE AND SECURITY STUDIES
Ex Libertate Veritas

CONTENTS

TASKING

Cryptocurrencies operate on decentralized networks, often without a central authority, making it difficult to trace transactions and hold individuals or entities accountable for illegal activities. Additionally, the regulatory landscape surrounding cryptocurrencies is still evolving and the absence of comprehensive regulations can create loopholes that criminals can exploit. Lastly, cryptocurrencies transcend national borders, posing challenges related to jurisdictional authority, international cooperation, and extradition processes when investigating and prosecuting transnational criminal organizations. The United States Secret Service is interested in original research that addresses the ways in which organized criminal organizations utilize the decentralized landscape of non-state-sponsored cryptocurrencies in order to enable and support their criminal activities.

GUIDING QUESTIONS

1. Who are the principal threat actors of cryptocurrency misuse?
2. How can threat actors be categorized based on their motivations?
3. What is the typology of the threat actors' targets in the digital domain?
4. What methods are threat actors using to launder funds through cryptocurrencies?
5. What is the degree of success of threat actors?
6. What are the emerging threat actors and/or methods of illicit cryptocurrency use?

ANALYSTS

CMC WHISKEY	CMC SIERRA	CMC YANKEE
Director	**Director**	**Director**
Hannah Albert	Brandon Macallair	Alejandro Olivares
Senior Analysts	**Senior Analysts**	**Senior Analysts**
Ryan Lindsey	Noah Ankenbrand	Joshua Koval
Sarantis Markaris	Mason Marlowe	Jordan Maple
Andrew Safer	Brenden Stell	Nathan Wynkoop

Faculty Direction and Supervision: **Dr. Joseph Fitsanakis**
Intelligence and Security Studies Department Chair: **Dr. Jonathan Smith**

KEY JUDGMENTS

- Open-source intelligence indicates a strong correlation between the increasing use of crypto-currencies and a rise in illicit activities by criminal actors.

- The two primary illegal activities involving cryptocurrency are the illegal acquisition of cryptocurrency and the use of cryptocurrency to fund and sustain physical criminal activities.

- Cybercriminal organizations primarily use ransomware, crypto-jacking, and theft to illegally acquire cryptocurrency.

- Ransomware groups are more likely to attack large corporations that have significant financial resources and rely heavily on proprietary data for their day-to-day operations.

- Convertible virtual currency (CVC) mixing online service providers are more likely to facilitate currency laundering for illicit actors, rather than victimize a certain demographic.

- Scammers are more likely to target those on the outlying edges of the age scale. Cybercriminal actors see younger and older demographic groups as more impressionable and more likely to fall for scams.

- China-based chemical companies, like Wuhan Shuokang Biological Technology and Suzhou Xiaoli Pharmatech, use cryptocurrency to sell precursors to opioids to Latin American cartels.

- Latin American criminal actors are highly sophisticated, operate internationally, and are well funded. These actors have cryptocurrency-facilitated contacts with China-based chemical companies, brokerages, and other criminal organizations operating overseas.

- The growth of Ransomware as a Service (RaaS) suggests a likely increase of cybercriminal actors who utilize ransomware. Ransomware on mobile devices may also increase as such devices become more ubiquitous in everyday life.

- Due to the adaptability of scams, it is highly likely that scammers using cryptocurrencies will increase, as new methods and typologies of targets are developed. New techniques, such as 'pig-butchering', which combines romance and investment schemes, are becoming more popular. This morphing of methods reinforces the versatility and adaptability of scamming techniques, which can be used to target a wider range of victims.

- The Vietnam-based Ocean Lotus (APT32), the Hamas-linked Izz ad-Din al-Qassam Brigades, as well as a variety of Lebanese cyber actors, are emerging state-backed cybercriminal actors in the field of illicit cryptocurrency use.

TECHNICAL OVERVIEW

Nathan Wynkoop – Senior Analyst, CMC YANKEE

What is Cryptocurrency?

Cryptocurrency is a virtual currency that operates on decentralized networks using blockchain technology. Unlike *fiat* currencies, such as the United States dollar (USD), cryptocurrency has no physical aspect to it. Blockchains are ledgers that track cryptocurrency transactions[1, 2]. Although technically all cryptocurrency transactions are public, the decentralized network does in some cases enable some transactions and accounts to remain relatively hidden from public view. Transactions are not controlled by a centralized authority; instead, multiple users are able to turn information into blockchain nodes. A node is the location where users run codes on a blockchain[3]. Thus, the main use of cryptocurrencies is to facilitate online transactions on a minimally centralized network.

There are thousands of cryptocurrencies[4]. However, they can be broadly categorized into those that tend to facilitate transparency in accounts and transactions and those that tend to emphasize anonymity[5, 6, 7].

Cryptocurrency Validity

Cryptocurrency usually has no intrinsic value, though this remains a topic of debate among experts. Public perception causes the price of cryptocurrency to rise and fall much like the pattern seen in the stock market. The price of cryptocurrency can also affected by supply and demand. Thus, a larger number of crypto-currency tokens available causes the price to fall, and vice versa. The cryptocurrency market follows basic market flow. There is a limited number of tokens for each cryptocurrency[8]. A token is a type of digital asset or unit of value, created and managed on a blockchain. Crypto-currency tokens represent a specific asset or utility and are often issued through Initial Coin Offerings (ICOs) or Token Sales.

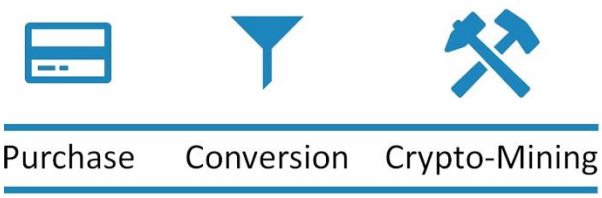


Figure 1: How do users acquire cryptocurrencies?

There are different types of tokens, which serve various purposes within the blockchain ecosystem. Utility Tokens provide access to a specific product or service within a blockchain platform. They are not designed as investments, but rather as a means of accessing a blockchain-based application or network. For example, if there is a decentralized platform for file storage, owning and using the utility token associated with that platform might grant the user the ability to store files on the blockchain. Security Tokens represent ownership in a real-world asset, such as shares in a company, and are subject to securities regulations. Security tokens often provide holders with certain financial rights, such as dividends or profit shares. Stablecoins are pegged to the value of a stable asset, like a *fiat* currency or a commodity. They are designed to reduce the volatility that is common in other cryptocurrencies. Finally, non-fungible tokens (NFTs) represent unique digital or physical assets on a blockchain, such as digital art, music, or virtual real estate. Each token is distinct and cannot be replaced or exchanged on a one-to-one basis with other tokens.

UNCLASSIFIED

Cryptocurrency tokens operate on existing blockchain platforms, such as Ethereum, Binance Smart Chain, or Solana, using smart contracts to define their functionalities and properties. Tokens can be traded on crypto-currency exchanges and stored in compatible wallets, providing users with control and ownership over their digital assets.

How do users acquire cryptocurrencies?

Purchase: Cryptocurrency can be purchased at cryptocurrency automated teller machines (ATMs), as well as online through cryptocurrency websites. One BTC token was worth $34,720.00 as of 4 November at 12:00 EST[9].

Conversion: Cryptocurrency users can obtain other types of cryptocurrencies by converting one type of cryptocurrency to another. For example, one BTC was equal to 18.87 ETH as of 4 November at 12:00[10].

Crypto Mining: Crypto mining refers to the process by which computers running code ensure the legitimacy of cryptocurrency transactions[11, 12]. Computers are required to have a certain hashrate to ensure the legitimacy of transactions and to earn tokens. Hashrate is the total power that a computer has to mine and process transactions on a blockchain[13]. A larger set up of computers allows for a user to calculate quicker. Once the problem is solved, a user earns a cryptocurrency token. Most users earn cryptocurrency through Proof of Work, which requires them to solve complex computational problems with their computer using algorithms[14, 15]. Those with the assets to calculate complex problems are able to earn cryptocurrency faster. Proof of Work is monopolized compared to Proof of Stake. To earn cryptocurrency through Proof of Stake, users must validate that transactions on the blockchain are valid[16]. Once a user validates the transaction, they earn a cryptocurrency token.

Cryptocurrency Transactions

Blockchains are decentralized and distributed digital ledgers used to record transactions across computers. They are used to make transaction records unlikely to be altered[17]. Blockchains are used for data storage, validation, and security. In some rare cases they track exchanges that are updated by a ledger; then information is sent into the blockchain. In terms of cryptocurrency transactions, blockchains ensure that purchases are not altered when entered into the system by using peer-to-peer (P2P) networks[18]. P2P networks are servers in which users write, read, and validate transactions on a blockchain.

