S. Hrg. 117–575

RISING THREATS: RANSOMWARE ATTACKS AND RANSOM PAYMENTS ENABLED BY CRYPTOCURRENCY

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

JUNE 7, 2022

Available via the World Wide Web: http://www.govinfo.gov

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE
50–846 PDF WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
ALEX PADILLA, California
JON OSSOFF, Georgia

ROB PORTMAN, Ohio
RON JOHNSON, Wisconsin
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
ALAN S. KAHN, *Chief Investigative Counsel*
STEPHANIE T. ROSENBERG, *Investigative Counsel*
VICTORIA G. KELLEY, *Reseach Assistant*
PAMELA THIESSEN, *Minority Staff Director*
SAM J. MULOPULOS, *Minority Deputy Staff Director*
WILLIAM H.W. MCKENNA, *Minority Chief Counsel and Chief Investigator*
PATRICK T. WARREN, *Minority Investigative Counsel*
LAURA W. KILBRIDE, *Chief Clerk*
THOMAS J. SPINO, *Hearing Clerk*

CONTENTS

WITNESSES

TUESDAY, JUNE 7, 2022

ALPHABETICAL LIST OF WITNESSES

APPENDIX

RISING THREATS: RANSOMWARE ATTACKS AND RANSOM PAYMENTS ENABLED BY CRYPTOCURRENCY

TUESDAY, JUNE 7, 2022

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10 a.m., via Webex and in room SD–342, Dirksen Senate Office Building, Hon. Gary Peters, Chairman of the Committee, presiding.

Present: Senators Peters, Hassan, Sinema, Rosen, Ossoff, Portman, Johnson, Lankford, Scott, and Hawley.

OPENING STATEMENT OF CHAIRMAN PETERS[1]

Chairman PETERS. The Committee will come to order.

I would first like to say thank you to our witnesses for joining us here. Today's hearing will provide a very important opportunity to discuss the rising threat posed by ransomware attacks, and the role that cryptocurrencies play in enabling these harmful cybercrimes.

In recent years, we have seen a scourge of increasingly complex and sophisticated ransomware attacks on both public and private networks, where the attackers prevent access to an entity's computer systems or threaten to release stolen data unless a ransom is paid.

From the Kaseya ransomware attack that affected between 800 and 1,500 small businesses, to alarming attacks on our critical infrastructure that caused gas shortages across the East Coast and temporarily shut down processing plants for the world's largest meat supplier, ransomware attacks have caused significant disruptions to daily life and imposed serious economic costs.

A single ransomware attack can force businesses to close their doors permanently, even if they pay the ransom demand. Cybercriminals may shut down computer systems, expose sensitive data, or erase data entirely, causing significant disruption to business continuity. Some of the longer-term impacts may include lost revenues, reduced profits, damage to brand reputation, employee layoffs, and loss of customers.

These malign actors almost exclusively demand cryptocurrencies when extorting large sums of money, because they can take steps

[1] The prepared statement of Senator Peters appears in the Appendix on page 29.

to obscure their transactions and circumvent regulatory scrutiny, making payments more difficult to trace.

In 2020, according to a Chainalysis study, malicious hackers received at least $692 million in cryptocurrency extorted as part of ransomware attacks, up from $152 million in 2019, and over a 300 percent increase year-over-year. These figures are likely a drastic underestimation of the actual number of attacks and ransomware payments made by victims.

While Bitcoin and many other cryptocurrencies provide a public ledger of transactions, known as a "blockchain," cryptocurrency wallets are not tied to an individual person, meaning account holders can take steps to conceal their identity to avoid being held accountable for criminal activities.

Anti-money laundering and other banking regulations that are meant to prevent criminal use of currency, including cryptocurrency, are also often inconsistently enforced, particularly in foreign jurisdictions, where many attackers are based.

For example, last year, according to Chainalysis, approximately 74 percent of global ransomware revenue went to entities either likely located in Russia, or controlled by the Russian government. Attacks from Russia-based entities are only expected to increase, especially as the United States continues its support of Ukraine against Russia's illegal and immoral invasion.

Last month, I released a report examining the role cryptocurrencies play in incentivizing and enabling ransomware attacks, and the resulting harm these attacks have on victims. I will now move to introduce this report[1] as part of the hearing record, and hearing no objection, this report will be entered into the record.

My investigation found that the Federal Government lacks sufficient data and information on ransomware attacks and the use of cryptocurrency as ransom payment in these attacks, and must collect better data to understand the scope of the threat.

The cyber incident reporting law that Ranking Member Portman and I authored and passed earlier this year marks a significant first step to getting the information the government needs to combat this growing threat. The legislation will require critical infrastructure owners and operators to report cyberattacks within 72 hours and ransomware payments within 24 hours, and I look forward to working with the Administration to ensure it is swiftly and effectively implemented.

The more information we have, the better suited we will be to combat ransomware attacks. That means continuing to build off our bipartisan cyber incident reporting legislation by holding foreign adversaries and cybercriminals accountable, and finding ways to reduce the incentives to conduct these attacks in the first place, including by examining their use of cryptocurrency.

While I am grateful to the many Federal law enforcement and regulatory agencies that have taken steps to address cybercriminals and the rising threat of ransomware attacks, more must be done to ensure cryptocurrencies are monitored appropriately, like their non-digital counterparts.

[1] The Majority Report appears in the Appendix on page 74.

Finally, in addition to addressing ransomware attacks and the use of cryptocurrency as ransom payment in those attacks, Congress must examine other criminal activity involving cryptocurrency that threatens our nation's national and economic security, such as human trafficking, the flow of illicit drugs across our borders, and other serious crimes.

I look forward to our hearing today and to hear from panel of expert witnesses who can further elaborate on the uses of cryptocurrency in ransomware attacks, and provide answers to ensure we have the necessary tools and resources to tackle this issue head on.

With that I would like to recognize our Ranking Member of this Committee, Ranking Member Portman, for his opening comments.

OPENING STATEMENT OF SENATOR PORTMAN[1]

Senator PORTMAN. Thank you, Mr. Chairman, and I thank you to our witnesses for being with us today, some in person, some virtually. We are going to hear from a private sector panel of cybersecurity professionals and incident responders who are going to provide us with a unique perspective, in each case, on what can be done to combat ransomware.

Obviously, the frequency and severity of ransomware attacks continues concern us because it continues to grow. Ransomware groups have professionalized their operations using a business model often now called ransomware-as-a-service, which involves ransomware developers selling or delivering their malware to individuals called "affiliates" who actually carry out the attack. It is a business model. This allows ransomware gangs to conduct more attacks with broader impact.

In March of this year, I released a report[2] documenting the experiences of three American companies victimized by the most notorious Russian ransomware gangs, called REvil . The companies profiled in the report are from different business sectors and vary significantly in size, revenue, and their information technology (IT) resources. This was done on purpose, to try to show that this is affecting companies of every size and sophistication. Despite these differences, all of these companies fell victim to REvil. This underscores the broad threat ransomware presents and the proactive steps all organizations must take to implement cyber best practices.

REvil was largely believed to be offline following the arrests of several key members last fall, but public reports indicate the gang may be resuming operations. We know it is common for ransomware criminals to claim retirement only to "rebrand" and reemerge under a new name.

About a year ago, this Committee held a hearing on the Colonial Pipeline ransomware attack. That incident was a painful reminder to many Americans that these attacks have real-world consequences impacting everybody.

Recognition of this challenge is one of the reasons Chairman Peters and I drafted cyber incident reporting legislation, which I

[1] The prepared statement of Senator Portman appears in the Appendix on page 31.

[2] The Minority Report appears in the Appendix on page 126.

am proud to say became law a couple of months ago. This law will enhance our nation's visibility into cyberattacks against the United States and will enable a more effective response including warning potential victims. It is really important that Cybersecurity and Infrastructure Security Agency (CISA) works with industry experts and stakeholders to implement this law immediately.

We know ransomware attacks will continue to be a national security threat for the foreseeable future. As the committee of jurisdiction over cybersecurity, we will continue to work to identify solutions that address the threats associated with ransomware attacks and the ways we can fortify our defenses.

Today we are going to have testimony from some real experts to ensure that we are making steps in the right direction, and I look forward to that testimony.

Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Ranking Member Portman.

It is the practice of the Homeland Security and Governmental Affairs Committee (HSGAC) to swear in witnesses. If each of you will please stand and raise your right hand, including folks joining us online.

Do you swear that the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Ms. STIFEL. I do.

Mr. SIEGEL. I do.

Ms. KOVEN. I do.

Chairman PETERS. Everyone has answered affirmatively. You may be seated.

Our first witness is Megan Stifel, Chief Strategy Officer (CSO) at the Institute for Security and Technology (IST), a partnership that provides public and private sector guidance on security and technology. In 2021, IST released a comprehensive report on combating ransomware.

Ms. Stifel previously served as an attorney in the National Security Division at the Department of Justice (DOJ), where she also spent time detailed as a Director for International Cyber Policy on the National Security Council (NSC). She also previously served as a Senior Policy Counsel for Global Cyber Alliance.

Welcome, Ms. Stifel. You may now proceed with your opening remarks.

TESTIMONY OF MEGAN H. STIFEL,[1] CHIEF STRATEGY OFFICER, INSTITUTE FOR SECURITY AND TECHNOLOGY

Ms. STIFEL. Chairman Peters, Ranking Member Portman, distinguished Members of the Committee, thank you for the opportunity to testify today about the critical importance of information about ransomware attacks and associated payments combating the ongoing ransomware scourge.

My name is Megan Stifel and I am the Chief Strategy Officer at the Institute for Security and Technology. We are a Bay Area-based nonprofit organization focused on staying ahead of security challenges resulting from our increasing dependence on technology.

[1] The prepared statement of Ms. Stifel appears in the Appendix on page 33.

Our current work focuses on nuclear command and control, artificial intelligence (AI), digital cognition and democracy, and most relevant for today's purposes, information security.

Early last year, in response to the growing threat posed by the escalating rise in ransomware incidents targeting critical infrastructure, IST convened the Ransomware Task Force (RTF), and I had the privilege of being a co-chair. The task force included participants from industry, academia, civil society, and governments, including the United States, the United Kingdom (UK), and Canada, as well as multilateral organizations such as Europol. In total, 60-plus organizations participated, including the organizations represented by my fellow witnesses.

In a span of four months, this coalition worked to identify measures to help all stakeholders better deter, disrupt, prepare, and respond to ransomware. As noted, we published a report last spring, including four goals, five priority recommendations, and a series of recommended actions, and totaling 48. The priority recommendations included the need for a sustained, coordinated, U.S.-led, multi-stakeholder collective action to meaningfully reduce the ransomware threat; an intelligence-driven anti-ransomware campaign, including support for operational collaboration with industry; the establishment of ransomware response and recovery funds, frameworks for preparation and mandated reporting of payments; as well as closer international regulation of the cryptocurrency sector that enables ransomware crime.

As noted just after the report's publication several high-profile ransomware attacks occurred, leading to the disruption of fuel and meat production, distribution, as well as health care. These incidents formed pivotal moments in which significant progress has been made in countering ransomware. Much of this progress aligns with the task force's recommendations.

Still, much work remains. I will focus my testimony today on the task force's recommendations related to information about ransomware incidents, especially payments, and helping government and industry effectively combat ransomware.

Before I address the essential role of information in the ransomware lifecycle I have to pause and emphasize that ransomware is a symptom of a broader problem, and that problem originated decades ago through a confluence of factors, each of which must be addressed to put a significant dent in the ransomware-related cybercrime, but also in all aspects of cybersecurity risk and resulting cybercrime.

Ransomware is 21st-century extortion, but extortion is not a 21st-century invention. New forms of extortionware are emerging. Thus, in examining collective measures by industry and government to combat ransomware, we are not just targeting today. We are working to better secure tomorrow against wherever these criminals turn next.

In my testimony before the House last year, I noted the task force's recommendations, but the scope and quality of information about ransomware incidents must improve. The reasons for this are manyfold. Higher-quality information can better equip governments and other stakeholders in developing the international strategy the task force called for to reduce ransomware risk at scale. It can also provide more detailed evidence to support a range of measures that can reduce the ability of these actors to operate from safe havens.

Of perhaps equal importance, higher-quality information can better inform the private sector's ability to protect its customers' right to property as well as enhance its capacity to collaborate with the government in combating ransomware and other cybercrimes.

As the task force noted in April 2021, improving the quality and volume of ransomware information would better enable deterrence, enhance preparedness, and inform disruption activities. There were several recommendations in the report.

Since ransomware is often a criminal endeavor to extract financial gain, one of the most effective tools in combating it is to follow the money. Information shared through voluntary and mandatory incident reporting, including ransom payments, is this tool's lifeblood. Yet to this date we have not found an adequate incentive structure to meaningfully empower this capability at scale.

