Chainalysis

The 2021 Crypto Crime Report

Everything you need to know about ransomware, darknet markets, and more

February 16, 2021

Table of Contents

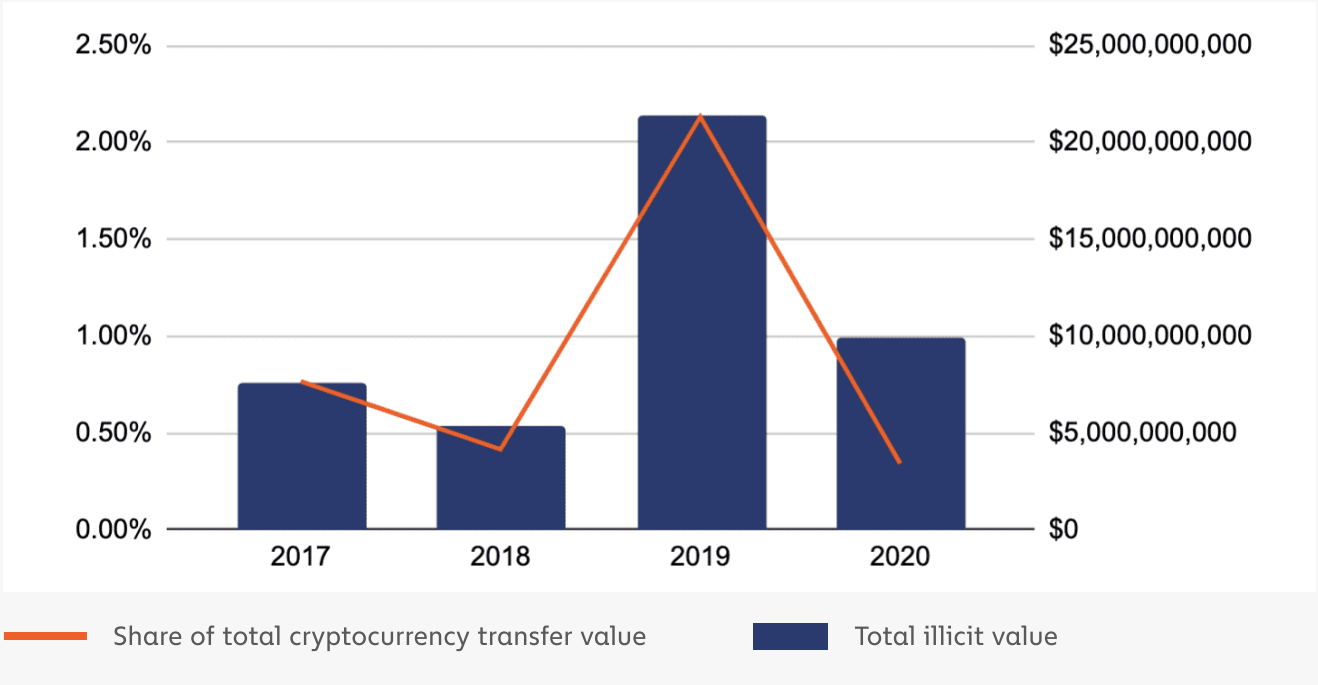
Introduction

2020 Crypto Crime Summarized: Scams and Darknet Markets Dominate by Revenue, But Ransomware Is the Bigger Story

2020 was an incredible year for cryptocurrency. Despite the devastation wrought by the worldwide Covid-19 pandemic, Bitcoin has shattered its previous price records, largely driven by the increased demand from institutional investors that many in the cryptocurrency community have long speculated would drive the asset to new heights.

However, cryptocurrency remains appealing for criminals, primarily due to its pseudonymous nature and the ease with which it allows users to instantly send funds anywhere in the world, despite its transparent and traceable design. But the good news is that cryptocurrency-related crime fell significantly in 2020.

Total cryptocurrency value sent and received by illicit entities vs. Illicit share of all cryptocurrency activity | 2020



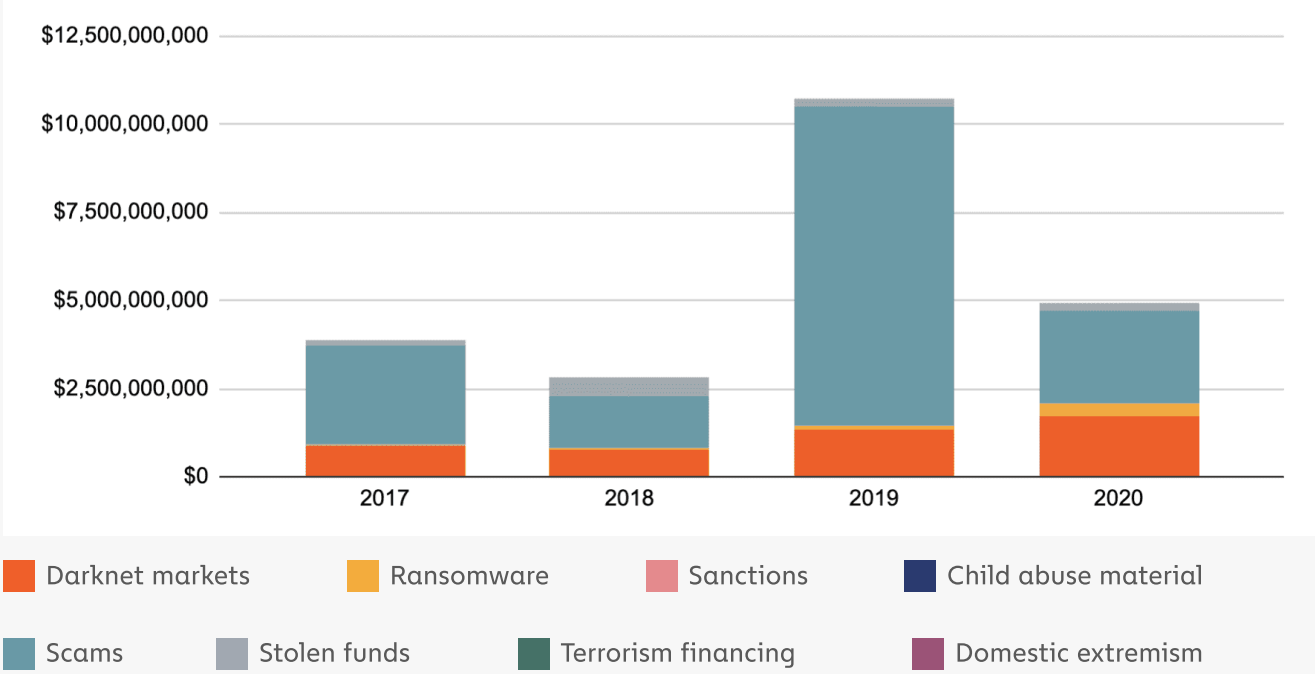
In 2019, illicit activity represented 2.1% of all cryptocurrency transaction volume or roughly $21.4 billion worth of transfers. In 2020, the illicit share of all cryptocurrency activity fell to just 0.34%, or $10.0 billion in transaction volume. One reason the percentage of illicit activity fell is because overall economic activity nearly tripled between 2019 and 2020.

We should note that at the time of writing last year's report, we reported 2019's illicit share of cryptocurrency activity to be 1.1%. The reason for the change is the identification of more addresses associated with illicit activity that was active in 2019. Most of those addresses were related to scams that had yet to be identified as such, primarily related to the PlusToken scam. Some are related to previously unreported ransomware attacks. For that reason, we should expect 2020's reported illicit activity numbers to rise over time as well.

Regardless, the good news is three-fold: Cryptocurrency-related crime is falling, it remains a small part of the overall cryptocurrency economy, and it is comparatively smaller to the amount of illicit funds involved in traditional finance.

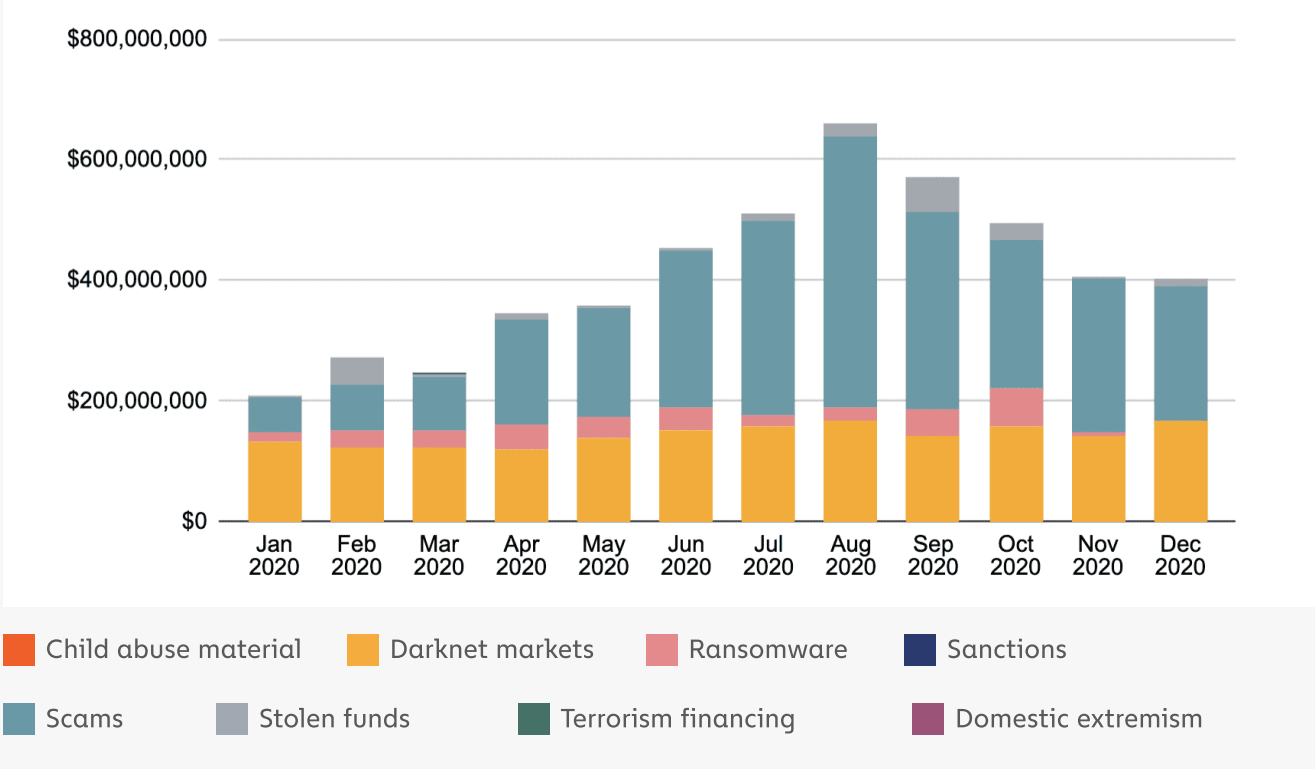
What kinds of crime drove that 0.34% of cryptocurrency transactions associated with illicit activity in 2020?

Total cryptocurrency value received by illicit entities | 2017 - 2020



The graph above shows which crime types received the most cryptocurrency in aggregate from 2017 through 2020. Note that this graph differs from the one above it in that it only tracks cryptocurrency received, which we generally associate with criminal revenue, rather than cryptocurrency sent from illicit addresses, which we generally associate with money laundering. The graph below shows the monthly amount received by different types of criminal entities on a monthly basis throughout the year.

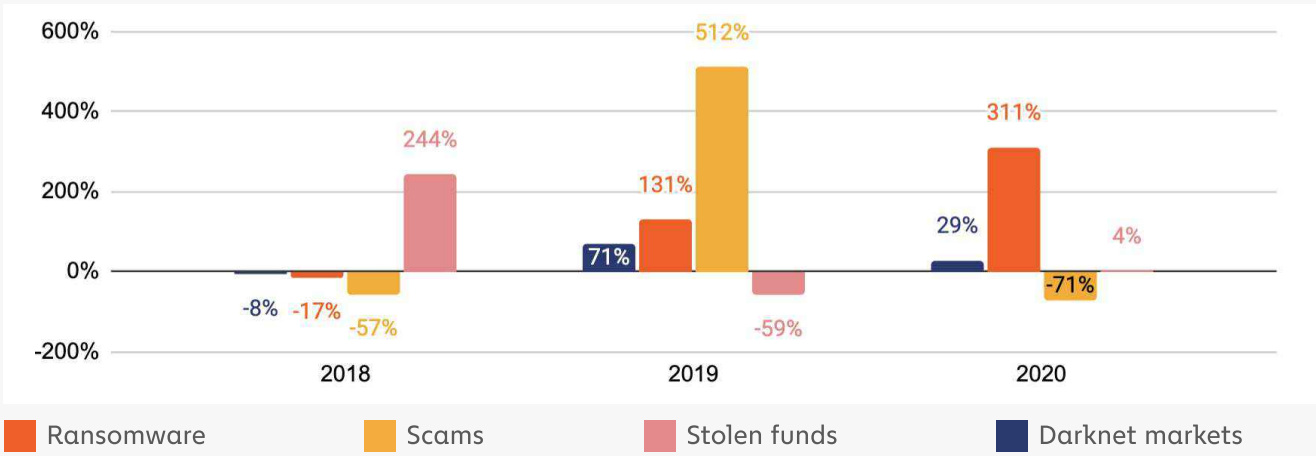
Total cryptocurrency value received by illicit entities | 2020



As was the case in 2019, scams made up the majority of all cryptocurrency-related crime, at 54% of illicit activity, representing roughly $2.6 billion worth of cryptocurrency received. However, both the raw value and share of all criminal activity represented by scams is much smaller than in 2019, as there were no scams in 2020 comparable to those like the enormous PlusToken Ponzi scheme, which took in over $2 billion from millions of victims. Darknet markets were once again the second-largest crime category, accounting for $1.7 billion worth of cryptocurrency activity, up from $1.3 billion in 2019.

However, the big story for cryptocurrency-based crime in 2020 is ransomware. That may sound counterintuitive, as ransomware accounted for just 7% of all funds received by criminal addresses at just under $350 million worth of cryptocurrency. But that figure represents a 311% increase over 2019. No other category of cryptocurrency-based crime rose so dramatically in 2020, as Covid-prompted work-from-home measures opened up new vulnerabilities for many organizations.

Crime categories by percentage increase in cryptocurrency received,
| 2018 - 2020



Keep in mind that ransomware estimates should always be considered lower bounds due to underreporting. The 2020 figure for total ransomware payments will likely grow as we identify more addresses associated with different strains, particularly in the later months of the year. Looking beyond the numbers, we also must note that ransomware is uniquely destructive in that attacks can cripple local governments and businesses for weeks, including several hospitals last year in the midst of the pandemic. When we consider the total economic losses not just from payments, but from businesses and governments being taken offline in attacks, some experts estimate that ransomware cost $20 billion in economic losses in 2020.

In this report, we'll delve into not just the data on cryptocurrency-based crime, but the story behind the numbers as well. We'll analyze multiple trends, including:

- Why the ransomware ecosystem may be smaller than it appears at first glance, and what that means for law enforcement
- How a small group of shady cryptocurrency services, mostly operating on top of large exchanges, conduct most of the money laundering that cybercriminals rely on to make cryptocurrency-based crime profitable
- DeFi platforms' unique vulnerability to hacking, as well as how cybercriminals such as those of the North Korea-affiliated Lazarus Group utilize DeFi platforms for money laundering
- Why so many darknet markets went offline in 2020
- And more!

By understanding these trends, law enforcement, regulators, and the private sector can work together to ensure cryptocurrency-based crime continues to fall. Thank you for reading, and keep in mind that you can reach out to Chainalysis with any questions at contact@chainalysis.com.

Money Laundering

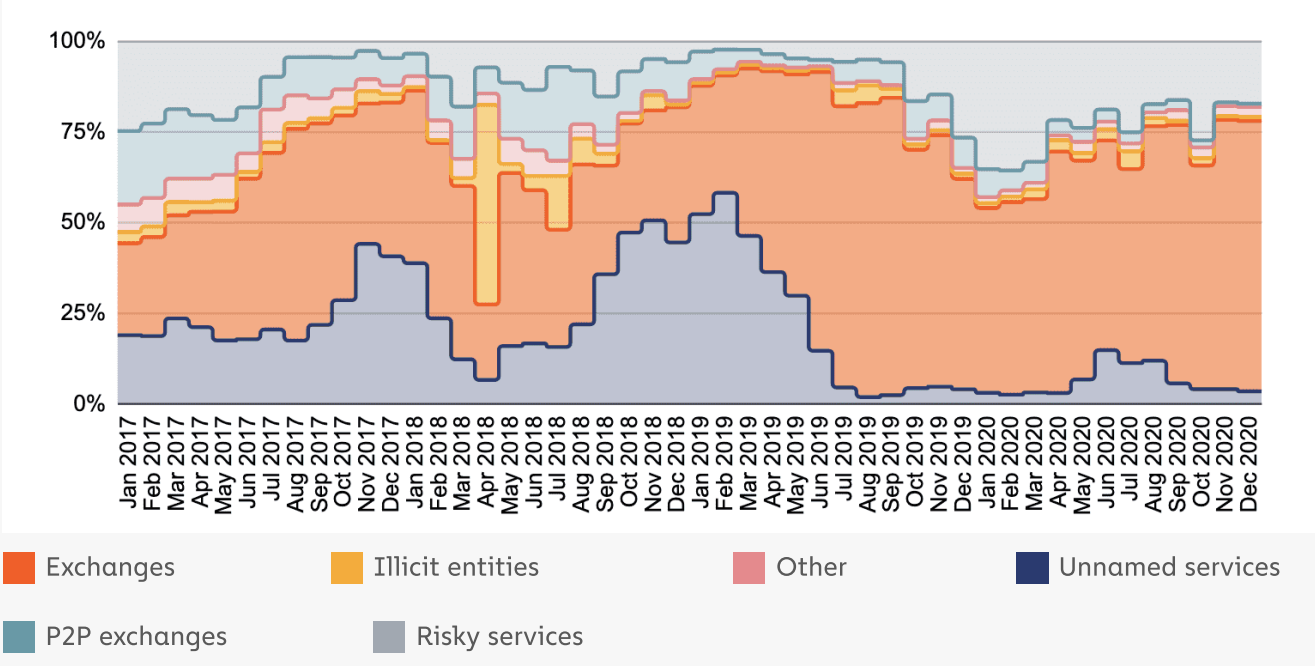
270 Service Deposit Addresses Drive 55% of Money Laundering in Cryptocurrency

Money laundering is the key to cryptocurrency-based crime. The primary goals of cybercriminals who steal cryptocurrency, or accept it as payment for illicit goods, are to obfuscate the source of their funds and convert their cryptocurrency into cash so that it can be spent or kept in a bank. Of course, thanks to the efforts of law enforcement and compliance professionals around the world, cybercriminals can't simply send their ill-gotten cryptocurrency to an exchange and cash out as a normal user would. Instead, they rely on a surprisingly small group of service providers to liquidate their crypto assets. Some of these providers specialize in money laundering services while others are simply large cryptocurrency services and money services businesses (MSBs) with lax compliance programs. Investigators could significantly damage cybercriminals' ability to convert cryptocurrency into cash by going after these money laundering service providers, thereby reducing the incentives for cybercriminals to use cryptocurrency in the first place.

Who are these money laundering service providers? First, let's look at the services that have received funds from criminal sources over the last few years.

Destination of all cryptocurrency sent from illicit addresses, monthly

| Jan '17 - Dec '20

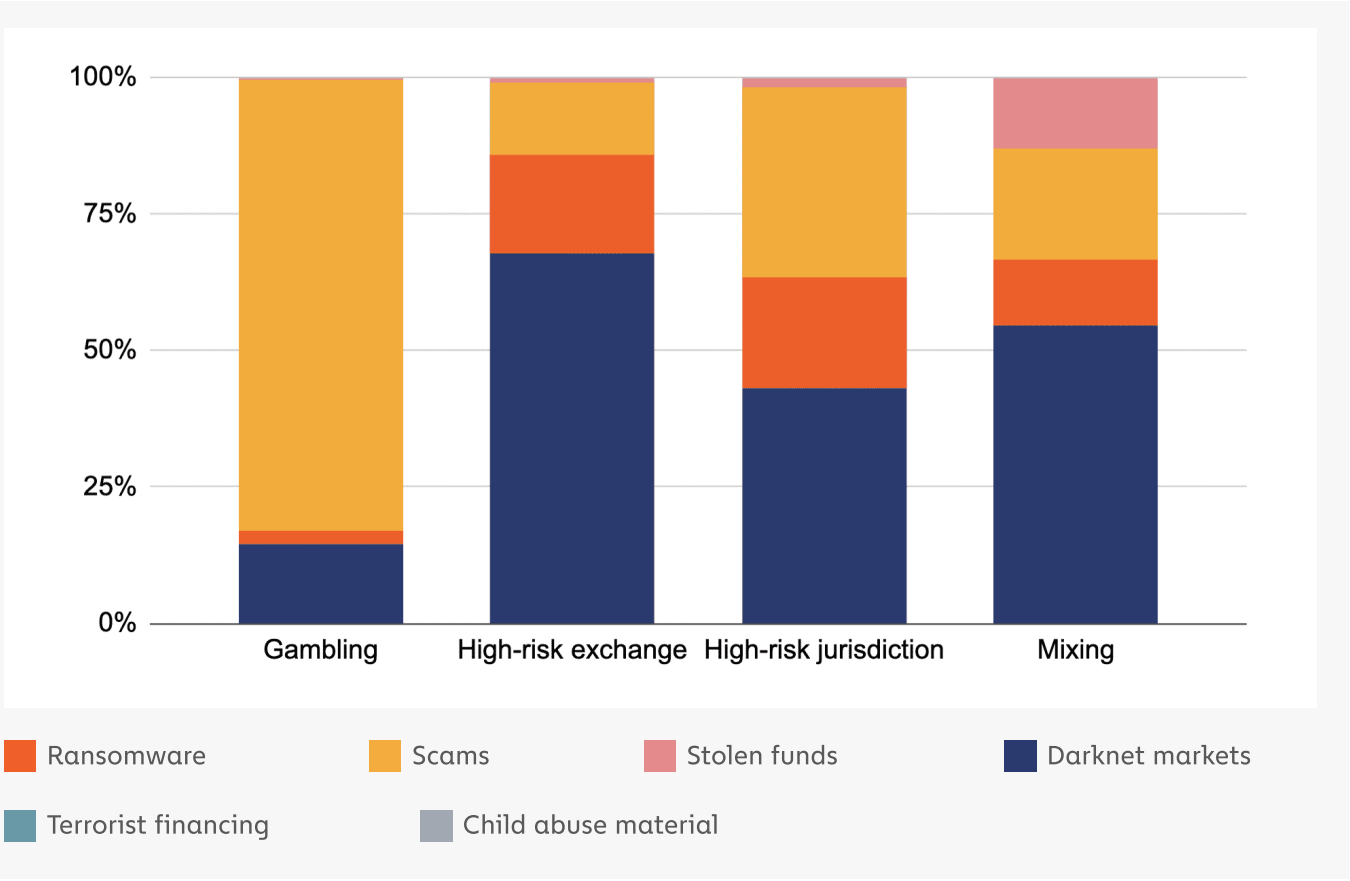


Currencies included: BAT ,BCH, BTC, ETH, LTC, MKR, OMG, PAX, TUSD, USDC, USDT

Historically, mainstream exchanges have been the primary destination of illicit cryptocurrency, and that didn't change in 2020. In fact, the share of all illicit cryptocurrency received by exchanges grew slightly in 2020.

We also see significant volume moving from illicit addresses to services we categorize as "risky," including high-risk exchanges, gambling platforms, mixers, and services headquartered in high-risk jurisdictions. Interesting trends arise when we look at the specific risky services receiving funds from different types of cryptocurrency-based crime.

Risky services receiving illicit funds by crime type | 2020

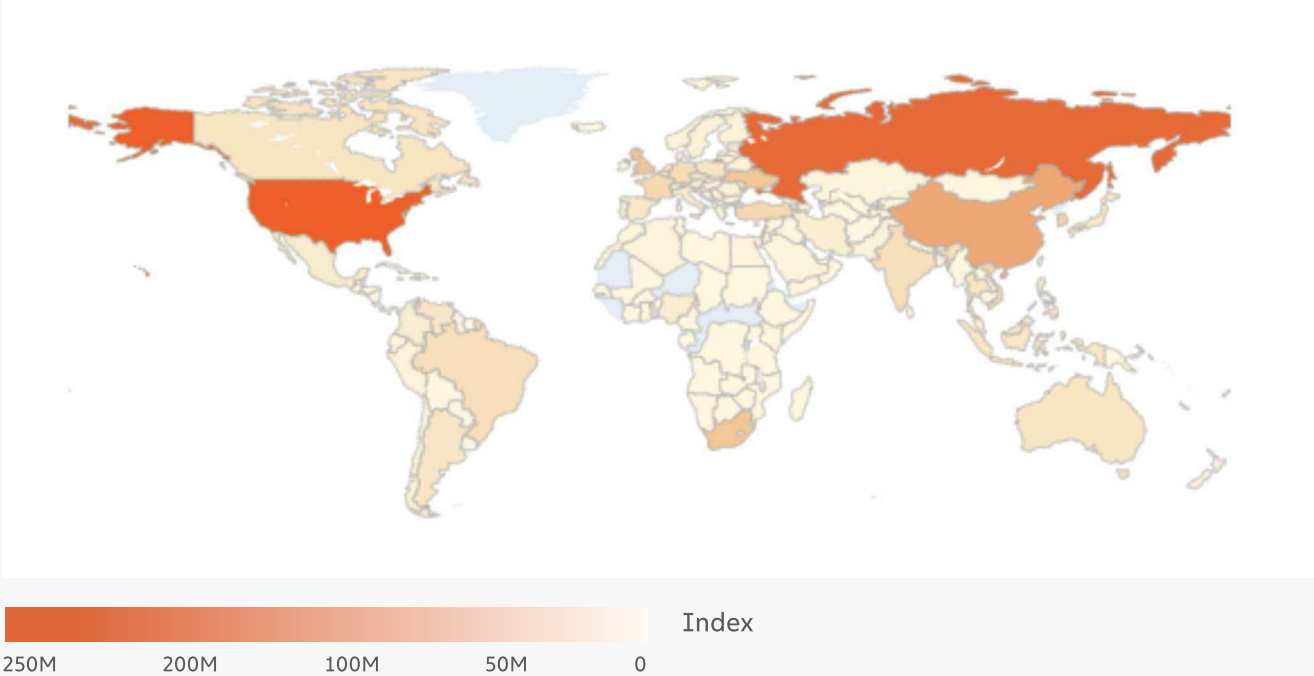


Currencies included: BCH, BTC, ETH, LTC, OMG, PAX, USDC, USDT

The most popular risky service categories for money laundering are similar for each crime category, with scams being the biggest exception. Scammers are much more likely than other cybercriminals to move funds to gambling platforms — a trend that began in 2020 and is best exemplified by the Mirror Trading International scam we cover elsewhere in this report — and to services headquartered in high-risk jurisdictions.

We can also see interesting trends when we look at money laundering through a geographic lens.

Destination of Funds Leaving Illicit Services | 2020



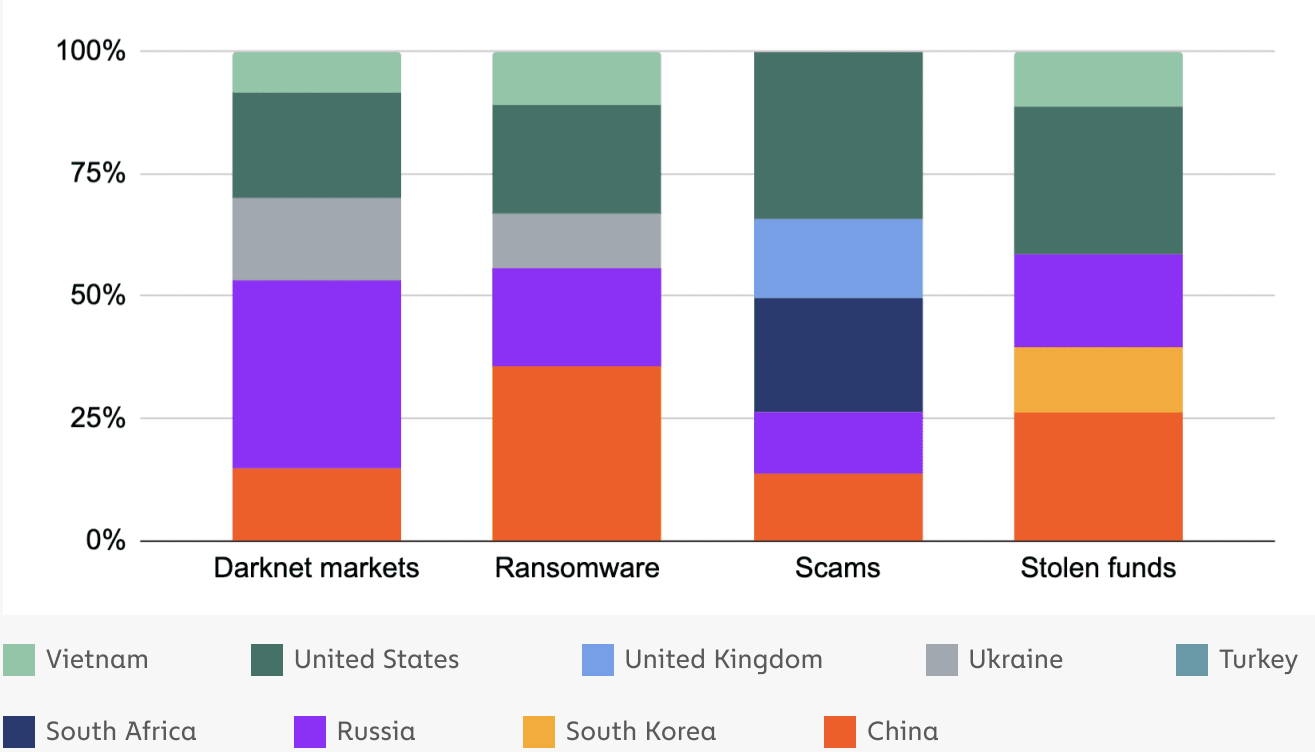
Currencies included: BAT, BCH, BTC, ETH, LTC, MKR, OMG, PAX, TUSD, USDC, USDT

The following countries receive the highest volume of cryptocurrency from illicit addresses, based on the breakdowns of the locations of the users for the services receiving those funds:

- United States
- Russia
- China
- South Africa
- United Kingdom
- Ukraine
- South Korea
- Vietnam
- Turkey
- France

However, patterns emerge when we look at the geographic destination of funds by crime category:

Top 5 countries estimated to receive illicit funds by crime type | 2020



Note: County estimations based on web traffic of services receiving illicit funds

The first trend that stands out is Russia's receipt of a disproportionately large share of darknet market funds, which is mostly due to Hydra. Hydra is the world's largest darknet market by revenue, and exclusively serves Russia and other Russian-speaking countries in Eastern Europe. China also stands out for receiving a disproportionate share of funds sent from addresses associated with stolen funds and ransomware. Some of this may come from cryptocurrency theft and ransomware activity associated with Lazarus Group, a cybercriminal syndicate linked to the North Korean government. A recent Department of Justice complaint identified two Chinese nationals who worked with Lazarus Group operatives to launder cryptocurrency that the group stole from exchanges. Other China-based cryptocurrency users could be engaged in similar activity. Finally, the United States is slightly overrepresented in funds received from addresses associated with scams and stolen funds.

Who are the money laundering service providers?

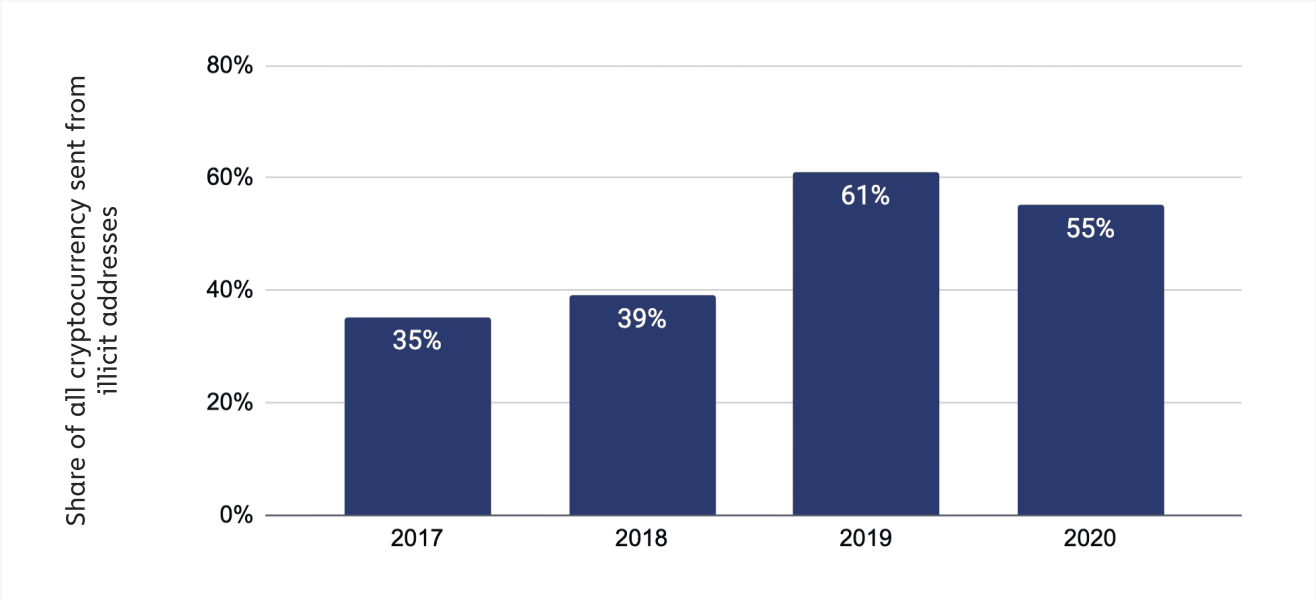
As we discuss above, most funds sent from illicit addresses make their way to deposit addresses at mainstream exchanges or at services we categorize as "risky," including high-risk exchanges (e.g. exchanges with lax or nonexistent compliance programs), mixers, gambling platforms, or services headquartered in high-risk jurisdictions. Some of the deposit addresses receiving illicit funds are likely controlled by the cybercriminals sending the funds in the first place. But we know from our law enforcement partners and our own investigations that many of these deposit addresses belong to third-party services who, sometimes explicitly or implicitly, provide money laundering services to cybercriminals.

These third-party services largely fall into a broad category called "nested services." Nested services operate within one or more larger exchanges, tapping into those exchanges' liquidity and trading pairs. From a blockchain analysis standpoint, this means that by default, nested services' transactions will show up as having been conducted on the underlying platform that hosts the nested service. Common examples of nested services include Over the Counter (OTC) brokers and instant exchangers. There's a huge range in how much illicit transaction volume nested services process — some are just as compliant as mainstream exchanges, while others appear to cater specifically to cybercriminals. Many appear to be large businesses for whom illicit activity is just a small share of total transaction volume, suggesting that these services are likely inadvertently moving illicit funds due to lax compliance policies, but could continue to operate if they stopped. However, some of these deposit addresses receive such a high percentage of their funds from illicit addresses that it seems impossible the activity could be accidental, or that the services could even continue to operate without serving cybercriminals.

Below, we'll share what we know about the deposit addresses facilitating money laundering, starting with the services hosting them.

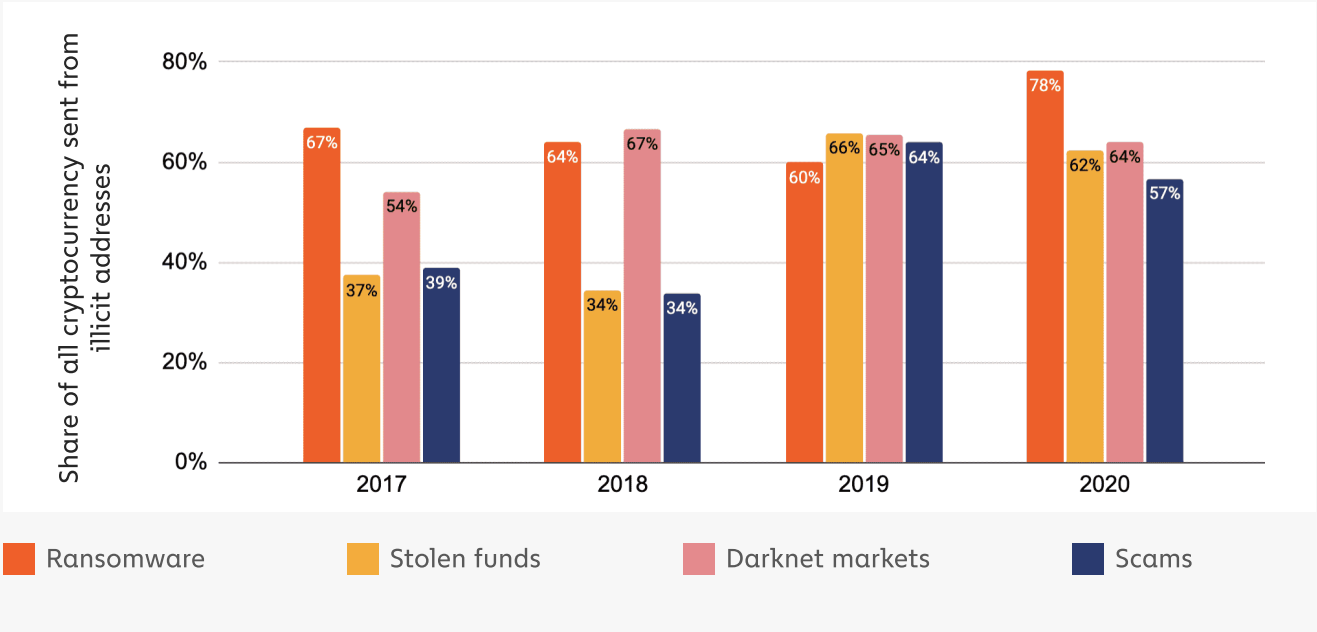
Cryptocurrency sent from illicit addresses tends to wind up at just a few services. Below, we show the share of all illicit funds going to the five services receiving the most illicit funds each year since 2017, both overall and broken down by crime type. The top two services receiving illicit funds have remained constant over the three years we studied, with some change in the third, fourth, and fifth spots. Together, the top two take in more than the other three do combined in any given year. Overall in 2020, these top five services received 55% of all funds moved from illicit addresses.

Share of all illicit funds going to top 5 illicit fund receiving services, | 2017 - 2020



Currencies included: BAT, BCH, BTC, ETH, LTC, MKR, OMG, PAX, TUSD, USDC, USDT

Share of all illicit funds going to top 5 illicit fund receiving services by crime type | 2017 - 2020

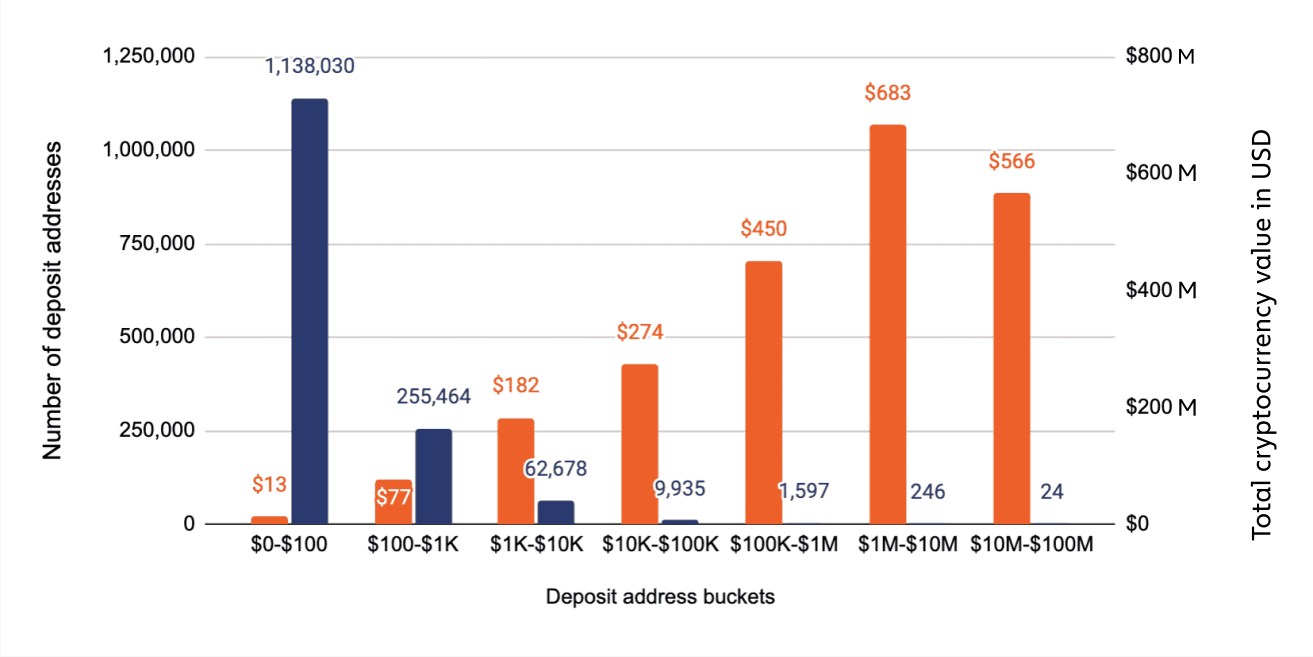


Currencies included: BAT, BCH, BTC, ETH, LTC, MKR, OMG, PAX, TUSD, USDC, USDT

Notably, addresses associated with ransomware have the highest share of sending activity concentrated to the top five services, at 78% in 2020.

But what happens if we go one level deeper from the services and look at the individual deposit addresses? In the graph below, we look at all service deposit addresses that received any illicit funds in 2020, broken down by the range of illicit funds received.

All illicit cryptocurrency received by service deposit addresses | 2020



Deposit addresses bucketed by total illicit cryptocurrency received

Total illicit value received

Number of deposit addresses

Currencies included: BTC

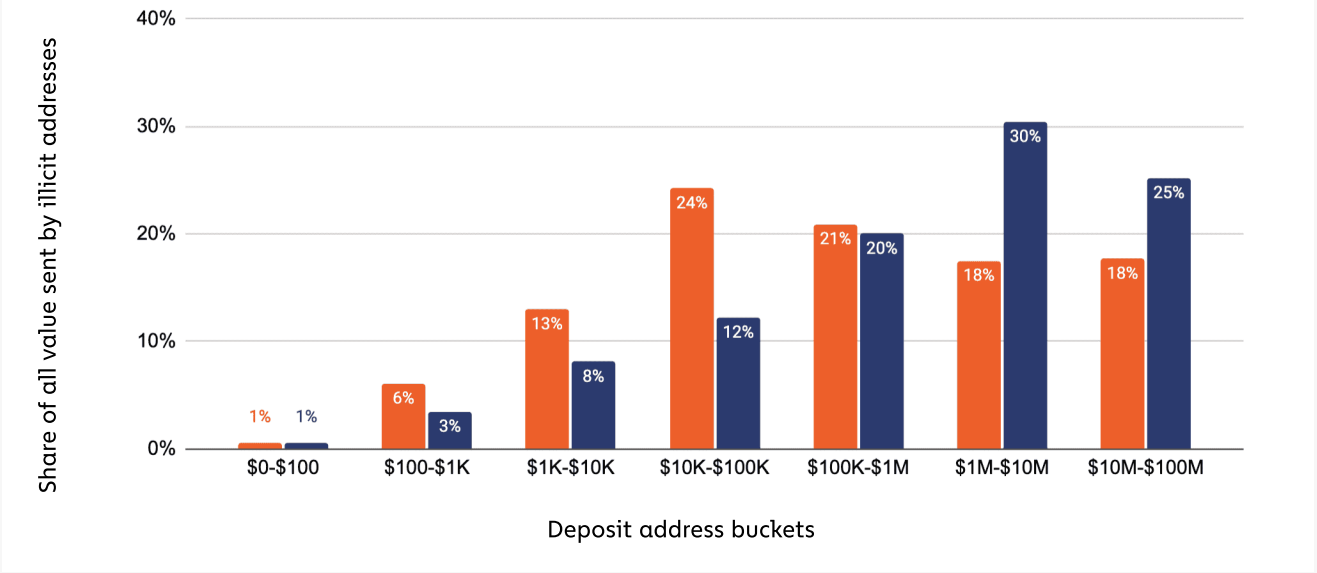
How to read this graph: This graph shows service deposit addresses bucketed by how much total illicit cryptocurrency value each address received individually in 2020. Each blue bar represents the number of deposit addresses in the bucket, while each orange bar represents the total illicit cryptocurrency value received by all deposit addresses in the bucket. Using the first bucket as an example, we see that 1,138,030 deposit addresses received between $0 and $100 worth of illicit cryptocurrency, and together all of those deposit addresses received a total of $13 million worth of illicit cryptocurrency.

Money laundering activity is even more concentrated at the deposit address level. In fact, the data above shows that a group of **just 1,867 deposit addresses received 75% of all cryptocurrency value sent from illicit addresses in 2020. A smaller group of 270 deposit**

addresses received 55%. Thinking in terms of raw value rather than percentages, those 270 addresses collectively received $1.3 billion worth of illicit cryptocurrency in 2020, and a smaller group of just 24 received over $500 million worth of illicit cryptocurrency in 2020.

This level of concentration is greater than in 2019. Below, we look at how the shares of all illicit cryptocurrency received by deposit addresses in each of the buckets shown above changed from 2019 to 2020.

Share of all illicit value received by deposit addresses in each bucket, 2019 vs. 2020

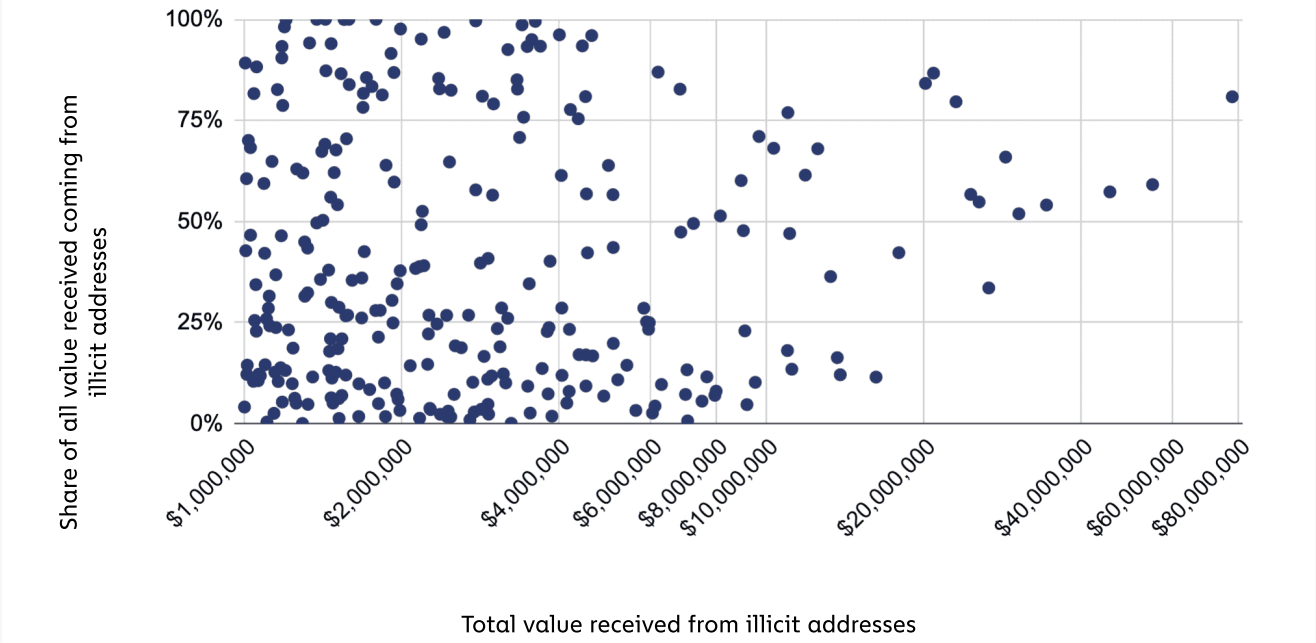


Currencies included: BTC

In particular, we see a much greater share of illicit cryptocurrency going to addresses taking in between $1 million and $100 million worth of cryptocurrency per year.

