Chainalysis

Written Testimony of Jacqueline Koven
Head of Cyber Threat Intelligence
Chainalysis Inc.

Before the
US Senate Committee on Homeland Security and Governmental Affairs

Hearing on
“Rising Threats: Ransomware Attacks and Ransom Payments Enabled by Cryptocurrency”

June 7, 2022

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

My name is Jacqueline Koven and I am the Head of Cyber Threat Intelligence for the blockchain data platform Chainalysis. In this role, I track ransomware operators and their enablers on the blockchain. I also coordinate global ransomware research, partnerships, and joint initiatives. Prior to joining Chainalysis, I served in the US Intelligence Community, including in Iraq and held several interagency assignments.

This hearing could not be more timely. We have seen ransomware attacks increase significantly over the past few years, with ransomware actors attacking critical infrastructure, law enforcement agencies, healthcare providers, municipalities, schools, and other businesses. While it is true that cryptocurrency is generally the preferred payment of choice in these cases, it is not true that cryptocurrency is the cause of ransomware attacks. In fact, due to its transparent nature, it can be much easier to investigate cases involving the illicit use of cryptocurrency than other forms of payment. In order to further enable this work, it is vital that we address this important issue by appropriately equipping government agencies to go after ransomware actors and bring them to justice.

Cryptocurrency and blockchain technology are some of the best available tools in the toolkit that the United States has to compete with the development of central bank digital currencies being developed in other countries, like China, along with other alternative payment systems. The entrepreneurial dynamism that cryptocurrencies present allows for innovators and builders to create universal access to financial products and re-engineer web2 business models to serve individuals and their data in a way that protects privacy and helps our communities. This technology is consistent with our American values and has the potential to be strategically more important in the global powers competition over the next few decades. Of course, we understand concerns about risk and abuse and that is why we are here today. At Chainalysis we share concerns about the illicit use of cryptocurrency, but we know that the inherent open nature of this technology can be leveraged to mitigate the risks associated with it and bring bad actors to justice.

If there is one point I want to make to the members of this Committee, it is that the transparency of cryptocurrency blockchains enhances the ability of policymakers and government agencies to detect, disrupt and, ultimately, deter illicit activity. By mapping a single illicit actor to a cryptocurrency wallet address, for example a ransom payment, 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, extensive 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.

Executive Summary

Chainalysis is the blockchain data platform that leverages the transparency of cryptocurrency blockchains to provide data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies. Our data platform powers investigations, 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 cryptocurrency safely. The transparency of the blockchain allows for effective investigations into ransomware groups, as we have seen in cases like the NetWalker takedown and the investigation into DarkSide's attack on Colonial Pipeline.

Our **ransomware data** shows that, as of May 2022, there were just over $694 million in 2020 ransomware payments. We have also identified just over $712 million worth of ransomware payments in 2021; this was a record breaking year in terms of ransomware revenue. These figures, which almost certainly undercount ransoms paid, show the magnitude of the ransomware problem and underscore the importance of tackling it.

Average ransomware payment sizes have grown significantly for the past few years. The average ransomware payment size was over $121,000 in 2021, up from $88,000 in 2020 and $25,000 in 2019. At the same time, the median transfer size sent to ransomware addresses is around $6000. This **median payment size has increased only modestly** from approximately $2500 in 2018 and 2019 and $4000 in 2020. This indicates that in addition to the larger ransomware targets that we often hear about in the news, there are likely also many other smaller victims, including small businesses.

While the title of this hearing is "Rising Threats: Ransomware Attacks and Ransom Payments Enabled by Cryptocurrency", **it is not our position that cryptocurrency enables ransomware**. Ransomware has existed since 1989, and cryptocurrency was only first documented as the payment method in 2013. The phenomenon of cryptocurrency being leveraged by ransomware actors represents criminals adapting to new technologies and payment methods - something we have seen criminals do throughout time. In fact, the transparency of cryptocurrency enables investigations into these sorts of attacks that would not be possible if they used other, less transparent forms of payment.

Ransomware groups have increasingly adopted the **Ransomware as a Service (RaaS)** model, meaning that affiliates do not have to develop the technology used to conduct these attacks, but rather carry out ransomware attacks using malware maintained by RaaS administrators. In these cases, the ransomware administrators take a moderate cut, and the affiliates' commissions usually range from 30-90% of the ransom or sometimes a fixed fee. They have also modified how they deploy their attacks, including not always encrypting data. This means that government agencies may have to be more flexible with the definition of ransomware as they propose reporting requirements for cyber attacks.

It is a **common misconception that cryptocurrency is completely anonymous and untraceable**. While some argue that the nature of cryptocurrency facilitates the crime of ransomware, its nature also facilitates incomparable visibility that benefits law enforcement immensely. In fact, the transparency provided by many cryptocurrencies' public ledgers is much greater than other traditional forms of value transfer. Using Chainalysis' blockchain analysis tools, law enforcement can trace cryptocurrency transactions to identify their origination and/or its cashout points at cryptocurrency exchanges. Law enforcement can serve legal process to cryptocurrency businesses to request identifying information related to the account associated with the illicit transaction, or request that the associated accounts be frozen. This information can be very powerful in furthering investigations into the illicit use of cryptocurrency, including ransomware. We have seen a number of government successes in this space, in part due to the use of blockchain analysis tools.

Over the past few years, we have seen the **rapid evolution of ransomware groups**. These groups, likely in large part due to effective law enforcement actions against them, rebrand extremely quickly, **evolving into new strains**, but conducting the same activities. The share of ransomware funds going to third-party sellers from ransomware operators spiked to its highest ever levels in 2021, suggesting an increase in ransomware actors **reinvesting their ill-gotten funds into other ransomware campaigns**. Some of the most prominent groups include **Conti**, which was the biggest ransomware strain in 2021, which extorted at least $200 million from victims. This group is known for announcing its support for the Russian government after the Russian invasion of Ukraine, as well as for the recent attack on Costa Rica, which shut down 27 government institutions there. **DarkSide** is another group that is notable, including for its role in the attack on the Colonial Pipeline. **NetWalker** was one of the most prominent strains of 2020. It operated as a RaaS and was taken down by an international law enforcement effort in 2021, in which $27 million in bitcoin was seized from just one affiliate.

Some of the most prominent **money laundering trends** we see in ransomware include the use of mixers, an increase in ransomware demands in privacy coins, and a concentration of cashout services, including to high-risk exchanges in parts of the world that do not regulate cryptocurrency businesses. The US government should work with other countries to aid in the development and implementation of rigorous anti-money laundering/countering the financing of terrorism (AML/CFT) laws to limit the ability of illicit actors to cash out in other jurisdictions.

An increase in **sanctions against ransomware actors and their facilitators, including exchanges, darknet markets, and mixers** by the Office of Foreign Assets Control (OFAC) of the US Department of the Treasury has helped slow down the effectiveness of those businesses, especially when cryptocurrency addresses are included in designations as identifiers. This demonstrates that compliant cryptocurrency exchanges have proven effective at stopping the flow of funds to designated individuals and entities with cryptocurrency wallet addresses.

While most ransomware attacks appear to be financially motivated, some appear to **conduct attacks that align with geopolitical objectives or employ ransomware as a cover for these goals**. Some of the most pervasive strains avoid targeting Commonwealth of Independent States (CIS), including Russia, and will fail to encrypt if they detect the operating system is located in a CIS country. Chainalysis data suggests roughly 75% of ransomware revenue in 2021 went to strains we can say are highly likely to be affiliated with Russia in some way. For example, researchers have identified nation states launching ransomware attacks as a cover for espionage and have even reported wiper attacks masquerading as ransomware for plausible deniability. Even more pointedly, after the start of the war, Conti ransomware group announced its support for the Russian government.

My **recommendations** for improving the government response to this threat include: 1) Improving ransomware reporting and information sharing; 2) Ensuring government agencies have adequate funding for the training, tools, and resources they need to conduct these investigations; 3) Improving coordination and collaboration between countries; 4) Providing assistance to countries to support their implementation of robust AML/CFT laws for cryptocurrency businesses; 5) Allowing for expanded definitions with malicious cyber activities that warrant reporting; and 6) Pursuing ransomware facilitators and enablers in order to have a broader impact on the ransomware ecosystem.

