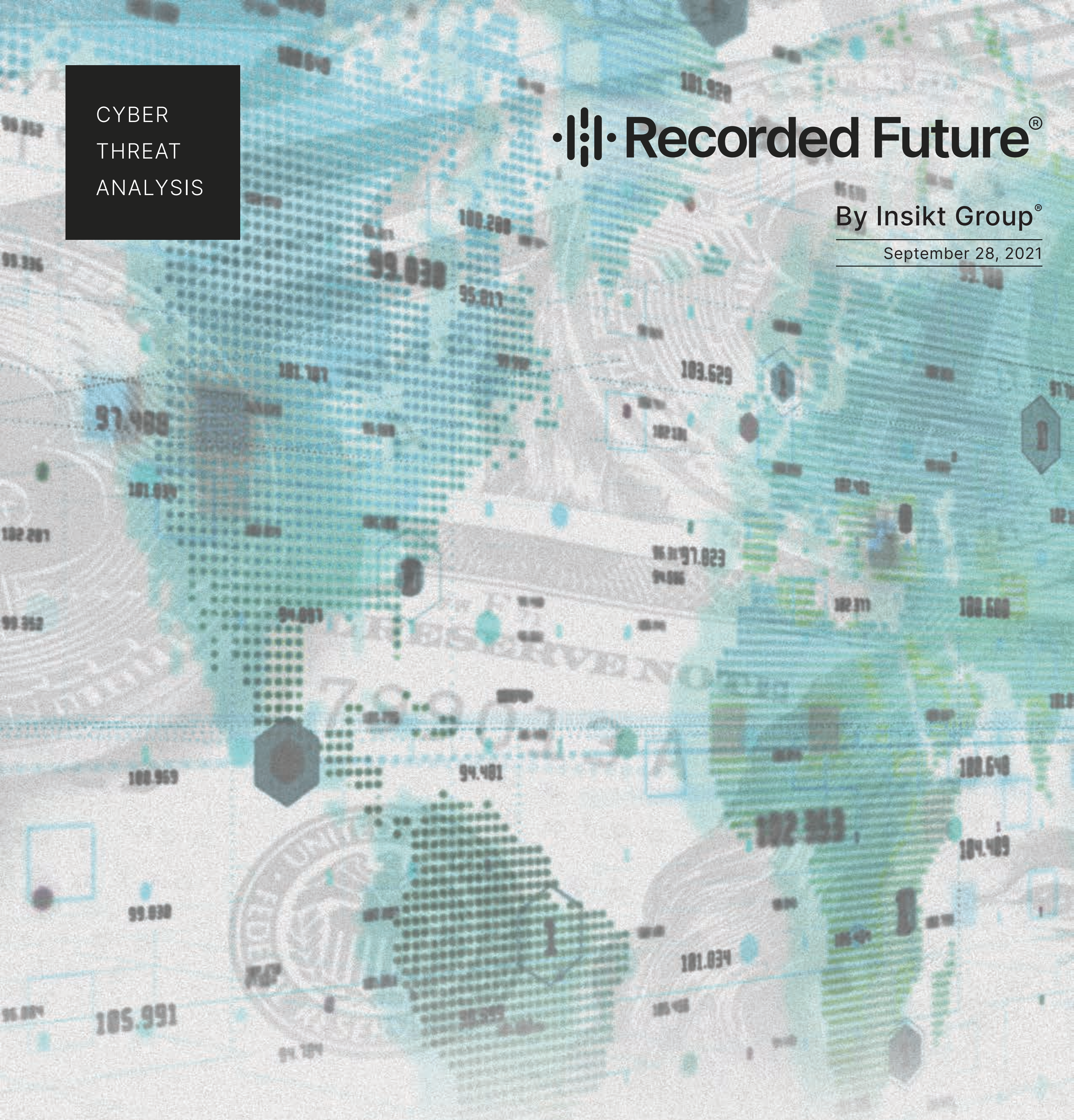
CYBER THREAT ANALYSIS



Recorded Future®

By Insikt Group®

September 28, 2021

THE BUSINESS OF FRAUD: Laundering Funds in the Criminal Underground

Recorded Future analyzed current data from the Recorded Future® Platform, dark web, and open-source intelligence (OSINT) sources to review money laundering services within underground sourcing and the methodology and operations used by threat actors. This report expands upon findings addressed in the first report of the Insikt Group's Fraud Series, "The Business of Fraud: An Overview of How Cybercrime Gets Monetized".

Executive Summary

Money laundering services within the dark web facilitate a combination of activities through which threat actors can conceal the origins of their money, transfer cryptocurrency, have funds sent to a bank account or payment cards, or exchange to physical cash via online payment solution platforms like WebMoney or PerfectMoney. Many of these services are linked to the use of cryptocurrency and rely on other mixing services to tumble funds and help threat actors remain anonymous when transferring them. Peer-to-peer (P2P) transactions are a convenient alternative to traditional financial platforms, with support for platforms such as Venmo being touted as key features within popular underground services.

Key Judgments

- Dark web money laundering services facilitate a multitude of combinations through which threat actors can clean their money and can transfer cryptocurrency into virtual currency, have funds sent to a bank account or payment cards, or exchange to physical fiat currency.
- Money laundering services referenced within underground sources over the past year have consistently relied on money mules, cash-out requests, exchangers, or mixers to succeed.
- Despite a high volume of arrests and takedowns of money laundering services or services that support laundering activity over the past year, underground actors generally appear disinclined to cease laundering operations they likely continue to deem profitable.
- Cybercriminals are likely to adopt new technologies such as NFTs and other laundering techniques in response to law enforcement action and growing private sector awareness of their activities.
- Ransomware operators likely use the multitude of dark web money laundering services operated by threat actors on well-known cybercrime forums such as Verified. Bitcoin is likely to continue to be the most widely used cryptocurrency in ransomware and laundering operations.

Background

The ability to monetize cyberattacks remains one of the most important aspects of cybercrime. As a result, money laundering services are a mainstay of any prominent dark web forum or marketplace involved in hacking or fraud; these services are likely familiar to the vast majority of ransomware operators and affiliates. Advertisements for money laundering services, tools, or procedures are often located within sections of an underground source specifically devoted to ads or discussions surrounding fraud topics as a whole, including other popular offerings related to counterfeit documents or crypto mining.