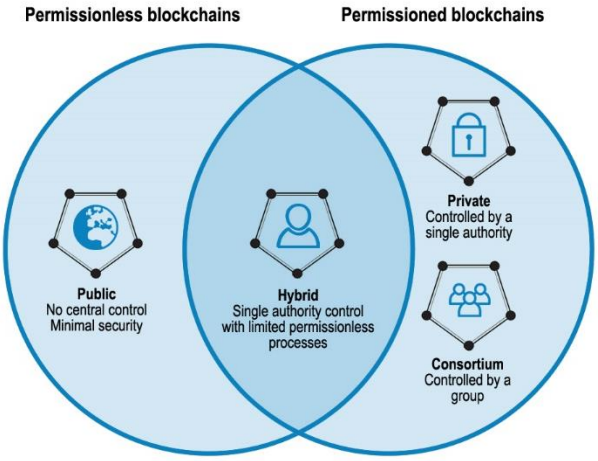


Figure 2: Types of blockchains

There are four types of blockchains. Public blockchains have no central authority. According to their critics, they have minimal security and are nonrestrictive. They point out that anyone with internet access can operate public blockchains as well as access records and crypto mine. Critics further-argue that a major disadvantage to public blockchains is the threat posed by hackers. If hackers take control of 51 percent of a blockchain, that blockchain can be used for malicious reasons[19]. Others, however, claim that public blockchains could be the most secure cryptocurrency networks in existence, because their design specifications are based

on cryptography. They also point out that blockchains are rarely —if ever— hacked, though individual users and exchanges have had their private keys hacked through various attack vectors.

Private blockchains operate in the same style as a public blockchain, but on a smaller scale. Because of their smaller scale, they often operate faster than public blockchains. Private blockchains are restrictive and disallow public access[20]. They do require transactions to be verified by Proof of Work or Proof of Stake. Like public blockchains, a major weakness of this type of blockchain is the threat posed by hackers operating online.

Hybrid blockchains are a combination of public and private blockchains. They are permission-based systems with public access[21]. This means that users must have permission to validate transactions on the blockchain, but the public has access to data in the blockchain. In some cases, confidential information is kept within the network. Hackers are not likely to take the majority of the blockchain because 51 percent of the blockchain is kept private —though it is technically possible for users who control smaller percentages to combine forces in order to share control of the blockchain. A disadvantage of hybrid blockchains is that the majority of the information within these types of block-chains is shielded, thus barring legal access by law enforcement and regulatory agencies. Also, there appears to be no user incentive for validating transactions within the blockchain.

Like hybrid blockchains, consortium blockchains contain private and public blockchain features. In a consortium blockchain, the organization writes the ledger in the blockchain, the users read the ledger on the blockchain, and together the organization and people validate the transaction. These users are selected to access the block-chain, as it is not public.

Wallets operate as access points for blockchains in cryptocurrency transactions. Wallets do not hold cryptocurrency. Wallets store the key that allows access to the blockchain that a user's cryptocurrency is on. The wallet is a string of characters unique to a user (for instance, 19emjx4vqHPn…). There are two types of wallets: hot and cold[22]. Hot wallets are online and to access the wallet a user must provide their key (password) to access the wallet. Cold wallets are physical objects, such as Universal Serial Bus (USB) drivers and hard drives.

In the domain of cryptocurrency, a key refers to a user's identification to access their crypto-currency, as well as their public address — though it must be stressed that a cryptocurrency user's public/private keys are not necessarily identifiers. There are two types of keys, private and public[23]. Private keys are personal passwords to be used in accessing one's cryptocurrency. Once a private key is deleted, it cannot be recovered. Private keys are likely to be a mnemonic phrase, QR code, binary code, or hexadecimal code. Conversely, public keys are the addresses that one uses to send cryptocurrency to a specific user.

CMC YANKEE – Alejandro Olivares

The Illicit Use of Cryptocurrency by Cybercriminal Organizations

Open-source intelligence indicates a strong correlation between the increasing use of crypto-currencies and a rise in illicit activities by cybercriminal actors.

The use of cryptocurrencies by cybercriminal actors occurs in three realms of cybercriminal activity: *ransomware*, which is the use of malware to encrypt data as leverage for payment; *convertible virtual currency (CVC) mixing*, which encompasses techniques used to convert 'dirty' money to 'clean' currency; and *scams*, which refer to the use of various methods to defraud individuals.

Who are the principal threat actors of crypto-currency misuse worldwide?

The following cybercriminal actors were investigated in this study because of their size, typology, operational success, and overall notoriety.

Ransomware. The LockBit ransomware gang is a large criminal organization of Russian speakers that largely contributes to the growing Ransomware as a Service (Raas) trend, in which the criminal group leases the malware to other groups for a profit. The ransomware, currently known as LockBit 3.0, which is an evolved version of an older malware, is used worldwide and continues to be prolific tool[24, 25].

Scattered Spider is a cybercriminal group likely made up of young native English-speakers from the United States or the United Kingdom[26]. The group's tactics, techniques, and procedures (TTPs) largely utilize social engineering to garner information, allowing ease of access into targeted systems[27]. Scattered spider is a newer ransomware group, having been active since May 2022[28].

Convertible Virtual Currency (CVC) Mixing. The cybercriminal actor known as Sinbad, likely a resurgence of Blender.io, is probably Russian-linked[29]. Sinbad has garnered significant recognition in the cybercriminal underworld, which has enabled it to provide its services across different platforms. It has been reported to consistently aid malicious actors, such as the North Korean HIDDEN COBRA operatives[30]. In 2023, Sinbad became the first CVC mixing cybercriminal actor to be sanctioned by the United States Department of Treasury's Office of Foreign Assets Control (OFAC)[31].

Another CVC mixing cybercriminal actor is Tornado Cash, founded by three individuals: Roman Semenov, Alexey Pertsev, and Roman Storm. Semenov and Pertsev are both Russian nationals. Storm, however, is from Auburn, Washington, but was a student at the South Ural State University in Chelybinsk, Russia[32]. The Russian-linked CVC mixer remains the largest Ethereum (ETH) mixer[33], despite the arrests of its two founders and the sanctions implemented by OFAC for aiding HIDDEN COBRA actors[34].

Scams. The majority of scammers involved in cryptocurrency activities operate independently, rather than as parts of organized criminal networks. While there is a chance that individuals may collaborate in smaller groups, the straightforward nature of scam operations suggests that such groups are unlikely to be large or highly notorious. It is more probable that the methods employed by these scammers are widely known due to their simplicity.

How can threat actors be categorized based on their motivations?

We have identified two areas of motivation: financial and ideological. The most common motives are financial, which are defined as reasons related to monetary income. The secondary motives identified are ideological. These motives incorporate actions taken to further the status or beliefs held by the members of a cybercriminal group.

The typology of ransomware targets indicates that cybercriminals are looking to receive a high payout from the attacks. Moreover, the commonality of the attacks suggests strong financial motives. It is important to note that Scattered Spider has diversified its *modus operandi*, from techniques such as Subscriber Identity Module (SIM) swapping to ransomware attacks on larger corporations, likely indicating a stronger monetary-oriented strategy[35].

LockBit's actions suggest moderate levels of ideological reasoning. It is likely LockBit wishes to be viewed as the best-known and best-performing ransomware group/RaaS provider. In the past, the group has hosted essay-writing competitions, conducted information campaigns on other ransomware groups, and challenged people to get a tattoo of the LockBit logo for a prize[36].

CVC mixing cybercrime actors primarily aim to aid in the laundering of cryptocurrency, earning a commission for cleansing funds derived from illegal activities. Nevertheless, these services might also collaborate with malicious groups based on a shared alignment with the values or goals upheld by such groups.

Scammers are primarily, if not solely, motivated by financial reasons. The quick payouts of some scams make the operations desirable. However, it is possible for actors to have ideological motives, depending on the scammers' outlook of the targets or victims.

What is the typology of their targets/victims in the digital domain?

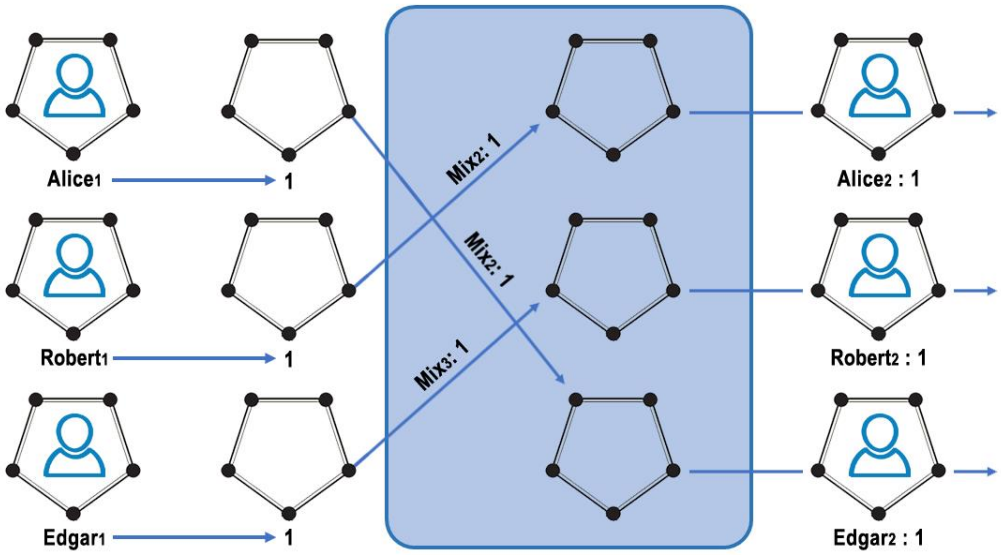
Ransomware attacks are more likely to target medium to large corporations that employ hundreds to thousands of personnel[37]. Larger companies tend to have more income and carry out more operations online, thus making them more willing to pay the ransom fee. Ransomware groups use locked information as leverage. Therefore, ransomware groups are highly likely to target industries that rely on processing larger amounts of information. Sectors such as healthcare, financial services, information technology, government, and education[38] are among the top industries targeted by ransomware groups[39]. In 2021, the number of attacks in Western countries increased by 234 percent in Europe and 180 percent in North America over the previous year[40].