We believe the growing concentration of deposit addresses receiving illicit cryptocurrency reflects cybercriminals' increasing reliance on a small group of OTC brokers and other nested services specializing in money laundering. In order to investigate further, we decided to look more closely at the 270 deposit addresses that received more than $1 million worth of cryptocurrency from illicit addresses in 2020. In the scatter chart below, we plot those addresses based on the total amount they've received from illicit addresses,versus the share those illicit funds make up of the addresses' total amount received.

Deposit addresses receiving over $1M worth of illicit cryptocurrency in 2020: Total illicit value received vs. illicit share of all value received



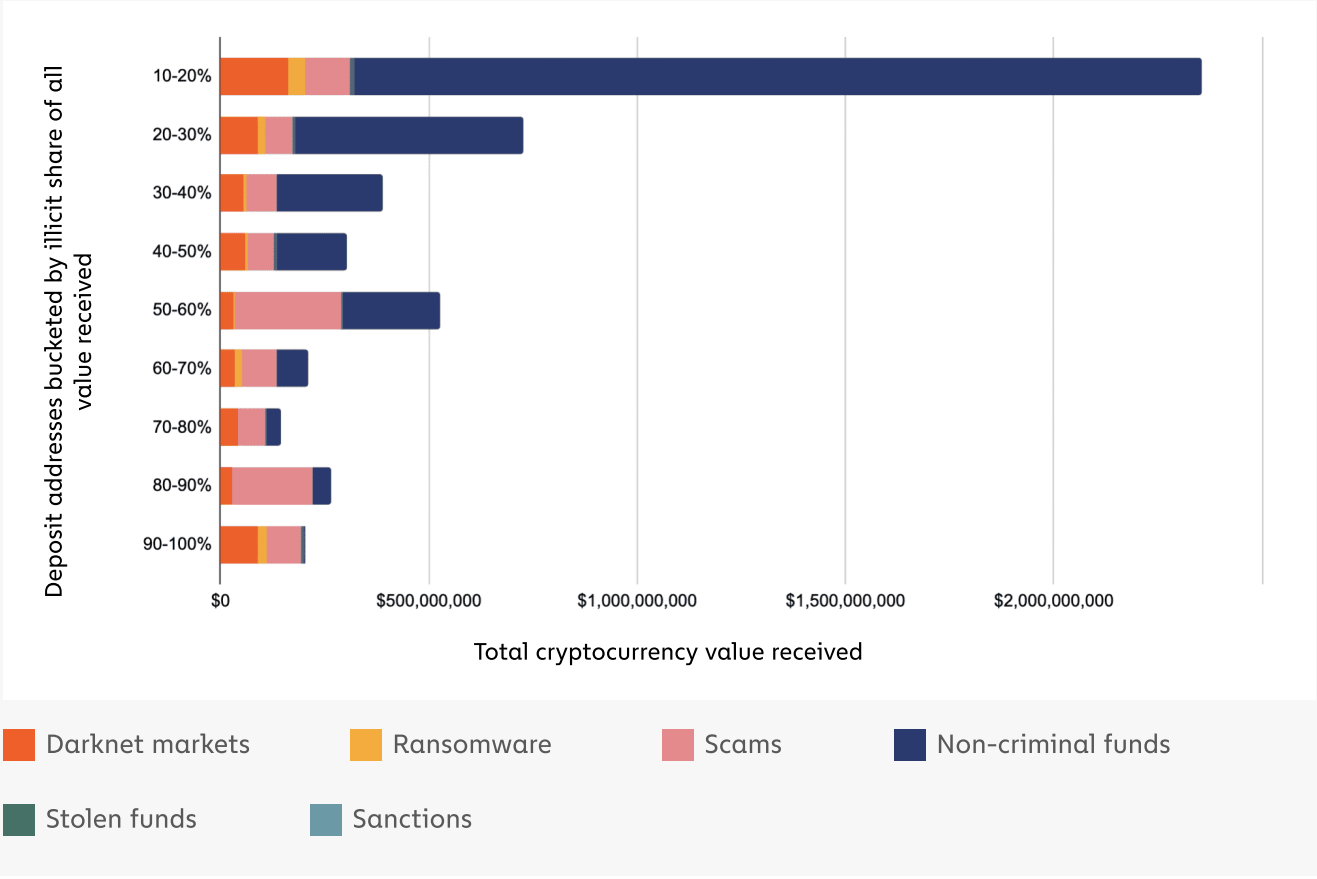
Currencies included: BTC

An interesting trend emerges when we look at the 270 deposit addresses that facilitate the most money laundering shown above. Though they individually and collectively may facilitate a great deal of money laundering, legitimate activity also makes up a significant share of total transaction volume for many of these deposit addresses, especially those that received less than $25 million in cryptocurrency from illicit addresses. In fact, illicit addresses account for under 10% of total cryptocurrency received for many of these addresses, even moreso below the $10 million mark. This suggests that the money laundering those addresses facilitate could simply be inadvertent and due to shortcomings in the compliance programs of the nested services controlling them.

However, we see no such evidence for any of the deposit addresses receiving over $25 million worth of cryptocurrency from illicit addresses. All of those deposit addresses receive at least 34% of their total funds from illicit sources, with that figure rising above 50% for most of them. It would be difficult to believe that these services are receiving such a high percentage of funds from illicit addresses by accident — those of them that represent nested services could likely not survive as businesses without those funds — so we characterize those addresses as primarily serving cybercriminals.

Below, we expand our set of deposit addresses to include all that received any funds from illicit addresses in 2020, and break them down by the share of all funds they receive that comes from illicit addresses. We see that the wallets receiving the most illicit funds overall are those for whom illicit funds make up the biggest percentage of all funds received. In other words, the small group of actors laundering the most money seem to specialize in it.

Total cryptocurrency value received by deposit addresses grouped by illicit share of all funds received | 2020



Currencies included: BTC

55% of all illicit funds moving to services end up at deposit addresses for which illicit addresses supply 50% or more of all funds. That figure rises to 71% for deposit addresses with 30% or more of all funds received coming from illicit addresses. In other words, a significant share of money laundering in cryptocurrency isn't flying under the radar at big services who can't sift through transactions to spot it, but is being actively facilitated by nested services for whom money laundering is a key part of the business model. **Law enforcement could significantly hamper cybercriminals' ability to convert cryptocurrency into cash by identifying and prosecuting the owners of these deposit addresses.** In addition, this shows that the services hosting these deposit addresses, most of which belong to nested services, need to be more diligent in their transaction monitoring. They too could make the cryptocurrency ecosystem safer by cracking down on the worst offenders.

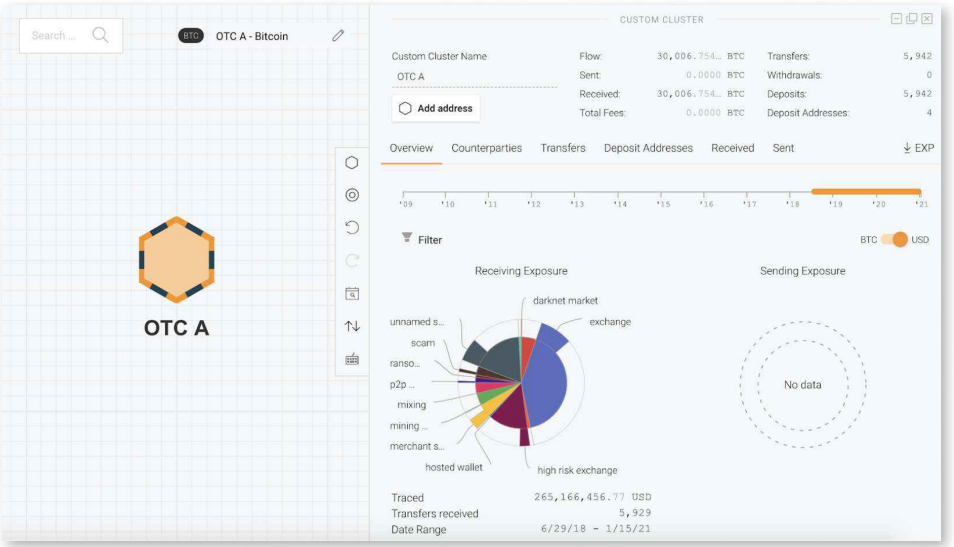
We should also note that even the non-illicit share of funds received for some of these addresses should be treated with suspicion, as they could represent money laundering associated with offline criminal activity — in other words, bad actors criminally-obtained exchanging fiat money for cryptocurrency in an effort to hide it. We'll explore this element of cryptocurrency money laundering in our case studies at the end of this section.

Overall, what the data makes clear is that most illicit funds travel to service deposit addresses for whom money laundering makes up a huge portion of their activity, to the point that many of them appear to have no other purpose. A smaller but still significant portion also goes to deposit addresses doing a high volume of legitimate transactions, which could allow the illicit activity to fly under the radar, reinforcing the need for compliance professionals and investigators to stringently assess all deposit addresses — especially those of nested services.

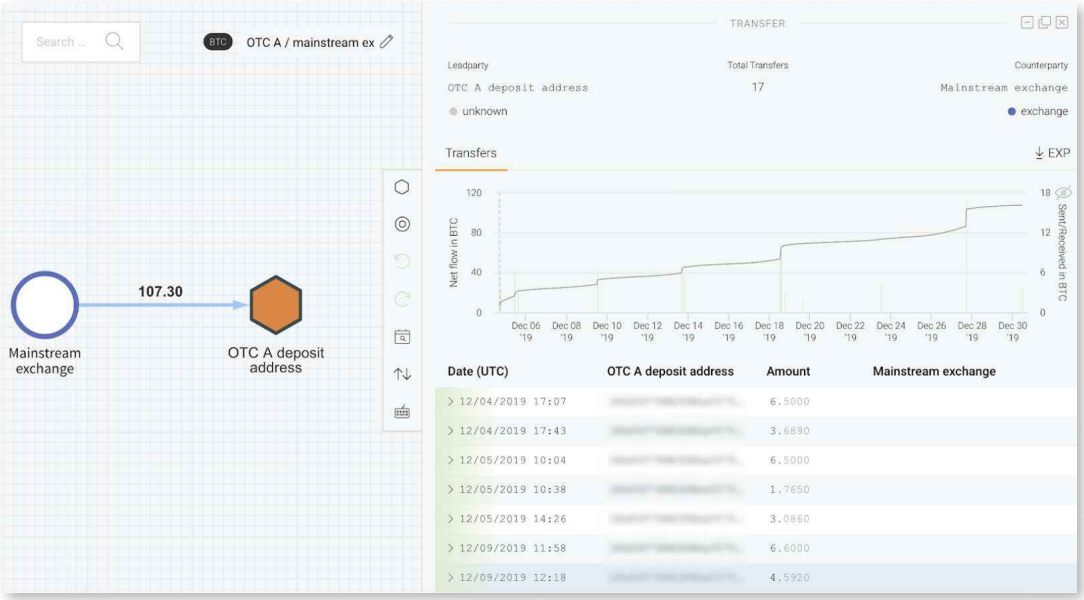
Case study: Russia-based money laundering ring helps ransomware attackers and darknet market vendors cash out

By examining the activity of deposit addresses with significant exposure to illicit addresses, we can learn more about how cybercriminals launder funds through different services, often switching between cryptocurrencies. Below, we'll break down the activity of what appears to be a money laundering ring helping cybercriminals convert large sums of cryptocurrency into cash.

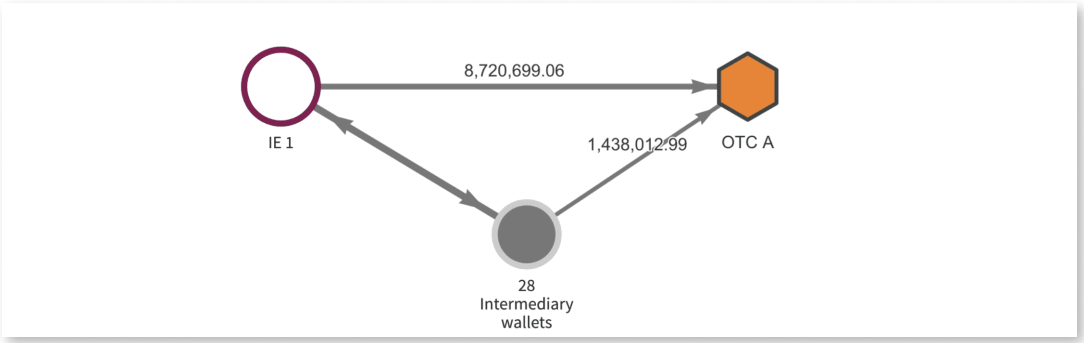
This money laundering ring involves multiple services. The first is a large, Russia-based OTC broker that nests primarily at two highly popular exchanges, which we'll refer to as **OTC A**. We've attributed seven deposit addresses at those two exchanges to OTC A, three of which are within the group of 270 that received more than $1 million in illicit funds in 2020. Below, we break down OTC A's Bitcoin received, much of which comes from illicit addresses.



OTC A has received over $265 million worth of cryptocurrency since becoming active in 2018. More than $2 million worth has come from ransomware strains such as Maze and Ryuk. Additionally, it's received $13.9 million worth of cryptocurrency from darknet markets — primarily Hydra — and $8.1 million worth or cryptocurrency from several scams. Overall, 9.29% of all Bitcoin received by OTC A comes from illicit addresses. OTC A also receives substantial funds without previous transaction history from other exchanges, meaning the funds were initially deposited in fiat form. We believe some of these may be linked to off-chain crime, meaning crime whose proceeds aren't initially derived in cryptocurrency. Below, we see an example of some of those funds — OTC A has received over 107 Bitcoin from a mainstream exchange that was converted directly from fiat.



It's possible that OTC A helps cybercriminals convert at least some of the Bitcoin they send into cash. However, our data also shows that OTC A makes significant transactions in Tether ERC-20 tokens (USDT_ETH). More specifically, it exchanges a good deal of USDT_ETH with another Russia-based service, this one an instant exchanger. We'll refer to it as Instant Exchanger 1, or IE 1. IE 1 allows users to exchange between cryptocurrencies like Bitcoin, Ether, and Tether, and a variety of different electronic fiat currencies powered by e-wallet providers like Perfect Money.



According to Reactor, OTC A has received significant sums of USDT_ETH from IE 1 — $8.7 million worth directly, and another $1.4 million through a network of 28 intermediary wallets. We don't know if OTC A sends Tether (or Bitcoin for that matter) to IE 1 — since all of OTC A's deposit addresses are hosted at larger services, it's impossible to trace the cryptocurrency they send. But it's worth noting that the intermediary wallets sitting between OTC A and IE 1 both send and receive large amounts of USDT_ETH to and from IE 1. Based on that, we believe it's possible that OTC A also sends large sums of USDT_ETH to IE 1 on behalf of cybercriminal clients, allowing them to cash out at IE 1.

This is just one example of how funds can be moved from illicit addresses to OTC brokers and other types of nested services.

Case study: Drug ring operating in the UK and Australia Shows How Cryptocurrency Can Be Used to Launder the Proceeds of Offline Crime

Nearly all of the illicit activity we cover in this report consists of cybercrime we'll refer to as "cryptocurrency native", meaning crime that is practically dependent on cryptocurrency or inherently intertwined with it. Take darknet markets, for example. Darknet markets as we know them run entirely on cryptocurrency, with millions of dollars' worth flowing through their centralized networks of wallets every day. Since these services actively solicit new customers online, it's not all that difficult for us to identify their cryptocurrency addresses and track their transaction activity.

But many investigators have wondered how often criminals engaged in traditional, non-cryptocurrency native crime — traditional drug trafficking, for example — are laundering their ill-gotten funds by converting them into cryptocurrency and sending them around the world. In these cases, the funds on-ramp into cryptocurrency directly from fiat rather than move from known illicit addresses, so it's harder to both investigate this activity in individual cases or to size it in the aggregate.

However, we do know that it's happening. Below, we'll share a case study of how a drug trafficking ring operating in the UK and Australia incorporated cryptocurrency into its money laundering strategy.

How the Harrod's drug trafficking ring used cryptocurrency

In 2019, police arrested multiple members of a drug trafficking ring operating in the UK and Australia. Notably, the traffickers in this case were inserting cocaine into items at the department store Harrod's, then having the unwitting staff send those items to addresses in Australia where co-conspirators could collect them.

However, our focus is on the methods they used to send drug money overseas to suppliers. The Harrod's ring followed a common strategy that many criminal enterprises use:

1. The **organized crime group (OCG)** contacts a **controller** who is in charge of a money laundering operation, and tells the controller how much illicit cash they need to move, the **counterparty** receiving it, and where that counterparty is located. In the Harrod's case, the OCG was a drug trafficker in the UK who would tell the controller they need to move funds — usually a sum in the hundreds of thousands — to their drug supplier.

2. The controller will then contact one of the many **coordinators** they work with whose job it is to ensure the money gets to the correct counterparty.

3. The OCG will text a picture of a bill to the controller with the serial number visible. The controller will pass this image on to the coordinator, who passes it to the **collector** tasked with physically receiving the cash. (We'll explain why later.)

4. Through the controller, the coordinator will communicate to the OCG the location where the cash will be handed off. The two parties will share other details, such as the make and model of the vehicles the individuals making the exchange will be driving. This is done to limit the risk of the meeting being infiltrated by police.

5. The OCG will then pass the bill from the picture in step 4, along with the cash to be transferred, to a **courier**. The courier then meets the collector at the designated place and time.

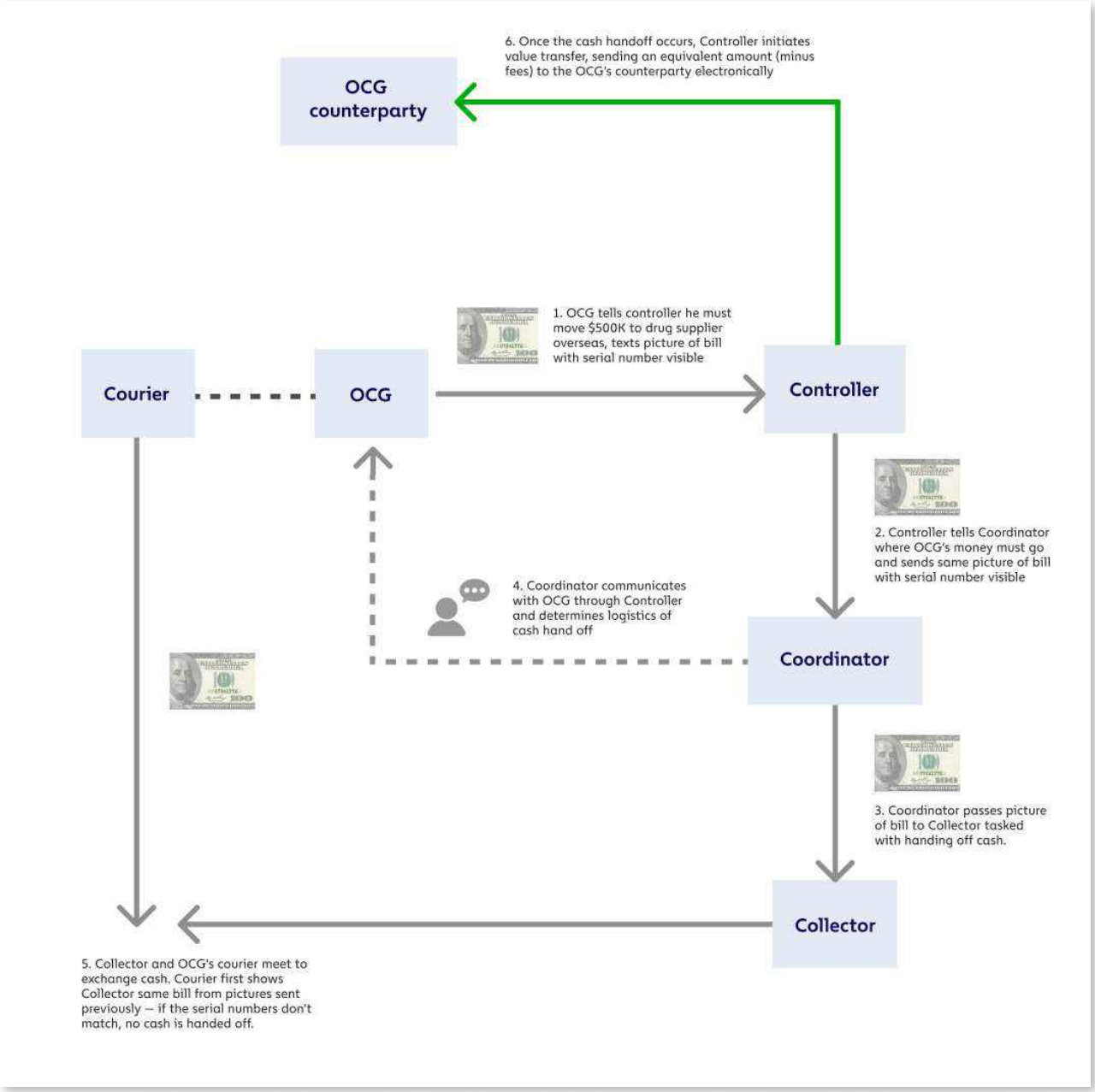
6. Upon meeting, the courier will pass the bill from the picture to the collector. The collector then checks to make sure the serial number matches the one in the picture he received. The transaction will not take place if they do not match. This is done to ensure to the collector that the courier, whom he's never met, is the correct person.

7. If the serial numbers match, the courier will hand the full amount of cash to be transferred to the collector.

8. The collector will communicate to the controller that the cash has been handed over. At that point, the controller conducts a **value transfer process**, whereby money is transferred electronically to a coordinator in the OCG counterparty's location. Traditionally, the electronic transfer is done through banks or traditional money services businesses (MSBs).

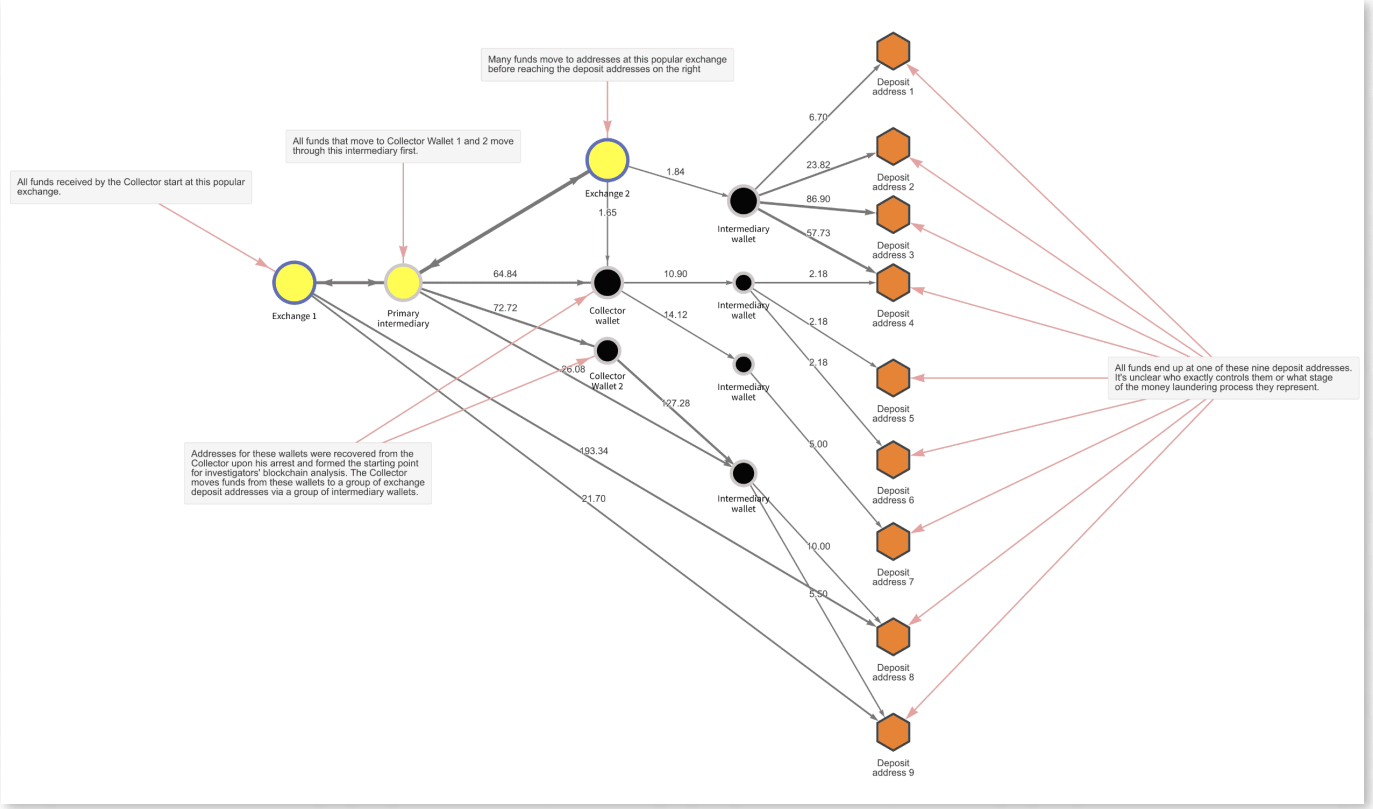
9. The controller and new coordinator then arrange for the same process described in steps 1-7 to be conducted in reverse in the OCG counterparty's location so that the counterparty receives an equivalent amount of cash — importantly, not the same cash handed over in the OCG's location.

We've condensed these steps in the diagram below:



The Harrod's drug ring followed this exact process, but with one twist: the value transfer process was conducted using cryptocurrency transactions rather than bank or MSB transfers.

Notably, the collectors were the ones responsible for carrying out the cryptocurrency transactions. Police tracking the Harrod's drug ring's activity arrested one of these collectors after a cash handover, recovered the cash, and discovered evidence on his person identifying bill serial numbers described above, as well as a list of several Bitcoin addresses. Below is a Reactor graph showing some of the collector's Bitcoin transactions related to the money laundering ring's activity.



The coordinator on the UK side of the operation fled following the collector's arrest, but returned several months later and was then arrested. Police recovered from him a hardware cryptocurrency wallet, whose transaction history showed £8 million worth of cryptocurrency being moved to a popular exchange within a six-month period. Because these funds entered the cryptocurrency ecosystem as fiat currency, blockchain analysis alone would never allow an investigator or compliance officer to identify them as risky.

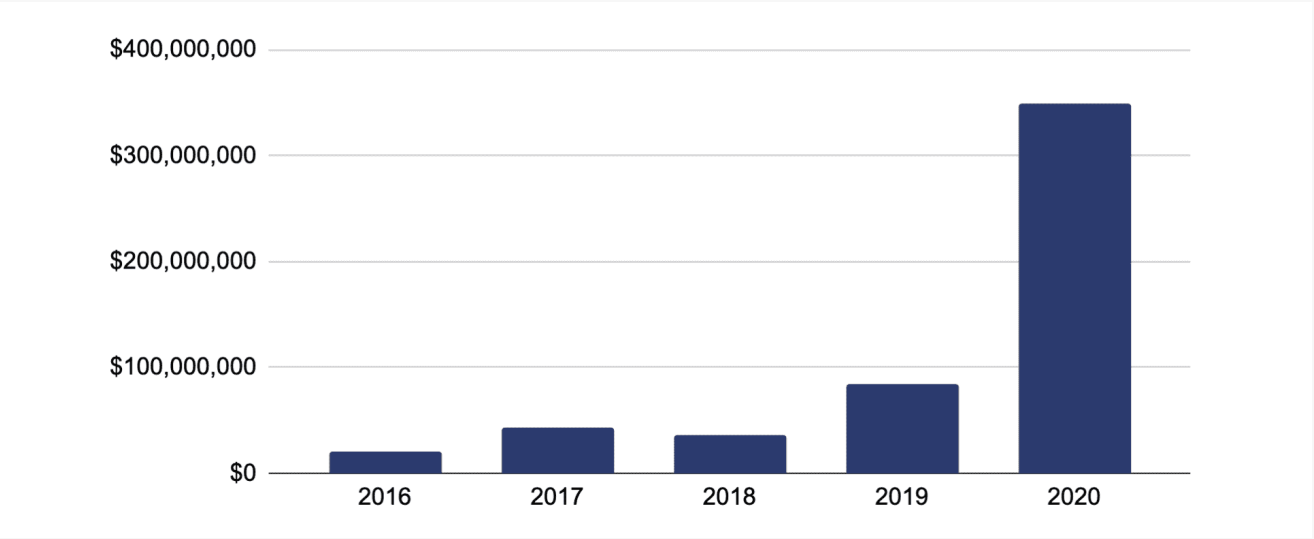
The Harrod's drug ring case shows how important it is for law enforcement investigators — even those not responsible for cybercrime — to understand how cryptocurrency and blockchain analysis work.

Ransomware

Ransomware Skyrocketed in 2020, But There May Be Fewer Culprits Than You Think

2020 will forever be known as the year of Covid, but when it comes to crypto crime, it's also the year that ransomware exploded.

Total cryptocurrency value received by ransomware addresses per year | 2016 - 2020

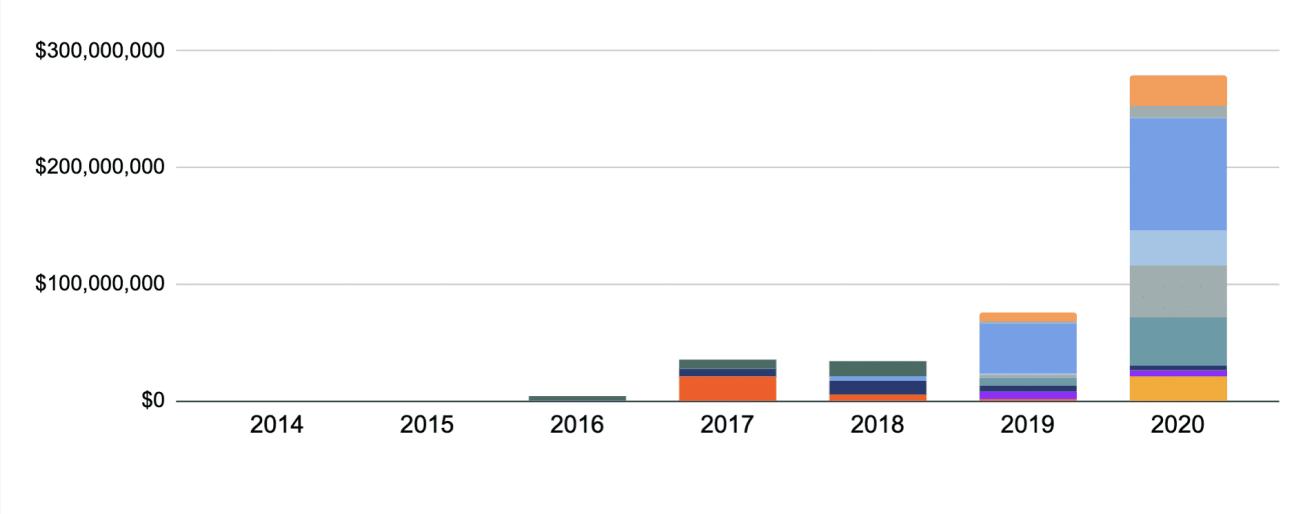


Currencies included:BCH, BTC, ETH, USDT

Blockchain analysis shows that the total amount paid by ransomware victims increased by 311% this year to reach nearly $350 million worth of cryptocurrency. No other category of cryptocurrency-based crime had a higher growth rate. Keep in mind that this number is a lower bound of the true total, as underreporting means we likely haven't categorized every victim payment address in our datasets.

2020's ransomware increase was driven by a number of new strains taking in large sums from victims, as well as a few pre-existing strains drastically increasing earnings.

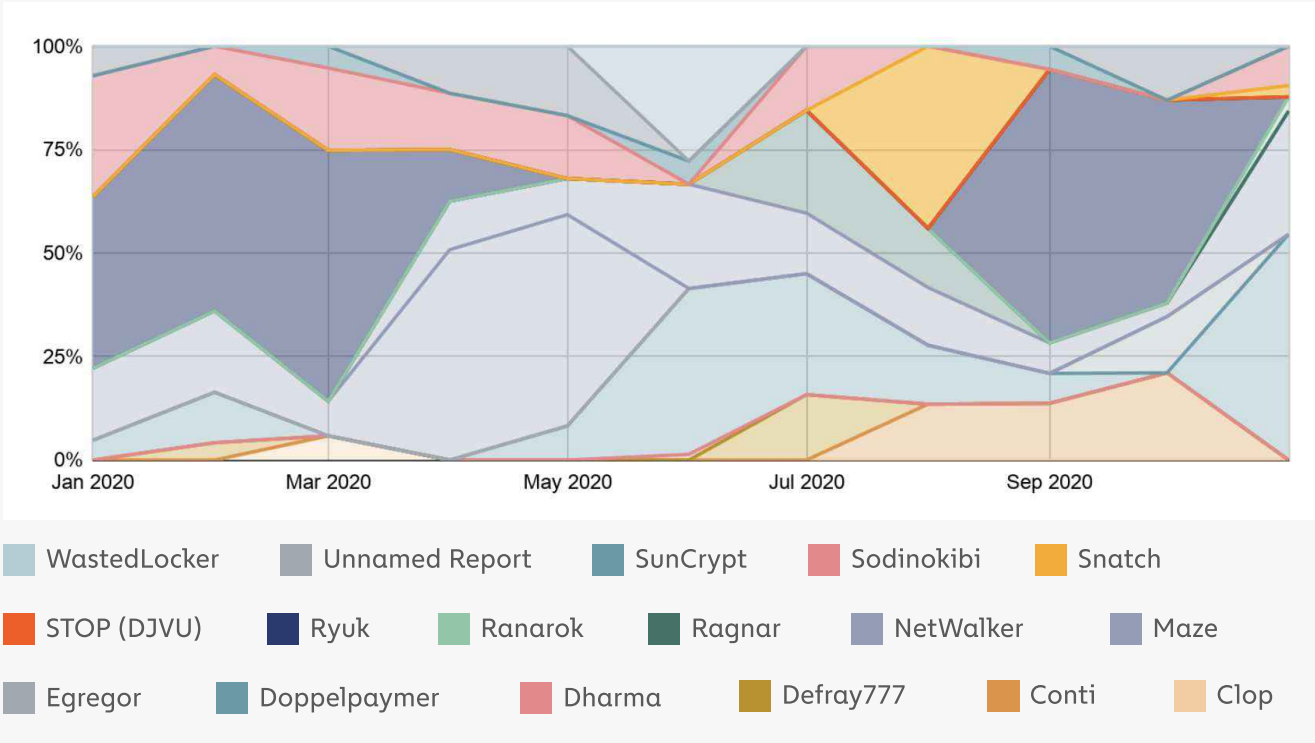
Top 10 ransomware strains by revenue by year | 2014 - 2020



Currencies included: BCH, BTC

Ransomware strains don't operate consistently, even month-to-month. Below, we see that the top-earning strains have ebbed and flowed throughout 2020.

Ransomware lifecycles: Top monthly strains by share of all ransomware revenue | 2020

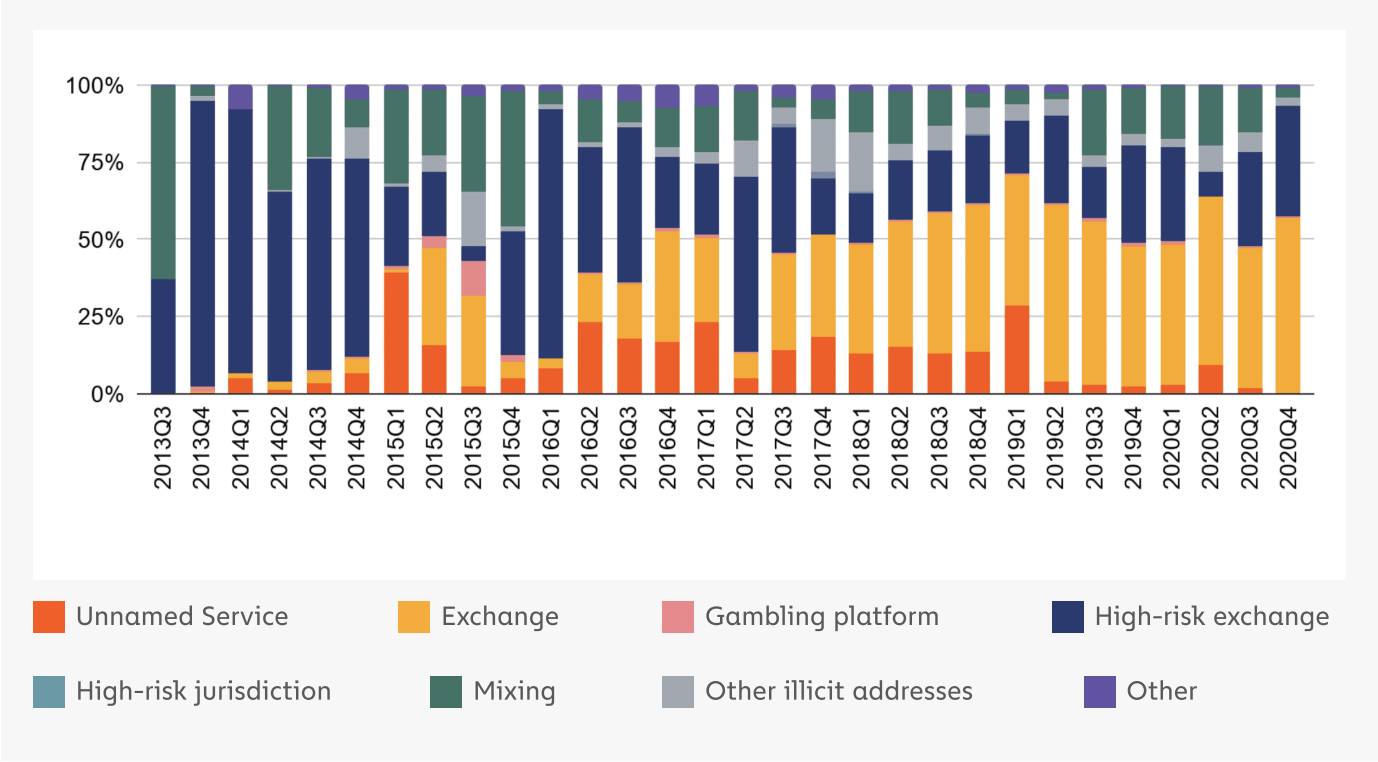


Currencies included: BTC

The number of strains active throughout the year may give the impression that there are several distinct groups carrying out ransomware attacks, but this may not be the case. As we explored in last year's Crypto Crime Report, many strains function on the RaaS model, in which attackers known as affiliates "rent" usage of a particular ransomware strain from its creators or administrators, who in exchange get a cut of the money from each successful attack affiliates carry out.

Many RaaS affiliates migrate between strains, suggesting that the ransomware ecosystem is smaller than one might think at first glance. In addition, many cybersecurity researchers believe that some of the biggest strains may even have the same creators and administrators, who publicly shutter operations of one strain before simply releasing a new, very similar strain under a new name. With blockchain analysis, we can shed light on some of these connections by analyzing how addresses associated with different ransomware strains transact with one another.

Destination of funds leaving ransomware wallets | Q3 2013 - Q4 2020



Currencies included: BTC, BCH, ETH

Ransomware attackers move most of the funds taken from their victims to mainstream exchanges, high-risk exchanges (meaning those with loose to non-existent compliance standards), and mixers. However, as we'll explore later in the section, the money laundering infrastructure ransomware attackers rely on may be controlled by just a few key players,

similar to the ransomware strains themselves. We'll explore the interconnectivity within the ransomware ecosystem below. But first, we'll look at an under-discussed issue ransomware victims face in addition to the loss of money and data: Sanctions risk.

Sanctions risk in ransomware

In October 2020, perhaps prompted by the massive uptick in ransomware attacks rocking both the public and private sector, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) released an advisory alert warning that making ransomware payments could be a sanctions violation for victims or companies that facilitate payments for victims. The facilitation point is important, as there's a robust industry of consultants who help ransomware victims negotiate with and pay ransomware attackers. The alert cited examples of ransomware creators and attackers who have been put on the OFAC sanctions list, such as the two Iranian nationals who laundered proceeds from the SamSam ransomware strain. October's alert bolsters previous government guidance not to pay ransomware attackers, as this incentivizes future attacks. However, this alert goes a step further in warning that ransomware victims and consultants who help them make payments could face the heavy penalties associated with sanctions violations.

But how big is the sanctions violation risk in ransomware? We looked back at all ransomware payments Chainalysis has tracked since 2016 and calculated the percentage of payment volume that was associated with sanctions risks.

We counted all ransomware payments that meet any of the three criteria below as constitutive of sanctions violation risk:

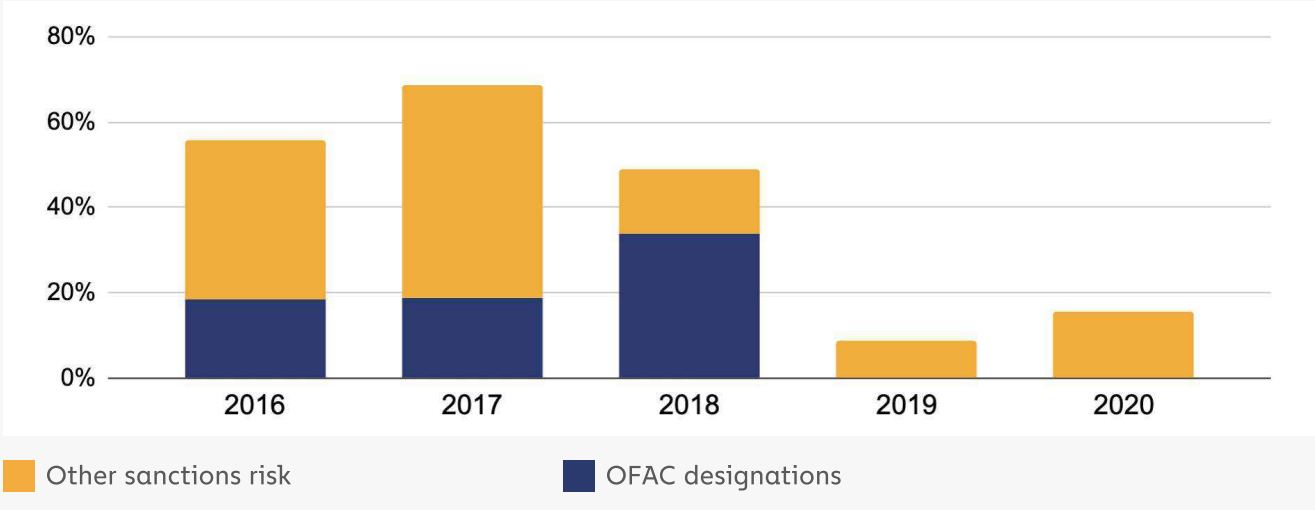
- Payments to addresses identified by OFAC as belonging to sanctioned individuals (note: this includes payments made before the addresses' owners were actually sanctioned.).
- Payments to addresses connected to ransomware strains whose creators have been sanctioned by OFAC.
- Payments to addresses connected to ransomware strains associated with cybercriminals based in heavily sanctioned jurisdictions such as Iran and North Korea.

Those criteria cover the following ransomware strains:

Strain	Description
SamSam	OFAC designated cryptocurrency address
Ouroboros	Linked to Iranian Actors
VoidCrypt	Linked to Iranian Actors
Sorena	Linked to Iranian Actors
Pay2Key	Linked to Iranian Actors
WannaCry 1.0, WannaCry 2.0	Linked to North Korean Actors
NotPetya	Associated with sanctioned actors in Russia.
CryptoLocker	Associated with sanctioned actors in Russia.
Bitpaymer	Speculated to be associated with sanctioned group Evil Corp.
Locky	Speculated to be associated with sanctioned group Evil Corp.
Doppelpaymer	Speculated to be associated with sanctioned group Evil Corp.
WastedLocker	Speculated to be associated with sanctioned group Evil Corp.
Clop	Disputed, but speculated to be associated with Evil Corp.

Based on those designations, we found that 15% of all ransomware payments made in 2020 carried a risk of sanctions violations. This was quite low compared to some previous years.

Share of all ransomware payments associated with OFAC designations and other sanctions risk | 2016 - 2020

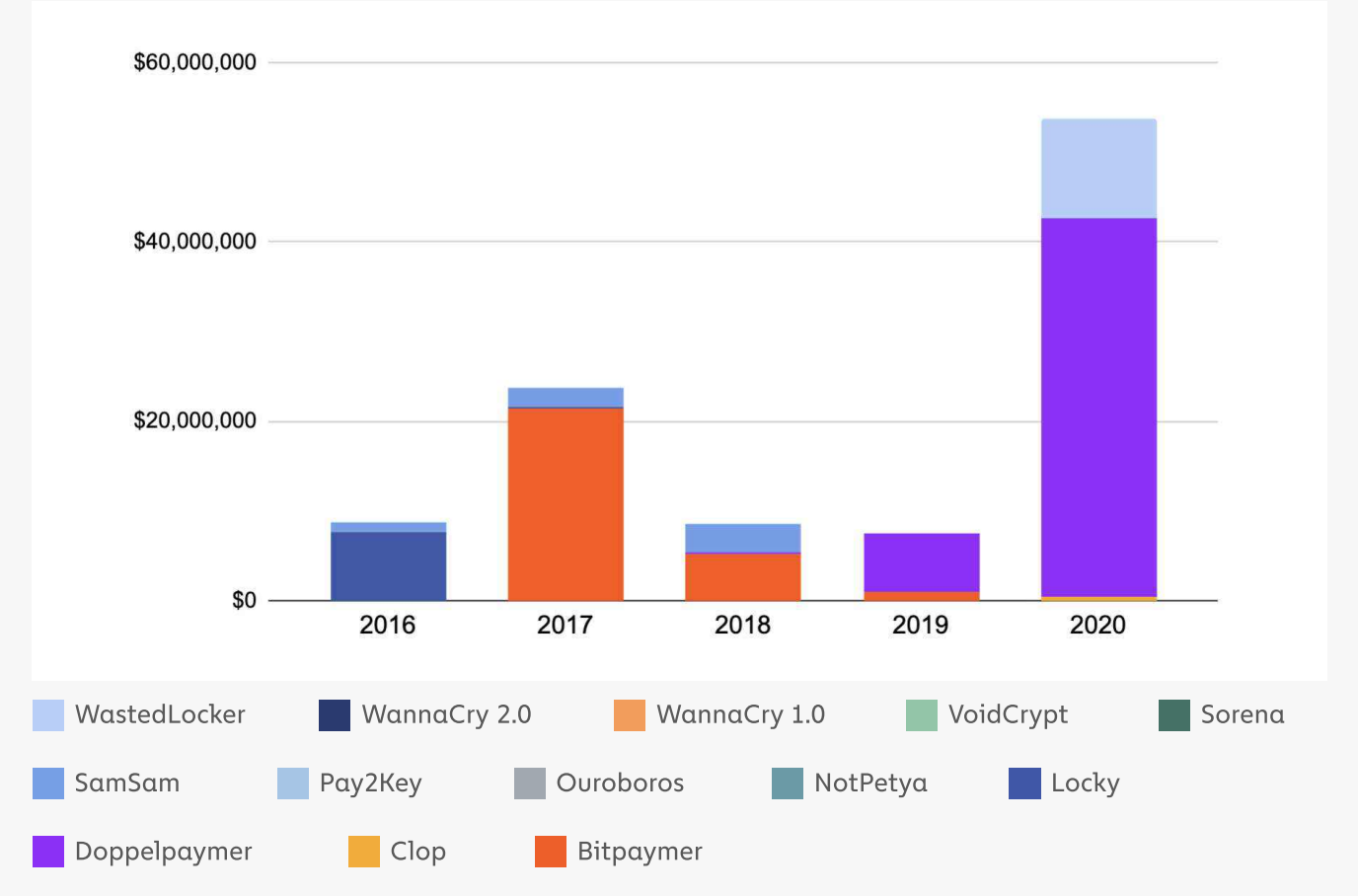


Please note that all payments to addresses associated with OFAC-sanctioned individuals or groups noted on this chart took place before those individuals or groups were added to the OFAC sanctions list.

