Ransomware 2021

Critical Mid-Year Update

May 2021

Table of Contents

Executive summary

Here's a summary of our key findings and takeaways on ransomware over the last two years:

- **Ransomware is a major growing cybersecurity issue for both the public and private sectors**. Known payments to ransomware attackers rose 337% from 2019 to 2020, when they reached over $400 million worth of cryptocurrency. Attackers show no signs of slowing down in 2021, and have already taken in more than $81 million from victims so far this year. It's important to keep in mind that these are low-end estimates, and that the true numbers are almost certainly higher.

- **Ransomware payments can create sanctions risk for victim organizations and companies that help them facilitate payments.** Chainalysis found that 13% of known ransomware payments in 2020 carried sanctions risk. So far, that number is down to 3% in 2021.

- **The average ransom payment has grown significantly.** In Q4 2019, the average ransomware payment we tracked was just $12,000 worth of cryptocurrency. In Q1 2021, the average payment size was $54,000. We believe this is due in part to ransomware attackers more effectively targeting larger organizations with the help of illicit, third-party vendors who sell them hacking tools, stolen data, and other assets to carry out more successful attacks.

- **More ransomware attacks appear to be carried out by cybercriminals in Russia and other Commonwealth of Independent States (CIS) countries.** We compared the top ten most prolific ransomware strains in 2020 and 2021, and found that the share of funds extorted by ransomware strains associated with cybercriminals based in Russia or other CIS countries has grown this year.

- **The United States government's ransomware policies must continue to evolve.** U.S. government agencies and policymakers have taken positive steps to address the ransomware issue. We examine these steps and make further policy recommendations in this report.

Keep reading to learn about these developments and other key trends in ransomware.

Introduction

When we published our latest Crypto Crime Report a few months ago, we noted that ransomware was 2020's fastest-growing segment of cryptocurrency-related crime, with victim payments to attackers growing 311% to reach nearly $350 million worth of cryptocurrency. Since then, Chainalysis joined the Institute for Security and Technology's Ransomware Task Force, alongside other technology providers like Amazon, Cisco, FireEye, McAfee, and Microsoft and government agencies like CISA, FBI, and the Secret Service. Together, the task force put out a report sizing up the ransomware problem and making recommendations on how governments around the world can address it. We're proud of this work and believe it is a great start in defining the problem and putting solutions in place to tackle it.

However, ransomware has only become more serious in recent months. Since publishing the Crypto Crime Report, Chainalysis has identified more active ransomware addresses and revised our estimate for the total amount of ransomware payments in 2020 to over $400 million. As we mentioned in our original report, this estimate is a lower bound of the true total, as this only includes payments our team has confirmed, and underreporting means we likely haven't categorized every victim payment in our datasets. Our data improves over time, and so we anticipate this estimate will continue to rise.

Further, ransomware attackers are becoming more sophisticated and more brazen in 2021, commanding larger ransoms from high-profile victims including:

- Airplane manufacturer Bombadier, attacked by Clop
- Computer maker Acer, attacked by REvil
- Washington D.C. Police Department, attacked by Babuk
- Oil pipeline operator Colonial Pipeline Company, attacked by DarkSide

The ongoing rise in attacks shows that it's more important than ever for governments, cybersecurity practitioners, financial institutions, and cryptocurrency businesses to work together against ransomware. This was recently recognized by the Biden Administration, which issued an executive order that proposes plans to improve the nation's cybersecurity by modernizing cybersecurity defenses and protecting federal networks, improving information-sharing between the U.S. government and the private sector on cyber issues, and strengthening the United States' ability to respond to incidents when they occur.
We hope this ransomware research report can support those goals. Inside, you'll find updated numbers on overall victim payments and the activity of the most prolific strains, as well as a breakdown of emerging trends and a few policy recommendations that may be helpful to regulators and policymakers.

If your company suffers a ransomware attack, we encourage you to follow the steps outlined by CISA, who may be able to provide specific guidance to help evaluate and remediate ransomware incidents. You can also request threat response assistance by contacting your local FBI Field Office or United States Secret Service Office. Reporting the incident, which includes providing essential information such as cryptocurrency addresses provided by the attackers, is the only way to ensure law enforcement entities can effectively investigate your attack and, in the long term, understand the scope of the wider ransomware issue so that others are less likely to be attacked in the future.

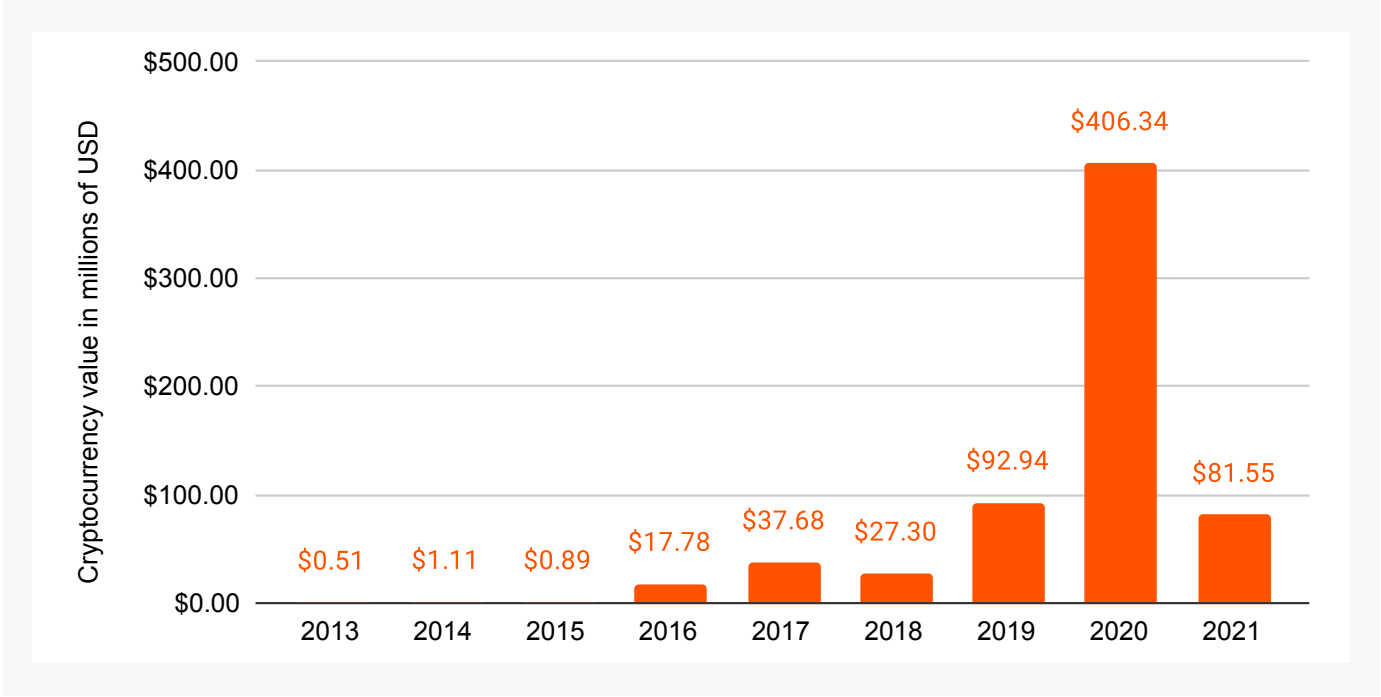
Thank you,

Don Spies
Director of Strategic Initiatives
Chainalysis

Ransomware in 2021 YTD

Ransomware exploded in 2020 and shows no signs of slowing down nearly five months into 2021.

Total cryptocurrency value received by ransomware addresses | 2016 - 2021 (YTD)



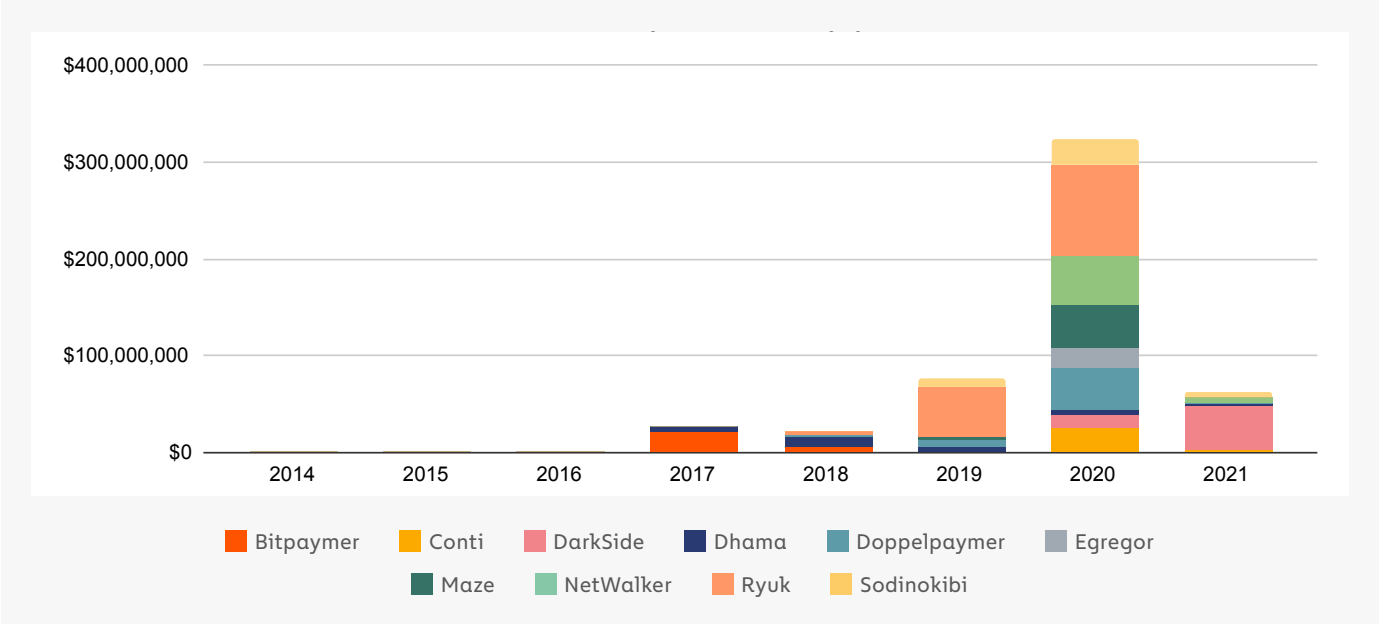
Currencies included: BCH, BTC, ETH, USDT

When we published the 2021 Crypto Crime Report in February, blockchain analysis showed that the total amount paid by ransomware victims increased by 311% in 2020 to reach nearly $350 million worth of cryptocurrency. No other category of cryptocurrency-based crime had a higher growth rate. However, we warned readers that that number was likely a lower bound of the true total. Sure enough, since publishing, we've identified new ransomware addresses with payments we'd yet to count, and now know that ransomware victims paid over **$406 million** worth of cryptocurrency to attackers in 2020. Again, that number will continue to grow as we discover more ransomware addresses.