As depicted in the ransomware payment diagram submitted with my written testimony, a range of organizations may have information that can enable public and private sector entities to follow the money. Today, however, there are only partial views spread across many stakeholders without a common process or pathway to stitch the pieces together.

Ultimately, there should be harmony among government reporting avenues. This would ease confusion among victims and streamline a collection and analysis of attack information. The recently passed reporting legislation will address aspects of this challenge. However, the need for consistency across reporting pathways is more immediate. It is especially critical while the rulemaking process is underway. It is also essential regardless of the rulemaking process, given the scope of entities that will likely be required to report pursuant to, or elect to share voluntarily under the legislation.

To meet the risks of tomorrow, information gathered must be useful and it must be appropriately disseminated within a meaningful period of time. It is also important to know that the same information may be of different value, depending on the agency's or organization's mission.

I must also pause to emphasize the need the task force placed on enabling disruptive capabilities through these channels. Disruptive actions taken in the past year to seize cryptocurrency assets could scale significantly if clear, concise, actionable information is made available to appropriate organizations as early as possible in the cryptocurrency kill chain.

Thank you for the opportunity to participate today, and I look forward to your questions.

Chairman PETERS. Thank you, Ms. Stifel.

Our next witness is Bill Siegel, Chief Executive Officer (CEO) and Co-Founder of Coveware, a cyber incident response firm that specializes in assisting victims of ransomware attacks. Mr. Siegel previously served as the Chief Financial Officer (CFO) for the cybersecurity rating company, SecurityScorecard, and the Chief Executive Officer of Secondmarket, and the Head of National Association of Securities Dealers Automated Quotations Stock Market (NASDAQ) Private Market.

Mr. Siegel, you may proceed with your opening remarks.

TESTIMONY OF BILL SIEGEL,[1] CHIEF EXECUTIVE OFFICER, COVEWARE

Mr. SIEGEL. Mr. Chairman, Ranking Member Portman, and Members of the Committee, thank you for the opportunity to share Coveware's perspective on ransomware attacks and the role of cryptocurrency in ransom payments.

My testimony today is derived from Coveware's experience which spans thousands of ransomware incidents over the last few years. During a given incident, we interact with the victim of the attack, privacy attorneys, forensic investigators, restoration firms, cyber insurance companies, and the law enforcement agencies that investigate these attacks.

Throughout the incident, we collect data firsthand, and the aggregated learnings from this data and our experience gives us a unique perspective on this problem. We collect and organize this data, because like any problem, you cannot solve it until you understand it. The analogy we use is that you cannot build safe cars without studying lots of car crashes.

In addition to analysis, our firm has voluntarily and proactively reported subsets of our data to law enforcement from every attack we have ever worked on since inception of our firm. This data is used by law enforcement to augment active investigations into the criminal groups that carry out these attacks.

We are grateful for the work that Chairman Peters and Ranking Member Portman, along with the Committee staff, have already completed in the publishing the staff report "Case Studies In Ransomware Attacks On American Companies" and the Majority Staff report "Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns." Both of these reports highlight acute issues and we are grateful that this Committee is collaborating with public and private industry on, and that the Committee Members are already pursuing new and passing new legislation.

I would like to quickly address two primary areas of focus in these reports, first with regards to cryptocurrency. Financially motivated cyber criminals almost universally denominate ransom demands in cryptocurrency. The popularity of cryptocurrency with cybercriminals is rooted in protecting the ransom payment law enforcement seizure and the efficiency with which the money can be laundered. The percentage of a ransom that finds its way to the cybercriminal's pockets is substantially higher when cryptocurrency is used versus other currencies or stores of value.

This is clear when looking at the recovery rates between two types of cybercrime, wire fraud and ransomware. If reported within 72 hours, illegitimate wires can typically be reversed and recovered. No such mechanism exists with crypto currency.

It is important to note that unlike financial theft, ransomware is much more akin to a kidnap and ransom incident. Victims may not

[1] The prepared statement of Mr. Siegel appears in the Appendix on page 44.

want their funds reclaimed out of fear that the criminals will not reciprocate with decryption keys, critical to restore an organization's business. Reclaiming a ransom also requires that the victim make a timely report to the correct branch of law enforcement. Moreover, for a trace and seizure to be successful the end destination of the cryptocurrency must be within the reach of Western law enforcement. Most of the time, one or several of these variables inhibit a trace or seizure from even being started, let alone successful.

It is also important to note that some form of currency, whether it be physical fiat, digital, or cryptocurrency, has always been used for lots of different types of extortion. Ransomware existed before the advent of cryptocurrency, and it will persist if cryptocurrency were to ever disappear. As long as ransomware attacks are profitable to carry out against organizations with weak cybersecurity, cybercriminals will continue to proliferate these attacks.

This brings us to the second topic of today's hearing, mandatory reporting. Coveware has been vocal in our support for mandatory reporting for some time. Our hope is that reporting requirements will eventually be extended to all victims of ransomware, not just organizations under the oversight of CISA.

As with any new law the efficacy lies in its implementation. This hearing is uniquely timed to allow policymakers to understand the dynamics of reporting and to ensure that final rules achieve the targeted impact.

We believe there will be two primary impacts to mandatory reporting. First, the U.S. Government will gain clarity on the scope of the problem. As was clearly documented in the Majority Staff Report, the variance between privately reported ransomware statistics and agency reported statistics is cavernous. Collecting accurate statistics is step No. 1 and table stakes.

Gaining clarity will allow agencies to more confidently resource their responses, and we are encouraged to see that the Cyber Incident Reporting Act authored by Chairman Peters and Ranking Member Portman has begun to outline a clear path for reporting and unique agency responsibility.

The second impact will be in providing greater clarity on what to do about the problem. Gaining this clarity will hinge on what information CISA collects, and if CISA or other regulatory or law enforcement agencies are able to scalable digest the information reported to them. This new legislation has the potential to answer major questions, and enable CISA, the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS) and other agencies to make meaningful progress on this problem.

If not implemented correctly, however, this new legislation also has the potential to completely bury these agencies with unstructured data that cannot be parsed or analyzed at scale. This would render this new legislation completely ineffectual. Great care and focus should be applied to what information is collected, and how this information is organized so that the velocity of analysis, recommendations and actions can achieve maximum efficacy.

Thank you very much, Mr. Chairman. I look forward to answering the Committee's questions.

Chairman PETERS. Thank you, Mr. Siegel.

Our final witness is Jackie Burns Koven, Head of Cyber Threat Intelligence at Chainalysis, one of the leading cyber analytics companies that specializes in providing data, software, services, and research on blockchain technology.

Ms. Koven has extensive knowledge and experience in the cybersecurity sector, and as the Head of Cyber Threat Intelligence Ms. Koven leads efforts to track ransomware operators and their enablers on blockchains. Prior to joining Chainalysis, Ms. Koven served in the intelligence community.

Ms. Koven, welcome. You may proceed with your opening remarks.

TESTIMONY OF JACKIE BURNS KOVEN,[1] HEAD OF CYBER THREAT INTELLIGENCE, CHAINALYSIS

Ms. KOVEN. Thank you. 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 with global law enforcement, ransomware research, partnerships, and joint initiatives.

This hearing could not be more timely. We have seen ransomware attacks increase significantly over the last few years, with ransomware attacks on critical infrastructure, law enforcement agencies, health care providers, municipalities, schools, and other businesses. While it is true that cryptocurrency is generally the predominant form of payment in these cases, it is not true that cryptocurrency is the cause of ransomware attacks.

If there is one point I want to make to the Members of this Committee it is that the transparency of cryptocurrency and blockchains enhances the ability of policymakers and government agencies to detect, attribute, and ultimately disrupt illicit activity. In fact, it can be much easier to investigate cases involving the illicit use of cryptocurrency than other forms of payment. By identifying an illicit actor's cryptocurrency wallet, for example, from a ransom payment, law enforcement can gain insight into not only the cash-out destination but also the network of accomplices and malicious tools underpinning the threat actor's campaign.

In contrast, in a traditional financial investigation where that same actor is tied to a bank account, it is the beginning of a long resource-intensive process to subpoena records that can seldom generate a remotely comparable amount of insight and certainly not as timely. The investigative challenges would compound even more were that same illicit actor tied to a cash-based transaction.

Our ransomware data shows that there are at least $712 million worth of ransom payments in 2021, and while almost certainly an undercount of ransoms paid, this figure constitutes a record-breaking year in terms of ransomware revenue. This shows the magnitude of the ransomware problem and underscores the importance of enhanced reporting initiatives.

[1] The prepared statement of Ms. Koven appears in the Appendix on page 48.

One of the biggest trends we have recently observed is an increase in the rebranding of ransomware strains. This is likely in part to evade government scrutiny but also, in some cases, to obfuscate a ransomer group's connection to a sanction entity so that victims might still pay. We can often discern these rebrand attempts via blockchain analysis, which enables us to identify links between ransomware gangs using their cryptocurrency footprint.

Extortion tactics have also evolved to skirt traditional definitions of ransomware. More groups have emerged that will not encrypt victims' files but will still exfiltrate data and threaten to release or sell the data unless a ransom is paid. This trend means that policymakers and government agencies will need to be flexible about cyberattack definitions when requesting reporting on these events to encompass emerging threats.

I further detail the evolution of ransomware groups in my written testimony, including the geopolitical aspects of this those threats, ransomware money-laundering techniques, and the impact of law enforcement and the Office of Foreign Assets Controls (OFAC) actions against ransomware actors and their facilitators.

U.S. policies must leverage a whole-of-government approach for reducing ransomware attacks and mitigating their impact that incorporate private-public sector partnerships. In my written testimony I make a number of recommendations for this Committee and Congress to consider in order to improve the government response to this threat, and I will share just a few of these now.

First, it is vital that we improve ransomware reporting and information sharing. There should be clear guidance on when, what, and where to report incidents, and this information should be shared swiftly with law enforcement agencies to operationalize. In addition, we must ensure government agencies have adequate funding for the training, tools, and resources they need to conduct these investigations that require the development of new skill sets and government agencies to work quickly in order to keep up with the evolving threat landscape.

Finally, the U.S. should also work with other countries around the world to assist them in the development and implementation of robust anti-money laundering laws for cryptocurrency businesses to ensure that bad actors are cutoff from cashing out their ill-gotten gains in unregulated jurisdictions.

Thank you, and I look forward to answering your questions.

Chairman PETERS. Thank you, Ms. Koven.

On May 24th, after a 10-month investigation, I released a report on the rise in ransomware attacks and the use of cryptocurrency as ransom payments in these attacks, a report I entered into the record in my opening comments. One of my report's key findings is that the Federal Government simply does not have comprehensive data on ransomware threat landscape.

Ms. Stifel, I have two questions for you. First off, do you agree with this finding, and second, in the Institute for Security and Technology's Ransomware Task Force report your organization advocates for mandatory reporting requirements on ransomware attack payments made in cryptocurrency. Why do you believe that this data is necessary? If you could answer both those questions I would appreciate it.

Ms. STIFEL. Senator, I do agree with the observation or the finding that there is not sufficient information within the government's holdings about payments in cryptocurrencies. We know, as has been highlighted in the testimony of Ms. Koven as well as Mr. Siegel, that there are many who attempt to comply with these requirements and regulations. However, there are also those who do not, and this leads to a significant amount of discrepancy in the amount of information that may be available to those in the ecosystem versus those who are receiving information the government side.

The other challenge here is that within the organizations that do collect information on the government side, whether it be the Financial Crimes Enforcement Network (FinCEN), CISA, or the FBI's Internet Crime Complaint Center (IC3), they ask for different types of information, which also contributes to a disaggregated picture of the threat.

With regard to your second question, Senator, we believe that the mandatory reporting requirement will help the government have a better picture of the actual scale and scope of this threat. We also believe that that information needs to get into the hands of the private sector who, as I mentioned in my testimony, can work with the government to collectively combat these actors when the information is delivered in a timely manner and is relevant.

I do agree significantly with Mr. Siegel's comment that the government needs to be very structured in the way that it seeks the information that it will receive under the reporting requirement of the recently passed legislation. It is critical that the information be relevant and that the government is equipped to manage the information, not only in analyzing it itself but also in ensuring that it can receive and disseminate the information to private sector actors who can appropriately manage the information and take appropriation action with respect to it.

Chairman PETERS. Thank you. During my investigation, Federal agencies expressed to my team concerns with gaps in the ability to enforce anti-money laundering laws applicable to cryptocurrency against illicit actors outside of the United States. The report found that such gaps impede law enforcement's ability to investigate, to prosecute, and prevent cryptocurrency-enabled crimes.

