Chainalysis

Written Testimony of Jonathan Levin
Co-Founder and Chief Strategy Officer
Chainalysis Inc.

Before the
Senate Banking Committee

Hearing on
Understanding the Role of Digital Assets in Illicit Finance

Thursday, March 17, 2022

Chairman Brown, Ranking Member Toomey, and distinguished members of the Committee. Thank you for inviting me to testify before you today on this very important topic.

My name is Jonathan Levin and I co-founded Chainalysis Inc. in 2014 with Michael Gronager, CEO of Chainalysis. I currently serve as Chief Strategy Officer.

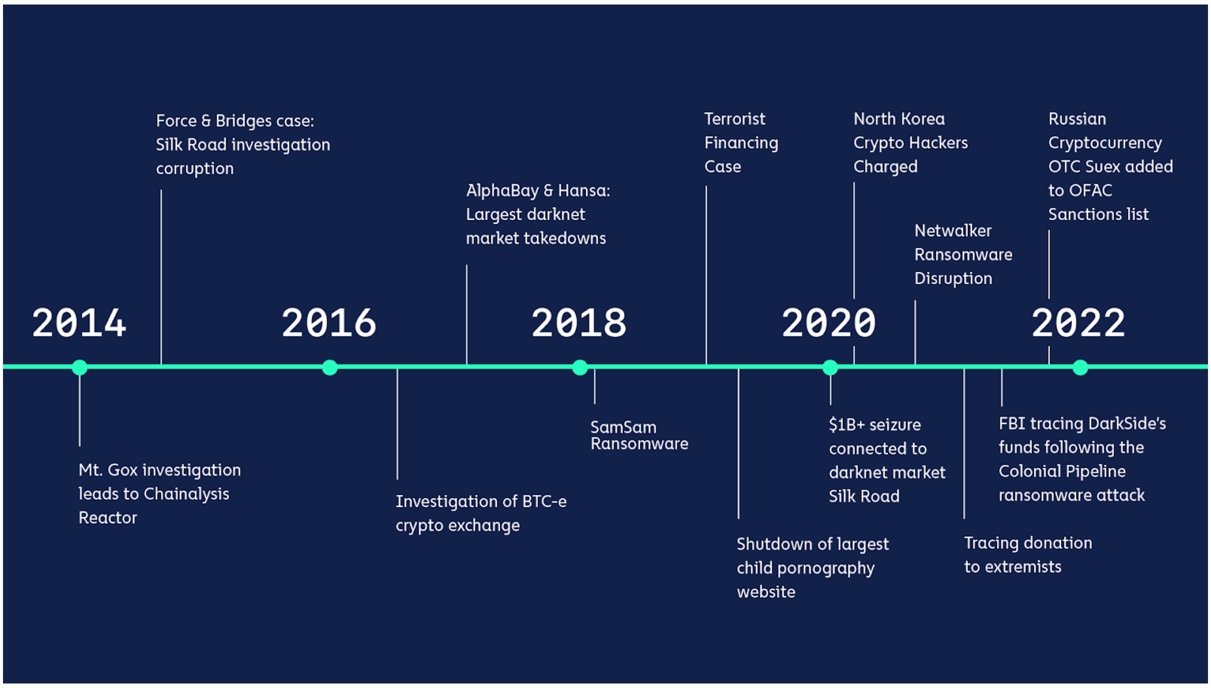
My family fled the pogroms of Eastern Europe and Lithuania to look for a better life in the West. They took nothing with them. We have a similar situation at present today in Ukraine where many people are crossing borders having left loved ones and possessions behind. We are connected to them through our commitment to humanity and democracy. This global community, organized on the internet, to provide support, humanitarian aid and assistance requires new ways to represent, store and transfer value. The pace of finance will always lag but ultimately catches up with the pace of information.

It is this ability for global communities to come together in this way that sparked my interest in digital assets 10 years ago. Bitcoin for me asked the best questions about the potential for global communities to coalesce around new systems of value and complement our existing financial infrastructure. It was clear that the existing financial infrastructure would not cover all of the ways that our children would want to organize, having grown up on the internet. Bitcoin is an example of a community that has evolved from no people knowing or caring about it 10 years ago to a more than 100 million strong community in its own right–and one that has spurred the innovation of many more digital asset communities around music, art, decentralized finance and even electric vehicles. These communities have now turned into economies that will continue to proliferate and impact many parts of the globe and the economy.

The Committee has selected excellent time to hold this hearing : a week after President Biden's Executive Order launched a whole-of-government approach to digital asset policy and just under a month after Russian troops invaded Ukraine triggering broad sanctions by the US and its allies that includes digital assets, provide the immediate context for today's important discussion. We applaud the members of the Banking Committee to taking a constructive approach to engaging with this technology. Digital asset markets now have a market capitalization of just under $2 trillion. Moreover, according to a recent Harris poll an estimated 28% of Americans trade digital assets, in addition to 12% who have traded them in the past.

Chainalysis is the blockchain data platform. We provide data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies. Chainalysis currently has over 660 customers in 65 countries. We currently have over 600 employees globally, 361 of whom are in the United States, across 27 states and the District of Columbia. Like many other digital asset-sector companies, we are growing rapidly and expect to hire over 300 additional employees in the US over the next year.

Our data platform powers investigation, compliance, and risk-management tools that have been used to solve many of the world's most high-profile cyber-crime cases and grow consumer access to digital assets safely. We have worked closely with law enforcement and regulators as they have worked to disrupt and deter illicit uses of digital assets. Below is a list of cases where we are able to publicly disclose our involvement:


2014
2016
2018
2020
2022
Force & Bridges case: Silk Road investigation corruption
Mt. Gox investigation leads to Chainalysis Reactor
AlphaBay & Hansa: Largest darknet market takedowns
Investigation of BTC-e crypto exchange
SamSam Ransomware
Terrorist Financing Case
Shutdown of largest child pornography website
North Korea Crypto Hackers Charged
$1B+ seizure connected to darknet market Silk Road
Netwalker Ransomware Disruption
Tracing donation to extremists
Russian Cryptocurrency OTC Suex added to OFAC Sanctions list
FBI tracing DarkSide's funds following the Colonial Pipeline ransomware attack

Chainalysis' partnerships with law enforcement and regulators are consistent with our corporate mission: to build trust in blockchains. Fundamentally, we believe in the potential of open, decentralized blockchain networks to drive new efficiencies, reduce barriers for innovators to create new financial and commercial products, encourage innovation, enhance financial inclusion, and unlock competitive forces across financial services and other markets. Our goal is to contribute our data, tools and expertise to drive illicit finance and other risks out of the digital asset ecosystem, enabling the realization of the technology's potential.

In my testimony and its appendices, I outline the many ways that digital assets can be exploited by illicit actors. Just as with any new technology, criminals have found ways to exploit digital assets. I want to be clear, though – and Chainalysis does a great deal of research on this front – that these transactions are the exception to the rule. Our 2022 Crypto Crime Report was released last month and it shows that transactions involving illicit addresses represented just 0.15% ($14 billion) of digital assets transaction volume in 2021 (not including centralized exchange volumes). This is because digital asset usage is growing faster than ever before and the legitimate use of digital assets is vastly outpacing the growth in their criminal use. This figure may rise slightly as we identify more addresses associated with illicit activity and incorporate their transaction activity into our historical volumes, and it also only reflects on-chain activity. This means, for example, that illicit activity happening within exchanges is not captured, as we do not have the internal order book data of exchanges. Those caveats aside, I do think it is important to note that illicit activities using digital assets is reflective of significantly less than 1% of transaction volumes, and this is thanks in part to the types of tools we provide to digital asset companies to support their AML/CFT compliance and the excellent work of law enforcement and regulators.

If there is one point we want to make to the Members of the Banking Committee, it is that the transparency of blockchains *enhances* the ability of policymakers and law enforcement to detect, disrupt and, ultimately, deter illicit activity. When it comes to detecting and disrupting illicit activity, by mapping a single illicit actor to a wallet address, e.g., a ransomware attacker or sanctions evader, law enforcement unlocks immediate insight into the network of wallet addresses and services (e.g., exchanges, mixers, etc.) that facilitate the illicit actor. In contrast, in a traditional finance investigation, a similar tip, linking an illicit actor to a bank account, is just the beginning of a long, expensive process to request and subpoena records that are manually reviewed and reconciled to generate a comparable amount of insight. Even with this insight, it comes with a significant time delay that creates opportunities for illicit actors to evade justice vs. the real-time monitoring capabilities of blockchain intelligence.

It is through this transparency that law enforcement, leveraging Chainalysis tools, was able to trace the Colonial Pipeline ransomware attackers (see case study below) and ultimately recover many of the funds sent to the attackers. It is also through this transparency that Chainalysis is able to produce a comprehensive global survey of illicit activity involving digital assets through our annual Crypto Crime Report ("Crime Report"). Key findings from the 2022 Crime Report published last month are highlighted below.

Moreover, a financial system built on blockchain rails can *enhance* the effectiveness of financial regulation more broadly. Policymakers should consider not just integrating digital assets into existing regulatory structures but leveraging their capabilities to improve oversight to reduce systemic risk and to protect consumers, among other traditional financial regulatory goals. With a blockchain-based financial system, regulators could have a real-time view into financial flows, risk exposures, and interconnectedness across all asset classes. Advanced risk analytics could provide regulators the ability to easily independently stress test the entire portfolio of a financial institution, as well as an entire financial system using current or historic portfolio data. Enhanced transparency afforded by blockchain technology could also facilitate and improve the efficacy of regulator and independent examinations, including as they relate to disclosure and reporting.

My testimony today will cover these topics:

- How blockchain data and analysis benefits investigations into illicit activity involving digital assets
- An overview of illicit activity involving digital assets from our Crime Report
- The risk of the use of digital assets by Russian specially designated nationals and blocked persons ("SDNs") to evade US sanctions
- Chainalysis' recommendations for how Congress and regulators can act to better detect, disrupt, and deter illicit uses of digital assets, including sanctions evasion

In **Appendix A,** we provide a summary of the 2022 Crime Report and in **Appendix B,** analysis relating to self-custodied "unhosted" wallets, putting their potential use by illicit actors in appropriate context. In **Appendix C,** we included a glossary of digital asset service types, including legal entities like retail exchanges or illicit activities like darknet markets, ransomware, or scamming.

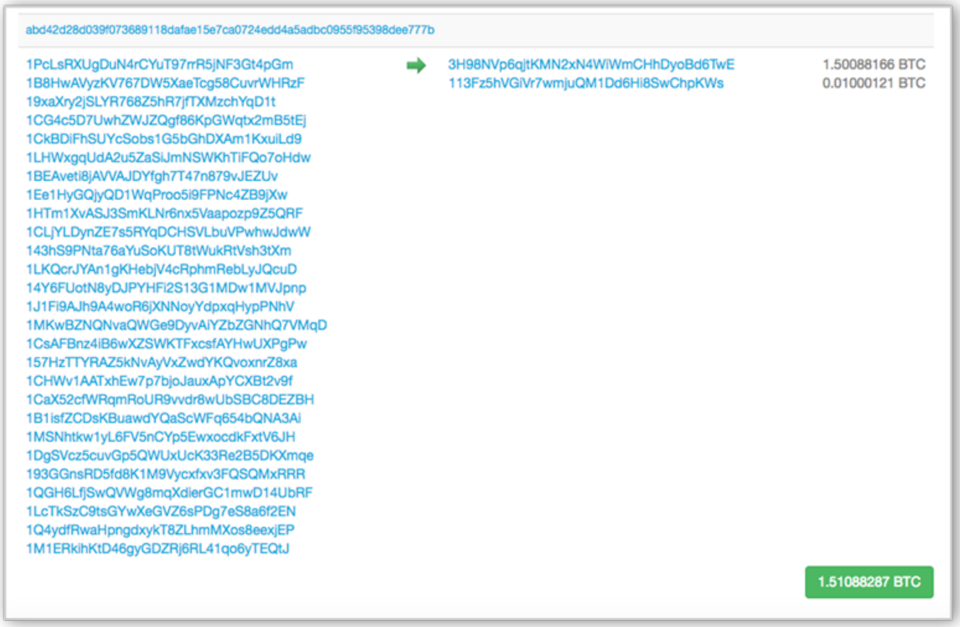
Before I launch into these topics, I want to highlight Chainalysis' announcement last week of free tools for digital asset businesses, including decentralized web3 organizations like decentralized exchanges ("DEXes"), decentralized finance ("DeFi") platforms, distributed autonomous organizations ("DAOs") to help them comply with sanctions requirements. These tools – an API and an on-chain oracle – will provide any digital asset business, protocol, organization, or developer a programmatic way to quickly check whether or not an address is on the sanctions list before allowing it to connect with their service.

We are excited about the potential of DeFi to democratize finance by putting asset owners of any size on equal footing with traditional market makers to earn returns based on contributing liquidity. Our tools help DeFi users remain compliant with sanctions requirements and therefore help unlock the potential of DeFi.

How blockchain data and analysis benefits investigations into illicit activity involving digital assets

It is a common misconception that digital assets are completely anonymous and untraceable. In fact, the transparency provided by many digital assets' public ledgers is much greater than other traditional forms of value transfer. Digital assets are assets that are issued and transferred using distributed ledger or blockchain technology, including, but not limited to, cryptocommodities, cryptocurrencies, non-fungible tokens ("NFTs"), securities tokens, stablecoins, etc. To understand the role of illicit activity in the digital markets, we need to set the stage by highlighting a foundational feature of blockchains: their transparency.

Each transaction on the blockchain is transparent and recorded in real-time on an immutable transaction ledger. Holdings of digital assets are visible as wallet balances which are also transparent and recorded on an immutable ledger. While the blockchain ledger publicly shows a string of random numbers and letters that transact with another string of random numbers and letters, the use of tools like Chainalysis enables these records to be transformed into an audit trail for monitoring current activity as well as historic activity by tying wallet addresses to real-world identities. Below shows what you might directly observe on a blockchain:

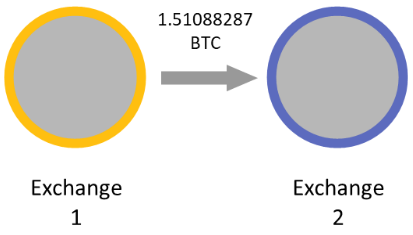


```
abd42d28d039f073689118dafae15e7ca0724edd4a5adbc0955f95398dee777b

1PcLsRXUgDuN4rCYuT97rrR5jNF3Gt4pGm        ➡   3H98NVp6qjtKMN2xN4WiWmCHhDyoBd6TwE    1.50088166 BTC
1B8HwAVyzKV767DW5XaeTcg58CuvrWHRzF            113Fz5hVGiVr7wmjuQM1Dd6Hi8SwChpKWs    0.01000121 BTC
19xaXry2jSLYR768Z5hR7jfTXMzchYqD1t
1CG4c5D7UwhZWJZQgf86KpGWqtx2mB5tEj
1CkBDiFhSUYcSobs1G5bGhDXAm1KxuiLd9
1LHWxgqUdA2u5ZaSiJmNSWKhTiFQo7oHdw
1BEAveti8jAVVAJDYfgh7T47n879vJEZUv
1Ee1HyGQjyQD1WqProo5i9FPNc4ZB9jXw
1HTm1XvASJ3SmKLNr6nx5Vaapozp9Z5QRF
1CLjYLDynZE7s5RYqDCHSVLbuVPwhwJdwW
143hS9PNta76aYuSoKUT8tWukRtVsh3tXm
1LKQcrJYAn1gKHebjV4cRphmRebLyJQcuD
14Y6FUotN8yDJPYHFi2S13G1MDw1MVJpnp
1J1Fi9AJh9A4woR6jXNNoyYdpxqHypPNhV
1MKwBZNQNvaQWGe9DyvAiYZbZGNhQ7VMqD
1CsAFBnz4iB6wXZSWKTFxcsfAYHwUXPgPw
157HzTTYRAZ5kNvAyVxZwdYKQvoxnrZ8xa
1CHWv1AATxhEw7p7bjoJauxApYCXBt2v9f
1CaX52cfWRqmRoUR9vvdr8wUbSBC8DEZBH
1B1isfZCDsKBuawdYQaScWFq654bQNA3Ai
1MSNhtkw1yL6FV5nCYp5EwxocdkFxtV6JH
1DgSVcz5cuvGp5QWUxUcK33Re2B5DKXmqe
193GGnsRD5fd8K1M9VycxfxV3FQSQMxRRR
1QGH6LfjSwQVWg8mqXdierGC1mwD14UbRF
1LcTkSzC9tsGYwXeGVZ6sPDg7eS8a6f2EN
1Q4ydfRwaHpngdxykT8ZLhmMXos8eexjEP
1M1ERkihKtD46gyGDZRj6RL41qo6yTEQtJ

                                                                                   1.51088287 BTC
```

Chainalysis can translate the digital asset wallet addresses into real identities, i.e. a 1.51088287 transfer of Bitcoin from Exchange 1 to Exchange 2:



Chainalysis’ core database maps these random characters on a blockchain – digital asset addresses– to real-world services and activities. This is how the blockchain can be used as an audit trail for monitoring current activity as well as historic activity. It should be noted that the extent of this audit trail is limited to identified wallets and digital assets held by custodians on behalf of their beneficial owners, which, most importantly includes digital asset exchanges and increasingly, banks and other fiduciaries.   Because the blockchain is permanent and immutable, investigators or consumers are able to see transactions in real-time or access them years later with confidence the records have not been altered. The same is not always the case with traditional fiat investigations and other asset types.