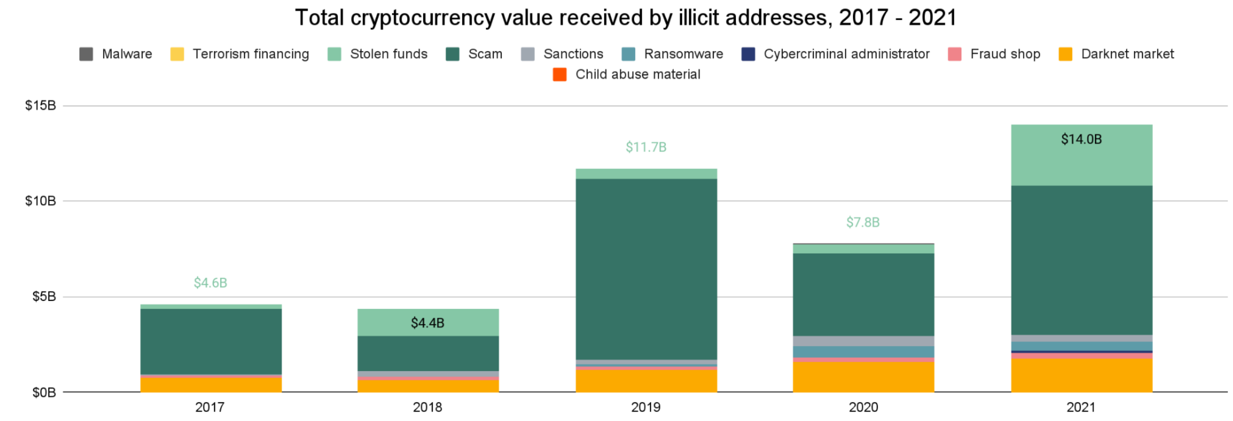
Chainalysis Background

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 750 customers in 70 countries. Our data platform powers investigations, 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 cryptocurrency safely. We have worked closely with law enforcement and regulators as they have worked to disrupt and deter illicit uses of cryptocurrency.

Chainalysis's 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 cryptocurrency ecosystem, enabling the realization of the technology's potential.

Chainalysis's data powers both investigative and compliance tools. Our investigative tool, Reactor, enables government agencies and investigative teams to trace the illicit uses of cryptocurrency, including money laundering, theft, scams, and other criminal activities. Our compliance tool, KYT (Know Your Transaction), provides cryptocurrency businesses and financial institutions the ability to screen their clients transactions and ensure that they are not attempting to interact with illicit entities. This transaction monitoring tool provides ongoing insights for cryptocurrency businesses so that they can protect their businesses and clients and ensure regulatory compliance.

Chainalysis also leverages our data to conduct research into the cryptocurrency ecosystem, including the illicit use of cryptocurrency. We publish a number of reports, including our annual Crypto Crime Report. Based on this research, we reported in our 2022 Crypto Crime Report that cryptocurrency-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. Top categories include scams, stolen funds, darknet markets, and – pertinent to this hearing – ransomware.

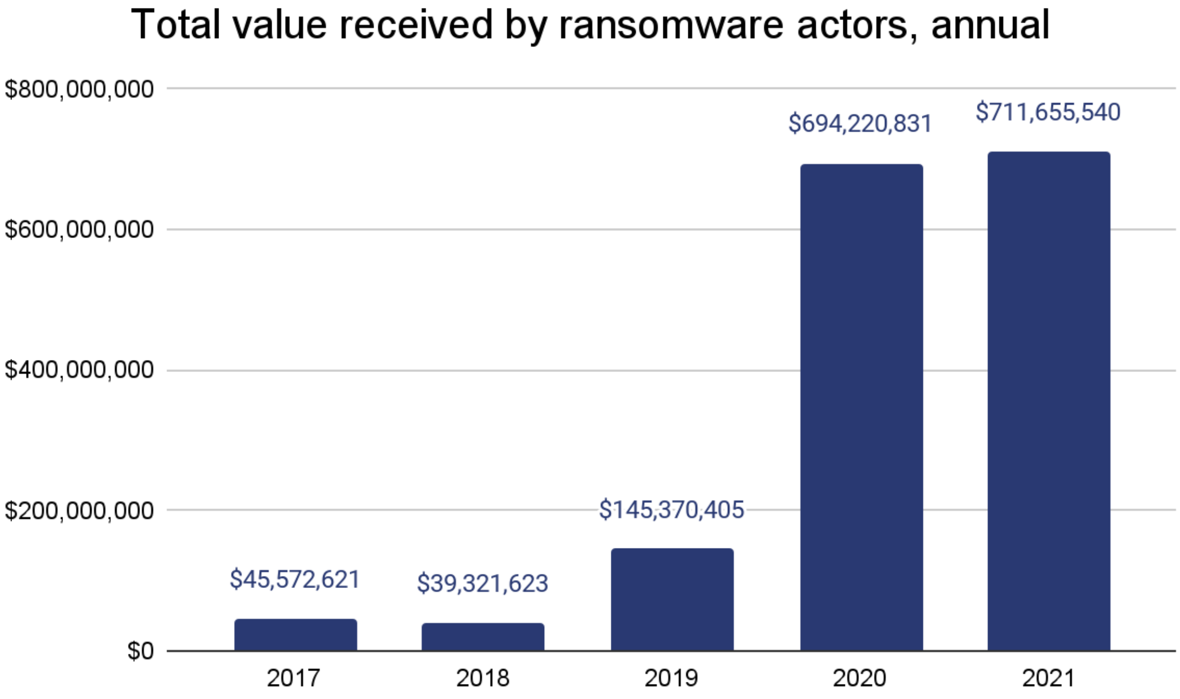


Despite this large increase in illicit transaction volume, illicit activity as a percentage of total volume has actually fallen dramatically since 2019. In 2019, the illicit share was about 3%, in 2020 it was just over 0.5%, and in 2021 it was 0.15%. The reason for this is that cryptocurrency usage is growing faster than ever before, so while cryptocurrency-related crime is definitely increasing, the legitimate use of cryptocurrency is far outpacing its use by illicit actors. This is good news for the cryptocurrency ecosystem, but government and industry must still put in place and implement the appropriate controls to mitigate risks in the system.

Ransomware statistics

In our 2021 Crypto Crime Report, Chainalysis deemed 2020 the “Year of Ransomware” due to the huge growth in cryptocurrency extorted in ransomware attacks. When we first released that report last year, we announced that we had tracked roughly $350 million worth of payments from victims to ransomware operators. As we explained at the time, this figure was likely an underestimate we would raise in the future due to both underreporting by ransomware victims and our continuing identification of ransomware addresses that have received previous victim payments.

Sure enough, as of May 2022, we’ve now identified just over $694 million in 2020 ransomware payments — nearly double the amount we initially identified at the time of writing last year’s Crypto Crime report. We also identified just over $712 million worth of ransomware payments in 2021, a record breaking year in terms of ransomware revenue. Despite this, we know that this too is an underestimate, and that the true total for 2021 is likely to be much higher. This helps to shed light on the scope of this problem and the importance of tackling it.