As of May 10, 2021, we know that ransomware attackers have taken in at least $81 million worth of cryptocurrency from victims. Again though, $81 million must be considered a floor for the time being, as the figure will almost certainly grow as we identify more ransomware addresses.

The increase in ransomware starting in 2020 has been driven by a number of new strains taking in large sums from victims, as well as a few pre-existing strains increasing earnings.

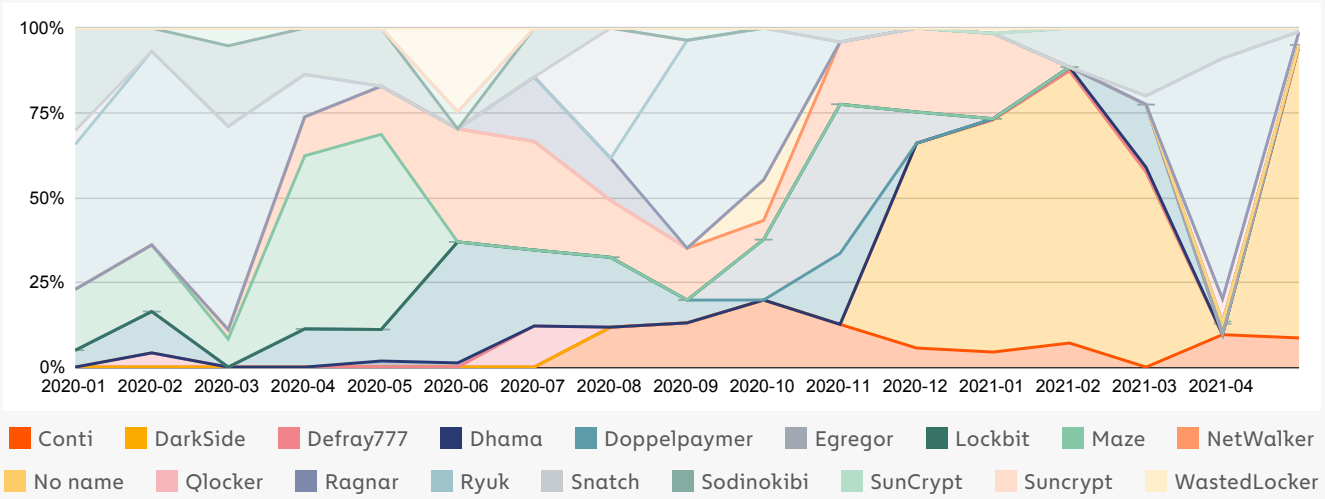
Top 10 ransomware strains by revenue by year | 2014-2021 Q1



Currencies included: BCH, BTC

Ransomware strains don't operate consistently, even month-to-month. Below, we see that the top-earning strains have ebbed and flowed from the beginning of 2020 to the present, based on our current data and address attributions.

Ransomware lifecycles: top monthly strains by share of all ransomware payments | 2021-present

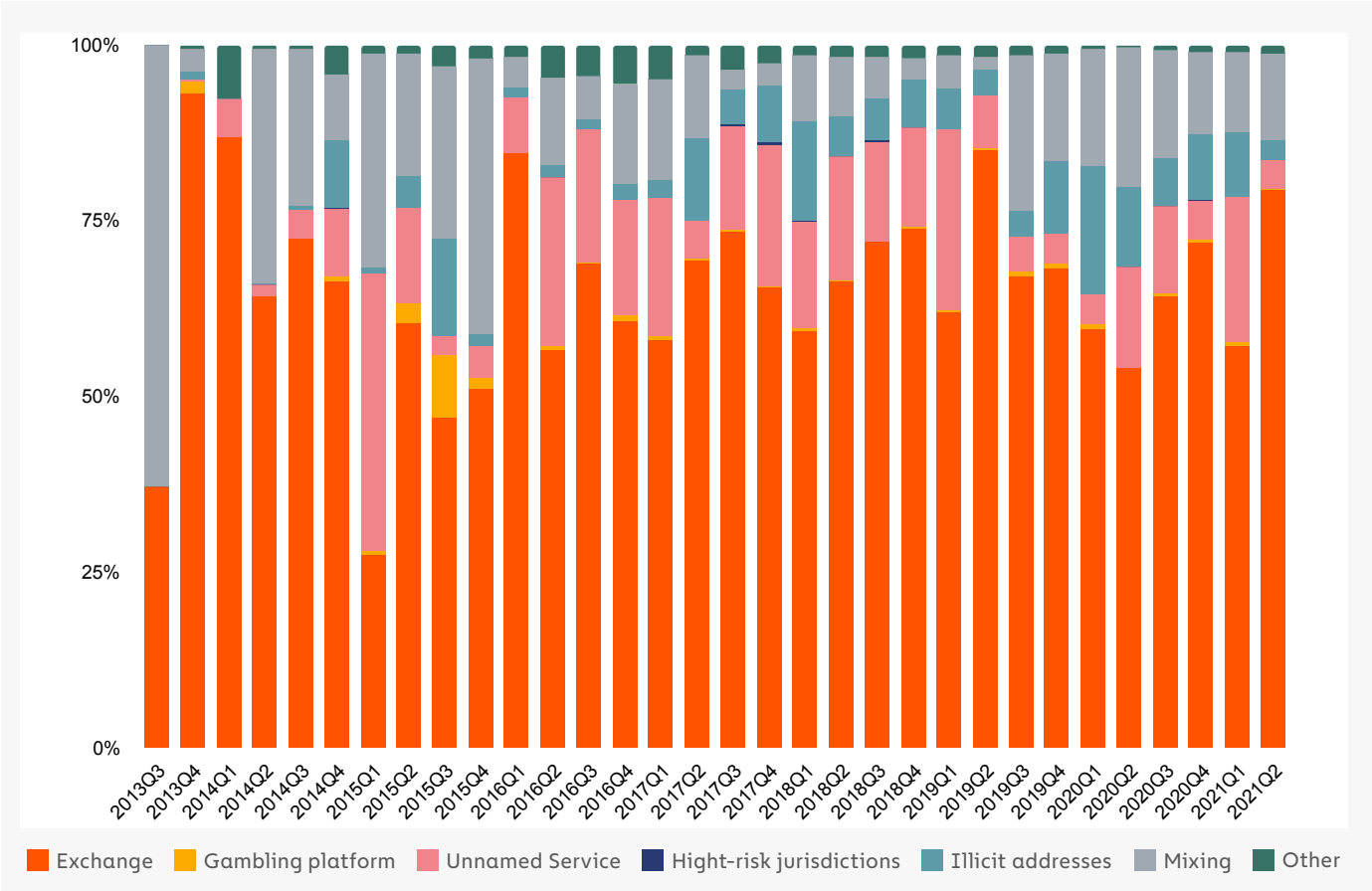


Currencies included: BTC

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

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

Destination of funds leaving ransomware wallets | 2013 Q3 - 2021 Q1



Currencies included: BTC, BCH, ETH

Ransomware attackers move most of the funds taken from their victims to mainstream exchanges, high-risk exchanges (meaning those with loose to non-existent compliance standards), and mixers.

Sanctions risk in ransomware

In October 2020, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN) released separate advisories related to ransomware payments that could be a sanctions violation for victims or financial intermediaries who facilitate payments for victims. The facilitation point is important, as there is a robust industry of consultants and subject matter experts (SMEs) who help ransomware victims negotiate with, and pay, ransomware attackers. The OFAC alert cited examples of ransomware creators and attackers who have been put on the OFAC sanctions list, such as the two Iranian nationals who laundered proceeds from the SamSam ransomware strain.

OFAC's alert bolsters previous government guidance not to pay ransomware attackers, as this incentivizes future attacks. However, OFAC's alert goes a step further in warning that ransomware victims and consultants who help them make payments could face the heavy penalties associated with sanctions violations. It also notes that license applications made to OFAC that involve ransomware payments demanded as a result of malicious cyber-enabled activities would be reviewed by OFAC, but with a presumption of denial.

To some industry members, this appeared to create a "catch-22" where ransomware victims were forced to choose between paying the ransom and possibly suffering an additional penalty in the form of OFAC sanctions, or not paying the ransom and suffering the loss of their data and the resulting financial and reputational harm. It also arguably created a disincentive for ransomware victims to do their due diligence in determining whether a ransomware payment would, in fact, open the victim or its financial intermediary to OFAC sanctions based on the attacking strain.

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

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

- Payments to addresses identified by OFAC as belonging to sanctioned individuals (note: this includes payments made before the addresses were actually sanctioned).
- Payments to addresses connected to ransomware strains whose creators have been sanctioned by OFAC.

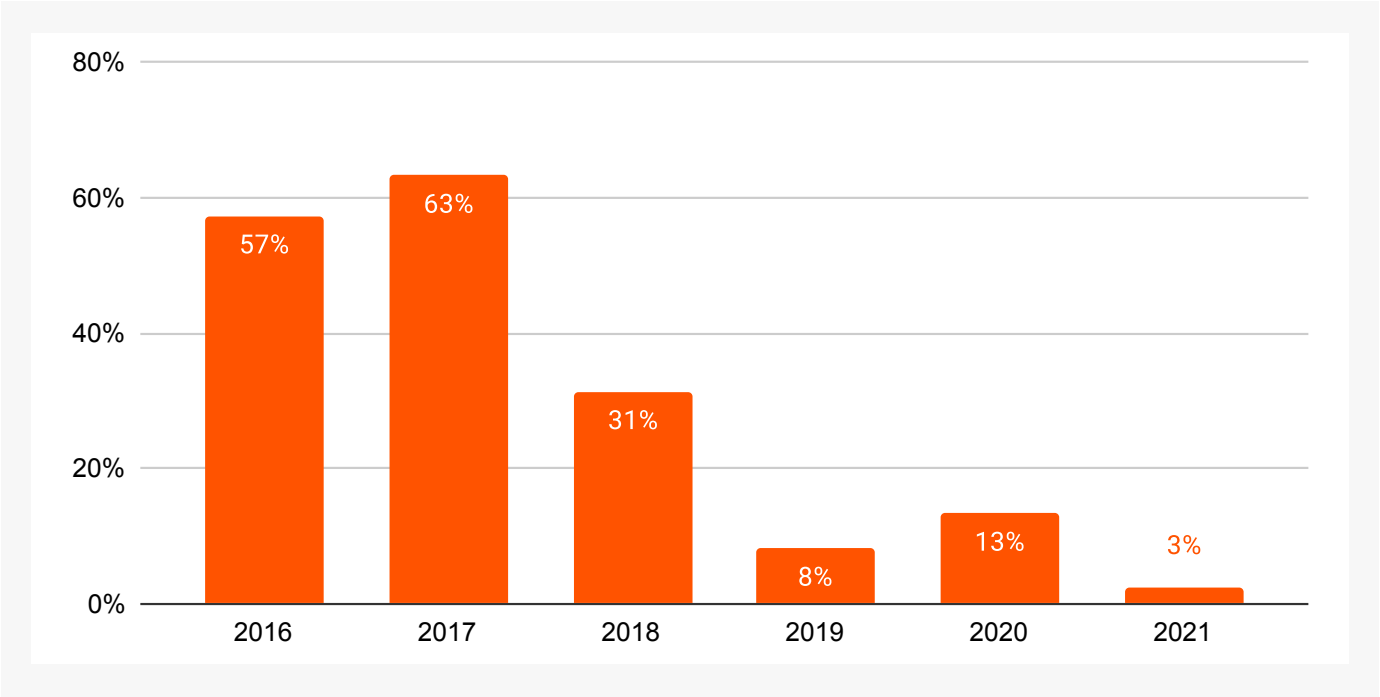
- Payments to addresses connected to ransomware strains associated with cybercriminals based in heavily sanctioned jurisdictions such as Iran and North Korea.