The threat that laundering operations pose to both the global economy and security communities is not a new phenomenon. However, the methods by which threat actors attempt to layer and eventually integrate illicit funds have changed over time in direct response to changes in technology and how financial institutions can monitor these platforms for irregular activities characteristic of fraud. Non-cash forms of money such as prepaid cards speed up transactions and reduce the amount of direct interaction with a representative of a financial institution that may impede opportunities at laundering funds.

Overall, the laundering process continues to be primarily divided into 3 distinct stages:

1. Placement: In the first stage, the proceeds of illegal activity enter the financial system and are disguised. Funds can be placed into circulation via mediums such as currency exchanges or other businesses like casinos, either locally or abroad.
2. Layering: Next, funds are "layered" using methods like converting cash into monetary instruments or wire transferring money between bank accounts to make it more difficult for law enforcement to detect or follow the trail of the illegal proceeds.
3. Integration: Finally, the illegal proceeds are reintroduced as legitimate funds through methods that make them appear to be the earnings from normal business activity.

Many fraudulent laundering services within underground sources are intricately linked to the use of cryptocurrency, with bitcoin (BTC) likely to continue to be the most widely used cryptocurrency for the foreseeable future. Although other cryptocurrencies such as Bitcoin Cash (commonly used by Thanatos ransomware), Monero (Kirk, SpriteCoin ransomware), Ethereum (HC7 Planetary ransomware), and Dash (Anatova ransomware) are sometimes used, the overwhelming majority of underground sources monitored by Insikt Group over the first half of 2021 reference either Bitcoin or Ethereum. Chinese-language sources in 2021 occasionally referenced Monero as a viable cryptocurrency alternative for laundering given features such as its circular signature, a digital signature that can be made by any member of a circular group, where all signatures are equivalent, and transaction mixing, meaning that when funds are sent, they are sent as a group of random transfers for the same amount, anonymizing who the real recipient and sender are.

Alternative forms of laundering money remain readily available for threat actors across the dark web regardless of their proficiency in navigating underground sources. For example, virtual currencies, such as Qiwi, have historically remained of interest to cybercriminals operating within Russia, particularly on underground marketplaces specializing in the sale of narcotics. Converting stolen funds into alternative virtual currencies remains a viable alternative for laundering despite efforts in countries such as Russia to outrzight ban cash deposits on anonymous electronic wallets.

Though the case studies and services detailed throughout this reporting often cater to criminal entities that operate exclusively within underground forums or marketplaces, the funneling of cryptocurrencies in support of laundering activity is not exclusive to dark web actors.

- In July 2021, details from a Hatewatch investigation into a Daily Stormer editor linked to multiple neo-Nazi websites detailed how they funneled money to a Russian darknet website that traffics in hacked personal data, drugs, ransomware, stolen credit cards, and money laundering services. Hatewatch identified the editor's transactions over several years, noting that they no longer solicit bitcoin donations on the Daily Stormer website but instead encouraged readers to donate Monero, likely in an attempt to evade the attention of blockchain analytic firms.
- Online gambling platforms have been highlighted throughout 2021 as popular avenues for money laundering, particularly in China. In June 2021, the Chinese Ministry of Public Security announced the arrest of over 1,100 people suspected of using cryptocurrencies to launder illegal proceeds from telephone and Internet scams in a coordinated crackdown. China's Payment and Clearing Association stated that nearly 13% of gambling websites supported virtual currencies and played a role in the rising number of crimes involving virtual currencies in the country.
- US law enforcement officials have stated that Chinese "money brokers" represent one of the most worrisome new threats in drug-related investigations. In the aftermath of a September 2020 sentencing memorandum

in Chicago against a Chinese businessman, US prosecutors stated that Chinese money brokers in Mexico had "come to dominate international money laundering markets", routing cartel drug profits from the US to China then on to Mexico via burner phones and Chinese banking apps. Similar to entities operating within the underground, drug trafficking organizations (DTOs) continue to employ a variety of money laundering methods to avoid detection. The launderers would pay small Chinese-owned businesses in the US and Mexico to help them move the funds, with most contact with the banking system occurring within China.

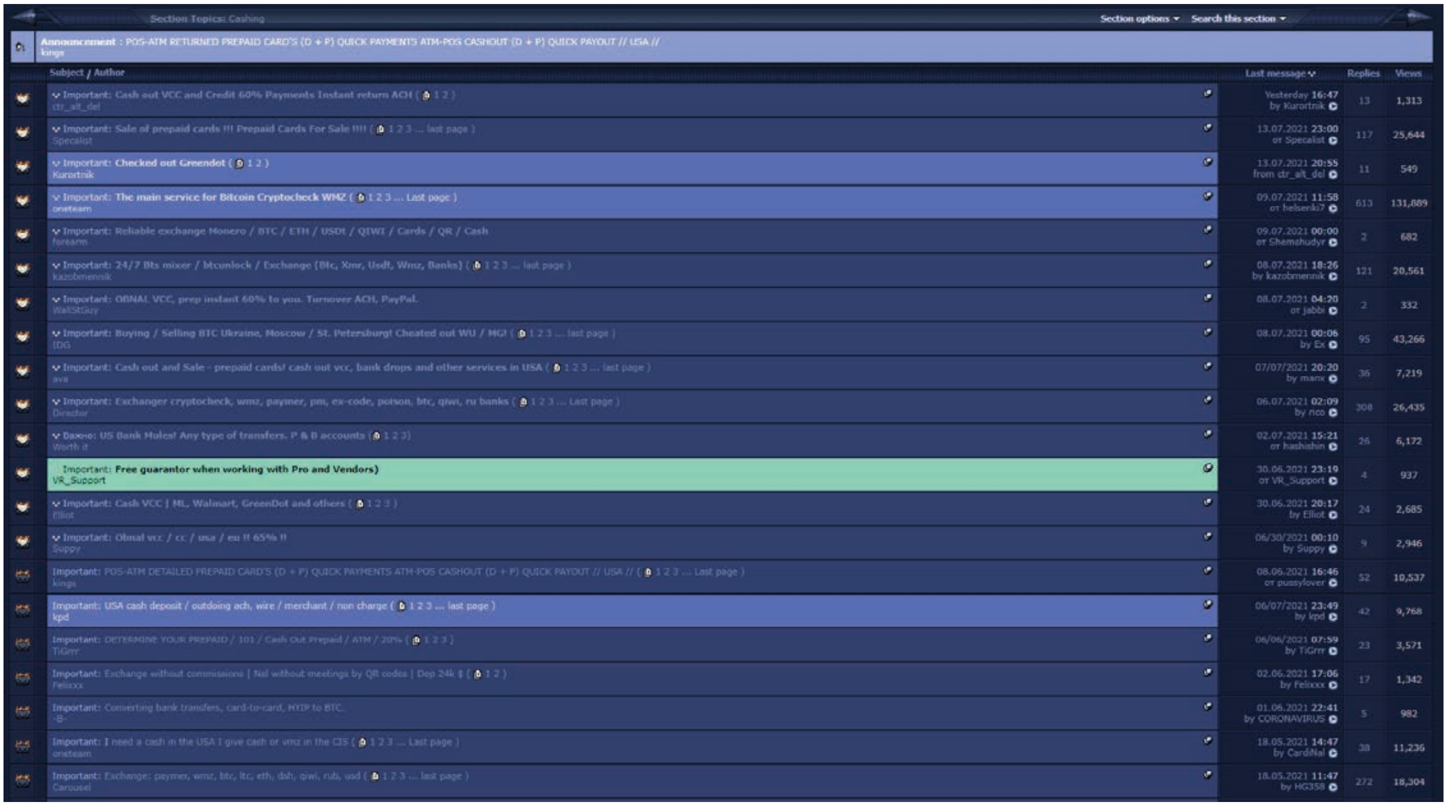
- The US Department of Treasury's National Strategy for Combating Terrorist and Other Illicit Financing 2020 stated that from intelligence they had gathered, DTOs did not historically outsource the laundering of drug proceeds as frequently but had increasingly turned to professional money launderers. Similar to underground actors operating on traditional dark web websites, these entities adapt in response to law enforcement action, regulatory changes, and growing private sector awareness of their activities. Asian communities (primarily Chinese) were cited within this assessment as relying more on entities that facilitate exchanges of Chinese and US currency or serve as money brokers in traditional trade-based money laundering schemes.