As online service providers (OSPs), CVC mixing actors are unlikely to directly target individuals as victims. Rather, their interaction with victims is more likely focused on facilitating the laundering of cryptocurrency that has been acquired by another illicit actor.

Scams are more likely to target those who are believed to be naïve and gullible. Scammers will cast a wide net to attract as many victims as possible, or they will directly target individuals that they believe would fall for scams, such as children or the elderly. The typology of the victims greatly coincides with the tactic of the scam[41].

device, the software may be automatically downloaded, or it may contain a file that, once clicked on, will execute the malware[42].

The second method, which is by far the most prominent, is performed through soft infiltration. Soft infiltration can occur through multiple means, such as phishing emails containing malicious attachments or links to conduct a drive-by download[43], embedded advertisements, or infected websites[44]. Once the targeted system is infected, the illicit actor can withhold the information as ransom until a payment is made, most likely using cryptocurrencies.



[130]

Figure 3: CVC mixer using tumbler software

What methods are used by illicit actors?

We have identified two overarching methods used by ransomware groups to infect systems with malware. The first method is through the use of hard infiltration. This technique uses cold devices, such as USB drivers containing a variety of malicious software. Once connected to a

CVC mixers are designed to obscure the sources, destinations, and amounts of cryptocurrency exchanges. The OSPs are most likely to use tumbling software. Tumblers work by mixing input transactions with a larger pile and then sending funds of the same value to a wallet of choice, or by random, minus the commission fee[45].

Other common methods, such as unregulated exchanges, gaming sites, and cryptocurrency ATMs, involve the use exploiting loopholes to obscure funds[46].

Since scams use high levels of social engineering and rely on the adaptability of techniques, they remain extremely versatile. Nonetheless, methods using cryptocurrencies are designed to fool the target into sending money to the scammer. The term investment scam is an umbrella term used to indicate multiple methods of operation. Investment scams promote a chance for targets to invest money for a large turn of profits. For instance, rug-pulling is a method where the scammer will promote a new opportunity, but the program's coding will not allow for withdrawal of funds from investors, leaving it to the scammer to withdraw funds. Another method is the social media giveaway. This technique has the scammer pose as a celebrity offering to give away cryptocurrency. Once the target is convinced that the offer is genuine, the victim will be forced to send a payment to 'verify' their wallet. The scammer will then steal the money. Other investment schemes can involve fake exchange sites, Ponzi schemes, or false employment offers. Another notable method used is romance scams. This social engineering-reliant tactic attempts to build a personal relationship with target to build trust. Once the relationship is established, the scammer will attempt to receive money from the target[47].

What is their degree of success?

Precise data about the degree of success of these methods are difficult to determine. Successful attacks are often reported, whereas failures are less likely to be known. To provide some context, in 2021, the FBI's Internet Crime Complaint Center (IC3) received 3,729 ransom-ware-related complaints in the United States[48], though were there an estimated 623 million attacks in the same year.[49]. A 2021 survey of thousands of companies worldwide found that 54 percent of ransom-ware attacks were successful[50]. In addition, ransomware profits are projected to increase from $20 billion in 2021 to $265 billion in 2031[51]. In 2021, a report from Chainalysis stated that $8.6 billion in cryptocurrency was laundered using CVC laundering techniques, which was a 30 percent increase from 2020[52]. From 2021 to the first quarter of 2022, the Federal Trade Commission reported that approximately 46,000 people had lost money to crypto-currency schemes totaling over $1 billion, with a median of approximately $2,600 in losses[53].

What are the emerging actors or methods of illicit cryptocurrency use?

Although ransomware attacks on operating systems like Windows are routine, ransomware attacks on smartphones are becoming more regular. Misconceptions that mobile phones are not likely to be infected can prevent targets from taking precautions[54]. RaaS makes it easier for a wider range of criminal groups to utilize ransomware attacks, since they no longer need to develop their own malware. Both the users and the providers of malware earn money from the attack. It is therefore likely that activities from other criminal groups or individuals using RaaS will increase[55]. Due to the adaptability of scams, it is highly likely that scammers using crypto-currencies will increase, as new methods and typologies of targets are developed.

Pig-butchering is one technique that is increasingly being used by cryptocurrency scammers. This method involves a mixture of investment scams and romance scams. In practice, the scammers will attempt to build a rapport with targets to establish a sense of trust. The scammer will then offer the target a chance to invest in a cryptocurrency. Once the target invests, the scammer will steal the money[56].

It is important to note that trends of crypto-currency scams are starting to shift to include younger people as victims because they are seen as naïve by criminal actors[57].

CMC WHISKEY – Hannah Albert

The Use of Cryptocurrency by Criminal Actors in Latin America

Latin American criminal actors are highly sophisticated, operate internationally, and are well funded. These actors have cryptocurrency-facilitated contacts with China-based chemical companies, brokerages, and other international organizations overseas.

Who are the principal threat actors of cryptocurrency misuse in Latin America?

China-based chemical companies. China-based chemical companies like Wuhan Shuokang Biological Technology (WSBT) and Suzhou Xiaoli Pharmatech (SXPC) use cryptocurrency to sell opioid precursors to Latin American cartels[58]. China-based chemical companies have received $3.6 million from Latin American cartels and $6.2 million from European actors, all in recorded cryptocurrency transactions[59]. These companies also launder money through crypto-currency[60].

Brokerages. The Los Zheng Cartel connects Chinese chemical companies with Mexican cartels. They use Global United Biotechnology Incorporated as a front for their main operations in Shanghai. In 2020, the United States Department of Treasury sanctioned four individuals in the company for their roles in managing the drug trade and using Bitcoin to launder drug proceeds. In China, about 2,000 Chinese nationals manage cryptocurrency transactions and the production and distribution of opioids. The Los Zheng Cartel uses crypto-currencies such as Bitcoin, Ethereum, and Monero to keep their operations and transactions off the radar[61].

The Traders Domain brokerage in the Caribbean was shut down in 2022. It managed a Ponzi scheme worth $500 million in cryptocurrency and had about $3.3 billion in liabilities[62, 63, 64], over 6 percent of all stolen cryptocurrencies were taken by Ponzi schemes in 2022. Crypto influencers Alex Santi and Ted Safranco are affiliated with the Traders Domain brokerage and Trubluefx, possibly the rebranded Traders Domain brokerage[65, 66, 67, 68].

Cartels. Mexican cartels launder approximately $25 billion annually through Bitcoin, which equals to about 2 percent of Mexico's GDP[69, 70]. The Sinaloa Cartel (CDS) uses Bitcoin and likely Ethereum and Monero for its transactions. In 2023, OFAC sanctioned a $740,000 Ethereum wallet linked to CDS[71]. CDS operates in 21 Mexican states and 50 countries in Latin America, Europe, Asia, and Africa. In 2023, it made unprecedented profits, as cocaine prices doubled in the U.S. and Europe[72]. The Jalisco Cartel (CJNG), like CDS, uses Bitcoin and likely Ethereum and Monero for most of its transactions. CJNG operates in at least 27 Mexican states, excluding Sinaloa, as the two cartels are rivals[73, 74]. Most transactions made by cartels are either facilitated through crypto-currency, or with cash, which gets 'cleaned' with the use of crypto-currency; transactions

are also made on the Darknet, which helps maintain user anonymity[75].

The Primeiro Comando da Capital, or PCC, is a Brazilian cartel with a Paraguayan presence. It makes up to $7.8 million in transactions per year, about 231 Bitcoin out of a total of 19 million Bitcoin mined[76, 77, 78]. Clan del Golfo, a Colombian Cartel works on the Colombia-Panama border. It is allied with the 'Ndrangheta mafia in Calabria, Italy[79]. Comando Vermelho is another Brazilian cartel working in drug trafficking. On Ethereum, the CVRL token is the Comando Vermelho token, yet information on the CVRL website claims there is no affiliation to the cartel[80].

Mara Salvatrucha-13, or MS-13, operates in El Salvador and Honduras, as well as in the U.S. It uses Bitcoin, a legal currency in El Salvador [81]. MS-13 made a deal with the Bukele administration in El Salvador which allegedly ended in March 2023. It includes a reduction in homicides committed by MS-13 in exchange for political support, government protection of certain imprisoned leaders of MS-13, and payments made by the Bukele administration to MS-13[82].

How can threat actors be categorized based on their motivations?

Actors are primarily financially motivated. China-based chemical companies make active changes to their operations regarding supply and demand[83]. Brokers often get paid commissions from the deals they broker[84], and each cartel wants to have or maintain regional power. However, there is also ego and ideology at play. Cartels are unique because their leadership is distinguished by blood ties. The businesses get passed on through generations and the leaders yearn to keep their families' reputations. Most cartels have rivalries, like the CDS and CJNG, which also motivate the organizations[85, 86].

What is the typology of their targets/victims in the digital domain?