Ms. Koven, and then Ms. Stifel, I will ask you to answer this question after Ms. Koven answers, what shortfalls do you see regarding enforcement of anti-money laundering regulations with respect to illicit cryptocurrency transactions, both in the United States and abroad? The second question, what has happened to address these shortfalls, and can regulations alone solve this problem, or does Congress have a role here?

If you could handle those questions for me now, and then Ms. Stifel after Ms. Koven.

Ms. KOVEN. Thank you for your question, Senator. Yes, we have observed a winnowing down of the cash-out destinations for illicit actors, including ransomware actors, mainly to offshore exchanges with little to no regulation and enforcement, which underscores our recommendation for enhanced U.S. assistance in implementing anti-money laundering (AML) laws, to cutoff those illicit cash-out destinations.

We have also observed the increased utilization of mixing services by these threat actors, to obfuscate the destination of these ransomware proceeds. I can point to a number of government successes over the last year that have actually used blockchain analysis to trace payments to these high-risk exchanges and law enforcement action against Garantex, Blender.io, Chatex, and Suex, primarily services based in Russia.

What we saw as a result of these designations, especially against Suex, was that deposits dropped nearly to zero as soon as the designations were rolled out.

There are a number of policy options for these illicit cash-out destinations, and blockchain forensics is a key tool in being able to identify where these threat actors are cashing out. If we look at Blender.io, that mixing service in particular, it was not only used by multiple ransomware groups, it was also used by North Korean launderers from stolen funds.

These threat actors are going for the paths of least resistance, but it has narrowed down considerably to a handful of services that the United States can help support with implementing AML regulations.

Chairman PETERS. Thank you, Ms. Koven. Ms. Stifel.

Ms. STIFEL. Thank you for the question, Senator. I would agree with Ms. Koven that the impact of regulation in the United States has resulted in many cases the offshoring of the ability for these actors to convert a cryptocurrency into fiat, and as a result the absence of regulation overseas has provided this pathway for the conversion to continue to facilitate the demand and the desire for ransomware as a tool to generate financial gain.

In other words, were we to have a more consistent regulatory environment internationally, through the application of know your customer anti-money laundering (KYC AML) and other regulatory measures, by working with partners, including through the Financial Action Task Force (FATF), that has been effective in the terrorism instances, that would provide a pathway, I think, for making a more significant impact on the ability for governments to obtain information that could facilitate arrests or other disruptive measures against these criminal actors.

Senator, you also asked about the role of Congress here, and I would agree. I think reporting legislation is a significant step forward. It was something that was called for in our task force report, as you mentioned. I think there is also an opportunity for Congress to continue to also clarify other measures that private sector entities may take with respect to information about cybersecurity incidents, including by clarifying the scope of the Cybersecurity Information Sharing Act of 2015, and to be constantly mindful of the importance of there being harmony across, and not overly complicating matters with respect to ongoing regulatory opportunities, looking to streamline the process to allow for consistency in application so that victims are clear where they need to report, what they need to report, and within what period of time. Also their role in ensuring that they are working to, and equipping them to better maintain their systems in a more secure manner to reduce the likelihood of ransomware in the future.

Chairman PETERS. Thank you. Senator Hawley, you are recognized for your questions.

OPENING STATEMENT OF SENATOR HAWLEY

Senator HAWLEY. Thank you very much, Mr. Chairman. Thanks to all of the witnesses for being here.

If I could start with you, Mr. Siegel. You said in your written testimony that financially motivated cybercriminals almost universally denominate ransom demands in cryptocurrency. Can you just expand on that? Why is that and what are the implications?

Mr. SIEGEL. For the most part ransomware actors know that they want to cash out their illicit proceeds using the most efficient means. Cryptocurrency is the most efficient means. It has great scale. They can move it very quickly across borders. It can be moved without worry of being reclaimed unless they make an operational security mistake or unless the move it through an exchange that participates with Western law enforcement. They also know that they have options to move their proceeds between different types of cryptocurrencies, which can further aid in the obfuscation and money laundering process and better the chances that a higher percentage of those ransom proceeds make it to their pocket at the end of the day.

Senator HAWLEY. Is there a specific cryptocurrency that is more often used than others for ransom demands, to your knowledge?

Mr. SIEGEL. Bitcoin is the predominant one, but I would note that some actors denominate their demands in other privacy-enhanced cryptocurrencies, like Monero. Even when Bitcoin is used for a ransom payment it is common for the Bitcoin to be exchanged into one of these privacy coins further down the money laundering process, to obfuscate the end destination.

Senator HAWLEY. Got it. Let me ask you this. I understand that there are about 10,000 active cryptocurrencies. That is up from 63, I think it was, a decade ago. That is incredible growth. Has the growing number of cryptocurrencies influence how ransom demands are being made, in your observation?

Mr. SIEGEL. No, it has not.

Senator HAWLEY. Interesting. Are new coins being made with criminal intentions in mind, do you think?

Mr. SIEGEL. It is certainly possible. I would bifurcate between new coins that are made with the express intent of committing financial fraud, these kinds of pump-and-dump schemes. Then what would appear to be legitimate projects, like Monero and others, that are aimed at the enhanced privacy of the coin itself, but with that come the attractiveness to the cybercriminals to use those coins for the money laundering process.

Senator HAWLEY. Are new coins being purposely designed or being made and purposely designed to be more opaque, in your observation?

Mr. SIEGEL. Some of these privacy coins are. That is the intention of the design, is to make them more private. I would note, though, that there are two challenging to having a coin actually be adopted by a large group of cybercriminals. No. 1, it has to work, and No. 2, it must be liquid. If there are thousands of completely illiquid privacy coins, but you cannot really buy or sell them, no one is going to use them, including cybercriminals. This is one of the reasons that Bitcoin is predominantly used is because it is the most liquid.

Senator HAWLEY. Got it. Ms. Koven, let me ask you, you said just a minute ago that the use of crypto can actually enhance these investigations, investigations into ransomware demands. You said in your written testimony that due to its transparent nature it can be much easier to investigate cases involving the illicit use of cryptocurrency than other forms of payment.

Can you just expand on that? I think that is an interesting point, maybe a counterintuitive point. Can you just say more about that?

Ms. KOVEN. Thank you for that question, Senator. As Mr. Siegel testified, Bitcoin is the predominant currency demanded in these ransomware cases. What blockchain forensics and the transparency of the blockchain can provide is able to see the cash-out destination of these currencies to exchanges that enable law enforcement to subpoena those exchanges, or know your customer information, as well as potentially freeze the accounts.

We can also move further up the kill chain to understand that threat actor and their wallet and the goods and services that they are purchasing that actually comprise that campaign, everything from Malware-as-a-service, access brokers, to compromised credentials and victim systems, to malware crypters, and all of those networks that are underpinning these attacks.

Senator HAWLEY. Why do you think it is that criminals are disproportionately using cryptocurrencies as opposed to, say, U.S. dollars? Do you agree with Mr. Siegel's analysis? I mean, what would you say about that?

Ms. KOVEN. Thank you. The same reason that Bitcoin is attractive to criminals is the same reason it is attractive for trading in a store of value. We have actually calculated that only 0.14 percent of overall transaction activity was criminal-related, of the $15 trillion of transactions last year.

It is the liquidity issue. Monero is illiquid and it is impractical to use. Many cryptocurrency exchanges have delisted Monero because of regulatory guidance about Monero and privacy coins in general.

Senator HAWLEY. Very good. Let me ask both of you about reporting requirements. I think, Mr. Siegel, in your written testimony you note that reporting requirements could burden Federal agencies with unstructured data that cannot be paired or analyzed at scale. Have I got that right? Am I remembering correctly?

So give me a sense, in light of that, how should agencies optimally implement reporting requirements, that they are effective?

Mr. SIEGEL. Sure. I believe that agencies should look to establish standardized frameworks such as National Institute of Standards and Technology (NIST) or the Mitre Att&ck framework that standardize the tactics, techniques, and procedures that the threat actors are utilizing. These frameworks come with standard hierarchies, standard names, standard codes. Ransomware attacks are incredibly repetitive.

The value of collecting the bottom end, the unstructured log data, which could be hundreds of gigabytes or terabytes for a single attack, is very minimal, but the value in abstracting that up a couple layers of altitude to just the tactics and techniques and procedures so that CISA could very quickly say, "OK, we have 10 reports that happened last week. They all used these tactics. These are tactics that we have not seen before. Let's get a timely warning out."

Conversely, if they were to collect the unstructured data it could require an army of individuals to perform weeks of forensic analysis before those same conclusions could be reached.

Senator HAWLEY. Do you have a view on this, Ms. Koven, about the optimal implementation of reporting requirements by agencies?

Ms. KOVEN. No, I agree with Mr. Siegel that the standardization is extremely important to be able to operationalize that information swiftly so that they can be used to subpoena cryptocurrency businesses and used for attribution and accountability of these threat actors. We had seen this in multiple high-profile cases, including the Netwalker ransomware takedown, where the most prominent affiliate of that group was actually arrested in Canada.

I think being able to operationalize and share these at scale can lead to further successes.

Senator HAWLEY. Very good. Thanks to you both. Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Senator Hawley. Next we have Senator Lankford, but Senator Lankford, I understand, has graciously agreed to recognize Senator Rosen, who has to preside.

Senator Rosen, you are recognized for your questions.

OPENING STATEMENT OF SENATOR ROSEN

Senator ROSEN. Thank you, Mr. Chairman. Thank you, Senator Lankford. I appreciate it. I want to thank the witnesses for being here and testifying today.

As a former software developer I helped to develop company-wide disaster recovery plans, develop and execute them, all the different scenarios. I have both experience and many thoughts on this matter, but we will talk about cryptocurrency today.

I want to talk a little bit about small business cybersecurity, because as the HSGAC Majority Staff Report on Ransomware and Cryptocurrency outlines, all it takes is one ransomware attack to cause a small company to go out of business. According to a recent Small Business Administration (SBA) survey, 88 percent of small business owners felt their business was vulnerable to a cyberattack.

Yet, of course, many businesses cannot afford to adopt professional IT solutions, hire cybersecurity professionals, and actually they have a limited time to devote to cybersecurity as they focus on growing their companies.

To help small business manage cyber risk, Senator Cornyn and I introduced the Improving Cybersecurity of Small Entities Act. This is bipartisan legislation to direct Federal agencies to develop common-sense cybersecurity recommendations, provide training for those small entities, including small businesses. This legislation passed out of this Committee in February, and hopefully will tell people the importance of offsite backups and how they use their journals, all kinds of things like that, of course, we know that they need to recover.

But ransomware, Mr. Siegel, how do the ransomware criminals choose their victims in the small business community? What are some of the trends that you are seeing, and in terms of tactics and techniques, what are they using specifically? Are they just going after the data? Are they going after modifying the programs with malware where restoring backups may not be as effective, or effective at all?

Mr. SIEGEL. Thank you for your question, Senator. We would describe ransomware attacks as opportunistic, not targeted. We view this problem as an economic problem, and targeting a specific company is uneconomical. There are numerous ways that ransomware actors can impact a small business or a large business, and most of those ways come from purchasing previously breached credentials or by mask-scanning the internet through freely available tools that allow them to look for vulnerabilities.

So they essentially are combing the internet, picking up lists very quickly, finding the lowest-hanging fruit, and then attacking those companies.

For instance, at the other end of the spectrum, the Colonial Pipeline attacks, I wholeheartedly believe that that was not a targeted attack meant to disrupt U.S. critical infrastructure. I do not think those attackers had any clue that that company controlled the volume of gasoline on the East Coast, and that would create a political issue, because U.S. consumers really do not like it when gas prices go up, and that it would cause a geopolitical issue. I think they saw a big energy company with a large balance sheet and the potential for a large ransom.

I think that same thinking applies to small businesses. When they find a target that is going to take them 15 to 20 minutes to compromise, and they can earn $50,000 to $100,000, potentially, of a ransom payment, that is too economical to not do.

A lot of the recommendations that we have made in our testimony, and a lot of the things that we talk about are to recognize that there is no silver bullet to this problem, but there are lots of different ways to impose costs. The ransomware kill chain, as we have discussed today, is one of those ways. But these incremental ways that companies can incrementally harden themselves, to make themselves harder targets, more expensive targets, we think are the best ways to actually achieve an exponential reduction in risk versus a linear one, as may be perceived, with just making small additions. But the reality is most small businesses have these very easy-to-exploit vulnerabilities present, and closing those vulnerabilities is a process of just knowing what they are and finding the time or budget to close them.

Senator ROSEN. Thank you. I agree with what you are saying, and obviously the data is bearing it out.