Threat Analysis

Cryptocurrency Mixing and Hopping Chains

A cryptocurrency tumbler or cryptocurrency mixing service is a service offered to mix potentially identifiable cryptocurrency funds with others as part of an effort to obscure the trail back to the fund's original source. Cryptocurrency mixing often combines a user's transaction with that of other random users who happen to be making separate transactions through the system at the same time. Essential aspects of dark web money laundering include the ability to mix and exchange cryptocurrency, transfers to and from virtual currency bank accounts, and the delivery of physical fiat currency.

It is highly likely that at least some members of more prominent cyber threat activity groups within open-source reporting over the past year, such as ransomware cartels, have accounts on underground forums and may also be using some of the vetted laundering services advertised there. At a minimum, cyber threat entities who receive their ransom payments in BTC require some level of BTC mixing to keep their personal BTC addresses unknown. Mature threat actors would likely do more than just this, and after mixing their BTC, they would have a variety of options to choose from provided by these laundering services. However, not all methods of laundering funds need to be performed exclusively using digital assets, with physical mediums such as prepaid debit cards also remaining an attractive commodity to criminals attempting to withdraw money from systems they would interact with such as an ATM.



Announcement : POS-ATM RETURNED PREPAID CARD'S (D + P) QUICK PAYMENTS ATM-POS CASHOUT (D + P) QUICK PAYOUT // USA //
kings

Subject / Author	Last message	Replies	Views
Important: Cash out VCC and Credit 60% Payments Instant return ACH (1 2) ctr_alt_del	Yesterday 16:47 by Kurortnik	13	1,313
Important: Sale of prepaid cards !!! Prepaid Cards For Sale !!!! (1 2 3 ... last page) Specalist	13.07.2021 23:00 от Specalist	117	25,644
Important: Checked out Greendot (1 2) Kurortnik	13.07.2021 20:55 from ctr_alt_del	11	549
Important: The main service for Bitcoin Cryptocheck WMZ (1 2 3 ... Last page) oneteam	09.07.2021 11:58 от helsenki7	613	131,889
Important: Reliable exchange Monero / BTC / ETH / USDt / QIWI / Cards / QR / Cash forearm	09.07.2021 00:00 от Shemshudyr	2	682
Important: 24/7 Bts mixer / btcunlock / Exchange (Btc, Xmr, Usdt, Wmz, Banks) (1 2 3 ... last page) kazobmennik	08.07.2021 18:26 by kazobmennik	121	20,561
Important: OBNAL VCC, prep instant 60% to you. Turnover ACH, PayPal. WallStGuy	08.07.2021 04:20 от jabbi	2	332
Important: Buying / Selling BTC Ukraine, Moscow / St. Petersburg! Cheated out WU / MG! (1 2 3 ... last page) IDG	08.07.2021 00:06 by Ex	95	43,266
Important: Cash out and Sale - prepaid cards! cash out vcc, bank drops and other services in USA (1 2 3 ... last page) ava	07/07/2021 20:20 by manx	36	7,219
Important: Exchanger cryptocheck, wmz, paymer, pm, ex-code, poison, btc, qiwi, ru banks (1 2 3 ... Last page) Director	06.07.2021 02:09 by rico	308	26,435
Важно: US Bank Mules! Any type of transfers. P & B accounts (1 2 3) Worth it	02.07.2021 15:21 от hashishin	26	6,172
Important: Free guarantor when working with Pro and Vendors) VR_Support	30.06.2021 23:19 от VR_Support	4	937
Important: Cash VCC | ML. Walmart, GreenDot and others (1 2 3) Elliot	30.06.2021 20:17 by Elliot	24	2,685
Important: Obnal vcc / cc / usa / eu !! 65% !! Suppy	06/30/2021 00:10 by Suppy	9	2,946
Important: POS-ATM DETAILED PREPAID CARD'S (D + P) QUICK PAYMENTS ATM-POS CASHOUT (D + P) QUICK PAYOUT // USA // (1 2 3 ... Last page) kings	08.06.2021 16:46 от pussylover	52	10,537
Important: USA cash deposit / outdoing ach, wire / merchant / non charge (1 2 3 ... last page) kpd	06/07/2021 23:49 by kpd	42	9,768
Important: DETERMINE YOUR PREPAID / 101 / Cash Out Prepaid / ATM / 20% (1 2 3) TiGrrr	06/06/2021 07:59 by TiGrrr	23	3,571
Important: Exchange without commissions | Nal without meetings by QR codes | Dep 24k $ (1 2) Felixxx	02.06.2021 17:06 by Felixxx	17	1,342
Important: Converting bank transfers, card-to-card, HYIP to BTC. -B-	01.06.2021 22:41 by CORONAVIRUS	5	982
Important: I need a cash in the USA I give cash or wmz in the CIS (1 2 3 ... Last page) oneteam	18.05.2021 14:47 by CardiNal	38	11,236
Important: Exchange: paymer, wmz, btc, ltc, eth, dsh, qiwi, rub, usd (1 2 3 ... last page) Carousel	18.05.2021 11:47 by HG358	272	18,304