Those criteria cover the following ransomware strains:

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

Based on those designations, we found that 13% of all known ransomware payments made in 2020 carried a risk of sanctions violations. This was quite low compared to some previous years. Please keep in mind that this represents a slight decline from our initial reports stating that 15% of 2020 ransomware payments carried sanctions risk. The reason for the change is the removal of the Clop ransomware strain from the list of strains with suspected sanctions risk, following more recent reporting from cybersecurity firm FireEye.

Share of known ransomware payments associated with OFAC designations and other sanctions risk | 2016 - 2021 (YTD)



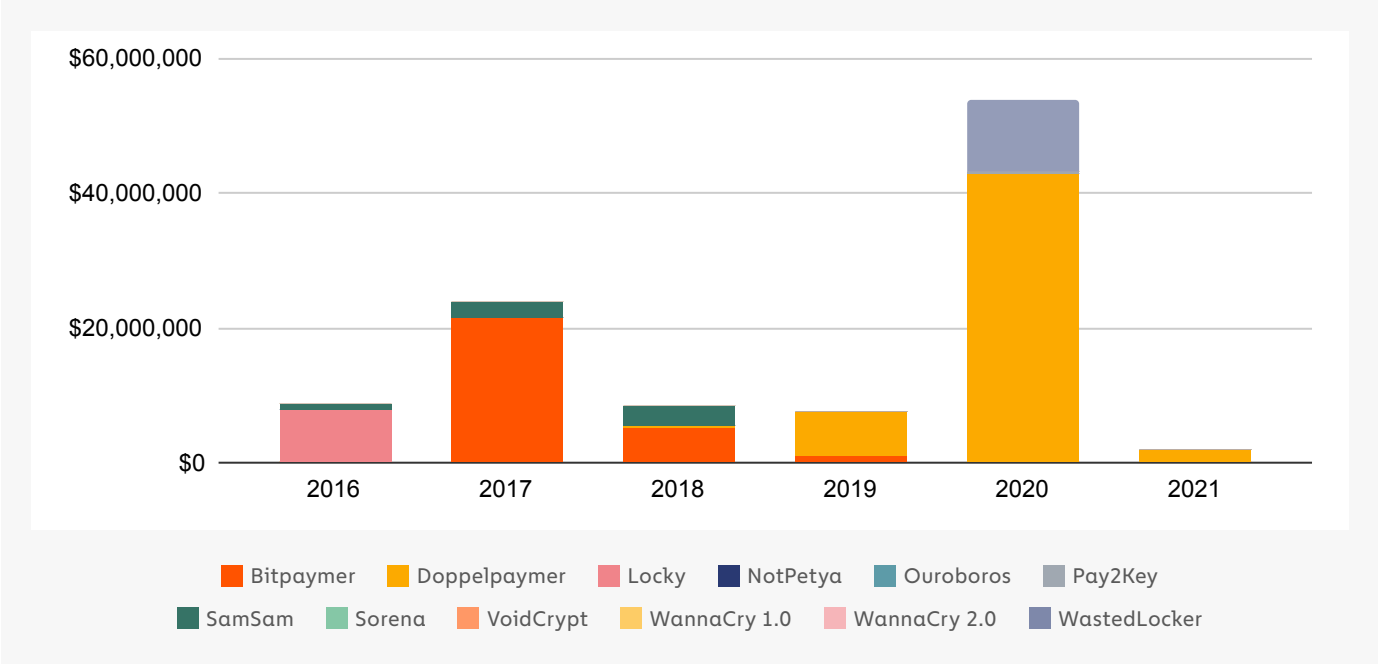
Please note that all payments to addresses associated with OFAC-sanctioned individuals or groups noted on this chart took place before those individuals or groups were added to the OFAC sanctions list.

Currencies included: BCH, BTC, ETH, USDT

Because overall ransomware payments increased in 2020, the dollar figure for ransomware payments with sanctions risk skyrocketed last year. Importantly, however, the actual rate of sanctions risk in known ransomware payments declined significantly in 2019 and 2020 from much higher figures in 2018 and prior. Based on what we know now, the current rate is much lower in 2021, with only 3% of known ransomware payments so far this year carrying sanctions risk. At this rate, the raw value paid to ransomware addresses with sanctions risk would be expected to fall even further. This trend could change if emerging strains receiving payments are connected to potential sanctions nexuses or if OFAC were to designate additional addresses. For instance, we've noticed that some Iranian strains have resurfaced recently under new names to disguise their connections to organizations and individuals with sanctions risk. This makes ransomware payment due diligence using blockchain analysis solutions even more critical, as the ability to determine actual sanctions risk improves while the amount of risk in each payment remains low.

Below, we show the yearly volume of known ransomware payments that constitute sanctions violation risk, broken down by strain.

Total value received by ransomware addresses associated with sancton risk by ransomware strain | 2016 - 2021



Currencies included: BCH, BTC

Nearly all of the known ransomware payments with sanctions risk in 2020 and 2021 went to Doppelpaymer and WastedLocker. In previous years, Bitpaymer, SamSam, and Locky have also been responsible for a high volume of ransomware payments associated with sanctions risk. We should also note that there are reports of increased activity from Iranian ransomware strains with sanctions risk in 2021, though our data doesn't yet confirm this trend.

Dealing with a ransomware attack is incredibly stressful. In cases where hospitals and other critical infrastructure systems have been attacked, lives have been at risk where computer systems were rendered inoperable. It is imperative that businesses and government entities prepare in advance so that during a stressful situation, a plan is already in place. Having a ransomware response plan that includes working with SMEs, who can coordinate with law enforcement and perform the necessary blockchain analytics on proposed payments to avoid sanctions violations, is critical. Further policy recommendations around ransomware and sanctions risk are provided below.

Case study: Netwalker

Earlier this year, the U.S. Department of Justice (DOJ) announced a coordinated international law enforcement action to disrupt the Netwalker ransomware strain, including the seizure of nearly half a million dollars in cryptocurrency, the disablement of a dark web resource used to communicate with Netwalker ransomware victims, and the arrest of a Canadian national, Sebastien Vachon-Desjardins, who obtained tens of millions of dollars by acting as a Netwalker affiliate.

This case highlights the sophistication with which Netwalker operated, the global impact of ransomware attacks, and the substantial funds ransomware actors steal from their victims.

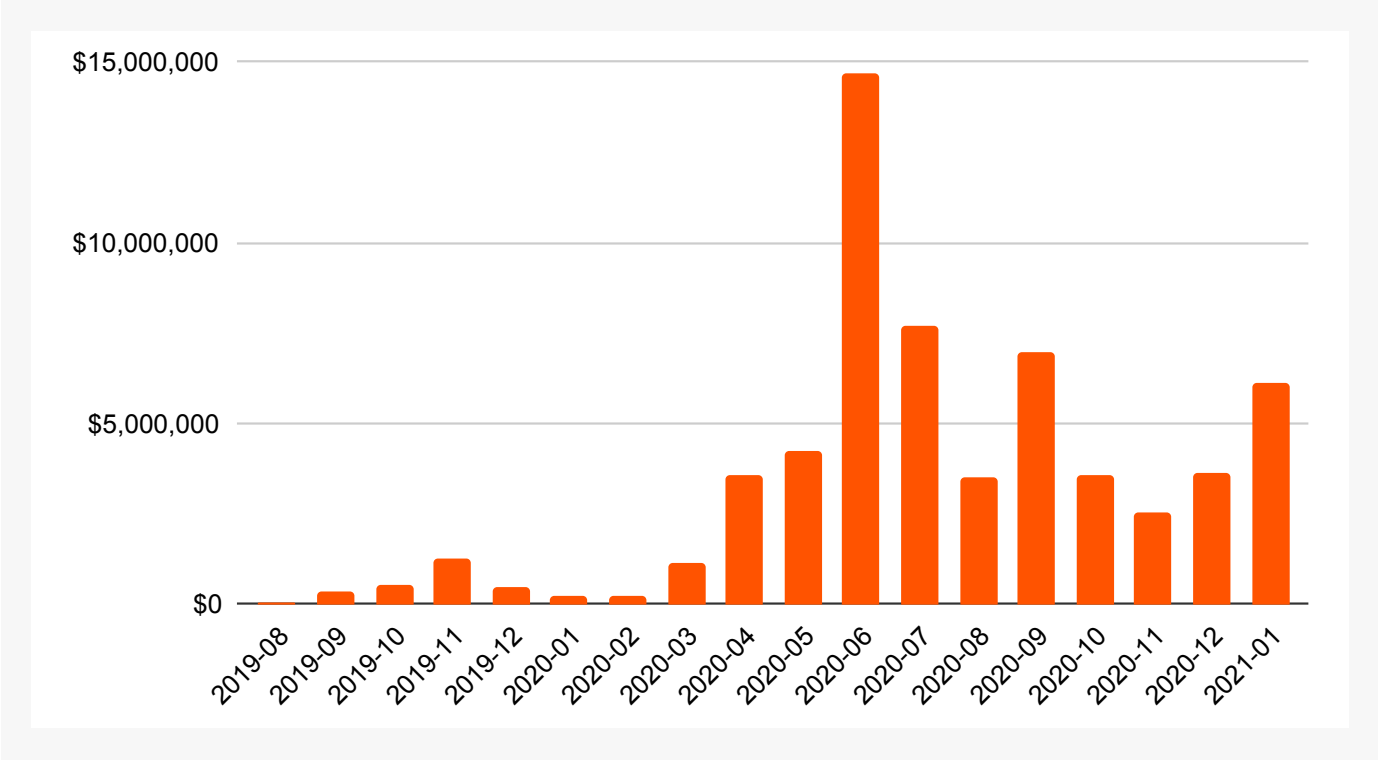
Seizure page of dark web hidden resource used to communicate with Netwalker ransomware victims. Source: *U.S. Department of Justice*

Below, we'll break down what blockchain analysis tells us about the Netwalker strain of ransomware and highlight specific elements of the investigation to show how law enforcement was able to trace the illicit funds.[1]

Like many strains, Netwalker functions on the (RaaS) model, in which attackers known as affiliates "rent" usage of a particular ransomware strain from its creators or administrators, who in exchange get a cut of the money from each successful attack affiliates carry out. RaaS has led to more attacks, making it even more difficult to quantify the full financial impact. But the trend is clear; no other category of cryptocurrency-based crime had a higher growth rate than ransomware in 2020.

Netwalker was a top ransomware strain by revenue in 2020, along with Ryuk, Maze, Doppelpaymer, and Sodinokibi. Chainalysis has traced nearly $94 million worth of funds in Netwalker ransoms, with payment dating back to 2018. It picked up steam in mid-2020, growing the average ransom to $33,000 last year, up from $7,000 in 2019. Payments stopped after the strain was taken down in late January of 2021.