In the two minutes I have left I want to move over to health care cybersecurity, because, of course, this has really been increasing, attacks on our hospitals and clinics. As we even use more medical devices we understand the vulnerabilities there. In the FBI's 2021 Internet Crime Report the health care sector fell victim to ransomware far more than any other critical infrastructure sector last year. Health care entities increasingly are the target of these malicious cyberattacks. They result not only in data breaches but driving up the cost of care, and maybe ultimately even affecting patient outcomes.

Senator Cassidy and I introduced the Health Care Cybersecurity Act. Again, it is bipartisan legislation that would require CISA to coordinate with and make resources available to health care and public health sector entities, including by developing products tailored to the specific needs of small and rural hospitals—they have been a big target—and our health clinics.

Mr. Siegel and then Ms. Koven, with the ransomware criminals rapidly evolving their tactics, techniques, and procedures, how do you think this variety of health care entities can stay ahead of these threats and heighten their defenses against ransomware?

Mr. SIEGEL. Thank you, Senator. I can testify from experience, having dealt with a number of hospital cases, that there is nothing more horrific than a ransomware attack on a health care institution that puts patient care at risk. It is the most sensitive areas—the emergency room (ER), the neonatal intensive care unit (NICU), oncology—that depend on electronic medical records (EMR) software to provide critical patient care. When those things go down that care cannot be delivered.

Our sense is that, especially for critical infrastructure companies, having proper security is no different than the maintenance of a bridge. It is part of the cost of doing business, and it should be properly overseen and properly regulated.

As these attacks and tactics evolve, there is no getting around these organizations making a substantial and continued investment in their people, in their technology so they can stay ahead of these things and continue to provide this critical care.

Senator ROSEN. I know I only have a couple of seconds left. I have to go preside. Can you speak briefly to it, and then I am going to run to the presiding chair on the floor. Thank you.

Ms. KOVEN. Thank you. It is easy to lose the human cost and the toll when you look at ransomware figures, like $712 million paid those smaller businesses and hospitals, for example. We have actually calculated the median ransom payment is $6,000, so potentially smaller victims that do not necessarily make headlines but the impact is still devastating. Whether or not these institutions pay can still be devastating with the costs of remediation.

The other issue is that a lot of these smaller businesses and hospitals are not necessarily equipped to be able to understand the sanctions risk of potential payments, and so being able to support them in that way is important.

I will also add that the threat actors that are targeting the small businesses are also targeting the hospitals and other forms of infrastructure. So being able to shine a light on those tools and services, those threat actors that are underpinning this criminal economy that is driving ransomware is critical to disrupting ransomware.

Senator ROSEN. Thank you so much. I really appreciate you being here. Thank you again, Senator Lankford. Mr. Chairman.

Chairman PETERS. Thank you, Senator Rosen. Senator Lankford, you are recognized for your questions.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Thank you. Thanks to all the witnesses that are here. I want to walk through a little bit of the reporting and the cooperation and duplication within government. Just back of the envelope, as I look at this, FBI, CISA, Homeland Security Investigations (HSI), Treasury, U.S. Secret Service (USSS), the Securities and Exchange Commission (SEC) all have cryptocurrency entitles, all say, "Report to us. We want to be able to help through all this process." From entities on the outside working this cornucopia of three-letter agencies that are across the Federal Government that all have a cryptocurrency, cryptocrimes section of it, what does that look like? What are you getting as far as feedback?

I would like all three of you to be able to respond to that. All three of you have some insight on that. Mr. Siegel, do you want to go first?

Mr. SIEGEL. Sure. While it would be great if one agency could handle all of this, the reality is all the agencies have a specific role and function in imposing costs on these threat actors. I think the legislation that has recently been passed has taken the appropriate first step of designating a single agency and possible cooperating agencies to handle the initial inbound and triage of the reporting data, and then routing that information to the proper branches for investigations of different shapes and sizes.

I think it was noted in the CEO of Colonial Pipeline's testimony some of the frustration that he felt being overwhelmed with the volume of inbound duplicative requests from law enforcement agencies and regulators while he was trying to manage his company through an incident. I felt Mr. Blount during that testimony. It can be distracting if a victim of ransomware contacts the wrong agency. It can be distracting.

I think it is important, through this legislation and the rulemaking process, that it be made crystal clear where victims of ransomware, based on their State jurisdiction, regulatory jurisdiction, by industry, where they should go and what those requirements are so that the private industry, principally attorneys that advise and assist these victims, can study this and then give practical, timely advice and direct those victims to the proper agency in a timely manner.

Senator LANKFORD. Ms. Koven.

Ms. KOVEN. Thank you, Senator. I commend the legislation, specifically the tenets to aggregate and standardize the reporting. As an example, our data has recorded 14 times more ransomware payments than what was reported to FBI via IC3. This legislation will help bolster their intelligence.

In order to handle this amount of data coming their way I would hope the agencies are resourced appropriately with the tools and resources they need to operationalize this information, that can lead to the arrest and seizures of cryptocurrency payments. We have seen a number of successes from multiple agencies over the last year, targeting various facets of the kill chain, targeting those illicit cash-out destinations that are laundering the proceeds, targeting specific threat actors and holding them accountable, and imposing costs by denying them of the cryptocurrency payment that they sought.

So enhanced training and tools to be able to operationalize the influx of data, but also, I think, global cooperation with the U.S. agencies and global agencies is very important as the threats that are facing our global partners are also the same ones that are attacking us today.

Senator LANKFORD. We will come back to that. Ms. Stifel.

Ms. STIFEL. Thank you, Senator. I would agree with my fellow witnesses that there needs to be, as I mentioned a few minutes ago, greater clarity and simplicity in the ability for victims to share information with the government.

The other piece of this, of course, though, is that, as Ms. Koven just alluded to, there is a significant need for there to be adequate resources within departments and agencies to both ingest the information but also really to establish those relationships in the first place that facilitate this information sharing from victims to the government. Some will be required to do so under the legislation once the rulemaking process is complete, but others will not.

The ability to have adequate resources within the field, whether it be within CISA's regional staff members, whether it is with Secret Service or FBI agents, it is really critical to establish those relationships within the community in order to better equip the government as well as the private sector to play a meaningful role in combating ransomware wherever we, as I mentioned, find cybercriminals going next.

Senator LANKFORD. When you say "the community," you are not talking about individual businesses. You are talking about entities that actually coordinate this, private businesses that work with other private businesses to be able to protect them from ransomware. Is that correct?

Ms. STIFEL. It is both, I would say. Yes, it is. It is those who are working to help victims manage their unfortunate ransomware incident but actually we often talk about and encourage organizations to establish a relationship with CISA and with FBI before they become the victim of an incident. It is better to know who to call and what may be useful to the government, learn that information ahead of time so that when the unfortunate day occurs there is already an established working relationship and that can facilitate a much more rapid response, both for the government but also for the victim.

Senator LANKFORD. That is part of the challenge I want to lay out here, though. You do not know if that relationship is with FBI, with CISA, with HSI, with Treasury, with Secret Service, who that might be. It is one thing to be able to say they need to develop relationships, but to be able to maintain relationships with all those entities because they all will come calling. I left out—you were talking about the Colonial Pipeline—with the Department of Transportation (DOT), they may show up as well, and multiple other entities would show up as regulators to say, "Did you fill out the paperwork?"

This is still a convoluted mess at the worst possible moment for a company, for a hospital, whatever it may be, that just had a ransomware attack, and now they are getting bombarded with all these different Federal entities, calling them and wanting information in detail on this.

There has to be a single source. I know we are in the process of working that through. But we have to also not just have one as a primary but the others turn that off in the process of going through that.

I do need to clarify, as well, Ms. Koven, you talked about trying to be able to actually follow through, arrest, recover the information. From the Chairman's information of what they worked through already on this, 74 percent of the entities that are doing ransomware are Russian, Russian-affiliated, or Russian-controlled. The recovery at that point, in working with local law enforcement, clearly they are not going to cooperate. What is the best tool at this point to be able to get engagement?

Ms. KOVEN. Thank you for that question, Senator, and that is a primary focus for us. There have been several examples over the last year that have illustrated that even if the perpetrator is out of reach of U.S. law enforcement we can still impose costs. We can still seize assets. We can leverage our global partnerships to be able to triangulate these threat actors. We have also taken actions against their cash-out destinations. A lot of Russian-based services like Garantex, Suex, and Chatex have been on the designation list, and it has severely inhibited their businesses.

There are a number of ways we can still impose costs and then also work up the kill chain to identify those threat actors and enablers that access brokers, malware-as-a-service providers that are also fueling these campaigns.

If the Netwalker case is any example, this is a global problem. That Network affiliate was a Canadian-based individual and the most profitable affiliate of that cybercrime ring.

Senator LANKFORD. OK. Mr. Chairman, thank you.

Chairman PETERS. Thank you, Senator Lankford. Senator Hassan, you are recognized for your questions.

OPENING STATEMENT OF SENATOR HASSAN

Senator HASSAN. Thanks so much, Mr. Chairman, and thanks to you and the Ranking Member for holding this hearing, and to all of our witnesses, thank you for sharing your expertise with us and for being here today.

I want to start with a question to Ms. Stifel. Cryptocurrency can be used for illicit purposes, including in cyberattacks, such as when most of the $2.3 million stolen from the town of Peterborough, New Hampshire, was quickly converted to cryptocurrency to make it unrecoverable.

Last September, I wrote letters to several agencies, including the Department of Justice, the Internal Revenue Service (IRS), and the Financial Crimes Enforcement Network asking what actions the Federal Government can take to help reduce the illicit use of cryptocurrencies.

In the IRS's response to my letter the agency made several suggestions, including increasing know-your-customer requirements and strengthening suspicious activity reporting and compliance for businesses connected to cryptocurrency markets.

Ms. Stifel, could you discuss why these are important and how you would strengthen these requirements to help combat illicit uses of cryptocurrency?

Ms. STIFEL. Thank you, Senator. The utility of KYC requirements, suspicious activity reports, and other mechanisms through which the government can receive information about ransomware attacks, and particularly payments associated with them is essential to, as we talked about, following the money and facilitating not only industry but also the government in getting an adequate picture of what is happening with these payments, the affiliates and the actors who are continuing to launch these types of incidents.

Unfortunately, though, as we have also talked about today, there is inadequate and inconsistent compliance with these requirements, particularly when you leave the United States' jurisdiction.

I would also note, though, that there are—and this is hopefully clear in the diagram that I shared in my written testimony—there are a number of other entities within the kill chain that may not have reporting requirements but may have relevant information, and oftentimes they currently work with each other to share that information with the government. I think there is an opportunity to look at other ways through which the government can obtain information, not necessarily from those who are currently subject to KYC and AML requirements.

Senator HASSAN. Thank you, and we will follow up with you on your diagram and information, as well.

To both Ms. Koven and Ms. Stifel, in your written testimony both of you commented that sanctions can be effective in preventing criminals from receiving or laundering ransomware payments. Do you believe that the Federal Government should more aggressively sanction ransomware groups and entities that help launder ransom payments, and what are the barriers to implementing more aggressive sanctions?

We will start with you, Ms. Koven.

Ms. KOVEN. Thank you for your question, Senator. I defer to policymakers on whether more sanctions should be enforced. But I will say that the impact of sanctions on some of these services that had been identified as participating in ransomware laundering—Garantex, Suex, Chatex, Blender, the mixing services—sanctions have been catastrophic to their business, severely damaging their operations. There has also been designations against specific individuals tied to ransomware groups.

I think we have also seen that sanctions have impacted ransomware groups' ability to receive payments from certain victims once they are designated, because we can use blockchain forensics to actually identify ransomware groups rebranding, trying to obfuscate their connection to sanctioned entities.

We do provide tools and services for transaction monitoring, to identify a payment is made to a sanctioned jurisdiction or potentially sanctioned entity, and I think further implementation of those can also help prevent or identify any kind of sanctions violations.

Senator HASSAN. Thank you. Ms. Stifel.

Ms. STIFEL. Thank you, Senator. In the task force's report that we published last year we noted, and as has been also discussed in the hearing today, the need for an all-tools approach to combating ransomware. As Ms. Koven has mentioned, and we have also seen recent reports from members of the Administration, it appears that sanctions have been effective in reducing the ability for ransomware actors to cash out their proceeds. So that suggests that they have been an effective tool.

With respect to your question about what barriers exist to the use of sanctions in this kind of all-tools approach, I would point to the concern around the degree of information that is reported about ransomware activity with an adequate picture of the scale and scope of this type of cybercrime. It inhibits the government's ability to identify and develop that sanctions package that allows them to fulfill the requirements under sanctions laws and regulations to have sufficient evidence to designate a particular entity and then for the private sector to then follow through with their requirements to prohibit and limit the ability for those actors to gain their proceeds.