Figure 1: Sample of money laundering service threads (Source: Verified Forum)

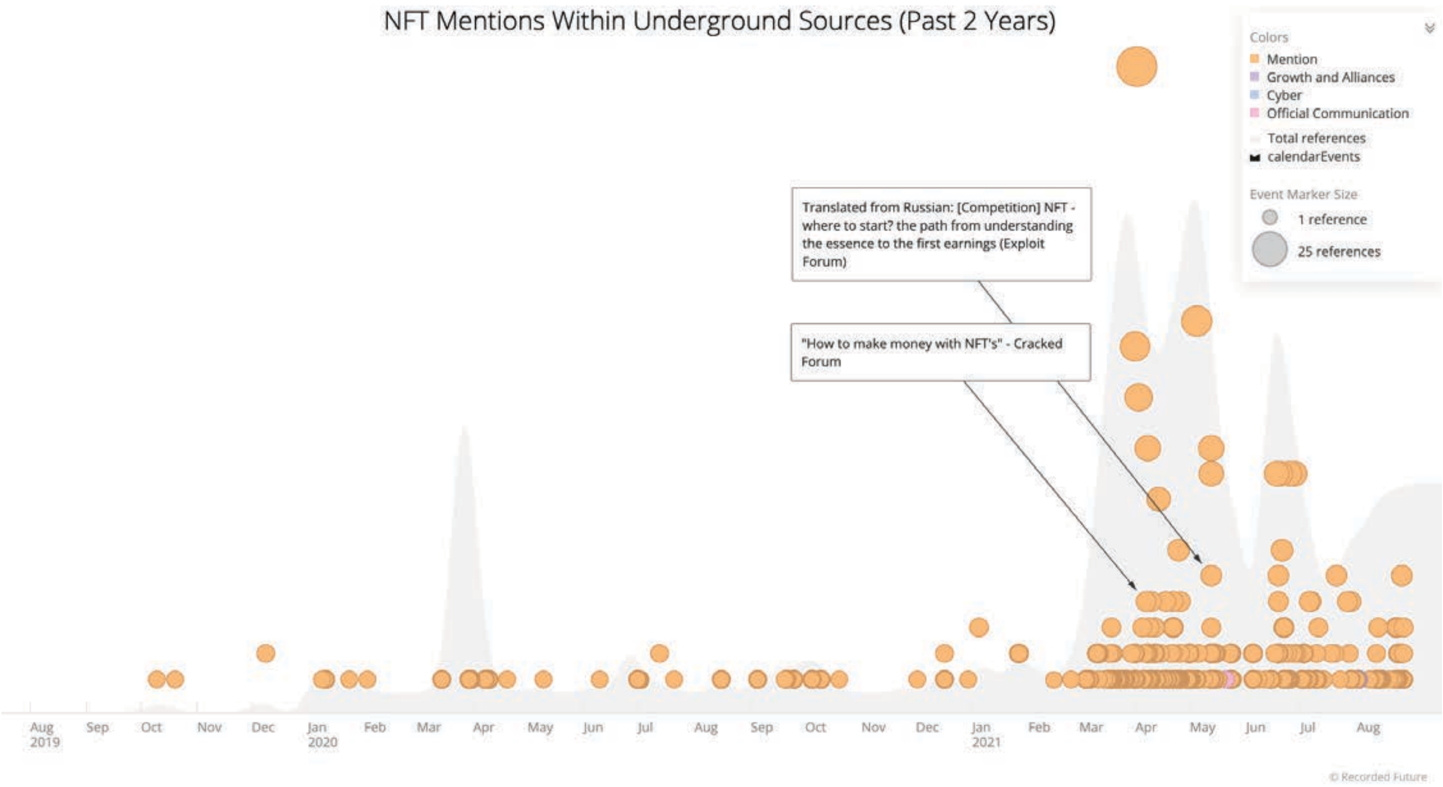


Figure 2: References to NFT technology within underground sources, July 2019 to July 2021 (Source: Recorded Future)

Actors have also relied on exchanging stolen funds via legitimate crypto trading platforms to swap them for "clean" cryptocurrency through which clients of an illicit service would then be able to withdraw the funds from any exchange. These methods are not exclusively shared across high-tier forums, with some entry-level "cleaning" tutorials being found on English-language forums such as Nulled Forum in 2021. Insikt Group reviewed references to open-source cryptocurrency mixing tools or services that were promoted by actors across both low- and high-tier forums over the past year and found that threat actors often recommended the same services when users requested assistance. Open-source mixing services seen promoted across multiple underground sources over the past year included the following:

- Blender (blender[.]io)
- UltraMixer (ultramixer[.]net)
- FoxMixer (foxmixer[.]com)
- Smart Mixer (smartmixer[.]io)

Ensuring that the funds are derived from exchanges that traditionally prohibit transactions affiliated with sources that may be considered "suspicious" would help a larger volume of actors successfully launder stolen funds and circumvent the efforts of law enforcement officials or blockchain analytic organizations from attributing them to a criminal entity.

While still relying on more traditional methods of laundering that rely on physical mediums such as prepaid debit cards, criminals also continue to innovate their laundering methods based around popular technologies that gained prominence over the past year. Non-fungible tokens (NFTs) are units of data stored on blockchain technology platforms that certify a digital asset to be unique and often represent common items such as photos, videos, or other types of digital files. NFT sales exploded in popularity in the first half of 2021, generating $2 billion in revenue within the first quarter. After criminals recognized their potential, NFTs were quickly adopted to launder money. While some forum members believe NFTs to be a short-term, unsustainable option, the volume of references observed by Insikt Group increased significantly, including on higher-tier forums such as Exploit Forum.

Conversations observed within Russian-language forums showed that actors promoting these services are fully aware of systems or organizations that devote company resources to specifically monitor the transfer of crypto funds, with companies such as Chainalysis, CipherTrace, Crystal Blockchain, LeoNovus, and BlockChain Alliance systems referenced as direct examples monitored by these actors for updates. Recent efforts directed at ransomware crews such as DarkSide also renewed conversations within the criminal underground around the capabilities of blockchain analytic organizations in 2021 in response to the US government's publications detailing law enforcement's success at preventing a portion of the funds associated with the Colonial Pipeline extortion event from being received by the actors responsible for it.