Currencies included: BCH, BTC, ETH, USDT

While the rate of sanctions risk in ransomware payments has declined from much higher figures in 2018 and prior, keep in mind how much ransomware payments overall increased in 2020. That means the dollar figure for ransomware payments with sanctions risk skyrocketed last year. Below, we show the yearly volume of ransomware payments that constitute sanctions violation risk, broken down by strain.

Total value received by ransomware addresses associated with sanction risk by ransomware strain | 2016 - 2020



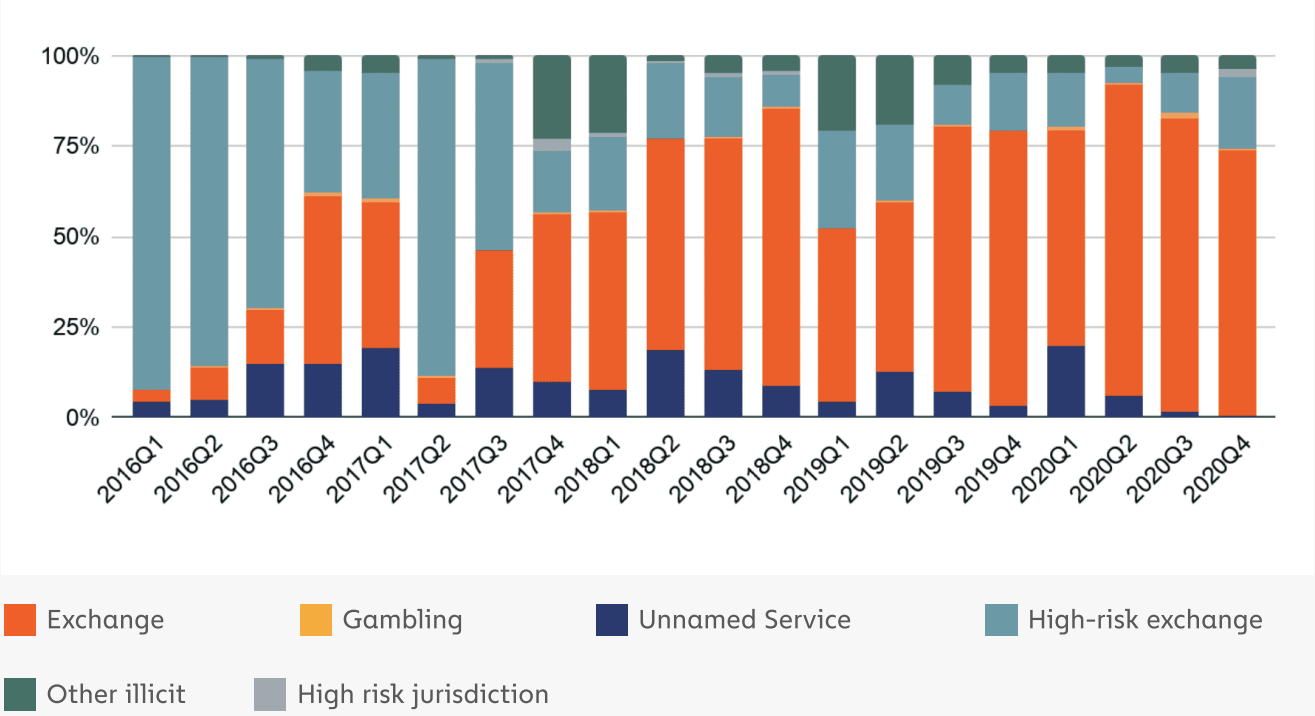
Currencies included: BCH, BTC

Overall, more than $50 million worth of cryptocurrency that victims paid out to ransomware addresses that we've identified carried sanctions risk in 2020, nearly all of which was composed of payments to Doppelpaymer and WastedLocker specifically. In previous years, Bitpaymer, SamSam, and Locky have also been responsible for a high volume of ransomware payments associated with sanctions risk.

It's also worth noting that exchanges and other cryptocurrency businesses could be at risk for any funds they receive from ransomware addresses in general, but especially those associated with sanctions risk.

Destination of funds leaving ransomware wallets with sanction risk

| Q4 2014 - Q4 2020



Overall in 2020, mainstream exchanges received more than $32 million from ransomware strains associated with sanctions risks.

Dealing with a ransomware attack is hard enough without victims having to worry about penalties and reputational damage down the line if it turns out they committed a sanctions violation for paying a ransom. We encourage all ransomware victims to work with a lawyer specializing in sanctions and financial crime before paying off an attacker, and to report the attack to law enforcement.

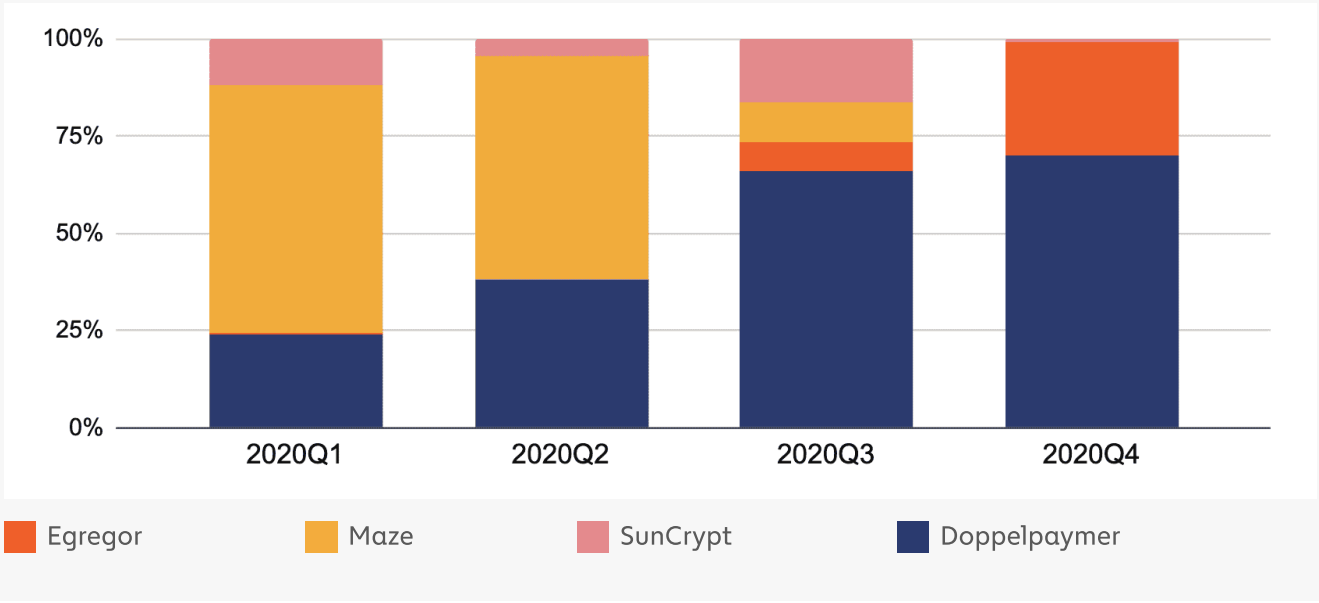
Blockchain analysis shows connections between four of 2020's biggest ransomware strains

As we mention above, there may be fewer cybercriminals responsible for ransomware attacks than one would initially think given the number of individual attacks, distinct strains, and amount stolen from victims. Cybersecurity researchers point out that many RaaS affiliates carrying out attacks switch between different strains, and many believe that seemingly distinct strains are actually controlled by the same people. Using blockchain analysis, we'll investigate potential connections between four of 2020's most prominent ransomware strains: Maze, Egregor, SunCrypt, and Doppelpaymer.

The four ransomware strains were quite active last year, attacking prominent companies such as Barnes & Noble, LG, Pemex, and University Hospital New Jersey, amongst others. All four use the RaaS model, meaning that affiliates carry out the ransomware attacks themselves and pay a percentage of each victim payment back to the strain's creators and administrators. All four also use the "double extortion" strategy of not just withholding victims' data, but also publishing pieces of it online as an extra incentive for victims to pay the ransom.

Below, we see the four strains' 2020 revenue broken out quarterly.

2020 Ransomware revenue by quarter: SunCrypt, Maze, Egregor, and Doppelpaymer

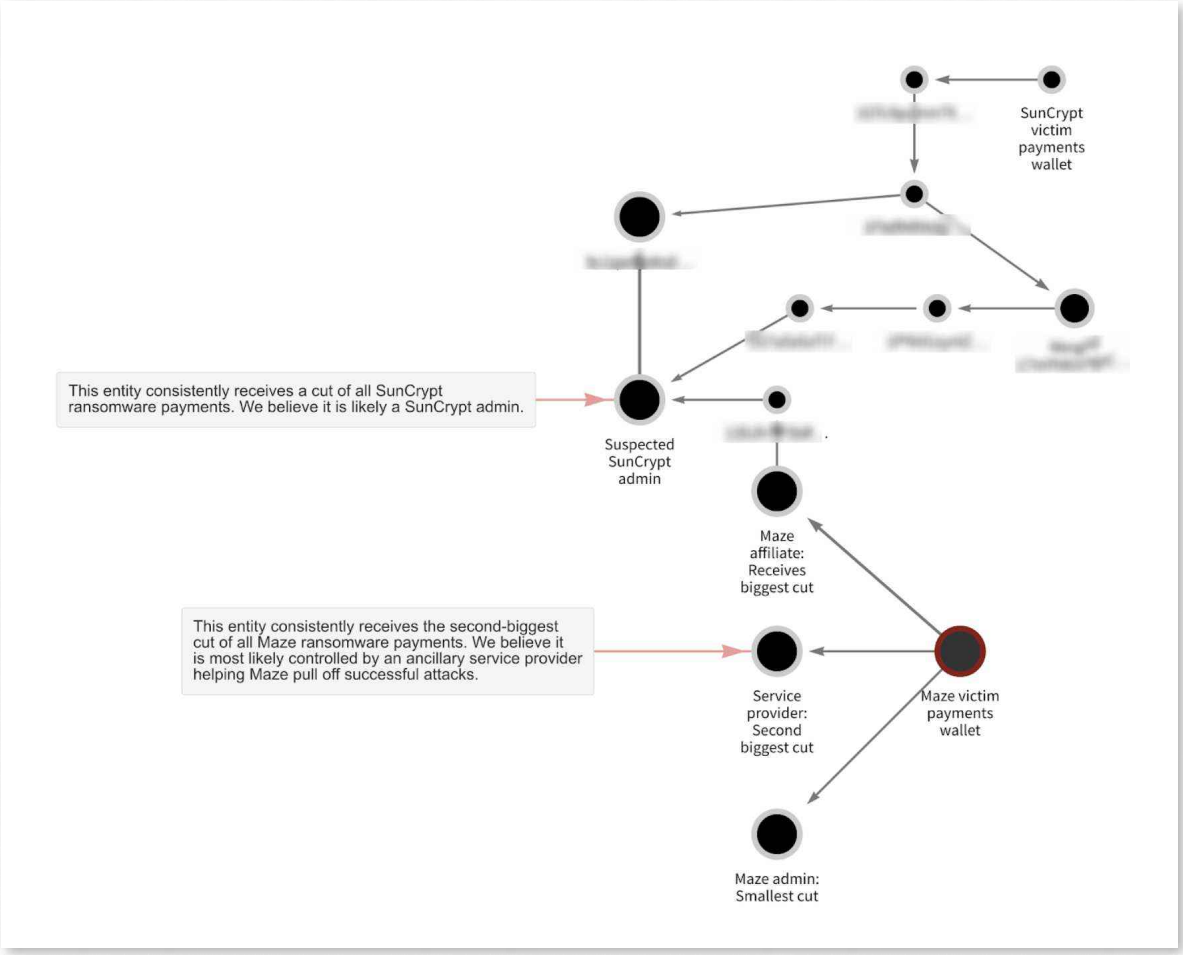


Note that Egregor only became active just before Q4 2020 (mid-September to be specific), soon after the Maze strain became inactive. Some cybersecurity researchers see this as evidence that Maze and Egregor are linked in some way. In early November, Maze's operators said the strain was shutting down in a press release posted to its website, following a slowdown in activity. Soon after, most of its affiliates migrated to Egregor, leading some to believe that the Maze operators have simply rebranded as Egregor and instructed the affiliates to join. This is relatively common in ransomware, though it's also possible that the affiliates have decided for themselves that Egregor is their best option. It's even possible that the Maze affiliates became unhappy with the Maze operators, leading to the split. However, as noted by Bleeping Computer, Maze and Egregor share much of the same code, the same ransom note, and have very similar victim payment sites. Cybersecurity firm Recorded Future notes this too, as well as similarities between Egregor and a banking trojan called QakBot.

It's not just Egregor either. In another story, Bleeping Computer claims that Suncrypt representatives contacted them claiming to be part of the "Maze ransomware cartel" prior to Maze's shutdown announcement, though Maze has denied this. However, the claim of a connection is also supported by a privately circulated report from threat intelligence firm Intel471 claiming that representatives from SunCrypt described their strain as a "rewritten and rebranded version of a 'well-known' ransomware strain." Intel471's report also claims that SunCrypt only works with a small number of affiliates at a time, whom the SunCrypt operators interview and vet extensively. Therefore, we believe any overlap in affiliates between SunCrypt and other ransomware strains would be more likely to suggest a deeper connection between the two strains, rather than just coincidence.

Blockchain analysis suggests affiliate overlap and other possible connections between Maze, Egregor, SunCrypt, and Doppelpaymer

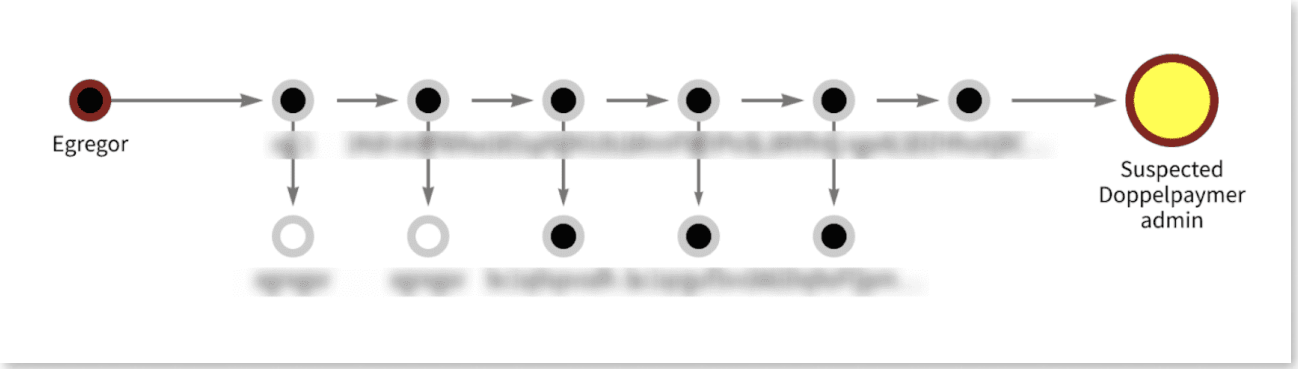
As we outline above, there's circumstantial evidence suggesting links between some of these four strains, as well as reports of affiliate migration. But what links do we see on the blockchain? Let's start with Maze and SunCrypt.



The Chainalysis Reactor graph above provides strong evidence suggesting that a Maze ransomware affiliate is also an affiliate for SunCrypt. Starting at the bottom of the graph, we see how Maze distributes funds taken in ransomware attacks. First, the majority of each successful ransom payment goes to the affiliate, as they're taking on the risk of actually carrying out the ransomware attack. The next biggest cut goes to a third party. While we can't know for sure what that third party's role is, we believe it's likely an ancillary service provider who helps Maze pull off attacks. Ransomware attackers often rely on third parties for tools like bulletproof hosting, penetration testing services, or access to vulnerabilities in victims' networks. These ancillary service providers can be found peddling their wares on cybercriminal darknet forums, but aren't necessarily involved in all ransomware attacks. Finally, the smallest cut of each ransom payment goes to another wallet that we believe belongs to the strain's administrators.

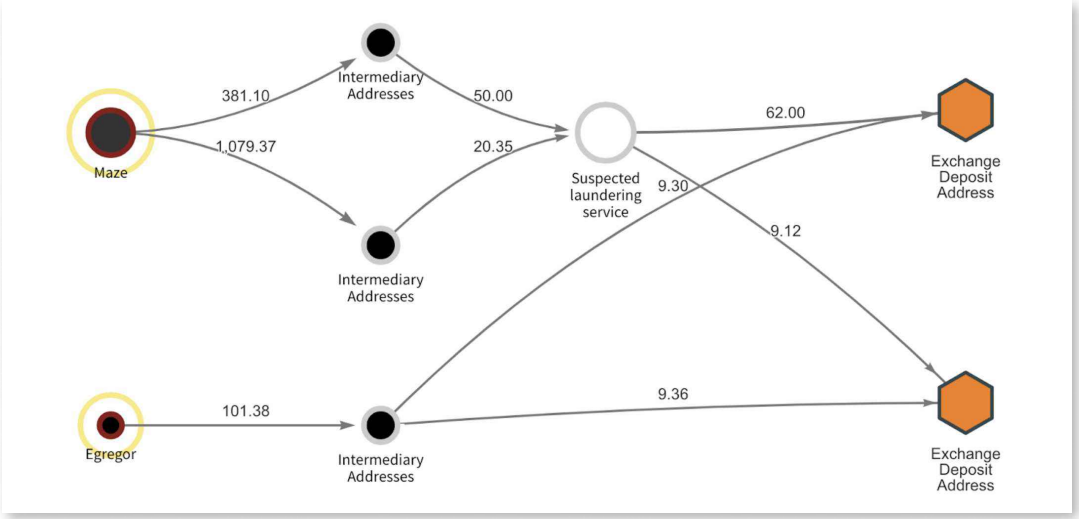
In this case, however, we see that the Maze affiliate also sent funds — roughly 9.55 Bitcoin worth over $90,000 — via an intermediary wallet to an address labeled "Suspected SunCrypt admin," which we've identified as part of a wallet that has consolidated funds related to a few different SunCrypt attacks. This suggests that the Maze affiliate is also an affiliate for SunCrypt, or possibly involved with SunCrypt in another way.

Another Reactor graph shows links between the Egregor and Doppelpaymer ransomware strains.



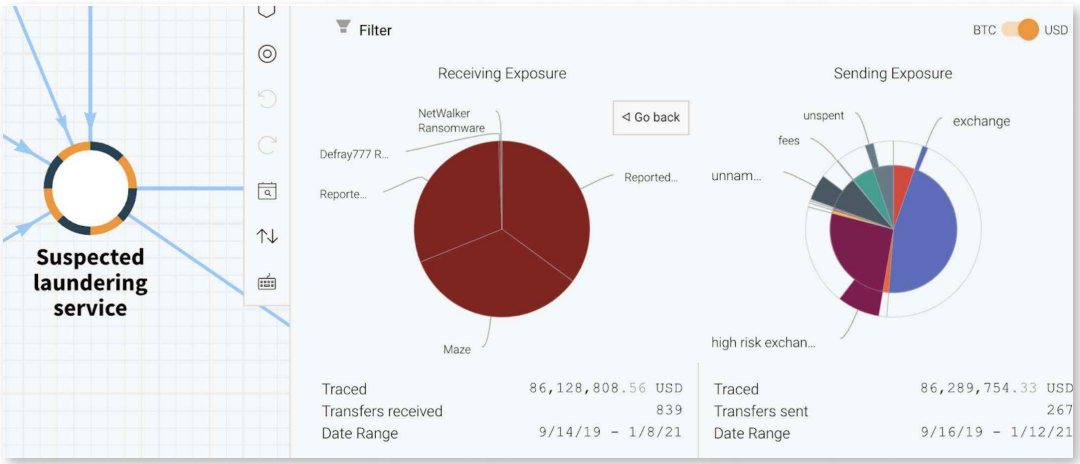
In this case, we see that an Egregor wallet sent roughly 78.9 BTC worth approximately $850,000 to a suspected Doppelpaymer administrator wallet. Though we can't know for sure, we believe that this is another example of affiliate overlap. Our hypothesis is that the Egregor-labeled wallet is an affiliate for both strains sending funds to the Doppelpaymer administrators.

Finally, the Reactor graph below shows what we believe is an instance of Maze and Egregor administrators using the same money laundering infrastructure.



Both strains' victim payments' wallets have sent funds to two deposit addresses at a prominent cryptocurrency exchange via intermediary wallets. Based on their transaction patterns, we believe that both deposit addresses belong to over-the-counter (OTC) brokers who specialize in helping ransomware operators and other cybercriminals trade illicitly-gained cryptocurrency for cash. In the case of Maze, those funds first flow through another suspected money laundering service before reaching the OTC addresses — it's unclear whether Maze receives cash from that service or from the OTCs themselves, and it's also possible that the OTC broker and those running the laundering service are one and the same.

While this doesn't suggest that Maze and Egregor share the same administrators or affiliates, it's still an important potential lead for law enforcement. Cryptocurrency-related crime isn't worthwhile if there's no way to convert ill-gotten funds into cash. By going after bad actors like the money laundering service or corrupt OTC brokers on the graph above — the latter of whom, again, operate on a large, well-known exchange — law enforcement could significantly hamper the ability of Maze and Egregor to operate profitably without actually catching the strains' administrators or affiliates. It's not just those specific ransomware strains either.



The suspected laundering service has also received funds from the Doppelpaymer, WastedLocker, and Netwalker ransomware strains, taking in nearly $2.9 million worth of cryptocurrency from the category as a whole. Likewise, it's received nearly $650,000 worth of cryptocurrency from darknet markets such as Hydra and FEShop. The two OTC broker addresses on the graph have similar criminal exposure as well.

What does this mean for ransomware?

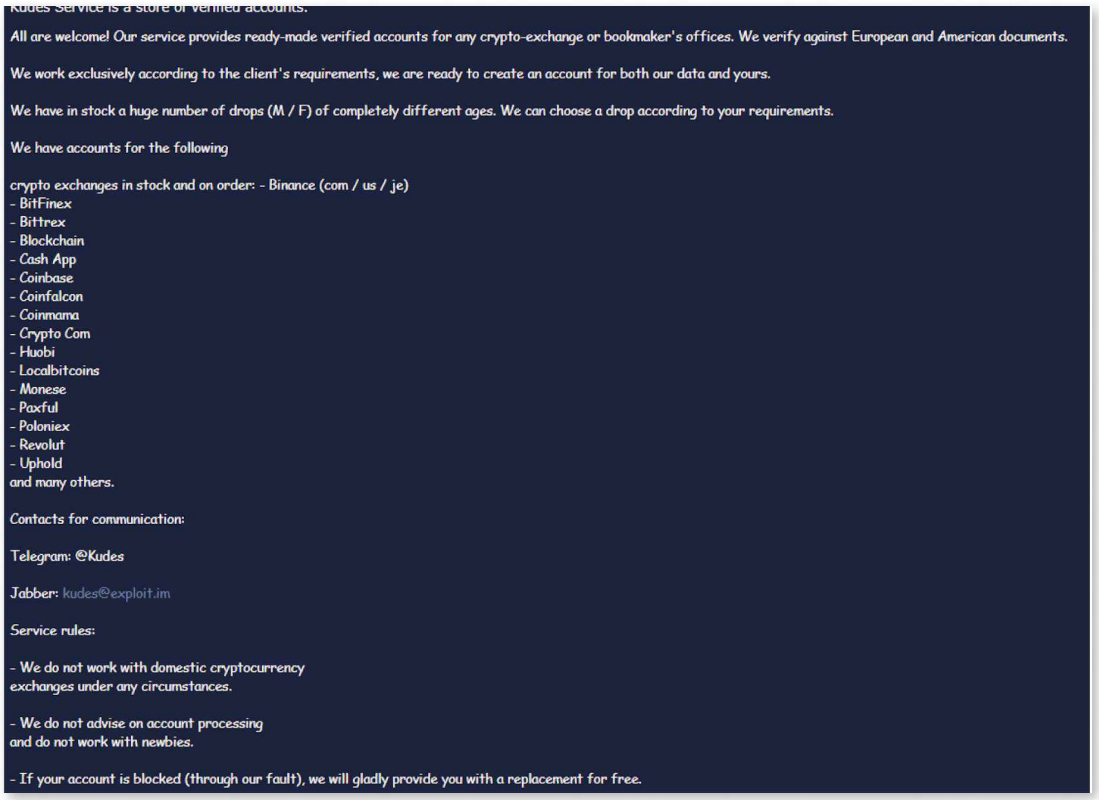
While we can't say for sure that Maze, Egregor, SunCrypt, or Doppelpaymer have the same administrators, we can say with relative certainty that some of them have affiliates in common. We also know that Maze and Egregor rely on the same OTC brokers to convert cryptocurrency into cash, though they interact with those brokers in different ways.

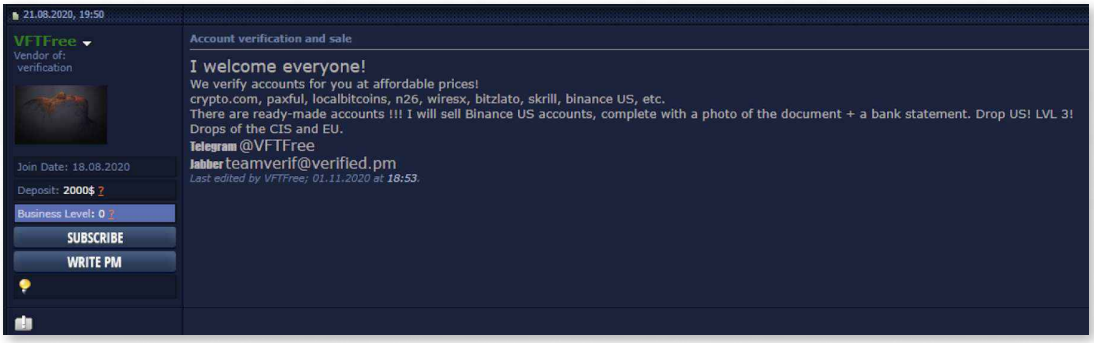
Regardless of the exact depth and nature of these connections, the evidence suggests that the ransomware world is smaller than one may initially think given the number of unique strains currently operating. This information can be a force multiplier for law enforcement. If they can identify and act against groups controlling multiple ransomware strains, or against OTCs enabling multiple ransomware strains to cash out their earnings, then they'll be able to halt or impact the operations of several strains with one takedown.

Mapping the ransomware ecosystem

As we show above, we can find connections between ransomware strains by examining common deposit addresses to which wallets associated with different strains send funds. We believe that most of the cases of deposit address overlap represent usage 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 victims pay them with — by taking one money laundering operation offline.

Overlap also wouldn't be surprising, as we see a small number of money laundering services advertising on various hacking forums. "Many of these services use mules and other means to register lots of fake accounts at big exchanges that they control," said Dmitry Smilyanets, ransomware expert and Threat Intelligence Analyst at cybersecurity provider Recorded Future. We see that reflected in the screenshots below.





Smilyanets also points out that many ransomware attackers are willing to wait to cash out their earnings. "They often feel safer waiting, and they believe in cryptocurrency and think it will keep growing, so they have no problem letting it sit for a few years."

However, money launderers aren't the only ones ransomware addresses send cryptocurrency to. Ransomware operators rely on several types of third-party providers to conduct attacks. These include:

- **Penetration testing services**, which ransomware operators use to probe potential victims' networks for weaknesses.
- **Exploit sellers**, who sell access to vulnerabilities in various types of software that ransomware operators and other cybercriminals can use to inject victims' networks with malware.

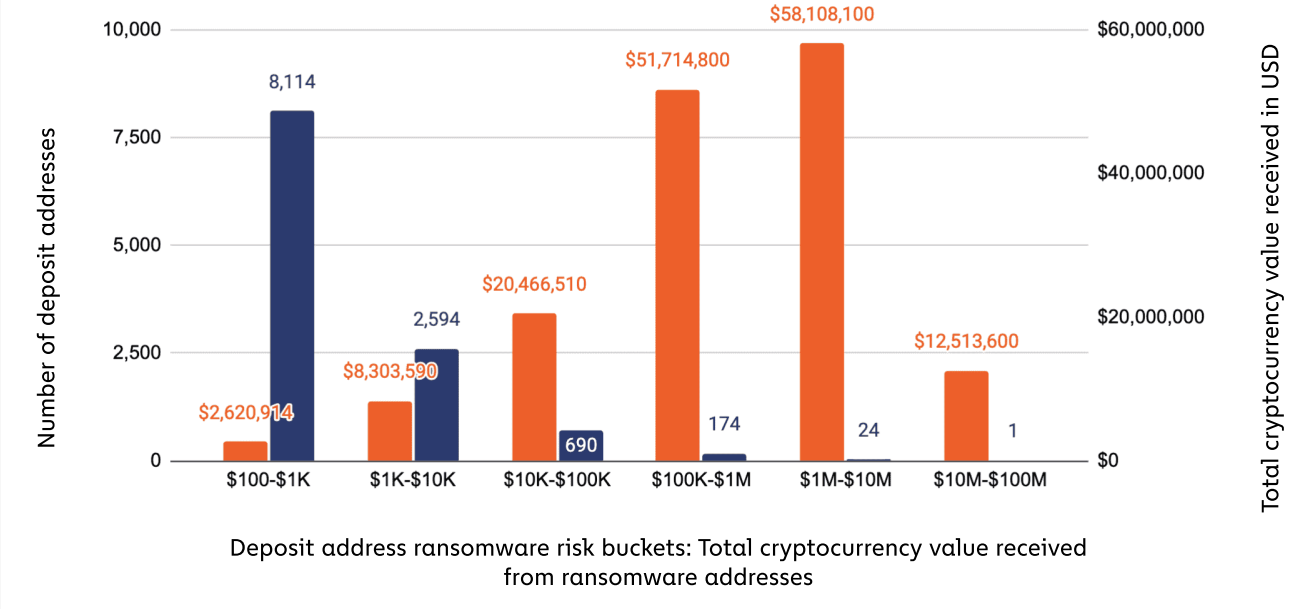
- **Bulletproof hosting providers**, who provide web hosting that customers can purchase anonymously and are generally lenient on the types of sites customers are allowed to host. Ransomware operators often need web hosting to set up command-and-control (C2) domains, which allow hackers' computers to send commands to victims' machines infected with malware.

Similar to money laundering services, law enforcement could theoretically disrupt several ransomware strains if agents were able to identify and act against service providers ransomware operators rely on to carry out attacks.

But just how concentrated are the deposit addresses receiving funds from ransomware addresses? Let's investigate.

As we mentioned at the beginning of the section, the majority of ransomware funds move to cryptocurrency exchanges. This activity is relatively concentrated to just a few services — a group of just five receives 82% of all ransomware funds. But what about when we look at the deposit address level?

Total illicit value received by deposit addresses by ransomware risk bucket vs. Number of deposit addresses per ransomware risk bucket | 2020



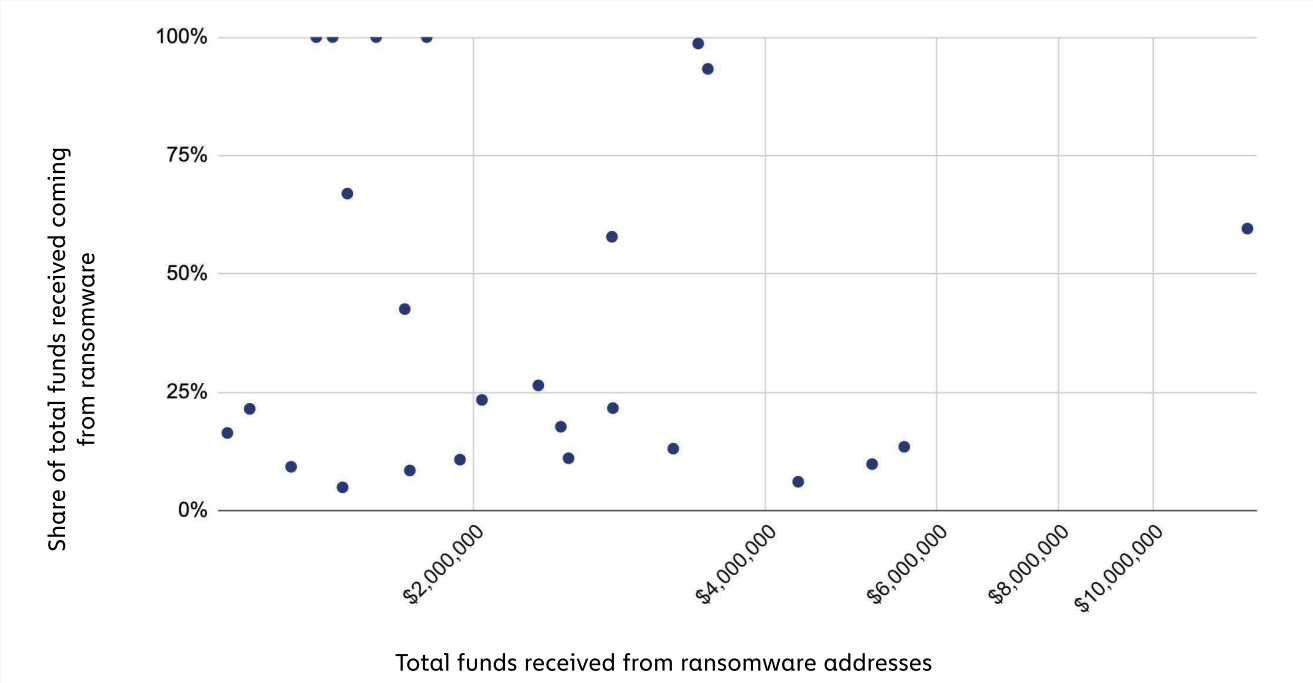
Accounts are bucketed by range of total value received from ransomware addresses. Each orange bar represents the total amount ransomware addresses sent to all addresses in the corresponding bucket, while each blue bar represents the number of individual deposit addresses in the bucket.

Currencies included: BTC

The data shows that ransomware money laundering is even more concentrated at the deposit address level. **Just 199 deposit addresses received 80% of all funds sent by ransomware addresses in 2020. An even smaller group of 25 addresses accounted for 46%.** Smilyanets and his colleague at Recorded Future, Roman Sannikov, reviewed these numbers and agreed the address sets taking in the most from ransomware strains were most likely money laundering services, while those taking in less were more likely to include third parties like exploit sellers and bullet-proof hosting providers. "Any address receiving $10,000 or less especially would much more likely be a service provider than a money launderer," said Sannikov.

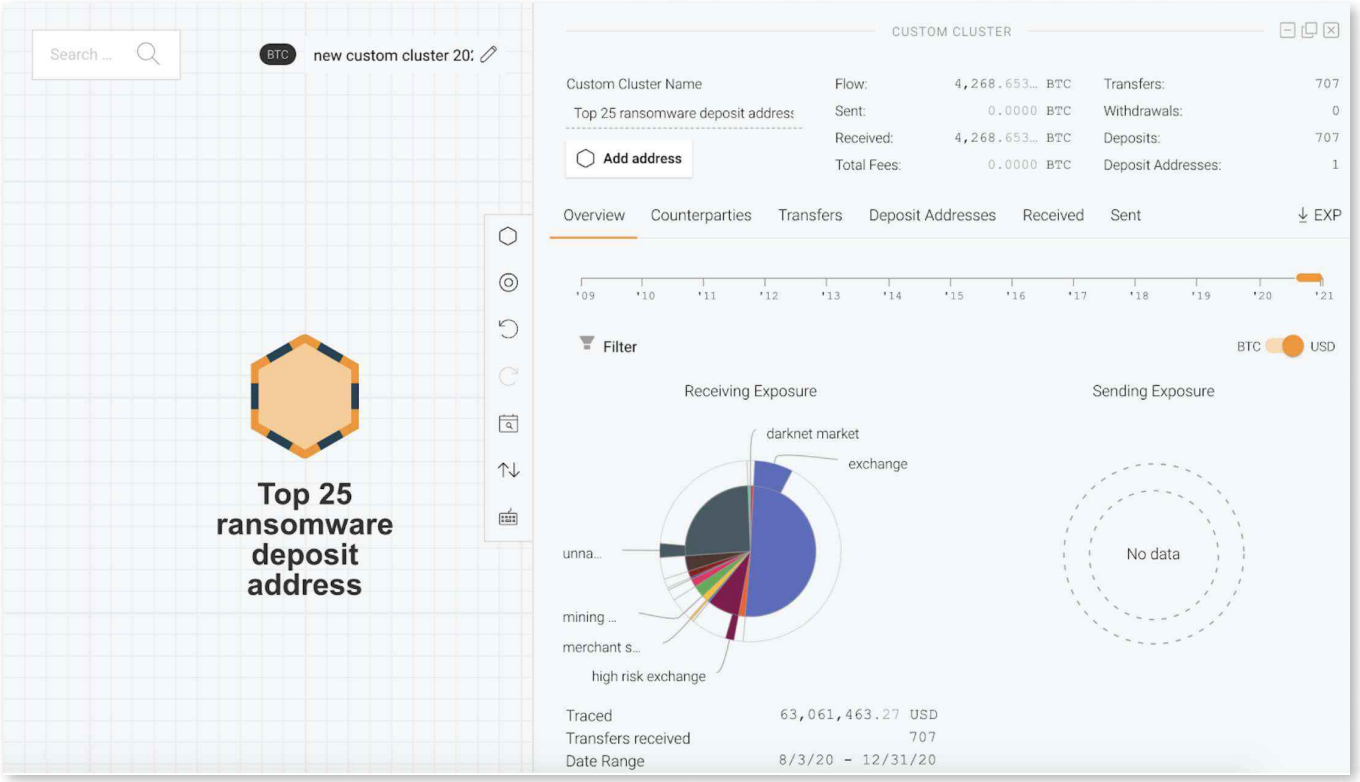
Let's look more closely at the addresses receiving the most from ransomware, and in particular the share of their total activity that's devoted to ransomware.

Top service deposit addresses for ransomware: Total funds received from ransomware addresses vs. Share of all funds received coming from ransomware addresses | 2020



Currencies included: BTC

On the scatter chart above, we sort the top 25 ransomware deposit addresses by the total amount they've received from ransomware addresses on the X axis, and the share of total funds they've received that ransomware makes up on the Y axis. We see that, save for a few outliers, ransomware makes up a relatively small percentage of all funds received by these deposit addresses. Below, we look more closely at the transaction history of one of those deposit addresses.



Please note that Chainalysis Reactor doesn't show sending activity for service deposit addresses, as services often move the funds received to their own internal addresses as needed. This means that tracing funds through service addresses can produce misleading results.

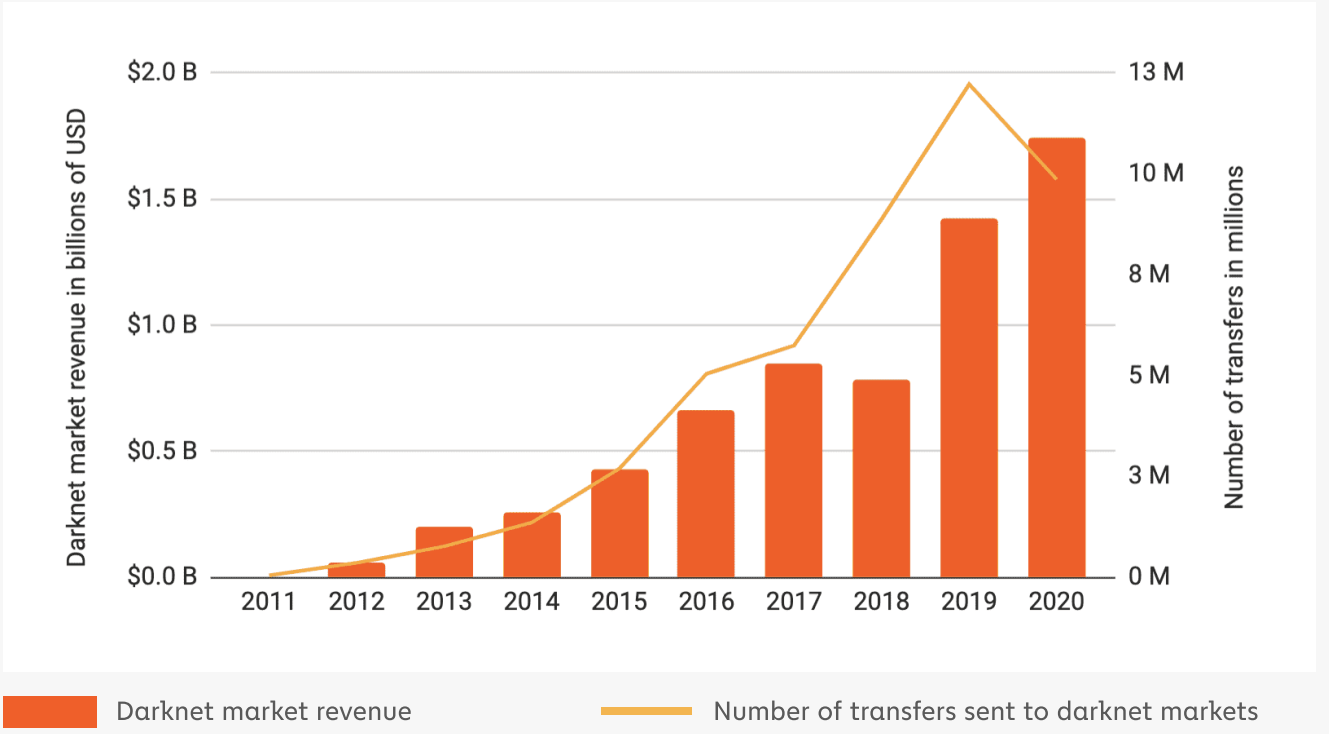
This deposit address belongs to a nested service hosted at a large, international cryptocurrency exchange and has been active since August 3, 2020. Between that date and the end of 2020, it received over $63 million worth of Bitcoin in total. Most of it appears to be non-illicit activity — nearly half of those funds come from other mainstream exchanges, though a quarter comes from unknown services that may be identified as linked to criminal activity at a later date. However, while the share is low, the address has still received over $1 million worth of Bitcoin from ransomware addresses, as well as $2.4 million from multiple scams. Overall, criminal activity accounts for 10% of the address' total cryptocurrency received. Most of the other deposit addresses on our scatter chart with low shares of total funds coming from ransomware fit a similar profile.

Darknet Market

Darknet Market Activity Higher Despite Fewer Purchases and Dwindling Number of Markets

Darknet market revenue vs. Total transfers to darknet markets

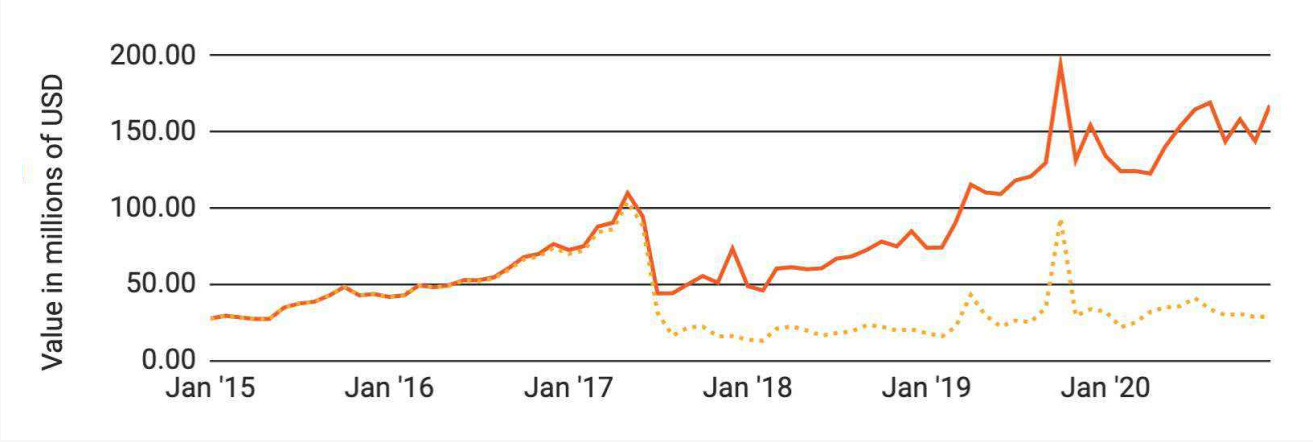
| 2011 - 2020



Currencies included: BCH, BTC, LTC, USDT

Darknet markets set a new revenue record in 2020, bringing in a total of $1.7 billion worth of cryptocurrency. Interestingly, this record comes as individual purchases from darknet markets declined, falling from 12.2 million in 2019 to fewer than 10 million in 2020. However, if we look more closely, we see that nearly all of the growth in darknet market activity 2020 can be attributed to one specific market: Hydra.

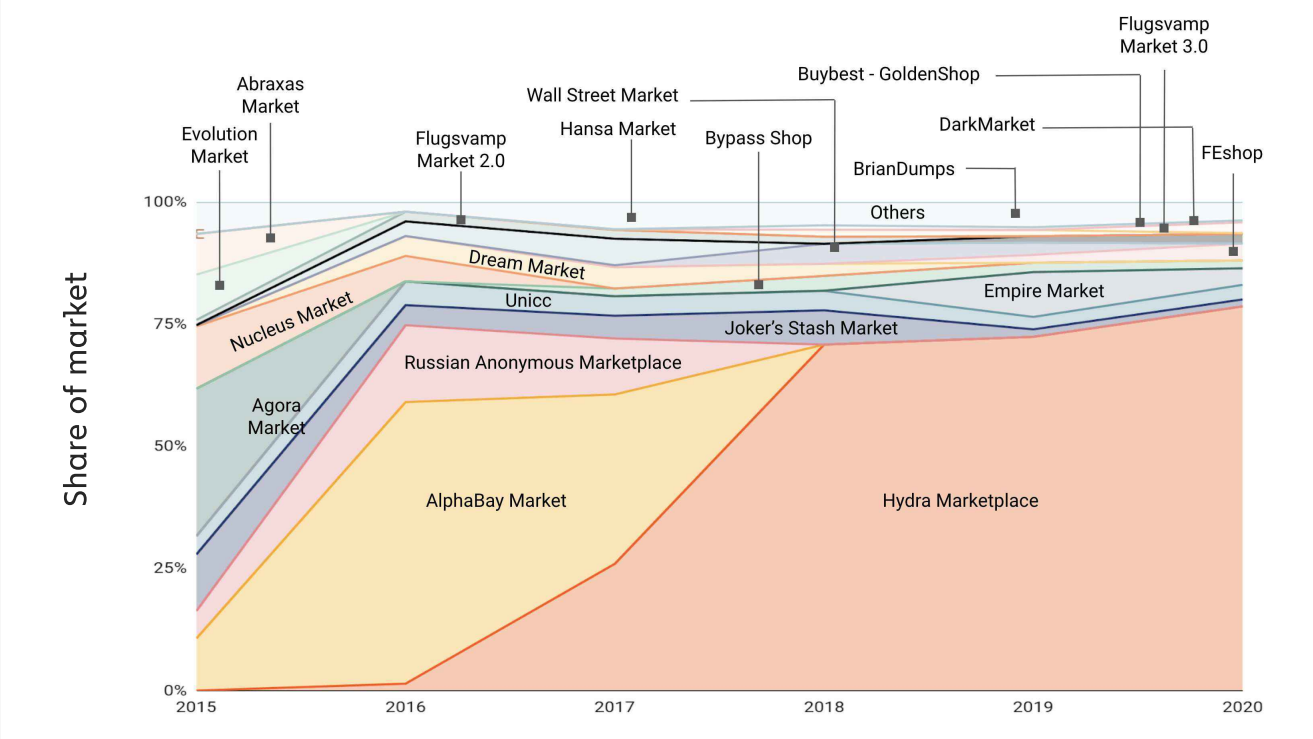
Monthly darknet market revenue | 2015 - 2020



Currencies included: BCH, BTC, LTC, USDT

If we exclude Hydra, we see that darknet market revenue stayed roughly flat from 2019 to 2020. Hydra is unique in that it only serves Russian-speaking countries and is by far the largest darknet market in the world, accounting for over 75% of darknet market revenue worldwide in 2020.