Senator HASSAN. Thank you.

Mr. Siegel, in your written testimony you indicated that some ransomware victims do not want law enforcement to try to recover their ransomware payment because they are worried that the criminals will not honor the commitments made in return for the ransom payment. This obviously presents a potential problem because those payments make ransomware profitable and help facilitate future cyberattacks. There are also likely other victims who do not want to involve law enforcement at all.

In your experience working with ransomware victims, what percentage of victims do not want to recover their payments, even if they are given a viable option, and what percentage of victims do not want to involve law enforcement at all, and what do you think we could do to alleviate their worries?

Mr. SIEGEL. I would say that if it were a risk that the victims would not get their deliverables, the decryption keys or these things, which they are a prize that that has a potential risk, that number could fluctuate between 0 and 100 percent. I would say that, in general, probably close to half of the victims would volunteer to have their money seized or reclaimed because they are not as concerned about possible recrimination from the threat actors.

As is relates to nonreporting, in the absence of requirements I would say that the minority of victims of ransomware would even both, because it is a hassle to them and they want to get on with their life.

One of the most challenges aspects that we cited in our discussions with the staff ahead of this were the ability for law enforcement to proactively reapproach victims to collect evidence in the proper format so they can be submitted as evidence to secure indictments. This process can take months, sometimes years. When we approached the percentage of those victims that voluntarily participate it is very low. That is very frustrating to law enforcement.

I think that through this rulemaking and through mandatory reporting the door is now open to try and not only collect more accurate information through the reporting but create mechanisms whereby law enforcement can reapproach victim of attacks and secure the evidence necessary to achieve these indictments.

I would also note, per your prior questions, a lot of the ability for our agencies to sanction these groups depend on the investigations, and when those investigations cannot conclude we cannot get to the finish line on imposing sanctions.

Senator HASSAN. Yes. Thank you. Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Senator Hassan.

Ms. Koven, you testified earlier that only, I think it is 0.15 percent of cryptocurrencies are used in illicit transactions, and yet according to your report, the 2022 report, the illicit use of cryptocurrency has grown from $7.8 billion in 2020, to an all-time high of $14 billion in 2021. The report explicitly acknowledges that such illicit activity, "represents a significant problem."

Clearly you have a very small percentage there, but I think the vast majority of all the transactions in crypto are people speculating back and forth, kind of similar to the Dutch tulip mania, as they bid the prices up.

My question to, though, is, do we know the percentage of cryptocurrency that is actually used to buy a legitimate good or service? I do not think folks are going to Walmart or CVS. Are people actually using this to buy something? What percentage?

Ms. KOVEN. Thank you for that question, Senator. Yes, we had noted 0.14 percent of transactions last year had an illicit component to it, and the vast majority of transactions were legitimate, trading, remittances, and viewing cryptocurrency as a store of value.

Chairman PETERS. But what percentage? What percentage are actually for products and goods?

Ms. KOVEN. I do not have that answer on hand. My team can get back to you. But I would say it is a near daily occurrence that a new business that you and I might frequent is offering cryptocurrency as a form of payment. While it is not certainly prolific—you cannot pay your rent in cryptocurrency today—there are more and more businesses that are adopting cryptocurrency as a form of payment. This is a global phenomenon. You can find more available in other jurisdictions.

What I will say is that because it is more difficult to buy goods and services with cryptocurrency today it is why individuals, and even threat actors, rely on cryptocurrency businesses like exchanges to convert their cryptocurrency to other forms of fiat, like dollars and euros, which is a great intelligence lead for investigations.

Chairman PETERS. Very good. Senator Sinema, you are recognized for your questions.

OPENING STATEMENT OF SENATOR SINEMA

Senator SINEMA. Thank you, Mr. Chairman. Thank you to our witnesses for joining us today.

Ransomware attacks have wreaked havoc on communities across Arizona and our country, from last year's attack on the city of Kingman to the recent attempted hack against Yuma Regional Medical Center. Ransomware disrupts our lives, breaches sensitive data, and causes real-world harm.

Our Bipartisan Infrastructure Law invests in State and local cybersecurity to combat ransomware, and I co-sponsored legislation creating new cyber incident reporting requirements. We need to continue to work together to enhance our cybersecurity and hold hackers and the countries that provide them safe harbor accountable.

My first question is for you, Ms. Koven. In March, your company's co-founder testified before the Senate Banking Committee. I asked him about some of the more sophisticated techniques used by ransomware gangs to make ransom payments harder to trace, including the use of mixer and tumbler services to combine cryptocurrency from illicit sources with crypto from lawful sources.

Mr. Levin noted that Chainalysis has actually been able to successfully demix certain transactions. Without revealing your specific demixing capabilities, could you expand on this, and how great of threat to ransomware investigations do cryptocurrency mixers currently pose?

Ms. KOVEN. Thank you for your question, and this is an especially important topic because we have identified mixers being incorporated more frequently into ransomware laundering techniques.

As you mentioned, we have recently publicly disclosed our demixing capabilities, and while we cannot go into details because of ongoing investigations, what I can say is that we make every effort to identify all available mixers that these threat actors might be able to use so that our law enforcement partners and investigators, when conducting and tracking ransomware payments, can understand when they are tracing into a mixer and do not attempt to trace through it.

Senator SINEMA. Mr. Siegel, you help victims negotiate with hackers and protect their specific company from further harm. While paying a ransom might be the smart move for a particular victim, these payments are the fuel that motivates hackers to keep launching additional attacks. How do you balance the immediate need to restore a client's systems with the concern that paying a ransom might put a target on your client's back in the future? When the decision is made to pay the ransom, how do you ensure that crypto is not sent in violation of U.S. sanctions, particularly given how many attacks are linked to countries like Russia and North Korea?

Mr. SIEGEL. Thank you for your question. With regards to the first part on how the decision is made, the use of data is key. There are certain types of ransomware that can cause a substantial amount of file corruption. There are certain threat actors that default if paid, i.e., they do not provide the decryption tools or keys. Providing accurate information on the forecasted outcome of what will actually happen if a ransom is paid is step No. 1, so the company can make a clear decision.

Step No. 2 is for the company to understand that this is an option of last resort. It has to be weighed against all other available paths to restore critical data. If there is one myth with ransom payments it is that it is easy and it is fast. It is the exact opposite. The vast majority of the time, when companies have adequate backups, even if those backups are going to take a very long time to recover, that is actually faster and is going to avail them to a much quicker recovery time than paying a ransom.

So step No. 1 is to make sure that they understand the facts and that they are making a good, data-driven decision.

To your second question about compliance, our firm has developed a comprehensive compliance program. It comes from our background. I personally came from the regulated financial services industry and ran and built large comprehensive compliance programs. We took with us that compliance program when we founded our company.

We do three principal things that revolve around the attribution of the threat actor and other characteristics of the attack. No. 1 is we are looking at qualitative technical forensic and cryptocurrency information to check along the lines of common Bank Secrecy Act (BSA) Know-Your-Customer lines that the threat actor is not immediately listed on any sanctions list, both domestically and internationally. No. 2, we are looking at the wallet address, using products like Chainalysis to determine if the wallet is clustered or cospent with any sanctioned wallets.

And No. 3, most poignantly, is we keep our own internal restricted list, whereby we are tracking all the known sanctioned actors, and as they change their identity and further try and obfuscate who they are over time, we are tracking these things so that when the same threat actor that was sanctioned a year ago is on variant number seven to try and obfuscate their identity, we can identify it.

That is actually the vast majority of the time when there is a sanctions issue in an active incident, it is not a one-for-one identification of this name that you were attacked by is on an actual list. It is this name that you were attacked by is actually this person or group, and here is the evidence of how we have made that attribution.

So we perform all of these checks well ahead of any payment being made. We provide all those facts and circumstances to the victim and allow them to make the decision accordingly.

Senator SINEMA. Thank you.

Ms. Koven, the hackers behind some of the most devastating ransomware attacks are often located, or in some cases even sponsored by the governments of countries like Russia, North Korea, China, Iran. This means that even when we are able to identify those behind an attack, our criminal justice system is not able to hold those hackers accountable. That makes it particularly important that we successfully recover more ransom payments so these attackers, at the minimum, are not rewarded for their crimes.

What lessons can we learn from the FBI's successful recovery of much of the cryptocurrency used to pay the Colonial Pipeline ransom, and with enhanced public-private partnerships and datasharing is it feasible to help ransomware victims recover ransom payments on a more routine basis?

Ms. KOVEN. Thank you for that question, Senator. Yes, we have identified nearly 74 percent of ransom payments have a Russian affiliation, and we have seen, over the last year, several successes, including the Colonial Pipeline, of asset recovery from threat actors that exist outside of U.S.-friendly jurisdictions.

Not only is asset seizure a powerful tool but we have also been able to cripple some of the primary cash-out destinations, including those exchanges based in Russia, like Garantex, Suex, and Chatex, that laundered a large amount of ransomware proceeds.

I would further like to say there has been nearly $50 million in ransomware funds seized from ransomware-related actors, and there is also the risk of nation-state actors getting involved in ransomware that are not focused on the monetary reward but are using ransomware as a cover for more strategic aims of espionage and disruption.

Then the question then becomes, how did these nation-state actors get their hands on those tools and services to conduct the attack? Blockchain forensics can shine a bright light on those necessary tools and services that facilitate nation-state actors as well as financially motivated criminal gangs.

Senator SINEMA. Thank you. Thank you, Mr. Chair.

Chairman PETERS. Thank you, Senator Sinema.

Ms. Koven, I want to go back to, because of the questions that I was asking related to transactions for goods and services, you said a lot of businesses now are starting to accept crypto. Do you have any numbers or any estimate as to what you are seeing in that area?

Ms. KOVEN. Senator, I apologize I do not have those figures on hand but we can get back to you.

What I did want to say previously is that we have seen a 500 percent increase in cryptocurrency transactions in the last year, and we have seen many institutional players getting involved in cryptocurrency and viewing it as an asset class. This has accelerated the adoption of cryptocurrency for legitimate use cases, and as you have pointed out, also an increase in the raw number of illicit transactions that we have been able to detect. It was $14 billion last year.

Chairman PETERS. But I want to be clear. When you are talking about all the transactions, these are investment transactions. They are not an increase of transactions of people actually going out and buying stuff. Maybe help me. If you are a business and you say you will accept crypto to pay for a service, if you accept dollars, you know the dollar tomorrow will still be worth a dollar, and next week it is still going to be worth a dollar. But crypto, like yesterday, I think many of the major cryptos dropped nine percent, or a 10 percent drop. That would be like the Dow Jones (DJIA) dropping 3,000 points in a day, which is a pretty huge drop.

If you are a business and you say, “I will sell you a product for crypto,” but it may be worth 10 percent less tomorrow, I do not know what it will be worth. It could be greater, I guess, as well. But based on what we have seen recently it has been falling because it is a highly speculative asset.

What is the incentive for a business to take crypto as opposed to a dollar when they are trading for an actual service?

Ms. KOVEN. Thank you for that question, Senator. I am possibly not best-suited to answer that question in my current role, but what I will say is that many investors are in cryptocurrency for the long haul, and they have experienced dips and spikes in the ecosystem over the past few years. The same with threat actors. They are also dealing with cryptocurrency, viewing it as a long-term investment. But we can get back to you on specific numbers if you would like, sir.

Chairman PETERS. Yes. I would just be curious if you are going to track this. Clearly we all know it is a speculative asset that people are investing in, and it is highly volatile. We get that. But it is a medium of exchange, and most people think of a medium of exchange as it is going to be fairly consistent worth. If you buy a good from me and you give me a dollar, I will be able to buy a dollar's worth of another good somewhere else in the next day or two, or whenever it may be, which is different than a speculative stock or investing in stock options or other kinds of speculative assets. They are different.

But we do know that because, for a variety of reasons, as we have heard today, that criminals are very attracted to crypto, and that is a big part of what the currency is used for when the actual kind of goods or services transaction is illicit. It is criminals that use this currency. In addition to speculators, it is criminals that seem to be using crypto.

My question for Ms. Stifel, are there some additional tools that could help the Federal Government recover cryptocurrency ransom payments that have already been made? What additional tools should we be thinking about?

Ms. STIFEL. Thank you, Senator. I think one of the biggest tools that can be made, in part thanks to the work of this Committee has been made, is investing both in the cyber funds and the emergency authorities that have come through with the legislation that has been passed but also thinking about what we have talked about previously is better equipping departments and agencies to manage the investigatory process that is required in order to follow the money through the blockchain.