The Traders Domain brokerage targets individuals. The Traders Domain brokerage ran a Ponzi scheme that required new victims to invest so that existing victims could be paid in small amounts. Eventually, every customer would have withdrawal issues as their money was being stolen by the Traders Domain brokerage or Trublufx, the suspected rebranding[87].

What methods are they using to launder funds through cryptocurrencies?

Smurfing Technique. The smurfing technique is a method used to avoid detection. Cash is transferred into cryptocurrency, and the crypto-currency is sent to the recipient in small intervals, sometimes with different cryptocurrencies[88, 89].

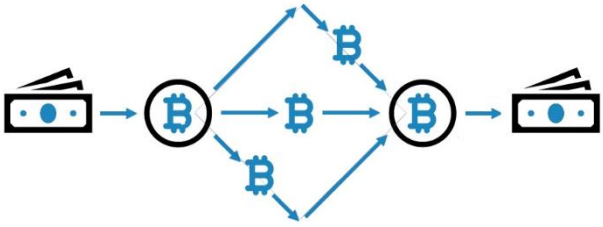


Figure 4: Smurfing technique

Mirror Transactions. Mirror transactions occur when cash earned through illegal business is made 'clean'. The cash is turned into crypto-currency and sent to a bank overseas where someone in that foreign country takes the

cryptocurrency out as cash in that foreign currency. The foreign currency is then sent back to the original party, often with a commission taken from it for the broker who helped make the transaction[90].

Hawala Technique. *Hawala* is Arabic for "trust" or "transfer". The method originates in the Middle East and is commonly used in the Middle East, Africa, and India[91]. The first party has intentions of providing money to a recipient overseas. That first party goes to a brokerage that has known contacts in both countries. The first party gives cash and a 'password' to their local contact. That first contact transfers the cash into cryptocurrency to send to the second contact, along with the 'password'. The second contract transfers the cryptocurrency into a foreign currency and takes the brokerage's commission. The recipient provides the second contact for the brokerage with the 'password' and, when it is verified, the second contact provides the recipient with the cash[92].

What is their degree of success?

High Degree of Success. The U.S. Drug Enforcement Administration (DEA) identified China as the top fentanyl precursor producer in 2019. In 2021, China was the world leader in chemical exports, with transactions of about $100 billion. In 2023, OFAC charged WSBT and SXPT for selling fentanyl precursor drugs. The OFAC also identified Chinese nationals who were involved in opioid production and distribution and for laundering money with Bitcoin[93]. These companies have faced few —if any— consequences for using crypto-currency to facilitate their operations.

The CDS makes up about 40-60 percent of all Mexican drug trade. In 2012, the CDS profited by around $3 billion[94]. The U.S. has placed sanctions on both the CDS and CJNG[95]. The DEA believes that CJNG leader 'El Mencho' (Nemesio Rubén Oseguera Cervantes, the most wanted person Mexico) is worth as much as $1 billion[96]. The U.S. has sanctioned nine members of the CDS for their roles in using cryptocurrencies to illegally launder money[97]. The PCC rakes several millions of dollars each month in profits and the Clan del Golfo is worth billions of dollars[98].

Low Degree of Success. In 2018, the U.S. indicted two leaders of the Los Zheng Cartel on 43 counts of manufacturing and shipping around 250 drugs including fentanyl precursors and distributing those drugs to 37 states and 25 countries[99]. The Traders Domain brokerage closed in 2022 and had a Red Warning released from the U.S. Commodity Futures Trading Commission[100].

What are the emerging locations of illicit crypto-currency use in Latin America?

We estimate with moderate confidence that Trinidad and Tobago is a significant emerging hotspot of illicit cryptocurrency use. The cost of energy in Trinidad and Tobago is low ($0.04 per Kilowatt-hour) compared to its region's average cost of energy ($0.33 kWh) and the U.S. average ($0.23 kWh). The Trinimine project for mining Bitcoin in Trinidad and Tobago is underway and about $500 million has already been invested in the project [101]. This is likely to attract cybercriminal actors in the coming years.

CMC SIERRA – Brandon Macallair

The Use of Cryptocurrency by State-Backed Criminal Organizations

In examining how state-backed criminal organizations utilize cryptocurrency to enable and support their illicit activities, we based our research and analysis on the *2023 Annual Threat Assessment of the United States Intelligence Community*. The document identifies China, Russia, Iran, and North Korea as strategic competitors, or as local or regional powers that are "seeking to exert their influence, often at the cost of neighbors and the world order itself"[102].

Who are the principal state-backed threat actors of cryptocurrency misuse?

We have selected two state-backed threat actors from each nation of interest as examples of that nation's cryptocurrency misuse.

China	Barium (APT41)*	Triads
Russia	Wagner Group	Evil Corp*
Iran	IRGC-QF	Phosphorus (APT42)*
North Korea	Lazarus Group (APT38)*	Thallium (APT43)*

Table 1: State-backed cybercriminal actors

The two primary illegal activities involving cryptocurrency are the illegal acquisition of cryptocurrency and the use of cryptocurrency to fund physical criminal activities. The above groups that are marked with an asterisk (*) are involved in the illegal acquisition of crypto-currency. The others use cryptocurrency to fund physical criminal activities.

Some of the threat actors that we analyzed are designated as Advanced Persistent Threat (APT) groups. According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA), an APT is "a well-resourced adversary engaged in sophisticated malicious cyber activity"[103] We will refer to groups with APT designations by their APT number.

Cybercriminal organizations primarily use ransomware, crypto-jacking, and theft to illegally acquire cryptocurrency. Ransomware is a cyberattack that encrypts a victim's files and demands a ransom payment in crypto-currency to regain access[105]. Crypto-jacking refers to attacks whose perpetrators use the victim's computing power to mine crypto-currency[104]. Cryptocurrency theft is the direct theft of cryptocurrency from a victim's digital wallet[106].

Ransomware is the most common type of cyberattack used by state-backed organizations because it offers them the ability to target large numbers of victims. In 2017, the North Korean-backed group APT38 compromised in excess of 250,000 computers internationally and demanded a ransom of $300-$600 in bitcoin from each victim[104]. Theft of cryptocurrency is the primary method used by North Korean cybercriminal groups, due to the high potential for profit. From June to September 2023, APT38 was responsible for the theft of almost $240 million in cryptocurrency from four

cryptocurrency brokerages[107]. This figure represents a significant increase in profit and change in target selection since the group's 2016 cyberheist of $81 million in cash from the Bangladesh Bank[108]. Crypto-jacking is the least profitable method. The attacker makes $1 for every $53 that their victim is billed for the computing costs of mining cryptocurrency[109]. Crypto-jacking is often a secondary objective, alongside national security interests. Between June and July 2022, the Iranian group APT42 conducted a crypto-jacking attack on a Federal Civilian Executive Branch (FCEB) agency of the United States[110].

Illegal Acquisition		Ransomware	Crypto-jacking	Crypto-theft
APT41	China	✓	✓	
Evil Corp	Russia	✓		
APT42	Iran	✓	✓	
APT38	North Korea	✓		✓
APT43	North Korea			✓

Table 2: Illegal cryptocurrency acquisition by state-backed cybercriminal actors

How can threat actors be categorized based on their motivations?

The eight groups we analyzed are motivated by financial gain, national security interests, ideology, or by a combination of those. Of the groups we examined, 75 percent are at least partially motivated by financial gain. This is likely due to crypto-currency's use as a medium of exchange. Financially motivated uses of cryptocurrency focus on funding operations carried out by the cybercriminal actor, or by the nation state that sponsors it[111], as well as sustaining the money-driven lifestyles of the cybercriminal actors' members[112].

National security interests are another common motivation of state-backed criminal organizations. Some of these efforts are funded by crypto-currency. For example, APT43 assists North Korea's nuclear weapons program by collecting intelligence on international negotiations and the foreign policies of other nations[113]

One of the eight threat actors we examined is motivated primarily by ideology: the Iran-backed Islamic Revolutionary Guard Corps – Qods Force (IRGC-QF). The IRGC-QF, a designated Foreign Terrorist Organization (FTO) [114], uses cryptocurrency to fund its operations and its partners in what Iran refers to as the "Axis of Resistance". The Axis of Resistance refers to an Iran-led geopolitical and ideological alliance that includes several countries and non-state actors that share common political goals and opposition to what they perceive as external threats, particularly from Western powers and Israel[115].

What is the typology of their targets/victims in the digital domain?

Individuals, companies, and governments are the primary targets of state-backed cybercriminal organizations. Regardless of its motivations, every APT group we analyzed has targeted all three. The Chinese group APT41 has targeted pro-democracy politicians and activists in Hong Kong[116], undisclosed companies in industries of interest to China, such as computer manufacturing[116], and U.S. Government networks[117]. An exception to this rule is Evil Corp, which has exclusively targeted private

companies[118]. This is likely due to the group's comparative lack of sophistication.

The state-backed cybercriminal actors that fund physical crimes with cryptocurrency have physical victims. The Chinese Triads are violent criminal organizations with connections that include Chinese government officials[119] and have used cryptocurrency in their activities. In 2021, a Triad gang kidnapped and assaulted a cryptocurrency trader in order to steal the passwords to his cryptocurrency accounts[120]. The Wagner Group is a private military company that conducts military operations around the world[121]. The IRGC-QF target Iranian dissidents, Western interests, and Israel [122]. They also fund other FTOs, such as Hezbollah, Hamas, Palestinian Islamic Jihad (PIJ), and the Iraqi Popular Mobilization Forces (PMF)[115].