Ransomware payments received by Netwalker | Monthly



[1] Chainalysis has a policy against commenting on active law enforcement cases prior to adjudication. However, an exception was made in this case after consultation and approval from our law enforcement partners.

According to U.S. authorities, Netwalker has impacted at least 305 victims from 27 different countries, including 203 in the U.S.

Hundreds of Netwalker victims around the world

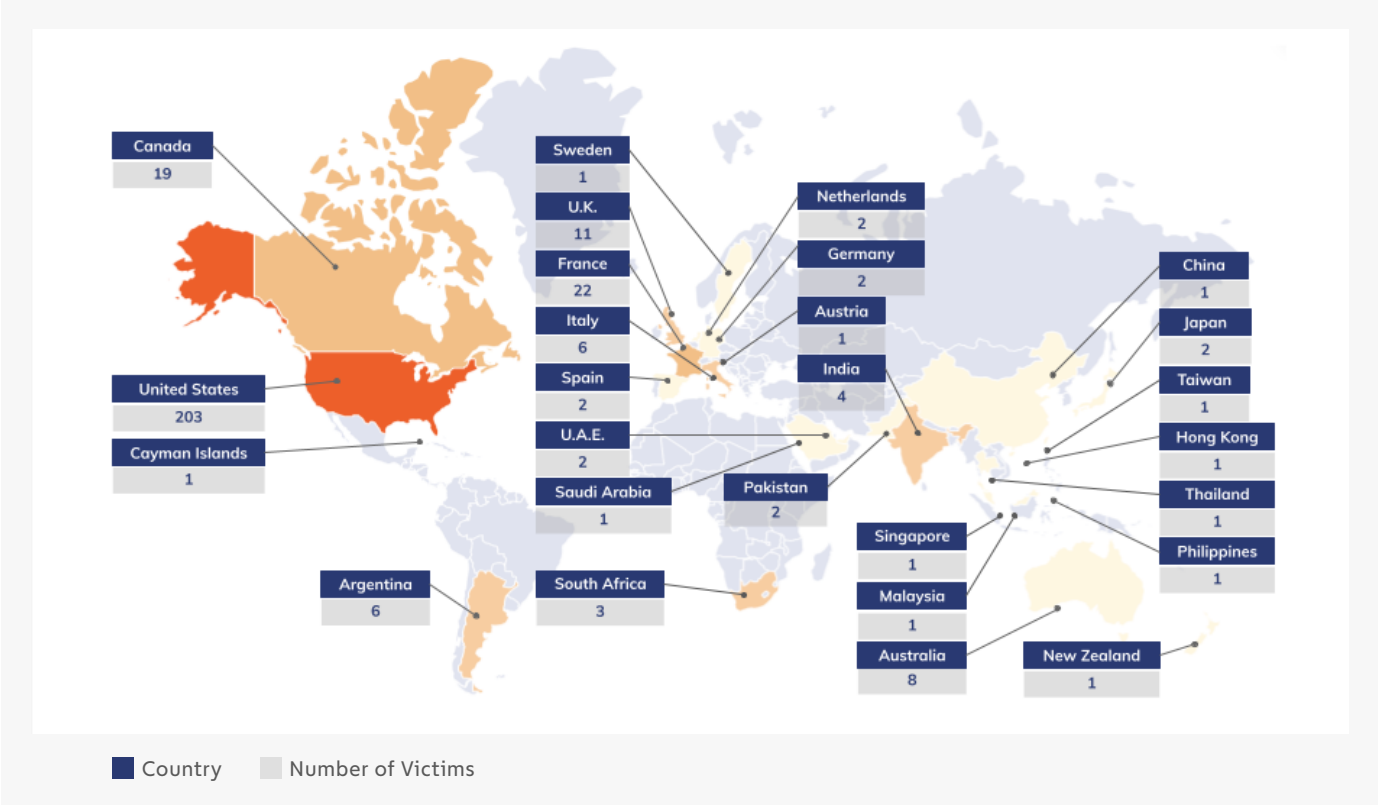
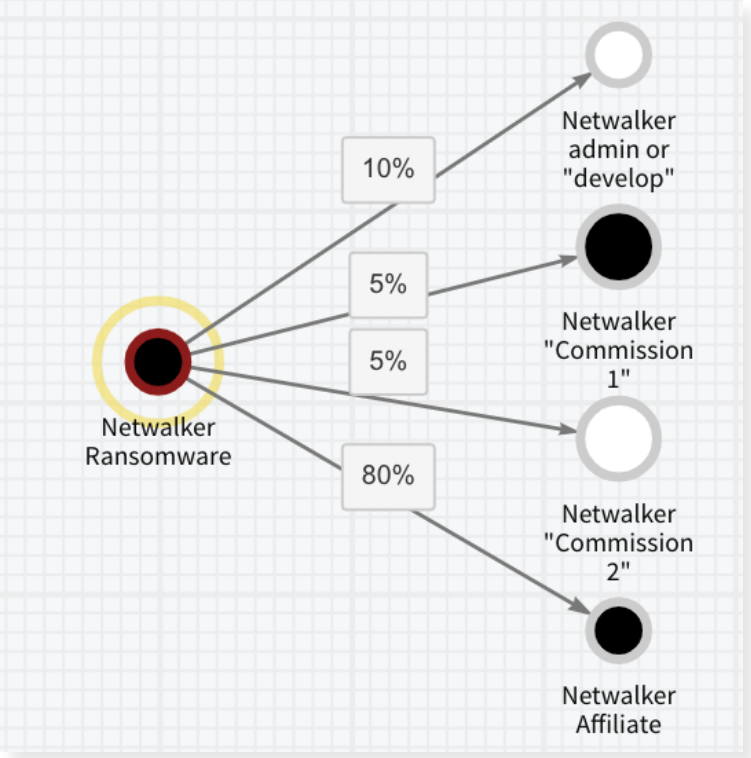


Chart created by Chainalysis with support and approval from law enforcement partners

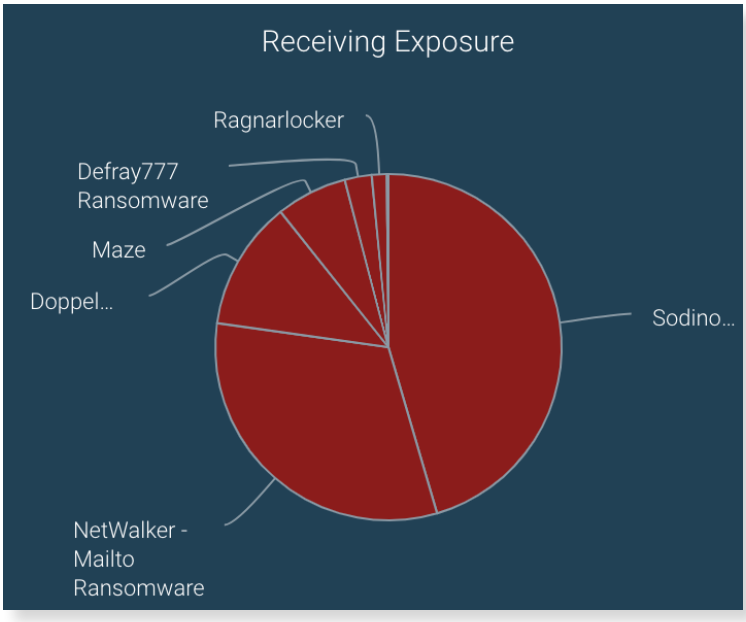
What blockchain analysis tells us about Netwalker operations and financials

Typically, there are four roles that receive proceeds from Netwalker attacks: the likely administrator or developer (8-10%), the affiliate (76-80%), and two commissioned roles (2.5%-5% each). An affiliate, like Vachon-Desjardins, is usually responsible for obtaining access to the victim network and deploying the malware. There are also cases when one wallet gets 100% of the payment, which we believe belongs to the Netwalker administrator and indicates that he or she may also be directly involved in some of the attacks.



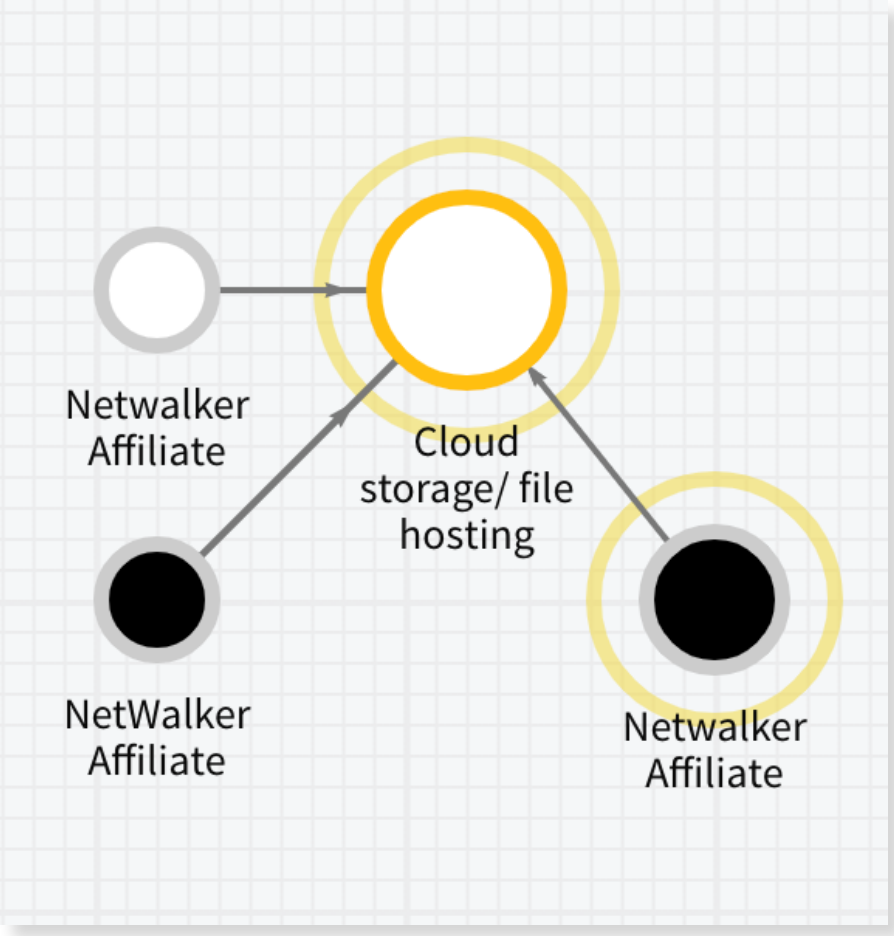
This screenshot of Chainalysis Reactor shows the typical transfer of funds from the ransom payment address to the different Netwalker actors.

Blockchain analysis reveals that there were actually fewer than 20 unique affiliates. Of those affiliates, some rarely deployed Netwalker. Some moved on to other RaaS strains, and we can use the Chainalysis Reactor exposure wheel to show that some affiliates have received payments from other variants.