In part due to the ability to leverage the transparency of digital assets and blockchain analytics, law enforcement has been able to disrupt terrorist financing campaigns, dismantle child sexual abuse material websites, and seize the ill-gotten proceeds of darknet marketplace administrators and the Colonial Pipeline ransomware attackers.

Blockchain analysis tools like ours are also used by financial institutions and digital asset exchanges to ensure they are meeting their anti-money laundering requirements. These tools can detect and alert users to patterns of potential high-risk activity among their customers. Using these tools, businesses can identify whether their customers are attempting to transact with US Treasury Office of Foreign Assets Control ("OFAC") sanctioned individuals, entities, or jurisdictions, or cashing out funds generated from darknet markets, scams, fraud, and other forms of illicit activity.

Blockchain and investigative analyses can be used to determine ownership or control of additional addresses associated with sanctioned individuals or entities based on information OFAC has provided publicly. For example, if OFAC lists a digital asset address as an identifier associated with a particular individual, using blockchain analytics, we can identify other wallet addresses likely controlled by the same individual and label them so that our customers also identify them as belonging to the sanctioned individual. Likewise, additional assets such as tokens or forks of blockchains, associated with the addresses and entities identified by OFAC can be determined through blockchain analytics.

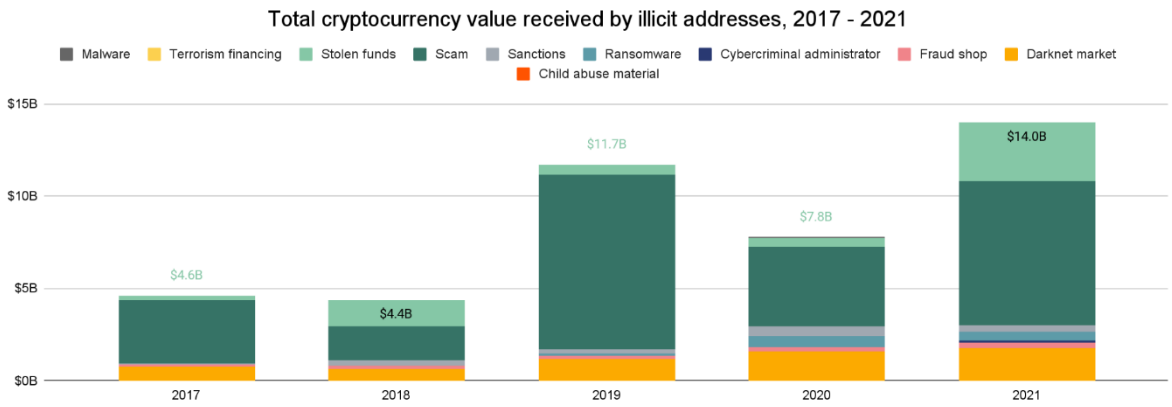
When OFAC lists digital asset addresses as identifiers associated with sanctioned entities, they are quickly labeled in our tools as sanctions-related and our customers receive alerts on historical or future exposure to these addresses. This means our technology enables digital asset exchanges and financial institutions to ensure that their customers are not interacting with addresses associated with sanctioned persons and identify and freeze any accounts that attempt to do so.

Blockchain analytics can also be used to identify trends and develop intelligence about who may be facilitating the evasion of sanctions or money laundering or other illicit activity. Using tools like the ones that Chainalysis develops, it's possible to map out illicit activity networks and patterns, something that would not be easily paralleled in traditional finance investigations. For example, by tracking their payments, our customers can identify virtual private network ("VPN") services, bulletproof web hosting services, and other providers sanctioned or malicious actors are using. All of this information is valuable intelligence that can allow investigators to determine new trends and patterns in sanctions evasion [and illicit finance] so that they can combat them.

Because of their inherent transparency and traceability, there are many advantages to digital assets when it comes to investigating sanctions evasion and illicit activity. Traditionally, bad actors have attempted to use misspellings, code words, and other techniques to evade sophisticated sanctions screening and anti-money laundering countermeasures. But with digital assets, the unforgeable addresses represent unavoidable, definitive evidence on a transparent record. Additionally, unlike some forensic evidence that degrades over time, blockchain evidence is permanent and immutable. What's more, our ability to analyze this evidence is only getting more sophisticated. Criminals who thought they evaded detection in months and years past often find they've left a permanent audit trail for law enforcement to follow.

An overview of illicit activity involving digital assets from our Crime Report

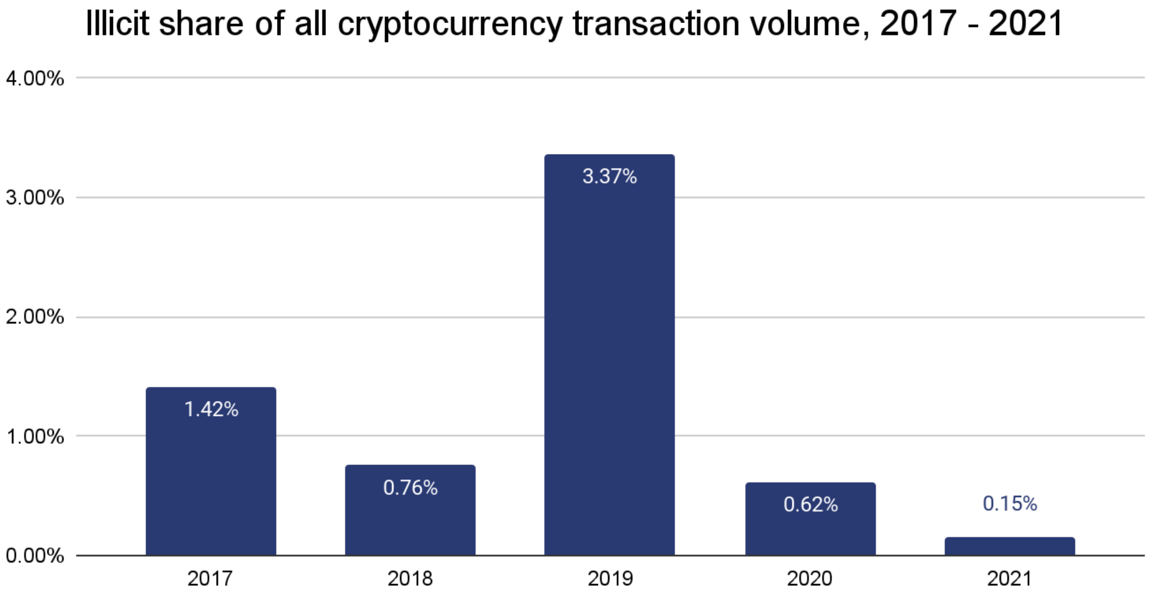
Digital asset-based crime hit a new all-time high in 2021, with illicit addresses receiving $14 billion over the course of the year, up from $7.8 billion in 2020. It is very important to note that these and below estimates of illicit activity are likely to rise as Chainalysis identifies more addresses associated with illicit activity and incorporates their transaction activity into our historical volumes. For instance, we found in our last Crypto Crime Report that 0.34% of 2020's digital asset transaction volume was associated with illicit activity — we can now revise that figure to 0.62%.



Note: "Cybercriminal administrator" refers to addresses that have been attributed to individuals connected to a cybercriminal organization, such as a Darknet market.

But those numbers don't tell the full story. Digital asset usage is growing faster than ever before. Across all digital assets tracked by Chainalysis, total transaction volume grew to $15.8 trillion in 2021, up 567% from 2020's totals. Given that roaring adoption, it's no surprise that more cybercriminals are using digital assets. But the fact that the increase was just 79% — nearly an order of magnitude lower than overall adoption — might be the biggest surprise of all.

In fact, with the growth of legitimate digital asset usage far outpacing the growth of criminal usage, illicit activity's share of digital asset transaction volume has never been lower.



Transactions involving illicit addresses represented just 0.15% of digital asset transaction volume in 2021 despite the raw value of illicit transaction volume reaching its highest level ever. The yearly trends suggest that with the exception of 2019 — an extreme outlier year for digital asset-based crime largely due to the PlusToken Ponzi scheme — crime is becoming a smaller and smaller part of the digital asset ecosystem.

The 0.15% of illicit transaction volume should be considered alongside illicit actors' digital asset holdings. It is impossible to know for sure, but we can estimate total illicit actor holdings based on the current holdings of addresses Chainalysis has identified as associated with illicit activity. As of early 2022, addresses believed to be associated with illicit actors held at least $10 billion worth of digital assets, with the vast majority of this held by wallets associated with digital asset theft. $10 billion is approximately 0.55% of the total digital asset market capitalization, which as of March 10, 2022, stood at $1.8 trillion.

We also need to note that these numbers only account for funds derived from "digital asset-native" crime, meaning cybercriminal activity such as darknet market sales or ransomware attacks in which profits are virtually always derived in digital assets rather than fiat currency. It's more difficult to measure how much fiat currency derived from offline crime — traditional drug trafficking, for example — is converted into digital assets to be laundered.

To put the 0.15% illicit activity volume number or 0.55% illicit actor digital asset holdings of total digital asset market capitalization in context, we note that the United Nations in 2020 estimated that money laundering activity accounted for $1.6 trillion per year or 2.7% of global GDP. According to one study, overall criminal activity imposes costs of about 3% of US GDP on the economy while another study published by an economist at the U.S. Bureau of Economic Analysis found that in 2017 crime in the US accounted for about 1.12% of US GDP.

Law enforcement investment in detection and disruption in the digital assets markets are, in my opinion, more likely to yield relatively better results per dollar invested than similar interventions in the broader economy. Compared to the non-digital asset economy, meaning anti-money laundering countermeasures (including *ex ante* measures like transaction monitoring controls or *ex post* measures like enforcement action and asset seizure) are generally more effective because a few key successes by law enforcement can disrupt a sizeable proportion of digital asset-related illicit activity, whereas an equivalent intervention in the non-digital asset economy is likely to yield less in terms of relative impact on reducing crime.

One promising development in the fight against digital asset-related crime is the growing ability of law enforcement to seize illicitly obtained digital assets. In November 2021, for instance, IRS Criminal Investigation announced that it had seized over $3.5 billion worth of digital assets in 2021 — all from non-tax investigations — representing 93% of all funds seized by the division during that time period or about 25% of illicit activity Chainalysis has identified to-date for 2021 (although the illicit activity underlying these seizures didn't necessarily occur in 2021). We've also seen several examples of successful seizures by other agencies, including $56 million seized by the Department of Justice in a digital asset scam investigation, $2.3 million seized from the ransomware group behind the Colonial Pipeline attack, and an undisclosed amount seized by Israel's National Bureau for Counter Terror Financing in a case related to terrorism financing.

For additional details of the different types of crimes that we see exploit the use of digital assets, please see the Appendix, where I outline the trends we see related to scamming, theft, malware, ransomware, terrorist financing, illicit activity with suspected links to North Korea, and illicit activity with suspected links to Iran, as well as present a case study of the Colonial Pipeline case.

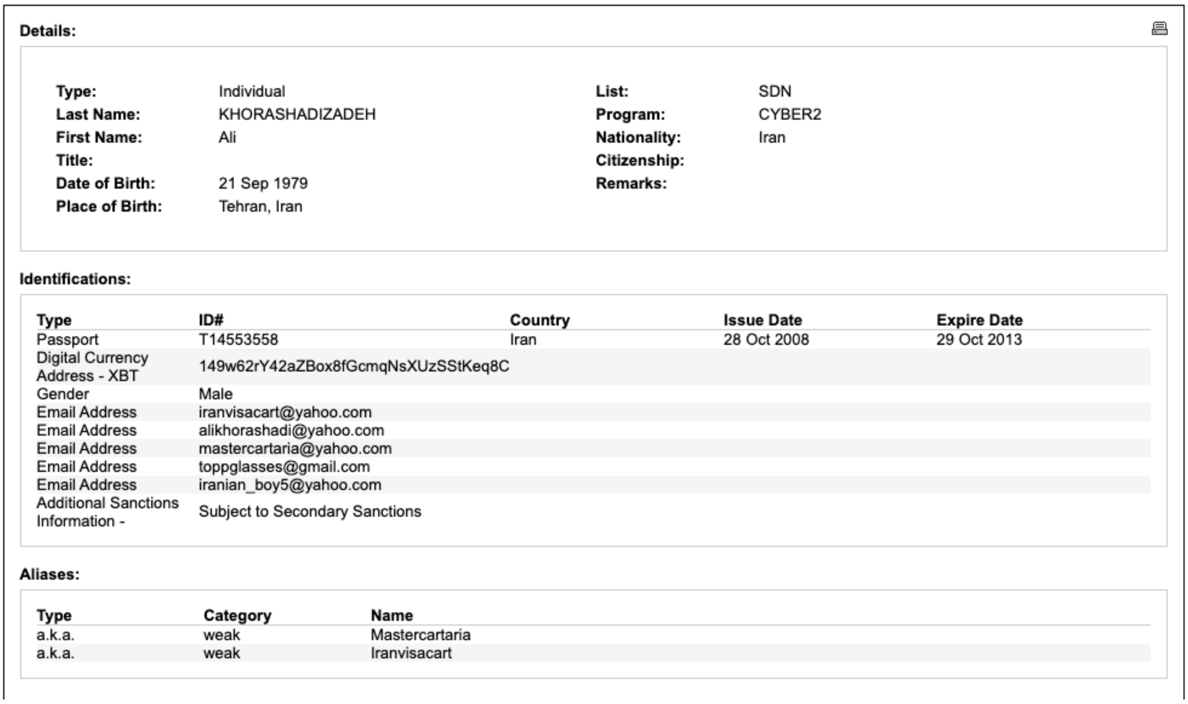
The risk of the use of digital assets by specially designated nationals and SDNs to evade US sanctions

Background regarding digital assets and sanctions

Since November 2018, OFAC has included 180 digital currency addresses in eight different designations. This has included designations against Chinese nationals for narcotics trafficking and money laundering, associates of the Democratic People's Republic of Korea ("DPRK") Lazarus Group, Russian nationals for their involvement in disinformation campaigns, and Russian cyber actors involved in digital asset exchange hacks. In April 2021, the Biden Administration announced several new sanctions against Russian intelligence service disinformation outlets and designated a Pakistani organization that provided cyber actors, including Russian disinformation actors, fraudulent identity documents used in the digital onboarding process at financial institutions.

On the SDN List, OFAC lists "Digital Currency Address" under sanctioned entities or individuals as identifiers as shown in the example below.

Example of OFAC "Digital Currency Address" Listing



Details:

Type:	Individual	**List:**	SDN
Last Name:	KHORASHADIZADEH	**Program:**	CYBER2
First Name:	Ali	**Nationality:**	Iran
Title:		**Citizenship:**	
Date of Birth:	21 Sep 1979	**Remarks:**	
Place of Birth:	Tehran, Iran		

Identifications:

Type	ID#	Country	Issue Date	Expire Date
Passport	T14553558	Iran	28 Oct 2008	29 Oct 2013
Digital Currency Address - XBT	149w62rY42aZBox8fGcmqNsXUzSStKeq8C			
Gender	Male			
Email Address	iranvisacart@yahoo.com			
Email Address	alikhorashadi@yahoo.com			
Email Address	mastercartaria@yahoo.com			
Email Address	toppglasses@gmail.com			
Email Address	iranian_boy5@yahoo.com			
Additional Sanctions Information -	Subject to Secondary Sanctions			

Aliases:

Type	Category	Name
a.k.a.	weak	Mastercartaria
a.k.a.	weak	Iranvisacart

OFAC has issued an "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" (in October 2020), as well as a brochure on Sanctions Compliance Guidance for the Virtual Currency Industry" (in October 2021). OFAC's advisory bolstered previous government guidance not to pay ransomware attackers, who typically demand ransom be paid in digital assets, as this incentivizes future attacks, and goes a step further in warning that ransomware victims and intermediaries and consultants who facilitate such payments could face heavy penalties associated with sanctions violations. It also noted that license applications made to OFAC that involve ransomware payments would be presumptively denied. The brochure outlined sanctions-related compliance requirements for digital asset businesses, consequences for non-compliance and examples of how timely reporting can mitigate those consequences, and best practices for building a risk-based compliance program.

On March 11, 2022 the White House announced that through new guidance, the Department of Treasury will continue to make clear that Treasury's expansive actions against Russia require all U.S. persons to comply with sanctions regulations regardless of whether a transaction is denominated in traditional fiat currency or virtual currency.

Under 2013 guidance from FinCEN, digital asset exchanges must register as money services businesses ("MSBs"). They therefore must meet certain anti-money laundering/countering the financing of terrorism (AML/CFT) requirements under the Bank Secrecy Act, including (i) establishing AML programs, (ii) adhering to certain regulatory reporting requirements, and (iii) maintaining certain books and records. This includes complying with sanctions regulations. This has led US-based digital asset exchanges to establish KYC programs to verify the identity of their customers and use transaction monitoring solutions to detect suspicious activity, making it more difficult for illicit actors or those trying to evade sanctions to cash out their ill-gotten digital assets for fiat currency.