What methods are they using to launder funds through cryptocurrencies?

The eight groups that we analyzed all launder their cryptocurrency through cryptocurrency exchanges, direct income, video games, or casinos. APT38 has used the virtual currency mixer Tornado Cash to transfer its illicit funds through several cryptocurrencies to mask the origin of the funds[123]. The Wagner Group and the IRGC-QF use "direct income", which refers to limited, if any, laundering and typically involves the direct conversion of cryptocurrency into a *fiat* currency[124].

APT41 and the Triads have both used unique money-laundering methods. APT41 has used video games[117], which involves purchasing in-game items with cryptocurrency and then selling them for clean money[125]. The Triads have used casinos that accept cryptocurrency transactions to mask the origin of illicit cryptocurrency[126].

Laundering Methods		Crypto Exchange	Direct Income	Video Games	Casinos
APT41	China			✓	
Triads	China				✓
Wagner Group	Russia		✓		
Evil Corp	Russia	✓			
IRGC-QF	Iran		✓		
APT42	Iran	✓			
APT38	North Korea	✓			
APT43	North Korea	✓			

Table 3: Cryptocurrency laundering methods by state-backed cybercriminal actors

What is their degree of success?

We designated these groups as high, moderate, or low success, based on the success and significance of their cryptocurrency use. The five groups with APT designations were considered as high success actors, due to their APT designation, responsibility for the most lucrative attacks, as well as their continued operations regardless of legal action by the U.S.[123].

Wagner Group, Evil Corp, and the IRGC-QF were designated as having had moderate success due to their lack of APT designations and less frequent use of cryptocurrency. Wagner Group received $2.2 million in cryptocurrency donations from February to July 2022[127]. For comparison, it may be noted that, from May 2022 to May 2023, the Wagner Group received $919 million from the Russian defense budget[128]. Even though the timelines do not align perfectly, its cryptocurrency income is approximately 0.2 percent of its cash income from the Russian state.

In 2021, Iran was providing weapons systems and support to Hamas[129]. Also in 2021, Israel seized $7.7 million in cryptocurrency from accounts linked to Hamas[130]. While this is a tactical failure of the IRGC-QF's cryptocurrency funding system, it is likely that other successful funding to groups like Hamas have occurred.

The Triads have been designated as low success due to the limited examples of cryptocurrency use by their members. Additionally, seven members of the Sun Yee On triad were arrested within three days of the kidnapping of the cryptocurrency trader[128] mentioned earlier.

What are the emerging threat actors and/or methods of illicit cryptocurrency use?

We have identified Ocean Lotus (APT32), the Izz ad-Din al-Qassam Brigades (IQB), and a variety of Lebanese organizations as emerging threat actors of potential illicit cryptocurrency use. They are not listed in order of importance or sophistication. APT32 is a Vietnam state-backed cybercriminal organization that is primarily motivated by national security interests[131]. In 2020, they were detected deploying crypto-jacking malware alongside their intelligence collection operations[132]. The IQB is the military wing of Hamas. In 2019, Hamas invited crypto-currency donations via their social media accounts. In 2021, Israel seized several cryptocurrency wallets belonging to the IQB, which contained an undisclosed amount of bitcoin[133]. The economy of Lebanon has been declining rapidly since 2020, when the nation's banks began to prevent withdrawals. Bitcoin has been gaining popularity as an alternative to the Lebanese pound[134]. Due to the weak economy and declining government, Lebanon may be a location of emerging cryptocurrency threats.

POLICY OPTIONS

Below are five policy options for possible implementation at the operational level. These options have been provided in ascending order of implementation complexity, ranging from the least to the most challenging.

☑ Intensify international efforts to identify and locate the individual actors behind illicit cryptocurrency use. As seen in the ChipMixer case, illicit cryptocurrency use can be stopped by apprehending the individuals that are operating the servers. Cybercriminal organizations are often international, and the investigations involve cooperation with local law enforcement. A potential risk is that, as more foreign agencies are involved in the investigation, there is a possibility that the suspects may be alerted and may evade apprehension.

☑ Implement legislation that requires cryptocurrency trading platforms to record users who make a suspiciously high number of transactions. A high number of small transactions may indicate a larger illicit cryptocurrency operation. A potential risk is that, by preventing this method of illegal cryptocurrency transactions, criminal organizations may devise alternative methods.

☑ Acquire the ransomware sold by organizations providing RaaS to identify coding vulnerabilities. Organizations such as Lockbit create ransomware and sell it to other groups. By obtaining the ransomware, likely through an undercover operation or by turning a previous customer into an informant, the U.S. Government could reverse-engineer the ransomware to identify its vulnerabilities. A potential risk is that, if cybercriminal groups become aware of these operations, they may create new versions of ransomware.

☑ Similarly to Operation Trojan Shield, construct a simulated brokerage that criminals would resort to in order to convert illegal cryptocurrency to *fiat* currency. Strategically permit nominal illegal transactions while logging them as evidence. When a transaction is significant enough to warrant intervention, the agency involved would block the transaction and seize the assets. Once the operation is completed, the agency involved could use the evidence collected on the smaller transactions to pursue legal action. A potential risk is that the transactions that are permitted will likely fund criminal activities.

☑ Create software to surveil transactions made through cryptocurrency mixers that support criminal organizations. A covert operation to implement software to collect evidence of illegal transactions may assist in building cases of illegal cryptocurrency use. Potential risks are exposure of the covert action and adversaries acquiring the software.

REFERENCES

[1] Patel, Dee. "A Beginner's Guide to Cryptocurrency." Penn Today, January 26, 2022. https://penntoday.upenn.edu/news/beginners-guide-cryptocurrency.

[2] "Research Guides: Fintech: Financial Technology Research Guide: Cryptocurrency & Blockchain Technology." Cryptocurrency & Blockchain Technology - Fintech: Financial Technology Research Guide - Research Guides at Library of Congress. Accessed November 6, 2023. https://guides.loc.gov/fintech/21st-century/cryptocurrency-blockchain.

[3] Federal Bureau of Investigation. (n.d.). *Internet crime complaint center (IC3): Scammers target and exploit owners of cryptocurrencies in Liquidity Mining Scam*. Internet Crime Complaint Center (IC3) | Scammers Target and Exploit Owners of Cryptocurrencies in Liquidity Mining Scam. https://www.ic3.gov/Media/Y2022/PSA220721

[4] Pazzanese, Christina. "Regulating the Unregulated Cryptocurrency Market." Harvard Gazette, September 30, 2021. https://news.harvard.edu/gazette/story/2021/09/regulating-the-unregulated-cryptocurrency-market/.

[5] Nelson, Alondra. "Fact Sheet: Climate and Energy Implications of Crypto-Assets in the United States." The White House, September 8, 2022. https://www.whitehouse.gov/ostp/news-updates/2022/09/08/fact-sheet-climate-and-energy-implications-of-crypto-assets-in-the-united-states/.

[6] "Securities and Exchange Commission November 2, 2023 and Rule - Sec.Gov." Release No. 34-9856. Self-Regulatory Organizations. Accessed November 6, 2023. https://www.sec.gov/files/rules/sro/cboebzx/2023/34-98846.pdf.

[7] Alonso, Kurt M. "Monero - Privacy in the Blockchain." Universitat de Barcelona. Accessed November 6, 2023. https://openaccess.uoc.edu/bitstream/10609/75205/6/alonsokTFM0118memoria.pdf.

[8] "Digital Currencies: Reserve Bank of Australia" Reserve Bank of Australia, May 4, 2023. https://www.rba.gov.au/education/resources/explainers/cryptocurrencies.html.

[9] "Bitcoin USD (BTC-USD) Price, Value, News & History." Yahoo! Finance, November 6, 2023. https://finance.yahoo.com/quote/BTC-USD/.

[10] "Bitcoin Eth (BTC-Eth) Price, Value, News & History." Yahoo! Finance, November 6, 2023. https://finance.yahoo.com/quote/BTC-ETH/.

[11] Front page | U.S. Department of the Treasury. Accessed November 6, 2023. https://home.treasury.gov/system/files/136/CryptoAsset_EO5.pdf.

[12] Wang, Luqin, and Yong Liu. "Exploring Miner Evolution in Bitcoin Network - New York University." New York University Polytechnic School of Engineering. Accessed November 6, 2023. https://eeweb.engineering.nyu.edu/faculty/yongliu/docs/BitCoin_TR.pdf.

[13] "Buying and Selling Crypto: What's Hashrate?" Robinhood. Accessed November 6, 2023. https://robinhood.com/us/en/support/articles/cryptocurrency-hashrate/.

[14] "Proof-of-Work, and Its Flaws, Explained." Hedera. Accessed November 6, 2023. https://hedera.com/learning/consensus-algorithms/proof-of-work-and-its-flaws-explained.

[15] Porat, Amitai. "Blockchain Consensus: An Analysis of Proof-of ... - Stanford University." Stanford University. Accessed November 7, 2023. https://www.scs.stanford.edu/17au-cs244b/labs/projects/porat_pratap_shah_adkar.pdf.