- Exploit Forum user "BitMaximum" created a thread in late 2019 advertising their cryptocurrency laundering service that generated a high volume of discussion on the forum through April 2020. The user wrote that they can exchange "dirty" cryptocurrency through a crypto trading platform, and that it would not be connected to their fraudulent funds. According to the details of the service, the scheme is implemented so that no one can trace the origin of the funds and the individual could pretend to be a trader. BitMaximum clarified in the thread that they had once reached their client limit, implying that the service was catered towards specific groups of buyers.

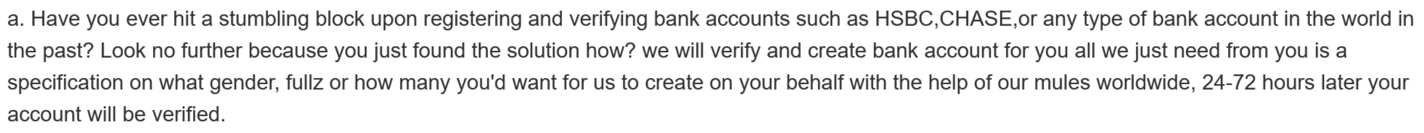
The sentiment among underground actors toward reputable exchanges such as Binance was similar to those expressed toward blockchain analytic firms throughout 2021. In response to the growing number of articles published by Binance that detailed the assistance they have provided to international law enforcement investigations into money laundering services, actors were observed encouraging one another to ensure that any funds associated with a laundering operation were not funneled through Binance. Earlier this year, Binance specifically referred to money connected to cyberattacks being laundered through nested services and suspicious exchanger accounts as one of the biggest security problems in the industry today. For several cases associated with illicit blockchain flows coming onto exchanges monitored by Binance, the exchange is not harboring the actual criminal group itself but rather being used as a middleman to launder stolen profits.

Role of Money Mules

A money mule (дропы — "drops" in Russian) is a person who transfers fraudulent money on behalf of someone else, whether they do it wittingly (не разводные) or unwittingly (разводные). Online threat actors recruit money mules to move money, either physically or electronically, through various bank accounts or many other methods. Once received, the mule will wire funds into a third-party bank account or withdraw the money received, possibly via several cashier's checks, convert the money into a virtual currency or a prepaid debit card, send the money through a money service business, or some combination of these. Criminals can then receive the laundered cash, originally stolen from victim accounts that were usually obtained by some form of account takeover. Criminal activities that don't require a nexus to underground marketplaces to succeed, such as drug sales and human trafficking, also rely on networks of money mules and enable actors to distance themselves from victims and the source of funds.

Money laundering services promoted or referenced within underground sources over the past year have consistently relied on money mules, cash-out requests, exchangers, or mixers. Mules are likely to continue to be used, knowingly or unknowingly, to launder money for various criminal operations. Cybercriminals who specialize in drops can place ads in legitimate job search websites or local newspapers to entice prospects to join their networks. For example, Russian classified networks such as Reklama place ads for jobs with high salaries, and ads in the classified sections/groups on Facebook look for individuals seeking to make quick cash.

In 2020, US law enforcement agencies took action against over 2,300 money mules, far surpassing 2019's efforts, which acted against around 600 money mules. The drops and money mules ecosystem starts with a recruitment process that allows cybercriminals to involve local personas in their criminal enterprise. These are individuals who are used as recipients of stolen funds, as those who cash out stolen payment cards at ATMs, or as individuals who use their accounts to launder funds between various accounts.



a. Have you ever hit a stumbling block upon registering and verifying bank accounts such as HSBC,CHASE,or any type of bank account in the world in the past? Look no further because you just found the solution how? we will verify and create bank account for you all we just need from you is a specification on what gender, fullz or how many you'd want for us to create on your behalf with the help of our mules worldwide, 24-72 hours later your account will be verified.

Figure 3: Underground vendor claiming to operate mule network to support card fraud activity (Source: Versus Market)