Current Chainalysis assessment of Russian sanctions evasion risk using digital assets

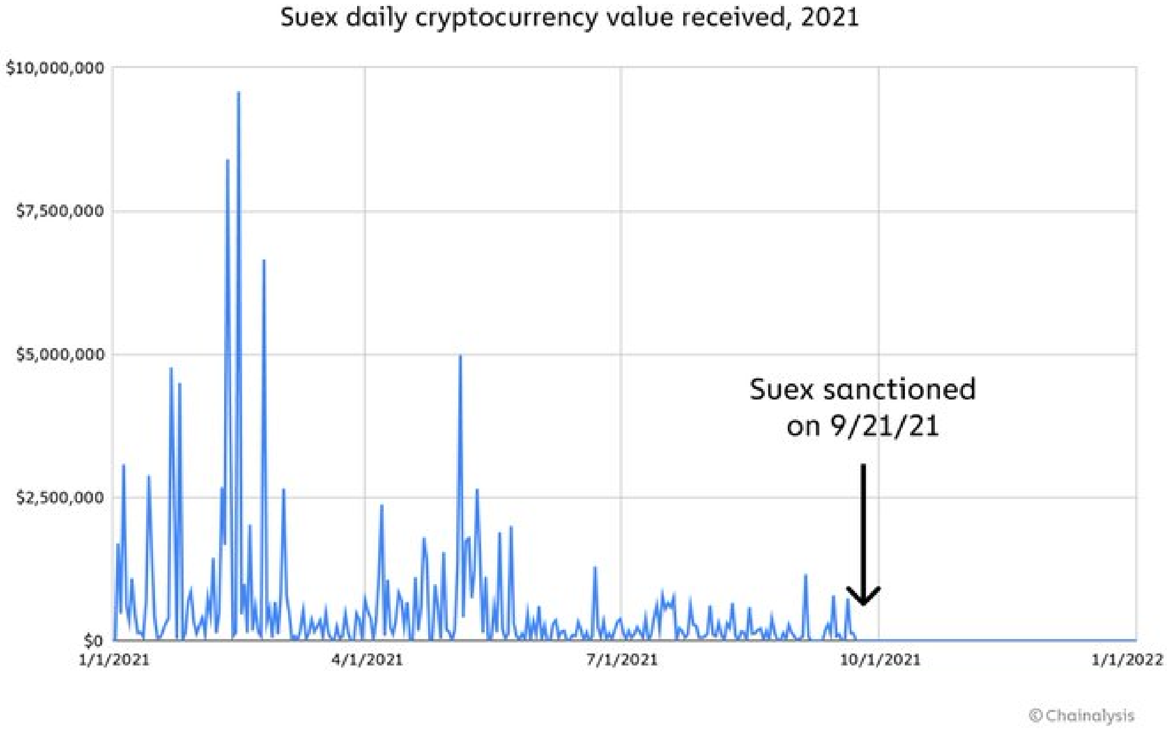
Our current assessment is that Russian SDNs are more likely to channel a greater portion of funds through traditional money laundering means, e.g., the "Russian laundromat" scheme, or through the use of alternative currencies and payment networks than through digital assets. Digital asset markets are a less useful tool for the sanctions evader relative to traditional financial systems for the following reasons:

- **High likelihood of detection:** Illicit activity, including sanctions evasion, is relatively easy to detect and monitor because of the immutable and transparent nature of blockchains. The ability to detect illicit activity is enhanced further through the use of blockchain analysis tools like those Chainalysis develops. In contrast, traditional financial networks require reconciliation, often conducted manually, of different ledgers of record across different institutions in different jurisdictions with different regulators, e.g., bank account or transfer records, customs records, etc. Moreover, investigation of financial activity through bank or payment records is generally historical while investigation of blockchain activity can be conducted in real-time.

- **High likelihood of seizure:** Because digital asset payment flows are easier to trace with limited reliance on process to obtain records, e.g., subpoenas, and can be monitored in real-time, this makes them more likely to be seized before illicit actors can move them off of a blockchain. See discussion above regarding the Colonial Pipeline ransomware fund seizure or the seizure of funds with connections to the Silk Road darknet market.

- **Countermeasures are particularly effective:** On September 21, 2021, OFAC announced sanctions against SUEX, a digital asset exchange that facilitated transactions involving illicit proceeds from at least eight ransomware variants. According to OFAC, over 40% of SUEX's known transaction history was associated with illicit actors.

After SUEX's designation, inbound transfers of digital assets into SUEX dropped to effectively zero.



Compliant digital asset market participants have proven effective at stopping the flow of funds to SDNs with digital asset wallet addresses. Sanctions are particularly effective in disrupting financial intermediaries in a digital asset network because once such an intermediary is designated, funds associated with it can be broadly flagged to compliant participants in the network as very high risk not just to immediate counterparties, but counterparties downstream. For example, if SUEX transfers funds to Wallet A and Wallet A transfers to Wallet B and Wallet B to Exchange X in order for Wallet B to cash-out, using a tool like Chainalysis, Exchange X will be able to trace the source of funds to SUEX, an SDN, and therefore block the transfer. Sanctions are therefore very effective at disrupting liquidity flowing through digital asset SDN intermediaries.

In contrast, source of funds would be more easily obscured in the traditional financial system. For example, if a bank intermediary is sanctioned (Bank A) and it transfers funds to Company B (which could be a shell company) who transfers to Company C who then transfers to Bank X, Bank X is less likely to trace source of funds through to Bank A and therefore facilitate Bank A's sanctions evasion, reducing the efficacy of sanctions as a foreign policy tool. At minimum, it would be slower and more costly for Bank X to determine source of funds for Company C in a traditional financial system relative to an equivalent financial intermediary in a blockchain system.

While the disruption of funds to wallet addresses included on sanctions lists is effective at disruption reception and transmission of funds for SDN digital asset intermediaries, traditional bank SDNs generally continue receiving and transmitting funds. One can therefore imagine that in a blockchain-based financial system, sanctions could be a more effective, less leaky, foreign policy tool for protecting US national security versus the current system.

Chainalysis' recommendations for how Congress and regulators can act to better detect, disrupt, and deter illicit uses of digital assets, including sanctions evasion

Below we provide some short-term recommendations aimed specifically at reducing the risk of sanctions evasion via digital assets and longer-term recommendations aimed at improving detection, disruption and deterrence of broader illicit uses of digital assets.

Short-term recommendations

- **Include digital asset wallets in designations when available.** Sanctions authorities should continue to work together and in cooperation with regulated institutions, as well as blockchain intelligence companies like Chainalysis, to identify links between SDNs and digital asset wallet addresses. As described above, the inclusion of wallet addresses as identifiers has been very effective at shutting off flows related to those wallets because compliance teams are readily able to screen for these addresses and freeze funds.

- **Consider designating specific services that facilitate sanctions evasion.** In the event that digital asset services such as exchanges and mixers are facilitating an unacceptable amount of sanctions evasion (something that could be transparently and quickly determined using blockchain intelligence as described above), OFAC may consider sanctioning the entities that facilitate sanctions evasion, just as they did with the designations of SUEX and Chatex.

- **Expand information sharing.** Information sharing is fundamental to the US government's ability to respond to the risks of illicit cyber activity to operate with better awareness of the threat landscape and should be expanded wherever possible.

Long-term recommendations

- **Congressional appropriations that fund blockchain intelligence capabilities.** We commend the Consolidated Appropriations Act for FY 2022 for increasing funding for FinCEN and the Office of Terrorism and Financial Intelligence ("TFI") in the Department of Treasury. We recommend that FinCEN and TFI, along with law enforcement, market regulators, and national security agency stakeholders, invest in blockchain intelligence and analytics capabilities, both headcount and tools/services, that will enhance their ability to detect, disrupt, and deter illicit uses of digital assets.

- **In addition to blockchain intelligence technology, Congress should ensure adequate funding, resources, and training for government agencies charged with investigating the illicit use of digital assets, including sanctions evasion**. Many government agencies have limited or inconsistent personnel dedicated to investigating the illicit use of digital assets because of a lack of training resources and a lack of funding for new personnel, tools, and training. Ensuring that these efforts are well-funded would ensure that when digital assets are exploited by criminals, investigators can trace these illicit transactions, seize funds, and bring criminals to justice.

- **Improve and promote interagency coordination through the creation of a Virtual Asset Coordination Center.** A coordination center would allow USG agencies to leverage existing capabilities across agencies, reduce duplication of efforts, and ensure that agencies are learning from each other, engaging in best practices, and sharing information through a shared real-time view on the illicit use of digital assets.

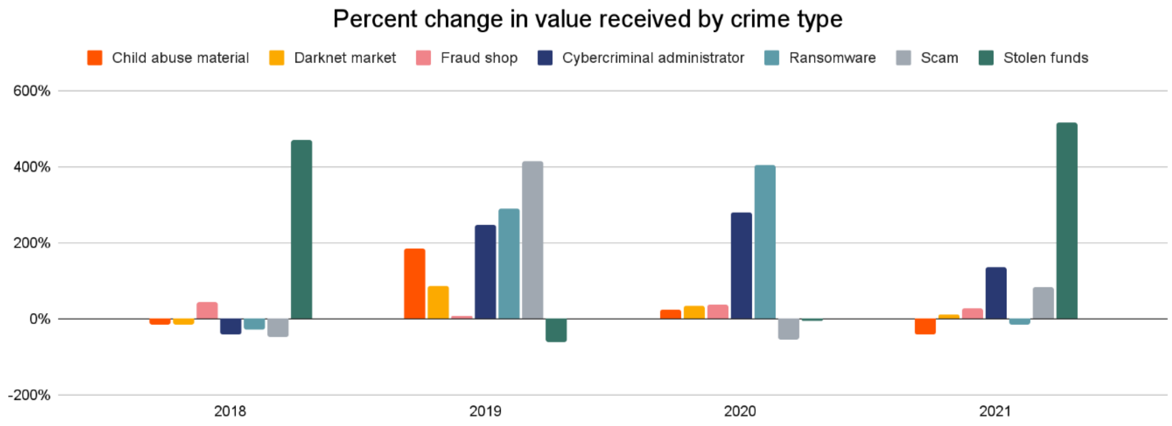
- **Provide market regulators with clear oversight authority over financial digital assets.** We recommend that jurisdictional authorities over financial (e.g., commodities and securities) digital assets be clearly allocated among the current leading market regulators, i.e. the Commodity Futures Trading Commission ("CFTC") and Securities and Exchange Commission ("SEC"), to provide the digital asset industry with legal clarity and statutory directives that provide these agencies with guidance and powers to police financial digital assets markets in a manner that reflects the unique risks and opportunities of the technology, e.g., as it relates to promoting investor protection, cybersecurity, market surveillance, and conflicts of interest, among other things. National security will be furthered by empowering the front-line market regulators to have a clear regulatory perimeter, reinforcing the capabilities of the broader government, including law enforcement.

The opportunity for policymakers, including this Committee, is to ensure that they understand and are balancing the benefits of this technology with the commitment to public and investor protection, as well as our need to retain the United States' dominance when it comes to providing the financial rails that everyone transacts with in a manner that not only protects our national security but *enhances* it. I look forward to working with you all in the future as you consider policies and legislation in this space.

APPENDIX A
Overview of 2022 Crime Report

In this Appendix, we will look at different categories of crime that exploit digital assets. More specifically, below we describe data relating to the extent of (1) scamming, (2) theft, (3) ransomware, (4) a case study of the Colonial Pipeline ransomware case, illicit activity with suspected links to (5) North Korea, (6) Iran, and (7) Russia, (8) terrorist financing, and (9) malware.

Based on our data, we can break down types of digital asset-based crime by transaction volume and analyze trends over time. Two categories stand out for their growth: stolen funds and, to a lesser degree, scams. DeFi is a big part of the story for both.



1. Scamming

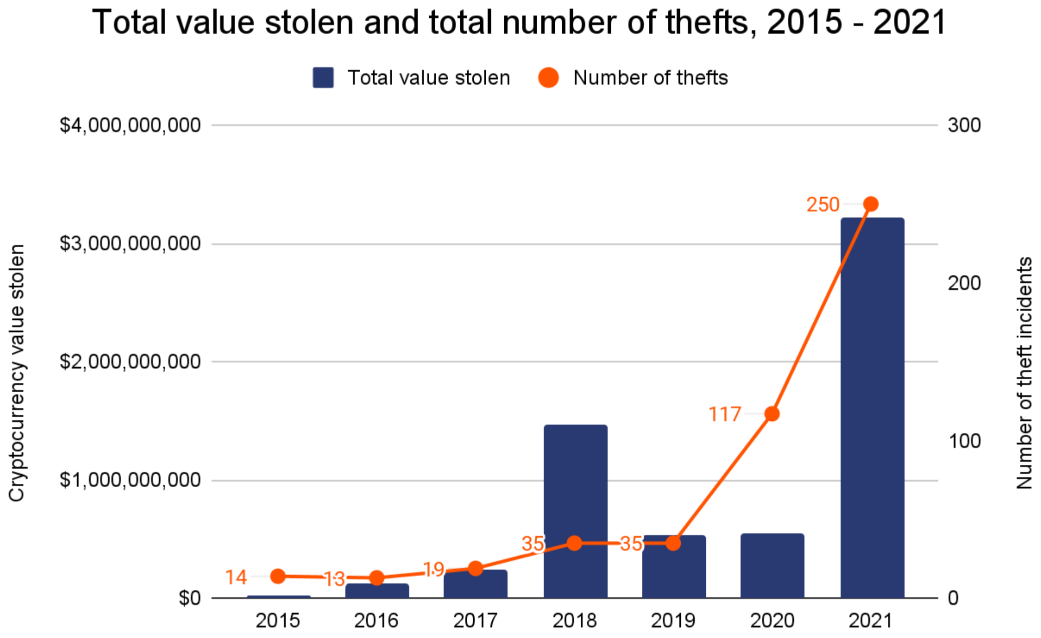
Scamming revenue rose 82% in 2021 to $7.8 billion worth of digital assets stolen from victims. Over $2.8 billion of this total — which is nearly equal to the increase over 2020's total — came from rug pulls, a relatively new scam type in which developers build what appear to be legitimate digital asset projects before taking investors' money and disappearing. Please keep in mind as well that these figures for rug pull losses represent only the value of investors' funds that were stolen, and not losses from the DeFi tokens' subsequent loss of value following a rugpull.

We should note that roughly 90% of the total value lost to rug pulls in 2021 can be attributed to one fraudulent centralized exchange, Thodex, whose CEO disappeared soon after the exchange halted users' ability to withdraw funds. However, every other rug pull tracked by Chainalysis in 2021 involved DeFi projects. In nearly all of these cases, developers have tricked investors into purchasing tokens associated with a DeFi project before draining the funds provided by those investors, sending the token's value to zero in the process.

We believe rug pulls are common in DeFi for two related reasons. One is the excitement around DeFi. DeFi transaction volume has grown 912% in 2021, and the incredible returns on decentralized tokens like Shiba Inu have many excited to speculate on DeFi tokens. At the same time, it's very easy for those with the right technical skills to create new DeFi tokens and get them listed on exchanges, even without a code audit. A code audit is a process by which a third-party firm or listing exchange analyzes the code of the smart contract behind a new token or other DeFi project, and publicly confirms that the contract's governance rules are ironclad and contain no mechanisms that would allow for the developers to make off with investors' funds. Many investors could likely have avoided losing funds to rug pulls if they'd stuck to DeFi projects that have undergone a code audit – or if DEXes required code audits before listing tokens.

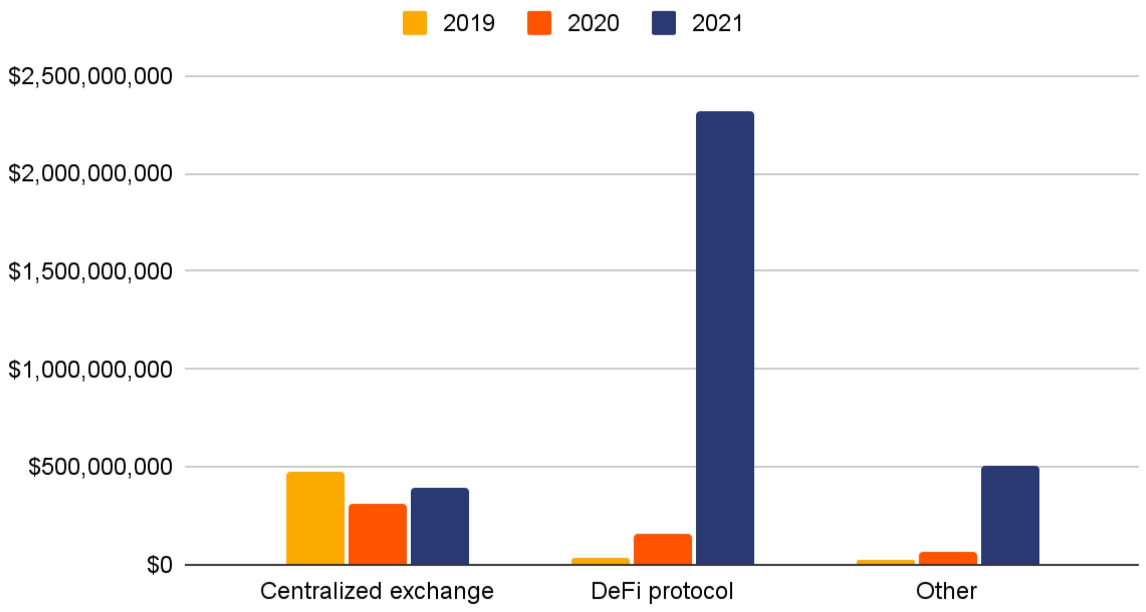
2. Theft

2021 was a big year for digital thieves. Throughout the year, $3.2 billion in digital assets were stolen from individuals and services — almost 6x the amount stolen in 2020.