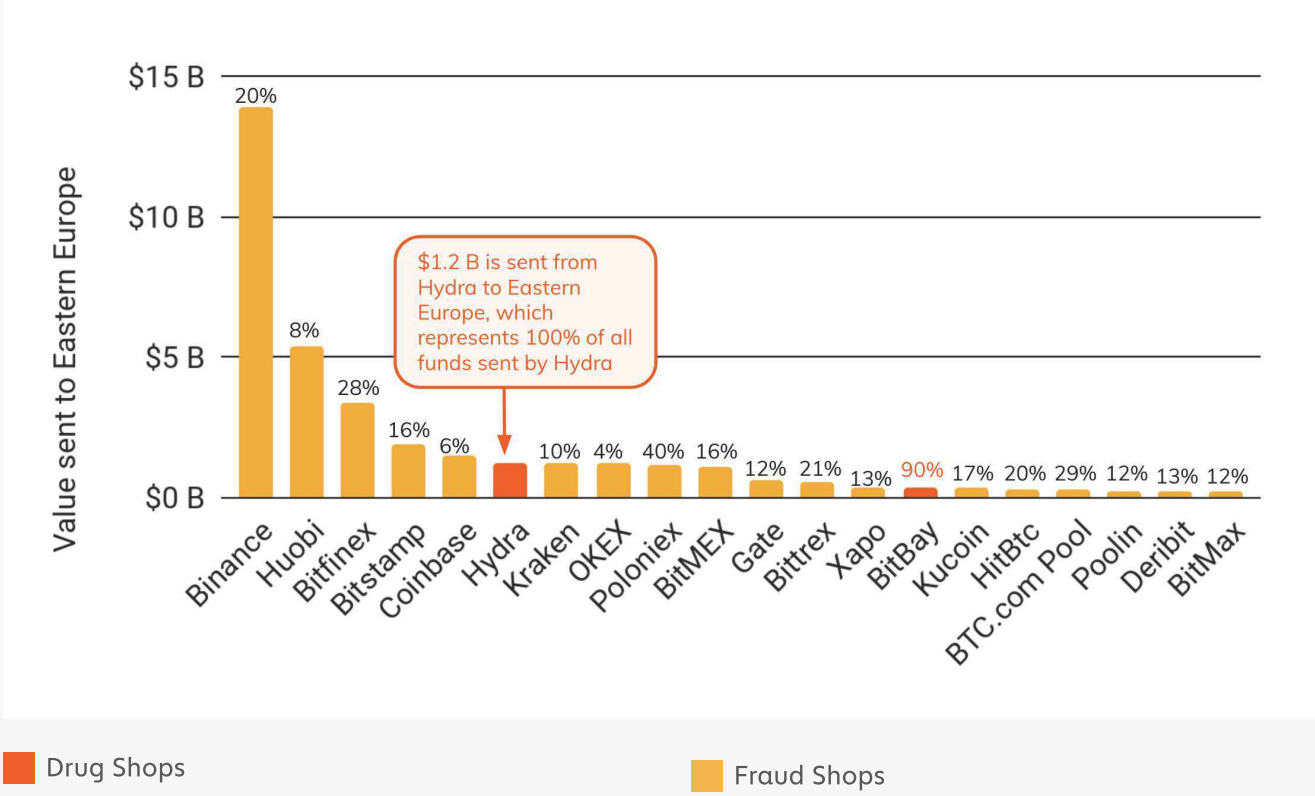
All darknet markets by share of total market size over time | 2015 - 2020



Currencies included: BCH, BTC, LTC, USDT

Hydra is a big driver of Eastern Europe's unique crypto crime landscape. Eastern Europe has one of the highest rates of cryptocurrency transaction volume associated with criminal activity and, thanks to Hydra, is the only region with a criminal service as one of the top ten entities sending cryptocurrency value to the region.

Top 20 services by value sent to Eastern Europe | Jul '19 - Jun '20

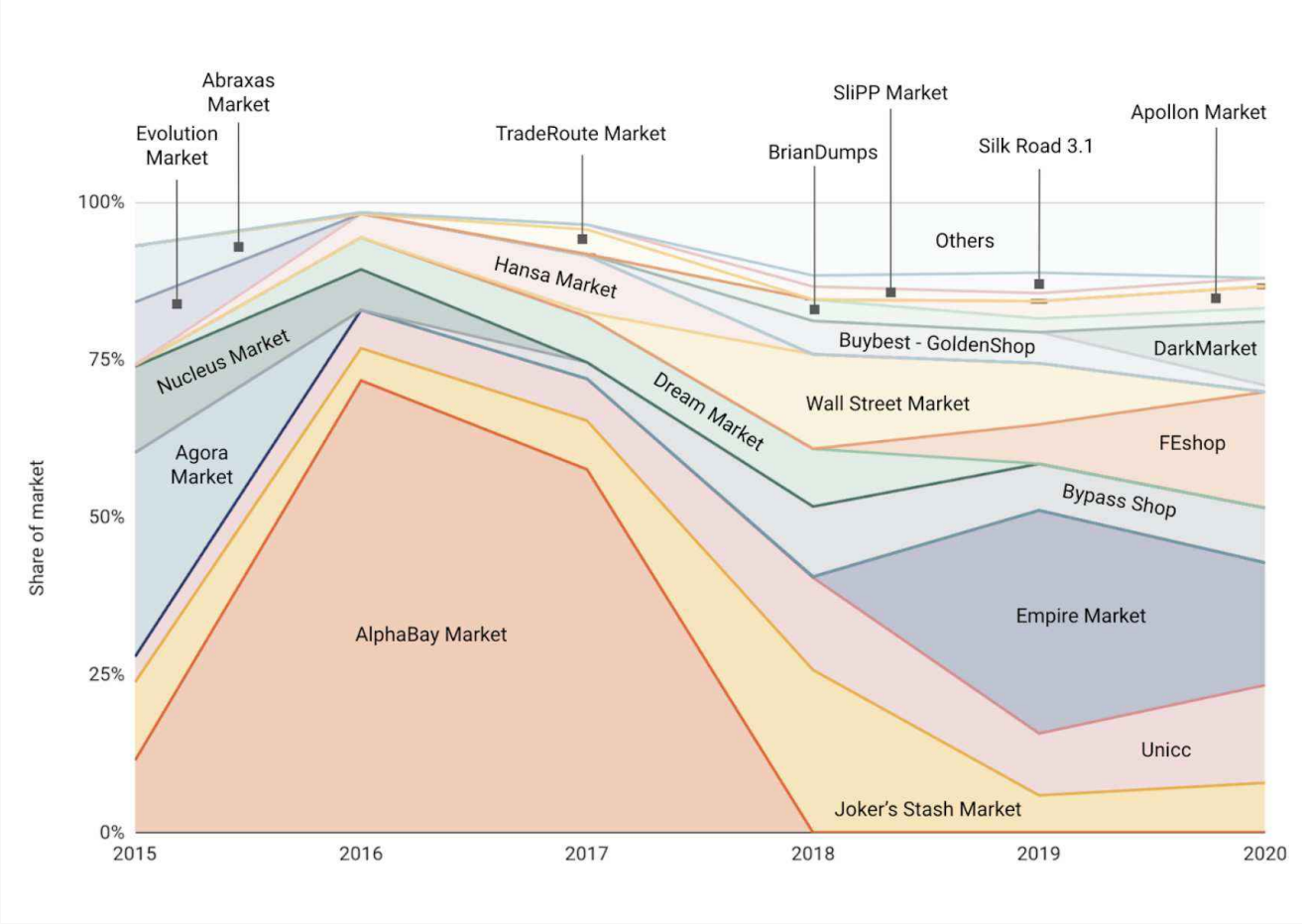


Currencies included: BAT, BCH, BNB, BTC, BUSD, CRO, CRPT, DAI, ETH, GNO, GUSD, HT, HUSD, ICN, LEO, LINK, LTC, MCO, MKR, MLN, OMG, PAX, PAXG, TGBP, TUSD, USDC, USDT, WETH, ZIL, ZRX

Hydra could eventually come to the English-speaking world as well. In December 2019, Hydra announced plans to raise $146 million in an ICO for a new global DNM service called Eternos. While it appears Covid put this plan on hold, the announcement suggests that Hydra plans to expand. That could create a significant challenge for U.S. and European law enforcement, as Hydra has developed uniquely sophisticated operations, such as an Uber-like system for assigning drug deliveries to anonymous couriers, who drop off their packages in out-of-the-way yet hidden public locations, commonly referred to as "drops," which are then shared with the buyers. That way, no physical exchange is made, and unlike with traditional darknet markets, vendors don't need to risk using the postal system.

Global darknet markets by share of total market size over time

| 2015 - 2020



Currencies included: BCH, BTC, LTC, USDT

If we exclude Hydra and other markets that serve customers in a particular region, we see that darknet market activity is much less concentrated outside the Russian-speaking world, with several different markets taking in significant revenue. Interestingly, many of the largest markets are fraud shops, which sell stolen credit card information and other data that can be used for fraud, including personally identifying information (PII), SOCKS5, stolen accounts for different services, and hacking exploits rather than drugs.

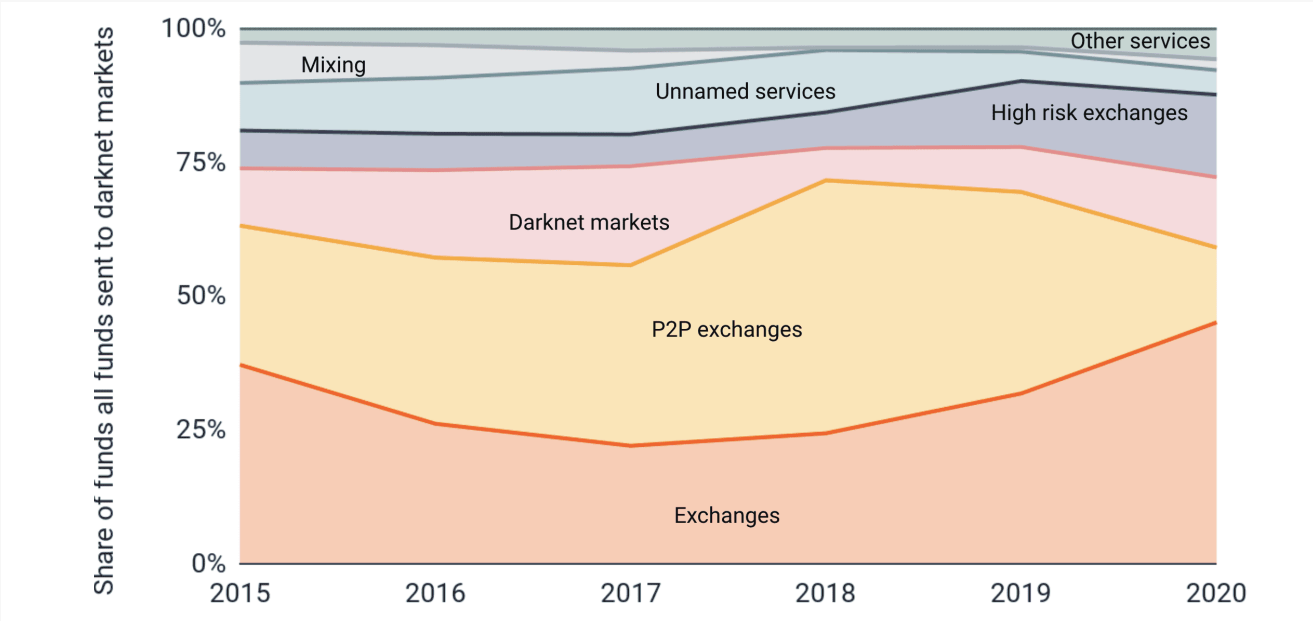
Top 20 global darknet markets by revenue | 2020

Currencies included: BCH, BTC, LTC, USDT

In fact, when we exclude Hydra, we see that card shops surpass drug shops in revenue amongst English language darknet markets.

What kinds of services are darknet market vendors and their customers using to facilitate these activities? We'll start with the customers. Below, we break down the services sending cryptocurrency to darknet markets by volume.

Origin of funds sent to darknet markets | 2015 - 2020

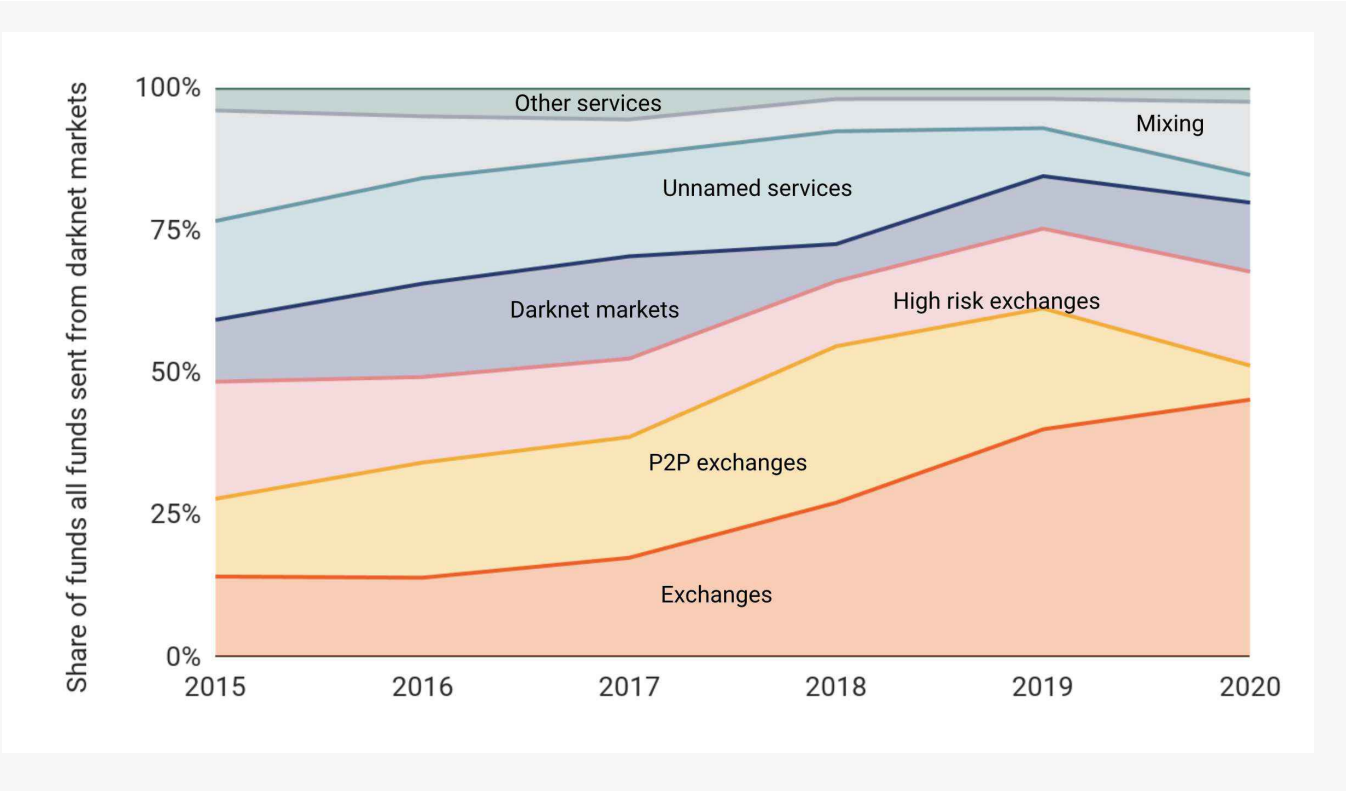


Currencies included: BCH, BTC, LTC, USDT

Standard exchanges, peer-to-peer (P2P) exchanges, high-risk exchanges, and other darknet markets account for nearly all of the cryptocurrency sent to darknet markets. Interestingly, 2020 has seen standard exchanges send a larger share of total darknet market revenue — about 45% in 2020 versus 31% in 2019 — while P2P exchanges' share has declined significantly. Given that standard exchanges tend to be more popular and easier to use, this could suggest that darknet markets attracted more first-time customers who are new to cryptocurrency in 2020, possibly due to declines in street sales during the Covid pandemic.

Below, we see the types of services receiving funds from darknet markets, which we use to approximate where darknet market vendors and administrators are cashing out their cryptocurrency earnings.

Destination of funds leaving darknet markets | 2015 - 2020

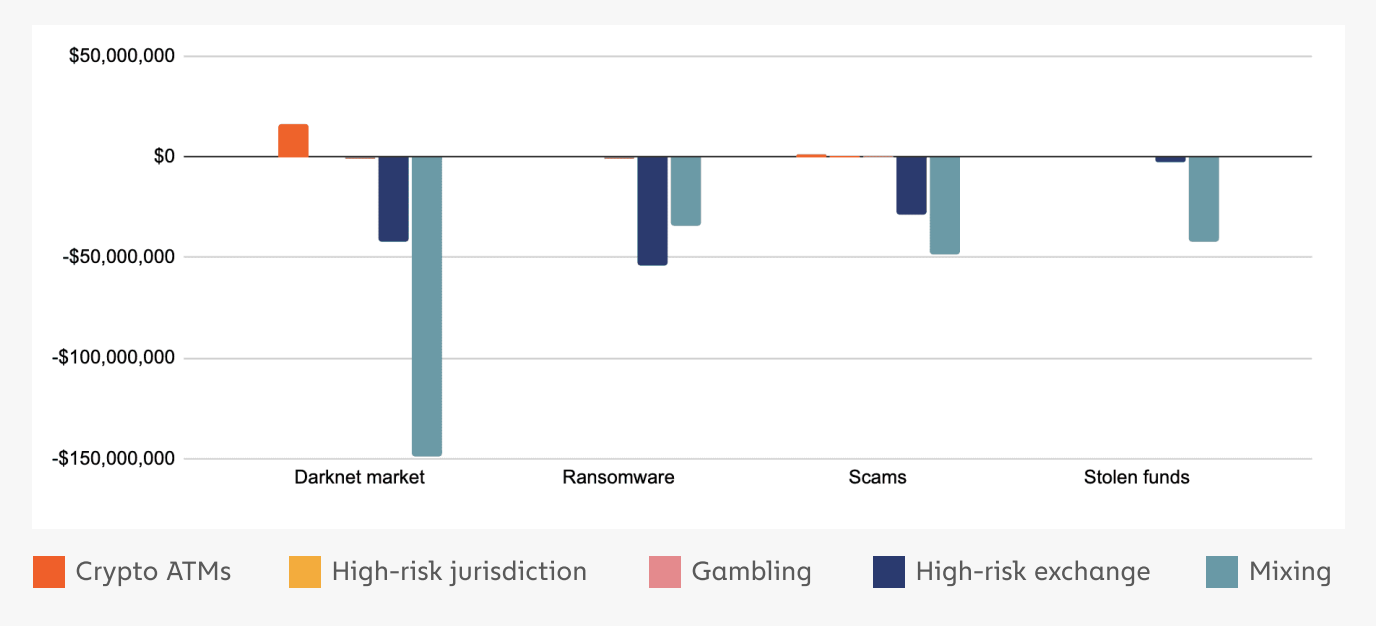


Currencies included: BCH, BTC, LTC

The numbers are somewhat similar to those on the receiving side, with standard exchanges taking in a larger share in 2020 compared to 2019, and P2P exchanges' share declining. However, we also see a significant uptick in the amount going to mixers as well, with their share more than doubling from 4.8% in 2019 to 13.7% in 2020. This may reflect increasing caution from darknet market vendors and administrators following law enforcement crackdowns.

Finally, if we combine these two analyses and examine darknet markets' net sending relationship with different cryptocurrency service types — meaning, the amount darknet market addresses receive from each service type minus what they send — and compare the results with other crime types, we see that darknet markets have an interesting relationship with cryptocurrency ATMs.

Criminal wallets' net value received by service type | 2020



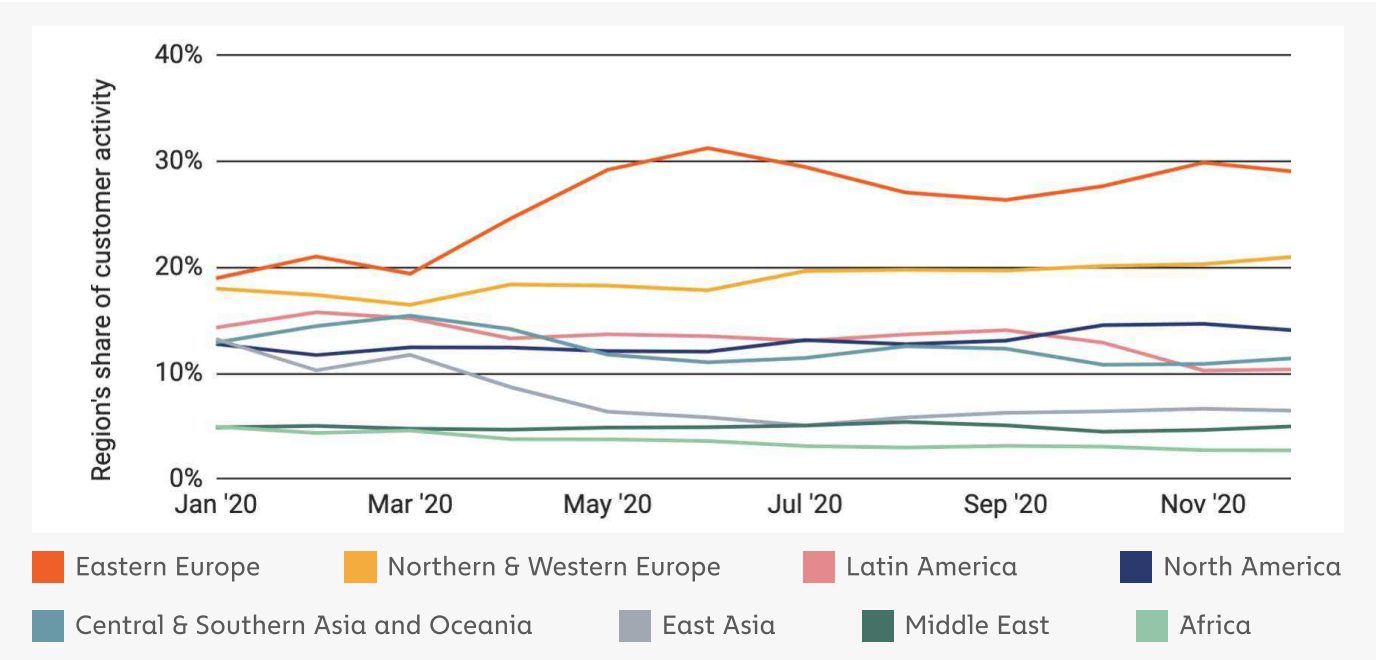
Currencies included: BAT, BCH, BTC, ETH, LTC, MKR, OMG, PAX, TUSD, USDC, USDT

On the chart above, a bar with a positive value means addresses in that crime category received more than they sent from that particular service type, and a negative value means they sent more. It's no surprise that every crime category has a negative net sending relationship with mixing services. Mixers are typically used to launder criminal funds, so it makes sense that illicit addresses would be sending more to mixers than they get back. But we also see that as a category, darknet markets received over $16.5 million on net from cryptocurrency ATMs. No other crime category-service pair had a similar relationship with ATMs. This could suggest that darknet market customers are funding their buying activity in fiat by depositing it at cryptocurrency ATMs, unlike those sending funds to addresses associated with other types of crime.

Geographic trends in darknet markets

Looking at transaction data across all darknet markets, we see that users in Eastern Europe, Northern & Western Europe, and North America are the biggest darknet market customers, based on the specific services that have sent the most cryptocurrency to darknet markets.

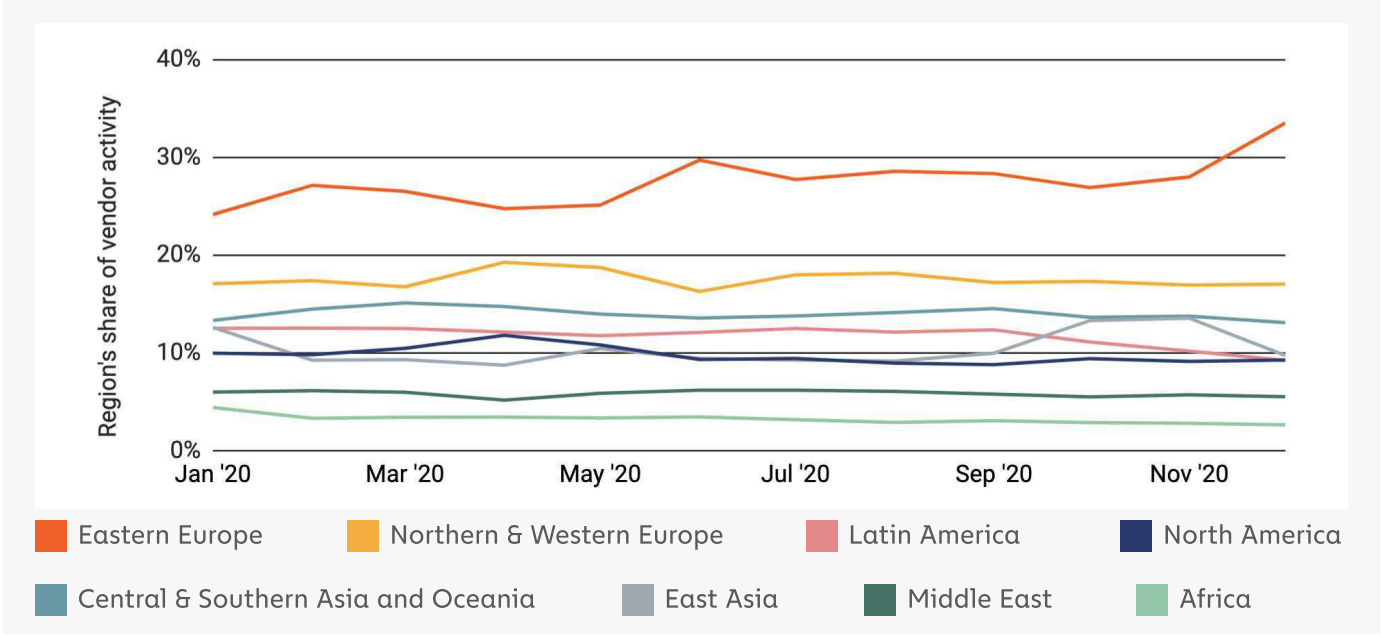
Value sent from drug-focused darknet market customers by region
|2020



Currencies included: BCH, BTC, ETH, LTC, OMG, PAX, USDC, USD

Eastern Europe also receives by far the most value from darknet market vendor addresses, though much of this is due to massive volumes from Hydra, whose size makes it a major outlier. Northern & Western Europe receives substantial amounts as well, as does Central & Southern Asia and Oceania, East Asia, Latin America, and North America.

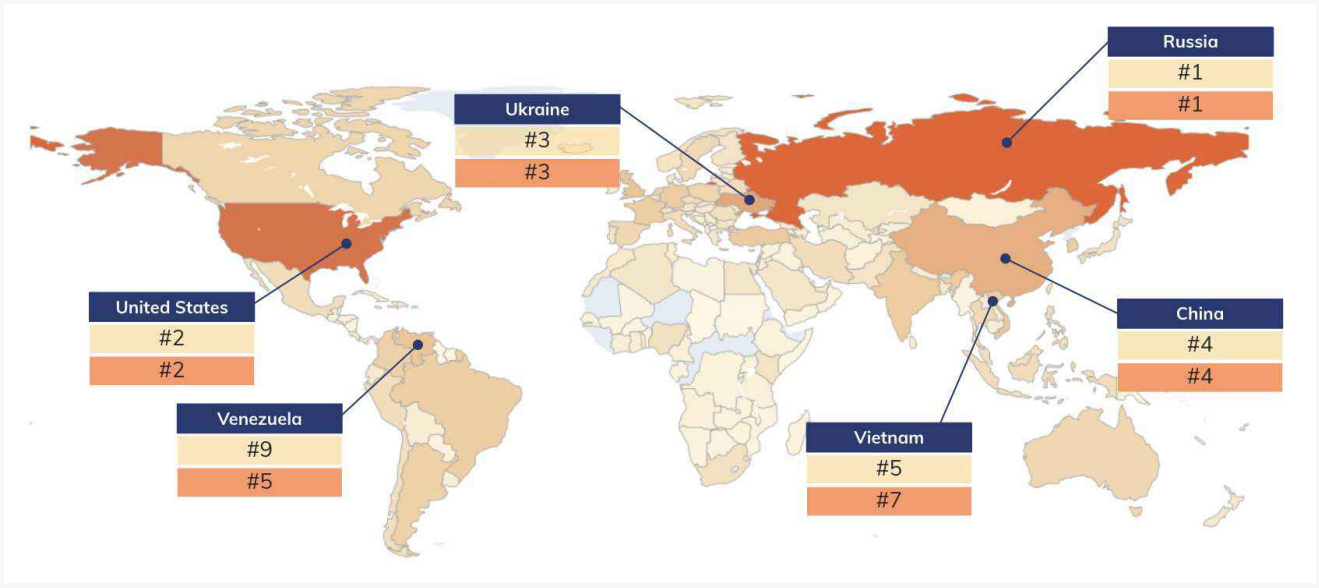
Value sent from drug-focused darknet market customers by region
|2020



Currencies included: BTC, BCH, LTC

That pattern fits with what we know about the geography of the global drug trade. Broadly speaking, drugs are grown or manufactured in Latin America and Asia and consumed in North America and Northern & Western Europe. Darknet vendors and administrators typically launder funds through cryptocurrency services — often over-the-counter (OTC) brokers — in China or Eastern Europe. We can see some of this activity in the blockchain data associated with darknet market transactions. On the map below, we show some of the most active individual countries' exposure to darknet markets in terms of value both sent and received.

Top countries by value sent to or received from drug-focused darknet markets | 2020



Currencies included: BCH, BTC, LTC, USDT

The geographic flows involving darknet markets roughly match what we would expect to see. The United States, Russia, Ukraine, and China dominate in terms of value both sent to and received from darknet markets. Venezuela and Vietnam also rank high on both sides, with their activity skewed slightly more toward darknet market buying, which could be related to the drug manufacturing activity prominent in both countries. We also suspect that a good deal of China and Russia's volume received by darknet markets represents funds flowing to money laundering services concentrated in those countries.

In the table below, we show the top ten countries by total cryptocurrency transaction volume flowing through darknet markets, with links to relevant news stories we believe exemplify each country's activity and role in the global drug trade.

Country	Value sent to darknet markets	Value received from darknet markets	Total value sent to or received from darknet markets	Rank of values (of 171 countries)			Examples and notes
				Value sent to darknet markets	Value received from darknet markets	Total value	
Russia	$169 M	$119 M	$288 M	1	1	**1**	Thanks to Hydra Marketplace, Eastern Europe is the only region with a criminal service as one of the top ten entities sending cryptocurrency value to the region.
United States of America	$115 M	$64 M	$179 M	2	2	**2**	A Costa Rican pharmacist and a co-conspirator were indicted in a US court for selling hundreds of thousands of opioid pills worth millions of dollars to US darknet market customers.
Ukraine	$47 M	$52 M	$98 M	3	3	**3**	Ukraine tops the Chainalysis Global Crypto Adoption Index which measures grassroots adoption, including exposure to Hydra Marketplace which Ukraine shares with Russia and other countries in Eastern Europe.
China	$45 M	$43 M	$87 M	4	4	**4**	Illicit proceeds are often laundered through OTC brokers based in China, a pattern that is also seen with fiat currency.
United Kingdom	$33 M	$22 M	$56 M	6	6	**5**	170 arrested and $6.5 million seized after law enforcement blew up ring importing MDMA from China and Canada to sell in US, UK and continental Europe.
Venezuela	$35 M	$20 M	$55 M	5	9	**6**	Former President of Venezuela Nicolás Maduro Moros and top government officials charged with narco-terrorism, corruption, drug trafficking.
Vietnam	$24 M	$24 M	$49 M	7	5	**7**	The most common material on Vietnamese darknet markets are narcotics, cryptocurrency exchange sites, and child abuse material.
Turkey	$23 M	$22 M	$45 M	11	7	**8**	Drug trafficking has been a big problem in Turkey for a long time.
India	$24 M	$18 M	$42 M	8	13	**9**	In a first, Indian drug vendor operating on Empire Market and Majestic Garden was arrested for shipping drugs to the US, UK, Romania, and Spain among other countries.
Germany	$23 M	$18 M	$42 M	10	11	**10**	Last year, the Dutch police and Europol arrested three men in Germany for running Wall Street Market. Germany has the third highest daily average TOR users after the US and Russia as of 2020.

Currencies included: BCH, BTC, LTC, USDT

It will be interesting to observe in 2021 and beyond how these currency flows change if more of the global drug trade continues to move to cryptocurrency, particularly on the money laundering side.

Market closures: Covid is causing shipping issues, but natural competitive forces are causing darknet market consolidation

As we mentioned above, while darknet market revenue in 2020 surpassed that of 2019, the overall number of purchases, and likely customers as well, has fallen significantly, though the remaining purchases are for higher values. Similarly, the number of active markets has fallen, with several prominent ones shutting down and fewer new ones popping up to take their place.

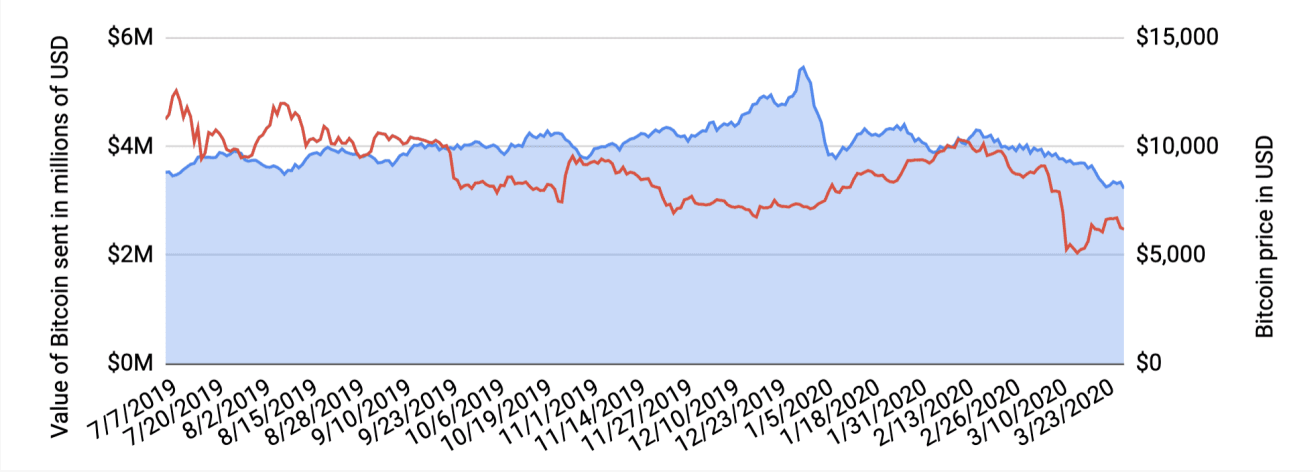
Why is this happening? One might think the ongoing Covid crisis is the obvious answer. As we'll explore below, the pandemic has indeed strained postal systems around the world, leading to delivery failures and delays for many darknet market vendors. But the experts we spoke to don't think that Covid is to blame for this year's rash of market closures. Instead, it appears that ever-increasing competition combined with the efforts of law enforcement are causing the darknet market ecosystem to consolidate to a few big players — a pattern familiar to the technology industry and other markets, both legal and illegal. Below, we'll share our findings on darknet market activity in 2020, how it's changed throughout the pandemic, and provide possible reasons for why so many markets have closed.

Darknet markets' initial reaction to the Covid pandemic and trends since March

Earlier this year, roughly three weeks after lockdowns began in the United States, we examine d the pandemic's effects on darknet market activity and found that transaction volume had dropped following a sharp decline in the price of Bitcoin and other cryptocurrencies.

Value of Bitcoin sent to darknet markets, 7-day moving average

| Jul '19 to Mar'20

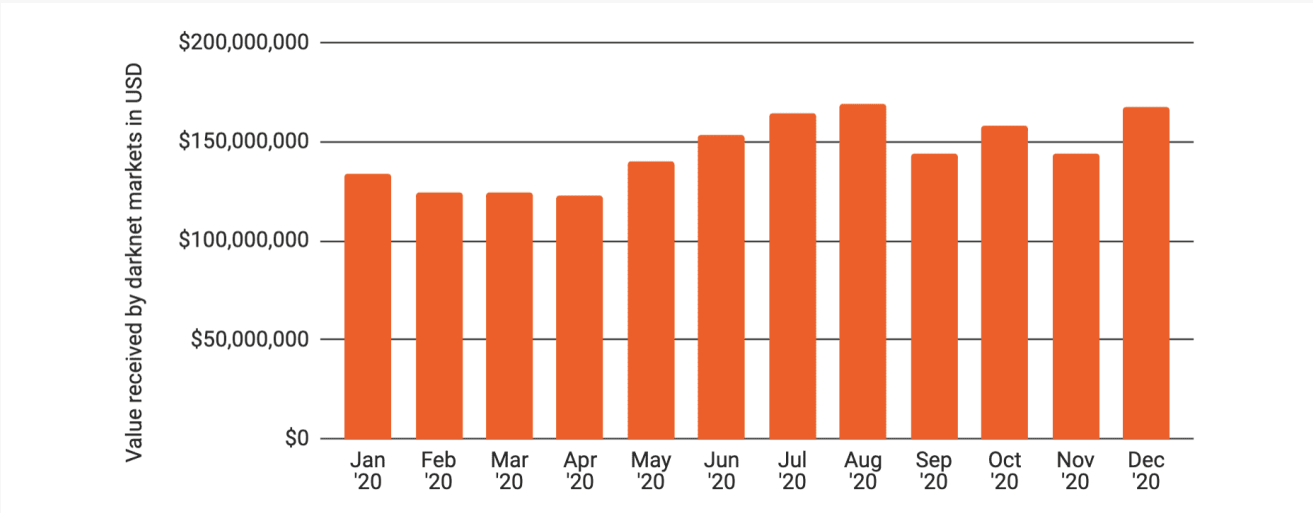


Currencies included: BCH, BTC, LTC, USDT

Notable in our findings was that up until this point, darknet market activity appeared to be impervious to Bitcoin market activity. Fluctuations in Bitcoin's price, which have always been common, rarely appeared to play a role in darknet market consumers' purchasing activity. However, when Bitcoin's price began to fall in mid-March following the first round of U.S. lockdowns, so too did darknet market activity.

But this change would prove to only be temporary. Starting around May, darknet market revenue returned to its previous state, no longer shifting in sync with Bitcoin's price. Since then, darknet markets' monthly revenue has steadily grown, save for small drops in September and November, which largely fall in line with seasonal trends.

Monthly darknet market revenue | 2020

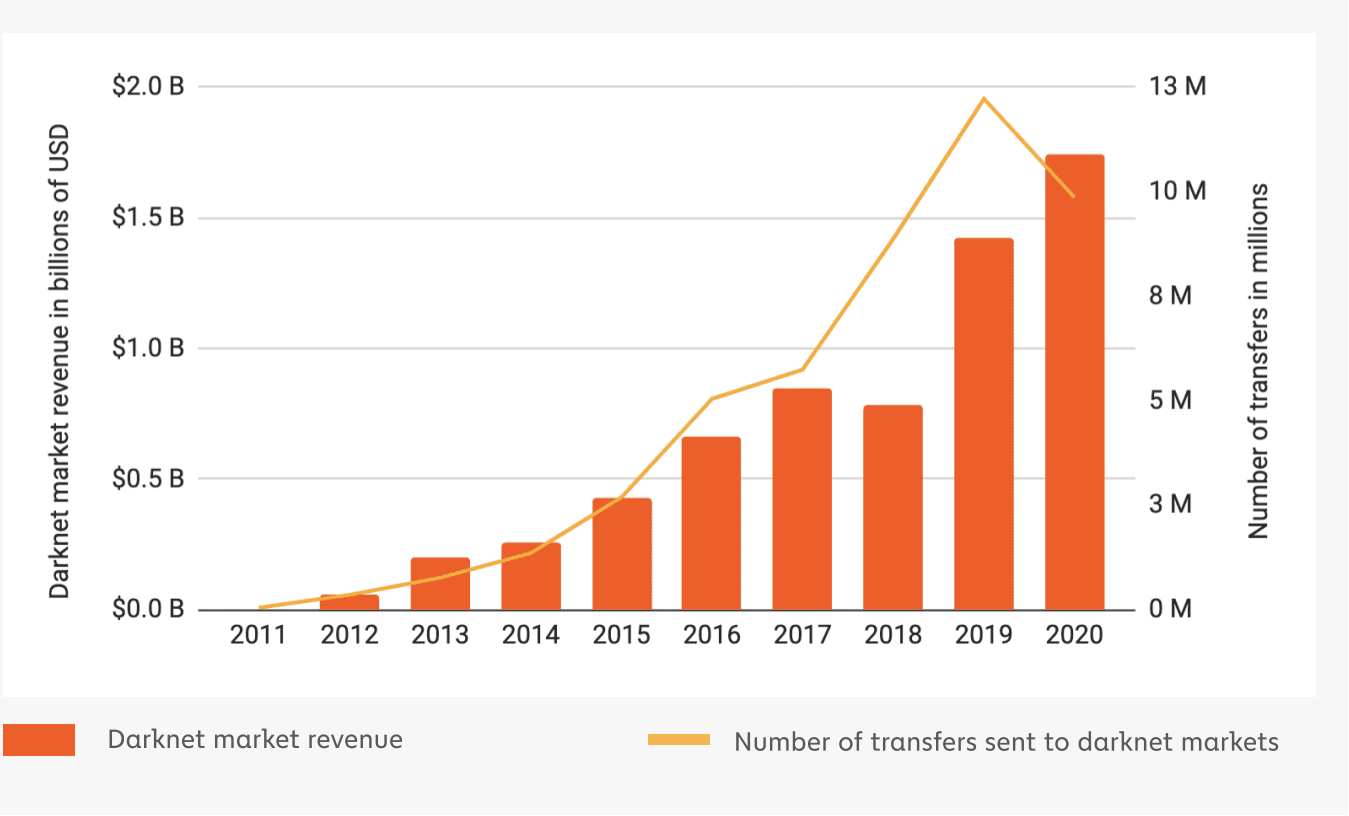


Currencies included: BCH, BTC, LTC, USDT

With these latest developments, overall darknet market revenue for 2020 surpassed that of 2019. But while total revenue may not change, other numbers indicate that tough times could be ahead for darknet markets.

Darknet market revenue vs. Total transfers to darknet markets

| 2011-2020

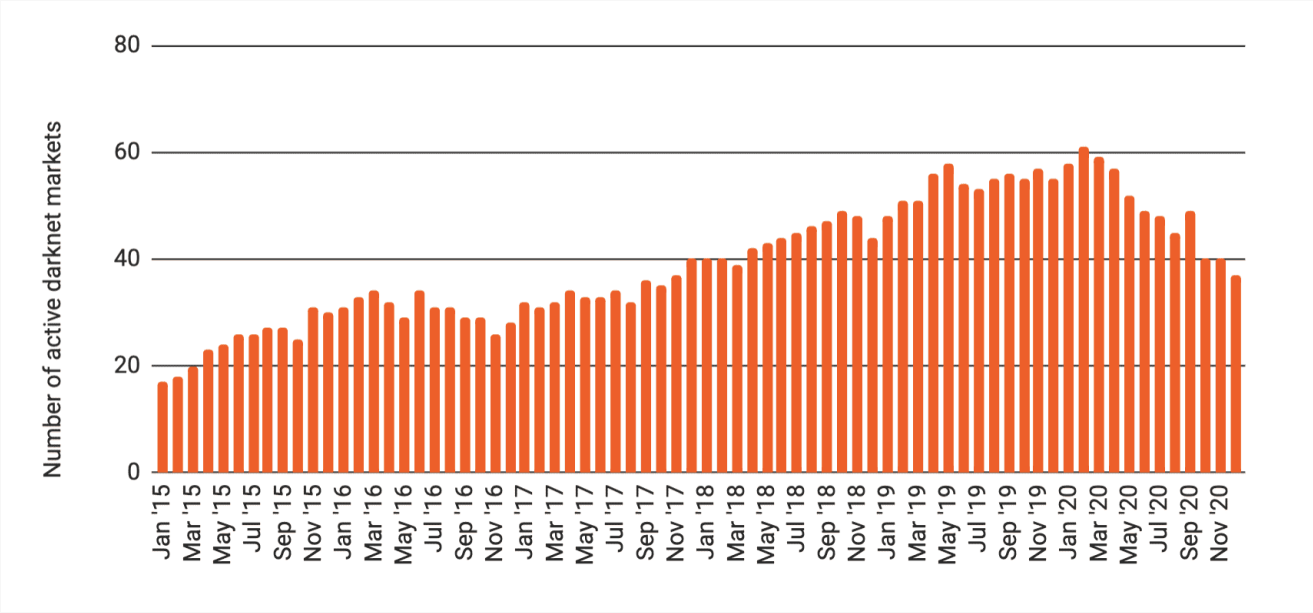


Currencies included: BCH, BTC, LTC, USDT

The graph above shows both total darknet market revenue by year, as well as the total number of transfers to darknet markets, which we can use to roughly approximate the number of individual customers and purchases. Interestingly, we see that while revenue surpassed its 2019 total, total transfers to darknet markets stand at just under 10 million — well below the 2019 total of over 12.0 million. The numbers show that customers in 2020 are making fewer purchases but for larger amounts per purchase compared to 2019. This could indicate that casual buyers or those buying drugs for personal use are shifting away from darknet markets, while those buying in larger amounts — either for personal use or to sell to others — are purchasing more. It could also mean that some casual buyers have begun placing larger orders to stock up amidst uncertainty.

We've also seen more darknet market closures in 2020, including prominent markets like Flugsvamp 2.0 and Empire. We see this reflected in the graph below, which shows the number of active markets in each month (active meaning the market has received at least $100 worth of cryptocurrency in a given month) since January 2015.

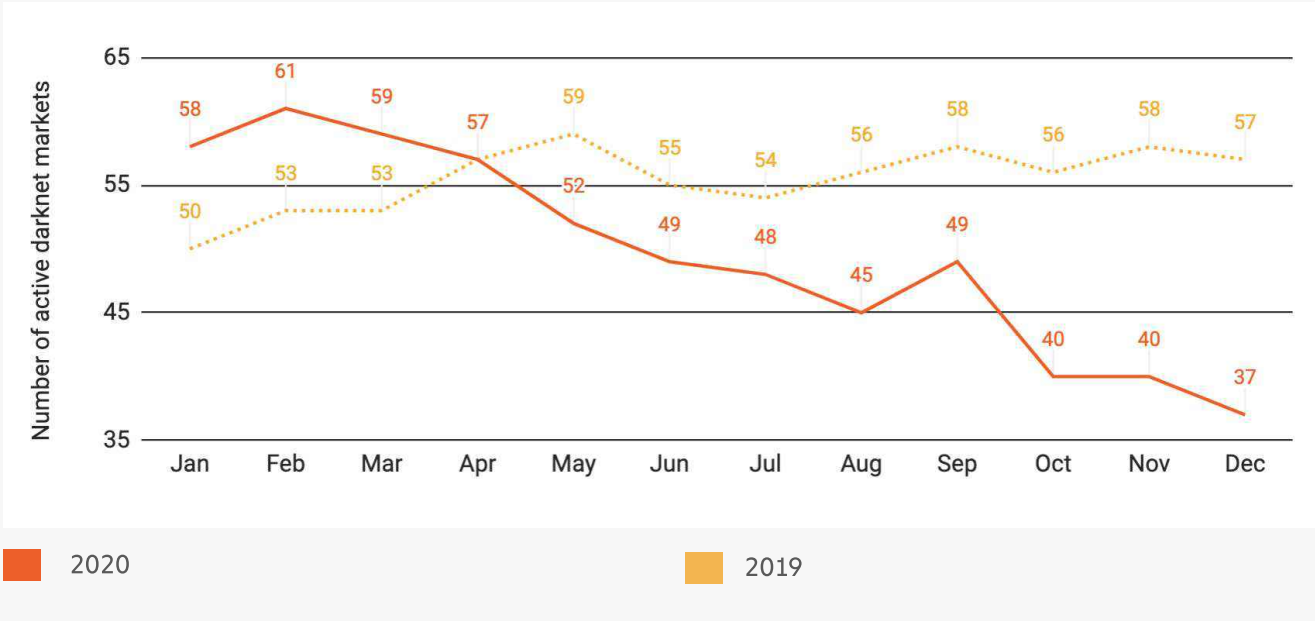
Number of active darknet markets | 2015-2020



Currencies included: BCH, BTC, LTC, USDT

While some markets claim their closures are only temporary, the 37 darknet markets active in December 2020 is the lowest total since November 2017. We saw no such decline in 2019. In fact, this year's decline in active markets follows a period of modest growth in the number of active markets from 2018 through February 2020.