Those investments also would be useful to better equip departments and agencies to engage their international counterparts and to push for the broader application of KYC, AML, and other measures more broadly internationally, including, as I mentioned, through the Financial Action Task Force but in other multilateral bodies where working with Europol, for example, or Interpol, more effective engagement can be made with counterparts in a range of countries where we know that cybercriminals are turning, for example, looking at Costa Rica, Peru most recently.

The United States is not the only country targeted with ransomware, and it is essential to really combat this at a global scale, that we have partners in a range of jurisdictions who are able to meaningfully engage with us as we seek to investigate these malicious activities.

Chairman PETERS. Thank you. Ms. Koven, the last question here. If you could explain to the Committee, talk a little bit more about unhosted wallets and what risk exists when crypto is transferred to unregulated, peer-to-peer exchanges and unhosted wallets. What should we know about that?

Ms. KOVEN. Thank you for your question. If I may address the previous comment, I do want to say that cryptocurrency is a technology, and as long as technologies have existed there have always been bad actors willing to exploit it. Yes, there is significant volatility in cryptocurrency. There is the mechanism of stablecoins, which can hold value. We do see legitimate trading activity as well as cryptocurrencies used in remittances, and it is an opportunity for the United States to be a key, predominant player in this financial ecosystem by harnessing this technology, and the applications that can be built on top of it provide tremendous opportunity and job growth for national security.

What I want to say about private wallets, we do focus on identifying services—exchanges, darknet markets, ransom payments. But in the course of our investigations we do sometimes come across private wallets belonging to a threat actor, which allows us to monitor that wallet and also understand that threat actor's spending habits, all the tools and services purchased by that threat actor, and also cash-out destinations like peer-to-peer or cryptocurrency exchanges.

Peer-to-peer services are also obligated to regulatory requirements—AML, CFT requirements—that do require KYC and other forms of identification.

Chairman PETERS. Right. Thank you.

I want to thank all of our witnesses for participating in today's discussion, and I look forward to building on what we have learned from today's testimony, including additional ways to combat the national and economic security threats posed by ransomware attacks.

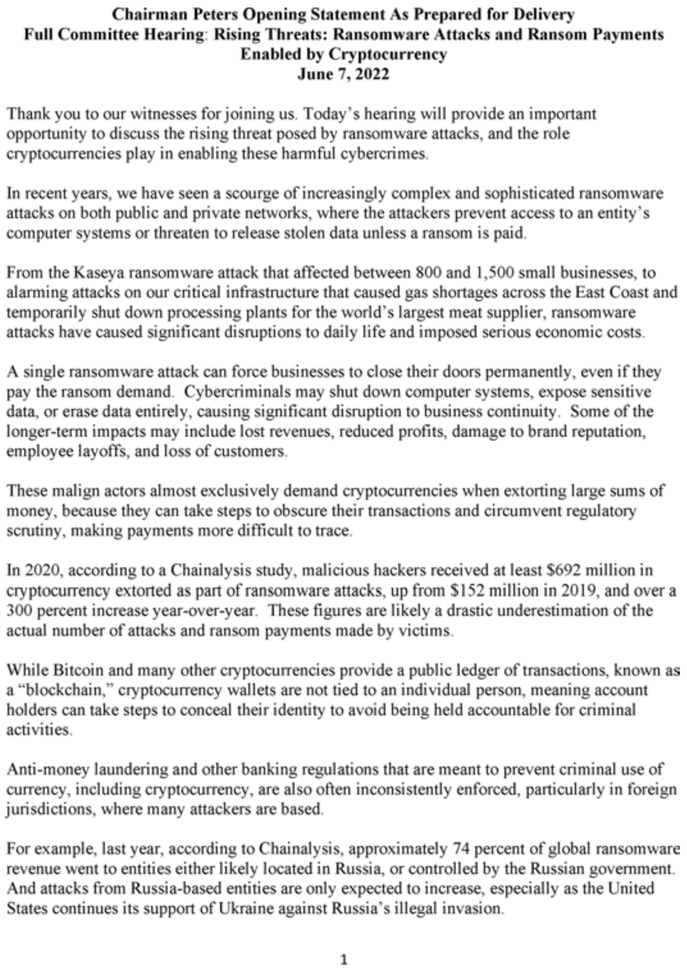
I plan to continue my investigation to further examine the role cryptocurrencies play in these cybercrimes and other criminal activities, and I look forward to exploring the issues identified during today's hearing in detail, including shortfalls in the enforcement of applicable anti-money laundering regulations for cryptocurrency transaction.

The record for this hear will remain open for 15 days, until 5 p.m. on June 22, 2022, for the submission of statements and questions for the record.

This hearing is now adjourned.

[Whereupon, at 11:24 a.m., the hearing was adjourned.]

APPENDIX



Chairman Peters Opening Statement As Prepared for Delivery
Full Committee Hearing: Rising Threats: Ransomware Attacks and Ransom Payments Enabled by Cryptocurrency
June 7, 2022

Thank you to our witnesses for joining us. Today's hearing will provide an important opportunity to discuss the rising threat posed by ransomware attacks, and the role cryptocurrencies play in enabling these harmful cybercrimes.

In recent years, we have seen a scourge of increasingly complex and sophisticated ransomware attacks on both public and private networks, where the attackers prevent access to an entity's computer systems or threaten to release stolen data unless a ransom is paid.

From the Kaseya ransomware attack that affected between 800 and 1,500 small businesses, to alarming attacks on our critical infrastructure that caused gas shortages across the East Coast and temporarily shut down processing plants for the world's largest meat supplier, ransomware attacks have caused significant disruptions to daily life and imposed serious economic costs.

A single ransomware attack can force businesses to close their doors permanently, even if they pay the ransom demand. Cybercriminals may shut down computer systems, expose sensitive data, or erase data entirely, causing significant disruption to business continuity. Some of the longer-term impacts may include lost revenues, reduced profits, damage to brand reputation, employee layoffs, and loss of customers.

These malign actors almost exclusively demand cryptocurrencies when extorting large sums of money, because they can take steps to obscure their transactions and circumvent regulatory scrutiny, making payments more difficult to trace.

In 2020, according to a Chainalysis study, malicious hackers received at least $692 million in cryptocurrency extorted as part of ransomware attacks, up from $152 million in 2019, and over a 300 percent increase year-over-year. These figures are likely a drastic underestimation of the actual number of attacks and ransom payments made by victims.

While Bitcoin and many other cryptocurrencies provide a public ledger of transactions, known as a "blockchain," cryptocurrency wallets are not tied to an individual person, meaning account holders can take steps to conceal their identity to avoid being held accountable for criminal activities.

Anti-money laundering and other banking regulations that are meant to prevent criminal use of currency, including cryptocurrency, are also often inconsistently enforced, particularly in foreign jurisdictions, where many attackers are based.

For example, last year, according to Chainalysis, approximately 74 percent of global ransomware revenue went to entities either likely located in Russia, or controlled by the Russian government. And attacks from Russia-based entities are only expected to increase, especially as the United States continues its support of Ukraine against Russia's illegal invasion.

Last month, I released a report examining the role cryptocurrencies play in incentivizing and enabling ransomware attacks, and the resulting harm these attacks have on victims.

I now move to introduce this report as part of the hearing record. … Without objection, the report will be entered into the record.

My investigation found that the federal government lacks sufficient data and information on ransomware attacks and the use of cryptocurrency as ransom payment in these attacks, and must collect better data to understand the scope of the threat.

The cyber incident reporting law that Ranking Member Portman and I authored and passed earlier this year marks a significant first step to getting the information the government needs to combat this growing threat.

The legislation will require critical infrastructure owners and operators to report cyber-attacks within 72 hours and ransomware payments within 24 hours, and I look forward to working with the Administration to ensure it is swiftly and effectively implemented.

The more information we have, the better suited we will be to combat ransomware attacks. That means continuing to build off our bipartisan cyber incident reporting legislation by holding foreign adversaries and cybercriminals accountable, and finding ways to reduce the incentives to conduct these attacks in the first place, including by examining their use of cryptocurrency.

While I am grateful to the many federal law enforcement and regulatory agencies that have taken steps to address cybercriminals and the rising threat of ransomware attacks, more must be done to ensure cryptocurrencies are monitored appropriately, like their non-digital counterparts.

Finally, in addition to addressing ransomware attacks and use of cryptocurrency as ransom payment in those attacks, Congress must examine other criminal activity involving cryptocurrency that threatens our nation's economic and national security, such as human trafficking, the flow of illicit drugs across our borders, and other serious crimes.

I look forward to hearing from today's panel of expert witnesses who can further elaborate on the uses of cryptocurrency in ransomware attacks, and provide answers to ensure we have the necessary tools and resources to tackle this issue head on.

OPENING STATEMENT
RANKING MEMBER ROB PORTMAN
RISING THREATS: RANSOMWARE ATTACKS AND RANSOM PAYMENTS ENABLED BY CRYPTOCURRENCY

June 7, 2022

Thank you, Mr. Chairman. And thank you to our witnesses for joining us.

Today we will hear from a private sector panel of cybersecurity professionals and incident responders who will provide their unique perspective on what can be done to combat ransomware.

The frequency and severity of ransomware attacks continues to grow. Ransomware groups have professionalized their operations using a business model often called ransomware-as-a-service—which involves ransomware developers selling or delivering their malware to individuals called "affiliates" who actually carry out the attack. This allows ransomware gangs to conduct more attacks with broader impact.

Back in March, I released a report documenting the experiences of three American companies victimized by one of the most notorious Russian ransomware gangs, called REvil [are-evil]. The companies profiled in the report are from different business sectors and vary significantly in size, revenue, and IT resources. Despite those differences, they all fell victim to REvil. This underscores the broad threat ransomware presents and the proactive steps all organizations must take to implement cyber best practices.

REvil was largely believed to be offline following the arrests of several key members last fall. But public reports indicate the gang may be resuming operations. We know it is common for ransomware criminals to claim retirement only to "rebrand" and reemerge under a new name.

About a year ago, this Committee held a hearing on the Colonial Pipeline ransomware attack. That incident was a painful reminder that these attacks have real-world consequences impacting the everyday lives of Americans.

Attacks like Colonial Pipeline or any of the numerous significant ransomware attacks over the past year demonstrate how difficult it is for organizations to account for all vulnerabilities and defend against sophisticated cyber adversaries.

Recognition of this challenge is one of the reasons Chairman Peters and I drafted cyber incident reporting legislation which I am proud to say became law in March.

This law will enhance our nation's visibility into cyberattacks against the United States and enable a more effective response including warning potential victims. It is important that CISA works with industry experts and stakeholders to implement this law quickly.

We know ransomware attacks will continue to be a national security threat for the foreseeable future. As the committee of jurisdiction over cybersecurity, we will continue to work to identify solutions that address the threats associated with ransomware attacks and the ways we can fortify our defenses.

I look forward to the testimony of our witnesses on these important issues.