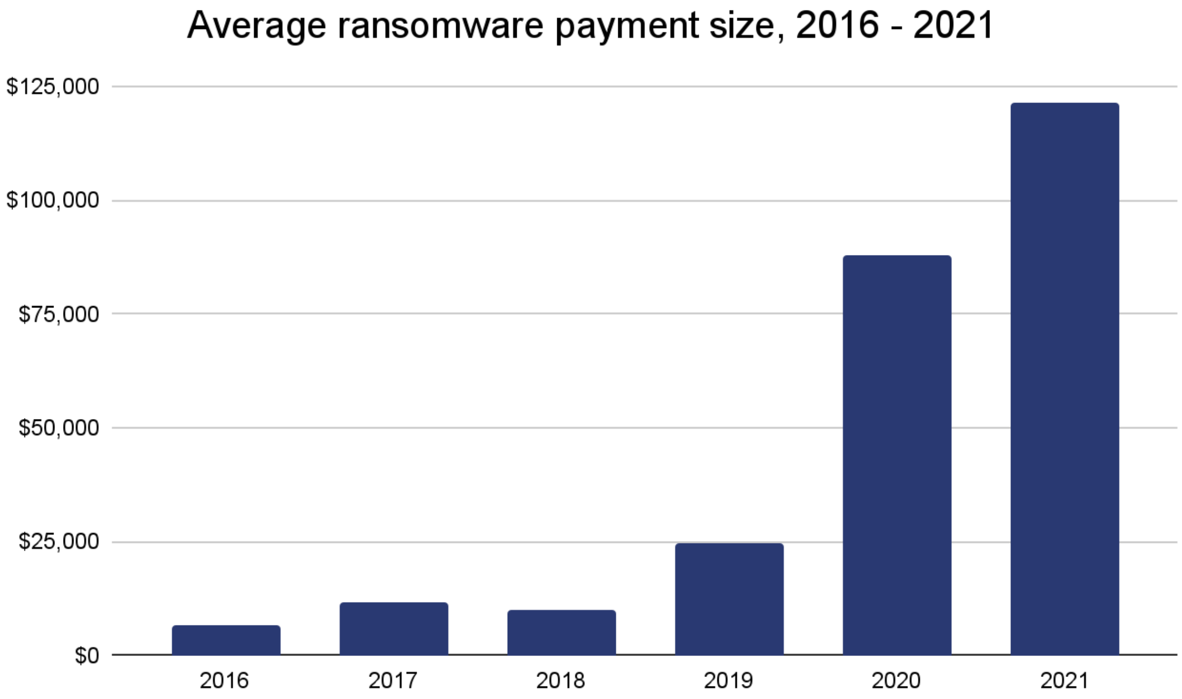


Ransomware payment trends

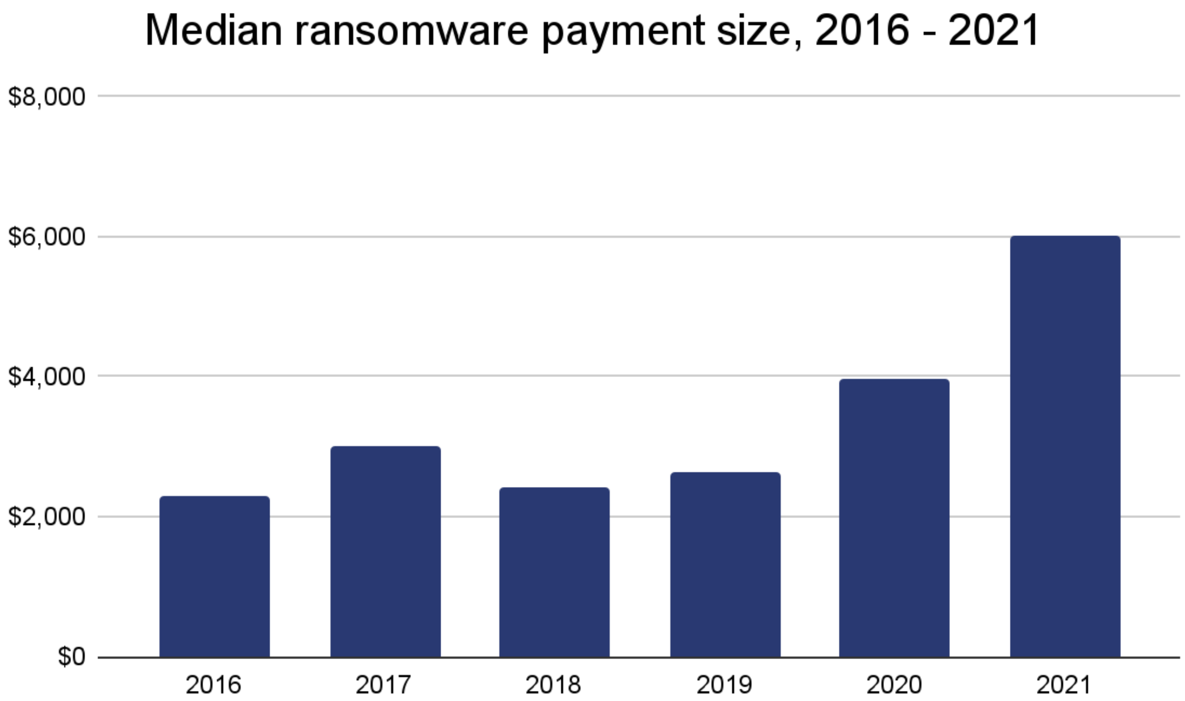
Ransomware payment sizes have grown significantly for the past few years. The average ransomware payment size was over $121,000 in 2021, up from $88,000 in 2020 and $25,000 in 2019. Large payments such as the record $40 million received by Phoenix Cryptolocker spurred this all-time high in average payment 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 the criminal underground and third-party providers to make their attacks more effective. These tools and professionalized underground services 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.



At the same time, the median transfer size sent to ransomware addresses is around $6000, indicating that in addition to the larger victims of ransomware attacks, there continue to be many smaller victims.



This demonstrates that in addition to a number of larger businesses being targeted, many smaller businesses and entities continue to fall victim to ransomware attacks.

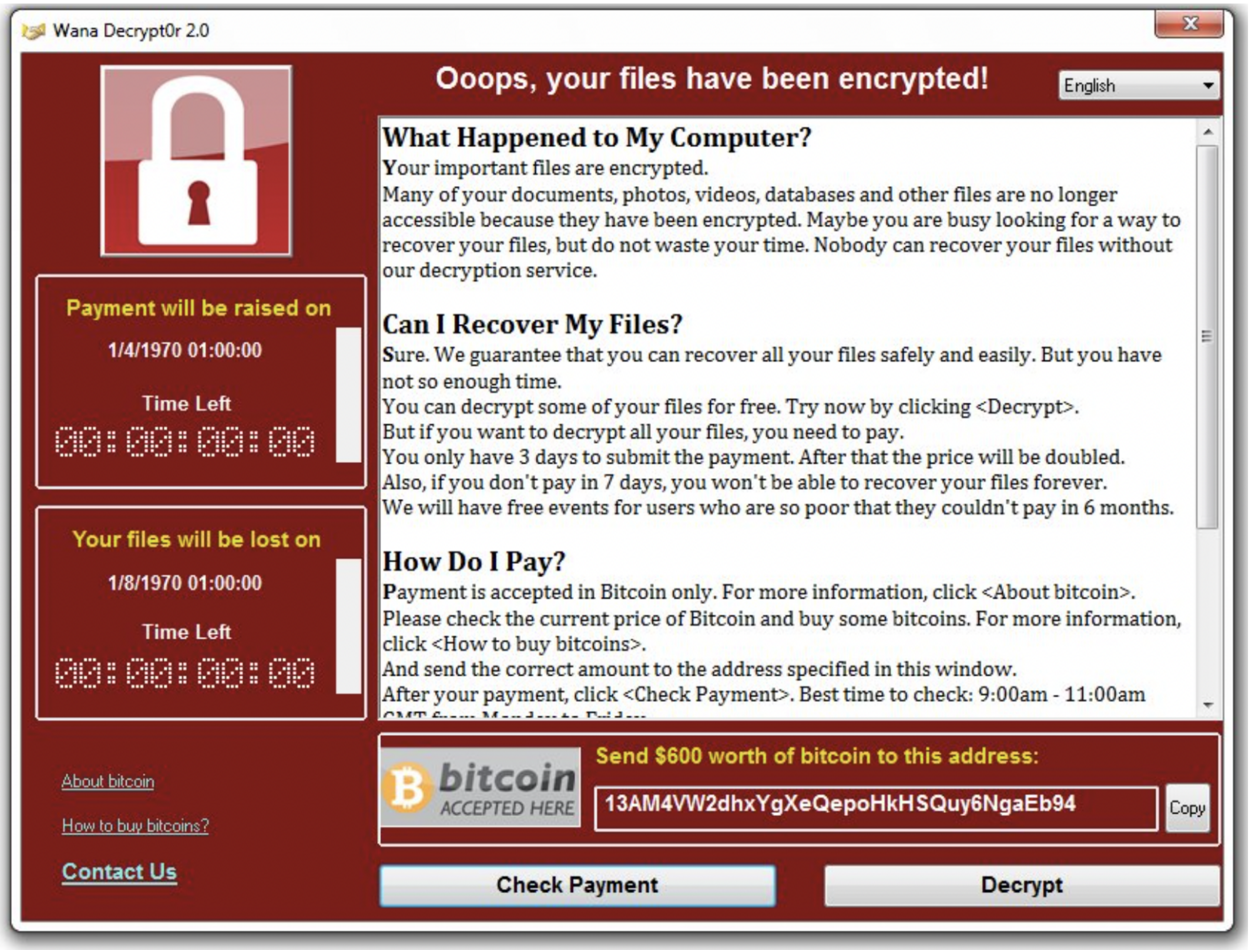
A history of cryptocurrency and ransomware

One item I would like to clarify is that cryptocurrency does not enable ransomware. It is merely an instrument used by illicit actors, whose tactics are forever evolving as new technologies come along. Although cryptocurrency is the payment method of choice for ransomware today, it would not be true to say that ransomware would not exist without cryptocurrency.

In fact, ransomware dates back to 1989, several decades before the creation of Bitcoin in 2009. In 1989, Joseph Popp, an AIDS researcher, distributed 20,000 floppy disks containing malware to fellow researchers saying they contained a computer-based application to analyze a person's risk of contracting AIDS based on a questionnaire. However, the infected disks contained malware, which activated after the computer was turned on 90 times, displaying a ransom note on the screen demanding between $189 and $378 in the form of a cashier's check or money order sent to a PO Box in Panama for a "software lease" (effectively a cryptographic key), according to a report from cybersecurity company Palo Alto Networks.

Similarly, in the early 2000s, Fake Antivirus scams and incidents collected millions from victims around the world using credit card payments. Fake Antivirus operators would load balance payments across a variety of processors and honor a certain number of charge-backs in order to maintain access to the processor's network.

Ransomware payments have come in many methods, including online payment processors, gift cards, credit cards, and other traditional money transmission services. It was not until 2013 that the first cases of ransomware demanding cryptocurrency as payment were documented. There have been several iterations to include what is known as “scareware,” a malware extortion technique that leverages fake security alerts or social engineering to frighten victims into paying for fake anti-virus protection. Scareware is typically conducted through spam campaigns and themes can also include blackmail. For instance, actors might claim to have incriminating web searches or access to the victim’s webcam, which is also known as “sextortion”. Crypto-centric ransomware began as spam for many years, indiscriminately spreading and leaving all victims with identical ransom notes and demanding payment at the same cryptocurrency address in exchange for the decryptor.



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on

1/4/1970 01:00:00

Time Left

00:00:00:00

Your files will be lost on

1/8/1970 01:00:00

Time Left

00:00:00:00

Send $600 worth of bitcoin to this address:

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

WannaCry ransomware re-used the same cryptocurrency address in ransom notes for multiple victims in 2017.