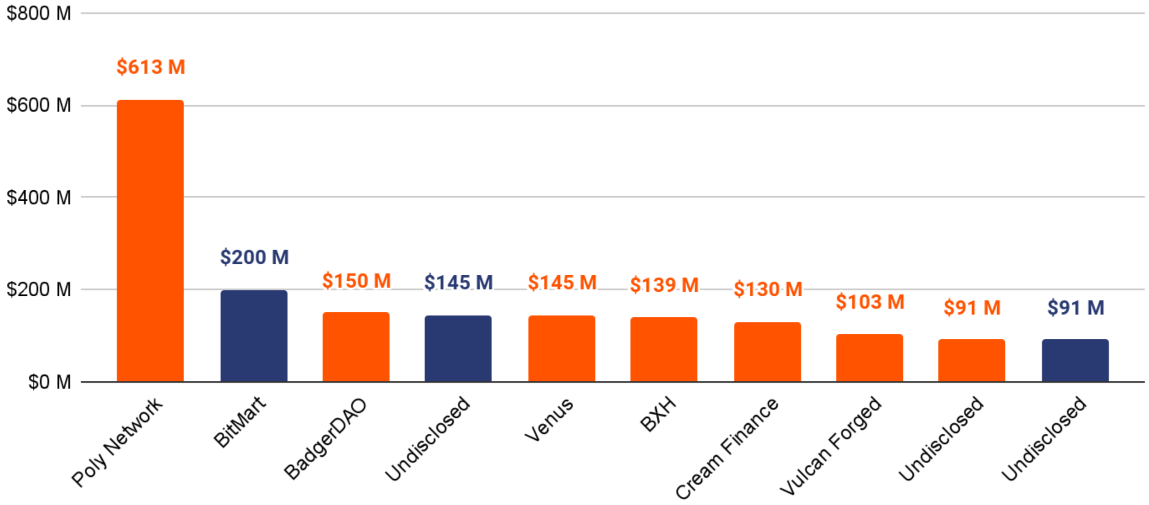
Digital asset theft grew disproportionately in 2021, with roughly $3.2 billion worth of digital assets stolen in 2021 — a 516% increase compared to 2020. Roughly $2.2 billion of those funds — 72% of the 2021 total — were stolen from DeFi protocols. The increase in DeFi-related thefts represents the acceleration of a trend we identified in last year's Crime Report.

Annual total cryptocurrency stolen by victim type, 2019 - 2021



Top ten cryptocurrency theft incidents by amount stolen, 2021

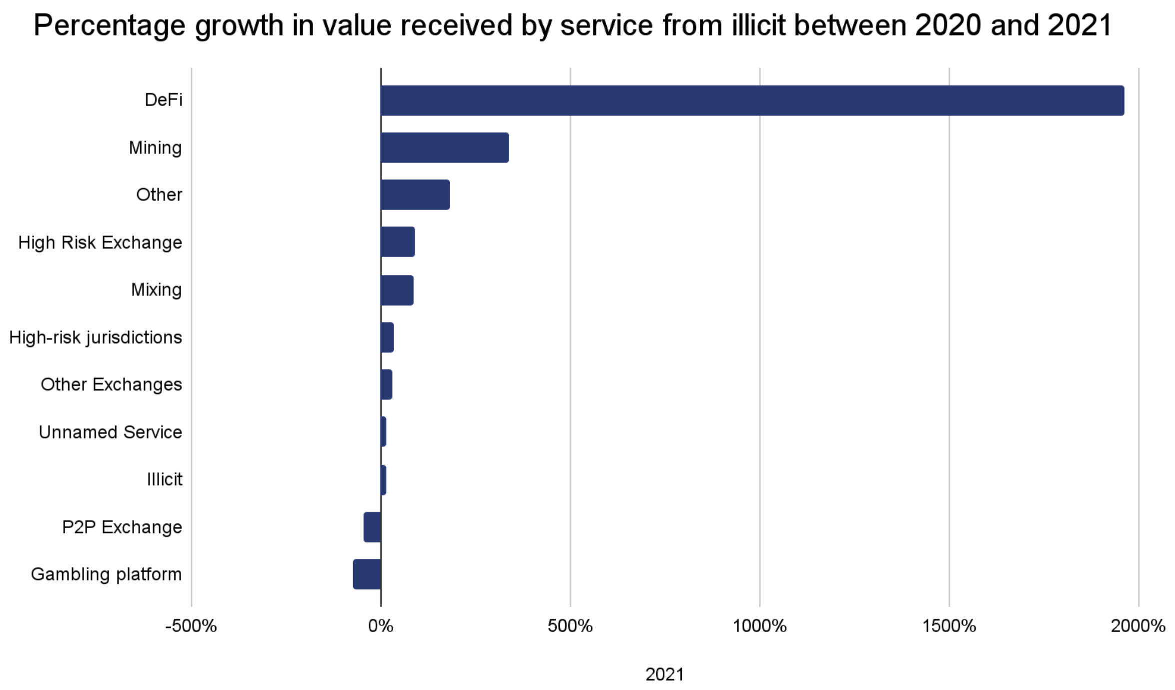
Orange = DeFi protocol. Blue = Centralized exchange



As is the case most years, the ten largest hacks of 2021 accounted for a majority of the funds stolen at $1.81 billion. Seven of these ten attacks targeted DeFi platforms in particular.

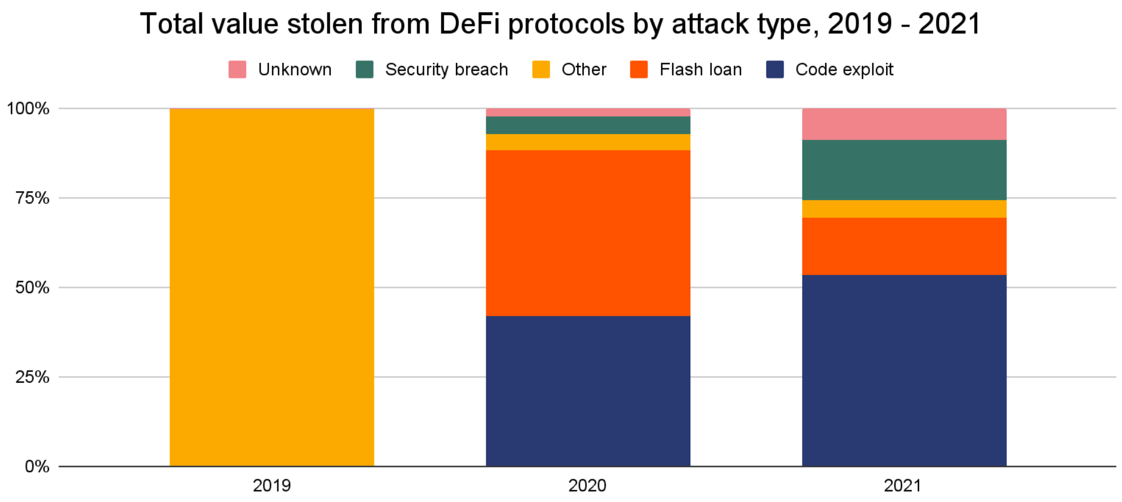
In 2020, just under $162 million worth of digital assets was stolen from DeFi platforms, which was 31% of the year's total amount stolen. That alone represented a 335% increase over the total stolen from DeFi platforms in 2019. In 2021, that figure rose another 1,330%. In other words, as DeFi has continued to grow, so too has its issue with stolen funds. Most instances of theft from DeFi protocols can be traced back to errors in the smart contract code governing those protocols, which hackers exploit to steal funds, similar to the errors that allow rug pulls to occur.

We've also seen significant growth in the usage of DeFi protocols for laundering illicit funds, a practice we saw scattered examples of in 2020 and that became more prevalent in 2021. The graph below looks at the growth in illicit funds received by different types of services in 2021 compared to 2020.



DeFi protocols saw the most growth by far in usage for money laundering at 1,964%.

With the increased prominence of smart contract capabilities that power DeFi platforms, deeper vulnerabilities have begun to emerge around the software underpinning these services. In 2021, code exploits and flash loan attacks—a type of exploit involving price manipulation—accounted for a near-majority of total value stolen across all services at 49.8%. And when examining only hacks on DeFi platforms, that figure increases to 69.3%.



These exploits occur for a variety of reasons. For one, in keeping with DeFi's faith in decentralization and transparency, open-source development is a staple of DeFi applications. This is an important and broadly positive trend: since DeFi protocols move funds without human intervention, users need to be able to audit the underlying code in order to trust the platform. But this also stands to benefit cybercriminals, who can analyze the scripts for vulnerabilities and plan exploits in advance.

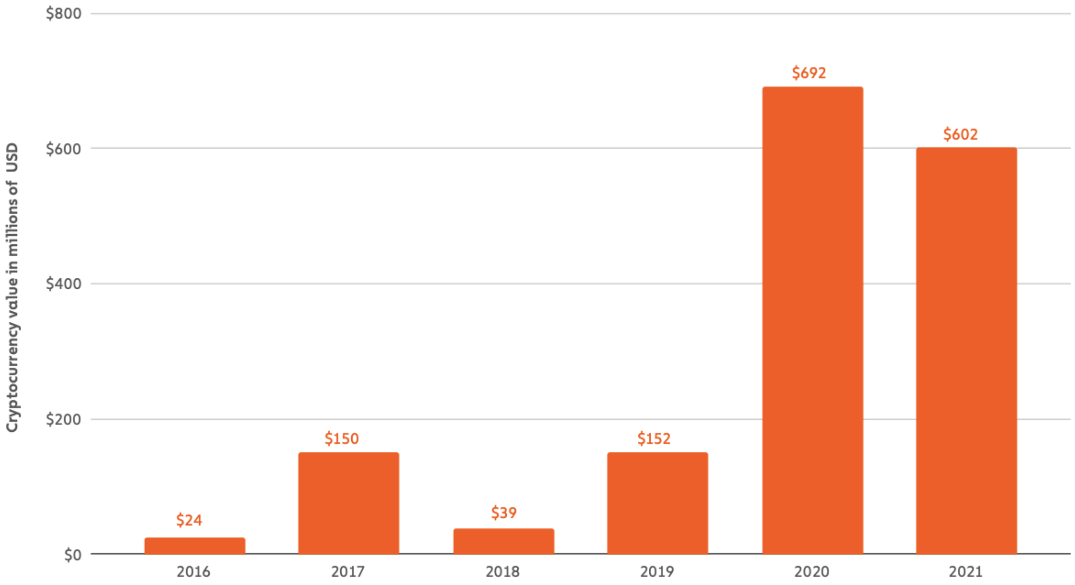
Another potential point of failure is DeFi platforms' reliance on price oracles. Price oracles are tasked with maintaining accurate asset pricing data for all digital assets on a platform, and the job isn't easy. Secure but slow oracles are vulnerable to arbitrage; fast but insecure oracles are vulnerable to price manipulation. The latter type often leads to flash loan attacks, which extracted a massive $364 million from DeFi platforms in 2021. In the hack of Cream Finance, for example, a series of flash loans exploiting a vulnerability in the way Cream calculated yUSD's "pricePerShare" variable enabled attackers to inflate yUSD price to double its true value, sell their shares, and make off with $130 million in just one night.

3. Ransomware

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files. Usually ransomware attackers gain access to victims' systems through some form of fraud, phishing for passwords in particular, or when a victim unknowingly visits an infected website that then results in malware being downloaded and installed without the user's knowledge.

Ransomware attackers often extort digital assets from their victims in return for access to their systems. These demands for digital assets include the ransomware attacker's wallet address that Chainalysis is then able to track.

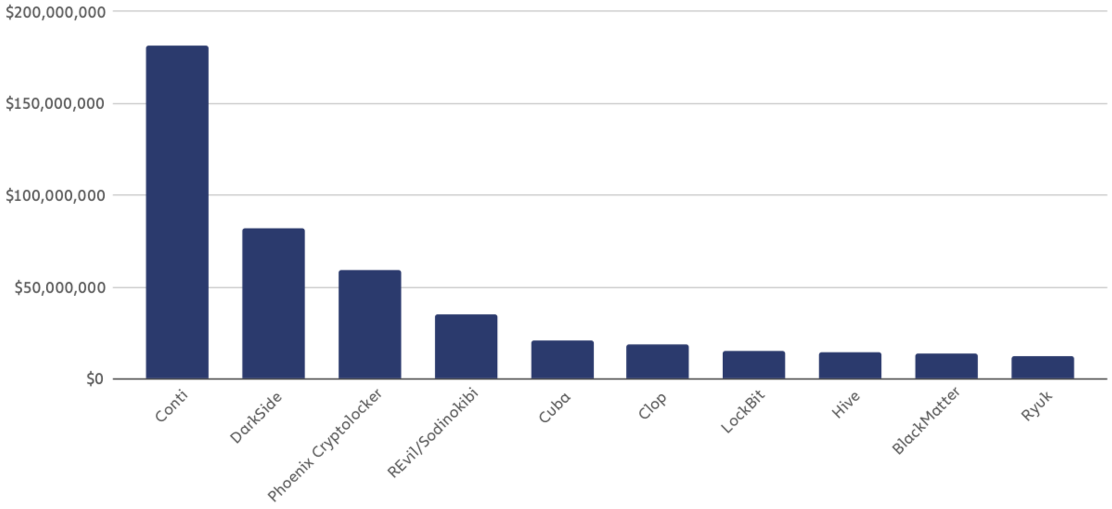
Total cryptocurrency value received by ransomware addresses | 2016–2021



As of March 14, 2022, we've identified just over $699 million worth of ransomware payments in 2021. However, just like last year, we know that this figure will likely increase as we record new ransomware recipient wallet addresses. The data we published in the 2022 Crime Report on February 16 had $602 million in 2021 ransomware payments.

Conti was the biggest ransomware strain by revenue in 2021, extorting at least $200 million from victims.

Top 10 ransomware strains by revenue | 2021



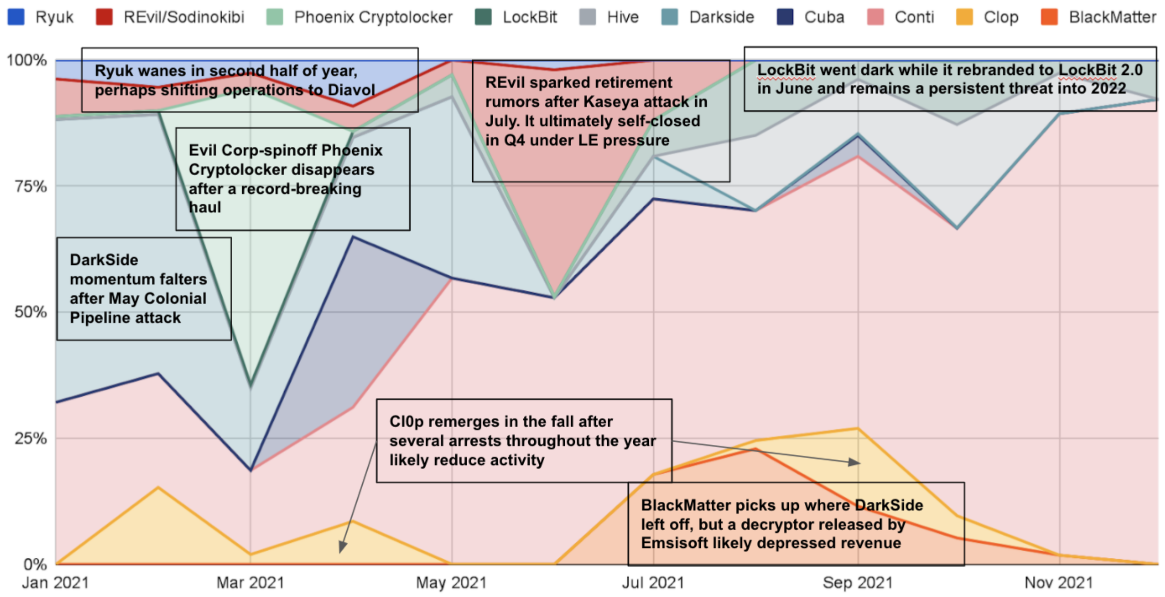
Believed to be based in Russia, Conti operates using the ransomware-as-a-service (RaaS) model, meaning Conti's operators allow affiliates to launch attacks using its ransomware program in exchange for a fee.

DarkSide is also notable, both for ranking second in 2021 in funds extorted from victims that we've been able to identify, and also for its role in the attack on oil pipeline Colonial Pipeline, one of the year's most notable ransomware attacks. The attack caused fuel shortages in some areas, which were exacerbated by subsequent panic buying as word of the attack's impact spread. The Colonial story serves as an important reminder of one reason ransomware attacks are so dangerous: They frequently target critical infrastructure we need to keep the country running — not just energy providers, but food providers, schools, hospitals and financial services companies as well.

However, as I discussed earlier in my testimony, the Colonial Pipeline attack also turned into a success story, as the U.S. Department of Justice was able to track and seize $2.3 million of the ransom that Colonial paid to DarkSide. Law enforcement's growing ability to seize payments after they're made represents a huge step forward in the fight against ransomware. It also serves as one more reason why more victims should report attacks — even if you pay, law enforcement may be able to help you get those funds back.

Overall, 2021 also saw more active individual ransomware strains than any other year.At least 140 ransomware strains received payments from victims at any point in 2021, compared to 119 in 2020, and 79 in 2019. Those numbers are emblematic of the intense growth of ransomware we've seen over the last two years. Most ransomware strains come and go in waves, staying active for a short amount of time before becoming dormant. We show this on the graph below, which shows how the top ten ransomware strains ebbed and flowed in activity throughout the year.