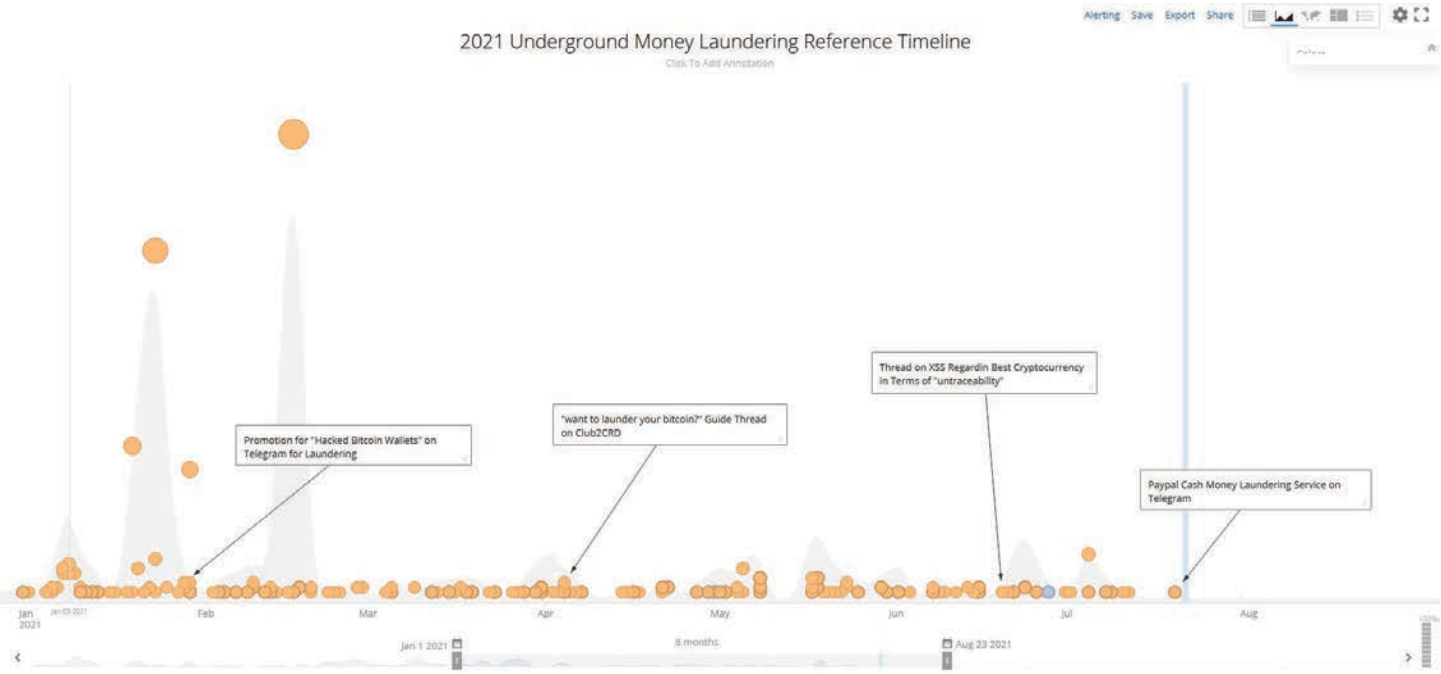

Alerting
Save
Export
Share
2021 Underground Money Laundering Reference Timeline
Click To Add Annotation
Promotion for "Hacked Bitcoin Wallets" on Telegram for Laundering
"want to launder your bitcoin?" Guide Thread on Club2CRD
Thread on XSS Regardin Best Cryptocurrency in Terms of "untraceability"
Paypal Cash Money Laundering Service on Telegram
Jan 2021
Feb
Mar
Apr
May
Jun
Jul
Aug
Jan 1 2021
8 months
Aug 23 2021

Figure 4: Money laundering references within underground sources in 2021 (Source: Recorded Future)

High Volume of Arrests

Alongside the consistent volume of services promoted within underground sourcing, Insikt Group has equally observed ongoing efforts by international law enforcement entities to disrupt them, particularly from the US Department of Justice. The details surrounding the arrests of administrators of multiple services throughout the past several years provide additional insight into the techniques and sources these actors rely upon to generate revenue, including their reliance on physical assets such as shell companies or other bank accounts through which they funnel illegally acquired funds, usually in the form of cryptocurrency.

- On August 28, 2020, the US Department of Justice announced the arrest of Roman Sterlingov, administrator of the Bitcoin Fog mixer since 2011. Bitcoin Fog was the longest-running cryptocurrency mixer at the time, according to the press release. The service moved over 1.2 million bitcoins over its lifespan — a total value of approximately $335 million at the time of the transactions. The bulk of this cryptocurrency came from dark web marketplaces and was tied to illegal narcotics, computer fraud and abuse activities, and identity theft.
- On March 31, 2021, the administrator of the DeepDotWeb (DDW), a website that connected internet users with other underground marketplaces that sold illegal commodities, including firearms, malware, and stolen financial data, pleaded guilty to money laundering conspiracy charges. The administrators received kickback payments from the marketplaces they promoted in the form of virtual currency and attempted to conceal their activity by transferring the payments from an underground bitcoin wallet they managed to other bitcoin accounts and bank accounts controlled in the names of shell companies.
- On April 9, 2021, the Department of Justice announced the arrest of an underground vendor known as NeverPressedRX (NPRX). The NPRX vendor store had claimed to sell authentic medications, including prescription opioids, sourced from US pharmacies. The admin allegedly laundered the proceeds of his criminal activity by cashing out his bitcoin drug payments into US dollars and moving the funds through various accounts, including his business bank accounts, to conceal his activity.
- In July 2021, the US Department of Justice unsealed a criminal indictment and criminal complaint charging Apostolos Trovias, also known as “The Bull”, with securities fraud and money laundering in connection with his scheme to solicit and sell stock trading tips and pre-release earnings and deal information regarding public companies. Apostolos Trovias attempted to hide his insider trading scheme behind unspecified anonymizing software, screen names, and bitcoin payments via encrypted messaging applications and emails.

In response to this consistent trend of arrests made by the US Department of Justice over the past year (and the publicly available reports of their details and outcomes), underground actors seem to review these publications with interest and make regular attempts to improve their tradecraft. For example, in the aftermath of several arrests tied to the Clop ransomware crew by Ukrainian law enforcement authorities, Insikt Group observed a thread on a Russian-language forum discussing the topic of which cryptocurrency was best in terms of "untraceability".

Underground Forums and Messaging Platforms

The following services historically operated across forums, shops, as well as popular messaging platforms such as Telegram, provide an overview of many of the features or methods through which modern money laundering services functioned over the past year within the criminal underground.

LAUNDROMAT

LAUNDROMAT is a money-laundering Telegram service with 646 members operated by the threat actor @GetChase. According to their official statement, they work with all member countries of the United Nations (UN), including Commonwealth of Independent States (CIS) countries. The service provides a personal manager for customer needs who is available online 24/7. LAUNDROMAT offers company registrations in offshore jurisdictions, provides printed documents, and can open bank accounts in offshore jurisdictions. At the time of writing, LAUNDROMAT suspended their activities with a promised comeback in fall 2021 (date not specified), and detailed their services:

- Direct deposits
- SEPA/IBAN/SWIFT
- PayPal (US/EU)
- Wire, Zelle, Skrill, Venmo, Neteller, and CashApp
- Bank accounts (US
- VCC (MoneyLion, RobinHood, Chime, Current, Sable, N26, Varo, Aspiration, Brex, SoFi, Monzo, MoCaFi, GoBank, and Stash)