Ransomware is a sub-category of malware, a class of software designed to cause harm to a computer or computer network. Often, ransomware is designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Ransomware actors then demand ransom in exchange for decryption keys that enable the victim to restore their files. Many threat actors involved in ransomware have been engaged in cybercrime long before the surge in ransomware in recent years; ransomware is simply the latest and currently most profitable iteration in cybercrime. An example of this is the Russia-based cybercriminal organization, Evil Corp, which has been sanctioned by OFAC. This group initially developed Dridex malware to infect computers and harvest login credentials from hundreds of banks and financial institutions in over 40 countries, causing more than $100 million in theft. However, in recent years, Evil Corp repurposed the malicious software to be a loader that downloads various modules that can perform different malicious behavior, such as installing additional payloads like ransomware.

Ransomware groups have increasingly adopted the Ransomware as a Service (RaaS) model, meaning that affiliates do not have to develop the technology used to conduct these attacks, but rather carry out ransomware attacks using malware maintained by RaaS administrators. Affiliates' commissions can range between 30-90% of the ransom in most cases or a fixed fee, while the ransomware administrators take a smaller cut of the payment from each successful attack. This phenomenon acts as a force multiplier for ransomware gangs, giving them the scale to build operational support for ransomware campaigns, including negotiation services, coding, web development, spamming, pentesting, and more.

Ransomware infiltrates systems in a number of ways, including through exploitation of cyber security vulnerabilities and social engineering tactics such as "phishing" emails that deceive employees within an organization to open attachments that launch the malware that then infects their networks. Once launched, the malware may connect to a command-and-control server to enable the criminals to move laterally across networks and encrypt and/or exfiltrate the organization's data. Ransomware victims are typically prompted with a screen informing them that their data has been encrypted, with instructions for how to contact the ransomware group to negotiate the restoration of their systems and the ransom payment amount cryptocurrency. The attackers often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid, as detailed by the Institute for Security and Technology's Comprehensive Framework report.

According to a global survey of 2,200 senior IT decision makers and IT security professionals, in 2021, 66% of respondents' organizations suffered at least one ransomware attack in the past 12 months. 24% of victims ended up paying the ransom – a similar figure to 2020 (27%). 96% of those who paid the initial ransom, also had to pay extortion fees.

How blockchain analysis aids in the investigation of ransomware cases

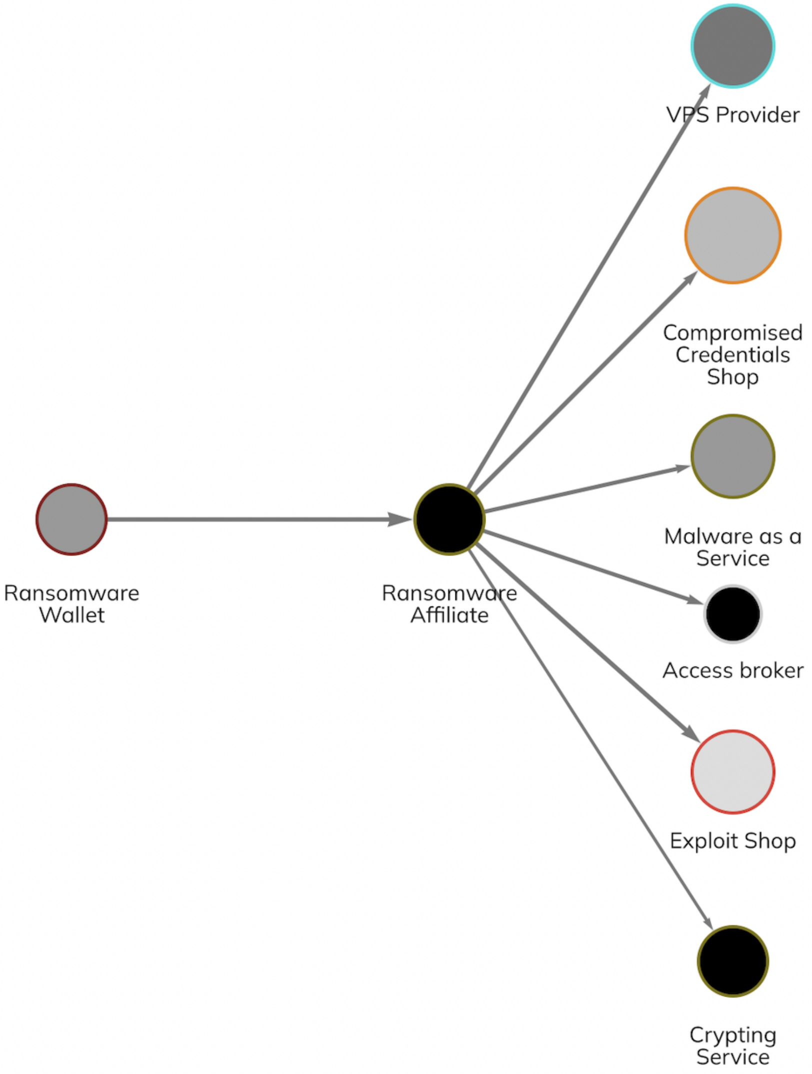
Today, ransom is often demanded in cryptocurrency. However, it is a common misconception that cryptocurrency is completely anonymous and untraceable. In fact, the transparency provided by many cryptocurrencies' public ledgers is much greater than other traditional forms of value transfer. Cryptocurrencies like Bitcoin operate on public, immutable ledgers known as blockchains. Anyone can look up the entire history of transactions on these blockchains. The ledger shows a string of random numbers and letters that transact with another string of random numbers and letters.

At its core, Chainalysis is a data company, and our data set maps these random numbers and letters – cryptocurrency addresses– to their real-world entities. For example, in Chainalysis products, we are able to see that a given transaction was between a user at a specific exchange, with a user at another exchange, or between a user at an exchange and a sanctioned entity, or any other illicit or legitimate service using cryptocurrency. Our data set and investigative tools are invaluable in allowing investigators to trace cryptocurrency transactions, identify patterns, and, crucially, see where cryptocurrency users are exchanging cryptocurrency for fiat currency ultimately lending valuable clues for attribution.

Using blockchain analysis tools, government agencies can trace cryptocurrency transactions to identify their origination and/or its cashout points at cryptocurrency exchanges. Law enforcement can serve subpoenas to these cryptocurrency exchanges, which are required to register as money service businesses here in the United States and collect Know Your Customer (KYC) information from their customers. In their response to legal process, the exchange will provide any identifying information that they have related to the cryptocurrency address, such as name, address, and government identification documentation, to law enforcement, allowing them to further their investigation. Law enforcement can also request that cryptocurrency exchanges freeze accounts through legal process. Cryptocurrency exchanges can also proactively freeze accounts and illicit funds on their platform, which provides a mechanism to make it more difficult for ransomware operators to profit.

Starting with one ransomware-related cryptocurrency address, an investigator can identify not only which address currently holds the funds, but which other addresses are associated with that ransomware actor, as well as which facilitating tools and services enable their attacks, such as access brokers, VPN providers or bulletproof hosting services, and which other groups these actors may be collaborating with. We can tell when members of one group are tied to a new group, whether that is a rebrand, or simply collaboration with another group.

Mapping out the Ransomware Supply Chain

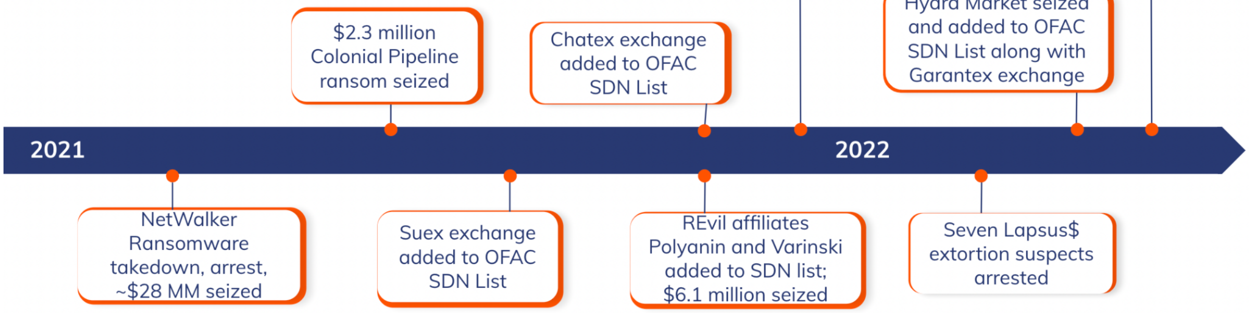


It is worth noting that sophisticated threat actors have largely wisened up to the traceability of the blockchain and now take measures to conceal their cryptocurrency wallet address from investigators. For example, most ransomware today gives unique extortion addresses for each victim and have removed the payment address from notes entirely. Many ransomware operators have opted for password-protected chats to directly and discreetly engage with the victim and will only provide the victim with their unique cryptocurrency address for payment once the ransom amount is settled in negotiation. Cryptocurrency addresses from extortion are a valuable investigative lead with unique potential for attribution and disruption of criminals; therefore, wallet information should be shared expeditiously with blockchain investigators to operationalize, but also protected amongst investigative professionals. Threat actors have enhanced their own datasets of cryptocurrency addresses to facilitate laundering. For example, an underground actor claimed to run a service for illicit actors to check if their wallets or transactions would set off flags at compliant exchanges. Some ransomware operators also threaten retaliation against victims that share details of negotiations including extortion addresses with law enforcement, adding greater importance to the safeguarding of this intelligence amid ongoing investigations.