The Netwalker administrator, who goes by the moniker "Bugatti" on darknet forums, posted an advertisement in May 2020 on a forum seeking additional Russian-speaking affiliates as vacancies had "freed up," which confirms our assessment of affiliates migrating to other strains.

Blockchain analysis can also show ransomware actors paying for services they need to operate their criminal enterprise. For example, we can see below that Netwalker actors paid for cloud storage hosting with cryptocurrency, likely used to host stolen victim data for further extortion. Indeed, Netwalker ramped up its extortion efforts in May 2020 by not only locking victims out of their data, but also by stealing it. Before encrypting computer files on a victim's network, Netwalker actors began to steal the data and automatically publish victim data on a leak site if the ransom was not paid by the deadline, another growing trend among several ransomware strains.



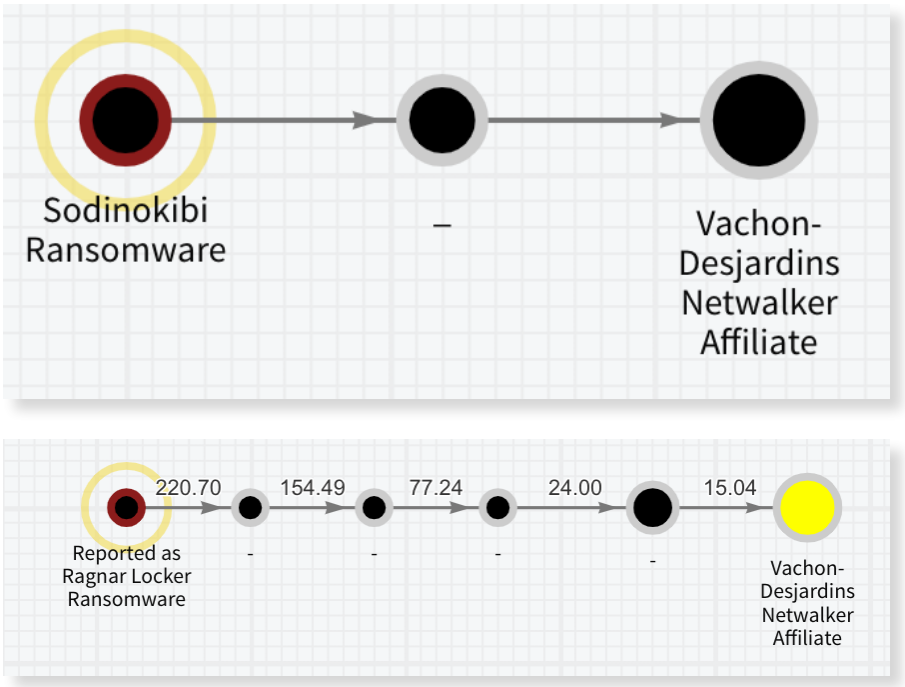
How authorities used blockchain analysis to trace the flow of Netwalker funds

According to the indictment unsealed this past January, Vachon-Desjardins was charged with intentional damage to a protected computer and transmitting a demand in relation to it. This involved a Netwalker ransomware attack against a victim company located in Florida.

Blockchain analysis revealed at least 345 addresses associated with Vachon-Desjardins going back to February 2018 with transactions continuing through late January of 2021. He allegedly received more than $14 million worth of Bitcoin at the time of receipt of the funds, ultimately possessing at least $27.6 million given its rising value.

According to government partners, Vachon-Desjardins was involved in at least 91 attacks using Netwalker ransomware since April 2020, deploying the malware as an affiliate and receiving 80% of the ransom.

In addition to Netwalker, we suspect Vachon-Desjardins was involved in the deployment of other RaaS strains like Sodinokibi, Suncrypt, and Ragnarlocker. This is relatively common; we often see affiliates migrate to different strains over time. Additionally, the Netwalker admin Bugatti has listed proof of prior hacking experience as a prerequisite to become a Netwalker affiliate, so it would make sense that affiliates like Vachon-Desjardins would have a track record.



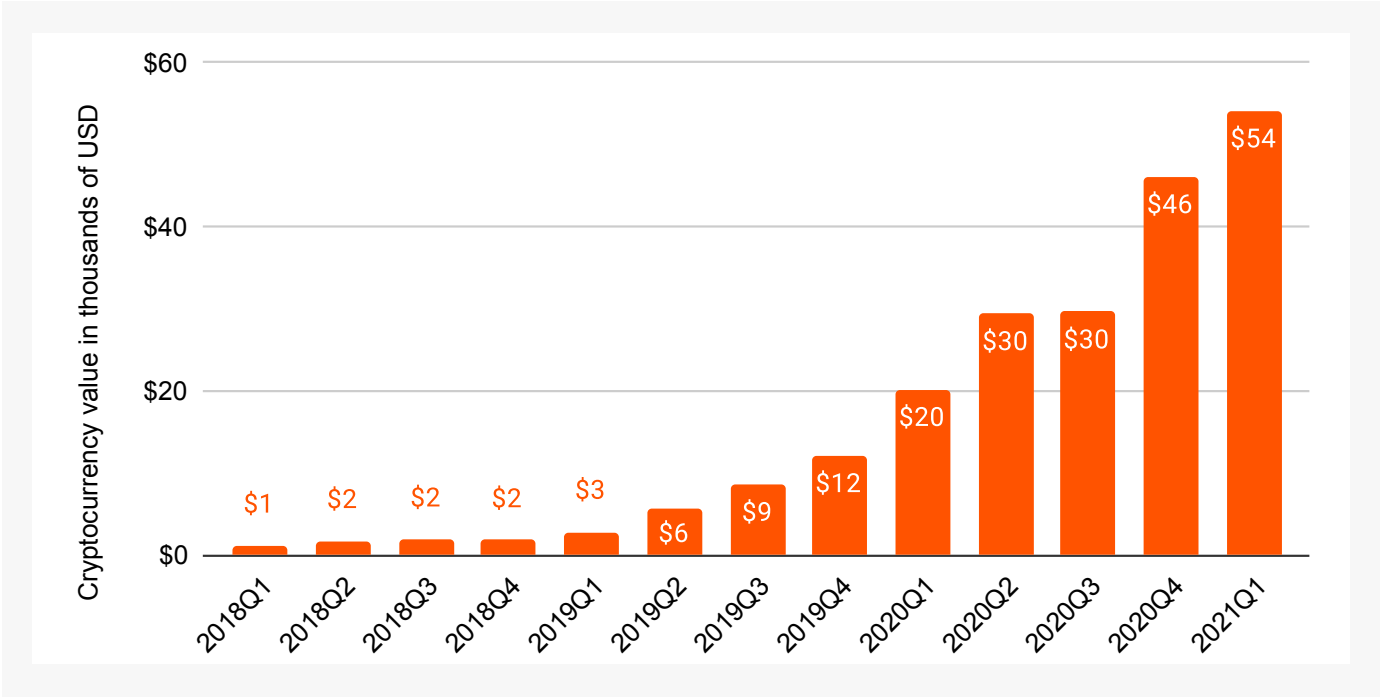
The Chainalysis Reactor graphs above show Netwalker affiliates with exposure to Sodinokibi and Ragnar Locker ransomware strains.

Affiliate overlap is an important phenomenon for authorities to understand in the fight against ransomware, as it suggests a relatively small number of attackers driving the issue despite the many strains active at any given time. This, along with our previous research showing that a small group of service deposit addresses receive most funds stolen in ransomware attacks, suggest that law enforcement can significantly reduce ransomware activity by disrupting a relatively small group of attackers and money laundering service providers.

2021 trend: Ransom sizes grow

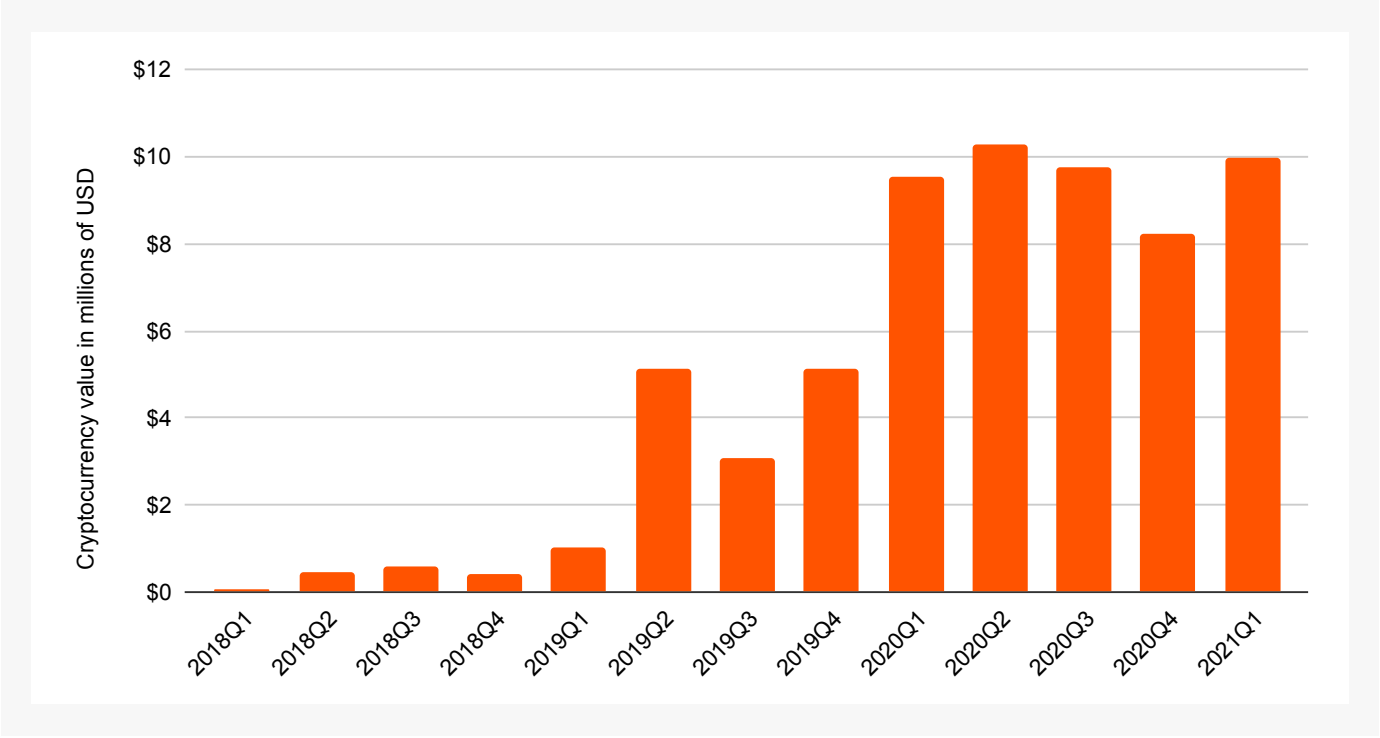
One key trend we've observed starting in 2020 is the drastic growth in the size of the average known ransomware payment.