Top 10 most active strains in 2021 by monthly revenue



Ryuk wanes in second half of year, perhaps shifting operations to Diavol

Evil Corp-spinoff Phoenix Cryptolocker disappears after a record-breaking haul

DarkSide momentum falters after May Colonial Pipeline attack

REvil sparked retirement rumors after Kaseya attack in July. It ultimately self-closed in Q4 under LE pressure

LockBit went dark while it rebranded to LockBit 2.0 in June and remains a persistent threat into 2022

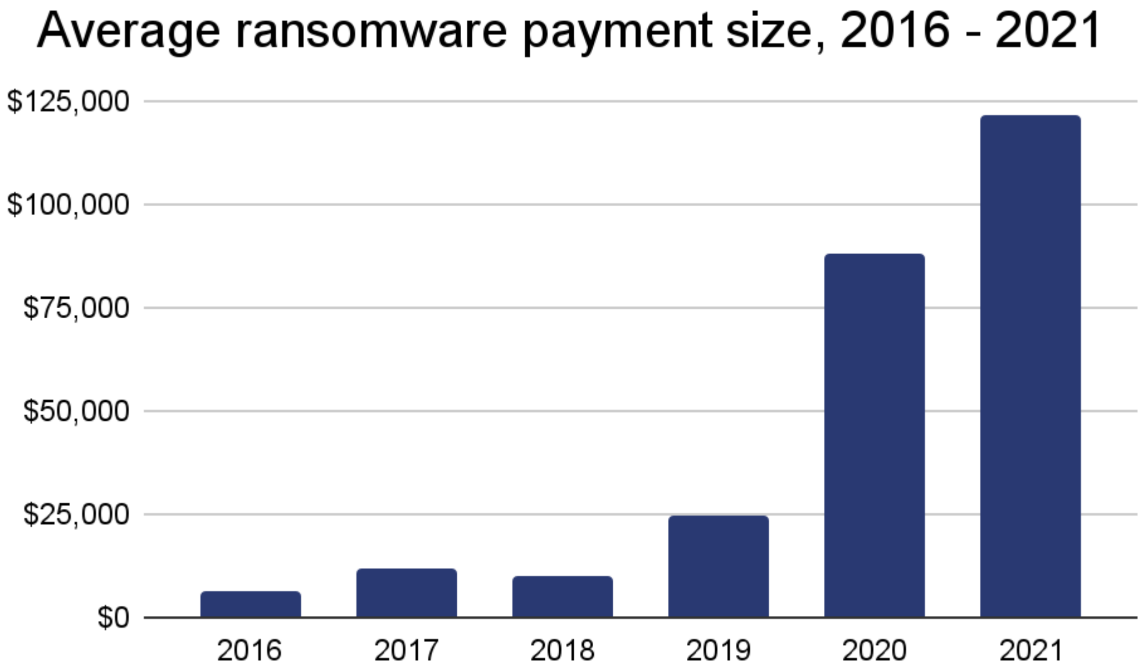
Cl0p remerges in the fall after several arrests throughout the year likely reduce activity

BlackMatter picks up where DarkSide left off, but a decryptor released by Emsisoft likely depressed revenue

Conti was the one strain that remained consistently active for all of 2021, and in fact saw its share of all ransomware revenue grow throughout the year. Overall though, Conti's staying power is increasingly outside the norm.

The growing number of active strains and generally short lifespan of most strains is also a result of rebranding efforts. More and more in 2021, we saw the operators of strains publicly "shut down" before re-launching under a new name, presenting themselves as a separate cybercriminal group. Often, the rebranded strain's financial footprint on the blockchain aligns with that of the original, which can tip investigators off as to who's really behind the new strain.

Ransomware payment sizes also continued to grow in 2021, a trend we've observed every year since 2018.



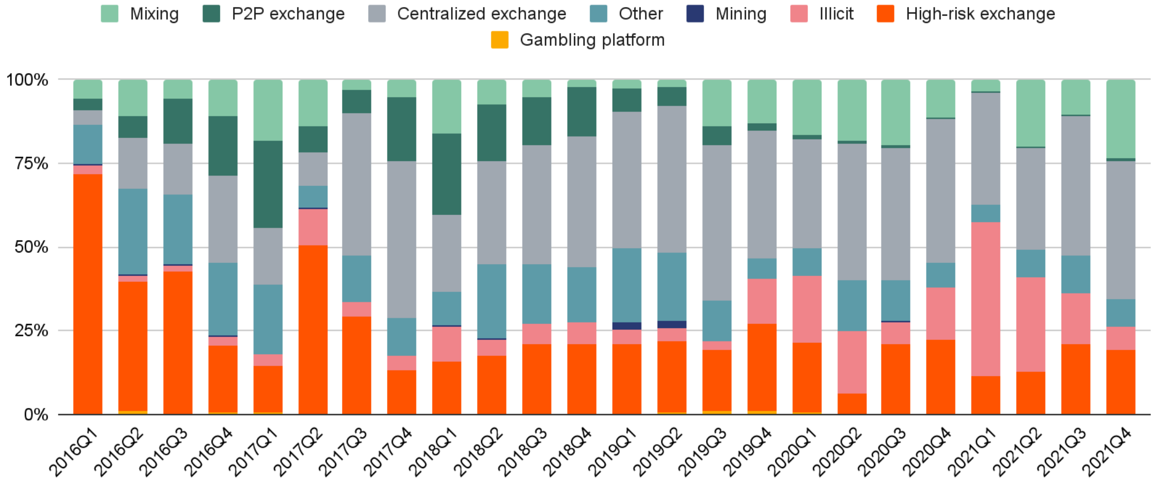
The average ransomware payment size was over $118,000 in 2021, up from $88,000 in 2020 and $25,000 in 2019. Large payments such as the record $40 million received by Phoenix Cryptolocker spurred this all-time high in average payment size. One reason for the increase in ransom sizes is ransomware attackers' focus on carrying out highly-targeted attacks against large organizations. This "big game hunting" strategy is enabled in part by ransomware attackers' usage of tools provided by third-party providers to make their attacks more effective. These tools range from illicit hacking aids to legitimate products, and include:

- Rented infrastructure such as bulletproof web hosting, domain registration services, botnets, proxy services, and email services to carry out attacks.
- Hacking tools like network access to already-infiltrated networks, exploit kits that scan victims' networks for vulnerabilities, and malware programs that help attackers distribute ransomware more effectively.
- Stolen data such as passwords, individuals' personally identifiable information, and compromised remote desktop protocol (RDP) credentials, which help attackers break into victims' computer networks.

Usage of these services by ransomware operators spiked to its highest ever levels in 2021.

Another important trend to monitor in ransomware is money laundering. The graph below shows where attackers move the digital asset they extort from victims.

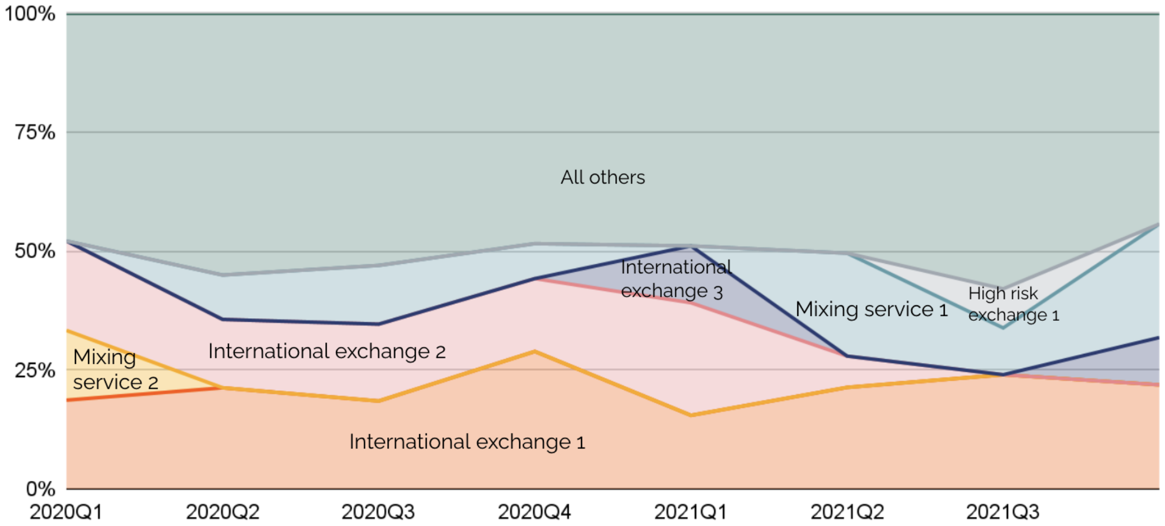
Destination of funds leaving ransomware wallets, 2016 - 2021



Over the last few years, most ransomware strains have laundered their stolen funds by sending them to centralized exchanges. We also see substantial funds sent to both mixers and addresses associated with other forms of illicit activity.

The money laundering trends get even more interesting if we drill down to the individual services receiving funds from ransomware.

Services receiving funds from ransomware addresses, 2020 - 2021



Amazingly, 56% of funds sent from ransomware addresses since 2020 have wound up at one of six digital asset businesses:

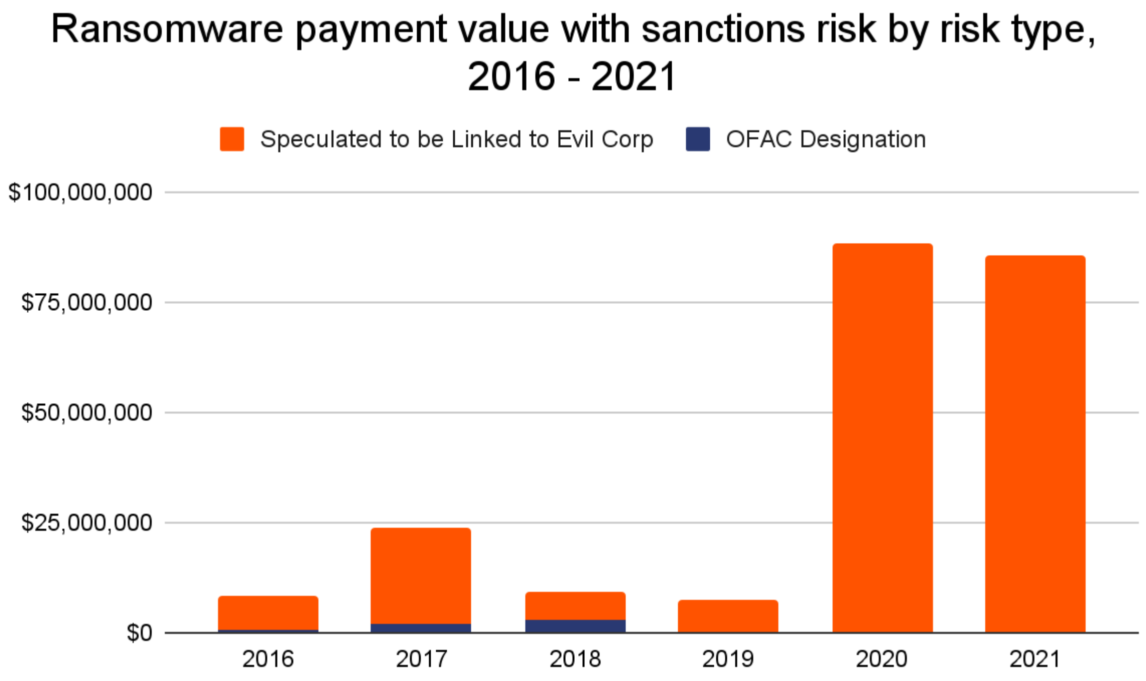
- Three large, international exchanges
- One high-risk exchange based in Russia
- Two mixing services

Similar to the rebranding activity we described above, these money laundering trends show how small the ransomware ecosystem really is. That's good news, as it means the strategy for fighting ransomware is likely simpler than it appears at first glance. By cracking down on the small number of services that facilitate this money laundering activity, law enforcement can significantly reduce attackers' options for cashing out, reducing the financial incentive to carry out ransomware attacks and hampering ransomware organizations' ability to operate.

Most ransomware attacks appear to be financially motivated. However, others appear to be motivated by geopolitical goals, and seem more geared toward deception, espionage, reputational damage and disruption of the enemy government's operations.

In cases where a ransomware strain contains no mechanism to collect payment or allow victims to recover their files, we can be more certain that money isn't the attackers' primary motivation. And that's exactly what we saw in a recent ransomware attack on Ukrainian government agencies by hackers believed to be associated with the Russian government.

Some ransomware payments carry with them sanctions risk for the victim. Virtually all ransomware payments with sanctions risk was due to payments to ransomware strains thought to be associated with Evil Corp, a cybercriminal organization whose leadership reportedly has ties to the Russian government.

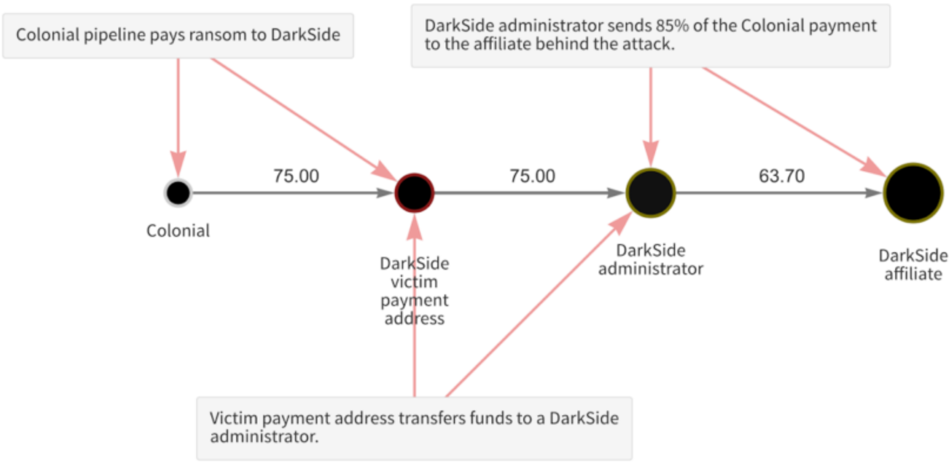


4. *Colonial Pipeline case study*

On May 7, 2021, Colonial Pipeline, an oil pipeline company that supplies energy to the southeastern United States, fell victim to a ransomware attack, forcing it to temporarily cease operations. Within hours of the attack, Colonial paid a ransom of 75 Bitcoin — worth roughly $4.4 million at the time — to DarkSide, the Russia-based cybercriminal group responsible for the attack. Six days later, Colonial was able to resume operations, but during that time, the shutdown combined with panic buying as the news spread resulted in fuel shortages in several areas.

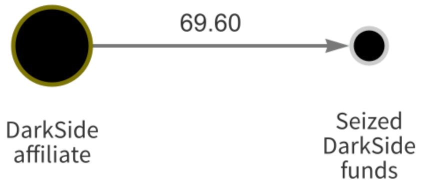
One month later, the Department of Justice announced that it had managed to seize $2.3 million worth of Bitcoin from Colonial's ransom payment following an FBI investigation. Chainalysis' tools aided the FBI.

Below is a chart describing the ransom payment itself and the initial movement of funds using Chainalysis Reactor, our blockchain forensics product.


Colonial pipeline pays ransom to DarkSide
DarkSide administrator sends 85% of the Colonial payment to the affiliate behind the attack.
75.00
75.00
63.70
Colonial
DarkSide victim payment address
DarkSide administrator
DarkSide affiliate
Victim payment address transfers funds to a DarkSide administrator.

First, on the left, we see the initial payment of 75 Bitcoin from Colonial to the address provided by the attackers. Soon after, that address transferred the funds to an address controlled by DarkSide's administrators, who then sent 63.7 Bitcoin — 85% of Colonial's payment — to the affiliate who controlled the attack. That point is key — DarkSide operates on the Ransomware as a Service ("RaaS") model, meaning the affiliates who carry out the attack effectively "rent" usage of DarkSide's technology from the core group of administrators who created and manage the ransomware strain itself. Administrators take a small cut of the payment from each successful attack in return, as we see above.

After tracking the funds to the affiliate's address, FBI investigators were able to seize the funds on May 28, 2021.



The Colonial Pipeline seizure represents a huge step forward in the fight against ransomware, and especially ransomware strains that attack our critical infrastructure. We continue to monitor the movement of funds using our tools so that we can provide helpful insight to authorities as they investigate further and, hopefully, seize the remainder of the funds.