We have seen a number of government successes in this space, in part due to the use of blockchain analysis tools. As the below timeline illustrates, since 2021, 11 major ransomware variants have shut down, US government agencies have arrested dozens of suspects and seized over $50 million in ransomware proceeds, and we have identified billions of dollars worth of cryptocurrency associated with designated entities. This demonstrates that, when equipped with the right tools, law enforcement can make a significant impact on the ransomware ecosystem.

2021-2022 Highlights

- **Over 11** major ransomware variants shut down
- Dozens of suspects arrested
- **$50MM** seized
- **Billions** worth of cryptocurrency associated with designated entities



2021

NetWalker Ransomware takedown, arrest, ~$28 MM seized

$2.3 million Colonial Pipeline ransom seized

Suex exchange added to OFAC SDN List

Chatex exchange added to OFAC SDN List

REvil affiliates Polyanin and Varinski added to SDN list; $6.1 million seized

$2.3 million seized from GandCrab/ REvil affiliate

2022

Seven Lapsus$ extortion suspects arrested

Hydra Market seized and added to OFAC SDN List along with Garantex exchange

Laundering service Blender[.]io added to OFAC SDN List

The evolution of ransomware groups

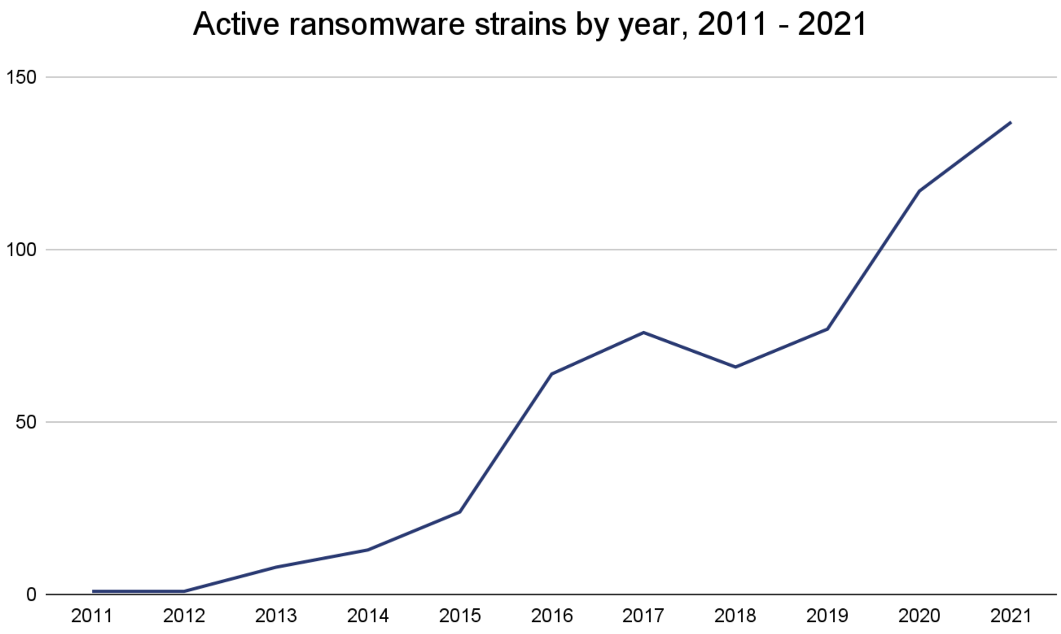
Rebranding of Ransomware Groups

One of the biggest trends we've recently observed in ransomware is an increase in renaming and rebranding of individual strains. These groups rebrand extremely quickly, spinning off new strains, but conducting the same activities. Extortion tactics have evolved to skirt the bounds of what is considered "ransomware". More groups have emerged that are infiltrating victims' systems, exfiltrating sensitive data and threatening to release or sell the data unless a ransom is paid, although no encryption occurs. There have also been reported instances of threat actors contacting victims and notifying them of the capability to deploy ransomware unless a ransom is paid – this tactic is sometimes referred to as "pre-ransom". A similar tactic is used with Distributed Denial of Service (DDoS) attacks, whereby an organization is contacted and threatened with a DDoS attack unless an extortion is paid, and in some cases DDoS is actually deployed against a victim organization until an extortion is paid.

Increasingly, not all attacks result in data encryption. According to a 2021 survey of 5,400 IT decision makers across 30 countries IT managers, cybercriminals succeeded in encrypting data in only 54% of incidents, compared to 73% of incidents in 2020. These extortion tactics that do not leverage ransomware's signature encryption are likely adopted by threat actors in part to attempt to circumvent government agency scrutiny, while still reaping financial reward. The benefit of blockchain analysis tools is that these extortions still leave a trail of evidence on-chain. This also means that policy makers and government agencies will need to be flexible about cyber attack definitions when requesting reporting on these events.

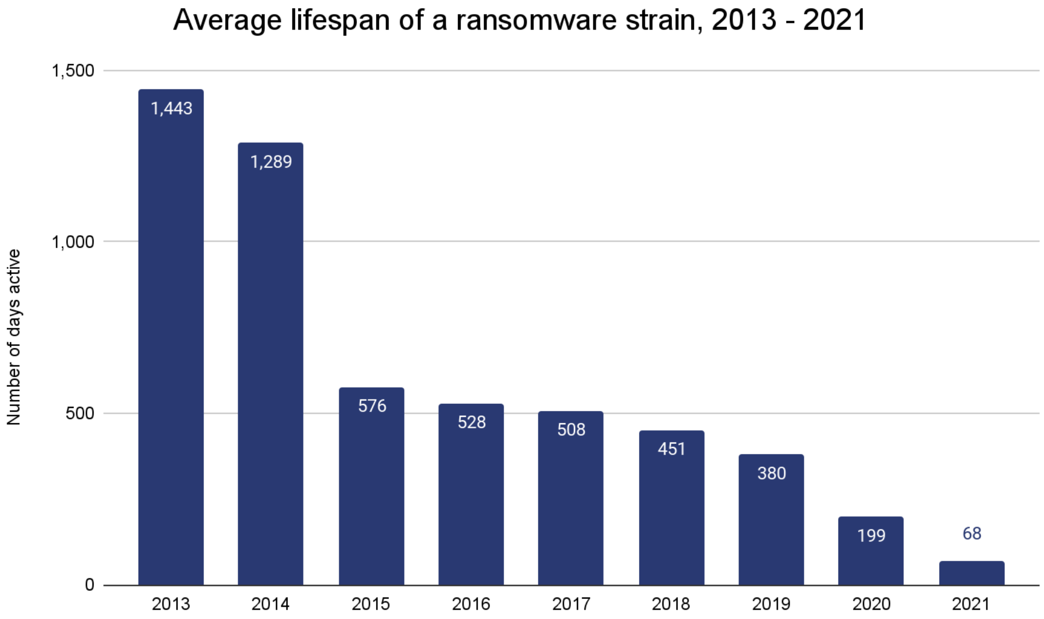
Overall, 2021 also saw more active individual ransomware strains than any other year. We do not believe this indicates the growth of the overall ransomware players, but rather the increase in rebranding efforts in this space - in fact, our data suggests that the ecosystem of ransomware players is relatively contained. Cybersecurity researchers have increasingly noted instances of ransomware attackers publicly claiming to cease operations, only to relaunch later under a new name — the giveaway is usually similarities in the ransomware's code, as well as intelligence gathered from cybercriminal forums and blockchain analysis. So, while at least 140 ransomware strains were active at 2021, many of those strains were in fact run by the same cybercriminal groups. This is a trend we've continued to see in 2022.

This chart shows the dramatic increase in the number of active ransomware strains by year.