Average known payment to identified ransomware strains by quarter | 2018 - 2021 Q1



The average known ransomware payment has more than quadrupled from $12,000 in Q4 2019 to $54,000 in Q1 2021. News stories have highlighted much larger outlier ransoms, such as the $50 million ransom payment that REvil demanded from computer parts manufacturer Acer earlier this year, though it's unclear if Acer paid. While we've yet to observe payments of that size, the largest observed ransom payment per quarter has grown substantially over the last two years.

Largest known payments to identified ransomware strains by quarter | 2018 - 20201 Q1



Prior to Q1 2020, we never saw a ransomware payment above $6 million, but since then have seen at least one per quarter.

These rises in ransom payment sizes coincide with an increase in payments from ransomware addresses to other illicit addresses associated with ancillary ransomware services. Illicit third-party services refer to a number of providers, some of whom operate explicitly as criminals, who can help cybercriminals carry out larger, more effective attacks. These tools, many of which are available on darknet markets, include:

- **Infrastructure as a Service providers.** Ransomware attackers need cyber infrastructure such as bulletproof web hosting, domain registration services, botnets, proxy services, and email services to carry out attacks. Additionally, many rely on cloud hosting and other forms of infrastructure to carry out data exfiltration attacks, which refers to a new strategy in which ransomware attackers leak data stolen from victims in an effort to force faster and larger payments. We see an example of this in the ongoing attack on the Washington, D.C. police force, reportedly by the ransomware group Babuk. Babuk has released the personal information of several D.C. police officers since the attack began in order to put pressure on the department.

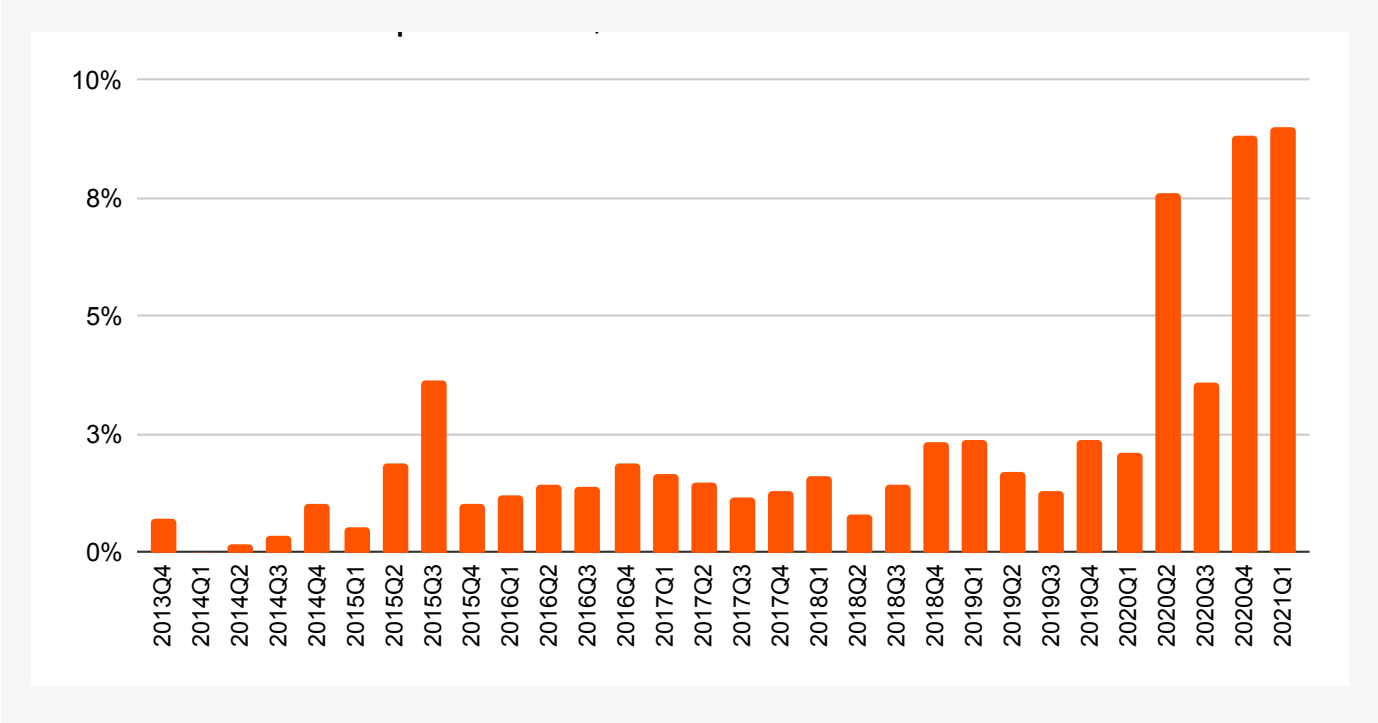
- **Hacking tools and access providers.** Ransomware attackers may purchase network access to victims who have already been compromised under a framework known as Access-as-a-Service. Others will buy tools to help them break into victims' networks themselves. One example is exploit kits. Exploit kits scan for vulnerabilities to establish an initial foothold on the network or deploy a payload like ransomware. These exploits make it possible for ransomware attackers to go after larger organizations with more advanced cybersecurity, who can typically afford higher ransoms than less sophisticated organizations. Another example would be malware as a service, which allows cybercriminals to lease software to distribute ransomware more effectively.

- **Fraud shops.** Fraud shops also play an important role in ransomware operations. Fraud shops are a subset of darknet markets that sell stolen data, including passwords and personally identifying information (PII) for many individuals, and even compromised RDP credentials used to gain access to a victim's network. Similar to the exploits and access described above, this information can help ransomware attackers break into victims' computer networks.

- **Post-attack services:** Some Ransomware and RaaS have adopted enhanced methods of extortion, such as hiring underground call centers to call victims directly, and layering in DDoS attacks on victims refusing to pay, likely leased through DDoS-as-a-Service providers. Ransomware administrators are even paying for salaried employees to help victims through the ransom payment process, including professional negotiators.

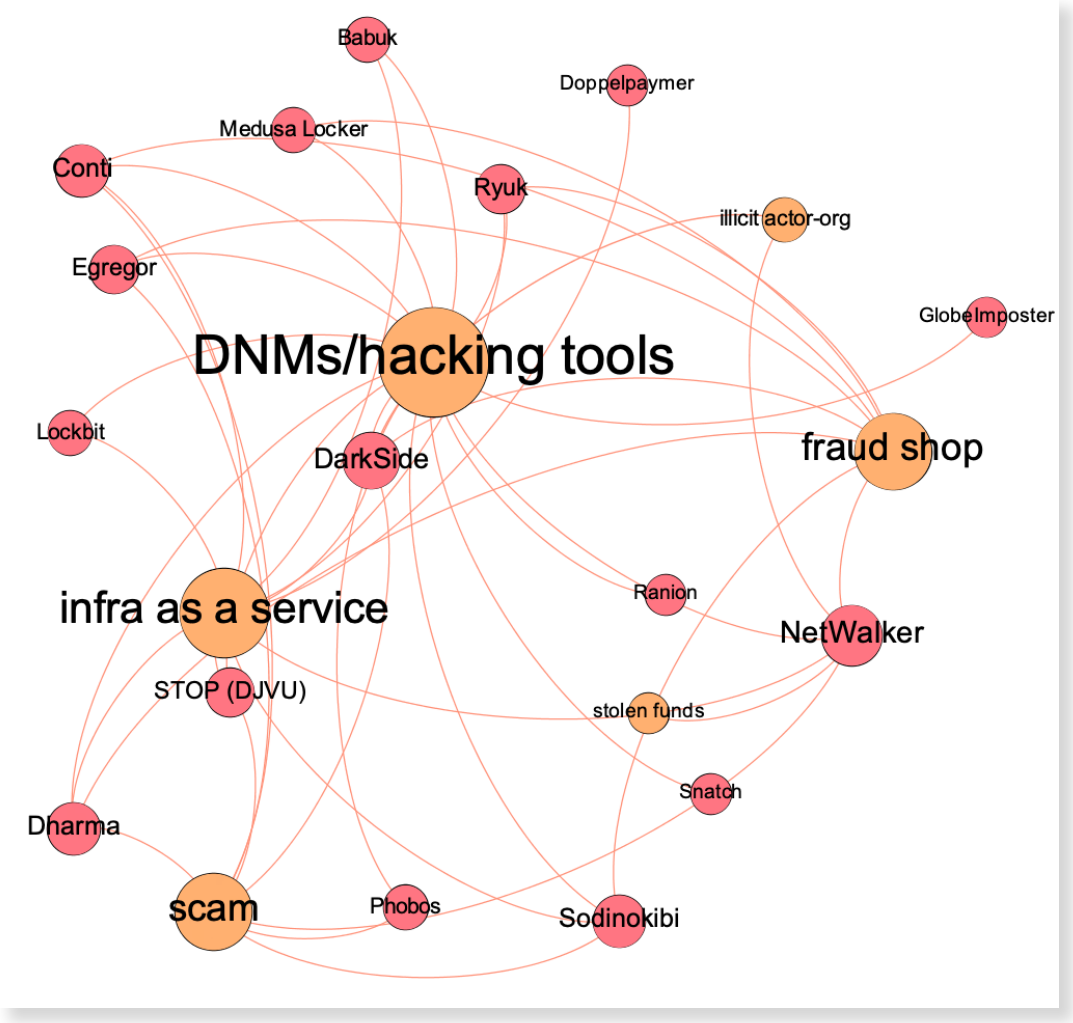
Share of ransomware funds going to illicit third-party providers

| Q4 2013 - Q1 2021



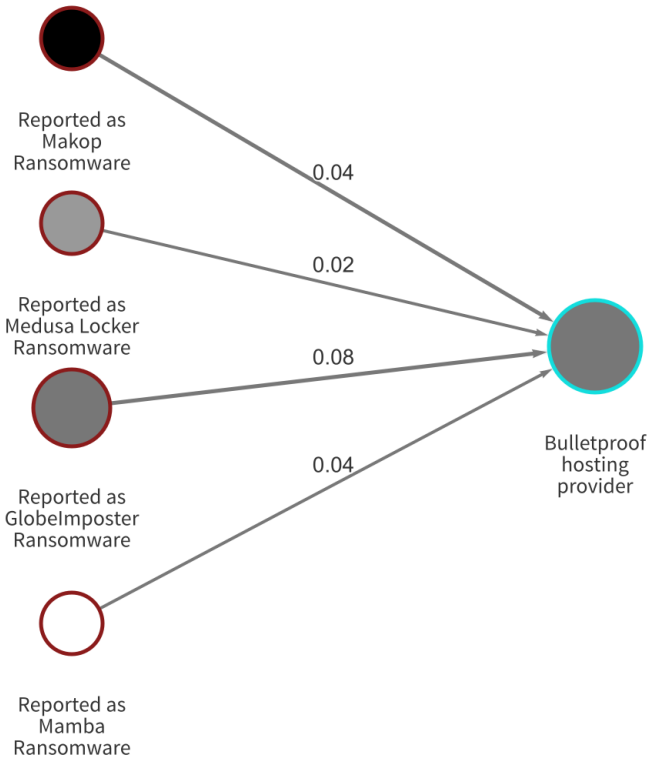
Prior to 2020, illicit third-party services rarely accounted for more than 3% of funds sent from ransomware addresses. Since then, they've increased significantly, often accounting for as much as 9% of spending. Keep in mind too that from 2020 on, the raw total of funds sent from ransomware addresses has increased significantly, meaning these figures represent significant increases in dollars spent on illicit services by ransomware attackers.