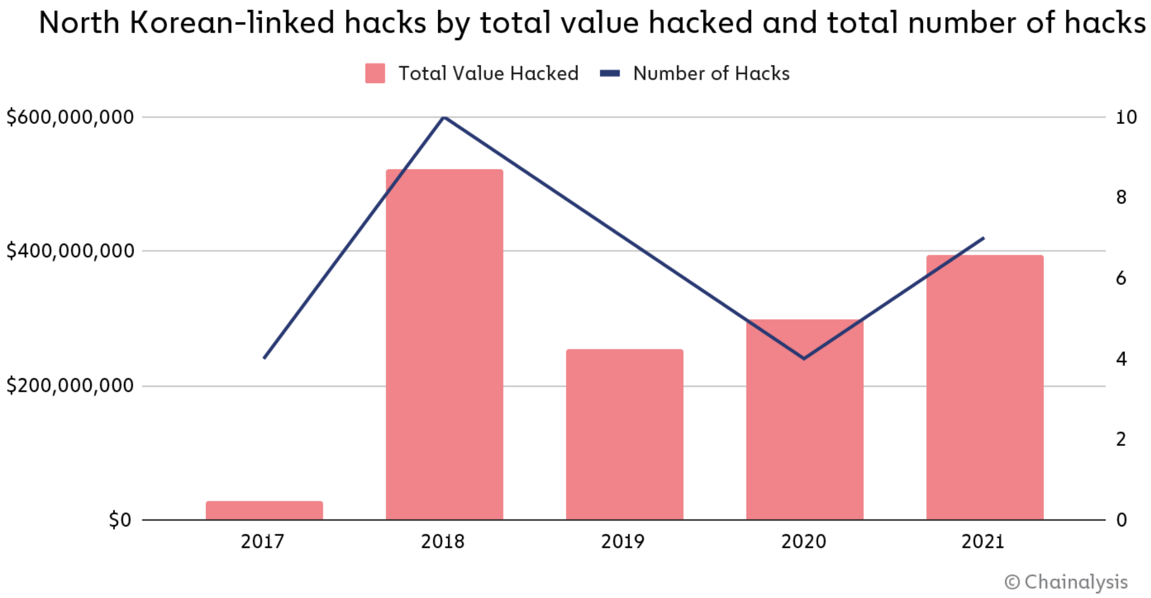
5. Illicit activity with suspected links to North Korea

North Korean cybercriminals launched at least seven attacks on digital asset platforms that extracted nearly $400 million worth of digital assets last year. These attacks targeted primarily investment firms and centralized exchanges, and made use of phishing lures, code exploits, malware, and advanced social engineering to siphon funds out of these organizations' internet-connected “hot” wallets into DPRK-controlled addresses. Once North Korea gained custody of the funds, they began a careful laundering process to cover up and cash out.

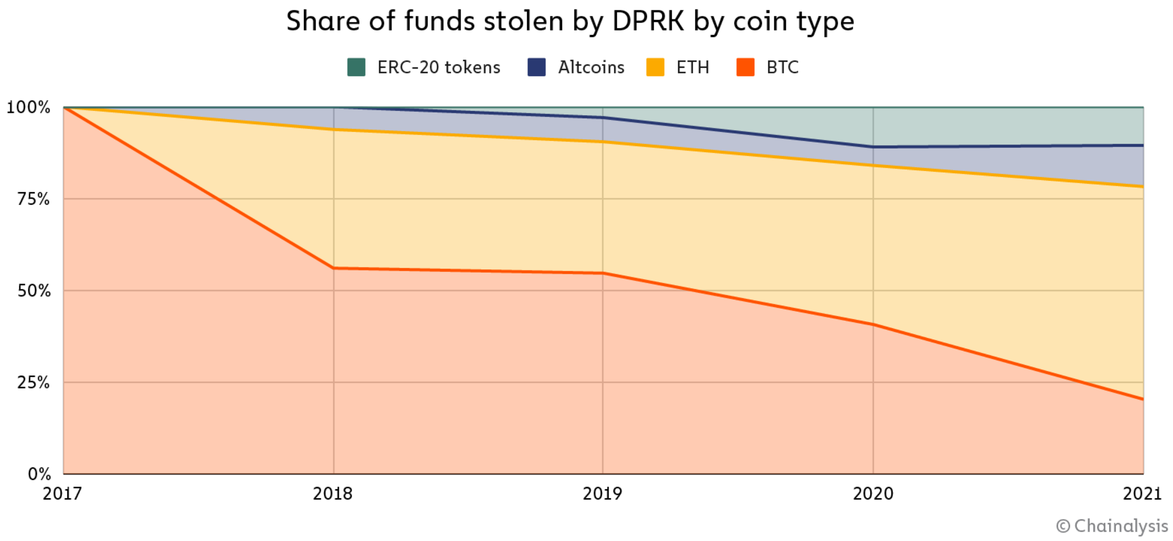
These complex tactics and techniques have led many security researchers to characterize cyber actors for the DPRK is especially true for APT 38, also known as “Lazarus Group,” which is led by DPRK’s primary intelligence agency, the US- and UN-sanctioned Reconnaissance General Bureau. While we will refer to the attackers as North Korean-linked hackers more generally, many of these attacks were carried out by the Lazarus Group in particular.

Lazarus Group first gained notoriety from its Sony Pictures and WannaCry cyberattacks, but it has since concentrated its efforts on digital asset crime—a strategy that has proven immensely profitable. From 2018 on, the group has stolen and laundered massive sums of virtual currencies every year, typically in excess of $200 million. The most successful individual hacks, one on KuCoin and another on an unnamed digital asset exchange, each netted more than $250 million alone. And according to the UN security council, the revenue generated from these hacks goes to support North Korea’s WMD and ballistic missile programs.

In 2021, North Korean hacking activity was on the rise once again. From 2020 to 2021, the number of North Korean-linked hacks jumped from four to seven, and the value extracted from these hacks grew by 40%.



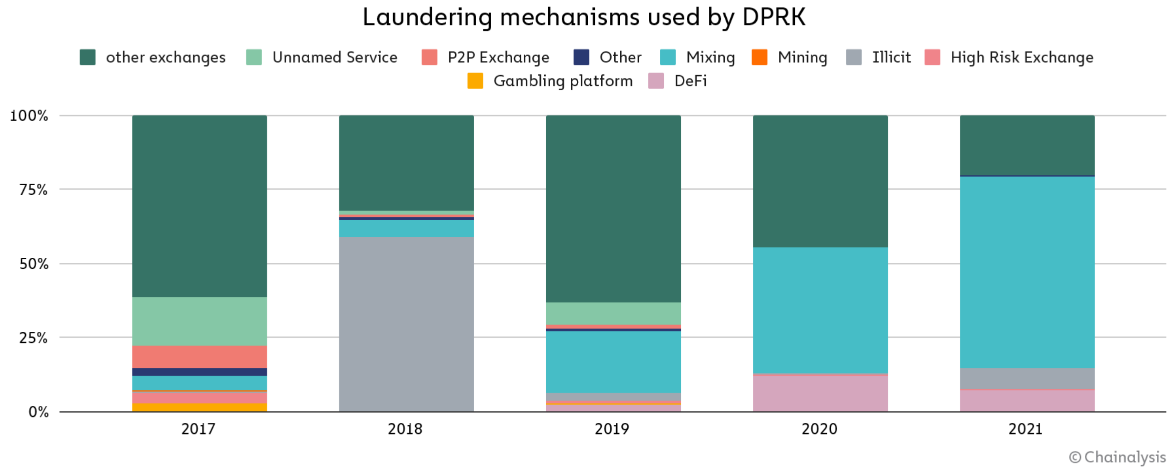
Interestingly, in terms of dollar value, Bitcoin now accounts for less than one fourth of the digital assets stolen by DPRK. In 2021, only 20% of the stolen funds were Bitcoin, whereas 22% were either ERC-20 tokens or altcoins. And for the first time ever, Ether accounted for a majority of the funds stolen at 58%.



The growing variety of digital assets stolen has necessarily increased the complexity of DPRK's digital asset laundering operation. Today, DPRK's typical laundering process is as follows:

6. ERC-20 tokens and altcoins are swapped for Ether via decentralized exchange (DEX)
7. Ether is mixed
8. Mixed Ether is swapped for Bitcoin via DEX
9. Bitcoin is mixed
10. Mixed Bitcoin is consolidated into new wallets
11. Bitcoin is sent to deposit addresses at crypto-to-fiat exchanges based in Asia —potential cash-out points

In fact, we observed a massive increase in the use of mixers among DPRK-linked actors in 2021.



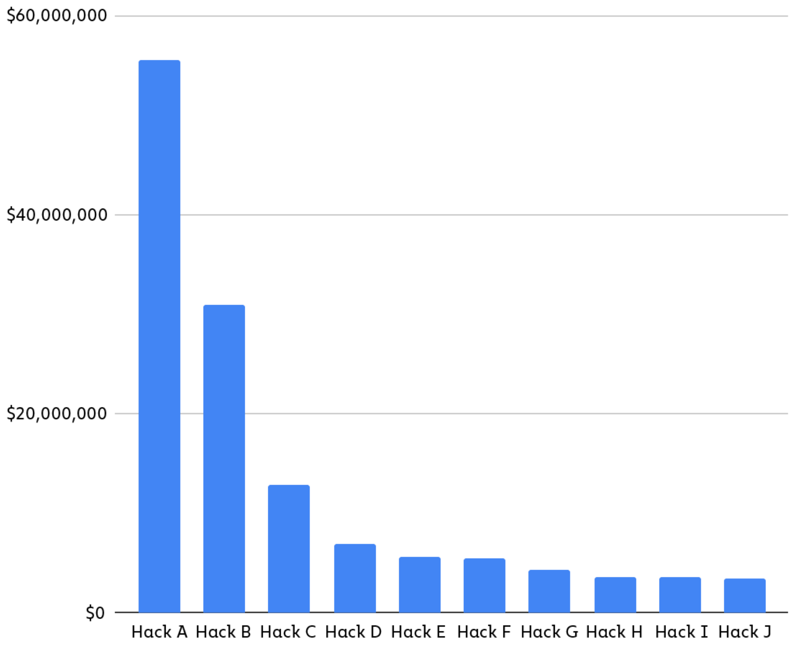
More than 65% of DPRK's stolen funds were laundered through mixers this year, up from 42% in 2020 and 21% in 2019, suggesting that these threat actors have taken a more cautious approach with each passing year.

Why mixers? DPRK is a systematic money launderer, and their use of multiple mixers —software tools that pool and scramble digital assets from thousands of addresses—is a calculated attempt to obscure the origins of their ill-gotten digital assets while offramping into fiat.

Why DeFi? DeFi platforms like DEXs provide liquidity for a wide range of ERC-20 tokens and altcoins that may not otherwise be convertible into cash. When DPRK swaps these coins for ETH or BTC they become much more liquid, and a larger variety of mixers and exchanges become usable. What's more, DeFi platforms don't take custody of user funds and many do not collect know-your-customer ("KYC")) information, meaning that cybercriminals can use these platforms without having their assets frozen or their identities exposed.

Chainalysis has identified $170 million in current balances—representing the stolen funds of 49 separate hacks spanning from 2017 to 2021—that are controlled by North Korea but have yet to be laundered through services. The ten largest balances by dollar value are listed below.

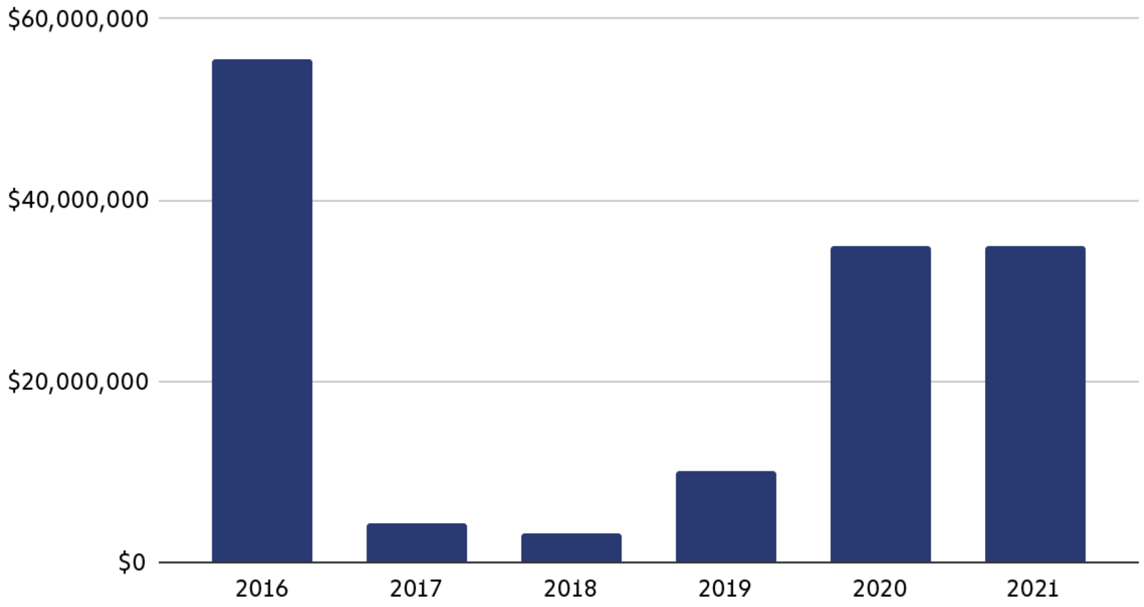
North Korea's largest unlaundered cryptocurrency holdings by hack



© Chainalysis

Of DPRK's total holdings, roughly $35 million came from attacks in 2020 and 2021. By contrast, more than $55 million came from attacks carried out in 2016—meaning that DPRK has massive unlaundered balances as much as six years old.

Total balances held by North Korean actors by date of attack



© Chainalysis

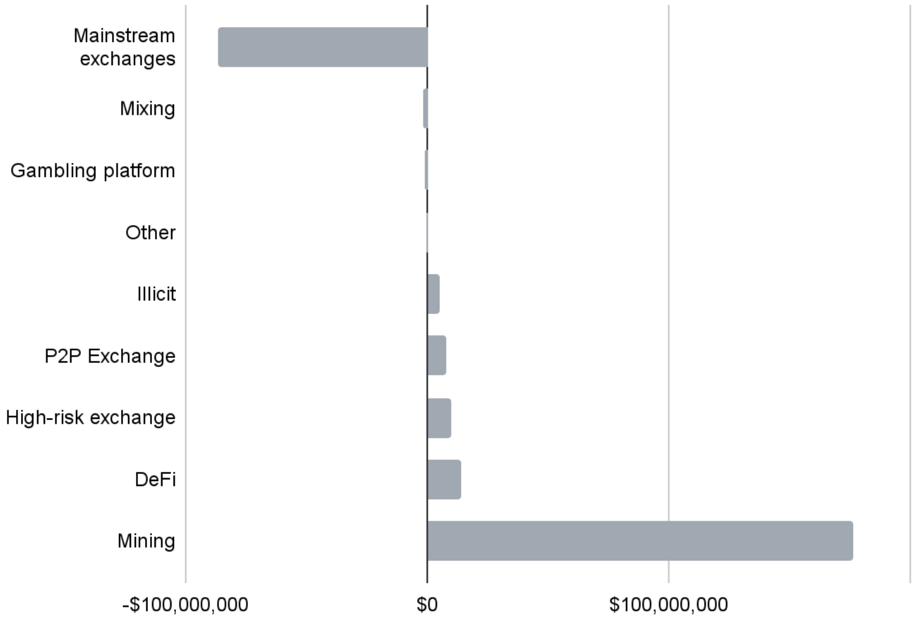
This suggests that DPRK-linked hackers aren't always quick to move stolen digital assets through the laundering process. It's unclear why the hackers would still be sitting on these funds, but it could be that they are hoping law enforcement interest in the cases will die down, so they can cash out without being watched.

6. Illicit activity with suspected links to Iran

Iran faces some of the most extensive U.S. sanctions of any country. Per the United States Treasury's Office of Foreign Assets Control (OFAC), U.S. businesses and individuals are effectively banned from transacting with Iranian businesses, including its biggest financial institutions and central bank. Some in the Iranian government have called for the country to use digital assets to circumvent these sanctions, and Bitcoin mining may provide the perfect opportunity to do so. As one of the world's largest energy producers, Iran has the low-cost electricity needed to mine digital assets like Bitcoin cheaply, providing an injection of monetary value that sanctions can't stop.

Our research indicates Iranian Bitcoin mining is well underway at a surprisingly large scale. From 2015 to 2021, we found that Bitcoin mining funneled more than $186 million into Iranian services, most of it within the past year.

Net flows to and from Iranian services, 2015 - 2021



Iranian state actors are well aware of the opportunity. In 2019, the Iranian government created a licensing regime for digital asset mining. And in March of this year, a think tank tied to the President's office released a report stressing its benefits.