Number of active darknet markets: 2019 vs. 2020

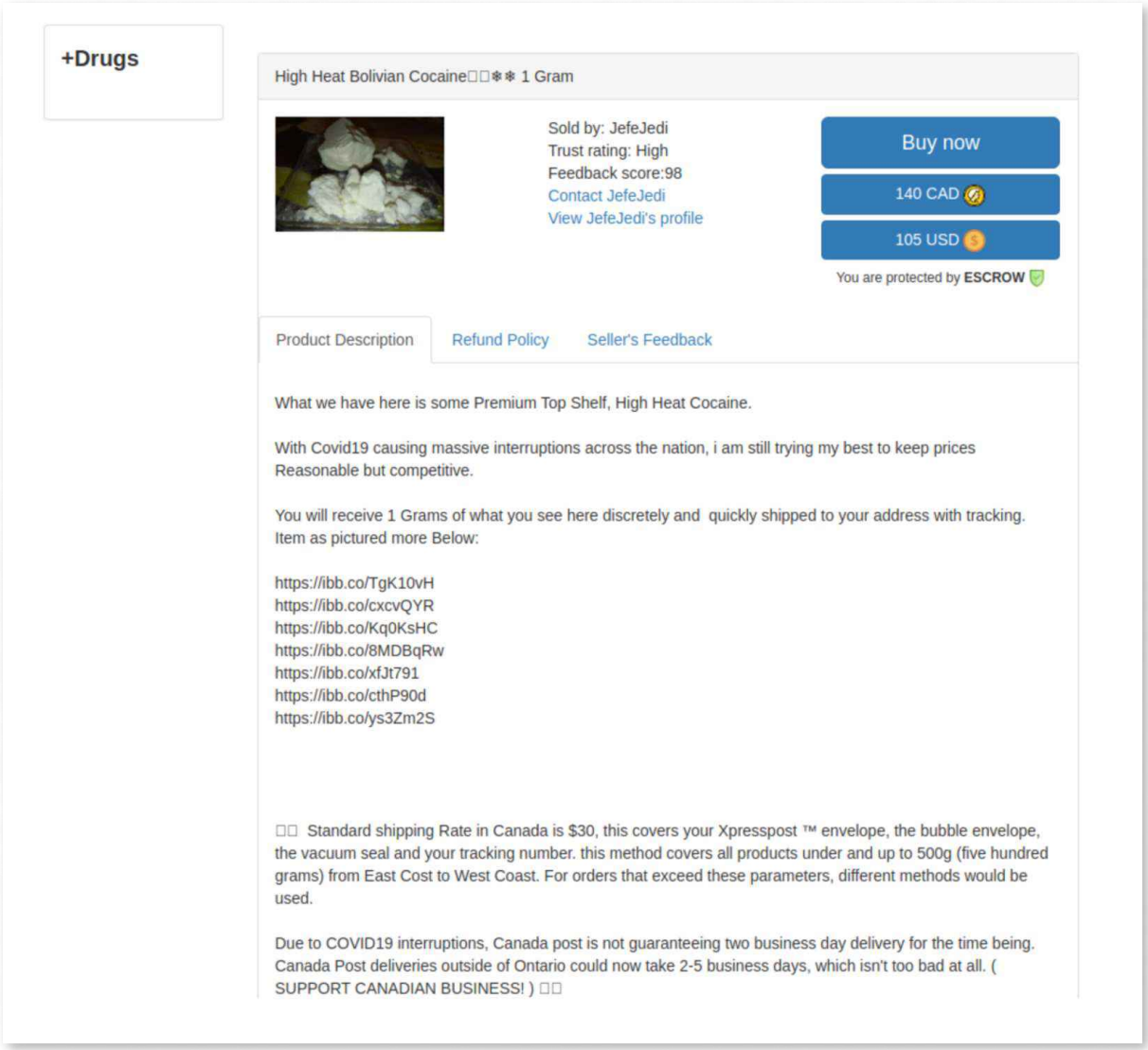


Currencies included: BCH, BTC, LTC, USDT

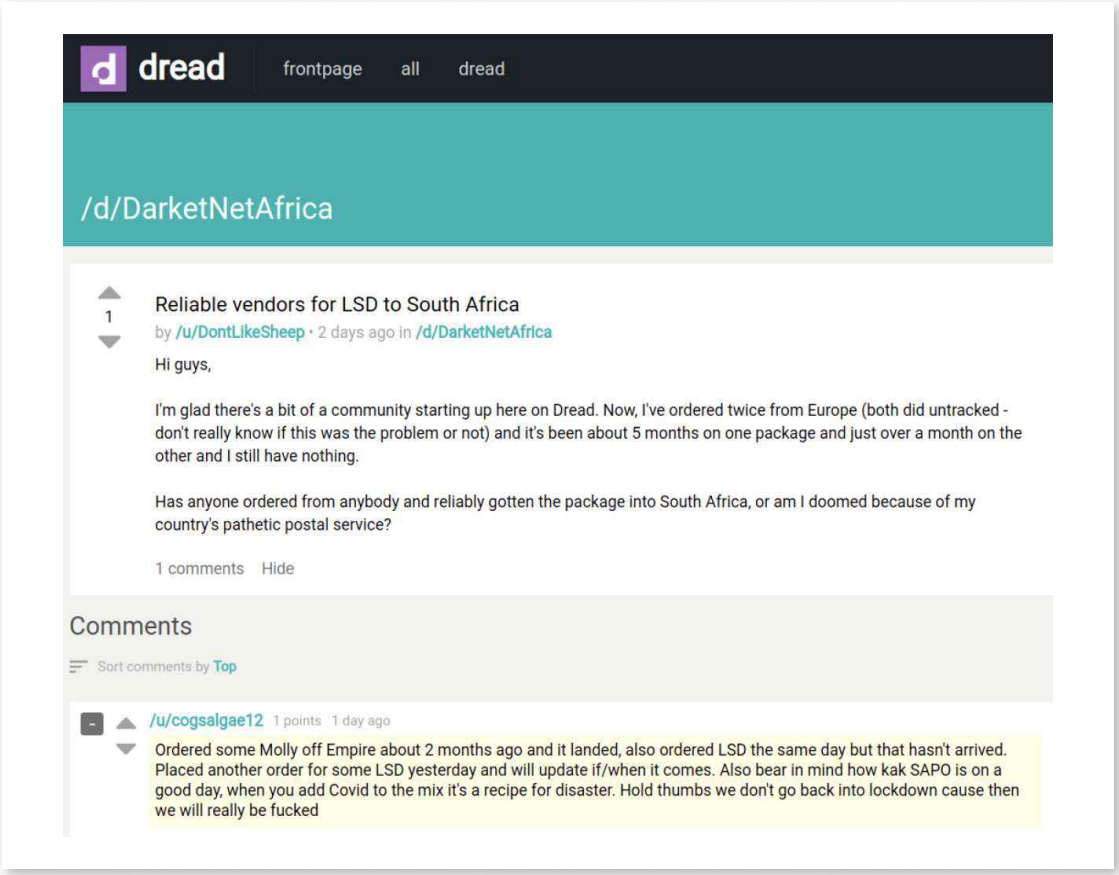
It's often difficult to tell why markets shut down when they do, as administrators commonly pull exit scams, in which the market ceases operations but publicly appears to still be active so that administrators can continue collecting money from purchases that will never be fulfilled. Other markets have fallen victim to denial-of-service (DoS) attacks from other markets, in some cases closing as an apparent result. We saw both phenomena in the case of Empire Market, a large and widely trusted darknet market whose operators exit scammed in 2020 two days after being hit by a DoS attack.

Is Covid causing darknet markets to close?

Covid has undoubtedly hindered darknet markets' sales and operations by causing supply chain disruptions, particularly shipping delays. Darknet market observers have seen this in the form of customer complaints on darknet market-focused forums like Dread and in notes from vendors setting expectations for buyers.



A darknet market vendor warns prospective buyers of shipping delays



Darknet market customers blame Covid for delayed orders

The evidence isn't just anecdotal either. Criminology researchers Andréanne Bergeron, David Décary-Hétu, and Luca Giommoni recently published a study analyzing hundreds of darknet market drug sales made before and after Covid lockdowns began in the U.S. and Europe to determine how much the virus impacted operations. They found that in the pre-Covid period of January 1 to March 21, 2020, between 60% and 100% of all orders on any given day were successful. After Covid lockdowns began, however, the study found that just 21% of all deliveries were successful and on time. Customers and vendors blaming Covid for longer delivery times therefore appear to be correct.

But are shipping delays and other Covid-related operational difficulties causing markets to shut down? We followed up with Lecturer Andréanne Bergeron and Professor David Décary-Hétu, two of the researchers behind the study, to ask their opinion. They reiterated their point that Covid has caused ongoing darknet market delivery delays by placing more strain on postal services. "The world hasn't gone back to normal yet, so it is unsurprising that the market hasn't corrected itself yet. Postal services aren't doing great," said Bergeron.

However, the researchers didn't think that any of the darknet market closures in 2020 were a direct result of Covid. "It's becoming more challenging than ever to run a darknet market — you have to enable security and guard against DoS attacks, and then on top of that there's competition. All of these factors limit the availability of drugs," said Décary-Hétu. He believes that these natural forces of competition, rather than the Covid crisis, were the real reason for increased closures, pointing to Chainalysis data to make his point.

"Excluding Hydra, if all darknet markets take in $250 million per year and administrators make 5% commission, that's $12.5 million total divided by all the markets, where a lot of employees have to be paid. It's simply not worth the risk of spending 100+ years in jail," said Décary-Hétu.

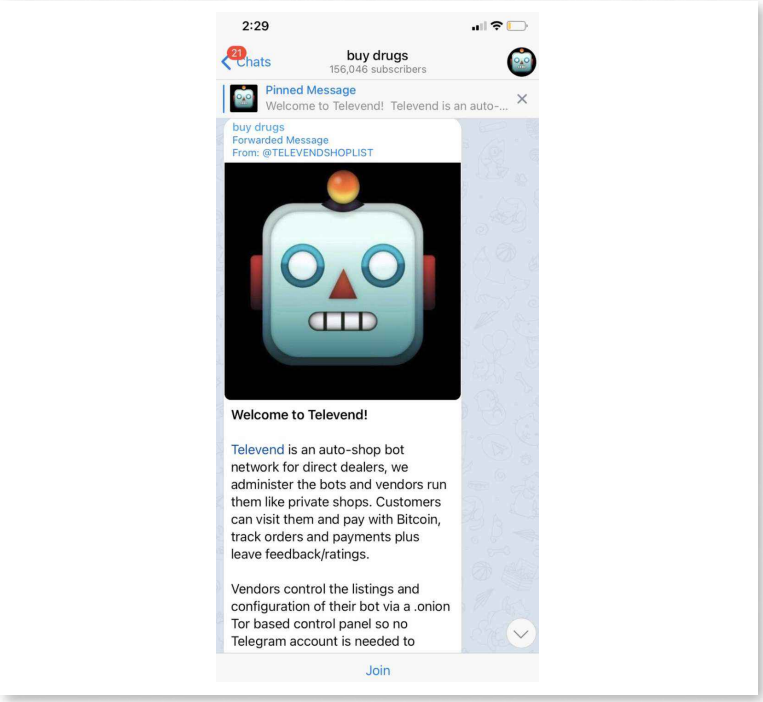
Will more darknet markets fail?

Darknet markets appear to be in a precarious position in 2020, with several closing down and the remainder relying on a shrinking pool of customers for revenue. Counterintuitively, and despite its impact on shipping times, Covid doesn't appear to be the primary cause of these issues. Instead, darknet market consolidation may be the result of competitive forces endemic to the category itself, with Covid at most simply speeding up a trend that already existed.

We see a similar dynamic play out in so-called winner-takes-all markets like technology, in which competition over time naturally whittles the market down to the biggest, most efficient players. There are, of course, key differences between darknet markets and technology companies — Apple, for instance, doesn't need to worry about being shut down by law enforcement. But still, as Professor Décary-Hétu points out, darknet markets are a tough business, and the dwindling number of markets suggests that not all of those standing today will survive.

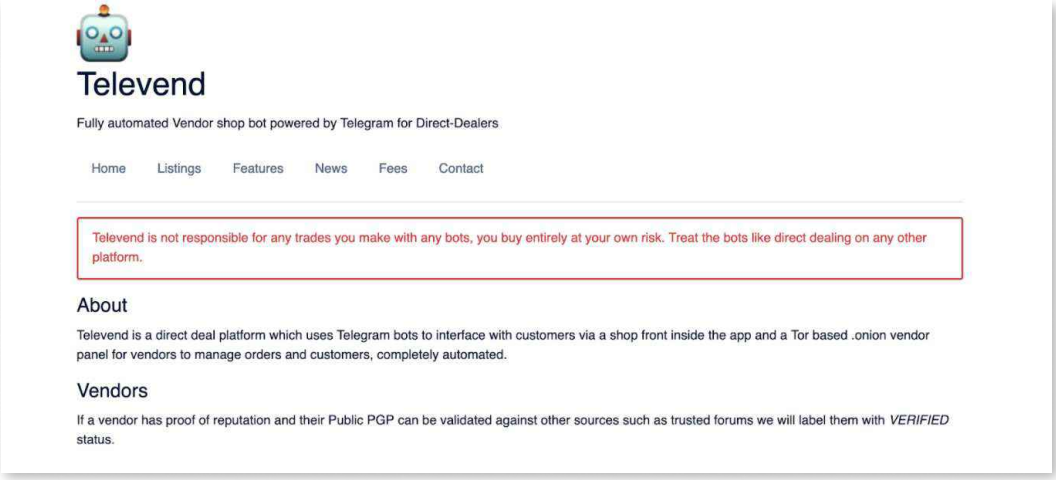
Decentralization is the next step for darknet markets

Despite 2020's difficulties, a new decentralized model embodied by platforms like Televend may solve many of these problems for darknet markets. Televend is a Telegram-based platform with over 150,000 users where darknet market vendors can sell drugs through automated chatbots, whose communications with buyers are highly encrypted.

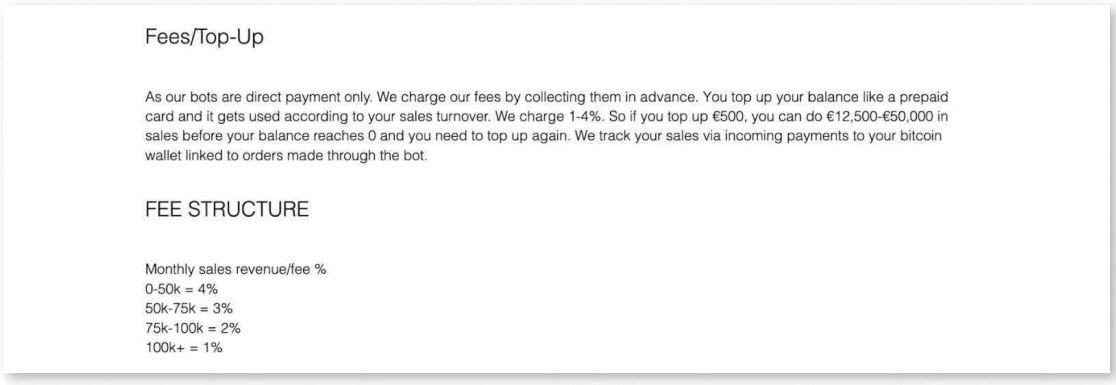


A screenshot of Televend

Buyers simply access Televend's Telegram group, where they find a directory of drug vendors broken down by region and products on offer. From there, they simply place orders with their chosen vendor's chatbot, receive an automatically-generated Bitcoin address to which they send payment, and wait for their drugs to arrive in the mail.



A screenshot from Televend's darknet site



Televend's fee structure explained

Televend receives commissions on each sale, but never actually touches the funds, so there's no central entity for law enforcement to track through blockchain analysis — the transactions blend in much more easily.

We studied the Bitcoin transaction history of one prominent Televend vendor, which you can see a summary of in the Chainalysis Reactor screenshot below.

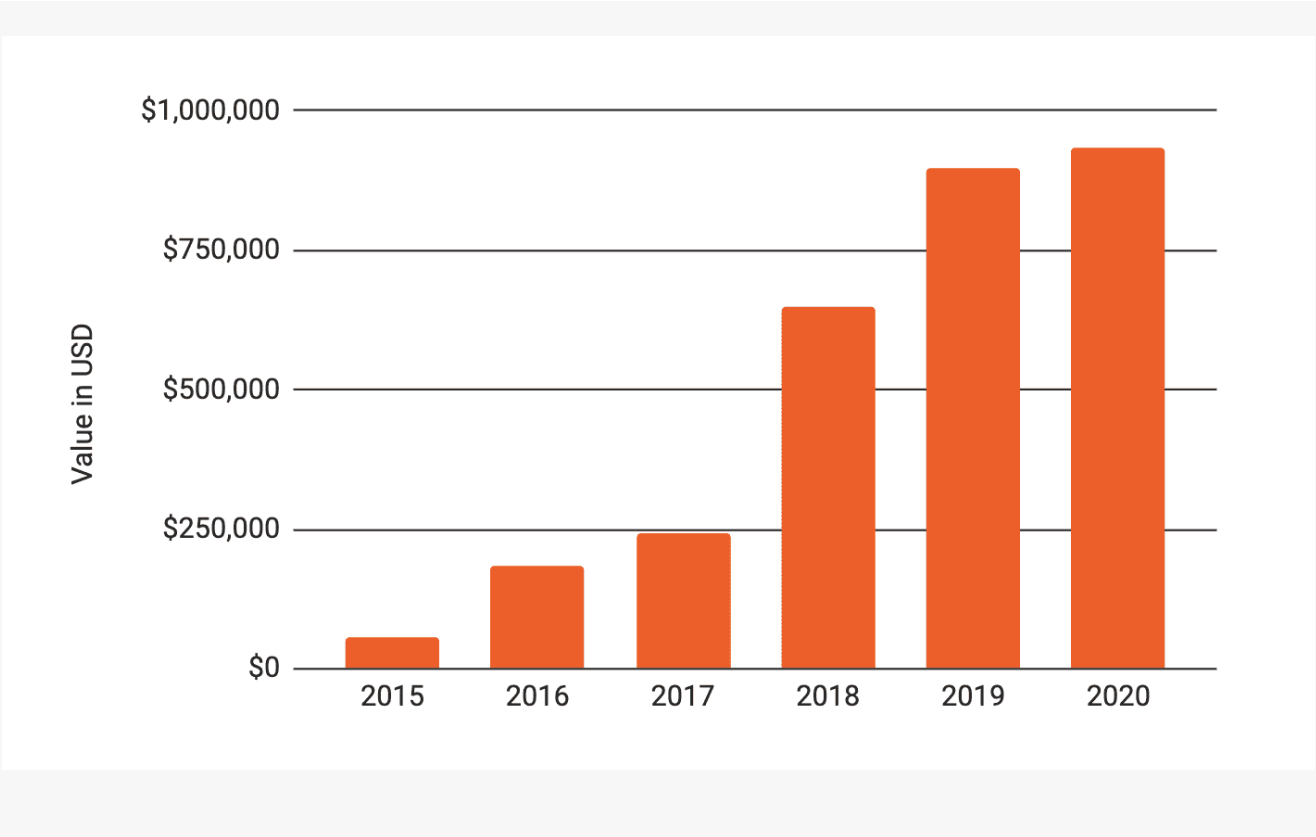
Since Televend became active in October 2020, this vendor's wallet has received over $270,000 worth of Bitcoin across nearly 500 transactions. Customers appear to have paid mostly through cryptocurrency exchanges, which is also where the vendor has sent most of the funds. However, while we don't show it above, this wallet has been active since June 2019 — Televend allows vendors to receive their earnings to any address of their choosing — and received an additional $1.4 million worth of Bitcoin before Televend opened. It therefore appears likely that this vendor was active on traditional darknet markets before migrating to Televend. This vendor is one of over 150 active on Televend, though it's unclear if the others are bringing in as much revenue.

We expect platforms like Televend to grow and take in a larger share of total darknet market revenue in 2021, as their decentralized nature makes them more resilient to attacks from both law enforcement and rival markets. While future decentralized markets may run on platforms other than Telegram, Televend shows that the encrypted messaging platform can offer customers an easy buying experience.

Child sexual abuse material and darknet markets

Darknet markets selling drugs and stolen data take in the vast majority of funds going to this service category. But while their revenue remains minuscule icompared to markets specializing in child sexual abuse material (CSAM), it is especially troubling.

Yearly revenue to child abuse material sites | 2015-2020

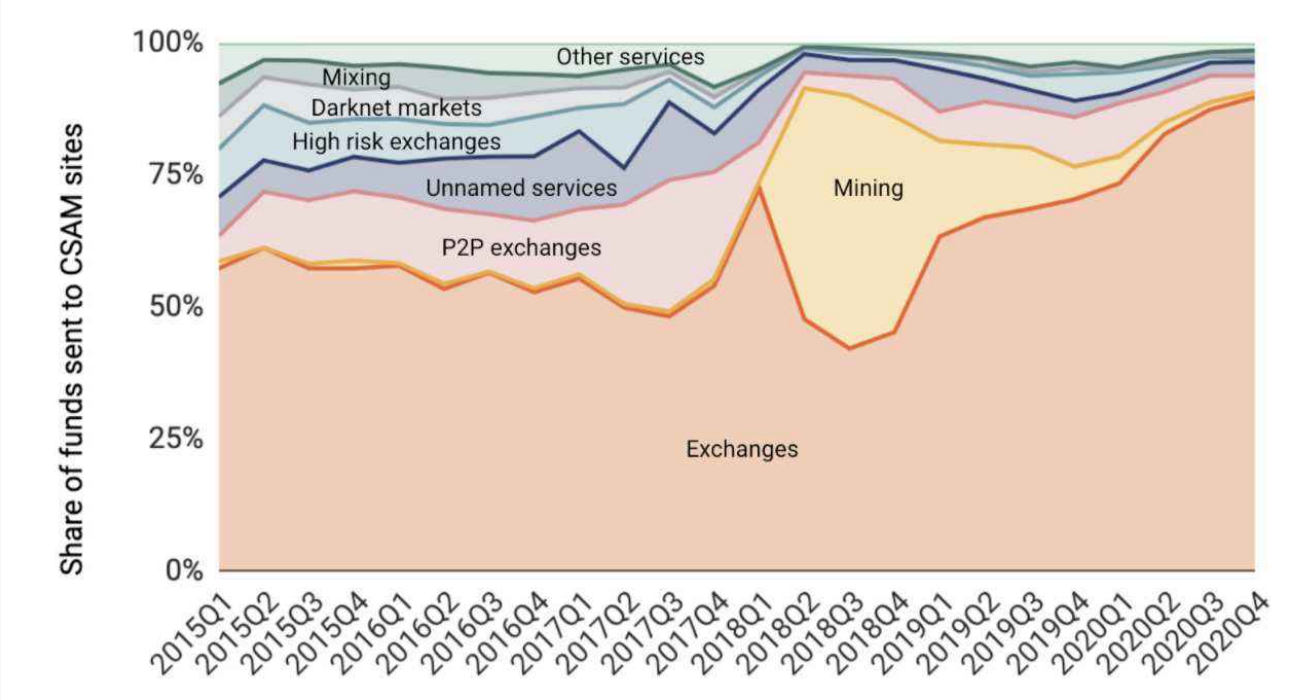


Currencies included: BCH, BTC, ETH, LTC, USDT, ZRX

As we see above, CSAM markets' revenue has increased each year since 2015. For clarification, these figures come from cryptocurrency addresses Chainalysis has attributed as belonging to CSAM markets in the course of our investigations alongside law enforcement, as well as from addresses flagged by Internet Watch Foundation (IWF), a UK-based non-profit dedicated to stopping the online proliferation of CSAM.

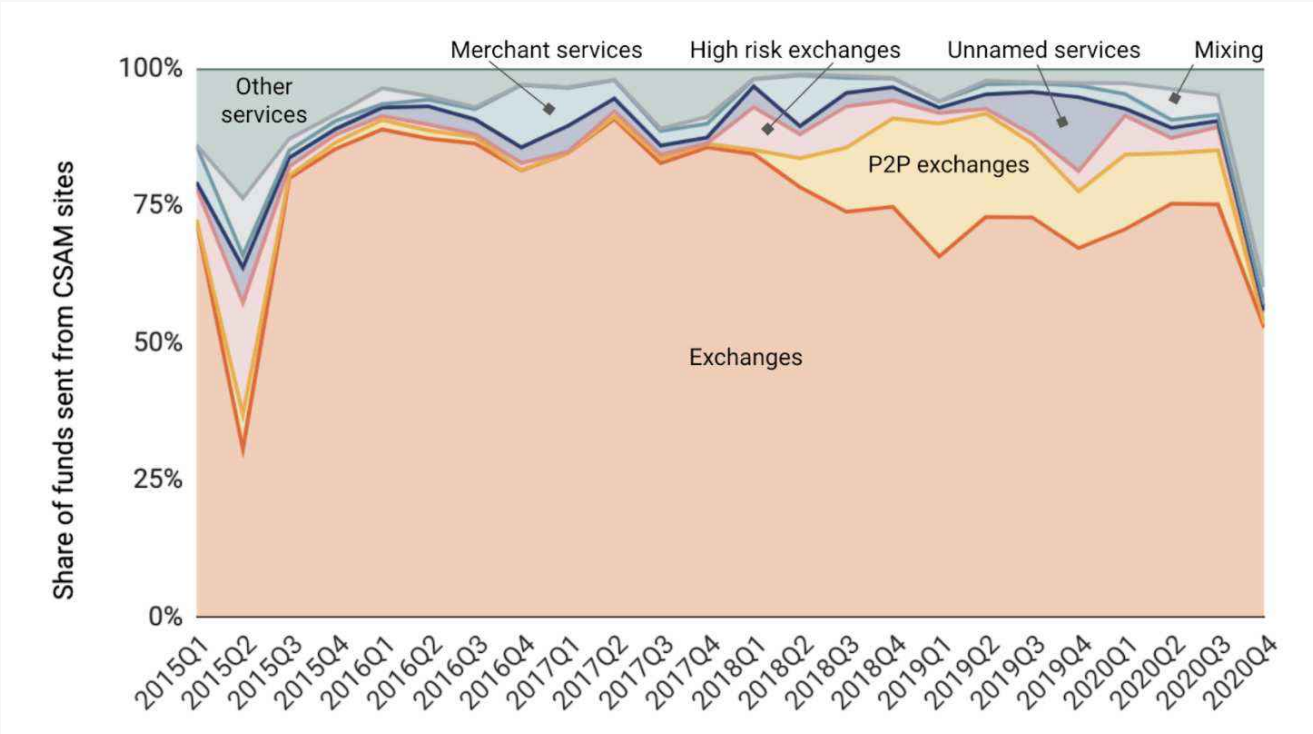
As is the case with most forms of cryptocurrency-based crime, payments to CSAM providers mostly come from exchanges. Similarly, CSAM addresses send most of the funds they receive to exchanges, which is presumably where they convert their cryptocurrency into cash.

Origin of funds sent to child abuse material sites | 2015-2020



Currencies included: BCH, BTC, ETH, LTC, USDT

Destination of funds sent from child abuse material sites | 2015 - 2020

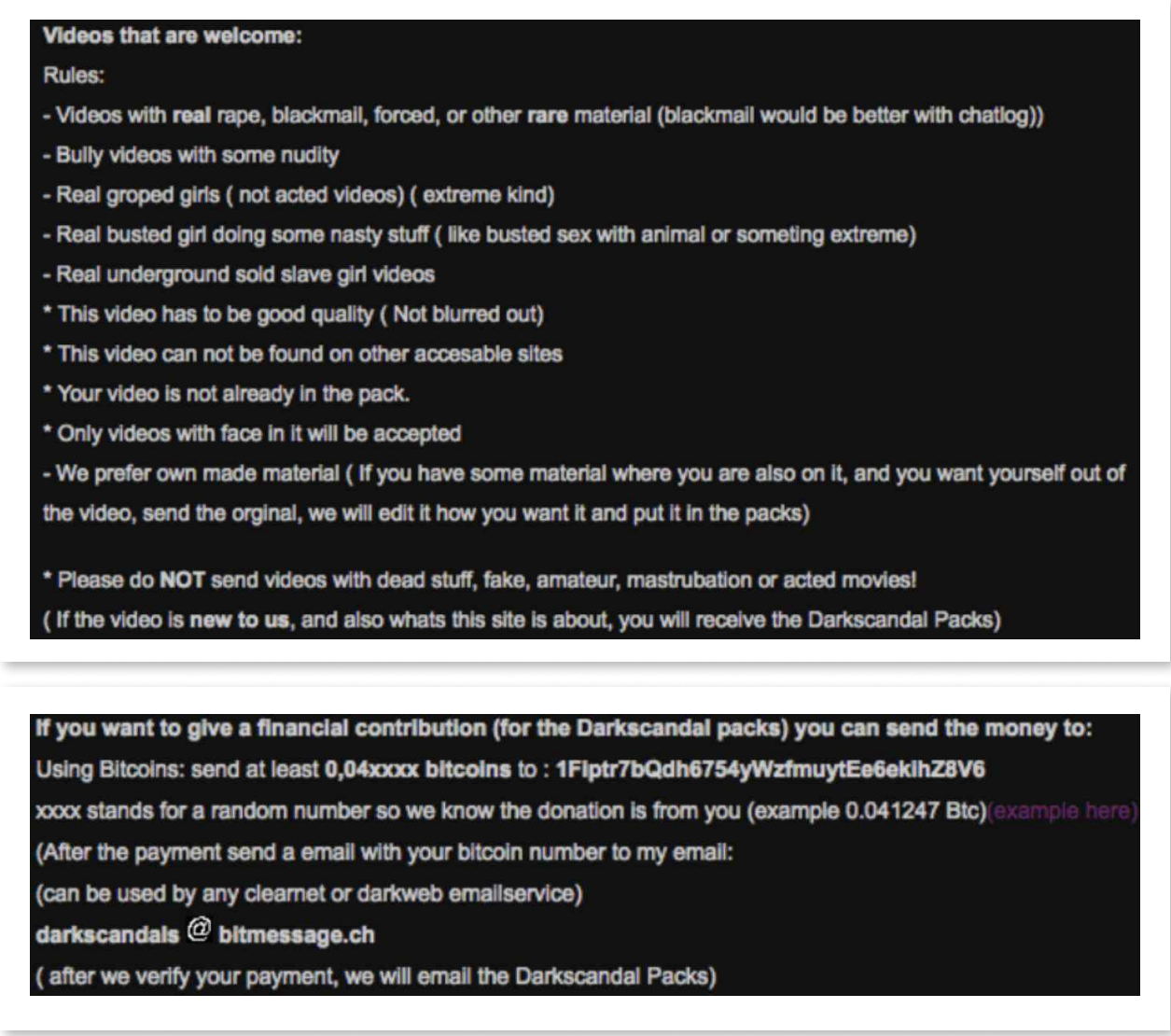


Currencies included: BCH, BTC, ETH, LTC, USDT

This isn't necessarily surprising, as it fits the wider patterns of cryptocurrency-based crime. Still, it's shocking that CSAM buyers and providers would use regulated, compliant exchanges, all of which collect KYC information (we count exchanges that don't in our "high-risk exchange" category), for such serious and rightly stigmatized criminal activity.

Case study: Dark Scandals

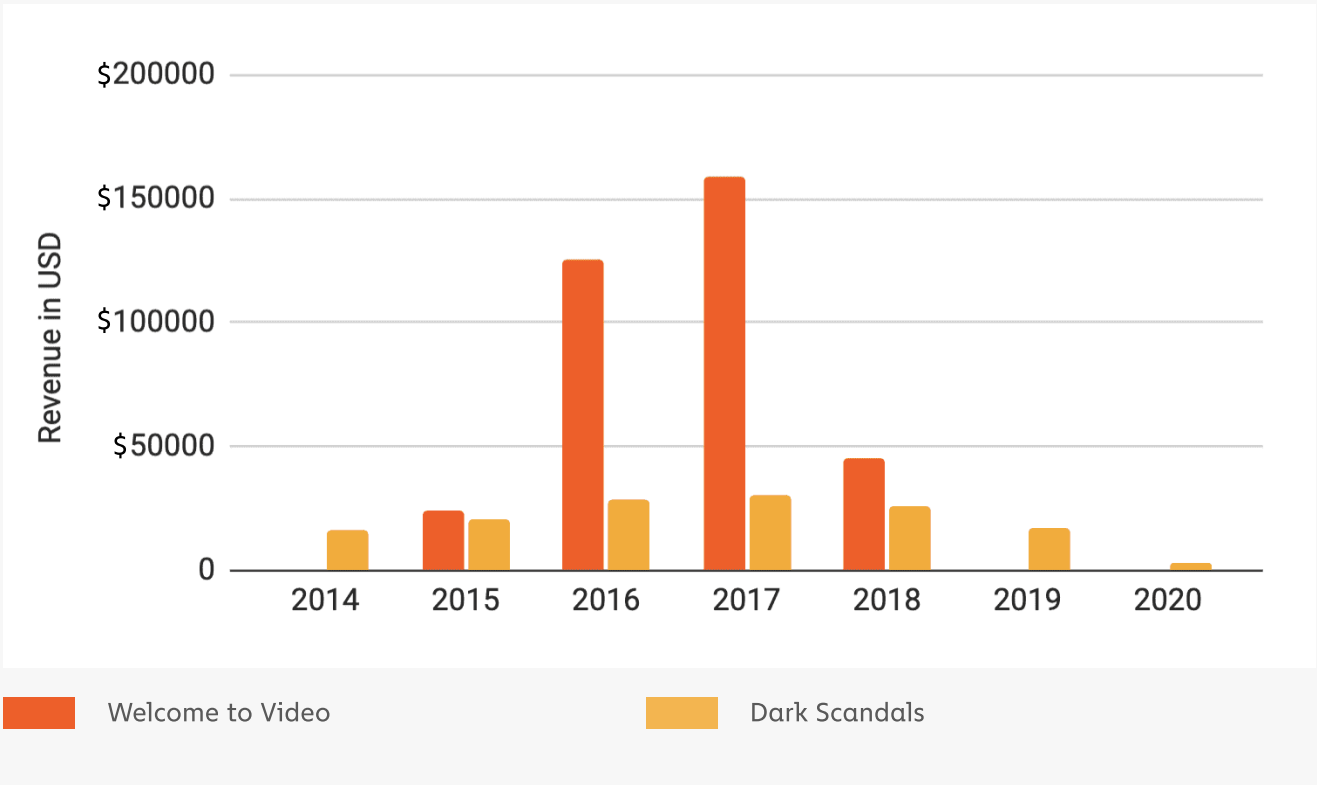
In 2019, Chainalysis helped strike a blow against CSAM on the darknet by assisting authorities in taking down Welcome To Video, the largest ever Bitcoin-powered CSAM marketplace identified to date. In March 2020, we assisted in the takedown of another darknet market for CSAM: Dark Scandals.



Instructions from Dark Scandals on the types of content users should upload

While Welcome To Video hosted more content than Dark Scandals and collected more revenue overall, the latter operated for longer and took in more money per transaction.

Yearly revenue to Welcome to Video and Dark Scandals | 2014-2020

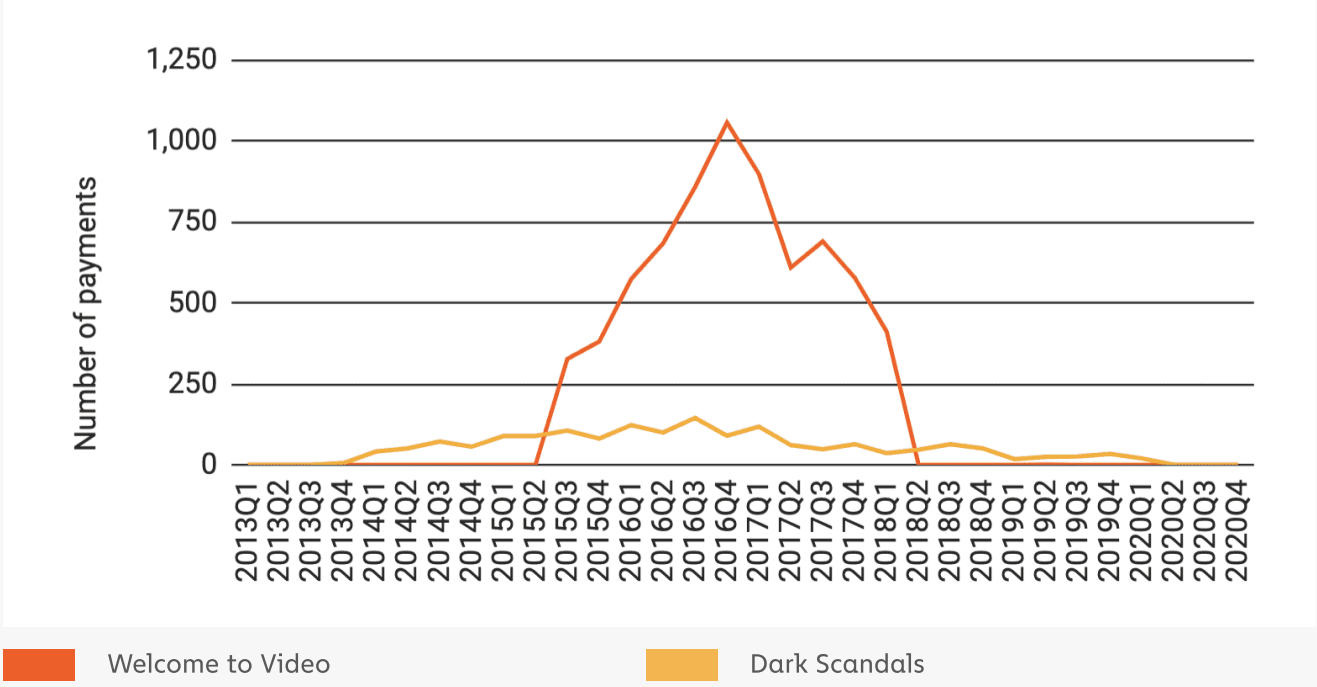


Currencies included: BCH, BTC, LTC, USDT

Overall, Dark Scandals took in just under $143,000 worth of cryptocurrency revenue during its time active from 2014 to March of 2020. We spoke to Special Agent Chris Janczewski of the IRS Criminal Investigations unit that led the Dark Scandals and Welcome to Video investigations, and he told us a bit about how Dark Scandals worked. "Dark Scandals differed from Welcome to Video in that it was all or nothing. Customers could pay once and get access to nearly all of its material, whereas Welcome To Video functioned on a points system where users could upload their own videos or pay money, and use their points to acquire a bit of content at a time. It was common to see people pay into Welcome To Video multiple times, versus just once for Dark Scandals," he said. "The websites themselves varied also. The Welcome to Video site automatically distributed the content, while the Dark Scandals site was more of an advertisement, and the administrator had to manually distribute the content via email and file hosting sites."

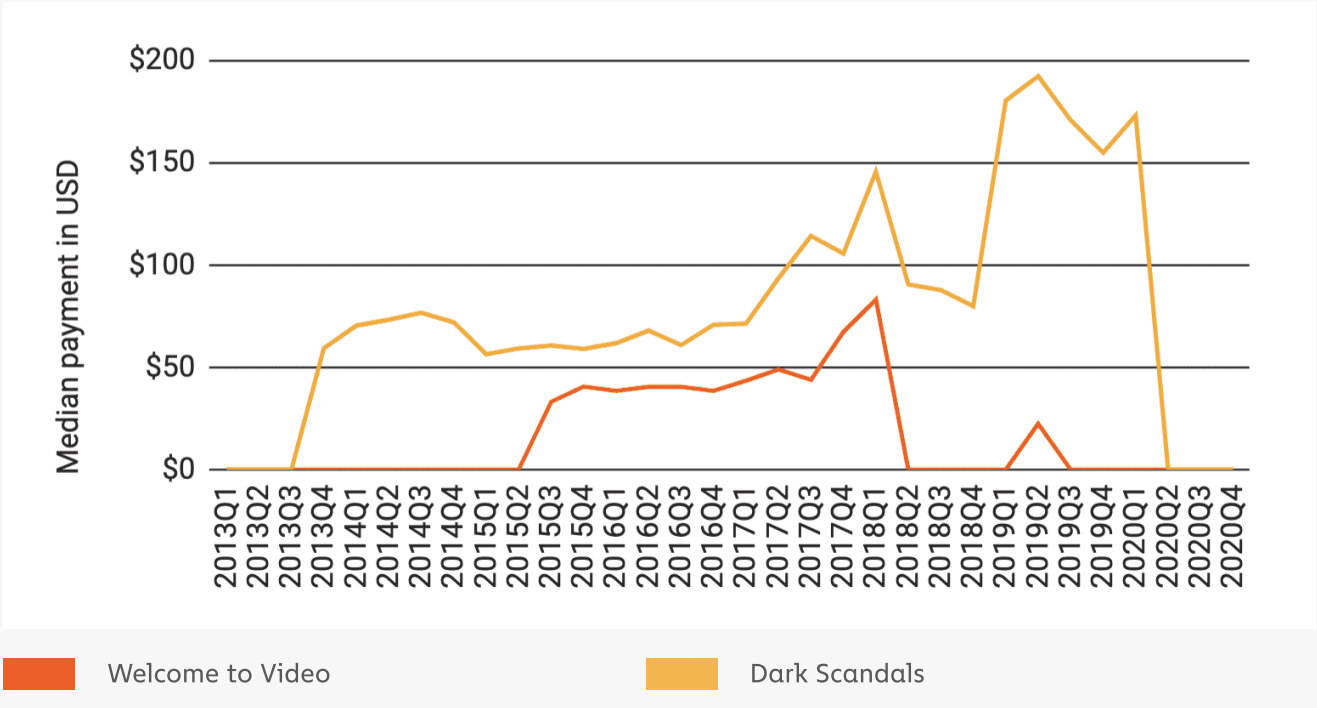
We see this dynamic reflected in a comparison of the two platforms' cryptocurrency transaction history.

Quarterly number of payments sent to Welcome to Video and Dark Scandals | 2014-2020



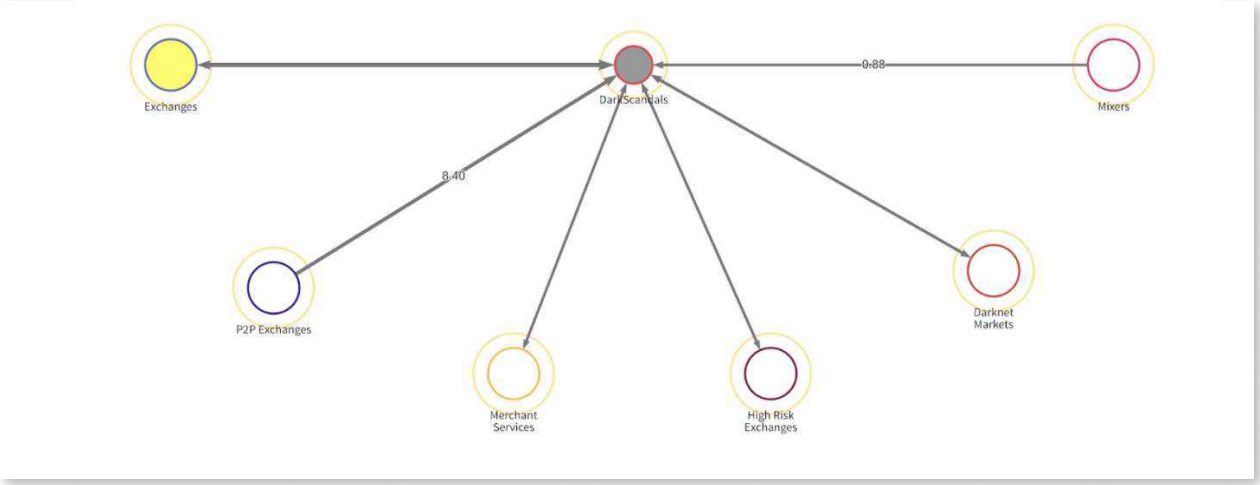
Currencies included: BCH, ETH

Quarterly median payment sent to Welcome to Video and Dark Scandals | 2014-2020



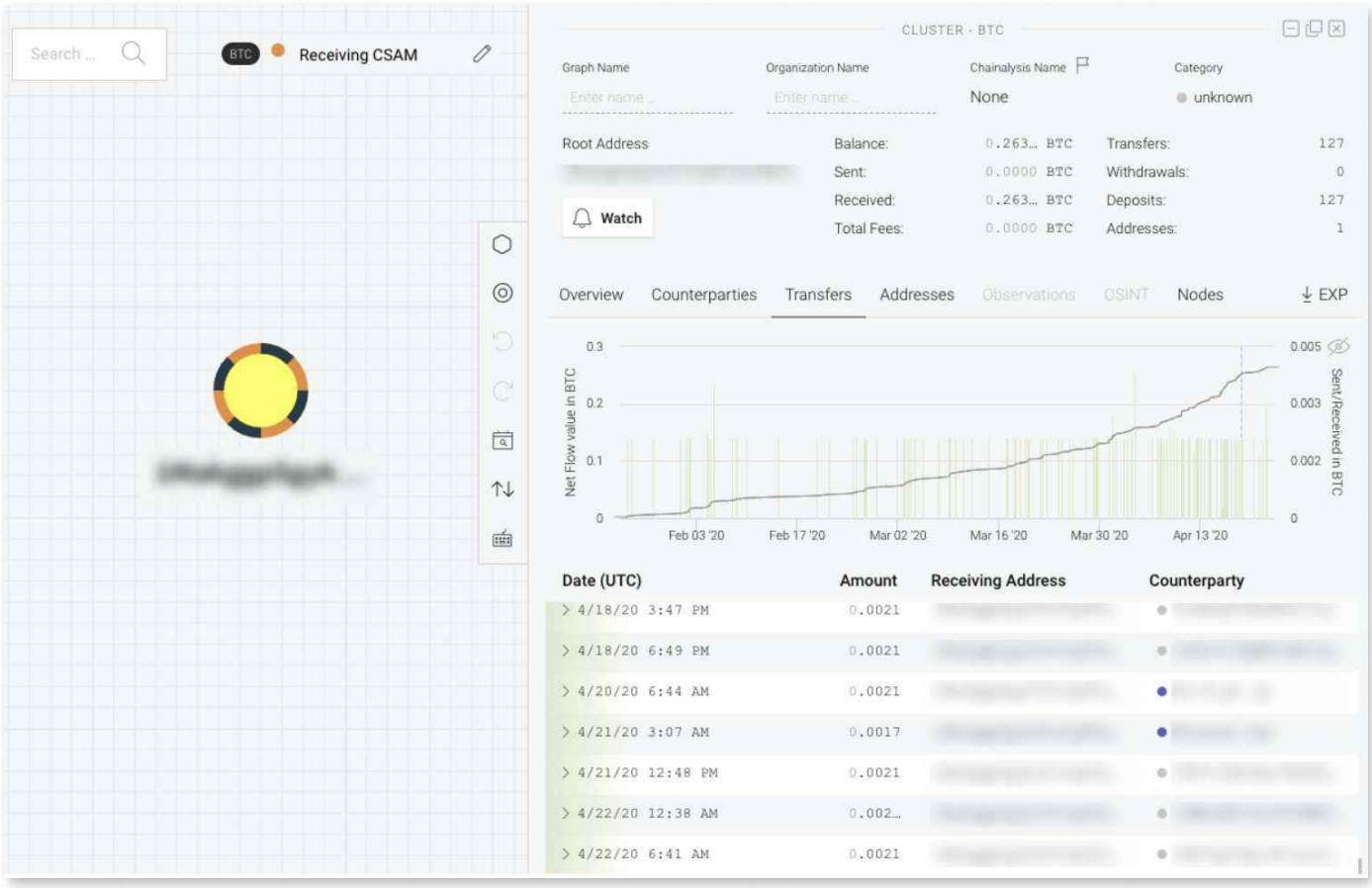
Currencies included: BCH, ETH

Dark Scandals received funds from a relatively small group of customers, who sent payments from a variety of different service types, with the majority coming from exchanges.