All of these third-party vendors enable ransomware attackers to target bigger organizations more effectively, and their increasing usage could be one reason for the higher ransom payments we've been seeing since 2020. Blockchain analysis reveals that these illicit service providers have become the connective tissue of the ransomware ecosystem. In the network chart below, for instance, we show how different types of providers in the aggregate connect many of the most prolific ransomware strains based on cryptocurrency transaction history.

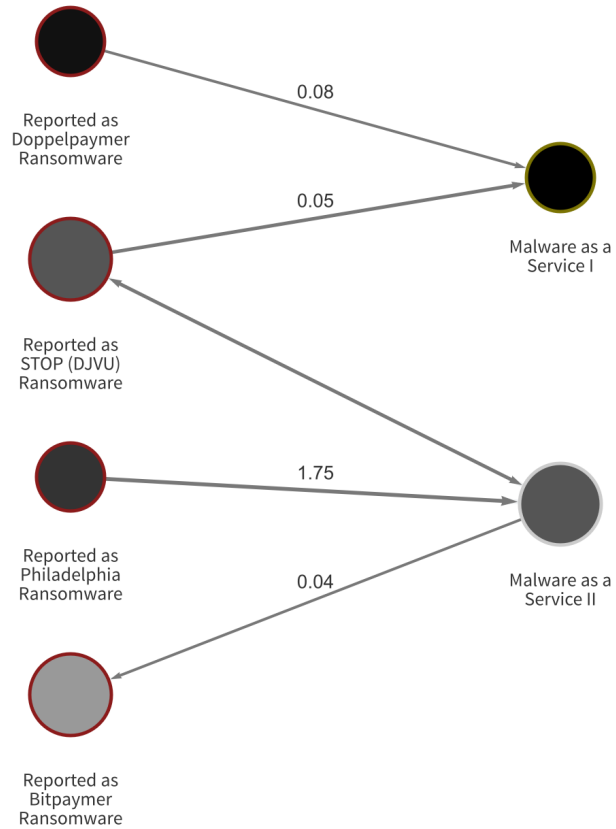


Red bubbles represent individual ransomware strains, while orange bubbles represent aggregated groups of services in the labeled category.

The Chainalysis Reactor graphs below provide more granular examples of this phenomenon. In the first, we see multiple ransomware strains sending funds to a popular bulletproof hosting provider.



In the second, we see other strains transacting with two Malware as a Service providers.

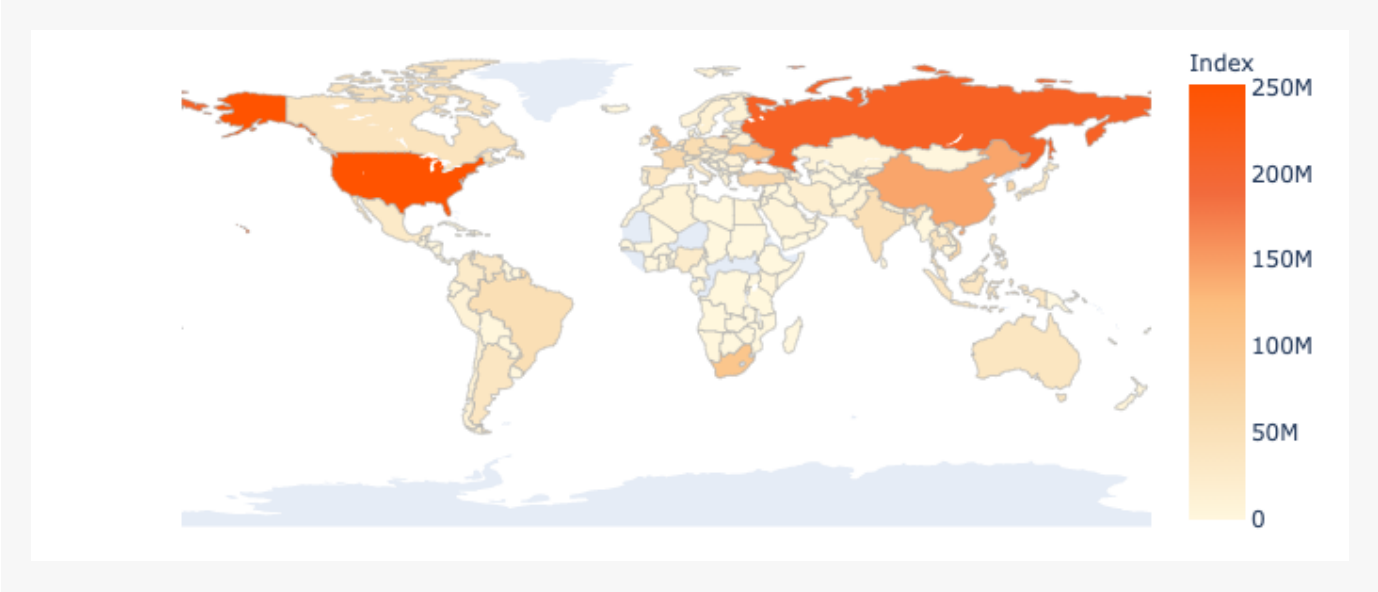


If ransomware attackers continue to have access to advanced infrastructure and tools provided by third-party vendors, we expect ransom payment sizes to continue increasing. Law enforcement and cryptocurrency businesses must work together to take down not just the attackers themselves, but also the providers of tools facilitating attacks.

2021 trend: Russian-affilated ransomware

As we covered above, many ransomware strains are associated with sanctioned cybercriminal groups based in or affiliated with Russia, such as the notorious Evil Corp, whose leadership reportedly has ties to the Russian government. Generally speaking, cybercriminals affiliated with Russia and other Russian-speaking countries in the Commonwealth of Independent States (CIS) — an intergovernmental organization of former Soviet countries — have been among the most prolific in the world. Russian-affiliated services received more cryptocurrency from illicit addresses than those in any other country, suggesting that Russian-affiliated cybercriminals were the year's biggest financial beneficiaries of cryptocurrency-based crime. Much of this activity was driven by Hydra, a Russia-based darknet market, which in addition to drugs sells stolen data that can be useful to ransomware attackers.

Destination of funds leaving illicit services | 2020



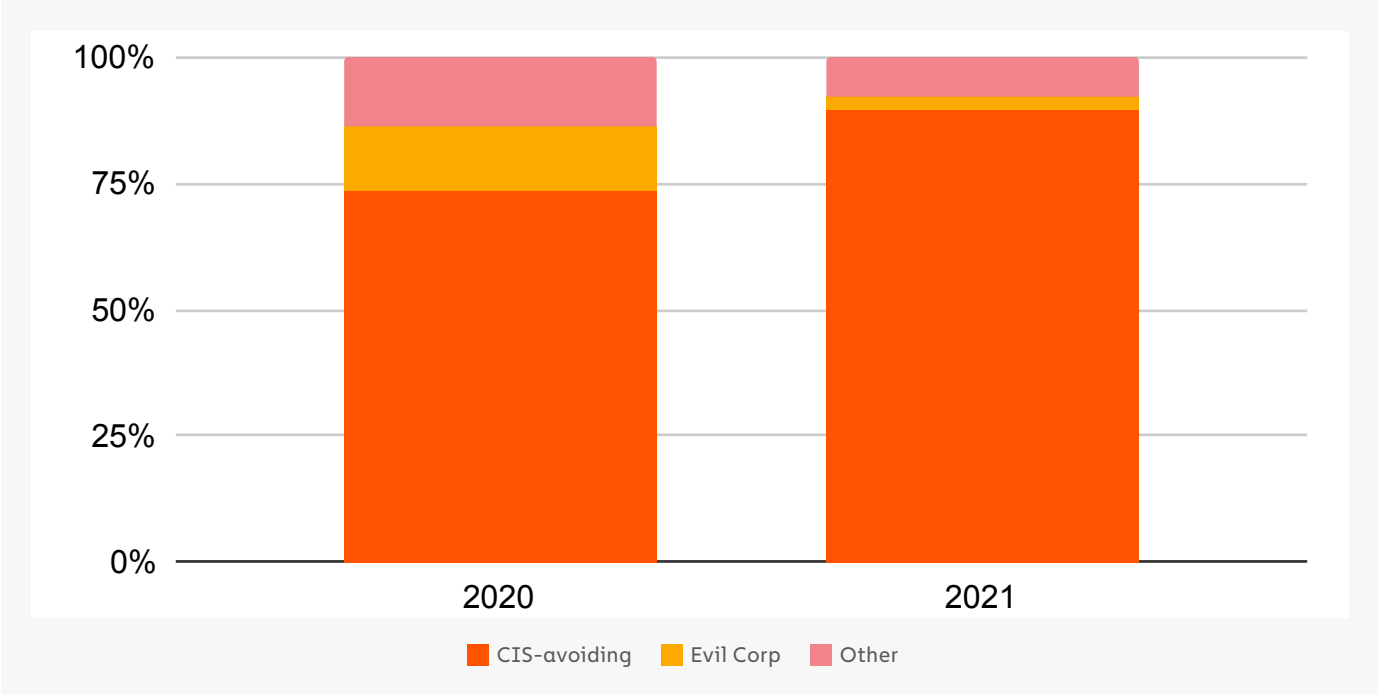
In 2021, ransomware strains associated with Russia and other CIS countries are accounting for a larger share of overall ransomware activity. We show this on the graph below by comparing activity in 2020 and 2021 for two categories of ransomware strains:

- Strains associated with Evil Corp.

- Strains with code that prevents encryption if the ransomware detects the victim's operating system is located in a CIS country. These strains can generally be assumed to have originated in Russia or other CIS countries.

The numbers are clear: Taken together, these ransomware strains are accounting for more activity in 2021 compared to 2020.

Share of ransomware proceeds: 2020 vs. 2021



Please note: This graph reflects the total amount of ransomware activity accounted for by the ten most prolific strains in 2020 and 2021. While this excludes many individual strains, it still reflects the majority of activity in both years.

In 2020, roughly 86% of ransomware proceeds studied could be attributed to ransomware strains that are either associated with Evil Corp or are designed to avoid CIS countries. So far in 2021, that figure is at 92%.

The U.S. government is already taking the threat of Russian cybercrime seriously, as President Biden announced several new sanctions against Russian groups and individuals following the SolarWinds hack earlier this year. The data on ransomware specifically suggests that blockchain analysis, as well as collaboration with other firms throughout the cryptocurrency industry, will be crucial to fighting cybercrime from groups aligned with Russia and other hostile nation states.

United States ransomware regulatory updates

As instances of ransomware have increased over the past few years, regulators and law enforcement have taken notice and issued guidance. As mentioned earlier, two bureaus within the U.S. Department of the Treasury– the Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN)– issued advisories related to facilitating ransomware payments. OFAC's advisory focused on the potential sanctions risks associated with ransomware payments, while FinCEN's advisory highlighted that the facilitation of ransomware payments may trigger FinCEN registration and Bank Secrecy Act (BSA) requirements and discussed financial red flag indicators of ransomware and associated payments.