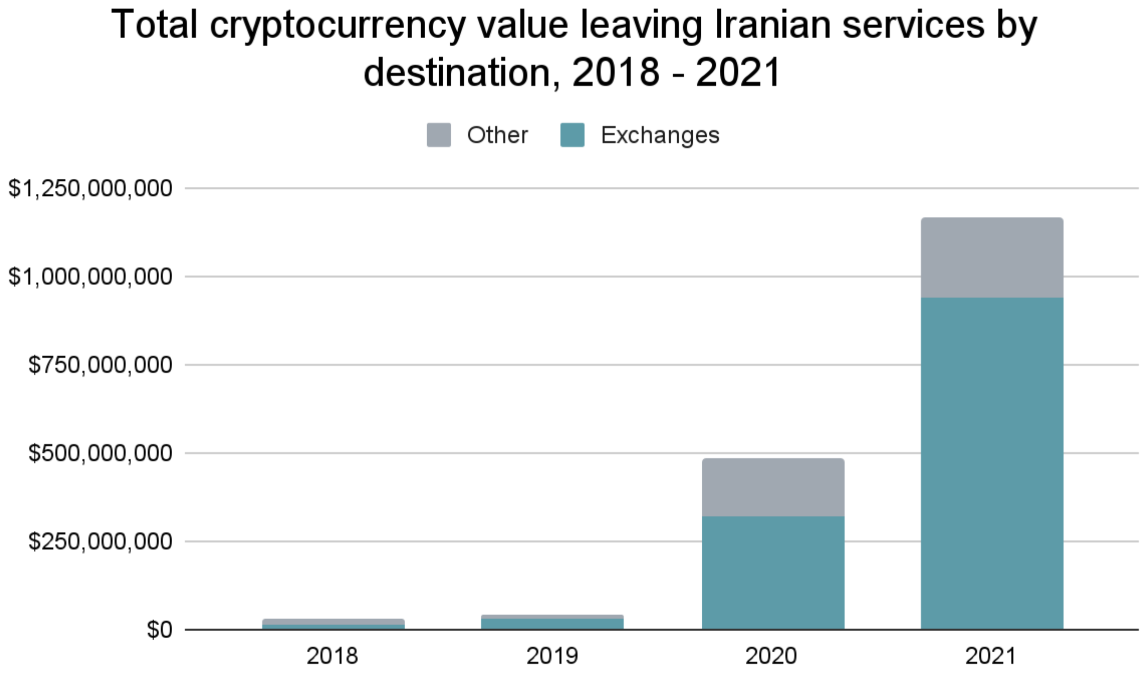
But the costs have extended beyond just electricity. The Iranian government has had to ban Bitcoin mining twice this year due to frequent blackouts, many of which Iran's state power agency has blamed on unlicensed Bitcoin mining. And unlicensed Bitcoin miners, for their part, allegedly account for "some 85%" of all activity in the country, per the Iranian president.

It has also opened up a new avenue of risk for digital asset businesses. U.S. businesses could face penalties or even criminal prosecution if found in violation of OFAC sanctions, which prohibit U.S. persons or companies from servicing financial accounts belonging to

Iranian persons or companies. That being said, businesses can monitor for exposure to Iranian miners to reduce this risk considerably.

It's also important to note that a nexus to sanctions is more attenuated at the transaction/mining fee level. If a U.S. business were to engage in a transaction and the fees paid from said transaction were received by an Iranian miner, the payer and payee would have had no say in who could receive these fees—the receiver of which is determined automatically by Bitcoin's proof-of-work protocol. To date, sanctions risk appears most prominent when a U.S. business transacts directly with the miner themselves.

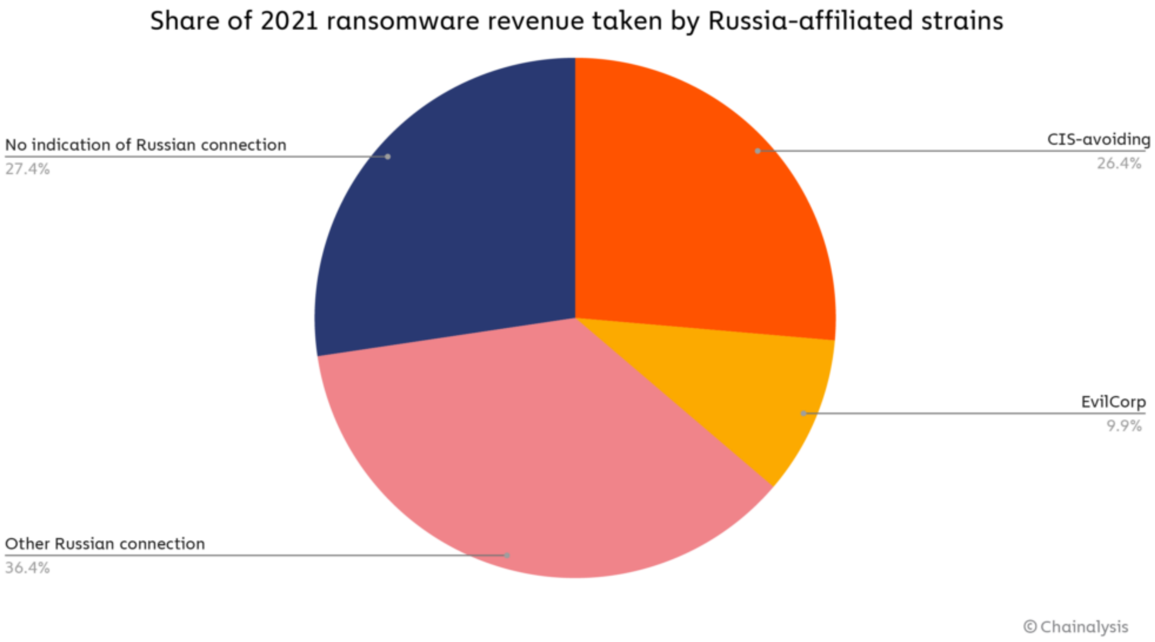
Many exchanges operating in jurisdictions without active sanctions, however, continue to provide financial services to Iranian businesses. In fact, in 2021, services outside of Iran received $1.16 billion from Iranian services—more than double the value received last year.



This transfer of funds from mining pools to Iranian services to services in the wider digital asset ecosystem is a corridor through which Iran evades sanctions.

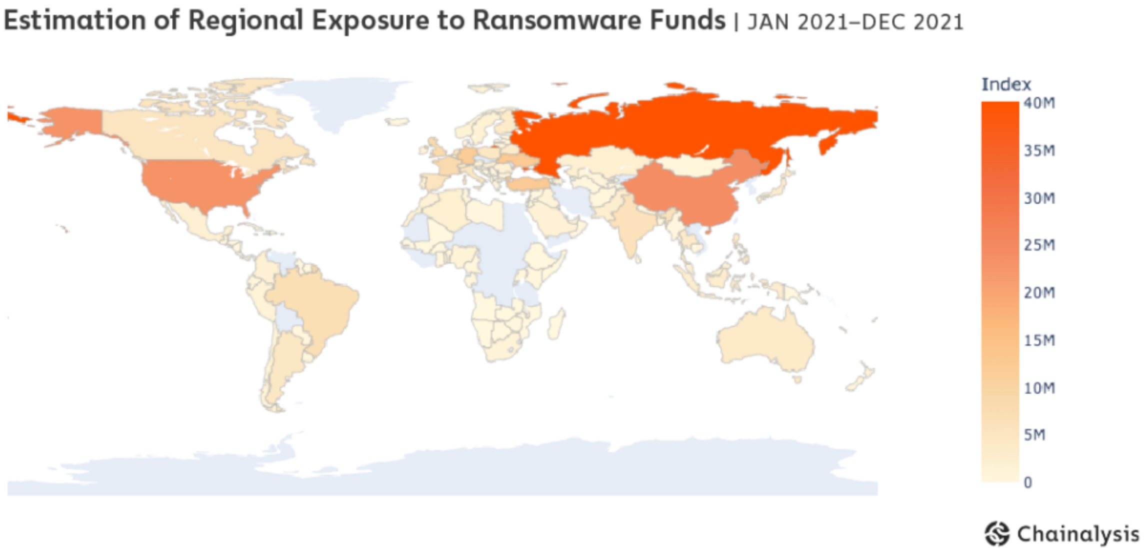
7. Illicit activity with suspected links to Russia

I show on the pie chart below the share of total ransomware revenue that went to strains affiliated with Russian organizations in 2021.



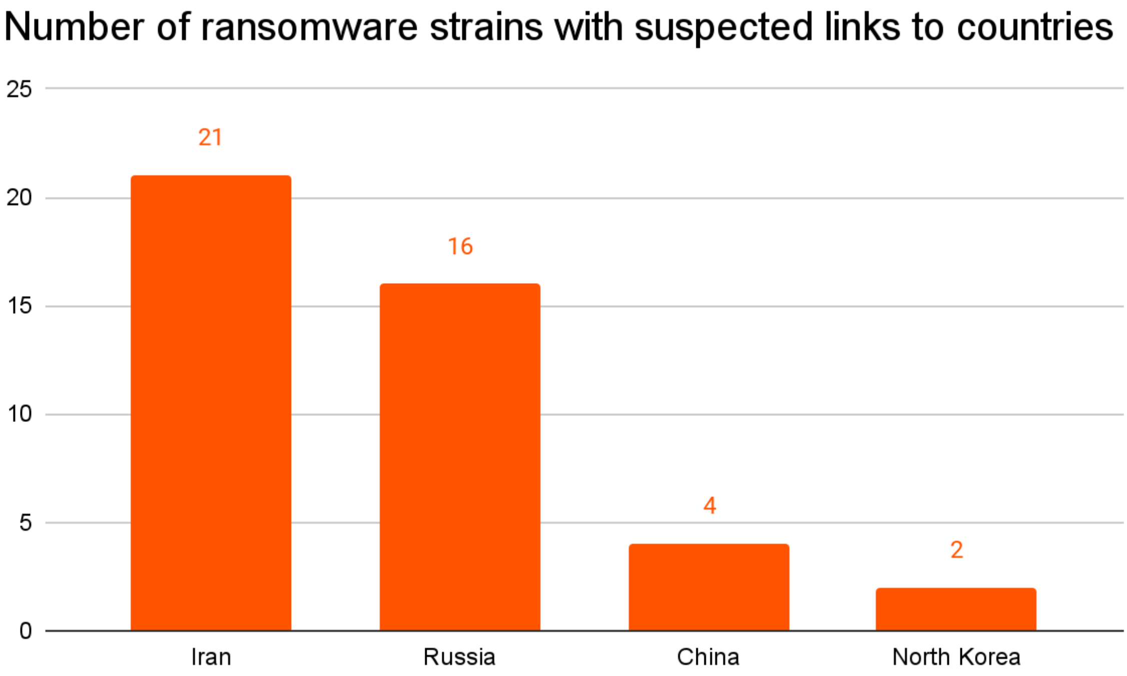
Overall, roughly 74% of ransomware revenue in 2021 — over $400 million worth of digital assets — went to strains we can say are highly likely to be affiliated with Russia in some way.

Blockchain analysis combined with web traffic data also tells us that after ransomware attacks take place, most of the extorted funds are laundered through services primarily catering to Russian users.


Estimation of Regional Exposure to Ransomware Funds | JAN 2021–DEC 2021
Index
40M
35M
30M
25M
20M
15M
10M
5M
0
Chainalysis

An estimated 13% of funds sent from ransomware addresses to services went to users estimated to be in Russia, more than any other region. A huge amount of digital asset-based money laundering, not just of ransomware funds but of funds associated with other forms of cybercrime as well, goes through services with substantial operations in Russia.

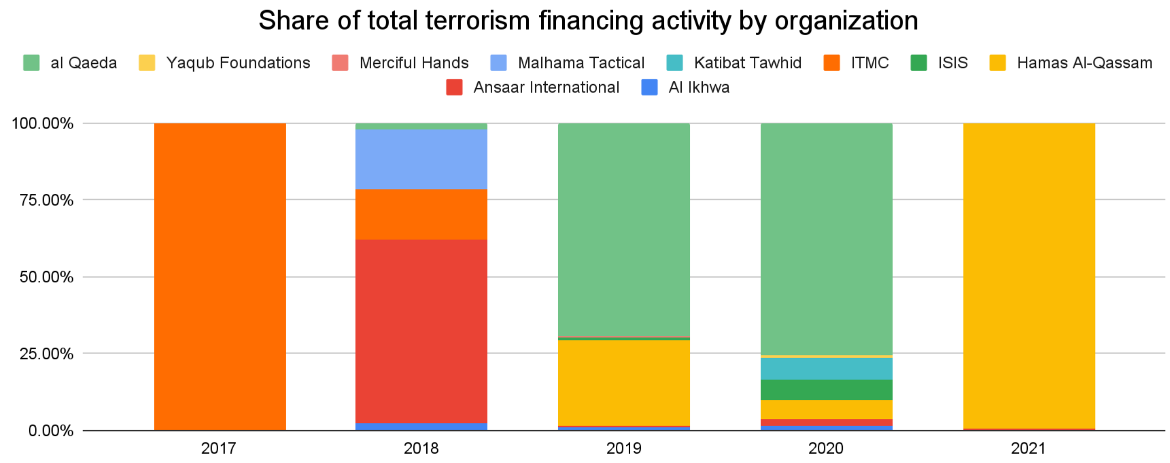
Russia-affiliated attackers aren't the only ones using ransomware for geopolitical ends. Cybersecurity analysts at Crowdstrike and Microsoft have concluded that many attacks by ransomware strains affiliated with Iran, mostly targeting organizations in the U.S., the E.U., and Israel, are geared more toward causing disruption or serving as a ruse to conceal espionage activity. Generally speaking, Chainalysis has seen significant growth in the number of ransomware strains attributed to Iranian cybercriminals in the past year — in fact, Iran accounts for more individual identified strains than any other country.



8. Terrorist financing

By the end of 2021, we've identified a number of terrorist organizations that have attempted to finance their operations with digital assets. What's harder to find, however, is a group that has gotten away with it.

- In 2019 and 2020, al-Qaeda raised digital assets through Telegram channels and Facebook groups. Thanks to the FBI, HSI, and IRS-CI, more than $1 million was seized from a money service business ("MSB") operator who facilitated some of these transactions.
- In early Spring of 2021, al-Qassam Brigades, Hamas' military wing, collected more than $100,000 in donations. In July, the Israeli government seized much of it from associated MSBs.



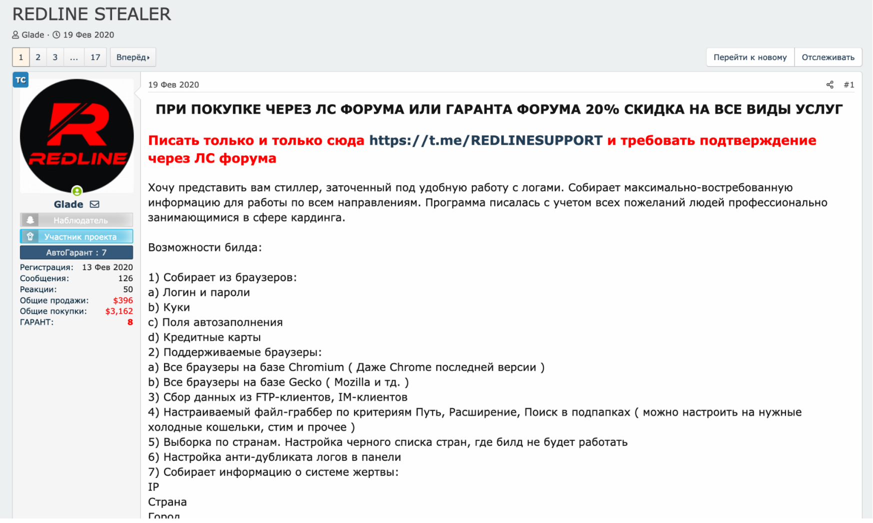
9. Malware

Malware refers to malicious software that carries out harmful activity on a victim's device, usually without their knowledge. Malware-powered crime can be as simple as stealing information or money from victims, but can also be much more complex and grand in scale. For instance, malware operators who have infected enough devices can use those devices as a botnet, having them work in concert to carry out distributed denial-of-service ("DDoS") attacks, commit ad fraud, or send spam emails to spread the malware further.

The malware families we discuss here are all used to steal digital assets from victims, though some of them are used for other activities as well. The grid below breaks down the most common types of digital asset-focused malware families.

Type	Description	Example
Info stealers	Collect saved credentials, files, autocomplete history, and digital asset wallets from compromised computers.	Redline
Clippers	Can insert new text into the victim's clipboard, replacing text the user has copied. Hackers can use clippers to replace digital asset addresses copied into the clipboard with their own, allowing them to reroute planned transactions to their own wallets.	HackBoss
Cryptojackers	Makes unauthorized use of victim device's computing power to mine digital asset.	Glupteba
Trojans	Virus that looks like a legitimate program but infiltrates victim's computer to disrupt operations, steal, or cause other types of harm.	Mekotio banking trojan

Many of the malware families described above are available to purchase for relatively little money on cybercriminal forums. For instance, the screenshots below show an advertisement for Redline, an info stealer malware, posted on a Russian cybercrime forum.



REDLINE STEALER

Glade · 19 Фев 2020

Регистрация: 13 Фев 2020
Сообщения: 126
Реакции: 50
Общие продажи: $396
Общие покупки: $3,162
ГАРАНТ: 8

19 Фев 2020 #1

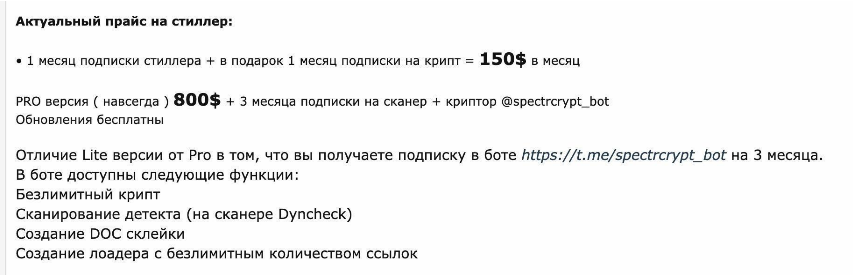
ПРИ ПОКУПКЕ ЧЕРЕЗ ЛС ФОРУМА ИЛИ ГАРАНТА ФОРУМА 20% СКИДКА НА ВСЕ ВИДЫ УСЛУГ

Писать только и только сюда https://t.me/REDLINESUPPORT и требовать подтверждение через ЛС форума

Хочу представить вам стиллер, заточенный под удобную работу с логами. Собирает максимально-востребованную информацию для работы по всем направлениям. Программа писалась с учетом всех пожеланий людей профессионально занимающимися в сфере кардинга.