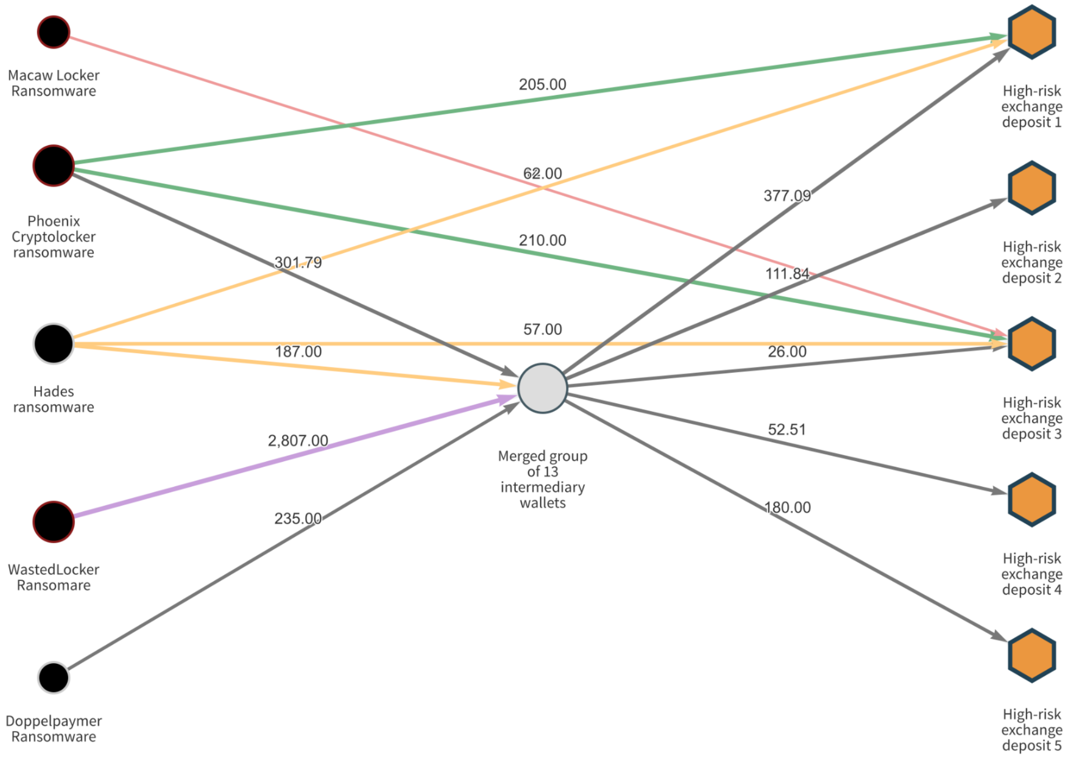


These strains attempt to create the illusion that they belong to different cybercriminal organizations by setting up separate victim payment sites and other infrastructure, but share similarities in their code, as well as in their cryptocurrency footprint. Evil Corp, a Russia-based cybercriminal gang behind several ransomware attacks in recent years, has launched several rebranded strains throughout its history, including Doppelpaymer, Bitpaymer, WastedLocker, Hades, Phoenix Cryptolocker, Grief, Macaw, and PayloadBIN. This rebranding trend is likely an attempt to stay under law enforcement's radar and obfuscate connections to designated strains so that victims will be more likely to pay, unaware of the potential sanctions risks. This is especially true after larger attacks may have drawn attention. In Evil Corp's case, their 2019 addition to the US Department of Treasury's Office of Foreign Assets Control's (OFAC's) Specially Designated Nationals And Blocked Persons List (SDN List) has also likely driven some of their rebranding efforts.

The growing number of active ransomware strains by year can be explained in part by how quickly these strains morph into "new" strains with different names as ransomware groups work to rebrand. The predominant ransomware strains in 2013 endured almost four years, while in 2021 the average lifespan of a ransomware strain was just over two months.



Blockchain analysis is an important tool in investigating links between different ransomware groups and determining when rebranding may have occurred. Using Chainalysis Reactor, we can see evidence of some of these ransomware strains' common ownership in their cryptocurrency transaction histories.

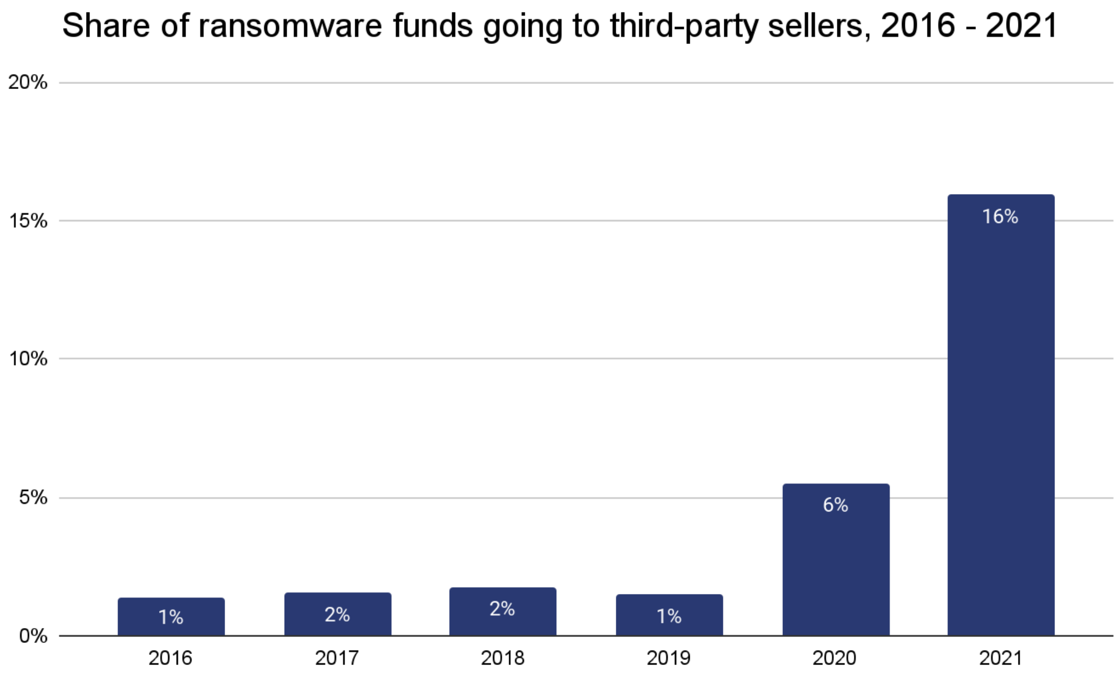

Macaw Locker Ransomware
Phoenix Cryptolocker ransomware
Hades ransomware
WastedLocker Ransomare
Doppelpaymer Ransomware
Merged group of 13 intermediary wallets
High-risk exchange deposit 1
High-risk exchange deposit 2
High-risk exchange deposit 3
High-risk exchange deposit 4
High-risk exchange deposit 5
205.00
62.00
377.09
210.00
301.79
111.84
57.00
187.00
26.00
2,807.00
52.51
235.00
180.00

This Chainalysis Reactor graph shows the money laundering process for five of the Evil Corp ransomware strains we mentioned above. While all of them appear to be run by separate organizations, most send funds derived from attacks to the same group of intermediary wallets, and from there move funds to many of the same deposit addresses at high-risk exchanges.

The uptick in ransomware rebranding is an important reminder that the ransomware ecosystem is smaller than it appears at first glance. While new strains pop up all the time, many of them are ultimately run or deployed by the same groups and individuals, all of whom are likely feeling the pressure from law enforcement's increasing efforts to prevent attacks, seize extorted funds, and arrest the individuals responsible. Rebranding is one way of evading those efforts, and suggests that investigators and cybersecurity professionals may be best served by studying ransomware attackers at the actor and organizational level, and focusing less on the unique strains.

Reinvestment into ransomware campaigns

The share of ransomware funds going to third-party sellers from ransomware operators spiked to its highest ever levels in 2021, suggesting ransomware actors increasingly reinvesting their ill-gotten funds into additional ransomware campaigns.



In 2021, 16% of all funds sent by ransomware operators were spent on tools and services used to enable more effective attacks, compared to 6% in 2020. While it's possible some of that activity constitutes money laundering rather than the purchase of illicit services, we believe that increasing use of those services is one reason ransomware attackers became more effective in 2021, as evidenced by rising average victim payment sizes.

Next, we outline several of the most well-known ransomware groups, all Ransomware as a Service groups, some that have utilized the rebranding strategy and have had a devastating impact: Conti, DarkSide, and NetWalker.

Conti Ransomware

Conti was the biggest ransomware strain by revenue in 2021, extorting at least $200 million from victims. Believed to be based in Russia, Conti operates using the RaaS model, meaning Conti's operators allow affiliates to launch attacks using its ransomware program in exchange for a fee or percentage of the ransom. 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.

Conti has made the news several times in the past year. After the Russian invasion of Ukraine, Conti announced its support for the Russian government: "If anybody will decide to organize a cyberattack or any war activities against Russia, we are going to use our all possible resources to strike back at the critical infrastructures of an enemy." Conti suffered a series of leaks of years'-worth of internal chats, revealing insights into their operations, roles, monikers, and cryptocurrency wallets. Since then, several cybercrime and hacktivist groups have publicized their support for the Russian Federation.

In April 2022, the Costa Rican government was faced with a series of cyber attacks from Conti ransomware group on multiple government agencies. In May, Costa Rican President Rodrigo Chaves declared a national emergency as a result of these attacks, which have affected 27 government institutions, including municipalities and state-run utilities.

At the end of May 2022, Conti allegedly shut down their operations. Other reports indicate, however, that they are likely rebranding and infiltrating existing strains.

DarkSide Ransomware

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. In this case, however, the Colonial Pipeline also turned into a success story, as the US Department of Justice was able to track and seize $2.3 million of the $4.4 million ransom that Colonial paid to DarkSide, demonstrating that when law enforcement has access to the right training, tools, and resources, they are able to effectively combat the ransomware threat.