Neither of these advisories includes major changes to the U.S. government's guidance; regulators and law enforcement have consistently stated that paying ransoms only encourages bad actors to make future ransomware payment demands. But they do make it clear that ransomware victims and those who facilitate payments on behalf of victims can be found in violation of sanctions violations and/or the BSA.

Ransomware victims, third party intermediaries that facilitate ransomware payments such as digital forensics and incident response companies and cyber insurance companies, cryptocurrency exchanges, and financial institutions should take a risk-based approach to managing responses to ransomware on behalf of themselves and their customers.

Here we break down the key takeaways from the OFAC and FinCEN advisories and point out where and how blockchain analysis can help mitigate risk of sanctions violations when making ransomware payments and ensuring compliance with BSA obligations.

OFAC advisory on potential sanctions risks for facilitating ransomware payments

OFAC has designated many malicious cyber actors, including perpetrators of ransomware attacks and those who facilitate ransomware transactions. U.S. persons are prohibited from engaging in transactions, directly or indirectly, with individuals or entities on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) and those covered by comprehensive country or region embargoes. A threat actor demanding a ransomware payment may be sanctioned or otherwise have a sanctions nexus, which means that ransomware victims, or

those facilitating payments on their behalf, must conduct the appropriate due diligence before making ransomware payments in order to avoid violating OFAC regulations. OFAC makes several important clarifications in their advisory:

1. **Facilitating ransomware payments on behalf of a victim may violate OFAC sanctions.**

   Third party ransomware facilitators and cryptocurrency exchanges could be in violation of sanctions if they facilitate a payment to a sanctioned actor.

   For example, Garmin reportedly used a third party to pay the WastedLocker ransomware demand rather than paying it directly. In this case, WastedLocker ransomware is believed to be a variant developed by Evil Corp, a designated entity. Blockchain analysis tools, including Chainalysis Reactor, can help victims and those working on their behalf identify cryptocurrency wallets associated with specific ransomware variants and OFAC designated actors to avoid making payments in violation of sanctions.

   The Evil Corp example also underscores the importance of understanding the various strains that designated entities run over time. OFAC originally sanctioned Evil Corp for its development and distribution of the Dridex strain, which was largely active in late 2015 and early 2016 before the group moved to other variants such as WastedLocker. It is therefore important to keep up with known variants that were operated in the past by an entity on the SDN List, as well as any new ones they begin to operate. One of the best ways to understand this connectivity is by using blockchain analysis to investigate where payments intersect. Blockchain analysis will provide insight into payment connections between strains and alert victims and those working on their behalf so they can avoid making payments to sanctioned addresses and individuals.

2. **Addresses and individuals covered by comprehensively sanctioned jurisdictions are also applicable.**

   OFAC's advisory not only covers entities on their SDN list, but also comprehensive country or region embargoes (e.g. Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria), as malicious cyber activities may enable criminals and adversaries in these jurisdictions to profit and advance their illicit aims or threaten U.S. national security interests. It can be difficult to determine where entities are located based on their cryptocurrency wallets or addresses. However, using blockchain analysis tools, it is possible to see where a cryptocurrency deposit address is located at an exchange or has interacted with an exchange, and to review that exchange's jurisdictional

information to see whether they are located in a comprehensively sanctioned jurisdiction. Blockchain analytics is imperative for this research.

3. **OFAC will review licensing applications involving ransomware payments on a case-by-case basis with a presumption of denial.**

   OFAC has a licence application process by which it is possible to apply to receive authorization from OFAC to engage in a transaction that otherwise would be prohibited. However, this advisory makes clear that licence applications involving ransomware payments as a result of malicious cyber-enabled activities will probably not be approved.

4. **Self-initiated, timely, and complete reports of a ransomware attack to law enforcement will be considered a significant mitigating factor if the situation is later determined to have a sanctions nexus.**

   OFAC also notes in the advisory that if a victim of a ransomware attack reports the attack to law enforcement, they will consider the "self-initiated, timely, and complete report" to be a significant mitigating factor if the situation is later determined to have a sanctions nexus when OFAC considers appropriate enforcement outcomes. They will also consider the victim's full and timely cooperation with law enforcement during and after the attack. Because effort is measured in relation to possible violations, it is important to work directly with law enforcement, OFAC, and FinCEN to ensure compliance with all of the appropriate obligations.

FinCEN advisory on ransomware and the use of the financial system to facilitate ransom payments

FinCEN's advisory provides important information on the role of financial intermediaries in the processing of ransomware payments, trends and typologies of ransomware and associated payments, ransomware-related red flag indicators, and information reporting and sharing. Typically, because ransomware attackers demand ransom be paid in cryptocurrency, processing ransomware payments usually involves at least one depository institution and one or more money service businesses (MSB). Upon receipt of the ransom, the attacker will launder the funds, integrating it back into the financial system. Because of this, the financial sector can play a critical role in identifying ransomware payments and financial institutions can play an important role in protecting the U.S. financial system from ransomware threats through compliance with their BSA obligations. Here are three important takeaways from the FinCEN advisory:

1. **Third-party ransomware facilitators like DFIR companies and CICs might be engaged in MSB activities.**

   Digital forensics and incident response (DFIR) and cyber insurance companies (CICs) that facilitate ransomware payments on behalf of their customers to ransomware attackers by converting their customers' fiat currency into cryptocurrency may be engaged in MSB activities (such as money transmission). This would trigger FinCEN registration and BSA requirements, including filing Suspicious Activity Reports (SARs). It is likely SAR filing reporting requirements would be triggered by every payment they process to ransomware attackers.

   The applicability of this guidance to DFIR companies and CICs would depend on whether payments were made directly, or whether they walked their customer through the process or connected them with someone who paid on their behalf.

   Any DFIR company or CIC making ransomware payments on behalf of customers should be aware of any OFAC-related obligations related to that activity as well, as outlined above.

2. **FinCEN considers a link between a customer's cryptocurrency wallet and ransomware activity to be a red flag indicator.**

   FinCEN identified several financial red flag indicators of ransomware-related illicit activity to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with ransomware attacks. Many of these red flags and typologies are associated with cryptocurrency, or convertible virtual currency (CVC), activity.

   In particular, red flag #3 is "*a customer's CVC address, or an address with which a customer conducts transactions, appears on open sources, or commercial or government analyses have linked those addresses to ransomware strains, payments, or related activity.*" Blockchain analysis is required to identify this in most circumstances.

3. **It still isn't clear if it's illegal to pay ransom if the entity is not sanctioned.**

   While we are still lacking clarity around the legality of paying ransom if the entity isn't sanctioned, what is clear is that operating as a money transmitter/MSB and not registering or filing SARs violates the BSA.

The recent OFAC and FinCEN advisories clarify two important regulatory grey areas: (1) there are potential sanctions issues associated with ransom payments, and licenses probably will not be granted and (2) companies facilitating ransom payments may need to register with FinCEN and file SARs. Blockchain analysis tools will be critical in enabling financial institutions, MSBs, and others to be compliant with regulatory guidance.

The FBI's Internet Crime Complaint Center (IC3) issued an advisory on common types of ransomware, how to minimize ransomware risks, and how to report attacks. CISA stood up a campaign focused on reducing the risk of ransomware and has released a number of guides and other resources focused on raising awareness and helping the public and private sectors mitigate ransomware risks. USSS Cybercrime Investigations has also released a guide to ransomware outlining how to prepare against, prevent, and respond to a ransomware attack.

U.S. ransomware policy 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. The foundation of these policies must be a comprehensive, whole-of-U.S. government strategy for reducing ransomware attacks. Recently, positive efforts were spearheaded by the White House as President Biden issued an Executive Order on May 12th to improve U.S. cybersecurity (the "Executive Order"). We laud any efforts towards promoting and implementing a cohesive cybersecurity policy. We believe that clear guidance and direction from the President 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 U.S. 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. We outline below some specific policies that Congress and government agencies should consider when determining future legislation and strategies necessary to combat ransomware.

Update and strengthen cyber hygiene regulations and standards

Current cybersecurity regulations and standards in the United States do not specifically address ransomware in a manner that would meaningfully prevent these attacks. The Executive Order will improve cybersecurity standards at the Federal level. This will be vital to improving our national security. It is also important that cybersecurity standards for private sector and non-profit businesses be updated and strengthened, in order to prevent the sorts

of ransomware attacks we have seen cripple our critical infrastructure, healthcare systems, schools, and private businesses. Regulations should be reviewed and updated, and legislation enacted if needed, to incorporate measures that would more directly mitigate ransomware attacks. One mechanism to consider, given how quickly this threat and technology progress compared to the process for updating laws and regulations, would be for Congress to mandate standards be set through a private- or public-sector standards body that reviews and sets minimum required cybersecurity standards on an annual basis.

Improve information sharing

In order to disrupt the existing ransomware ecosystem, public-private information sharing could be improved and incentivized. Information is not currently shared in a consistent or reliable manner, and it does not always reach a broad enough audience. There is also 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.

Campaigns educating the general public and the private sector about ransomware attacks, how they can be prevented, and encouraging the reporting of events could be developed. In conjunction with these campaigns, mechanisms for sharing information related to ransomware incidents could be developed. The development of information sharing networks, both within the government, and between the government and the private sector, would improve the quality and volume of information about ransomware incidents. It may be worth considering a standard format for ransomware incident reporting to promote consistency, or providing suggested fields to include, such as cryptocurrency wallet addresses, transaction hashes, and ransom notes. Incentives could be put in place to facilitate information sharing between the private sector, financial institutions and MSBs, law enforcement, and regulators.

The Executive Order removes barriers to threat information sharing between government and the private sector, and is an important start. However, it does so through proposed revisions to government contracting language that would only impact businesses contracting with the federal government. Congressional action that regulates or incentivizes private companies to share intelligence about ransomware actors with law enforcement, by removing legal barriers and requiring providers to share breach information, is critical. Additionally, regulatory advisories to the private sector 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. Increased information sharing would also better enable investigators to prioritize incidents and the private sector to

prepare themselves and improve their security measures against ransomware incidents.

Increase investigative resources

In order to comply with Treasury Department regulatory guidance on ransomware payments, ransomware victims must report attacks to law enforcement. If victims want to pay ransom to a sanctioned address, individual, or entity, they must apply for a license from OFAC. It will be critical that regulators and law enforcement have the tools and resources they need to conduct compliance checks and investigations into ransomware attacks. Ransomware is usually paid in cryptocurrency, so blockchain analysis tools are a vital tool in the investigator's toolkit.

Using blockchain analysis tools, regulators can confirm compliance with regulatory guidance and law enforcement can trace the ransom paid in cryptocurrency to attackers to 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.

Conclusion

The importance of more comprehensive and standardized information gathering in ransomware investigations, whether provided by victims or gathered by law enforcement, cannot be understated. This may require Congress, Federal agencies, or State and Local governments to remove legal barriers and potentially provide incentives for public and private sector entities to be able to report ransomware incidents without fear of additional damages. 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 U.S. 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.

Chainalysis

Building trust in blockchains