Возможности билда:

1) Собирает из браузеров:
a) Логин и пароли
b) Куки
c) Поля автозаполнения
d) Кредитные карты
2) Поддерживаемые браузеры:
a) Все браузеры на базе Chromium (Даже Chrome последней версии)
b) Все браузеры на базе Gecko (Mozilla и тд.)
3) Сбор данных из FTP-клиентов, IM-клиентов
4) Настраиваемый файл-граббер по критериям Путь, Расширение, Поиск в подпапках (можно настроить на нужные холодные кошельки, стим и прочее)
5) Выборка по странам. Настройка черного списка стран, где билд не будет работать
6) Настройка анти-дубликата логов в панели
7) Собирает информацию о системе жертвы:
IP
Страна
Город



Актуальный прайс на стиллер:

• 1 месяц подписки стиллера + в подарок 1 месяц подписки на крипт = **150$** в месяц

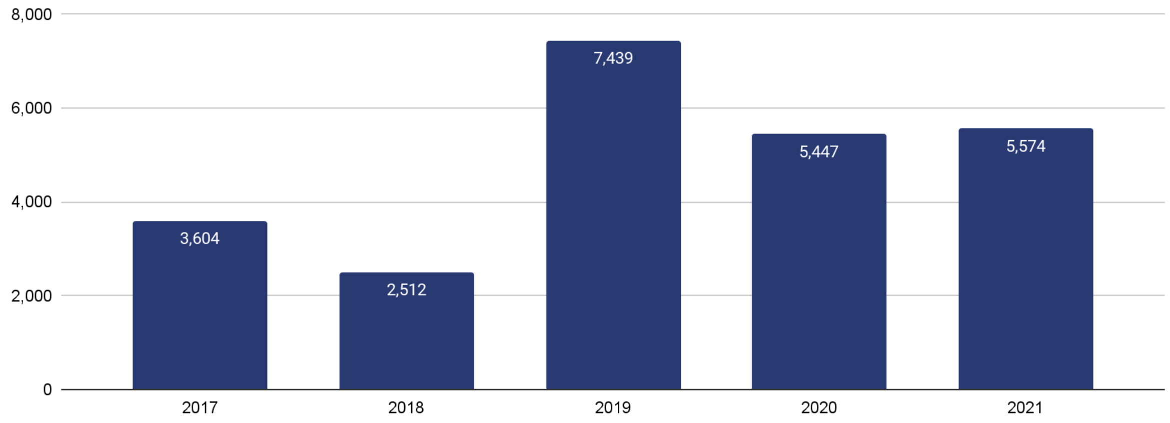
PRO версия (навсегда) **800$** + 3 месяца подписки на сканер + криптор @spectrcrypt_bot
Обновления бесплатны

Отличие Lite версии от Pro в том, что вы получаете подписку в боте *https://t.me/spectrcrypt_bot* на 3 месяца.
В боте доступны следующие функции:
Безлимитный крипт
Сканирование детекта (на сканере Dyncheck)
Создание DOC склейки
Создание лоадера с безлимитным количеством ссылок

The seller offers cybercriminals one month of Redline access for $150 and lifetime access for $800. Buyers also get access to Spectrum Crypt Service, a Telegram-based tool that allows cybercriminals to encrypt Redline so that it's more difficult for victims' antivirus software to detect it once it's been downloaded. The proliferation of cheap access to malware families like Redline means that even relatively low-skilled cybercriminals can use them to steal digital assets. Law enforcement and compliance teams must keep this in mind, and understand that the malware attacks they investigate aren't necessarily carried out by the administrators of the malware family itself, but instead are often carried out by smaller groups renting access to the malware family, similar to ransomware affiliates.

The graph below shows the number of victim transfers to digital asset addresses associated with a sample of malware families in the info stealer and clipper categories investigated by Chainalysis.

Transfers to info stealer and clipper malware addresses tracked from 2017 - 2021



Note: *This graph does not reflect activity by cryptojackers or ransomware.*

Overall, the malware families in this sample have received 5,974 transfers from victims in 2021, up from 5,449 in 2020.

APPENDIX B

Self-custody or “unhosted” wallets

Below we provide analysis relating to self-custodied “unhosted” wallets, putting their potential use by illicit actors in appropriate context.

In December 2020, when Treasury published a notice of proposed rulemaking for transactions with unhosted wallets and certain foreign jurisdictions, Chainalysis reviewed the data on cryptocurrency transactions involving unhosted wallets.

The data showed that the majority of the funds held in unhosted wallets often come from virtual asset service providers (“VASPs”) and are related to investing purposes or are the vehicle for individuals or organizations to move funds between regulated exchanges.

It is important to mention that 2021 data didn’t vary significantly in comparison to the 2020 analysis. There are still three trends related to the usage of unhosted wallets.

The vast majority of the bitcoin funds transferred to unhosted wallets came from VASPs

During Q3 of 2021, almost 83% of the bitcoin sent from an unhosted wallet to another unhosted wallet originated from cryptocurrency exchanges, and only 2% came from illicit services. This means that in the vast majority of cases law enforcement can investigate illicit activity related to unhosted wallets by working with cryptocurrency exchanges, which are obligated entities, and obtain KYC information from them through legal process.

The majority of bitcoin sent to non-VASPs are eventually sent to a VASP

A high number of the transfers sent and received by unhosted wallets have VASPs on the other side of the transaction. If cryptocurrency is being used for illicit purposes, eventually criminals will need to cash their illicit proceeds out. This means going through a cryptocurrency exchange (we can see this behavior reflected in our data). As long as they are in a country that regulates cryptocurrency exchanges – and this list is growing – exchanges will collect KYC information. Access to this information is vital to financial crime investigations.

During Q3 2021, the percentage of funds that were not sent to an exchange service decreased from 29% to 18% in comparison with Q2 2020. While the percentage of funds sent to exchanges increased from 62% to 71%. This means that crypto holders moved the funds they were holding inside unhosted wallets to an exchange, maybe to take out some profits due to the crypto bull market we experienced this year.

The transaction activity levels among unhosted wallets highly suggests that their primary use is for investment

After funds are deposited to an unhosted wallet from an exchange, the percentage of bitcoin moved to another unhosted wallet in a given month is significantly low. The majority of the bitcoin stays in the original wallet for a long period of time. On average, the funds originated from a VASP to unhosted wallets move only once a month, which likely indicates that the primary use case is investment.

Chainalysis' robust blockchain dataset provides key insights into the role of unhosted wallets in the cryptocurrency ecosystem. If the main purpose of these regulatory requirements is to decrease illicit transactions and avoid money laundering, targeting unhosted wallets may not accomplish the intended objective.

What our blockchain analysis data makes clear is that unhosted wallets are not inherently risky and unhosted wallets do not inhibit law enforcement's ability to investigate the illicit use of cryptocurrency. Blockchain analytics can inform risk analysis and compliance programs so that risks can be mitigated responsibly and effectively by compliance teams.

APPENDIX C

Glossary
Chainalysis Service Category Definitions

Most cryptocurrency volume travels through services, including legal entities like retail exchanges or illicit entities like darknet markets. To identify and assess the risk of a service, Chainalysis groups the wallet addresses into clusters. Then we attribute the clusters to specific entities and organizations (e.g., a particular exchange, mixing service, or darknet market, etc.). After attributing the clusters to a specific entity, we then categorize them according to the type of real-world service that they belong to. Chainalysis refers to these categories as Service Categories.

Child abuse material site
Child abuse material includes forums and sites operating on the dark web which facilitate the buying, selling, and the spread of child sexual abuse material. These sites are often coded and difficult to access.

Darknet markets
Darknet markets are commercial websites that operate on the dark web, which can be accessed via anonymizing browsers or software such as Tor or I2P. These sites function as black markets by selling or advertising illicit goods and services such as drugs, fraud materials, and weapons, among others. Darknet markets use cryptocurrency payment systems, often with escrow services and feedback systems to help develop trust between the vendor and customer. Darknet markets have become more security conscious over the past few years due to multiple law enforcement shutdowns.

Decentralized exchange contract
Decentralized exchanges are services which facilitate cryptocurrency and token trades by using automated smart contracts. Trades on a decentralized platform are peer-to-peer and have no third party or central authority other than the smart contract which executes the trades.

ERC-20 token

ERC-20 tokens are a blockchain-based asset that can be sent and received using an Ethereum wallet. It is the technical standard for most smart contracts on Ethereum blockchain, enabling token issuance for ICOs (a crowdfunding mechanism).

Ethereum contract

Ethereum is a blockchain with its own cryptocurrency and a built-in functionality for smart contracts. Smart contracts can store information related to a deal and automatically self-execute when the terms of the contract are fulfilled. Smart contracts can be agreed upon and enforced between two parties without the need for a third, since they don’t actually execute until each side has fulfilled their obligations.

Exchanges
Exchanges allow users to buy, sell, and trade cryptocurrency. They represent the most important and widely-used service category in the cryptocurrency industry, accounting for 90% of all funds sent by services.

Fraud shop

Financially motivated shops selling different types of data including, PII (Personally Identifiable Information), credit card data, stolen accounts, and more. Unlike Darknet Markets, Fraud Shops are normally operated by a single actor/team and are the sole merchant within the service. Fraud shops also tend to have behavioral differences from darknet markets such as top-up depositing of funds (incremental increases to the total amount), as well as no customer withdrawals. Therefore, most outgoing transactions can be linked to the operators of the Fraud Shop.

Gambling

Online gambling can take many forms from resembling a typical casino where you can play card games like blackjack and poker, slot games and the like, to sites for wagering bets on sports or eSports outcomes.

The industry has been an early adopter of cryptocurrency. Users will send cryptocurrency as a convenient alternative to fiat, and get started betting. Gambling is treated differently depending on the jurisdiction, and many sites have lax KYC requirements. Because of this, there's potential for these sites to be used for laundering money. Many of these companies are located in/operating out of island nation-states (such as Curaçao, Cyprus, or Malta).

High risk exchange

Chainalysis' designates an exchange as high risk according to the following criteria:

- **No KYC**: The exchange requires no customer information before allowing any level of deposit or withdrawal. This is also applicable if they require name, phone number, or email address but do not attempt to verify that this information actually belongs to the customer.
- **Criminal ties**: The exchange has publicly documented ties to criminal activity.
- **High risky exposure**: The exchange has high amounts of exposure to risky services such as darknet markets, other high risk exchanges, or mixing. Chainalysis examines if the exchange's exposure to illicit activity is an outlier compared to other exchanges. A service with direct high risk exposure one standard deviation away from the average across all exchanges identified by Chainalysis over a 12 month period is considered a high risk exchange.

High risk jurisdiction

The high risk jurisdiction category comprises cryptocurrency services that are based in specific jurisdictions, including Iran and Venezuela. Chainalysis considers both cryptocurrency activity as well as the global regulatory landscape when deciding which jurisdictions to include in this category. Given stringent guidelines for the financial system's interactions with Iran and Venezuela, Chainalysis has opted to more prominently surface services operating in these areas. Chainalysis will continue to add services to this category over time.

Hosted wallets

Hosted wallets are an alternative to core wallets (full node wallets). Wallet software allows users to store their public and private keys, and connects to blockchain nodes to transfer funds and check balances. Wallets that control the user's private keys are considered custodial, or hosted, while software that allows users to retain full control of private keys is considered non-custodial.

Hosted wallets can be risky because the user doesn't actually hold their funds, thus opening the possibility of being scammed. It's also possible the service does not implement sufficient security measures, and is vulnerable to attack. However, a reputable hosted wallet service that takes advanced security measures is likely more reliable and convenient than a non-technical or careless individual.

ICO

An ICO (Initial Coin Offering) is a means of crowdfunding for new cryptocurrency or related projects, similar to an IPO in the traditional market. The entity behind the new cryptocurrency makes their pitch and sells units of the token to investors in exchange for fiat currency or more mainstream cryptocurrencies like Bitcoin or Ether.

Many ICOs have proven to be scams. There are countless examples of bad actors who build a flashy site promoting an ambitious project, raise funds through an ICO, then pocket the money and walk away.

Illicit actor organization

Individuals and/or organizations that operate directly or indirectly in various forms of illicit activities. These entities are directly or indirectly involved with risky entities such as darknet markets, fraud shops, extremist financing, hacking, etc.

Lending contract

Lending is one of the biggest uses for smart contracts and DeFi currently. Holders of assets can lend them to others and earn interest on the loan. Borrowers have to put up collateral above the value of the loan to protect against price fluctuations.

Merchant services

Merchant services are authorized financial services that enable businesses to accept payments on their customer's behalf. They are also known as payment gateways or payment processors. These services allow merchants to accept cryptocurrency for invoicing and online or in-person payments. This often includes conversion to local fiat currency and settling funds to the merchant's bank account.

Merchant services is generally a low-risk category. Users mostly comprise mainstream, traditional businesses on one end and their customers on another. However, it's worth noting that scammers sometimes integrate merchant services with a malicious website to accept cryptocurrency payments from their victims.

Mining and Mining pools

Mining is the process by which cryptocurrency is generated. Mining pools are special services where miners can pool their resources - typically GPU or specialized ASIC mining hardware - together towards mining cryptocurrency. By pooling mining resources the pool has a bigger chance of mining a block and the returns are divided among all the miners according to how much mining power each contributed.

Mining pools typically only receive funds from direct mining activity, and as such are typically low risk. However, a pool that accepts deposits from sources other than mining can be exploited for money laundering.

Mining is used for coin generation, when new coins are minted from the mining process.

Mixing services

Mixers are websites or software used to create a disconnection between a user's deposit and withdrawal. Mixing is done either as a general privacy measure or for covering up the movement of funds obtained from theft, darknet markets, or other illicit sources.

Mixers typically pool incoming funds from many users and re-distribute those funds with no direct connection back to the original source.

Other

This category is used when the entity does not represent a widely popular field of operation or is a particular type of operation or entity such as donation addresses, social network bots, seized funds, among others. This category does not have any inherent risk but may contain risky entities.

Peer to peer (P2P) exchange

P2P exchanges are online sites that facilitate the buying, selling, and trading of cryptocurrency between two individuals while, usually, not being directly in possession of the funds. Some P2P exchanges will not require any KYC, making them attractive for money laundering activities.

Protocol privacy

Protocol privacy applies to the two shielded pools built into the Zcash blockchain.

Zcash offers users the possibility to encrypt blockchain activity; this is known as shielding. Zcash provides this capability through shielded pools - a collection of encrypted addresses where the balances and transactions within the pool are always encrypted. Transactions into, out of, and between the pools are transparent but the counterparty addresses within the pool remain encrypted. The pools appear in Reactor as named entities and single address clusters, which are categorized as Protocol privacy. While we can't show activity or addresses within the pool, we display activity into and out of the pool.

Mined ZEC cannot be sent straight to transparent addresses but must first go to one of the shielded pools. Hence receiving exposure from a shielded pool doesn't necessarily mean that the funds were mixed or deliberately obfuscated. Other users must opt in to take advantage of Zcash's privacy features. Roughly 14% of Zcash transactions involve one of Zcash's two shielded pools.

Ransomware

Ransomware is special malware designed to encrypt a victim's computer data and automatically request a ransom to be paid in order to decrypt the data. Attackers employ social engineering and phishing schemes that trick people and organizations into downloading the malicious software.

Sanctions

Sanctions refer to entities listed on economic/trade embargo lists, such as by the US, EU, or UN, with which anyone subject to those jurisdictions is prohibited from dealing. Currently this includes the SDN list of the US Department of the Treasury's Office of Foreign Assets Control. The prohibition on dealing includes any instrumentalities of the sanctioned entities, including operating companies, bank accounts, and cryptocurrency addresses used by the sanctioned entities. In some instances, persons subject to those jurisdictions are also required to block/freeze assets belonging to the sanctioned entities to prevent further benefit or movement.

Scam

Scams can impersonate a variety of services, including exchanges, mixers, ICOs, and gambling sites. This category also encompasses scam emails, extortion emails, and fake investment services. They usually offer unrealistic returns on investment, many times trying to mask a pyramid scheme, or pretend to have incriminating personal data on the victim and ask for money in order to not disclose it.

Smart contract

Some blockchains have a built-in functionality for smart contracts. Smart contracts can store information related to a deal and automatically self-execute when the terms of the contract are fulfilled. Smart contracts can be agreed upon and enforced between two parties without the need for a third, since they don't actually execute until each side has fulfilled their obligations.

Stolen funds

Stolen funds comprise instances of hacked exchanges and services. Attackers engage in sophisticated and persistent social engineering, and exploit pre-existing vulnerabilities to transfer funds from exchange hot wallets to their control. The payoff for actors can be enormous with single incidents often resulting in tens of millions of dollars in losses.

Terrorist financing

Terrorist financing pertains to the funding of designated terrorist groups and affiliates of terrorist groups, entities, and individuals. Financing is fundamental for the survival and operation of terrorist groups and is used to support a multitude of their activities, including recruitment, propaganda, day-to-day activities, and military operations. Terrorist groups secure the flow of funds in a variety of ways, including through the use of cryptocurrencies.

Token smart contract

Tokens are a blockchain-based asset that can be sent and received using a wallet. There are different technical standards for the different types of smart contracts on various blockchain, enabling token issuance for ICOs (a crowdfunding mechanism).

Unnamed Service

Clusters we identify as behaving as services fall into this category. These are services that have not yet been identified but show the behavior expected of a service. There isn't a standard risk for this category, but once any entity in this category is identified, it is labeled and moved to an appropriate category.