[16] Yao, David D. "Trading under the Proof-of-stake Protocol - Columbia University." Columbia University, May 9, 2023. http://www.columbia.edu/~wt2319/ExchPOS.pdf.

[17] "How Does Blockchain Work? | Stanford Online." StandfordOnline. Accessed November 6, 2023. https://online.stanford.edu/how-does-blockchain-work.

[18] Viswanath, Pramod. "Peer to Peer Networking for Blockchains." University of Illinois, February 4, 2021. https://courses.grainger.illinois.edu/ece598pv/sp2021/lectureslides2021/ECE_598_PV_course_notes4.pdf.

[19] Bansod, Smita, and Lata Ragha. "Challenges in Making Blockchain Privacy Compliant for the Digital World." Sādhanā, 2022. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9387419/.

[20] "3 Considerations to Help Businesses with Cryptocurrency." Fisher Phillips, March 1, 2022. https://www.fisherphillips.com/en/news-insights/public-vs-private-3-considerations-help-businesses.html#:~:text=A%20private%20blockchain %20is%20run,not%20open%20for%20public%20participation.

[21] Hu, Jiejun, Martin J Reed, Mays Al-Naday, and Nikolaos Thomos. "Hybrid Blockchain for IoT." Sensors (Basel, Switzerland), January 5, 2021. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7796099/.

[22] "Cryptocurrency and Cybersecurity: How to Store Your Crypto Safely." EC- Council University, October 19, 2023. https://www.eccu.edu/blog/cybersecurity/cryptocurrency-cybersecurity-how-to-store-your-crypto-safely/.

[23] Reiners, Lee, and Anna January 19. "The Custody of Cryptocurrencies: OCC Opens the Door for Banks to Take Part in the Fintech World." The FinReg Blog, January 19, 2021. https://sites.duke.edu/thefinregblog/2021/01/19/the-custody-of-cryptocurrencies-occ-opens-the-door-for-banks-to-take-part-in-the-fintech-world/.
[24] "Understanding Ransomware Threat Actors: LockBit | CISA." 2023. Cybersecurity and Infrastructure Security Agency CISA. June 14, 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a.
[25] ReliaQuest. 2021. "Ransomware Q3 Roll up - ReliaQuest." ReliaQuest (blog). October 25, 2021. https://www.reliaquest.com/blog/ransomware-q3-2021-roll-up/.
[26] Vicens, Aj. 2023. "Groups Linked to Las Vegas Cyber Attacks Are Prolific Criminal Hacking Gangs." CyberScoop, September 16, 2023. https://cyberscoop.com/las-vegas-mgm-caesars-cyber-attack/.
[27] "Why Are You Texting Me? UNC3944 Leverages SMS Phishing Campaigns for SIM Swapping, Ransomware, Extortion, and Notoriety" 2023. Mandiant Intelligence (blog). September 14, 2023. https://www.mandiant.com/resources/ blog/unc3944-sms-phishing-sim-swapping-ransomware.
[28] "Scattered Spider: The Modus Operandi." 2023. Trellix.Com. August 17, 2023. https://www.trellix.com/about/newsroom/stories/ research/scattered-spider-the-modus-operandi/.
[29] Arghire, Ionut. 2023. "'Scattered Spider' Cybercrime Group Targets Mobile Carriers via Telecom, BPO Firms." SecurityWeek. January 22, 2023. https://www.securityweek.com/scattered-spider-cybercrime-group-targets-mobile-carriers-telecom-bpo-firms/.
[30] "Has a Sanctioned Bitcoin Mixer Been Resurrected to Aid North Korea's Lazarus Group? | Elliptic." 2023. Elliptic Connect. February 13, 2023. https://hub.elliptic.co/analysis/has-a-sanctioned-bitcoin-mixer-been-resurrected-to-aid-north-korea-s-lazarus-group/.
[31] "U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats." 2022. U.S. Department of The Treasury. May 6, 2022. https://home.treasury.gov/news/press-releases/jy0768.
[32] Department of Treasury. 2023. "Federal Register, Volume 88 Issue 203 (Monday, October 23, 2023)." October 23, 2023. https://www.govinfo.gov/content/pkg/FR-2023-10-23/html/2023-23449.htm.
[33] Storm, Roman. 2018a. "Roman Storm." LinkedIn. September 1, 2018. https://www.linkedin.com/in/romanstorm.
[34] Osorio, Nica. 2023. "Tornado Cash Remains The Largest Crypto Mixer On Ethereum Despite 85% Drop In Trading Volume." International Business Times, October 12, 2023. https://www.ibtimes.com/tornado-cash-remains-largest-crypto-mixer-ethereum-despite-85-drop-trading-volume-3714984.
[35] Associated Press. 2023. "Founders of Crypto Mixer Arrested, Sanctioned after US Cracks down on Tornado Cash." US News & World Report, August 23, 2023. https://www.usnews.com/news/business/articles/2023-08-23/founders-of-crypto-mixer-arrested-sanctioned-after-us-cracks-down-on-tornado-cash.
[36] Hoffman, Chad. 2023. "Ransomware Diaries: Volume 1 | Analyst1." Analyst1. September 1, 2023. https://analyst1.com/ransomware-diaries-volume-1/.
[37] Kochovski, Aleksandar. 2023. "Ransomware Statistics, Trends and Facts for 2022 and Beyond." Cloudwards. April 24, 2023. https://www.cloudwards.net/ransomware-statistics/.
[38] Robb, Brenda. 2023. "The State of Ransomware in 2021 | BlackFog." BlackFog (blog). July 3, 2023. https://www.blackfog.com/the-state-of-ransomware-in-2021/.
[39] "Mid-Year Update: 2021 SonicWall Cyber Threat Report." 2021. SonicWall. 2021. https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2021-cyber-threat-report.pdf.
[40] "Who Experiences Scams? A Story for All Ages." 2022. Federal Trade Commission. December 8, 2022. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/12/who-experiences-scams-story-all-ages.
[41] Boyd, Christopher. 2022. "Attackers Are Mailing USB Sticks to Drop Ransomware on Victims' Computers." Malwarebytes. January 10, 2022. https://www.malwarebytes.com/blog/news/2022/01/attackers-are-mailing-usb-sticks-to-drop-ransomware-on-victims-computers.
[42] "How Does a Computer Become Infected with Ransomware?" n.d. https://security.berkeley.edu/faq/ransomware/how-does-computer-become-infected-ransomware.
[43] "Ransomware." n.d. FBI. https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware.
[44] "What Is a Cryptocurrency Mixer and How Does It Work?" 2022. March 27, 2022. https://cryptonews.net/news/security/4260735/.
[45] Guerra, Gustavo Rabay, and Henrique Marcos. 2019. "Legal Remarks on the Overarching Complexities of Crypto Anti-Money Laundering Regulation." Revista Jurídica 4 (57): 83. https://doi.org/10.21902/revistajur.2316-753x.v4i57.3757.
[46] "Bitcoin Money Laundering: How Criminals Use Crypto." 2019. Elleptic. September 18, 2019. https://www.elliptic.co/ blog/bitcoin-money-laundering.