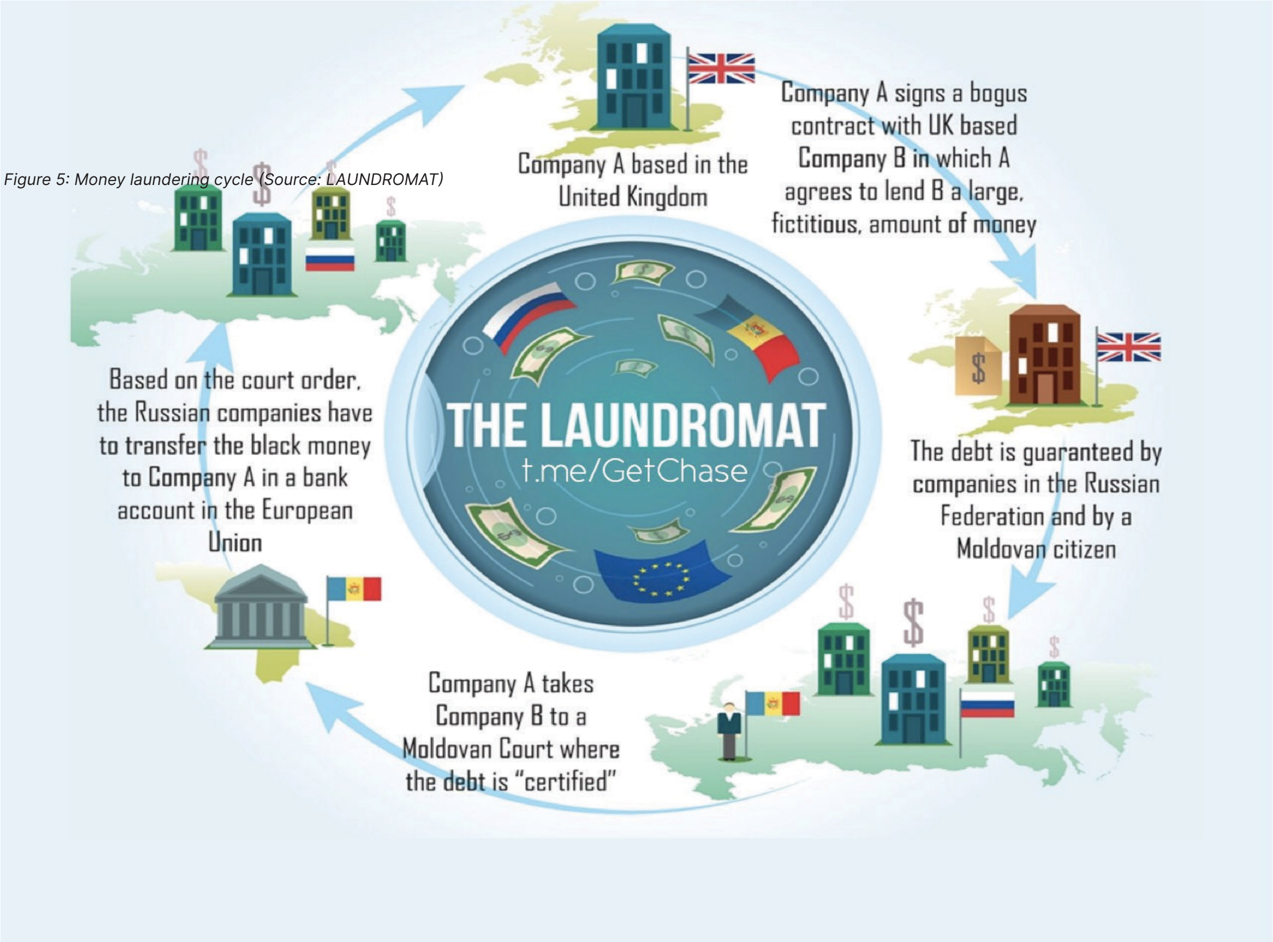

Company A based in the United Kingdom
Company A signs a bogus contract with UK based Company B in which A agrees to lend B a large, fictitious, amount of money
The debt is guaranteed by companies in the Russian Federation and by a Moldovan citizen
Company A takes Company B to a Moldovan Court where the debt is "certified"
Based on the court order, the Russian companies have to transfer the black money to Company A in a bank account in the European Union
THE LAUNDROMAT
t.me/GetChase

Figure 5: Money laundering cycle (Source: LAUNDROMAT)

approved_calls

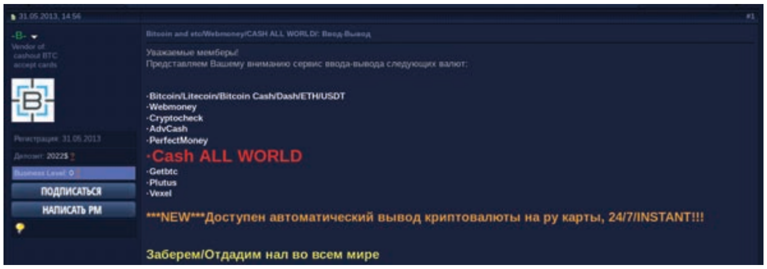
“approved_calls”, a member of the high-tier forums Maza and Verified, has advertised a calling service catering to various fraud-related operations in the US and other countries since September 2015. According to the threat actor, they currently employ phone operators that speak any language, with male and female voices. approved_calls is offering their services for the following fraud-related activities:

- Recruitment of drops and mules (such as social engineering individuals)
- Carding — payment card fraud (such as calling banks and pretending (social engineering) to be a legitimate cardholder)
- Spoofing calls (to portray themselves as someone they are not)
- Reshipping fraud (such as confirming orders and deliveries)
- Dating fraud (scamming and social engineering users of dating sites)
- Drafting correspondence (for dating fraud and fake recruitment purposes)
- Receiving calls to a specific number (dating fraud only)
- Calling to render a target’s phone lines inoperable/busy (advertised as “phoning DDoS”)
- Follow-up calls (to support and reinforce spamming campaigns)

Their prices vary from $5 to $15 per phone conversation, with $5 per call for bulk orders or calls to mules and drops, $8 to $10 per call to businesses (such as online stores), and $15 per call for dating fraud purposes. The threat actor noted that they use phone numbers with the same country codes as the call recipients. The service accepts payments in BTC, WebMoney, and Qiwi and is open for business 24/7, but approved_calls’s service does not extend to CIS countries and they will not make calls in Russian.

-B-

Money laundering services operated by the threat actor “-B-” offer features such as the transfer of BTC into virtual currencies popular in CIS countries such as PerfectMoney and WebMoney. For Russian citizens, money can be directly deposited into “payment cards” (likely referring to prepaid cards). -B- further claims they can deposit or send physical cash to locations throughout the world. -B- is an active member of Verified Forum.



Bitcoin and etc/Webmoney/CASH ALL WORLD: Ввод-Вывод

Уважаемые мемберы!
Представляем Вашему вниманию сервис ввода-вывода следующих валют:

·Bitcoin/Litecoin/Bitcoin Cash/Dash/ETH/USDT
·Webmoney
·Cryptocheck
·AdvCash
·PerfectMoney
·Cash ALL WORLD
·Getbtc
·Plutus
·Vexel

NEWДоступен автоматический вывод криптовалюты на ру карты, 24/7/INSTANT!!!