This Reactor graph aggregates the addresses that sent funds to Dark Scandals by service type

Law enforcement initially discovered Dark Scandals by analyzing the transaction history of an individual under investigation for purchasing CSAM from Welcome to Video and examining other addresses to which they had sent funds.



Note the uniformity of payments received by Dark Scandals. Nearly every one is equivalent to roughly $15 worth of Bitcoin

Law enforcement agents made undercover payments to Dark Scandals in order to obtain and verify its customer-facing cryptocurrency addresses. Many of those addresses were hosted at compliant exchanges, so agents were able to subpoena them for the account holders' identity. Similar tactics, paired with other cyber-investigative techniques, allowed them to identify Michael Rahim Mohammed, a Dutch national, as the platform's alleged operator.

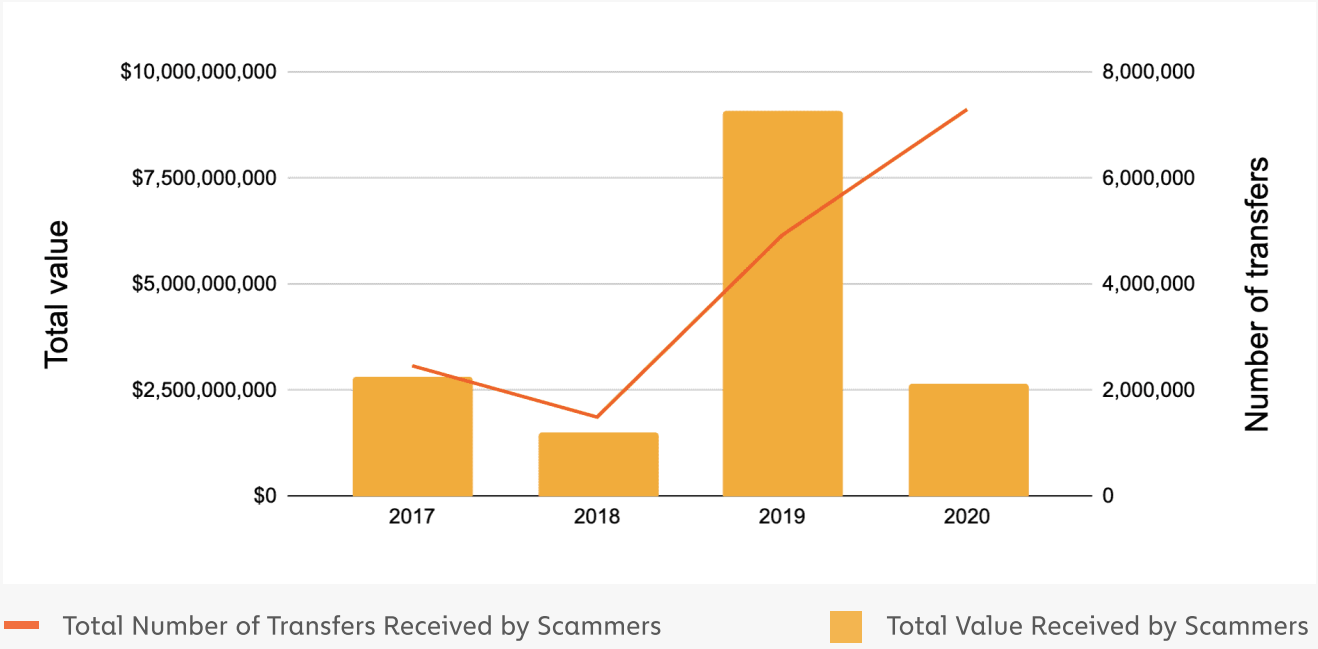
Since Mohammed's arrest though, Special Agent Janczewski notes that sites imitating Dark Scandals have popped up, at least some of which are scams. "There were no videos on the darknet version of Dark Scandals itself," Janczewski said. "The website advertised what addresses clients should make a payment to. Then the administrator replied to the client's email with a download link for a file hosting site so that the client could receive the content. It's been easier for scammers to spoof Dark Scandals versus Welcome to Video and trick people into paying." Chainalysis continues to track payments to Dark Scandals imitators and others alleged to monetize CSAM.

Overall, the takedown of Dark Scandals has Janczewski optimistic about law enforcement's ability to fight cryptocurrency-based CSAM markets. "Traditional CSAM investigators are working with cryptocurrency experts to get better at tracking transactions. Tools and educational efforts from blockchain analysis companies and government agencies have been invaluable," he said. "As the CSAM ecosystem adapts, so too does law enforcement."

Scams

Cryptocurrency Scam Revenue Fell 75% in 2020 Despite Increase In Victims

Total cryptocurrency value received by scammers vs. Total Number of transfers to scammers | 2017 - 2020

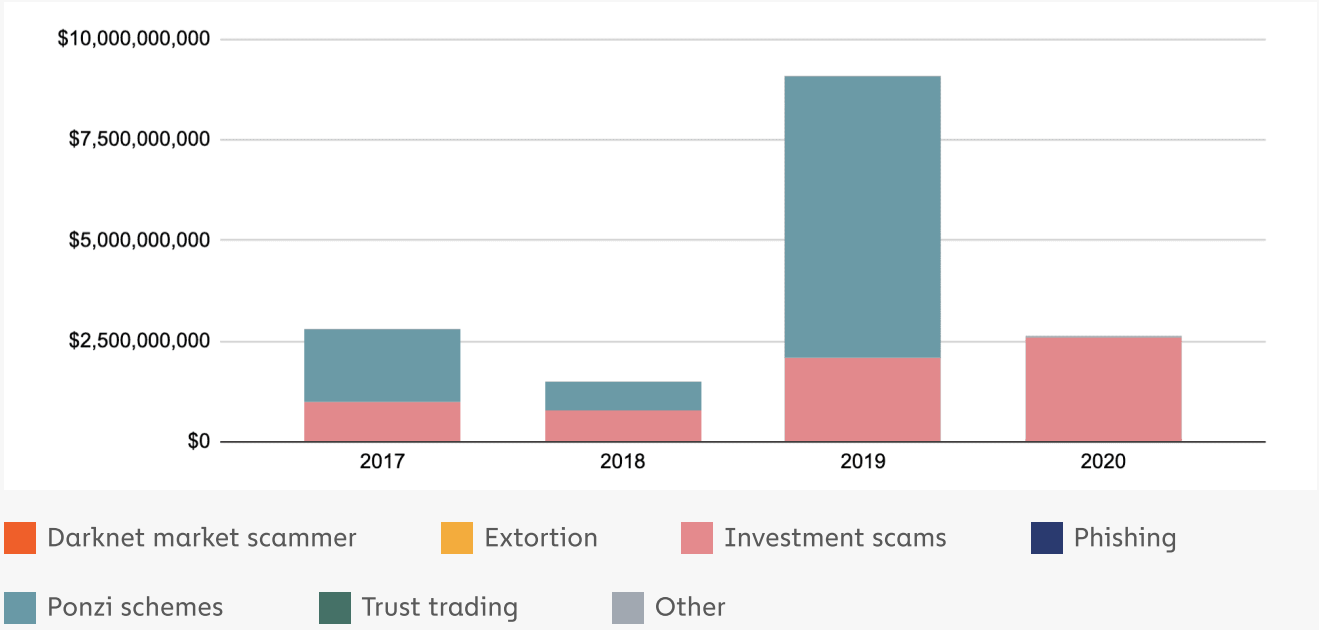


Currencies included: BCH, BNB, BTC, ETH, HT, LTC, MKR, OMG, PAX, TUSD, USDC, USDT

While scams remain the highest-grossing form of cryptocurrency-based crime, total scam revenue fell drastically in 2020, from roughly $9 billion to just under $2.7 billion. Interestingly though, the number of individual payments to scam addresses rose from just over 5 million to 7.3 million, suggesting that the number of individual scam victims rose by more than 48%.

Why did scam revenue decline even as the number of victims grew? The reason is that there were no large-scale Ponzi schemes like those we saw in 2019. Below, we break down yearly scam revenue by type of scam.

Total cryptocurrency value received by scam category | 2017 - 2020



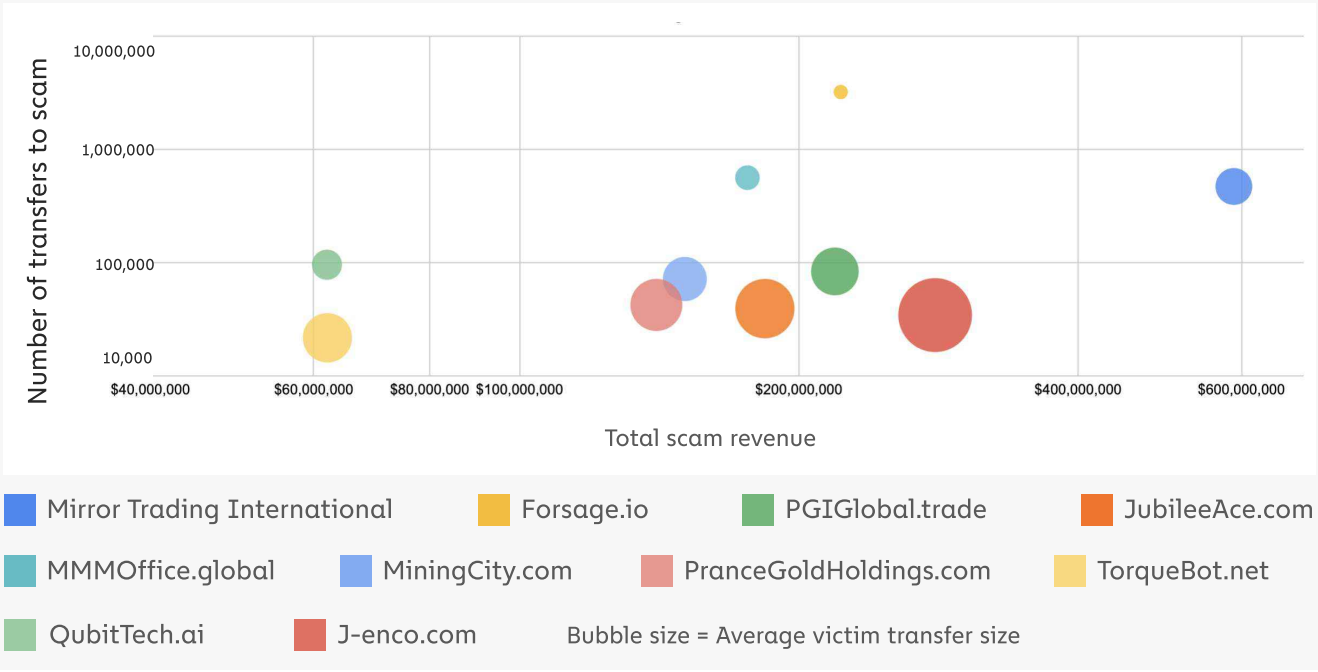
Currencies included: BCH, BNB, BTC, ETH, HT, LTC, MKR, OMG, PAX, TUSD, USDC, USDT

Ponzi schemes took in nearly $7 billion worth of cryptocurrency in 2019, which is more than double what all scam categories made in 2020. Even more shocking is the fact that just six individual Ponzi schemes accounted for that $7 billion. Most notable of the six was the infamous PlusToken scam, a Ponzi scheme that reaped at least $3 billion worth of cryptocurrency from millions of victims, mostly in Asia. Since we covered PlusToken in last year's Crypto Crime Report, Chinese authorities have arrested 109 individuals associated with the scam and prosecuted six of the most prominent.

Luckily, we're not aware of any other Ponzi schemes comparable to PlusToken that took place in 2020. This suggests that cryptocurrency users and the general public have grown more suspicious of such scams, or that potential Ponzi scheme operators have been scared off by the punishments doled out to the PlusToken operators.

Instead, nearly all scam revenue in 2020 went to smaller-scale investment scams. Investment scams have been a more consistent mainstay of cryptocurrency-based crime, as there are many more happening at any given time compared to Ponzi schemes. Unlike Ponzi schemes, these more generic investment scams don't tend to pay out fake proceeds to early investors and take in less cryptocurrency from each individual victim. We see this reflected in the graph below, which shows 2020's biggest scams — all of which are generic investment scams — broken down by total revenue, total victims (approximated by the number of individual payments), and average amount received per victim.

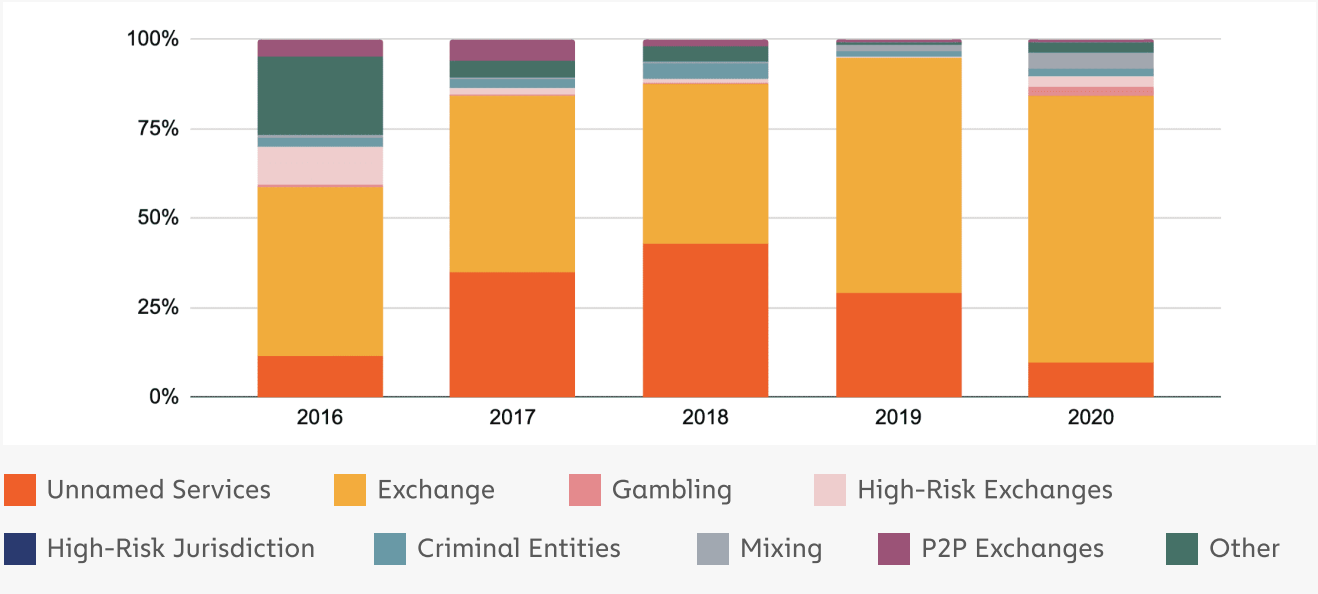
2020 Top 10 cryptocurrency investment scams



Currencies included: BTC, ETH, OMG, PAX, USDC, USDT

Mirror Trading International was by far the year's biggest scam, taking in $589 million worth of cryptocurrency across more than 471,000 deposits, suggesting a number of victims in the hundreds of thousands. We'll dive more into Mirror's business model and operations later in the section. Other notable scams included J-enco and Forsage.

Destination of funds sent from scam addresses | 2016 - 2020



Currency included: BCH, BTC, ETH, LTC, OMG, PAX, TUSD, USDC, USDT

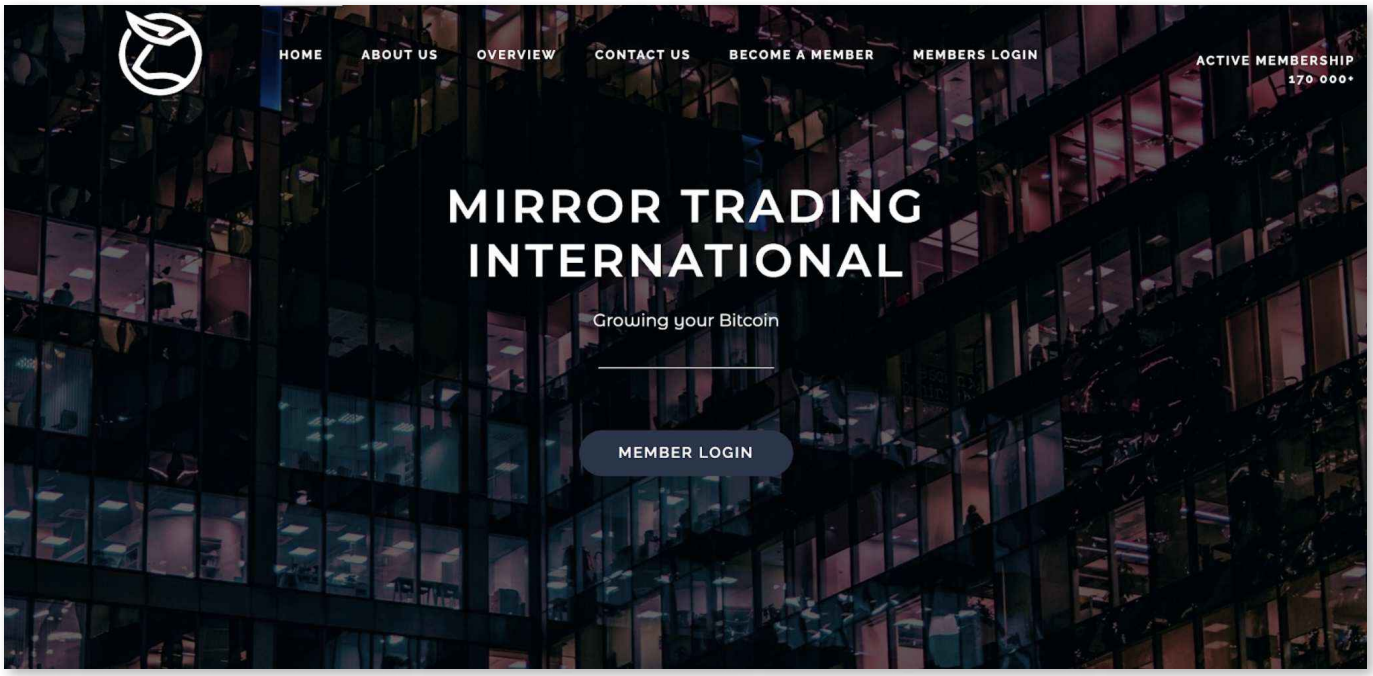
As was the case in previous years, scammers moved cryptocurrency received from victims primarily to exchanges in order to convert it into cash.

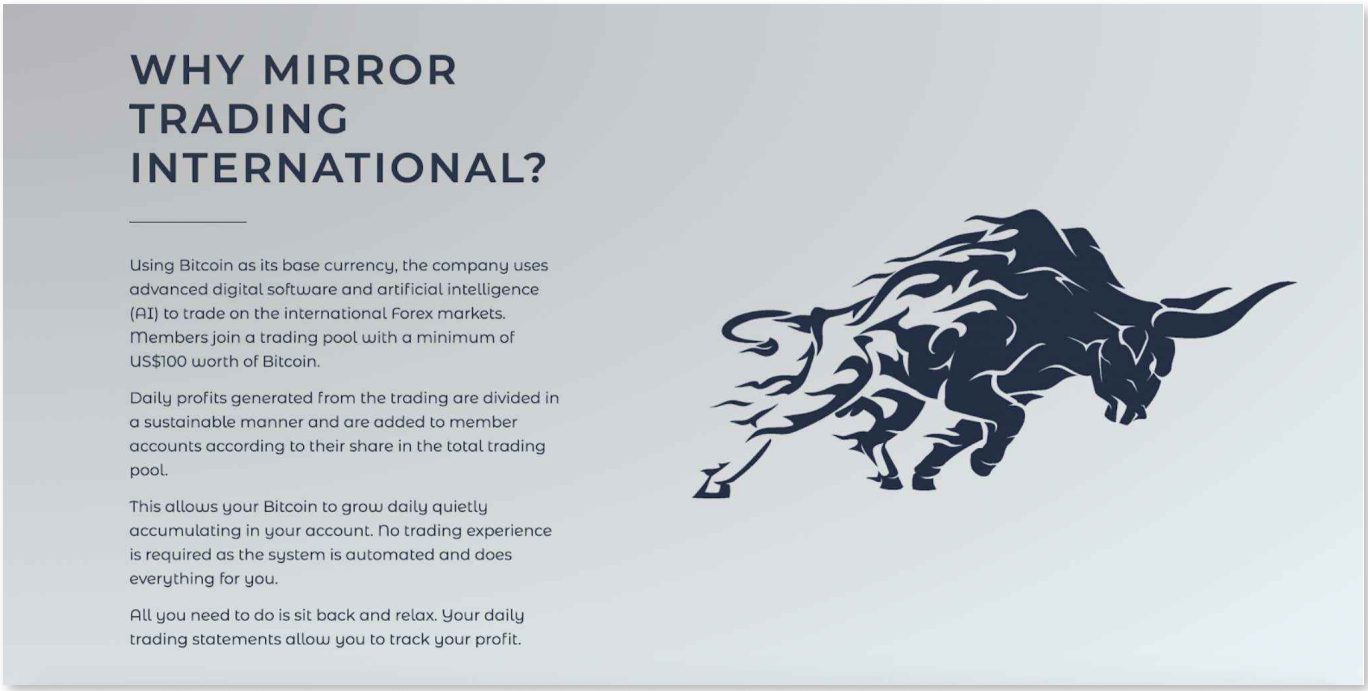
However, we also saw an increase in the share of scam proceeds sent to mixers and high-risk exchanges, meaning those with weak or non-existent compliance programs. This may be a sign that some scammers are becoming warier of compliant exchanges, which are more likely to flag illicit activity using a transaction monitoring solution and cooperate with law enforcement investigations.

Below, we'll analyze two prominent 2020 scams.

Investigating 2020's biggest investment scam: Mirror Trading International

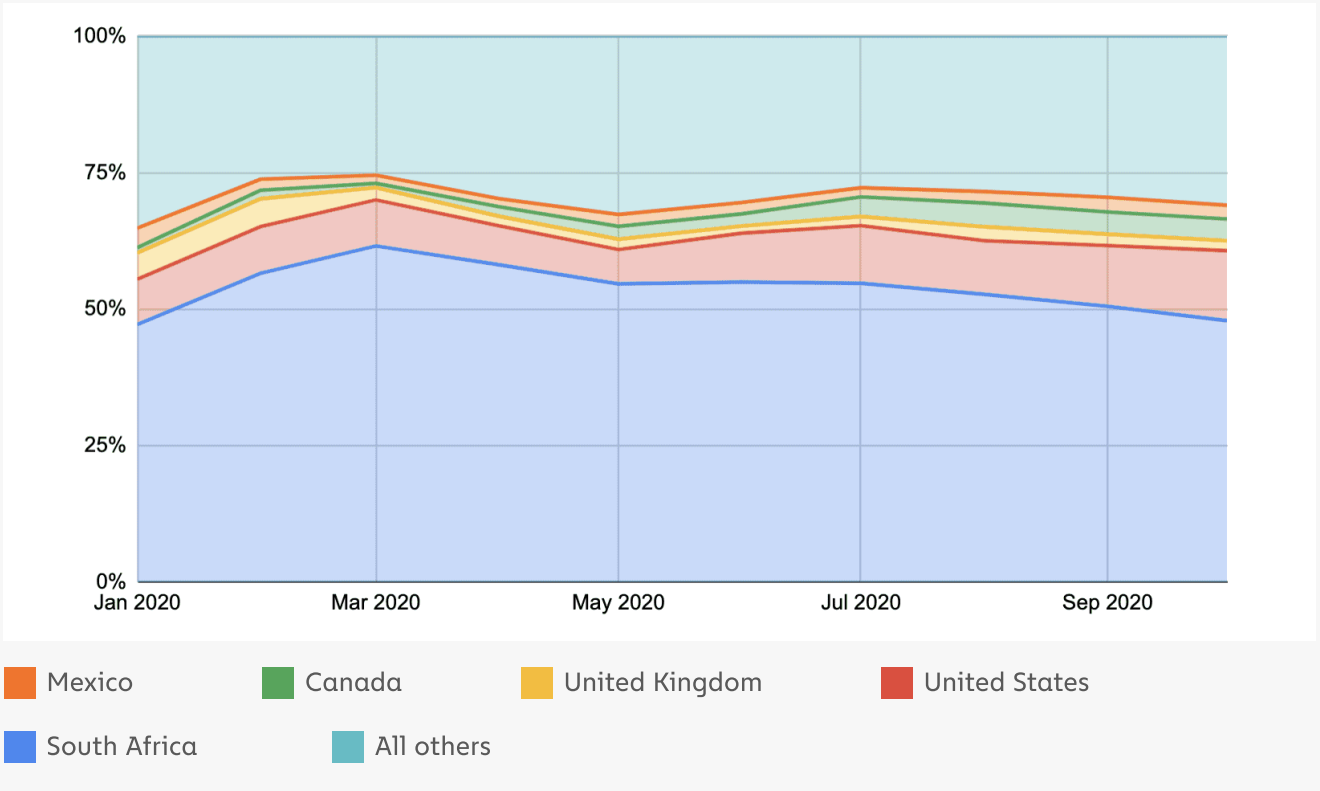
Mirror Trading International (MTI) presents itself as a passive income source. According to its website, users simply deposit a minimum of $100 worth of Bitcoin, and MTI promises to grow it using an AI-powered foreign exchange trading software. The site indicates that customers can achieve consistent daily returns of 0.5%, which would translate to yearly gains of 500%. Algorithmic trading is a common premise for many cryptocurrency investment scams.





MTI is based in South Africa, and claims to have offices in Stellenbosch and Johannesburg. Its web traffic falls in line with that, as more than half comes from South Africa.

Mirror Trading International Web Traffic Data

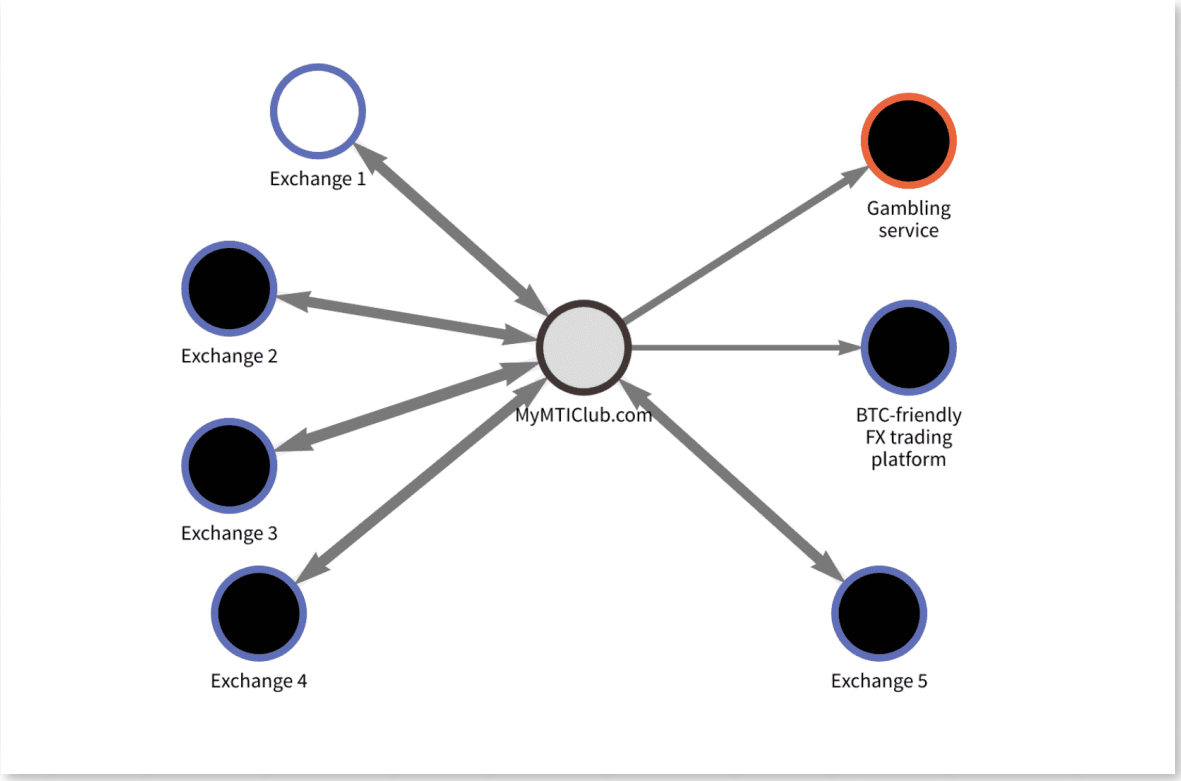


Currency included: BCH, BTC, ETH, LTC, OMG, PAX, TUSD, USDC, USDT

The U.S., U.K., Canada, and Mexico also make up significant portions of MTI's web traffic. We assume from this that most MTI victims hail from these countries in similar proportions as well. MTI has been actively receiving Bitcoin from "customers" since June 2018 and even has 150 employees listed on its LinkedIn company page.

However, despite these airs of legitimacy, Google searches reveal that people have been rightly speculating that the company is a scam for most of its existence. In August 2020, CoinDesk published an article encouraging all MTI users to withdraw their funds as soon as possible, citing the decision of Texas state regulators to formally label the company a scam, as well as a pending investigation by South Africa's Financial Services Conduct Authority (FSCA). On December 18, 2020, the FSCA filed charges against MTI after its investigation found that the company falsified trade statements, didn't declare losses and committed other acts of fraud to deceive the market. The investigation also found that MTI had over 16,000 Bitcoin of claimed customer investment funds unaccounted for. MTI claimed to have transferred those funds to a new FX trading platform after its old platform banned MTI due to its scamming reputation, but the new platform says these funds were never deposited. Since those charges were filed, MTI customers have complained that they can no longer access or withdraw funds they've deposited to the platform, and MTI CEO Johan Steynberg has fled South Africa.

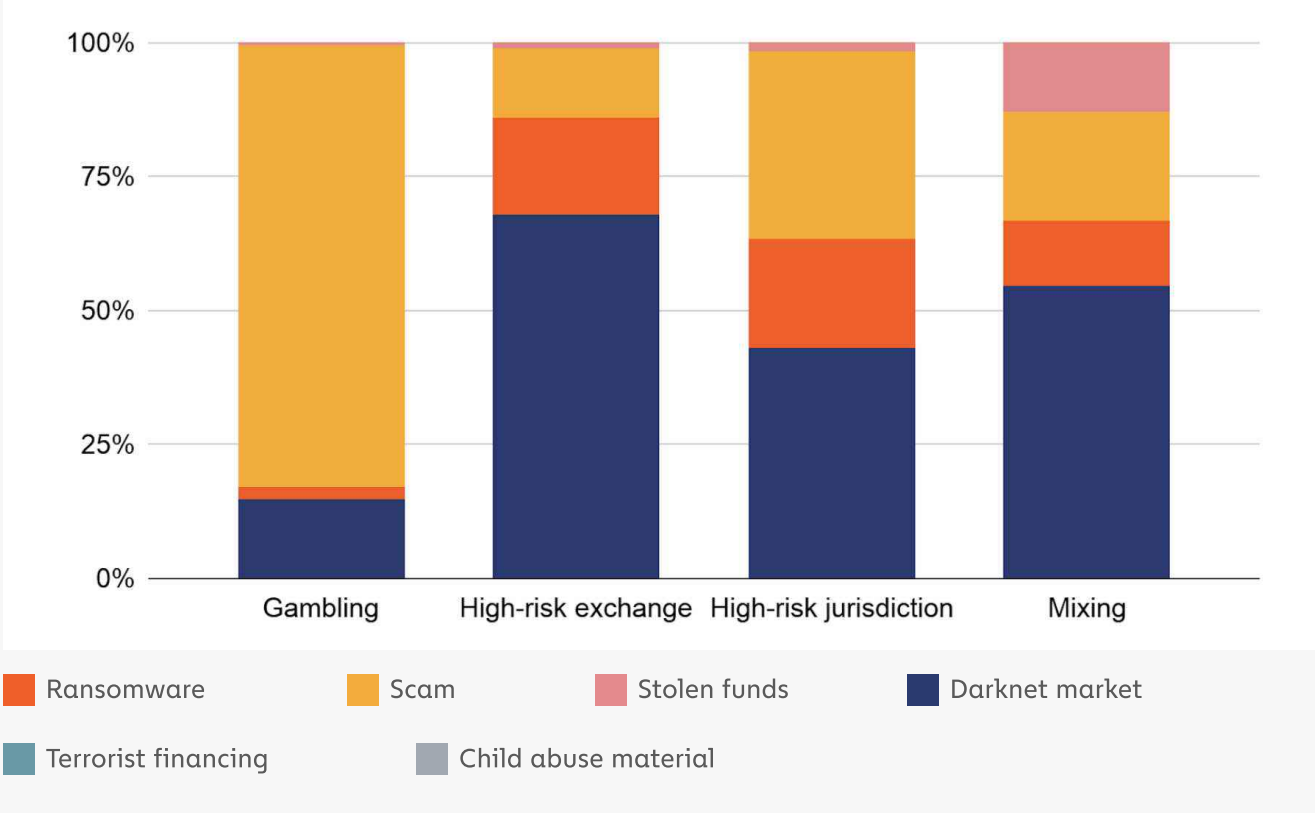
Using Chainalysis Reactor, we can analyze MTI's cryptocurrency transaction history to learn more about the scam.



MTI Club has received $588 million worth of Bitcoin across more than 470,000 transactions, primarily from exchanges, but also from self-hosted wallets. MTI has also sent and received significant funds to and from a popular, Bitcoin-friendly FX trading platform, as we show in the Reactor graph above.

Perhaps most interesting is MTI Club's apparent usage of a popular cryptocurrency gambling service as a money laundering and cash out mechanism. The platform is the biggest risky destination of MTI funds by volume, having received $39 million worth of cryptocurrency from the scam in 2020. Cryptocurrency observer and venture capitalist Dovey Wan has remarked that this is becoming a common money laundering technique for many cybercriminals who use cryptocurrency, as gambling platforms can be used similarly to mixers to obscure the origins and flows of illicitly-obtained funds. Our data suggests that this is especially true for scammers.

Risky services receiving illicit funds by crime type | 2020



Currencies included: BCH, BTC, ETH, LTC, OMG, PAX, USDC, USDT

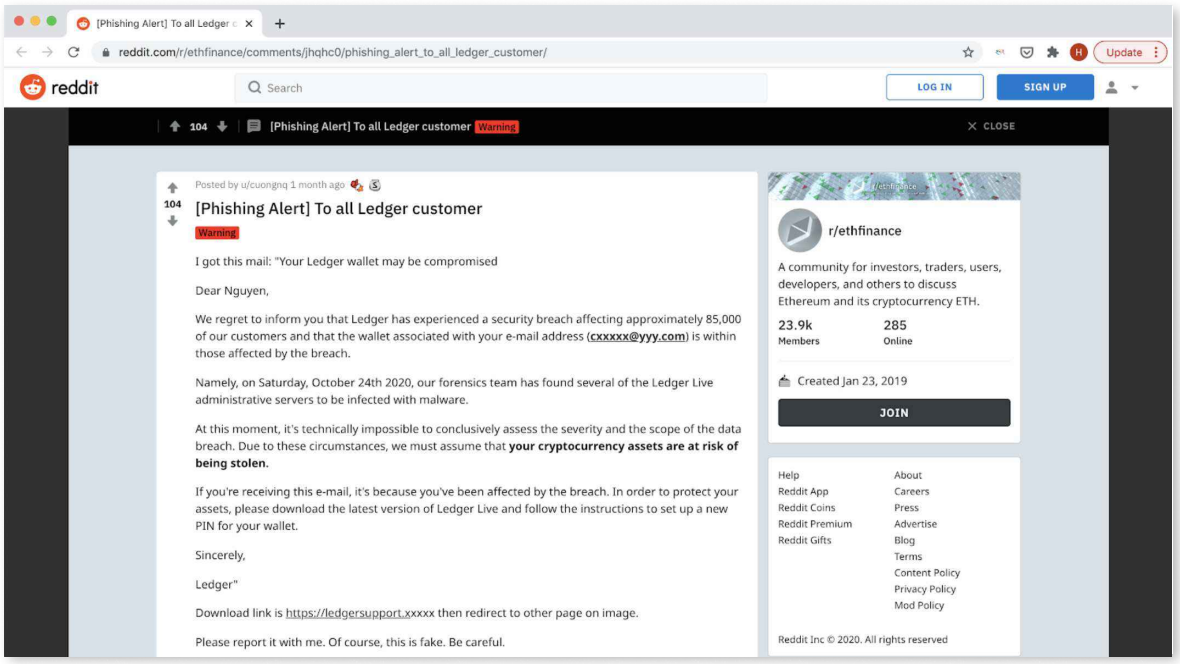
As the above chart shows, scammers are disproportionately likely to send funds to gambling platforms rather than other services frequently used for money laundering.

Mirror Trading International is another example of why the industry must spread the word that algorithmic trading platforms promising unrealistically high returns are nearly always scams. When cryptocurrency exchanges and other services learn of these scams and receive their cryptocurrency addresses, they should discourage users from sending funds to those addresses or at least warn them that financial losses are highly likely. In addition, exchanges, gambling platforms, and other services that these scams use to launder funds should consider blocking incoming transactions from businesses that relevant government bodies label as scams or potential scams, as removing the ability to convert funds to cash makes it more difficult for scams to operate.

The Ledger phishing scam is a wake up call for exchanges

While phishing scams made up a very small share of overall scam revenue in 2020, one phishing scam in particular has received a great deal of attention due to its high visibility and the number of potential victims: The Ledger phishing scam.

Ledger is a popular provider of hardware cryptocurrency wallets, which are physical devices on which cryptocurrency can be stored, similar to a conventional cryptocurrency wallet. In July 2020, the company published a blog post revealing that many users' email addresses had been compromised in a data breach. A few months later in October, Ledger customers reported receiving emails from closely spoofed versions of the Ledger website domain. The email claimed that Ledger's servers had been hacked with malware and that customers' funds were in danger of being stolen unless they clicked a link in the email to download the latest version of Ledger's software. Clicking the link leads users to a web page that mimics the Ledger website.



A reddit post describing the phishing emails.

The email and website however, are part of a sophisticated phishing scam. Instead of a software update, Ledger users who click the download link on the fake web page actually download malware that drains their Ledger wallet. Overall, CoinTelegraph reported that Ledger users lost 1.1 million XRP (roughly $645,000) within the first week of the phishing campaign. We should also note that since the leaked Ledger database has been sold on the dark web, it's possible that more than one criminal group has launched phishing attacks against Ledger users. This is also backed up by the fact that since October, Ledger users have received multiple waves of phishing messages, including some delivered by SMS and using different social engineering techniques.

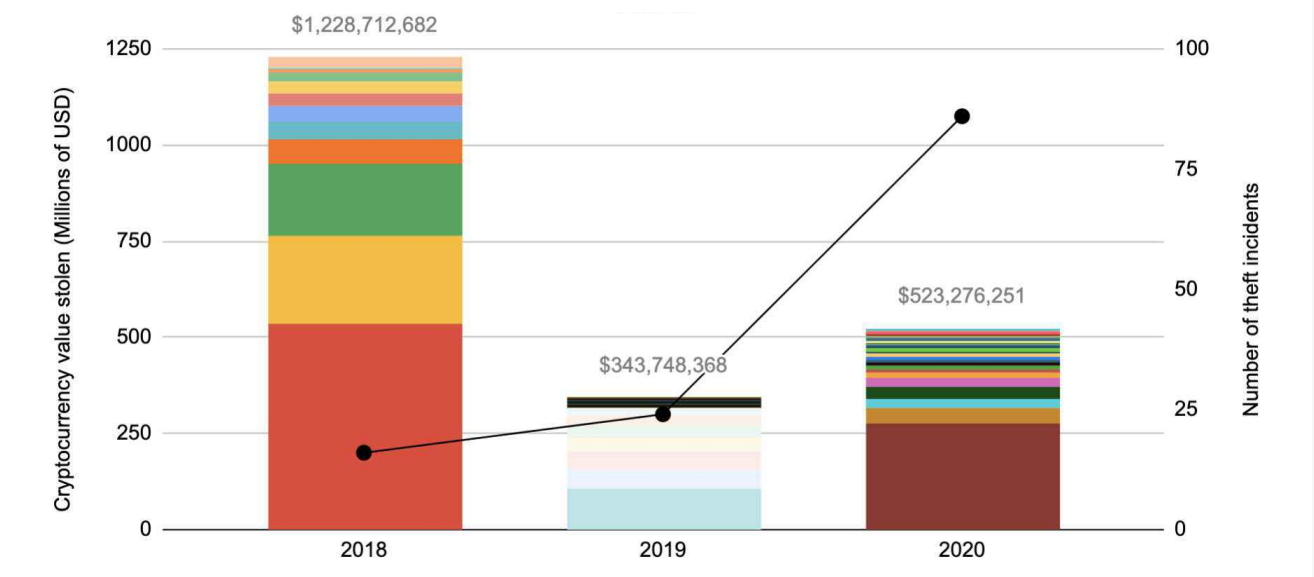
Our analysis of a selection of the suspected scammers' addresses reveals that their wallets have been active since 2018, suggesting that the cybercriminals may have been conducting phishing scams for at least two years preceding the publication of the Ledger scam in 2020. In addition, we found that the assets stolen from Ledger customers span many cryptocurrencies, a large share of which have been moved to exchanges and other services. The stolen assets we've identified amount to upwards of €3 million.

The Ledger phishing scam shows how important it is for exchanges and other cryptocurrency services to educate customers on phishing techniques, especially if they know customers' emails or other personal information has been compromised, thereby making customers more vulnerable to phishing attacks.

Stolen Funds

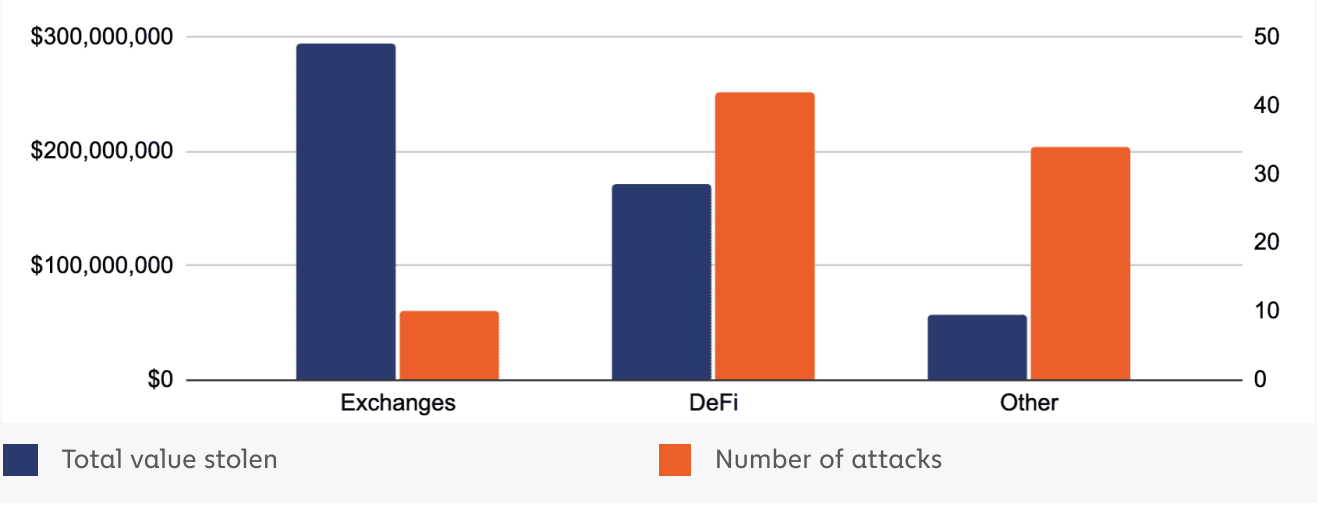
More Cryptocurrency Stolen in 2020 As DeFi Platforms Appear Uniquely Vulnerable to Attack

Number of cryptocurrency theft incidents vs. Total value stolen by year | 2018 - 2020



Different colors denote different instances of cryptocurrency theft. Please note that this graph relies in part on public reporting, so we cannot list all currencies included.

Total value stolen and number of attacks by victim type | 2020



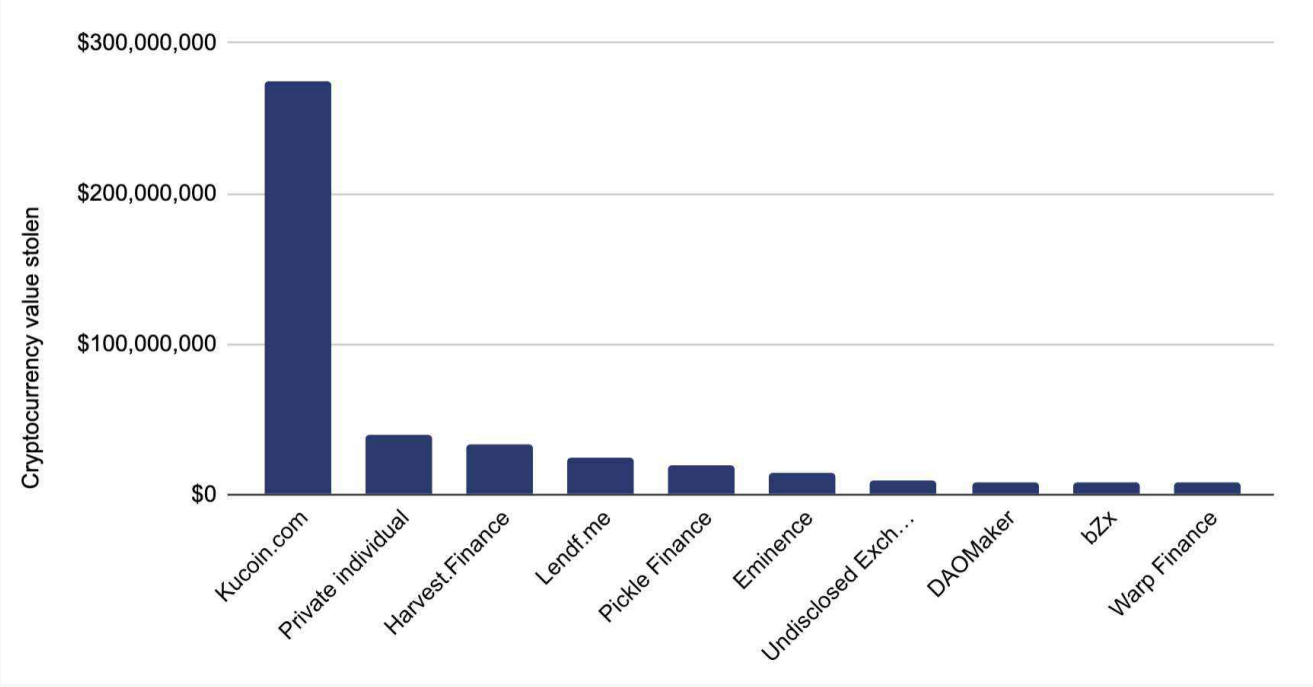
Note: The "other" category here refers to cryptocurrency thefts from individuals or from cryptocurrency businesses other than exchanges.

Year	Number of attacks	Received USD
2018	16	$1.23B
2019	24	$343.7M
2020	86	$523.3M

In 2020, over $520 million worth of cryptocurrency was stolen from services and individuals through hacks and non-technical attacks like social engineering or phishing efforts. That represents an uptick from 2019 following a huge decline from the amount stolen in 2018, most of which could be attributed to the $534 million Coincheck hack. **More than half of the amount stolen in 2020 was from the hack of the exchange KuCoin, which we can now publicly attribute to Lazarus Group, a notorious North Korea-aligned cybercriminal syndicate responsible for hacking numerous cryptocurrency exchanges over the last few years.** The hackers managed to take $275 million worth of cryptocurrency from KuCoin, making it the biggest cryptocurrency theft of the year and third-largest of all time, though KuCoin claims to have recovered most of the funds. Later in this section, we'll look more at this hack and share details on how Lazarus Group's money laundering strategy changed in 2020.

The chart and table below provide details on the ten largest cryptocurrency thefts of 2020.