[47] Hetler, Amanda. 2023. "10 Common Cryptocurrency Scams in 2023." WhatIs.Com. June 22, 2023. https://www.techtarget.com/whatis/feature/Common-cryptocurrency-scams.
[48] "Federal Bureau of Intesitgation Internet Crime Report 2021." n.d. IC3.Gov. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.
[49] "Number of Ransomware Attempts per Year 2022 | Statista." 2023. Statista. August 31, 2023. https://www.statista.com/ statistics/494947/ransomware-attempts-per-year-worldwide/.
[50] "The State of Ransomware 2021." 2021. Sophos. April 2021. https://assets.sophos.com/X24WTUEQ/at/k4qjqs73jk9256hffhqsmf/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469.
[51] Freeze, Di. 2023. "Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031." Cybercrime Magazine. July 10, 2023. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.
[52] McCarthy, Adam Morgan. 2022. "Cybercrooks Laundered $8.6 Billion Worth of Dirty Crypto Last Year as Laundering Surged 30%, Chainalysis Says." Markets Insider, January 26, 2022. https://markets.business insider.com/news/currencies/crypto-crime-blockchain-money-laundering-bitcoin-ethereum-defi-chainalysis-2022-1?op=1.
[53] "Reports Show Scammers Cashing in on Crypto Craze." 2022. Federal Trade Commission. August 11, 2022. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze.
[54] Chebac, Andreea. 2022. "Mobile Ransomware: The next Step for Cybercriminals." Heimdal Security Blog. November 17, 2022. https://heimdalsecurity.com/blog/mobile-ransomware-the-next-step-for-cybercriminals/.
[55] Unit 42. n.d. "Ransomware Threat Report 2022." Directed by Ryan Olson. Paloalto Networks. https:// www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2022-unit42-ransomware-threat-report-final.pdf.
[56] Szabó, Márk. 2023. "Pig Butchering Scams: The Anatomy of a Fast-Growing Threat." March 29, 2023. https://www.welivesecurity.com/2023/03/29/pig-butchering-scams-anatomy-fast-growing-threat/.
[57] Handley, Erin, Hellena Souisa, Iris Zhao, and Angelique Lu. 2022. "Inside the 'pig-Butchering' Scams Seeing Thousands Trafficked into Cyber Slavery." ABC News, September 15, 2022. https://www.abc.net.au/news/2022-09-16/cambodia-human-trafficking-online-scam-pig-butchering/101407862.
[58] Team, Chainalysis. "Opioid Crisis and Crypto: Blockchain Analysis on Fentanyl Sales." Chainalysis, September 19, 2023. https://www.chainalysis.com/blog/cryptocurrency-fentanyl-analysis-2023/.
[59] Moloney, Anastasia, and Diana Baptista. "How Crypto Helps Latin America's Drug Cartels Do Business." Context, September 4, 2023. https://www.context.news/digital-rights/how-crypto-helps-latin-americas-drug-cartels-do-business.
[60] Team, Chainalysis. "Opioid Crisis and Crypto: Blockchain Analysis on Fentanyl Sales." Chainalysis, September 19, 2023. https://www.chainalysis.com/blog/cryptocurrency-fentanyl-analysis-2023/.
[61] Illicit Fentanyl from China: An evolving global operation. Accessed November 5, 2023. https://www.uscc.gov/sites/default/files/2021-08/Illicit_Fentanyl_from_China-An_Evolving_Global_Operation.pdf.
[62] Caribbean firm used crypto to launder $500 million - thestreet. Accessed November 5, 2023. https://www.thestreet.com/crypto/investing/crypto-sleuth-coffeezilla-says-caribbean-firm-used-crypto-to-launder-500-million.
[63] "Scam Alert: The Traders Domain Is Not Regulated." BrokersView. Accessed November 5, 2023. https://www.brokersview.com/news/scam-alert-the-traders-domain-is-not-regulated-112209.
[64] "Traders Domain Top MLM Recruiters Named & Shamed." BehindMLM RSS. Accessed November 5, 2023. https://behindmlm.com/companies/traders-domain-top-mlm-recruiters-named-shamed/.
[65] "Terms and Conditions." trubluefx. Accessed November 5, 2023. https://trubluefx.com/terms-and-conditions.
[66] "Detailed Information about 'Trubluefx.'" BrokersView. Accessed November 5, 2023. https://www.brokersview.com/ brokers/trubluefx.
[67] "WikiFX.US - the Ponzi Scammer V5 Forex Global Changed Its..." Facebook. Accessed November 5, 2023. https://www.facebook.com/WikiFX.US/posts/the-ponzi-scammer-v5-forex-global-changed-its-name-to-hilton-meta-fxhttpswwwwiki/661669845982697/.
[68] "Trubluefx Is Rated 'Poor' with 2.4 / 5 on Trustpilot." Trustpilot, December 31, 1969. https://www.trustpilot.com/review/trubluefx.com.
[69] John A. Cassara - congress.gov. Accessed November 5, 2023. https://www.congress.gov/118/meeting/house/115542/witnesses/HHRG-118-BA10-Wstate-CassaraJ-20230323.pdf.
[70] "Mexican Drug Cartels Sneak in $25 Billion a Year Using Bitcoin to Fund Operations." Bitcoinist.com, March 13, 2022. https://bitcoinist.com/mexican-drug-cartels-launder-25-billion/.
[71] "U.S. Treasury Targets Sinaloa Cartel Adding Crypto Address to Sanctions List: Trm Insights." RSS. Accessed November 5, 2023. https://www.trmlabs.com/post/u-s-treasury-targets-sinaloa-cartel-adding-crypto-address-to-sanctions-list.

[72] Chaparro, Luis. "The Cocaine Trade Is Booming, and Smugglers Have Their Eyes on a New Market." Business Insider. Accessed November 5, 2023. https://www.businessinsider.com/cocaine-trade-is-booming-and-smugglers-are-expanding-in-europe-2022-3.
[73] "Sinaloa Cartel." Encyclopædia Britannica, October 27, 2023. https://www.britannica.com/topic/Sinaloa-cartel.
[74] Sandra Pellegrini, María Fernanda Arocha. "Actor Profile: The Jalisco New Generation Cartel (CJNG)." ACLED, June 6, 2023. https://acleddata.com/2023/04/14/actor-profile-the-jalisco-new-generation-cartel/.
[75] United Nations Office on Drugs and Crime (UNODC). Accessed November 5, 2023. https://www.unodc.org/res/opioid-crisis/index_html/08_OnlineTrafficking_Report_Revised.pdf.
[76] Toledano, Javier Sutil. "Primeiro Comando Da Capital (PCC): From São Paulo to the World." Grey Dynamics, September 20, 2023. https://greydynamics.com/primeiro-comando-da-capital-pcc-from-sao-paulo-to-the-world/#30_Rivalries_and_Alliances.
[77] "Institutionalization of Crypto Latin America: FTI." FTI Consulting. Accessed November 5, 2023. https://www.fticonsulting.com/insights/articles/institutionalization-crypto-latin-america.
[78] Abrol, Ayushi. "How Many Bitcoins Are There and How Many Are Left to Mine? [Updated]." Blockchain Council, September 28, 2023. https://www.blockchain-council.org/cryptocurrency/how-many-bitcoins-are-left/#:~:text=Summary,million%20left%20to%20be%20mined.
[79] Klein, Written by David. "Sting Operation Reveals 'Ndrangheta-Colombian Cartel Partnership." OCCRP. Accessed November 5, 2023. https://www.occrp.org/en/daily/16451-sting-operation-reveals-ndrangheta-colombian-cartel-partnership.
[80] Cvrltoken.byethost24.com. Accessed November 5, 2023. http://cvrltoken.byethost24.com/.
[81] Cryptocurrency regulations by country - Thomson Reuters. Accessed November 5, 2023. https://www.thomsonreuters.com/en-us/posts/wp-content/uploads/sites/20/2022/04/Cryptos-Report-Compendium-2022.pdf.
[82] "El Salvador - United States Department of State." U.S. Department of State, March 20, 2023. https://www.state.gov/ reports/2022-country-reports-on-human-rights-practices/el-salvador/.
[83] "Justice Department Announces Eight Indictments against China Based Chemical Manufacturing Companies and Employees." DEA, October 4, 2023. https://www.dea.gov/documents/2023/2023-10/2023-10-03/justice-department-announces-eight-indictments-against-china#:~:text=The%20two%20drug%20cartels%20that,fentanyl%20precursors%20come%20from%20China.
[84] Kagan, Julia. "What Is Hawala? Money Transfer without Money Movement." Investopedia. Accessed November 5, 2023. https://www.investopedia.com/terms/h/hawala.asp.
[85] Felbab-Brown, Vanda, Vanda Felbab-Brown Nathaniel Parish Flannery, Peter A. Petri, Sharan Grewal, and Mallie Prytherch Patricia M. Kim. "How Mexico's Cartel Jalisco Nueva Generación Rules." Brookings, June 1, 2022. https://www.brookings.edu/articles/how-mexicos-cartel-jalisco-nueva-generacion-rules/.
[86] Toledano, Javier Sutil. "Primeiro Comando Da Capital (PCC): From São Paulo to the World." Grey Dynamics, September 20, 2023. https://greydynamics.com/primeiro-comando-da-capital-pcc-from-sao-paulo-to-the-world/#30_Rivalries_and_Alliances.
[87] "Scam Alert: The Traders Domain Is Not Regulated." BrokersView. Accessed November 5, 2023. https://www.brokersview.com/news/scam-alert-the-traders-domain-is-not-regulated-112209.
[88] Hayes, Adam. "What Is a Smurf and How Does Smurfing Work?" Investopedia. Accessed November 5, 2023. https://www.investopedia.com/terms/s/smurf.asp.
[89] "What Is Smurfing? Here's How 'Micro-Money Laundering' Works." Chargebacks911, October 24, 2023. https://chargebacks911.com/smurfing/#:~:text=Smurfing%20refers%20to%20a%20money,the%20intention%20of%20avoiding%20detection.
[90] Illicit Fentanyl from China: An evolving global operation. Accessed November 5, 2023. https://www.uscc.gov/sites/default/files/2021-08/Illicit_Fentanyl_from_China-An_Evolving_Global_Operation.pdf.
[91] "Hawala." Corporate Finance Institute, May 24, 2023. https://corporatefinanceinstitute.com/resources/wealth-management/hawala/.
[92] Kagan, Julia. "What Is Hawala? Money Transfer without Money Movement." Investopedia. Accessed November 5, 2023. https://www.investopedia.com/terms/h/hawala.asp.
[93] Team, Chainalysis. "Opioid Crisis and Crypto: Blockchain Analysis on Fentanyl Sales." Chainalysis, September 19, 2023. https://www.chainalysis.com/blog/cryptocurrency-fentanyl-analysis-2023/.
[94] Mexico: Organized crime and drug trafficking organizations. Accessed November 5, 2023. https://sgp.fas.org/crs/row/R41576.pdf.
[95] "Treasury Sanctions Individuals Linked to CJNG's Arms Trafficking, Fuel Theft, and Money Laundering." U.S. Department of the Treasury, June 6, 2023. https://home.treasury.gov/news/press-releases/jy1523.