Заберем/Отдадим нал во всем мире

Figure 6: Money laundering services operated by the threat actor “-B-” (Source: Verified Forum)

[Translation: Bitcoin and etc/Webmoney/CASH ALL WORLD: Buy or Sell
Dear members!
We would like to bring to your attention the service of buying and selling the following currencies:

- *Bitcoin/Litecoin/Bitcoin Cash/Dash/ETH/USDT*
- *Webmoney*
- *Cryptocheck*
- *PerfectMoney*
- *Cash ALL WORLD*
- *Getbtc*
- *Plutus*
- *Vexel*

****NEW*** Available - automated transfer of cryptocurrencies into RU cards, 24/7/INSTANT!!!*
We will pick up/drop off cash all over the world]

国际洗钱公司 *(International Money Laundering Company)*

The entity 国际洗钱公司 (International Money Laundering Company) has been advertising their service on the Chinese-language dark web marketplace United Chinese Escrow Market since its inception in June 2018. It claims to work mostly with repeat customers. For new clients, a $500 deposit is required for any detailed inquiry. The entity claims to be able to move funds both inside China and abroad. The default currencies accepted are RMB, US dollars, and euros. It claims to be able to open Swiss bank accounts for clients without real names. For any new client, the minimum amount for laundering is $50,000, and there is no upper limit. The service fee is dependent on the difficulty of the task and is negotiable. The International Money Laundering Service has no reviews shown on its page but the website statistics show that it conducted 782 transactions and received 105 “likes” at the time of this report.

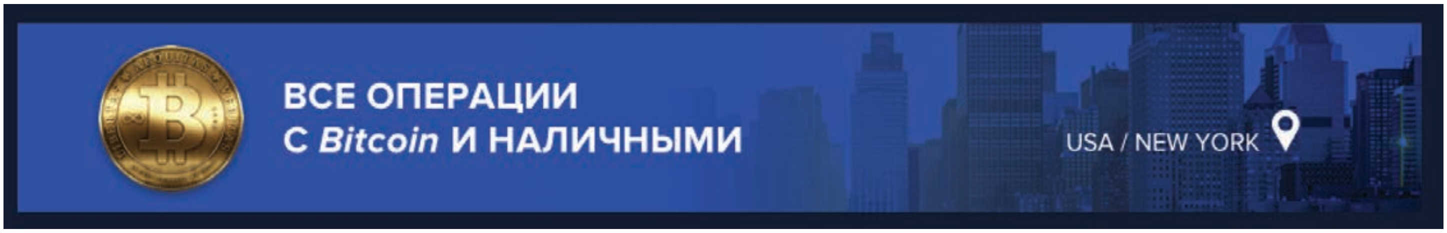


Figure 7: Ad banner on Verified Forum advertising Oneteam Operations in New York, US (Source: Verified Forum)
[Translation: ANY TYPE OF OPERATION WITH Bitcoin AND CASH USA/NEW YORK]

Use in Ransomware Operations

Ransomware operators likely use the multitude of dark web money laundering services operated by threat actors on well-known cybercrime forums, such as Verified Forum. According to messages reviewed via the Verified Forum Direct Messages source dump, actors such as Oneteam engaged with the threat actor danger1488, an operator of Conti ransomware. Deposit address overlaps reveal the use of common money laundering services by different ransomware strains, as we posited in the example of transactions connecting Maze and Egregor. Again, instances of overlap in money laundering services is important information for law enforcement, as it suggests they can disrupt the activity of multiple strains — in particular, their ability to liquidate and spend the cryptocurrency — by taking one money laundering operation offline.

While cryptocurrencies such as Monero offer additional security features and more stringent security measures that enable their users to more easily circumvent law enforcement, threat actors rely heavily on the capability of victims with little background in cryptocurrencies to be able to transfer funds. Separate cryptocurrency mixing services will almost certainly continue to be used by criminal entities to assist in obfuscating their trail, which is still only considered to be pseudo-anonymous.

Additionally, ransomware affiliates of more pronounced groups that operated in 2021, including REvil, expressed reluctance to launch ransomware attacks against companies located within countries that adhere to what they consider to be strict anti-money laundering laws, serving as evidence that affiliates find targets constrained by laws that make them less likely to pay a ransom more difficult to target.

- Gemini Advisory research previously discovered that the REvil affiliate "evil_genius" claimed to be the hacker behind the ransomware attacks against Apex America and the Taiwanese company Quanta Computer. evil_genius had expressed reluctance to launch ransomware attacks against other large Taiwanese companies specifically due to Taiwan's strict anti-money laundering laws.

Despite the lack of forum threads pertaining to affiliate recruitment or updates to certain ransomware families, it is likely these threat actors are indeed present on more prominent dark web forums and chat channels. Insikt Group has observed multiple dark web forum and chat advertisements for those seeking partners with experience in penetration testing or those with access to corporate networks — the type of profile matching used by the "Big Game Hunters" that deploy ransomware on high-value targets for ransoms in the hundreds of thousands or millions of dollars. Cryptocurrency users are advised to protect their earnings by using cold storage such as a USB drive, physical BTC, or a paper or hardware wallet. While this does not guarantee 100% security, disciplined storage practices definitively decrease any potential risk of losing one's cryptocurrency.

Outlook

Ransomware has dominated the cyber threat landscape of 2020 and 2021 so far, and it is often necessary for those ransoms to be laundered before they can be used. Money laundering services will likely remain an essential part of the criminal underground ecosystem. Though privacy-focused cryptocurrencies such as Monero are occasionally referenced as preferred forms of payments within underground services, we anticipate bitcoin to remain the most widely used cryptocurrency across both ransomware and laundering operations. The influx of references throughout the year to digital assets that have not traditionally garnered much attention across open source reporting, such as NFTs, demonstrate that criminal actors are always looking for new opportunities to commit fraud via avenues that may be unfamiliar to defenders. The growing criminal interest in NFTs for various purposes, including laundering funds and delivering malware, demonstrates the need for security and threat intelligence professionals to remain vigilant to new criminal tactics, techniques, and procedures.

Mitigations

Below are mitigation strategies to consider when monitoring for indicators of laundering activity:

- Monitor shops and marketplaces for accounts or terminology relevant to your enterprise.
- Evaluate how third-party companies within your supply chain handle or process cryptocurrency transactions to ensure they are adhering to regulatory requirements.
- Monitor how fraudulent activity adapts in response to the changing demands of consumers of commodities that circulate within underground sources, as exemplified by the rise of new laundering schemes based around NFT technology.
- Consider pursuing opportunities internally to have your organization participate in information sharing initiatives to send and receive intelligence associated with laundering activity.
- When the transfer of money is a necessity, use a method that protects the transaction. For example, many banks, credit cards, and services such as PayPal may offer fraud protection.
- Consider the risks associated with failing to properly adhere to regulatory business processes and policies that may result from your organization’s responsibility to assist with processing transactions such as authorizing.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.