Top 10 cryptocurrency theft attacks | 2020



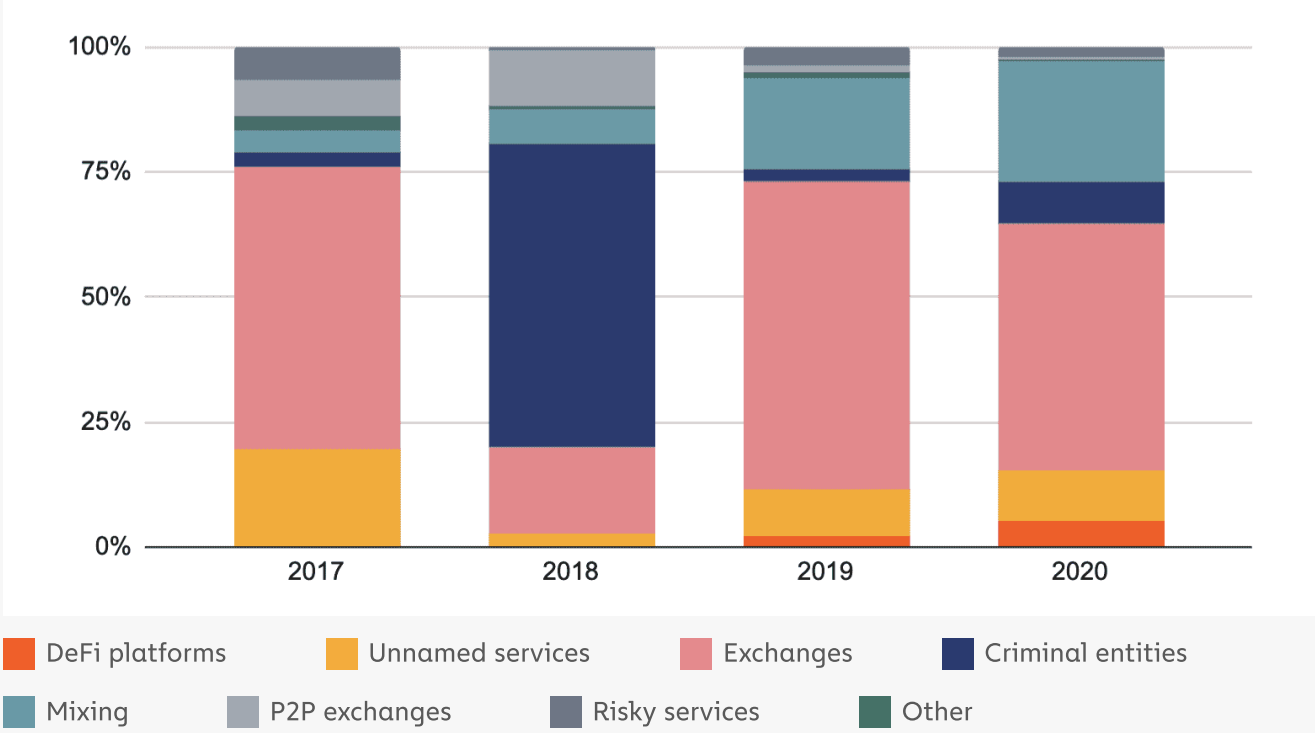
The Top 10 Cryptocurrency Thefts of 2020

Victim	Victim type	Amount stolen (USD)	Description
KuCoin	Exchange	$275 million	Third-largest cryptocurrency theft ever. Lazarus Group hackers accessed private keys of KuCoin hot wallets and stole numerous types of cryptocurrency. Hackers then used DeFi platforms like Uniswap and Kyber to swap stolen funds for different types of cryptocurrency.
Josh Jones	Personal Attack	$40 million	Funds stolen from the private wallets of Josh Jones, CEO of Bitcoin Builder.
Harvest Finance	DeFi platform	$34 million	Cybercriminals launched a flash loan attack, using borrowed funds to manipulate cryptocurrency prices and artificially increase their share of Harvest's yields.
Lendf.me	DeFi platform	$25 million	Cybercriminals exploited a code vulnerability in Lendf.me, a DeFi lending platform, to pull off a reentrancy attack.
Pickle Finance	DeFi platform	$20 million	Cybercriminals launched a flash loan attack.
Eminence	DeFi platform	$15 million	Cybercriminals launched a flash loan attack.
Undisclosed exchange	Exchange	$9 million	Due to ongoing investigations, we can't reveal the victim or nature of this exchange hack.
MakerDAO	DeFi platform	$8.3 million	Cybercriminals exploited vulnerability in MakerDAO's price oracle during flash crash.
bZx	DeFi platform	$8 million	Cybercriminals exploited code error to manipulate their balances and create new tokens at will.
Warp Finance	DeFi platform	$8 million	Cybercriminals launched a flash loan attack.

One trend that jumps out is the amount that's been stolen from DeFi platforms. DeFi platforms' usage has skyrocketed in 2020 but has also given cybercriminals a new, uniquely vulnerable service to attack. Despite representing just 6% of all cryptocurrency activity, DeFi platforms lost roughly 33% of all cryptocurrency stolen in 2020 and were victims in nearly half of all individual attacks. Later in the section, we'll examine what makes DeFi platforms so susceptible to attacks.

DeFi platforms also figure prominently when we look at the services cybercriminals have used to launder stolen cryptocurrency and convert it into cash.

Destination of stolen cryptocurrency by year | 2017 - 2020



Currencies included: BAT, BCH, BTC, ETH, LTC, MKR, OMG, PAX, TUSD, USDC, USDT

Stolen funds primarily move to exchanges, as is the case with proceeds from other forms of cryptocurrency-related crime. But DeFi platforms' share of all stolen funds received more than doubled in 2020. Their decentralized nature is likely what makes DeFi platforms attractive as a money laundering mechanism — since these platforms never directly take custody of funds deposited to them, many don't collect know your customer (KYC) information or report on transaction activity as demanded by the Bank Secrecy Act (BSA) and other financial regulations.

What makes DeFi platforms vulnerable to attack?

DeFi's extraordinary growth has been one of cryptocurrency's biggest stories of 2020. DeFi stands for decentralized finance, the decentralization arising from the fact that DeFi platforms can, at least in theory, run autonomously without the support of a central company, group, or person. DeFi platforms are built on top of smart contract-enriched blockchains — primarily the Ethereum network — and can fulfill specific financial functions determined by the underlying code, executing specific transactions like trades and loans automatically when certain conditions are met. Without the need for centralized infrastructure or human governance, DeFi platforms can enable users to execute financial transactions at lower fees than other fintech applications or financial institutions. Overall, DeFi platforms received $86.5 billion worth of cryptocurrency in 2020, which represents a 67x increase over the 2019 total.

However, cybercriminals stole more than $170 million from DeFi platforms in 2020, which is disproportionately high in comparison to the share of total cryptocurrency activity DeFi accounts for. The primary reason for this is that DeFi platforms are uniquely vulnerable to **price manipulation attacks**. Price manipulation was the key to nearly every notable attack on DeFi platforms in 2020. Transactions happen almost instantly in DeFi with very few mechanisms in place to prevent shady transactions, so bad actors can reap huge gains by manipulating a cryptocurrency's price on one or more DeFi platforms. DeFi platforms rely on tools called price oracles to get asset pricing data from an external source — usually from another exchange, other service, or data provider like CoinMarketCap — to ensure its assets are priced in accordance with the rest of the market. However, most DeFi platforms use centralized price oracles, which rely on just one node to feed data to the rest of the platform and often draw on a single source of pricing data, leaving them vulnerable to attack.

Price manipulation might seem like an unlikely attack method for cybercriminals, as upping the price of any one crypto asset requires upfront capital to pump up its value, right? Not so in DeFi, thanks to **flash loans**.

Flash loans allow DeFi users to instantly receive loans without putting up collateral, use the loaned funds to make trades elsewhere, and repay the loan in one instant transaction. If they don't pay back the loan, the entire transaction is instantly rolled back, meaning the lender receives the original capital back as if the loan never happened, something only possible with smart contracts. In effect, this means little to no risk for either side: If the trade the borrower wants to make with the loaned funds doesn't work out and they can't pay back the loan, neither they nor the lender loses anything. This also means lenders can charge very low interest on flash loans. Traders often use flash loans to get the funds necessary to exploit arbitrage opportunities, using borrowed funds to take advantage of pricing disparities across platforms and come away with a small profit after paying back the loan.

However, in 2020, cybercriminals weaponized flash loans by using the borrowed funds to purchase a crypto asset, pump up its price, and sell it for a large profit, thereby enabling them to easily pay off the original loan and pocket the remaining funds. We saw an example of this in February's two hacks of bZx, a DeFi protocol that allows users to build apps for decentralized lending, margin trading, and other financial activities. In the first hack, the cybercriminals borrowed a large amount of Ether from bZx in a flash loan, used it to buy and pump up the price of wrapped Bitcoin on Uniswap — at one point, the wrapped Bitcoin price on Uniswap reached 109.8 ETH, compared to 38 for the market in general. The attacker then exchanged their wrapped Bitcoin for a healthy profit of Ether, some of which was used to pay off the original flash loan. All in all, the attacker netted $350,000 worth of Ether. The second attack, a copycat of the first, netted $633,000. The identity of the hackers is unknown, and it's unclear whether or not the same individual or group is responsible for both hacks.

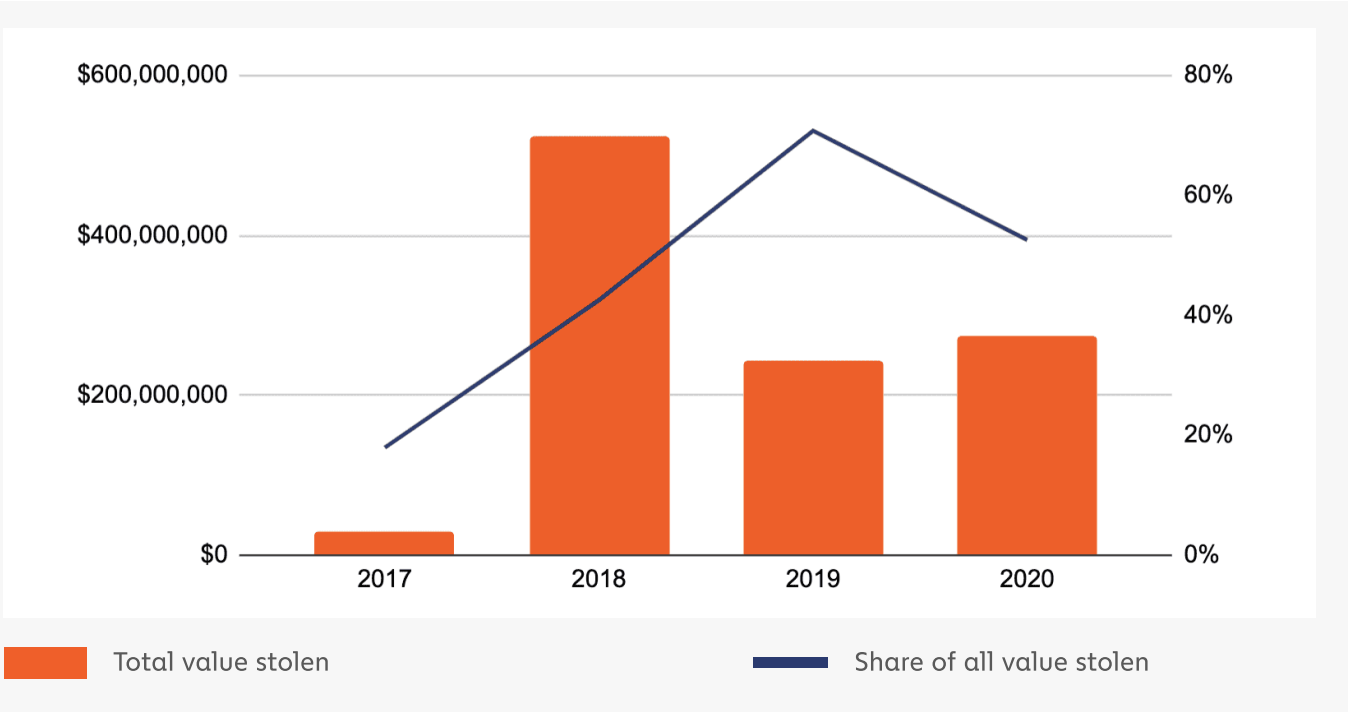
These attacks on bZx worked because the platform's code contained no failsafes to account for large price jumps on other DeFi platforms, which may have caught the cybercriminals pumping wrapped Bitcoin's price on Uniswap. bZx's GitHub repository shows the issue has now been fixed. But this underlines another reason DeFi platforms are vulnerable to attack: their use of open-source code. DeFi platforms move users' funds based solely on their underlying code without human intervention, so users need to be able to audit that code in order to trust the platform, making open source a necessity. However, that means cybercriminals can also analyze the code for vulnerabilities and plot the perfect attack, as it appears they did in the case of the bZx flash loan attacks. In fact, bZx was hacked again later in the year to the tune of $8.1 million, all because a single misplaced line of code allowed users to manipulate their own balances under certain circumstances, creating new tokens for themselves at will.

These attacks go to show how important it is for DeFi platforms to implement the latest and greatest security measures. One provider to watch here is Chainlink, a company that helps DeFi platforms protect against price manipulation attacks with **decentralized price oracles**. Decentralized price oracles aggregate pricing data from more sources and deliver it to the DeFi platform on-chain through a network of independent nodes, thereby making it harder for price manipulators to target a single weak spot. However, even with such advancements, regulators and law enforcement should look for ways to ensure the extremely promising DeFi space remains safe for investors.

Lazarus Group pulled off 2020's biggest exchange hack and appears to be exploring new money laundering options

Lazarus Group is a cybercriminal syndicate working on behalf of the North Korean government. Lazarus has been responsible for numerous cryptocurrency exchange attacks, such as the 2019 UpBit hack, which netted them more than $49 million worth of cryptocurrency. Overall, the group is believed to have stolen more than $1.75 billion worth of cryptocurrency in the time it's been active. Experts believe proceeds from Lazarus Group hacks go toward North Korea's nuclear weapons program, so combatting their activity is of utmost importance for international safety and stability. That's why in 2020, the U.S. government took actions such as sanctioning two Chinese nationals who helped Lazarus Group launder funds stolen in multiple cryptocurrency hacks, and filing forfeiture complaints against 280 cryptocurrency addresses associated with Lazarus Group hacks.

Total cryptocurrency value stolen by Lazarus Group vs. Lazarus Group's share of all stolen cryptocurrency | 2017 - 2020

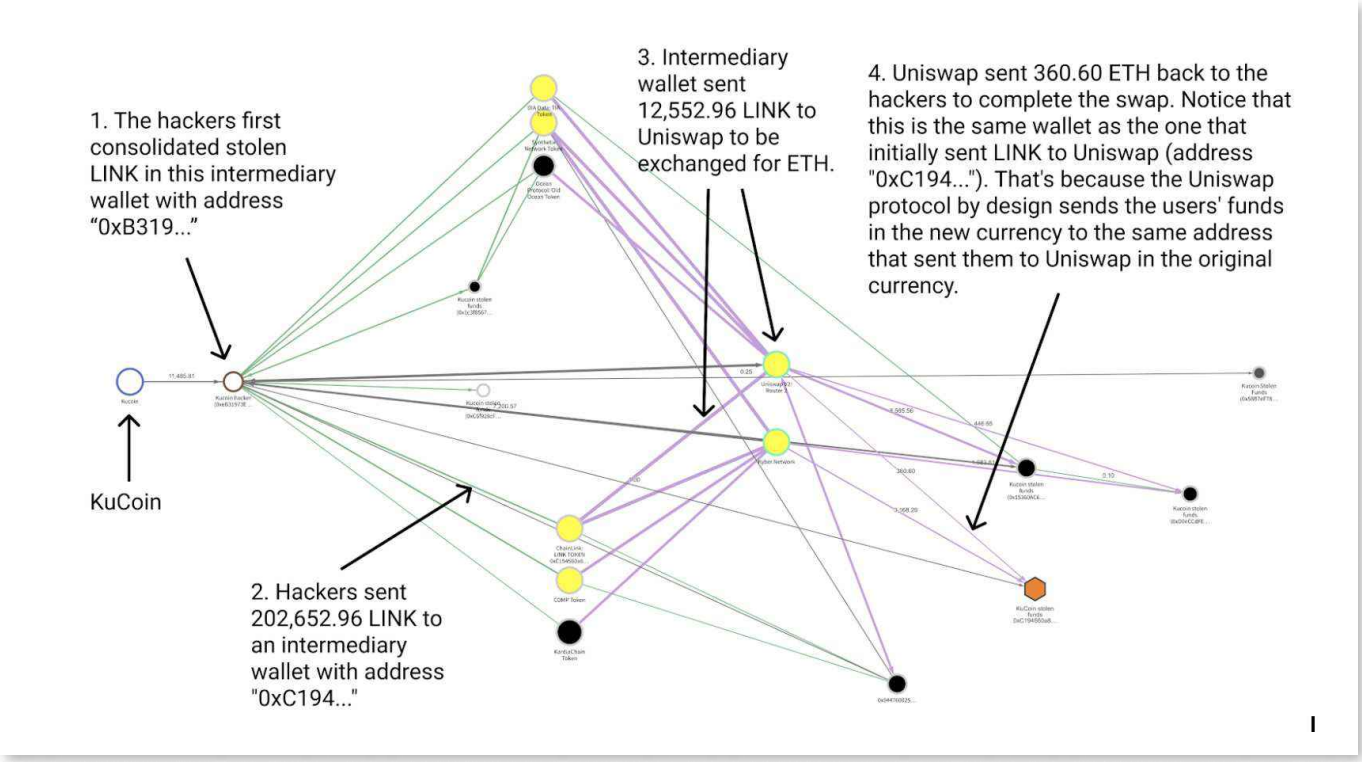


Currencies included: BAT, BCH, BNB, BTC, ETH, LTC, MKR, OMG, PAX, TUSD, USDC, USDT

However, Lazarus Group still managed to pull off the biggest cryptocurrency theft of the year, stealing roughly $275 million worth of cryptocurrency from the cryptocurrency exchange KuCoin. The $275 million represents over half of all cryptocurrency stolen in 2020. According to KuCoin's CEO, the hack occurred after cybercriminals gained access to the private keys to the exchange's hot wallets. Soon after, he claimed that the exchange had recovered $204 million worth of the stolen funds.

We were able to attribute this hack to Lazarus Group due in part to the KuCoin hackers' use of a specific money laundering strategy Lazarus has frequently used in the past. The strategy involves sending stolen funds to mixers in structured payments of the same size — usually an amount just below a round number in Bitcoin — that can be higher or lower depending on the size of the total amount to be laundered. Lazarus typically waits for each payment's output to be confirmed by the mixer before sending a new one, allowing them to minimize losses in the event the mixer fails. Once the funds are mixed, Lazarus Group then typically sends funds to OTC brokers on one of a few exchanges. The KuCoin hackers utilized this strategy for portions of the funds stolen. This, along with other pieces of evidence we're unable to share at this time, helped us identify Lazarus Group as the culprits. Additionally, two deposit addresses to which Lazarus Group sent stolen cryptocurrency this year also received funds stolen in the Harvest Finance hack, leading to speculation that Lazarus Group may have carried out that attack as well. However, this is still unconfirmed.

One new aspect of the KuCoin hack was how Lazarus Group used DeFi platforms to launder a portion of the stolen funds. DeFi platforms allow users to swap one type of cryptocurrency for another without a centralized platform ever taking custody of the users' funds. The lack of custody means that many DeFi platforms believe they don't have to take KYC information from customers, making it easier for cybercriminals to move funds with greater anonymity. The Reactor graph below gives an example of how exactly Lazarus Group used DeFi platforms to launder a portion of the funds stolen from KuCoin.

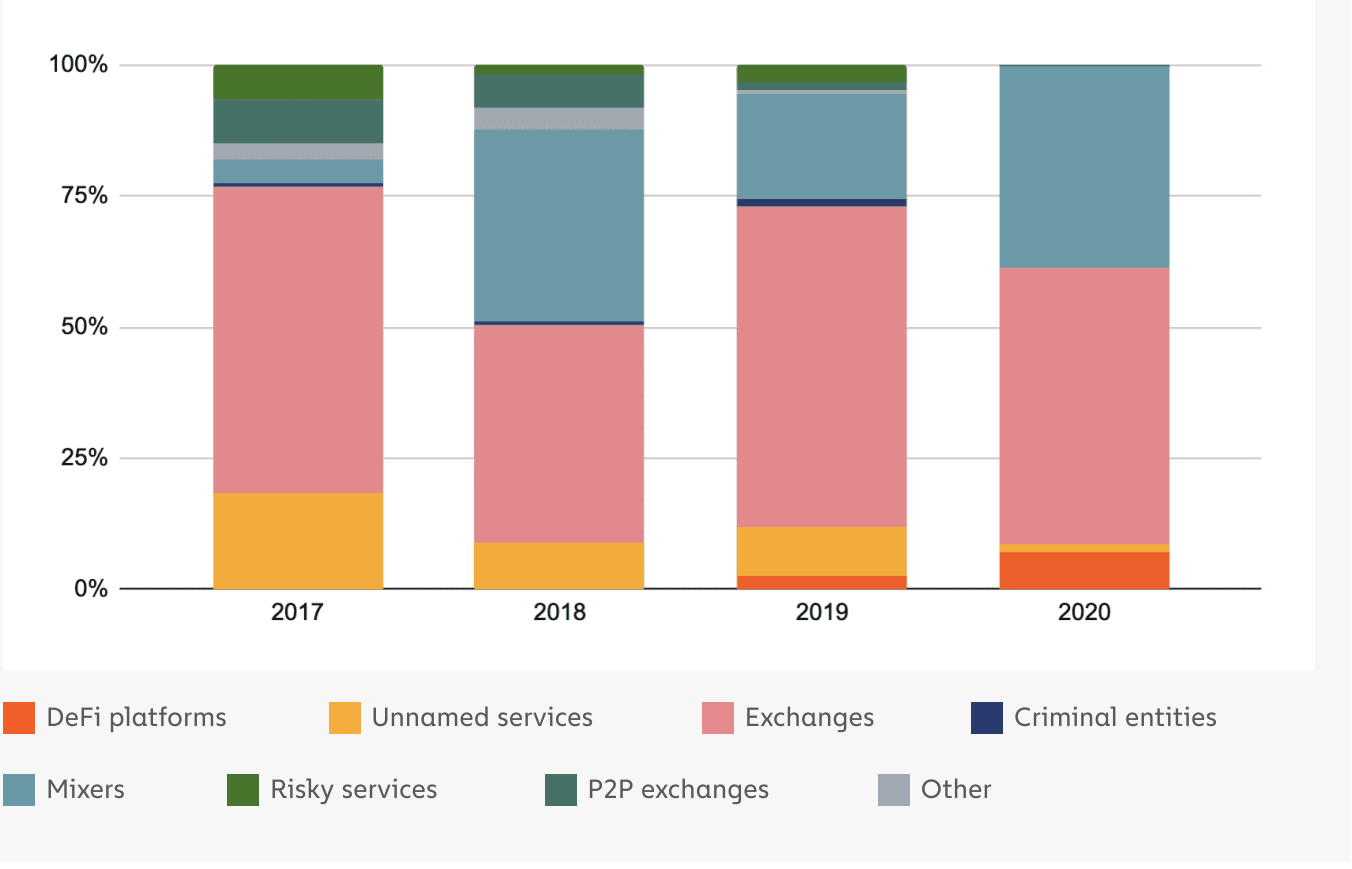


Green lines represent ETH or Token transfers. Purple lines represent DeFi platform interactions.

The cybercriminals first moved stolen LINK from their initial wallet to an intermediary, and from there, sent it to Uniswap to be traded for ETH. As a DeFi platform, Uniswap allows users to swap between ETH and several types of ERC-20 tokens without Uniswap ever taking custody of the funds, meaning that users don't have to provide KYC information. Users simply send funds to Uniswap from one address, and receive the equivalent amount back (minus minimal fees) at the same address in the token of their choice. So, in this case, the Kucoin hackers sent 12,552.96 LINK to Uniswap from the address "0xC194..." and received 360.60 ETH back to the same address. If investigators didn't already know that the hackers controlled the wallet that sent and received these funds, it would have been difficult to trace the funds' movements and spot the swap. As we can see on the graph, the hackers carried out many similar DeFi transactions using other types of tokens stolen in the hack.

The use of DeFi platforms represents a shift in Lazarus Group's money laundering strategy. The graph below shows the breakdown of the types of services the group has sent stolen funds to over the last few years.

Destination of cryptocurrency stolen by Lazarus Group | 2017 - 2020

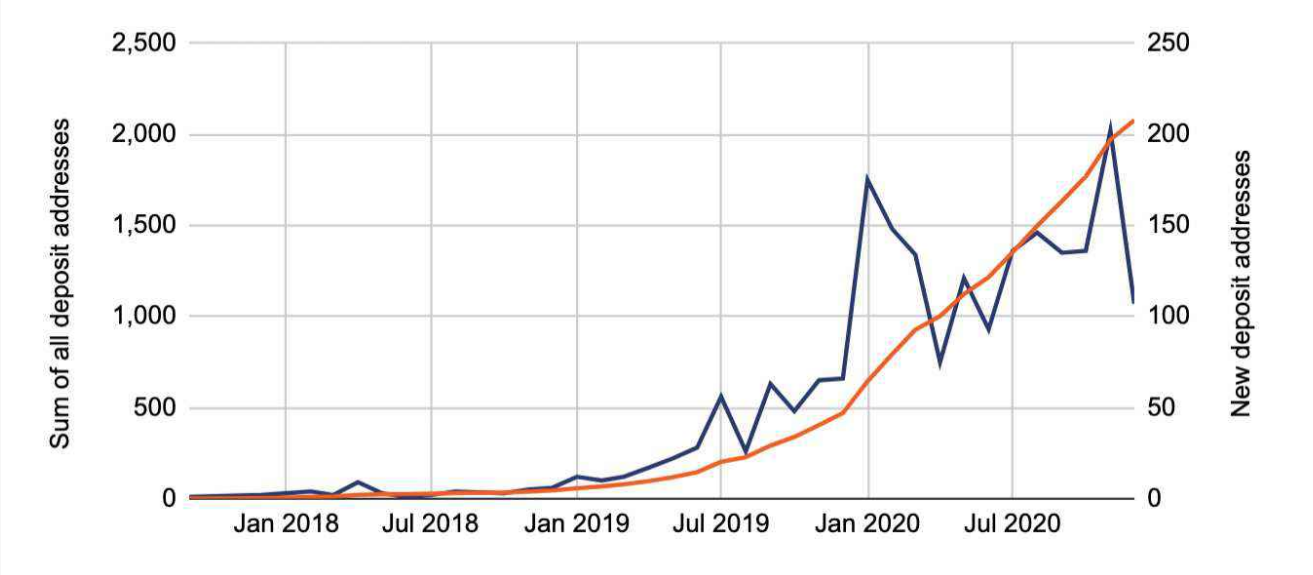


Currencies included: BCH, BTC, ETH, LTC, MKR, OMG, PAX, TUSD, USDT

Lazarus Group's use of DeFi platforms nearly doubled in 2020. The other trend that jumps out is the group's declining use of mainstream exchanges. While exchanges received the majority of funds stolen by Lazarus Group in 2019, much of that volume went to mixers in 2020. This may be a result of increased security efforts by exchanges following the DOJ's civil complaint against in August, which highlighted how Lazarus Group hackers frequently moved stolen funds through exchanges and OTC brokers using addresses nested at exchanges.

However, even if Lazarus Group isn't sending as high a percentage of funds to services, they're using more and more unique deposit addresses at services to launder funds. This trend accelerated in September 2019 and has continued since. Lazarus Group typically favors deposit addresses at a group of 20 different exchanges. In the chart below, we show the growth of deposit addresses at those exchanges that have received funds from Lazarus Group since 2018.

New deposit addresses vs. Cumulative sum of all deposit addresses used by Lazarus Group | Sep '17 to Dec '20



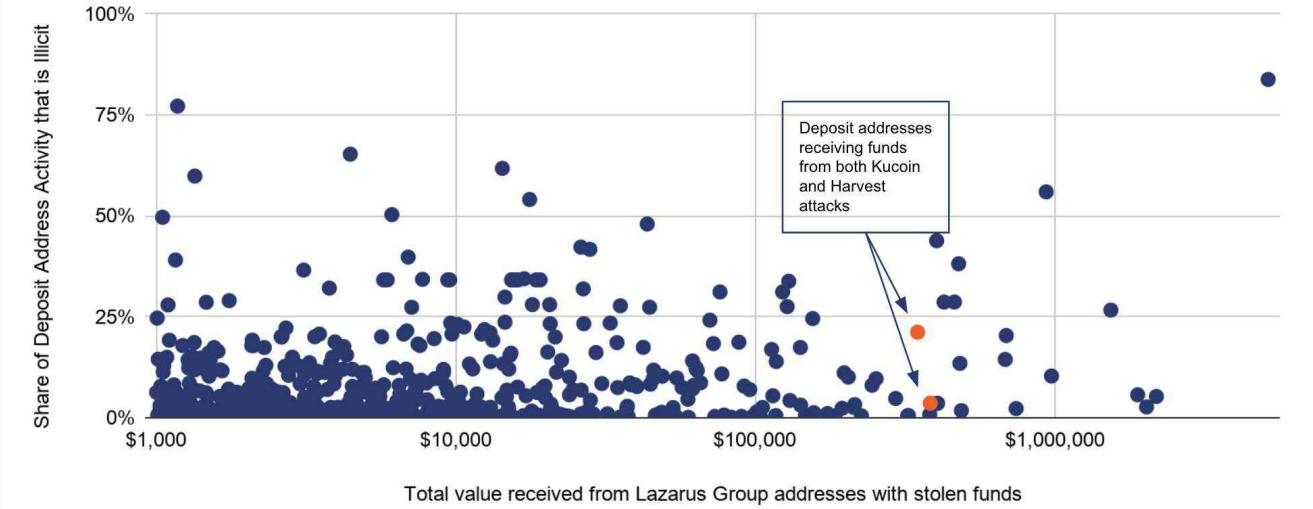
Currencies included: BCH, BTC, LTC, USDT

Note: Only includes deposit addresses at Lazarus Group's top 20 preferred exchanges

In December 2019, Lazarus Group had 470 separate cryptocurrency addresses at its top 20 exchanges that had received at least $1,000 worth of stolen cryptocurrency. By the end of December 2020, that number had risen to 2,078. This suggests that Lazarus Group is spreading its funds around more to mitigate the risk of any one address being identified and frozen. It also fits a pattern of adaptability on the part of Lazarus Group — each year, their money laundering strategy changes as services improve their security efforts.

We can't say for sure how many of these addresses are directly controlled by Lazarus and how many are controlled by OTC brokers and other nested service providers moving funds on behalf of Lazarus. However, we try to approximate it below by analyzing the activity of all service deposit addresses that have received more than $1,000 worth of cryptocurrency from Lazarus Group addresses in 2020, looking at the total value they've received from those addresses versus the share of all funds they've received that come from criminal sources.

Deposit Addresses Receiving Illicit Funds with Lazarus Group Connections



Currencies included: BTC

The majority of the funds go to deposit addresses that have received large sums from Lazarus Group and other criminal addresses, but whose overall activity is mostly non-illicit, and may therefore appear safe at first glance. Those addresses likely belong to nested services mostly processing legitimate transactions, rather than to wallets only moving illicit funds. That trend underlines the importance of exchanges digging into the details on the transactions carried out by nested services on their platforms — even large nested services for whom risky transactions make up a low share of total activity can be moving hundreds of thousands on behalf of rogue state actors like Lazarus Group, making them much more dangerous than they first appear.

Terrorism and Extremism Financing

Countries Around the World Collaborate to Fight Growing Cryptocurrency Usage in Terrorism Financing

In 2020, government agencies around the world uncovered, investigated, and prosecuted more terrorism financing schemes involving cryptocurrency than ever before. The most notable example came in August, when the United States Department of Justice (DOJ) announced the largest ever seizure of cryptocurrency from a terrorist group. Following an investigation into several different cryptocurrency donation campaigns, U.S. government agencies recovered more than $1 million worth of Bitcoin from wallets controlled by terrorist groups and their financial facilitators.

Below, we'll summarize the cryptocurrency-based terrorism financing campaigns law enforcement agencies investigated and prosecuted in 2020.

Disruptions of terrorism financing networks involving cryptocurrency announced in 2020

Case 1: al-Qaeda and ISIS

Investigating country: France
Destination of funds: Syria
Date of activity: 2019 - 2020
Summary: French authorities arrested 29 individuals in a cryptocurrency-based terrorism financing scheme. Dozens of people in France bought cryptocurrency coupons worth $11-$165. The coupons were credited to accounts opened abroad by jihadis who then converted them into cryptocurrency. Hundreds of thousands of euros are thought to have been supplied via the network, benefitting members of al-Qaeda still hiding out in northwest Syria, as well as jihadis of the Islamic State group.

Case 2: ISIS

Country investigating: U.K.
Destination of funds: Syria
Date of activity: 2016 - 2020
Summary: Hisham Chaudhary of Leichester, England is alleged to have gathered and transferred Bitcoin to jihadist groups, allowing captured ISIS militants to escape Kurd-controlled prison camps in northern Syria.

Case 3: The al-Qassam Brigades (Hamas' military wing)

Country investigating: U.S.
Destination of funds: Multiple
Date of activity: 2019 - 2020
Summary: Starting in 2019, the al-Qassam Brigades posted calls on its social media pages for Bitcoin donations to fund terror campaigns, before moving solicitation to its official websites and incorporating more sophisticated cryptocurrency wallet infrastructure.

Case 4: al-Qaeda and affiliated terrorist groups in Central Asia and elsewhere

Country investigating: U.S.
Destination of funds: Syria
Date of activity: 2019 - 2020
Summary: Terrorist organizations in several countries — primarily Syria, but also Central Asian countries such as Uzbekistan — solicited cryptocurrency donations from around the world on Telegram and other social media platforms, often posing as charity groups to bypass platform policies. These groups laundered and distributed funds using a Syria-based cryptocurrency exchange called BitcoinTransfer.

Case 5: Islamic State Khorasan Province

Country investigating: India
Destination of funds: India and Syria
Date of activity: 2019 - 2020
Summary: Kashmiri couple Jahanzaib Sami and Hina Bashir Beigh were arrested in Delhi on March 8 for allegedly planning to carry out attacks in India. The couple was accused of soliciting cryptocurrency donations to a Bitcoin address they received from a Syria-based ISIS operative. Sami discussed the possibility of using cryptocurrency donations to source weapons and explosives.

Let's dive into a few of these cases, starting with the most prominent: the now-disrupted terrorism financing campaigns launched by al-Qassam Brigades and al-Qaeda in Syria.

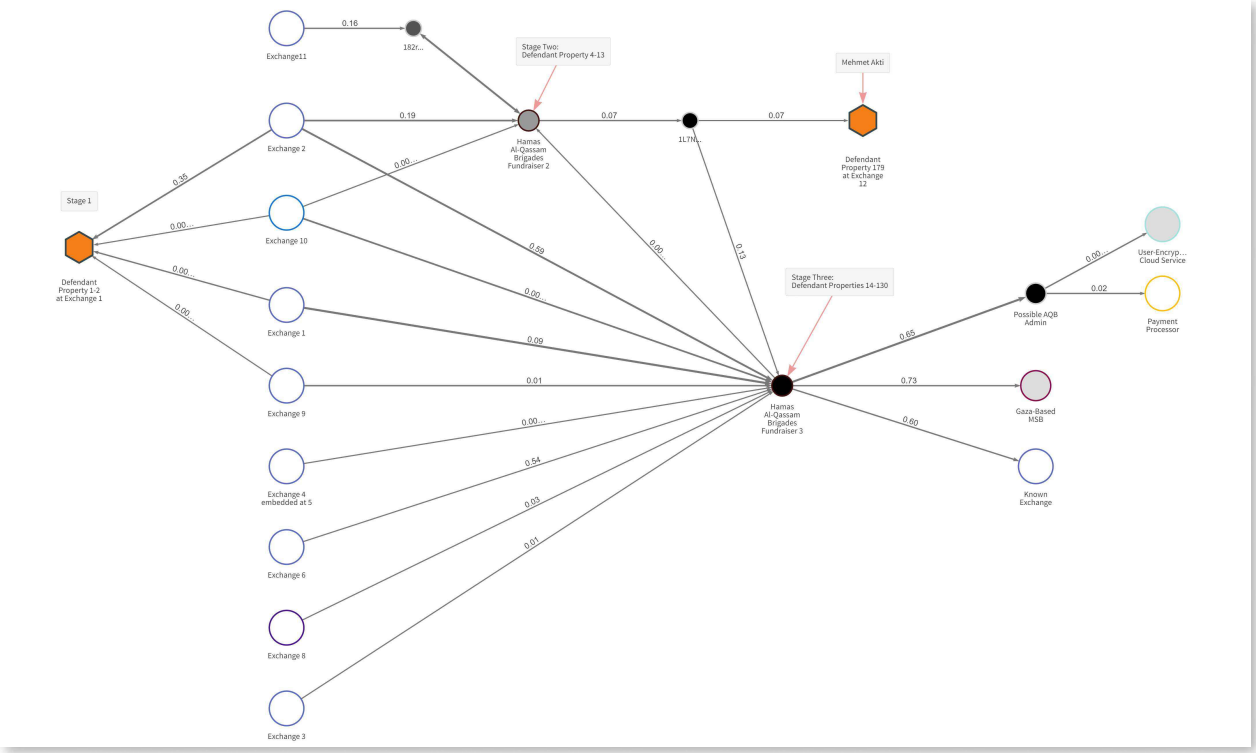
Taking down two large-scale terrorism financing campaigns

In August 2020, the Department of Justice announced the takedown of two of the most significant cryptocurrency-based terrorism financing campaigns seen to date. The first campaign (number 3 on our map) was conducted by Hamas' military wing, the al-Qassam Brigades (AQB), and took in tens of thousands of dollars' worth of Bitcoin between 2019 and 2020. The second campaign (number 4 on our map) was conducted by al-Qaeda and several associated groups in Syria, who used an Idlib, Syria-based cryptocurrency exchange called BitcoinTransfer to launder donations and distribute them between the groups involved. We'll recap both below.

Revisiting the al-Qassam Brigades' terrorism financing campaign

We covered AQB's terrorism financing campaign in last year's Crypto Crime Report, while the campaign was still ongoing. Our analysis focused on the campaign's growing sophistication throughout the year. Prospective donors were initially invited to send Bitcoin to a static address posted on social media, but within months, AQB built out a wallet infrastructure that generated a new, unique address for each individual donor, making the funds more difficult to trace. Jessi Brooks, an Assistant U.S. Attorney who prosecuted the AQB case, told us about the transformation. "It's a perfect example of how terrorists are learning more and more about cryptocurrency and figuring out how to use the technology for their own benefit," Brooks said. "During the investigation, we could literally see the financiers getting better at soliciting cryptocurrency donations in real time. I'm sure other terrorist groups will only build on AQB's techniques in the next campaigns."

Since then, however, U.S. agents seized AQB's primary web page promoting the campaign, and the organization hasn't received any new donations since October 2020. The Reactor graph below shows the three wallets AQB used throughout its campaign, which unfolded in three distinct stages of increasing technological sophistication. On the left, we see donations come in from several addresses, mostly hosted at large, mainstream exchanges, and on the right, we see where AQB moved cryptocurrency donations in an effort to launder and convert them to cash.



AQB used a mainstream cryptocurrency exchange, cryptocurrency merchant services provider, and two unlicensed money services businesses (MSBs) to convert cryptocurrency donations into cash. One of the unlicensed MSBs ran its cryptocurrency operation as a nested service, meaning it conducted all transactions using addresses at a mainstream exchange. Agents reached out to the exchange hosting those addresses and learned that they belonged to a Turkish national named Mehmet Akti, who owns and operates the unlicensed MSB. Most of the more than $1 million worth of cryptocurrency seized in this investigation came from Akti's businesses. According to the DOJ complaint, the main address he used to run his MSB received over $80 million worth of cryptocurrency and U.S. dollar wire transfers between October 2017 and March 2019, though the majority of this was likely unrelated to terrorism financing.

Unlicensed MSBs, many of which function on the hawala model, have always been important for terrorism financing. According to Brooks, that isn't changing, as many of these MSBs have incorporated cryptocurrency services as another means of sending funds around the world. "Terrorist groups taking cryptocurrency donations have a huge reliance on unlicensed MSBs because they need to turn their crypto into cash, but can't go to services that follow the

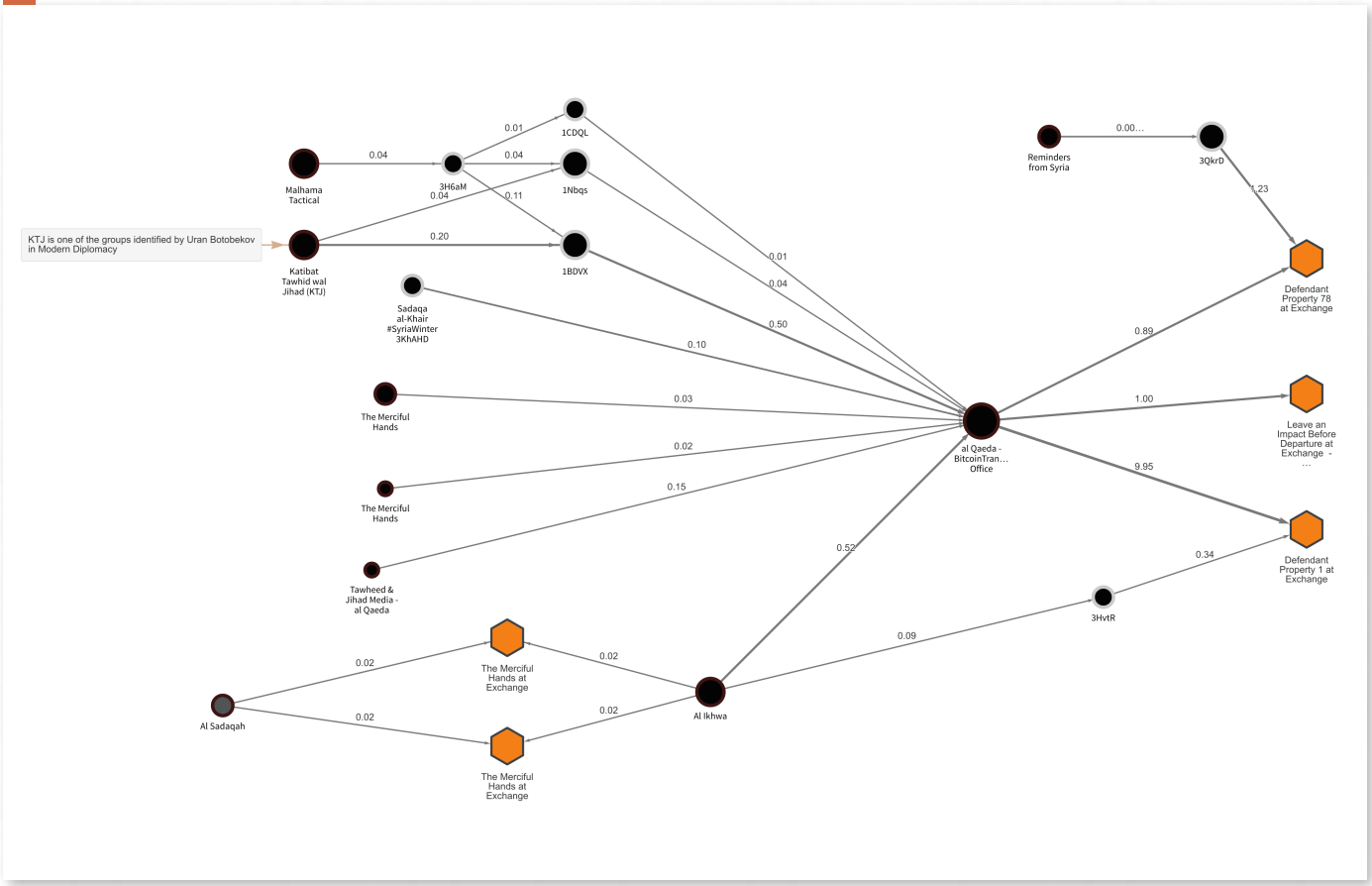
regulations," she said. "These businesses aren't solely working with terrorists. Terrorists aren't moving enough money to build a business around. What's scary is that many of them just don't care — they don't bother with KYC, and they get big while allowing terrorist groups to abuse them, but still transact with legitimate cryptocurrency businesses and with U.S. users."

How al-Qaeda used a cryptocurrency exchange as the hub of several linked donation campaigns

The DOJ also announced the takedown of a web of connected terrorism financing campaigns conducted by al-Qaeda and associated groups the same day it announced the takedown of the AQB campaign. The key difference between the al-Qaeda and AQB cases is that it involved several groups launching a shared infrastructure for collecting donations. In most cases, the terrorist groups presented themselves online as Syria-focused charities, but many of their posts and private communications made it clear that donations would be used to purchase weapons for jihadist groups. The terrorist groups involved include:

- **Malhama Tactical**, a private military contractor from Uzbekistan that has provided training for and fought alongside several terrorist groups in Syria.
- **Al Sadaqah**, a Syrian organization active on social media that purports to be a charity but has been implicated in terrorism financing.
- **Al Ikhwa**, a terrorist organization with documented ties to terrorist groups like Hay'at Tahrir al-Sham.
- **Reminders from Syria**, a Telegram channel affiliated with terrorist groups that frequently interacts with and boosts content from Al Ikhwa on social media.
- **The Merciful Hands**, another Syrian organization active on social media that purports to be a charity but has been associated with armed groups in Syria.

From there, these groups used multi-layered transactions to obfuscate the movement of these donations to a central hub of addresses, from which funds are then redistributed to the individual groups. Through blockchain analysis, we identified that central hub as BitcoinTransfer, a cryptocurrency exchange based in Idlib, Syria. BitcoinTransfer purports to be a cryptocurrency exchange but has been implicated in several terrorism financing schemes and appears to be fully under the control of terrorist groups. BitcoinTransfer processed more than $280,000 worth of Bitcoin between December 2018 and July 2020, much of it related to terrorism financing.



On the left, we see the addresses associated with the campaigns of the terrorist groups we listed earlier. Donations were consolidated at BitcoinTransfer, which we see in the middle, before moving to addresses at exchanges, where funds could be converted into cash or distributed elsewhere as needed.

In response to news of the takedown of this terrorism financing campaign, Kyrgyz political scientist Dr. Uran Botobekov published an article in Modern Diplomacy on several Central Asian jihadist groups' collection of Bitcoin donations (number five on our map). In addition to Malhama Tactical, the Uzbek group we cite earlier, Botobekov points to groups like Katibat Tawhid wal Jihad (KTJ), Katibat Imam al Bukhari (KIB) and the Islamic Jihad Group (IJG), whose members hail from Central Asia but have been active in Syria. Based on the transaction histories of the two Bitcoin donation addresses Botobekov provides in his article, these groups appear to have raised roughly $16,000 worth of cryptocurrency in 2020.

The groups involved in the BitcoinTransfer donation network, as well as the additional groups Botobekov cites in his article, underscore an important reason cryptocurrency is a valuable tool for terrorist groups: It's an easy way to send money around the world. While these groups were all focused on getting money to Syria at the time of these campaigns, they're based in different parts of the Middle East and Central Asia. Cryptocurrency allows them to send money across borders and coordinate the financing of their operations, with

less chance of transfers being blocked — especially when they rely on non-compliant cryptocurrency exchanges and unlicensed MSBs. However, as the takedown shows, their plans are far from fool-proof.

Collaboration is the key to fighting cryptocurrency-based terrorism financing

Another important lesson from the BitcoinTransfer case comes from what happened in its aftermath. After U.S. agents pinpointed the Syrian service as a hub of terrorism financing activity, agencies in other countries around the world were able to investigate suspicious transactions associated with it and uncover more terrorism financing schemes. Jessi Brooks told us more about how terrorism investigations involving cryptocurrency foster collaboration between agencies and countries. "It's one of the reasons I enjoy working on cryptocurrency cases," she said. "Right now, U.S. agencies are at the forefront of blockchain analysis. That's opened the door to more cooperation and allows our work to have an international impact."