IST Institute for SECURITY + TECHNOLOGY

securityandtechnology.org

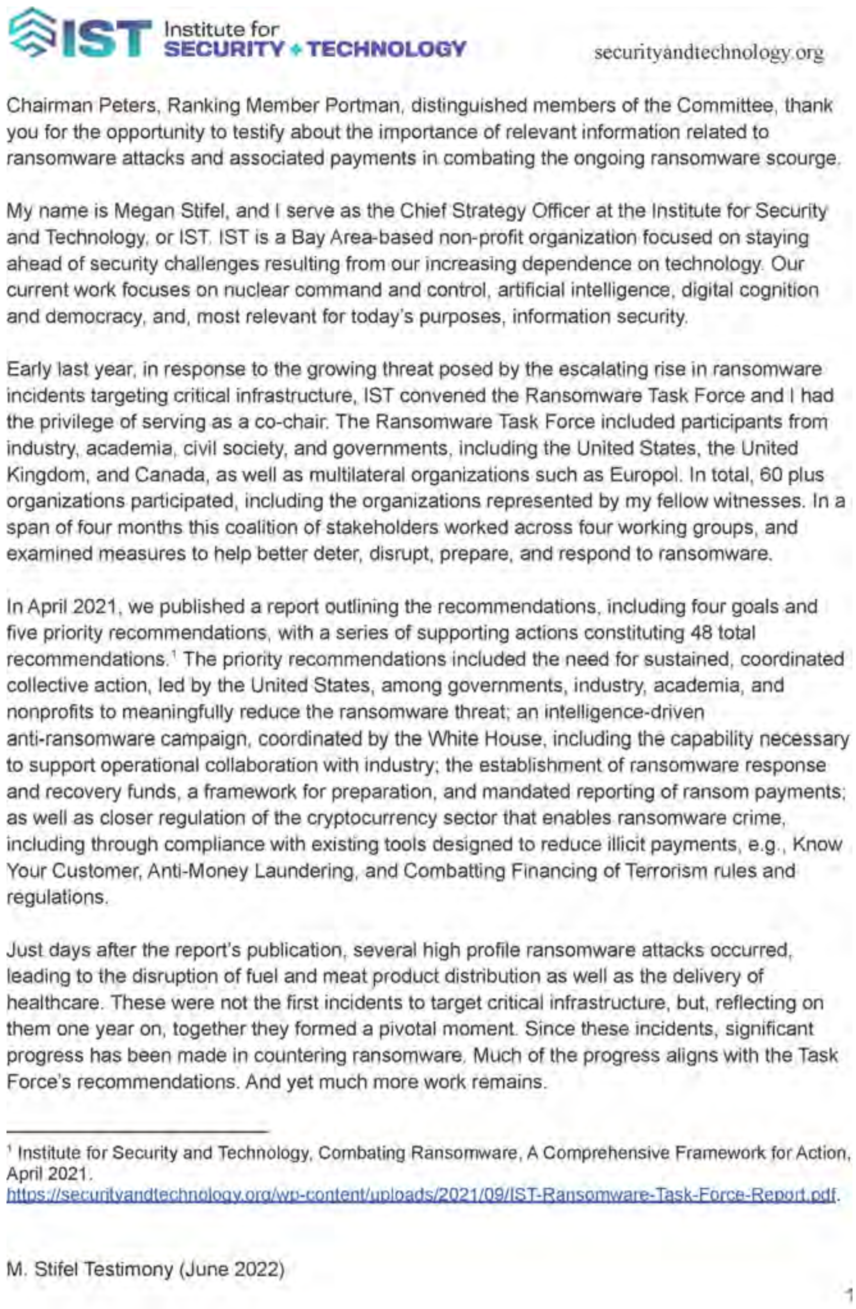
Testimony of

Megan H. Stifel
Chief Strategy Officer
Institute for Security and Technology

Before the
United States Senate
Committee on Homeland Security

"Rising Threats: Ransomware Attacks and Ransom Payments, Enabled by Cryptocurrency"

June 7, 2022



IST Institute for SECURITY + TECHNOLOGY

securityandtechnology.org

Chairman Peters, Ranking Member Portman, distinguished members of the Committee, thank you for the opportunity to testify about the importance of relevant information related to ransomware attacks and associated payments in combating the ongoing ransomware scourge.

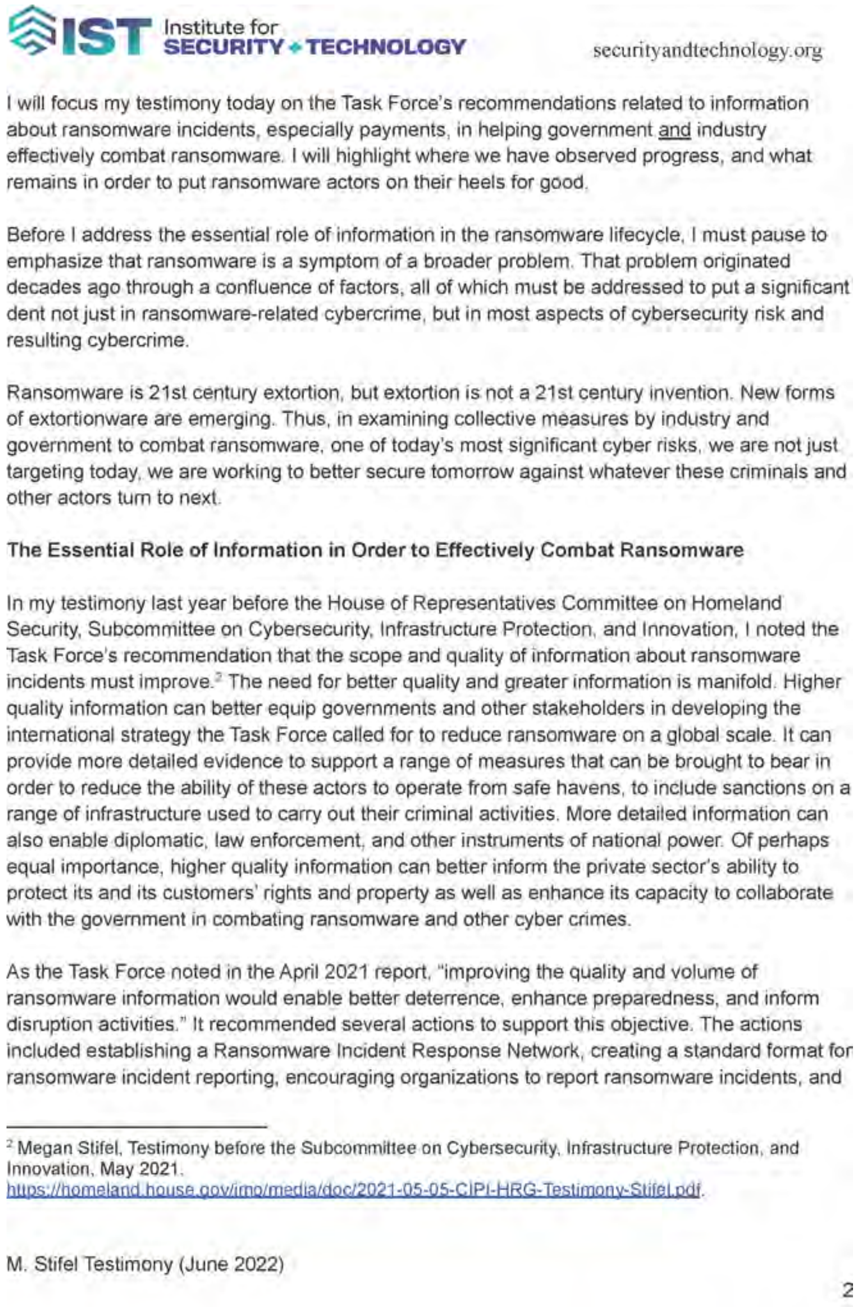
My name is Megan Stifel, and I serve as the Chief Strategy Officer at the Institute for Security and Technology, or IST. IST is a Bay Area-based non-profit organization focused on staying ahead of security challenges resulting from our increasing dependence on technology. Our current work focuses on nuclear command and control, artificial intelligence, digital cognition and democracy, and, most relevant for today's purposes, information security.

Early last year, in response to the growing threat posed by the escalating rise in ransomware incidents targeting critical infrastructure, IST convened the Ransomware Task Force and I had the privilege of serving as a co-chair. The Ransomware Task Force included participants from industry, academia, civil society, and governments, including the United States, the United Kingdom, and Canada, as well as multilateral organizations such as Europol. In total, 60 plus organizations participated, including the organizations represented by my fellow witnesses. In a span of four months this coalition of stakeholders worked across four working groups, and examined measures to help better deter, disrupt, prepare, and respond to ransomware.

In April 2021, we published a report outlining the recommendations, including four goals and five priority recommendations, with a series of supporting actions constituting 48 total recommendations.[1] The priority recommendations included the need for sustained, coordinated collective action, led by the United States, among governments, industry, academia, and nonprofits to meaningfully reduce the ransomware threat; an intelligence-driven anti-ransomware campaign, coordinated by the White House, including the capability necessary to support operational collaboration with industry; the establishment of ransomware response and recovery funds, a framework for preparation, and mandated reporting of ransom payments; as well as closer regulation of the cryptocurrency sector that enables ransomware crime, including through compliance with existing tools designed to reduce illicit payments, e.g., Know Your Customer, Anti-Money Laundering, and Combatting Financing of Terrorism rules and regulations.

Just days after the report's publication, several high profile ransomware attacks occurred, leading to the disruption of fuel and meat product distribution as well as the delivery of healthcare. These were not the first incidents to target critical infrastructure, but, reflecting on them one year on, together they formed a pivotal moment. Since these incidents, significant progress has been made in countering ransomware. Much of the progress aligns with the Task Force's recommendations. And yet much more work remains.

[1] Institute for Security and Technology, Combating Ransomware, A Comprehensive Framework for Action, April 2021. https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf.



I will focus my testimony today on the Task Force's recommendations related to information about ransomware incidents, especially payments, in helping government and industry effectively combat ransomware. I will highlight where we have observed progress, and what remains in order to put ransomware actors on their heels for good.

Before I address the essential role of information in the ransomware lifecycle, I must pause to emphasize that ransomware is a symptom of a broader problem. That problem originated decades ago through a confluence of factors, all of which must be addressed to put a significant dent not just in ransomware-related cybercrime, but in most aspects of cybersecurity risk and resulting cybercrime.

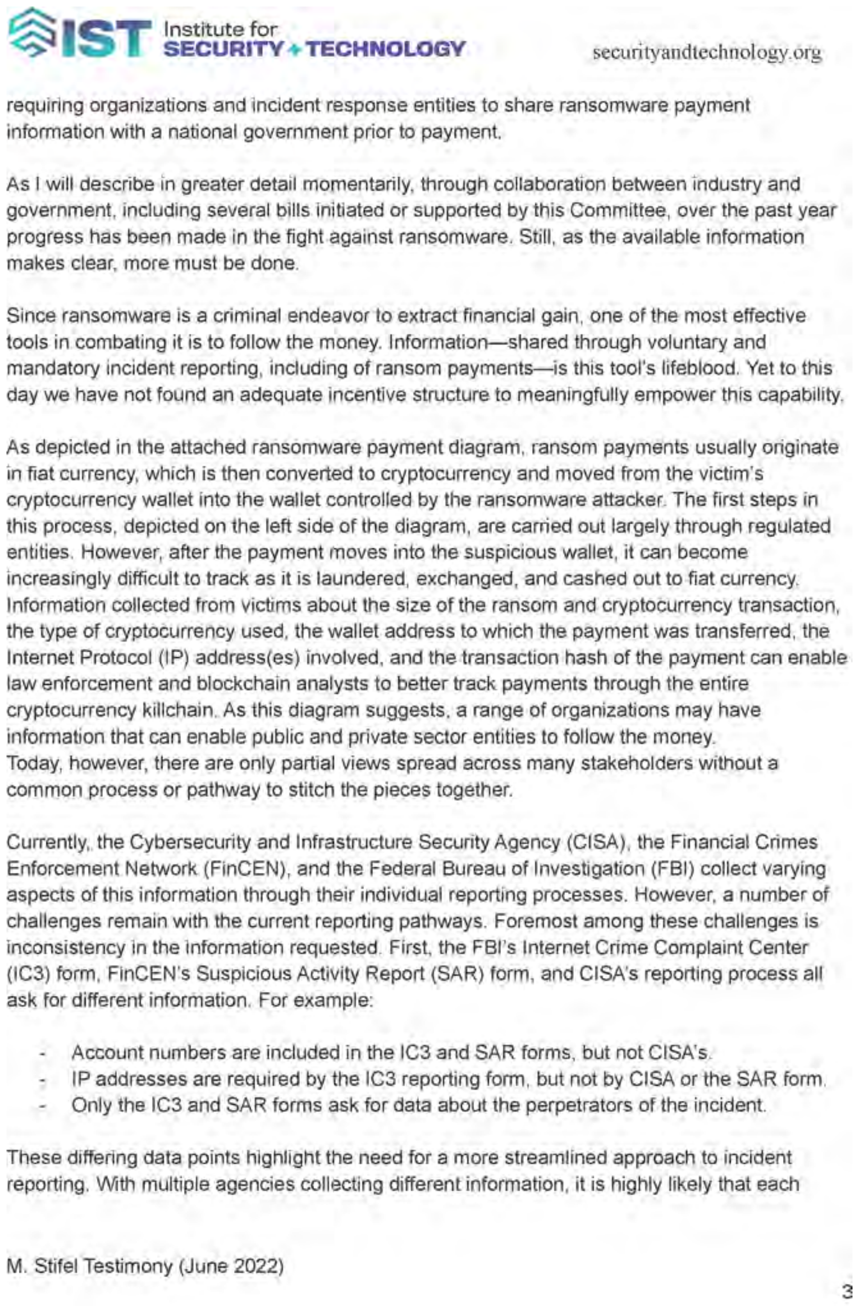
Ransomware is 21st century extortion, but extortion is not a 21st century invention. New forms of extortionware are emerging. Thus, in examining collective measures by industry and government to combat ransomware, one of today's most significant cyber risks, we are not just targeting today, we are working to better secure tomorrow against whatever these criminals and other actors turn to next.