[96] Sinembargo. “Could the Jalisco Cartel’s ‘El Mencho’ Really Be a Billionaire?” InSight Crime, April 24, 2023. https://insightcrime.org/news/analysis/jalisco-cartel-el-mencho-billionaire/.
[97] “United States Sanctions Sinaloa Cartel Fentanyl Traffickers and Colombian Clan Del Golfo Leader - United States Department of State.” U.S. Department of State. Accessed November 5, 2023. https://www.state.gov/united-states-sanctions-sinaloa-cartel-fentanyl-traffickers-and-colombian-clan-del-golfo-leader/#:~:text=The%20United%20States%20is%20sanctioning,production%20and%20trafficking%20in%20Colombia.
[98] InSight Crime. “First Capital Command - PCC.” InSight Crime, October 4, 2023. https://insightcrime.org/brazil-organized-crime-news/first-capital-command-pcc-profile/.
[99] “Two Chinese Nationals Charged with Operating Global Opioid and Drug Manufacturing Conspiracy Resulting in Deaths.” Office of Public Affairs | Two Chinese Nationals Charged with Operating Global Opioid and Drug Manufacturing Conspiracy Resulting in Deaths | United States Department of Justice, August 31, 2018. https://www.justice.gov/opa/pr/two-chinese-nationals-charged-operating-global-opioid-and-drug-manufacturing-conspiracy.
[100] “Red List: The Traders Domain.” CFTC. Accessed November 5, 2023. https://www.cftc.gov/node/241251.
[101] “Bitcoin Mining Farm, Trinimine, in the Works for T&T.” Trinidad Guardian, April 17, 2022. https://www.guardian.co.tt/business/bitcoin-mining-farm-trinimine-in-the-works-for-tt-6.2.1480985.5eed6afd60.
[102] Annual Threat Assessment of the U.S. Intelligence Community. February 6, 2023. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.
[103] Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats-and-nation-state-actors.
[104] Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/stopransomware.
[105] "Cryptojacking." Interpol. https://www.interpol.int/en/Crimes/Cybercrime/Cryptojacking.
[106] "Top cryptocurrency theft statistics of 2023." Persona. https://withpersona.com/blog/cryptocurrency-theft-statistics#:~:text=Cryptocurrency%20theft%20refers%20to%20the,them%20into%20a%20fraudulent%20transaction.
[107] "How the Lazarus Group is stepping up crypto hacks and changing its tactics." Elliptic. Last modified September 15, 2023. https://www.elliptic.co/blog/how-the-lazarus-group-is-stepping-up-crypto-hacks-and-changing-its-tactics.
[108] "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions." U.S. Department of Justice. Last modified September 6, 2018. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.
[109] Lang, Nick, and Anna Belak. "Cryptojacking: Free Money for Attackers, Huge Cloud Bill for You." The New Stack. Last modified November 16, 2022. https://thenewstack.io/cryptojacking-free-money-for-attackers-huge-cloud-bill-for-you/#:~:text=performing%20these%20calculations.-,Cryptojacking%20is%20when%20threat%20actors%20use%20stolen%20cloud%20resources%20to,%2453%20their%20victim%20is%20billed.
[110] "Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester." Cybersecurity and Infrastructure Security Agency. Last modified November 25, 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-320a.
[111] "APT38: Details on New North Korean Regime-Backed Threat Group." Mandiant. Last modified October 19, 2023. https://www.mandiant.com/resources/blog/apt38-details-on-new-north-korean-regime-backed-threat-group.
[112] Corfield, Gareth. "How the West broke the grip of Lamborghini-driving Russian hackers." The Telegraph. Last modified June 13, 2022. https://www.telegraph.co.uk/technology/2022/06/13/west-broke-grip-lamborghini-driving-russian-hackers/.
[113] "APT43: North Korean Group Uses Cybercrime to Fund Espionage Operations." Mandiant. https://www.mandiant.com/resources/reports/apt43-north-korea-cybercrime-espionage.
[114] "Islamic Revolutionary Guard Corps (IRGC)." Director of National Intelligence. Last modified March 2022. https://www.dni.gov/nctc/ftos/irgc_fto.html#:~:text=The%20US%20State%20Department%20designated,Global%20Terrorist%2C%20in%20October%202007.
[115] Al-Kassab, Fatima. "What is the 'axis of resistance' of Iran-backed groups in the Middle East?" National Public Radio. Last modified October 26, 2023. https://www.npr.org/2023/10/26/1208456496/iran-hamas-axis-of-resistance-hezbollah-israel#:~:text=The%20%22axis%20of%20resistance%22%20is,one%20another%20and%20to%20Tehran.
[116] "Seven International Cyber Defendants, Including 'Apt41' Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally." Office of Public Affairs - U.S. Department of Justice. Last modified September 16, 2020. https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer.
[117] "Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments." Mandiant. Last modified August 9, 2023. https://www.mandiant.com/resources/blog/apt41-us-state-governments#:~:text=Campaign%20

Overview&text=During%20this%20timeframe%2C%20APT41%20successfully,web%20application%20compromises%2C%20APT41%20conducted%20.
[118] Cimpanu, Catalin. "Bit Paymer Ransomware Hits Scottish Hospitals." Bleeping Computer. Last modified August 29, 2017. https://www.bleepingcomputer.com/news/security/bit-paymer-ransomware-hits-scottish-hospitals/.
[119] "China's backers and 'triad' gangs have a history of common foes. Hong Kong protesters fear they are next." The Washington Post. Last modified July 23, 2019. https://www.washingtonpost.com/world/asia_pacific/chinas-backers-and-triad-gangs-have-history-of-common-foes-hong-kong-protesters-fear-they-are-next/2019/07/23/41445b88-ac68-11e9-9411-a608f9d0c2d3_story.html.
[120] "Triads, cops still hunt mafia boss who stole $2.6M crypto from Tether trader." Protos. Last modified November 24, 2021. https://protos.com/triads-crypto-tether-trader-kidnapped-boss-hunted-by-cops-own-gang/.
[121] "Special Report Wagner Group: The Evolution of a Private Army." The Soufan Center. Last modified June 2023. https://thesoufancenter.org/wp-content/uploads/2023/06/TSC-Special-Report-The-Wagner-Group-The-Evolution-Of-Putins-Private-Army.pdf.
[122] Report on IRGC Terrorist Activity. https://tenney.house.gov/sites/evo-subsites/tenney.house.gov/files/evo-media-document/2023_Tenney_Report_Opportunity_V5.pdf.
[123] "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash." U.S. Department of the Treasury. Last modified August 8, 2022. https://home.treasury.gov/news/press-releases/jy0916.
[124] "United States and United Arab Emirates Disrupt Large Scale Currency Exchange Network Transferring Millions of Dollars to the IRGC-QF." U.S. Department of the Treasury. Last modified May 10, 2018. https://home.treasury.gov/news/press-releases/sm0383.
[125] "Online Video Games and Money Laundering." Sanction Scanner. https://sanctionscanner.com/blog/online-video-games-and-money-laundering-183.
[126] "How Triad-linked gang used crypto and casinos to launder $10B." Protos. Last modified February 6, 2023. https://protos.com/how-triad-linked-gang-used-crypto-and-casinos-to-launder-10b/.
[127] "$2 Million and Counting: How Dozens of Pro-Russian Groups Are Using Cryptocurrency Donations to Fund the War in Ukraine." Chainalysis. Last modified July 29, 2022. https://www.chainalysis.com/blog/pro-russian-crypto-donations- war-in-ukraine/.
[128] Rainsford, Sarah, and Kathryn Armstrong. "Wagner mutiny: Group fully funded by Russia, says Putin." BBC News. Last modified June 27, 2023. https://www.bbc.co.uk/news/world-europe-66029382.
[129] "Country Reports on Terrorism 2021: Iran." U.S. Department of State. https://www.state.gov/reports/country-reports-on-terrorism-2021/iran/#:~:text=In%202021%2C%20Iran%20continued%20providing,Liberation%20of%20Palestine %2DGeneral%20Command.
[130] Asmakov, Andrew. "Israel Seizes $1.7M From Crypto Accounts Linked to Iran's Quds Force, Hezbollah: Report." Decrypt. Last modified June 28, 2023. https://decrypt.co/146539/israel-seizes-1-7m-from-crypto-accounts-linked-to-irans-quds-force-hezbollah-report.
[131] "Advanced Persistent Threats (APTs)." Mandiant. https://www.mandiant.com/resources/insights/apt-groups.
[132] "Microsoft links Vietnamese state hackers to crypto-mining malware campaign." ZDNET. Last modified November 30, 2020. https://www.zdnet.com/article/microsoft-links-vietnamese-state-hackers-to-crypto-mining-malware-campaign/.
[133] Following Terrorist Attack on Israel, Treasury Sanctions Hamas Operatives and Financial Facilitators. October 18, 2023. https://home.treasury.gov/news/press-releases/jy1816.
[134] Sigalos, MacKenzie. "In bankrupt Lebanon, locals mine bitcoin and buy groceries with tether, as $1 is now worth 15 cents." CNBC. Last modified November 5, 2022. https://www.cnbc.com/2022/11/05/-in-bankrupt-lebanon-locals-mine-bitcoin-and-buy-groceries-with-tether.html.


CMC WHISKEY
CMC YANKEE
CMC SIERRA
APPLIED INTELLIGENCE PROJECT
INTELLIGENCE AND SECURITY STUDIES
UNITED STATES SECRET SERVICE
299e6def278e1d502089e8d3832c30bc8f88