She also emphasized that it's not just government agencies collaborating on these cases. It's cryptocurrency exchanges and other industry players as well. "If a big bank suffers a cyberattack or inadvertently facilitates terrorism financing, other banks don't really care. But if something like that happens to an exchange, it can affect Bitcoin's value, so everyone has skin in the game," she said. "The cryptocurrency world is smaller, so it's much easier for normal users to interact with an address that has ties to terrorism financing if that address isn't shut down, which creates problems for everyone. So partly for that reason, exchanges have responded really well and been helpful when we reach out for help on these cases."

Domestic extremism case study: Alt-right groups and personalities involved in January 2021 Capitol riot received over $500K in Bitcoin from French donor one month prior

Terrorism doesn't originate solely overseas. In recent years, U.S. law enforcement agencies have made it a priority to fight domestic extremism too. We're working alongside our government partners to investigate designated domestic terrorist groups' usage of cryptocurrency and ensure digital assets aren't used to fund acts of violence. The case study below is the result of our investigation into cryptocurrency donations received by figures and groups involved in the January 2021 riots at the U.S. capitol.

On January 6, 2021, Americans were shocked as a large group of Donald Trump supporters stormed the U.S. Capitol Building in protest of his 2020 election loss, following a rally that included a speech from Trump himself. Five people died, including two police officers, and significant damage was done to the building, including to many congressional representatives' offices. Several prominent members of the alt-right either took part in the raid or were present just outside the Capitol, including internet personality Nick Fuentes.

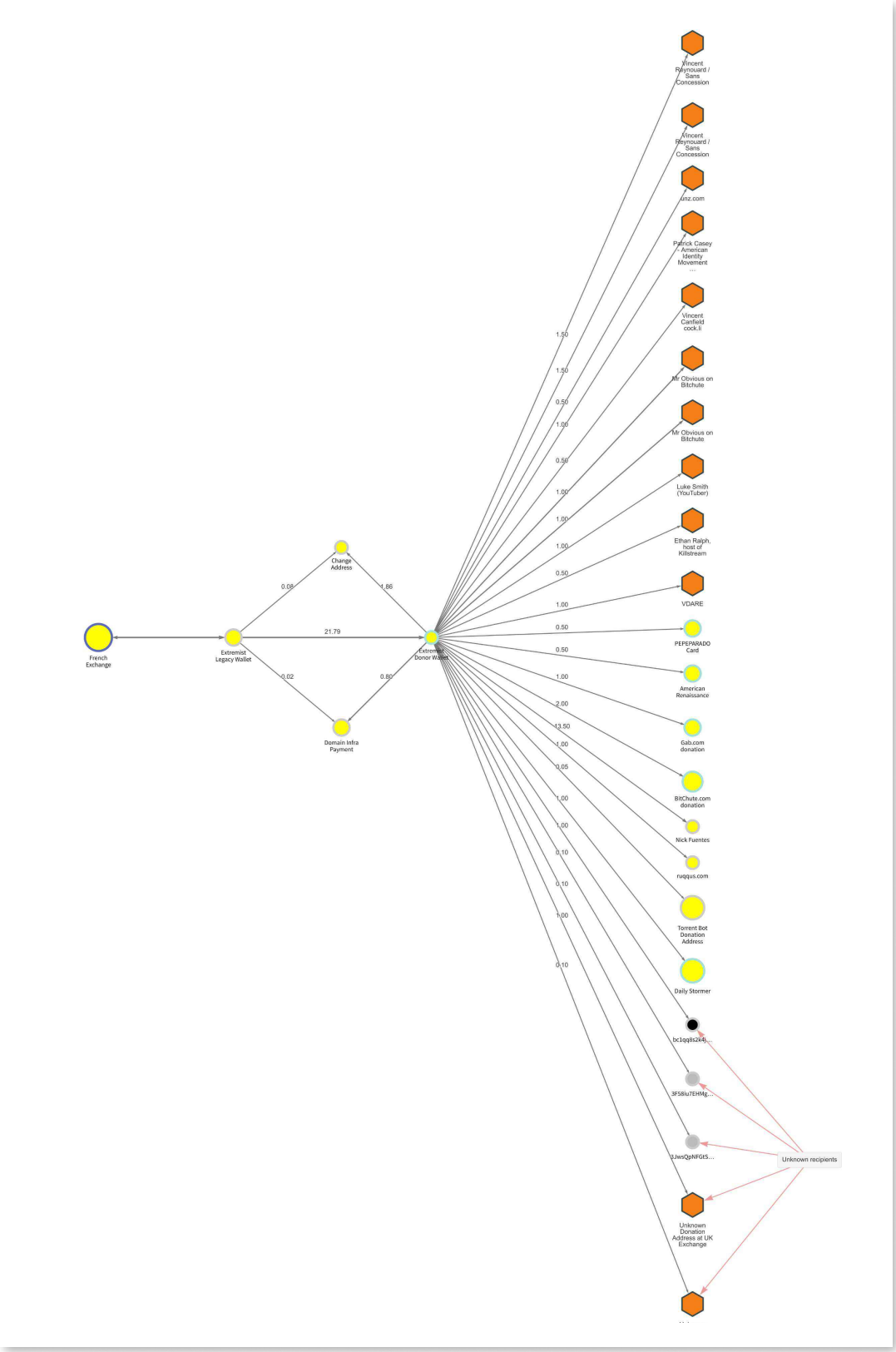
Nick Fuentes outside the Capitol. Photo credit to Nick Fuentes on Twitter.

It's unclear to what degree the attack on the Capitol was planned in advance. ProPublica reports that in the weeks leading up, many Trump supporters discussed turning the event violent on Parler, a rightwing social media app now banned by most major tech platforms. However, we now have evidence that many alt-right groups and personalities, including Fuentes, received large Bitcoin donations in a single transaction that occurred a month before the riot on December 8. We have also gathered evidence that strongly suggests the donor was a now-deceased computer programmer based in France.

While we won't share the donor's identity publicly, we'll walk you through how we made the identification and provide details on the donations below. The information we've uncovered shows that domestic extremism isn't strictly domestic. International networks play a role as well, which we see reflected in the nationality of this donor. The donation, as well as reports of the planning that went into the Capitol raid on alt-right communication channels, also suggests that domestic extremist groups may be better organized and funded than previously thought.

The donations

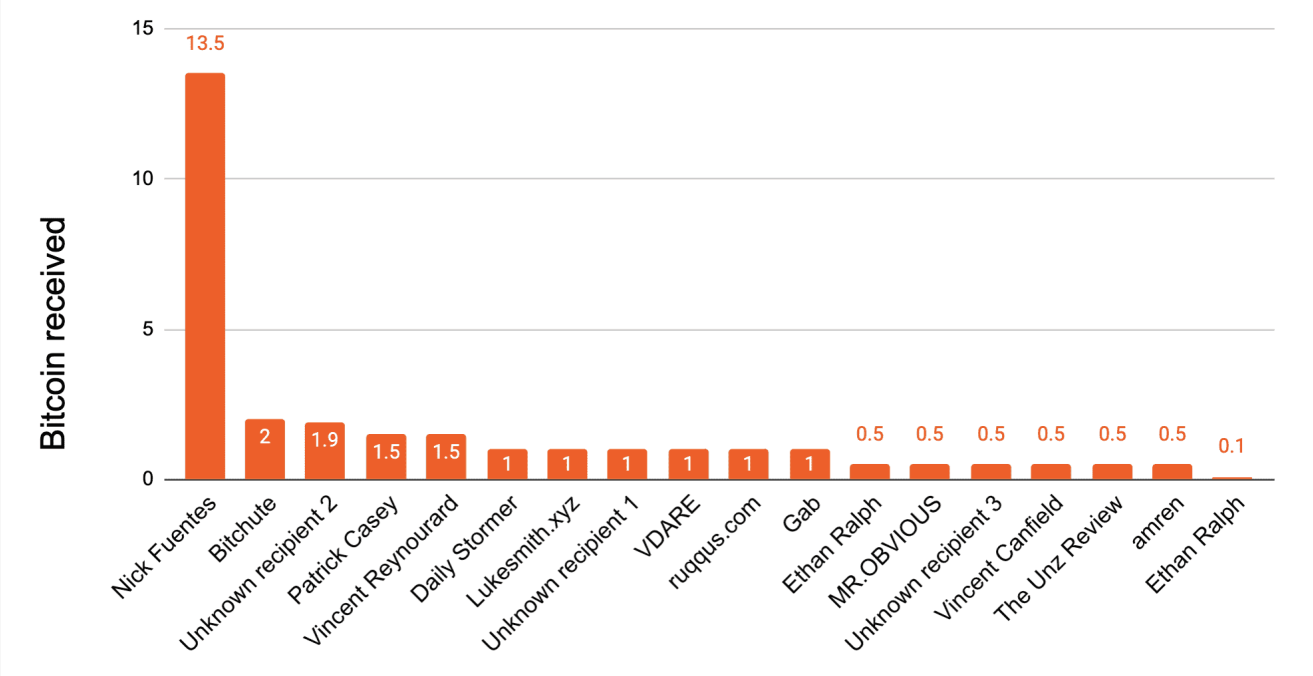
On December 8, 2020, a donor sent 28.15 BTC — worth approximately $522,000 at the time of transfer — to 22 separate addresses in a single transaction. Many of those addresses belong to far-right activists and internet personalities.



Here, we see that the donor sent Bitcoin to several alt-right organizations and online personalities. Unknown recipients are grouped in the lower right-hand corner.

Nick Fuentes received 13.5 BTC — worth approximately $250,000 at the time of the transfer — making him by far the biggest beneficiary of the donation. However, several others received significant funds as well, including anti-immigration organization VDARE, alt-right streamer Ethan Ralph, and several addresses whose owners are as yet unidentified.

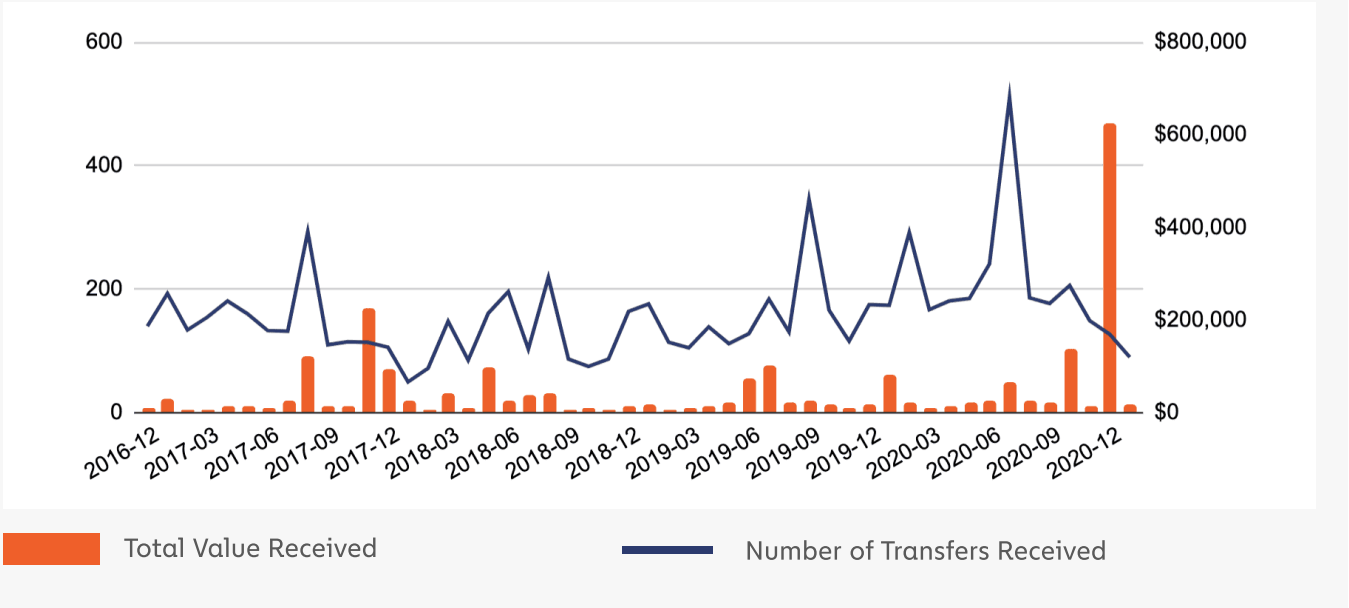
Who received funds from the December 8, 2020 extremist donation?



While there's no evidence yet that Fuentes entered the Capitol — in fact, he explicitly denies entering the building — he was present at the initial rally and seen outside the Capitol as the rioting began. Fuentes promoted the rally that preceded the violence in the month before on social media. PBS notes that in the days leading up, Fuentes encouraged his audience to engage in extreme behavior to prevent Joe Biden's election from being certified, even implying that they should kill state legislators. Fuentes had previously been banned from YouTube for hate speech, including Holocaust denial and promotion of other conspiracy theories.

The December 8 donation of over $250,000 worth of Bitcoin is by far the largest cryptocurrency donation Fuentes has ever received. Previously, the most he had ever received in a single month was $2,707 worth of Bitcoin.

Total Value Received by Domestic Extremists in Cryptocurrency

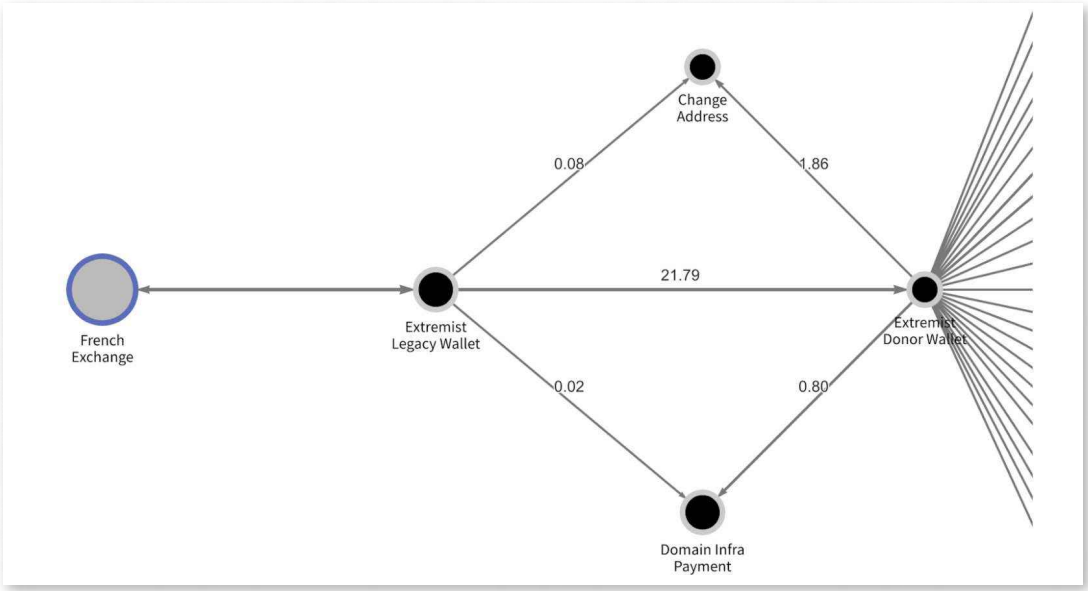


Currencies included: BTC

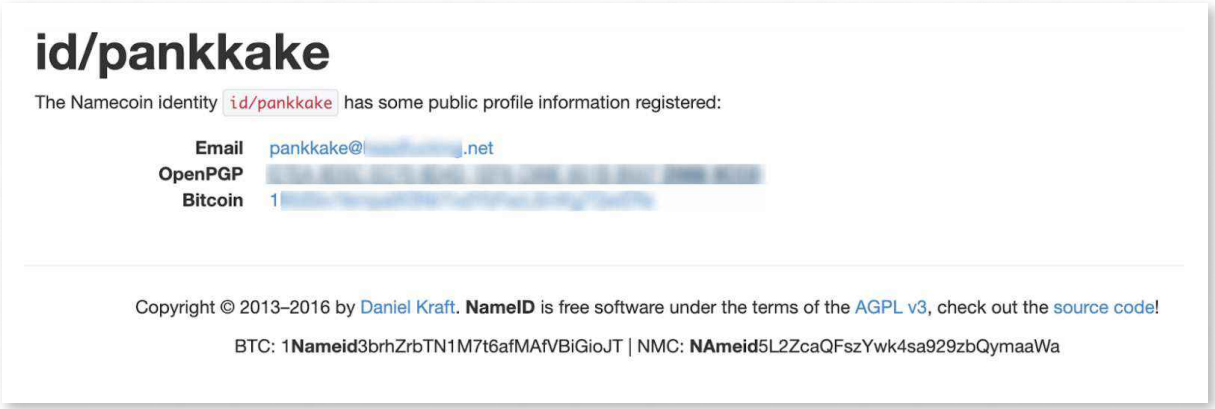
In fact, as we see in the graph above, this multi-recipient donation made December 2020 the single biggest month we've ever observed in terms of cryptocurrency received by addresses associated with domestic extremism. Still, this donation isn't a one-off. The data shows that domestic extremists have been receiving a steady stream of cryptocurrency donations since 2016.

Who is the extremist donor?

The extremist donor funded his donation wallet with cryptocurrency from a French exchange, which he moved to the donation wallet via an intermediary we've labeled "Extremist Legacy Wallet."

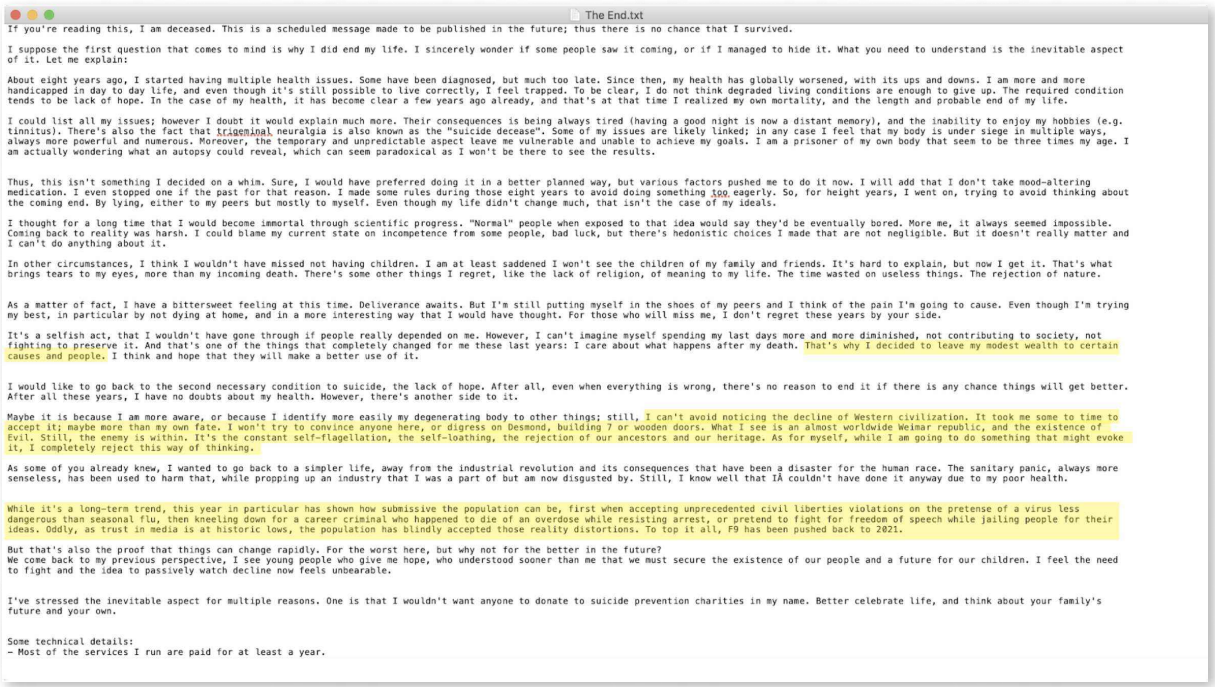


The Extremist Legacy Wallet first became active in 2013, suggesting that the extremist donor is a relatively early adopter of Bitcoin whose holdings have grown in value significantly. Using open-source intelligence, we discovered one BTC address associated with the Extremist Legacy Wallet is registered on NameID, a service that allows users to associate their online identity, email address, and other information with their Bitcoin address. In this case, the extremist donor associated his Bitcoin address with the pseudonym "pankkake."



In addition to his Bitcoin address, the extremist donor also listed an email address and an OpenPGP signature.

Searching for information on the email address led us to a personal blog we believe belongs to the extremist donor, and which identifies him as a French computer programmer. They had been inactive since 2014 until a new post was published on December 9, 2020 — the day after the donations were made. Shockingly, the post appears to be a suicide note. You can read it in the screenshot below.


The End.txt

If you're reading this, I am deceased. This is a scheduled message made to be published in the future; thus there is no chance that I survived.

I suppose the first question that comes to mind is why I did end my life. I sincerely wonder if some people saw it coming, or if I managed to hide it. What you need to understand is the inevitable aspect of it. Let me explain:

About eight years ago, I started having multiple health issues. Some have been diagnosed, but much too late. Since then, my health has globally worsened, with its ups and downs. I am more and more handicapped in day to day life, and even though it's still possible to live correctly, I feel trapped. To be clear, I do not think degraded living conditions are enough to give up. The required condition tends to be lack of hope. In the case of my health, it has become clear a few years ago already, and that's at that time I realized my own mortality, and the length and probable end of my life.

I could list all my issues; however I doubt it would explain much more. Their consequences is being always tired (having a good night is now a distant memory), and the inability to enjoy my hobbies (e.g. tinnitus). There's also the fact that trigeminal neuralgia is also known as the "suicide decease". Some of my issues are likely linked; in any case I feel that my body is under siege in multiple ways, always more powerful and numerous. Moreover, the temporary and unpredictable aspect leave me vulnerable and unable to achieve my goals. I am a prisoner of my own body that seem to be three times my age. I am actually wondering what an autopsy could reveal, which can seem paradoxical as I won't be there to see the results.

Thus, this isn't something I decided on a whim. Sure, I would have preferred doing it in a better planned way, but various factors pushed me to do it now. I will add that I don't take mood-altering medication. I even stopped one if the past for that reason. I made some rules during those eight years to avoid doing something too eagerly. So, for height years, I went on, trying to avoid thinking about the coming end. By lying, either to my peers but mostly to myself. Even though my life didn't change much, that isn't the case of my ideals.

I thought for a long time that I would become immortal through scientific progress. "Normal" people when exposed to that idea would say they'd be eventually bored. More me, it always seemed impossible. Coming back to reality was harsh. I could blame my current state on incompetence from some people, bad luck, but there's hedonistic choices I made that are not negligible. But it doesn't really matter and I can't do anything about it.

In other circumstances, I think I wouldn't have missed not having children. I am at least saddened I won't see the children of my family and friends. It's hard to explain, but now I get it. That's what brings tears to my eyes, more than my incoming death. There's some other things I regret, like the lack of religion, of meaning to my life. The time wasted on useless things. The rejection of nature.

As a matter of fact, I have a bittersweet feeling at this time. Deliverance awaits. But I'm still putting myself in the shoes of my peers and I think of the pain I'm going to cause. Even though I'm trying my best, in particular by not dying at home, and in a more interesting way that I would have thought. For those who will miss me, I don't regret these years by your side.

It's a selfish act, that I wouldn't have gone through if people really depended on me. However, I can't imagine myself spending my last days more and more diminished, not contributing to society, not fighting to preserve it. And that's one of the things that completely changed for me these last years: I care about what happens after my death. That's why I decided to leave my modest wealth to certain causes and people. I think and hope that they will make a better use of it.

I would like to go back to the second necessary condition to suicide, the lack of hope. After all, even when everything is wrong, there's no reason to end it if there is any chance things will get better. After all these years, I have no doubts about my health. However, there's another side to it.

Maybe it is because I am more aware, or because I identify more easily my degenerating body to other things; still, I can't avoid noticing the decline of Western civilization. It took me some to time to accept it; maybe more than my own fate. I won't try to convince anyone here, or digress on Desmond, building 7 or wooden doors. What I see is an almost worldwide Weimar republic, and the existence of Evil. Still, the enemy is within. It's the constant self-flagellation, the self-loathing, the rejection of our ancestors and our heritage. As for myself, while I am going to do something that might evoke it, I completely reject this way of thinking.

As some of you already knew, I wanted to go back to a simpler life, away from the industrial revolution and its consequences that have been a disaster for the human race. The sanitary panic, always more senseless, has been used to harm that, while propping up an industry that I was a part of but am now disgusted by. Still, I know well that IA couldn't have done it anyway due to my poor health.

While it's a long-term trend, this year in particular has shown how submissive the population can be, first when accepting unprecedented civil liberties violations on the pretense of a virus less dangerous than seasonal flu, then kneeling down for a career criminal who happened to die of an overdose while resisting arrest, or pretend to fight for freedom of speech while jailing people for their ideas. Oddly, as trust in media is at historic lows, the population has blindly accepted those reality distortions. To top it all, F9 has been pushed back to 2021.

But that's also the proof that things can change rapidly. For the worst here, but why not for the better in the future?
We come back to my previous perspective, I see young people who give me hope, who understood sooner than me that we must secure the existence of our people and a future for our children. I feel the need to fight and the idea to passively watch decline now feels unbearable.

I've stressed the inevitable aspect for multiple reasons. One is that I wouldn't want anyone to donate to suicide prevention charities in my name. Better celebrate life, and think about your family's future and your own.

Some technical details:
- Most of the services I run are paid for at least a year.

French publication 20 Minutes eventually confirmed the death of a French computer programmer who appears to have been the owner of the Bitcoin wallet from which the extremist donations were sent in December, and the blog on which the suicide note was published.

Most of the note details the author's health difficulties, which he says prompted him to commit suicide, but the sections we've highlighted provide strong evidence that the author is the extremist donor. He mentions that he has "bequeathed [his] fortune to certain causes and certain people," and cites several alt-right talking points in his analysis of the world today. For instance, he states his belief that "Western civilization is declining," and claims that Westerners are encouraged to hate their "ancestors and heritage." He also seemingly alludes to his belief that George Floyd died of a drug overdose rather than due to the actions of the police officer who violently apprehended him. All of these are common beliefs on the alt-right, and paint a picture of the donor's motivations for sending cryptocurrency to so many far right extremist figures.

Standing together against domestic extremism

While we don't know if these donations directly funded the violent gathering at the Capitol or any associated activity, the timing certainly warrants suspicion. As the Biden administration gears up to fight domestic extremism, these donations are a reminder of the need to track the cryptocurrency activity of all groups and individuals designated as terrorists, including those operating on U.S. soil. As mainstream payment platforms remove extremist groups and figures, we may see them embrace cryptocurrency more as a donations mechanism. Luckily, thanks to the inherent transparency of cryptocurrency blockchains, law enforcement can track these transactions in real time and work with cryptocurrency businesses to prevent funds from reaching violent groups who may use them to fund their operations and commit acts of violence. Chainalysis is actively looking to identify any additional extremist payments and activity and will keep our customers updated.

Conclusion

Crypto Crime Predictions for 2021

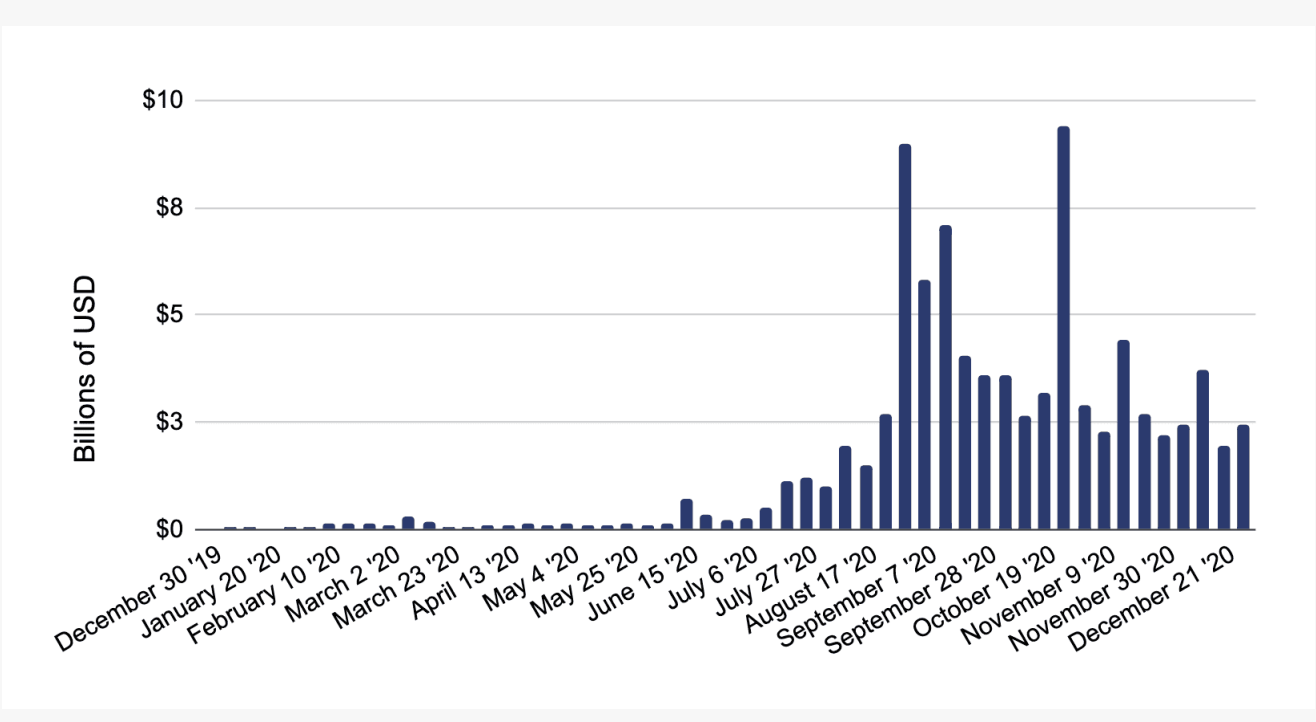
Cryptocurrency is an exciting industry because it's always evolving. In 2020, we've seen DeFi take off, institutional dollars flow in thanks in part to tailor-made platforms like Coinbase Prime, and exchanges like Kraken become chartered banks following new regulatory guidance from the U.S. government. Perhaps most exciting is that all of this happened in the face of a global pandemic — a true test of cryptocurrency's value as a safe haven asset — during which Bitcoin's price surged.

However, just as the cryptocurrency industry is always evolving, so too are the bad actors who commit cryptocurrency-related crime. Below, we offer our predictions for how crypto crime will change in 2021.

DeFi will play a bigger role in crypto crime

As we alluded to above, DeFi, which stands for decentralized finance, has skyrocketed in popularity this year.

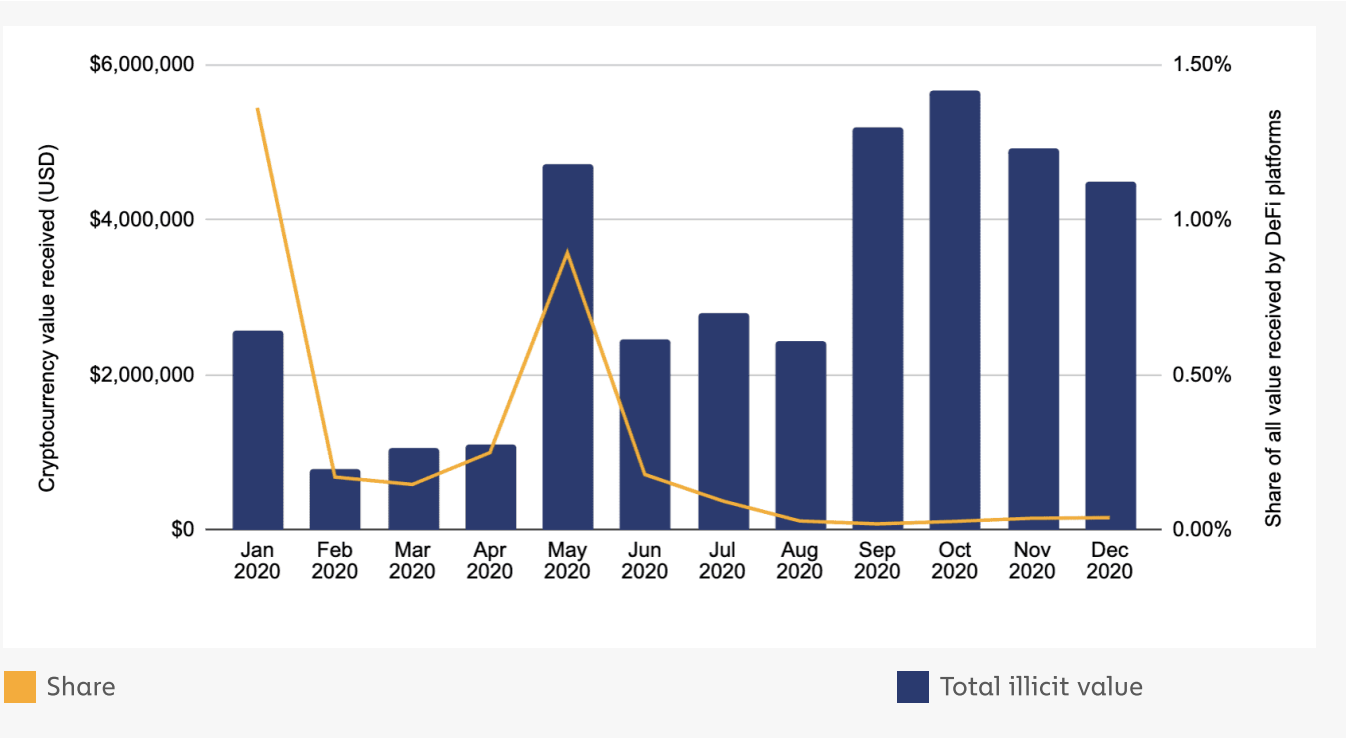
Total Weekly Value Received by DeFi Platforms | 2020



For context, DeFi platforms are decentralized apps built on top of smart contract-enriched blockchain platforms — primarily the Ethereum network — that let users automatically execute specific financial transactions such as trades and loans when certain conditions are met. DeFi platforms never take possession of a user's funds, and instead simply route them between users' wallets based on the conditions outlined in the underlying smart contracts without human intervention. Many believe that means they aren't subject to the same regulations as typical cryptocurrency businesses that take custody of users' funds. And because DeFi platforms can theoretically run without human intervention, there's often no team or organization keeping records or intervening when something goes wrong.

The potential lack of human intervention makes DeFi platforms appealing to users who value privacy, but potentially also to criminals looking to launder ill-gained funds. In the chart below, we approximate that activity thus far by looking at the volume of cryptocurrency that's moved from criminal addresses to DeFi platforms.

Total value and share of all value sent to DeFi platforms from criminal addresses | 2020



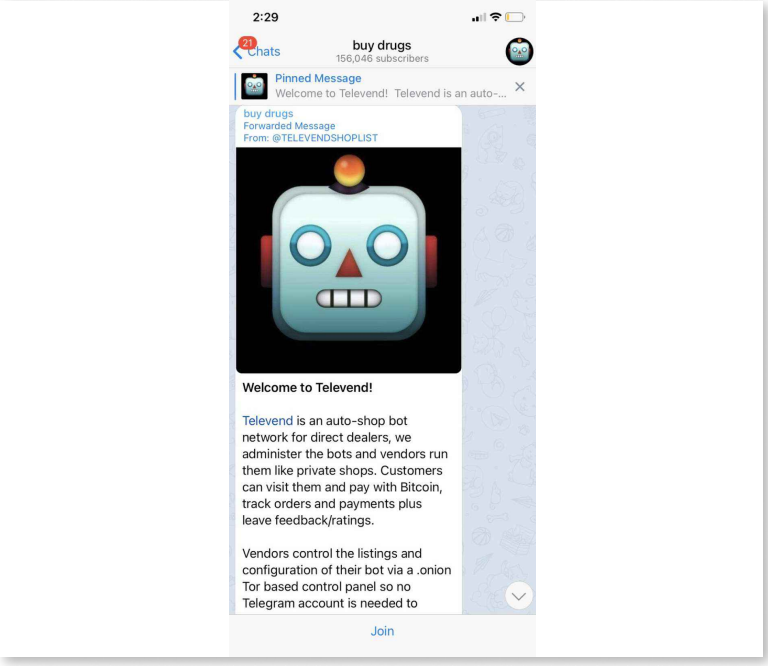
In total, more than $38 million worth of illicit cryptocurrency moved to DeFi platforms in 2020, with the monthly figure generally rising throughout the year. The KuCoin exchange hack was a notable example of this, as the cybercriminals involved moved substantial portions of the $275 million worth of cryptocurrency stolen to DeFi platforms — though in this case, luckily, the creators of the platforms in question retained enough control to freeze some of the transfers.

Still, we expect cybercriminal use of DeFi for money laundering to increase in 2021. DeFi platforms such as decentralized exchanges have existed for years, but took off in 2020 due in large part to improvements in user interfaces, which made them much easier for relatively inexperienced cryptocurrency users. This in turn led to greater liquidity, which made DeFi platforms even more appealing, creating a flywheel effect that led to even more growth. We expect those trends to continue in 2021, which will only make DeFi more attractive to criminals. The question that remains is whether the most popular platforms will be those where administrators retain enough control to prevent criminal transactions, as we saw in the KuCoin hack.

More decentralization in darknet markets

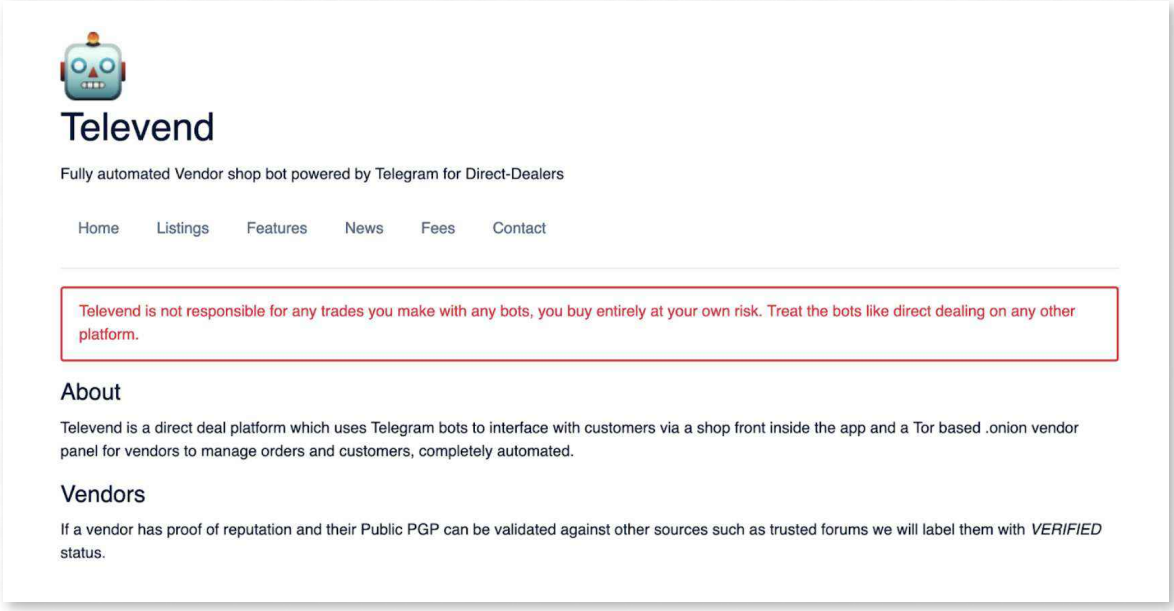
Darknet market decentralization is another trend we've seen pick up in 2020, and that we think will continue into 2021 and beyond. As we discuss elsewhere in this report, it's never been harder to run a darknet market. More markets went out of business than ever in 2020, and not due to Covid. Competition has intensified between darknet markets, with some initiating denial-of-service (DOS) attacks against rival markets, and several others exit scamming, which has significantly reduced buyer trust. At the same time, law enforcement is shutting down more markets and putting administrators in jail, leaving market administrators — who despite all the risk they take on receive roughly 5% commissions on sales — less willing to continue their work.

But a new decentralized model embodied by platforms like Televend may solve many of these problems for darknet markets. Televend is a Telegram-based platform with over 150,000 users where darknet market vendors can sell drugs through automated chatbots, whose communications with buyers are highly encrypted.

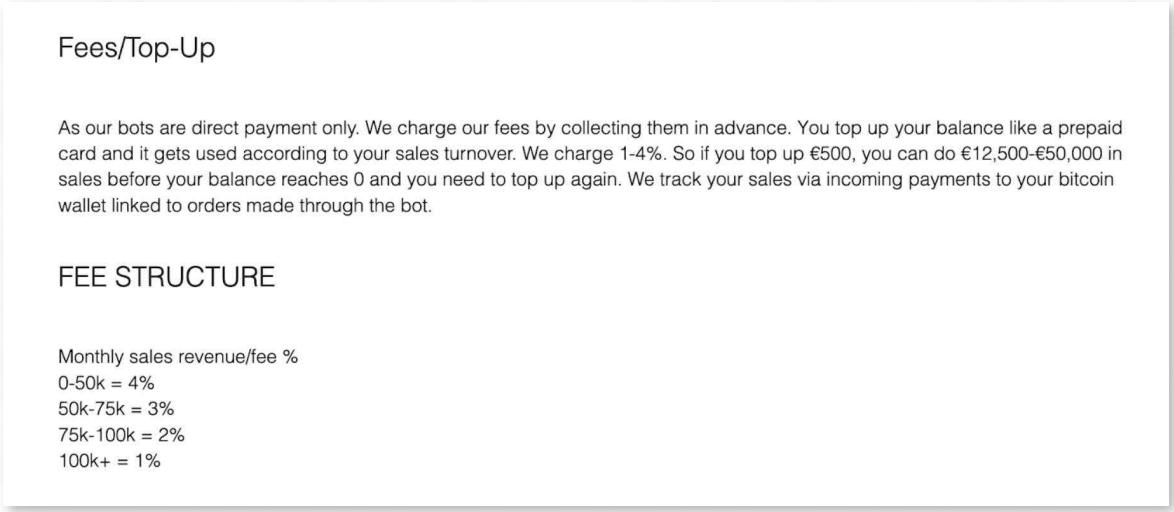


A screenshot of Televend

Buyers simply access Televend's Telegram group, where they find a directory of drug vendors broken down by region and products on offer. From there, they simply place orders with their chosen vendor's chat bot, receive an automatically-generated Bitcoin address to which they send payment, and wait for their drugs to arrive in the mail.



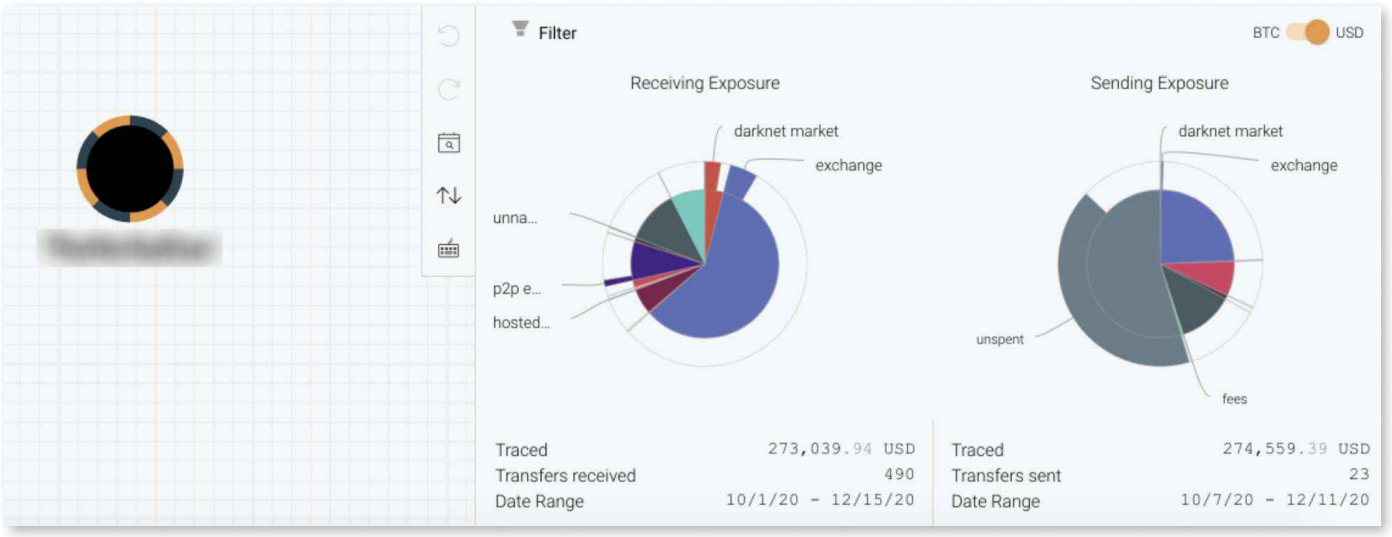
A screenshot from Televend's darknet site



Televend's fee structure explained

Televend receives commissions on each sale, but never actually touches the funds, so there's no central entity for law enforcement to track through blockchain analysis — the transactions blend in much more easily.

We studied the Bitcoin transaction history of one prominent Televend vendor, which you can see a summary of in the Chainalysis Reactor screenshot below.



Since Televend became active in October 2020, this vendor's wallet has received over $270,000 worth of Bitcoin across nearly 500 transactions. Customers appear to have paid mostly through cryptocurrency exchanges, which is also where the vendor has sent most of the funds. However, while we don't show it above, this wallet has been active since June 2019 — Televend allows vendors to receive their earnings to any address of their choosing — and received an additional $1.4 million worth of Bitcoin before Televend opened. It therefore appears likely that this vendor was active on traditional darknet markets before migrating to Televend. This vendor is one of over 150 active on Televend, though it's unclear if the others are bringing in as much revenue.

We expect platforms like Televend to grow and take in a larger share of total darknet market revenue in 2021, as their decentralized nature makes them more resilient to attacks from both law enforcement and rival markets. While future decentralized markets may run on platforms other than Telegram, Televend shows that the encrypted messaging platform can offer customers an easy buying experience.

Exchanges will treat other services with more scrutiny as risk-based compliance becomes the norm

Traditionally, too many exchanges have relied on other cryptocurrency services' (including other exchanges') publicly stated KYC and AML policies when assessing their riskiness. If the policy checked out, many exchanges would treat the service as if it were safe. But that won't cut it anymore in an era when institutional dollars are flowing into cryptocurrency like never before. Whether they're buying cryptocurrency of their own as an investment, offering custodial services, or accepting cryptocurrency businesses as banking clients, mainstream

financial institutions are going to need to enforce compliance more stringently than cryptocurrency businesses themselves have. That means they won't be taking compliance policies at face value. Instead, they'll insist on taking advantage of cryptocurrency's inherent transparency.

In a monetary system where every transaction is recorded on a public, unchangeable ledger, why wouldn't a financial institution aggressively analyze that information to ensure they're working with the safest possible businesses? Exchanges and other cryptocurrency businesses who want to work with these financial institutions will need to follow suit and assess their own counterparties with equal rigor. Increased compliance scrutiny by cryptocurrency exchanges will drive crypto crime down, as more wrongdoers will be reported to the authorities and stopped sooner than they otherwise would have been. In the long run, these efforts by exchanges will also remove some of the incentive to use cryptocurrency in criminal activity, as it will become much harder for cybercriminals to convert cryptocurrency into cash if they can't use exchanges.

The crypto crime outlook has never been better

Some of the upcoming advancements of cryptocurrency will make it more difficult for law enforcement and compliance professionals to detect and fight criminal activity. However, we remain confident that both groups, along with the institutional investors we discussed earlier, can come together to meet the challenge, and ultimately create a safer cryptocurrency ecosystem for all participants. Chainalysis looks forward to supporting their efforts.

Authors

Kim Grauer
grauer@chainalysis.com

Henry Updegrave
henry.updegrave@chainalysis.com

ABOUT CHAINALYSIS

Chainalysis is the blockchain analysis company. We provide data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies in over 50 countries. Our data platform powers investigation, compliance, and risk management tools that have been used to solve some of the world's most high-profile cyber criminal cases and grow consumer access to cryptocurrency safely. Backed by Accel, Addition, Benchmark, Ribbit, and other leading names in venture capital, Chainalysis builds trust in blockchains to promote more financial freedom with less risk. For more information, visit **www.chainalysis.com**.

GET IN TOUCH:

info@chainalysis.com

FOR MORE CONTENT:

visit blog.chainalysis.com

Chainalysis

Building trust in blockchains