NetWalker Ransomware

In January 2021, one of the most prominent strains of 2020, NetWalker was taken down by US law enforcement, in coordination with Canadian and Bulgarian authorities. The NetWalker tor domain was seized and a prolific affiliate, Sebastien Vachon-Desjardins, was arrested in Canada. Canadian authorities seized slightly less than 720 Bitcoin, over $27 million dollars worth of cryptocurrency. Vachon-Desjardins was extradited from Canada to the United States in March 2022. Vachon-Desjardins has since pleaded guilty.

Money laundering and ransomware

Another important trend to monitor in ransomware is money laundering. Over the last few years, most ransomware strains have laundered their extorted funds by sending them to higher risk offshore exchanges that tend to have relaxed compliance procedures. The money laundering trends get even more interesting if we drill down to the individual services receiving funds from ransomware. Interestingly, since 2020, about half of ransomware funds sent from ransomware addresses have wound up at one of six cryptocurrency businesses.

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. This will require international collaboration to implement strong AML/CFT laws around the world for cryptocurrency businesses. By requiring robust AML/CFT regimes and providing adequate supervision of cryptocurrency businesses, governments can help to stem the ability of illicit actors exploiting cryptocurrency to cash out their ill-gotten funds.

We also see substantial funds sent to both mixers. To offset Bitcoin's traceable properties, threat actors have increasingly incorporated mixers, also known as tumblers, into their laundering regimen. Some are even integrating mixing services directly into the ransomware payment platform in an attempt to obfuscate the destination of the ransomware proceeds. It will be important for government agencies to invest in technologies and resources that can mitigate obfuscation provided by mixers and help unmask illicit actors.

We assess that Bitcoin remains the cryptocurrency used in the overwhelming majority of ransomware payments. Monero, a privacy coin,[1] is more challenging to use than Bitcoin. Monero also lacks the liquidity to be able to easily source the large sums demanded in ransomware attacks, as many exchanges do not list it. In addition to Bitcoin, we are also tracking an increase in ransomware strains demanding ransoms paid in Monero. Only a handful of ransomware strains demand Monero exclusively, and nearly all strains accept Bitcoin payments as an alternative, albeit often at a premium. This trend underscores the need for US agencies to invest in research and resources that will allow them to trace privacy coin transactions.

What is the sanctions nexus to ransomware?

Over the past few years, a number of ransomware groups and facilitators have been designated by OFAC. This has been very effective in shutting down the flow of funds to designated entities and individuals, in particular when cryptocurrency addresses have been included as identifiers. Due to the designations of ransomware actors, these SDNs are less likely to receive payments due to the inherent risk of a sanctions violation and the capacity of compliant cryptocurrency businesses to screen for sanctioned individuals and their cryptocurrency addresses.

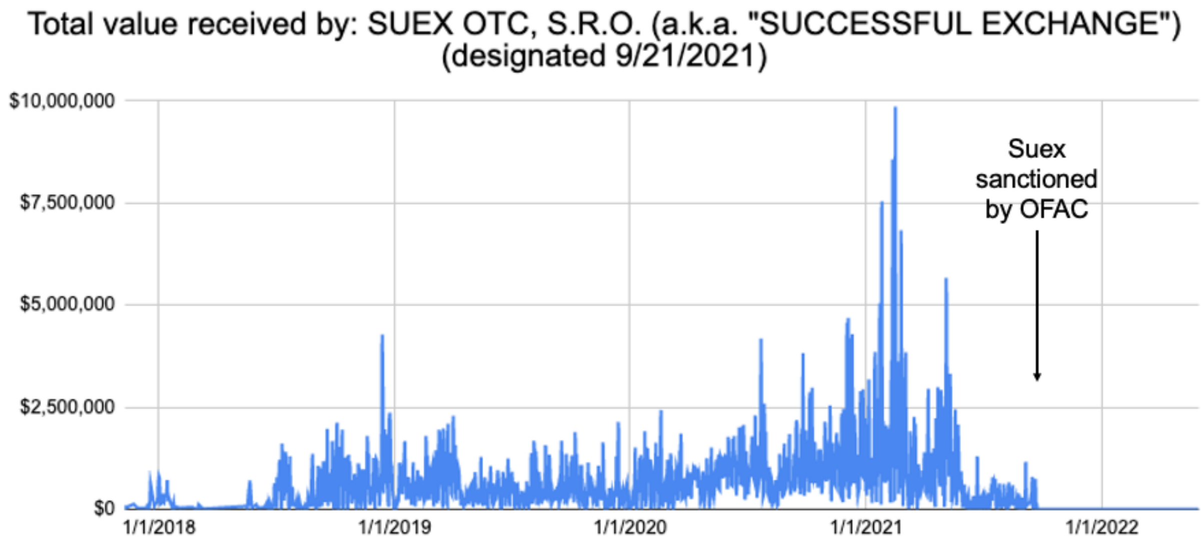
In October 2020, OFAC released an advisory warning that making ransomware payments could result in a sanctions violation for victims or companies that facilitate payments to designated ransomware actors. The facilitation point is important, as there's a robust industry of consultants who help ransomware victims negotiate with and pay ransomware

[1] Privacy coins are cryptocurrencies that preserve anonymity by obscuring the flow of money across their networks.

attackers. The advisory cited examples of ransomware actors who have been designated by OFAC, such as the two Iranian nationals who laundered proceeds from the SamSam ransomware strain. As previously mentioned, ransomware group Evil Corp was also designated by OFAC, and we know that they have rebranded a number of times since then. October's advisory bolsters previous government guidance and notes that paying ransom may incentivize future attacks and warns that ransomware victims and consultants who help facilitate payments could face the heavy penalties associated with sanctions violations.

More recently, OFAC has designated several cryptocurrency businesses that were known for facilitating money laundering for ransomware groups and other illicit actors. This approach of going after not just bad actors but their facilitators helps to limit and cut off their cash out points.

On September 21, 2021, OFAC announced sanctions against Suex, a Russia-based cryptocurrency Over The Counter (OTC) broker 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 cryptocurrency into Suex's addresses included as identifiers on the SDN List dropped to effectively zero. Suex's designation represents a significant blow to many of the biggest cyber threat actors operating today, including leading ransomware attackers, scammers, and darknet market operators.



On November 8, 2021, OFAC designated Chatex, a virtual currency exchange, and its associated support network, for facilitating financial transactions for ransomware actors. OFAC also designated two ransomware operators, Yaroslav Vasinskyi and Yevgeniy Polyanin "for their part in perpetuating Sodinokibi/REvil ransomware incidents against the United States. Vasinskyi deployed ransomware against at least nine US companies. Vasinskyi is also responsible for the July 2021 ransomware activity against Kaseya, which caused significant disruptions to the computer networks of Kaseya's customer base. Polyanin also deployed ransomware, targeting several US government entities and private-sector companies. These two individuals are part of a cybercriminal group that has engaged in ransomware activities and received more than $200 million in ransom payments paid in Bitcoin and Monero.

On April 5, 2022 OFAC designated two Russia-based services, including Hydra, a darknet market and Garantex, a cryptocurrency exchange. Garantex was associated with illicit actors and darknet markets, receiving nearly $6 million from Russian RaaS ransomware group Conti and also approximately $2.6 million from Hydra. And most recently, on May 6, 2022, OFAC designated Blender.io, a cryptocurrency mixer, citing their involvement in facilitating money-laundering for ransomware groups, including Trickbot, Conti, Ryuk, Sodinokibi, and Gandcrab.

Compliant cryptocurrency exchanges have proven effective at stopping the flow of funds to OFAC SDNs where cryptocurrency wallet addresses are included as identifiers in their designation. Sanctions are particularly effective in disrupting financial intermediaries in the cryptocurrency ecosystem because once such an intermediary is designated, funds associated with it can be broadly flagged to compliant participants in the network due to the transparency of the blockchain, and therefore easier to prevent further exposure to the designated network.

Ransomware as a geopolitical weapon

While most ransomware attacks appear to be financially motivated, some appear to conduct attacks that align with geopolitical objectives or employ ransomware as a cover for these goals. Researchers have identified nation states launching ransomware attacks as a cover for espionage and have even reported wiper attacks masquerading as ransomware for plausible deniability.

Some of the most pervasive strains avoid targeting Commonwealth of Independent States (CIS), including Russia, and will fail to encrypt if they detect the operating system is located in a CIS country. And where that fails, ransomware operators have been identified returning decryptors in cases of inadvertent targeting of Russian entities. This suggests at least a tacit tolerance of financially motivated ransomware activities by the Russian government. For example, the Russian government has been very reluctant to pursue these groups. In January 2022, Russia arrested 14 alleged members of the REvil ransomware gang, but just this month reports indicated that they intended to drop most of the charges. In other cases, ransomware groups like Evil Corp have been explicitly tied to the Russian government.

Individuals and groups based in Russia — some of whom have been sanctioned by the United States in recent years — account for a disproportionate share of activity in several forms of cryptocurrency-based crime. Chainalysis data suggests roughly 75% of ransomware revenue in 2021 went to strains we can say are highly likely to be affiliated with Russia in some way.

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.

As the Computer Emergency Response Team of Ukraine (CERT-UA) describes here, a cyber attack occurred on January 13, 2022, disrupting several government agencies' ability to operate. The attack appeared like a ransomware incident, replete with a note and cryptocurrency address provided for payment, that actually belied a malicious wiper that was deleting data at Ukrainian entities known as WhisperGate. Interestingly, CERT-UA released a report showing that the wiper contains code repurposed from WhiteBlackCrypt, a ransomware strain active in 2021 that was also designed to wipe victims' systems rather than extort them for money.

The gambit shows how far state actors using ransomware to attack foes will go to conceal their attacks' origins and maintain plausible deniability but also leaves clues on the blockchain that can aid in attribution to investigations. We saw a similar situation unfold in 2017, when the Russia-based NotPetya ransomware strain, which contained no viable payment mechanism, targeted several Ukrainian organizations and was also widely judged to be a geopolitically motivated disruption attempt by the Russian military rather than a money-making effort.

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 US, the EU, and Israel, are geared more toward causing disruption or serving as a ruse to conceal espionage activity. Generally speaking, Chainalysis has seen significant growth over the last year in the number of ransomware strains attributed to Iranian cybercriminals in the past year.

To be clear, many of those Iranian ransomware strains are used for financially motivated attacks by cybercriminals operating in the country. Iran has a highly educated population but limited occupational opportunities, which likely contributes to the allure of ransomware. However, other strains behave more like tools of espionage, extorting negligible amounts of cryptocurrency from victims. Other analysts have previously identified instances of strains affiliated with China, such as ColdLock, carrying out similar geopolitical attacks on Taiwanese organizations.

Ransomware is a useful cover for strategic denial and deception against enemy states because attacks can be carried out cheaply, and it gives the attacking nation some measure of plausible deniability, as they can always claim the attack was carried out by mere cybercriminals or another nation state. But even ransomware attacks carried out for non-financial reasons leave a trail on the blockchain. For that reason, it's crucial that agencies focused on national security understand how to trace funds using blockchain analysis, as this is the key to identifying the individuals involved in the attacks themselves, the tools they use, and how they launder any funds obtained from victims.

Recommendations

Given the recent increase in ransomware attacks, as well as their potentially devastating impacts, Chainalysis believes it is important to enact meaningful policies to deter, detect, and disrupt ransomware. We support the numerous on-going ransomware initiatives and believe the foundation of US policies must be a comprehensive, whole-of-US government strategy leveraging collaborative private-public sector partnerships and information sharing for reducing ransomware attacks. We believe that clear guidance and direction will enable a unified inter-agency response and facilitate government agencies to work more effectively with the private sector to combat this important issue and protect US national security interests. This threat is too big for one agency or entity to attack themselves -- it must be a concerted joint public-private effort with strong, unequivocal leadership. I outline below some specific recommendations for policymakers to consider when contemplating legislation and strategies to combat ransomware.

Improve ransomware reporting and information sharing

In order to disrupt the existing ransomware ecosystem, it is important to improve and standardize ransomware reporting to empower policymakers and US government agencies with the data they need to investigate, attribute, and disrupt the ransomware supply chain. Cryptocurrency addresses from extortion demands are a valuable investigative lead with unique potential for attribution and disruption of criminals; therefore, wallet information should be shared with blockchain investigators to operationalize, but also kept safeguarded amongst investigative professionals and data platforms. Threat actors have been identified abusing publicly available addresses to enhance their laundering, and some have taken to threatening retaliation against victims for sharing details related to the incident.

Information sharing should be improved and reporting incentivized. Information is not currently shared in a consistent or reliable manner, and it does not always reach a broad enough audience. As this Committee noted in its report, there is currently underreporting of ransomware events, which obfuscates the true scope of the issue and means that law enforcement does not have all of the necessary information to prioritize and investigate ransomware events.

Mechanisms for sharing information related to ransomware incidents should be improved and developed. Information sharing networks – within the government, and between the government and the private sector, and between governments – would improve the quality and volume of information about ransomware incidents. Government agencies should routinely share advisories that include information about ransomware threat actors' tactics and techniques, indicators of compromise, and other ransomware trends would also allow the private sector to better identify and protect itself against potential attacks, as well as raise awareness, which would likely promote increased reporting.

Additionally, the US government should provide guidance to the private sector about reporting requirements for victims and incident response firms to standardize reporting fields and expedite sharing with pertinent law enforcement entities. Currently victims are directed to report ransomware incidents to CISA, FBI, or Secret Service, and incident response firms that qualify as MSBs may file incident information to Treasury through Suspicious Activity Reports (SARs) per guidance from FinCEN advisories. The multiple reporting channels and inconsistent reporting fields inhibit the actionability of the intelligence and slow efficient information sharing. In addition, some incident response firms have registered as MSBs and file suspicious transaction reports (SARs) on ransomware payments, but this intelligence is reportedly very slow to be shared with law enforcement agencies.

Ensure government agencies have adequate funding for the training, tools, and resources they need to conduct blockchain investigations.

As ransomware groups adopt further money laundering techniques, it's critical for the US government to keep up. Government agencies that have embraced blockchain analysis have seized millions of dollars in cryptocurrency and successfully shut down ransomware groups—further evidence that with the proper tools, investigators can cut ransomware groups off from their ill-gotten funds. Many government agencies have limited or inconsistent personnel dedicated to investigating the illicit use of cryptocurrency 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 cryptocurrencies are exploited by criminals, investigators can trace these illicit transactions, seize funds, and bring criminals to justice.

Improve coordination and collaboration between countries

Ransomware is a global issue and investigations often cross borders due to the global nature of cyber crime. We must improve information sharing and coordination between US government agencies and their counterparts in other countries. It is important that countries work together and with private industry to enable cross-border investigations of ransomware threats. Establishing and improving upon coordination and collaboration mechanisms between countries can help to streamline investigations and enable law enforcement to bring bad actors to justice.

Provide assistance to countries to support their implementation of robust AML/CFT laws for cryptocurrency businesses

The US should work with other countries to support their efforts to implement comprehensive Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) laws for cryptocurrency businesses to limit illicit actors opportunities for jurisdictional arbitrage. By requiring cryptocurrency exchanges, cryptocurrency kiosks, peer-to-peer exchangers, over-the-counter (OTC) trading “desks”, and other cryptocurrency businesses to implement robust AML/CFT laws, including Know Your Customer (KYC) laws, illicit actors will have fewer cashout opportunities to turn their ill-gotten cryptocurrency into fiat currency. The US government should provide assistance through the US Department of State and other mechanisms to other countries to assist in the development and implementation of these laws, as well as capacity building to enforce them. This will help to limit the regulatory arbitrage opportunities available to bad actors.

Allow for expanded definitions of malicious cyber activities that warrant reporting

As with all criminals, malicious cyber actors, including ransomware actors, routinely revise their tactics, techniques, and practices (TTPs) in order to evade law enforcement detection. Ransomware is a rapidly evolving ecosystem: everything from the tools and tactics used for exploitation, payment laundering mechanisms, variant names, extortion methods, and cryptocurrency types are all subject to change. Many of today’s ransomware threat actors have evolved from other forms of malicious cyber intrusions, and it is imperative to track these actors and activities as these intrusions morph and change outside of traditionally defined ransomware.

Investment into research that unravels the core tools and skills underpinning these attacks is vital to tracking and disrupting this crime. As such, we must account for expanded definitions of extortion that don’t necessarily involve encryption in our counter-ransomware policies, in order to maintain visibility and pressure on these actors amid any ongoing or future changes in tactics.

Pursue ransomware facilitators and enablers in order to have a broader impact on the ransomware ecosystem

It is imperative that governments around the world work together to track ransomware payments and shut off the exit ramps for financially motivated crime. However, a holistic counter-ransomware strategy must also encompass the entire ransomware kill chain by focusing on not only the end goal of extortionists - the ransomware payment itself - but also the “how.” The suppliers of tools and services further up the kill chain that enable the ransomware ecosystem to thrive are important to understand. The same supply chains of ransomware are the same ones that underpin other malicious cyber activity today, and greater capacity for executive agencies to have a full understanding of the landscape can surface critical centers of gravity for action that can ultimately impact how much ransomware gets perpetrated.

Conclusion

Ransomware isn’t just dangerous. It’s also one of the most dynamic, constantly changing forms of crime that exploits cryptocurrency. Ransomware is a crime that can threaten every aspect of our lives, from infrastructure and commerce, to national security risks. And while some argue that the nature of cryptocurrency facilitates the crime of ransomware, its nature also facilitates incomparable visibility that benefits law enforcement immensely. By incentivizing and encouraging the reporting of cryptocurrency addresses that are associated with known threat actors, and by providing the resources necessary to understand and combat them, law enforcement and the US government as a whole will be able to do more comprehensive analysis of ransomware attacks, provide better threat prevention assistance to the public, and protect the country from national security risks.