The Essential Role of Information in Order to Effectively Combat Ransomware

In my testimony last year before the House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, I noted the Task Force's recommendation that the scope and quality of information about ransomware incidents must improve.[2] The need for better quality and greater information is manifold. Higher quality information can better equip governments and other stakeholders in developing the international strategy the Task Force called for to reduce ransomware on a global scale. It can provide more detailed evidence to support a range of measures that can be brought to bear in order to reduce the ability of these actors to operate from safe havens, to include sanctions on a range of infrastructure used to carry out their criminal activities. More detailed information can also enable diplomatic, law enforcement, and other instruments of national power. Of perhaps equal importance, higher quality information can better inform the private sector's ability to protect its and its customers' rights and property as well as enhance its capacity to collaborate with the government in combating ransomware and other cyber crimes.

As the Task Force noted in the April 2021 report, "improving the quality and volume of ransomware information would enable better deterrence, enhance preparedness, and inform disruption activities." It recommended several actions to support this objective. The actions included establishing a Ransomware Incident Response Network, creating a standard format for ransomware incident reporting, encouraging organizations to report ransomware incidents, and

[2] Megan Stifel, Testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, May 2021. https://homeland.house.gov/imo/media/doc/2021-05-05-CIPI-HRG-Testimony-Stifel.pdf.



requiring organizations and incident response entities to share ransomware payment information with a national government prior to payment.

As I will describe in greater detail momentarily, through collaboration between industry and government, including several bills initiated or supported by this Committee, over the past year progress has been made in the fight against ransomware. Still, as the available information makes clear, more must be done.

Since ransomware is a criminal endeavor to extract financial gain, one of the most effective tools in combating it is to follow the money. Information—shared through voluntary and mandatory incident reporting, including of ransom payments—is this tool's lifeblood. Yet to this day we have not found an adequate incentive structure to meaningfully empower this capability.

As depicted in the attached ransomware payment diagram, ransom payments usually originate in fiat currency, which is then converted to cryptocurrency and moved from the victim's cryptocurrency wallet into the wallet controlled by the ransomware attacker. The first steps in this process, depicted on the left side of the diagram, are carried out largely through regulated entities. However, after the payment moves into the suspicious wallet, it can become increasingly difficult to track as it is laundered, exchanged, and cashed out to fiat currency. Information collected from victims about the size of the ransom and cryptocurrency transaction, the type of cryptocurrency used, the wallet address to which the payment was transferred, the Internet Protocol (IP) address(es) involved, and the transaction hash of the payment can enable law enforcement and blockchain analysts to better track payments through the entire cryptocurrency killchain. As this diagram suggests, a range of organizations may have information that can enable public and private sector entities to follow the money.
Today, however, there are only partial views spread across many stakeholders without a common process or pathway to stitch the pieces together.

Currently, the Cybersecurity and Infrastructure Security Agency (CISA), the Financial Crimes Enforcement Network (FinCEN), and the Federal Bureau of Investigation (FBI) collect varying aspects of this information through their individual reporting processes. However, a number of challenges remain with the current reporting pathways. Foremost among these challenges is inconsistency in the information requested. First, the FBI's Internet Crime Complaint Center (IC3) form, FinCEN's Suspicious Activity Report (SAR) form, and CISA's reporting process all ask for different information. For example:

- Account numbers are included in the IC3 and SAR forms, but not CISA's.
- IP addresses are required by the IC3 reporting form, but not by CISA or the SAR form.
- Only the IC3 and SAR forms ask for data about the perpetrators of the incident.

These differing data points highlight the need for a more streamlined approach to incident reporting. With multiple agencies collecting different information, it is highly likely that each agency will have a different picture of the attack, and the relevant steps needed to help the victim and prevent the next attack.

Ultimately, there should be harmony among government reporting avenues. This would ease confusion among victims, and streamline the collection and analysis of attack information. A common reporting format, which the Task Force recommended, would significantly assist this effort, and is something that we at IST, together with members of the Task Force, are working to develop.

The Cyber Incident Reporting for Critical Infrastructure Act will address aspects of this challenge, however, the need for consistency across reporting pathways is more immediate. It is especially critical while the rulemaking process is underway. It is also essential regardless of the rulemaking process, given the narrow scope of entities that will likely be required to report pursuant to it or share voluntarily under it.

Second, and compounding this problem, the extent of information sharing between these agencies remains unclear. The Committee's reports offer examples of information silos among agencies. For example, it is only recently the case, under the Cyber Incident Reporting for Critical Infrastructure Act, that CISA is required to share all incident reports it receives with the FBI. This type of information sharing will better position the FBI to investigate those responsible for ransomware attacks, while also allowing CISA to provide the technical assistance victims need to recover.

To meet the risks of tomorrow, information gathered must be useful and it must be appropriately disseminated within a meaningful period of time. It is also important to note that the same information may be of different value depending on an agency's or organization's mission. Within this same spectrum of challenges, it is also important to recall the emphasis placed by the Task Force on the need for disruptive capabilities of these payment channels: greater regulatory enforcement and reporting will help. The disruptive actions taken in the past year via coordinated action between departments and agencies to seize cryptocurrency assets could scale significantly if clear, concise, actionable information is made available to appropriate organizations as early as possible in the cryptocurrency killchain. When that information is provided days and weeks following an incident and/or payment, often the window for disruptive action may have already closed.

Recent Progress through Policy and Legislation

This Committee has led efforts to fund modernization of the nation's digital infrastructure, including through the passage of the Cyber Response and Recovery Act that established the Cyber Response and Recovery Fund, and the State and Local Cybersecurity Improvement Act, which were enacted in the Infrastructure Investment and Jobs Act. More recently, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 requires reporting of incidents and payments for organizations identified through the ongoing rulemaking process. These funds, and the information ultimately provided pursuant to the legislation, should enhance our collective ability to combat the ransomware risk.

The policy measures initiated by the Administration included several measures to clarify expectations for preparation and response for critical infrastructure,[3][4] create more alignment and whole-of-government focus on deterring, disrupting, and prosecuting ransomware actors,[5] while reducing opportunities for attackers to realize a payday.[6] In addition, the June 2021 Group of Seven (G7) Summit Communique outlined a commitment to *"urgently address the escalating shared threat from criminal ransomware networks"* and called on all states to *"urgently identify and disrupt ransomware criminal networks operating from within their borders, and hold those networks accountable for their actions."*[7] In October, the United States also hosted a meeting with government officials from 30 nations to launch the Counter Ransomware Initiative. This meeting resulted in a joint statement and pledge for follow up actions that proved the impact of an international coalition.[8]

This leadership at the executive level exemplified recognition of, and response to, ransomware as a threat to national security. The commitment to stabilization was a watershed moment, setting a tone for a deep focus and hard work on this critical issue from various governments, including members of the G7.

Legislation together with policy developments designed to help the government better organize itself and its interactions with industry has aligned with over 85 percent of the Task Force's recommendations. In May 2022, the RTF published a report summarizing the progress of the 48 recommendations published in its April 2021 report.[9] The progress report referenced analysis from Crowdstrike and Chainalysis that found an 82% increase in ransomware attacks between

[3] U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, "Colonial Pipeline Cyber Incident." https://www.energy.gov/ceser/colonial-pipeline-cyber-incident.

[4] Biden, Joseph R., Executive Order on Improving the Nation's Cybersecurity, The White House, May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[5] Monaco, Lisa, Memorandum for All Federal Prosecutors, "Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion," U.S Department of Justice, June 3, 2021. https://www.justice.gov/opa/press-release/file/1402001/download

[6] U.S. Department of the Treasury, Office of Foreign Assets Control, "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," September 21, 2021. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.

[7] Carbis Bay G7 Summit Communiqué, "Our Shared Agenda for Global Action to Build Back Better," G7 UK 2021, June 13, 2021. https://www.g7uk.org/wp-content/uploads/2021/06/Carbis-Bay-G7-Summit-Communique-PDF-430KB-25-pages-3.pdf.

[8] Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting, The White House, October 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/.

[9] Institute for Security and Technology, "The Ransomware Task Force: One Year On," May 2022. https://securityandtechnology.org/wp-content/uploads/2022/05/rtf-progress-report-may22-1.pdf.

2020 and 2021 and a 70% increase in ransomware payments over that same period. The progress report also noted "while security cryptocurrency researchers are pointing to these increases continuing in 2022, law enforcement, governments and cyber insurers are seeing reports of ransomware incidents slow down or even decrease."

This dichotomy in the overall direction of ransomware incidents points to a much broader problem. The limited operational collaboration and scale of information-sharing among and between government agencies and private industry partners has inhibited cooperation on disruptive actions against criminals. While significant progress has been made over the past year, governments still need to do more to support the private sector. In particular, the lack of comprehensive information about ransomware attacks continues to frustrate the private sector's ability to protect itself, inform policy development, and help take collective action against ransomware actors.

No matter how effective we become at deterring, disrupting, and preventing ransomware attacks, some percentage of attacks will succeed nonetheless. Many of the RTF's recommendations were aimed at increasing the availability of information about ransomware attacks in terms of frequency, volume, and other characteristics. This information is not just helpful for establishing trends–it will support effective use of the funds and authorities the Committee supported. Further, developing a clear understanding of the threat is a critical element in designing productive incentive structures to address the broader issues of cyber risk giving rise to the current ransomware spree. More immediately, enhanced information can help encourage victims not to pay ransoms, increase cooperation between law enforcement and victims, and support organizations that have fallen victim to a ransomware attack.

Keeping up the Momentum, Encouraging Voluntary Action

Legislation has been a necessary early step, but it is not enough, for several reasons. First, the timeline under which the requirements will be implemented spans several years. CISA has up to two years after passage of the Act to issue the notice of proposed rulemaking, and another 18 months to issue the final rule. This timeline does not reflect the urgency of the threat at hand. As I noted above, compared with 2020, in 2021, observed ransomware incidents rose by 82% and known payments rose by 70%. Those increases topped the prior years' record breaking rises. This growth pattern suggests it will rise again in 2022 and beyond, yet it will be several years before the types of organizations required to report become known, and even longer before they must report.

In the meantime, it is essential to increase utilization of other tools that can help organizations reduce the ransomware risk, including redoubling efforts to improve cyber hygiene and increase voluntary reporting.

To support organizations in improving their hygiene, later this summer the Task Force will publish the Blueprint for Ransomware Defense. Over the past several months, members of the Task Force worked together to develop a clear, actionable framework for ransomware mitigation, response, and recovery. The Blueprint aims to equip small and medium sized enterprises (SMEs) in particular with the security controls known to be most effective in mitigating ransomware risk. Tools that can assist in implementing the control recommendations will accompany the Blueprint. For the Blueprint to be effective, collaboration with SMEs and the managed service and managed security service providers, together with other support organizations, is essential. Members of the Blueprint working group are actively engaging these organizations in order to develop a solid foundation upon which to publish these resources.

The Blueprint addresses the Task Force's recommendation to develop guidance to support these organizations' preparation and response. As noted in the Task Force's April 2021 report, better equipping these organizations is essential to reducing their risk, and can also facilitate their ability to report information. While SMEs are currently not subject to the mandatory reporting requirements, by expanding the types of organizations sharing information related to incidents, relevant stakeholders will have a more comprehensive picture of the threat and be better equipped to prevent similar such incidents as well as help leverage appropriate tools to identify the responsible actors.

Even if victims more consistently share and report information about the incidents they experience, the mechanisms to collect, analyze, and disseminate that information remain immature. The statistics cited above reflect this problem; at best, they are estimates from a particular company's or government agency's point of view. While aggregating these different reports can provide a general sense of the trends, policy decisions and priorities should be based on more reliable data. Unfortunately, efforts to improve information sharing about ransomware attacks have been slow, due to competing priorities, legal and regulatory restrictions, and other perceived downsides.

The data we have is largely knit together through collaborations among law enforcement, government agencies, insurers, and researchers, but even this patchwork view is incomplete and likely distorts our understanding of the real situation. The resulting picture fails to capture the scope, scale, and impact of ransomware attacks, making it hard to accurately interpret available and incomplete data to assess the efficacy of actions being taken. This situation should improve as reporting requirements come into effect, but that takes time that we do not have while the threat landscape continues to evolve.

The willingness of victims to report incidents is likely an additional factor contributing to the lack of coherence about the direction of attack trends. Security researchers and cryptocurrency analysts are monitoring attacker-side activity visible on the dark web. By contrast, law enforcement and insurers are reliant on organizations making reports, which they often prefer not to do, particularly as sanctions and other regulatory requirements increase. For researchers, one other element that is currently providing more visibility of attacks is the growing double extortion trend. Researchers are able to track criminal groups selling or leaking stolen data. Due to the historic lack of clear and consistent reporting, it is unclear whether increased reports of stolen data for sale on the dark web amount to more ransomware attacks, or simply more attacks that incorporate double extortion.

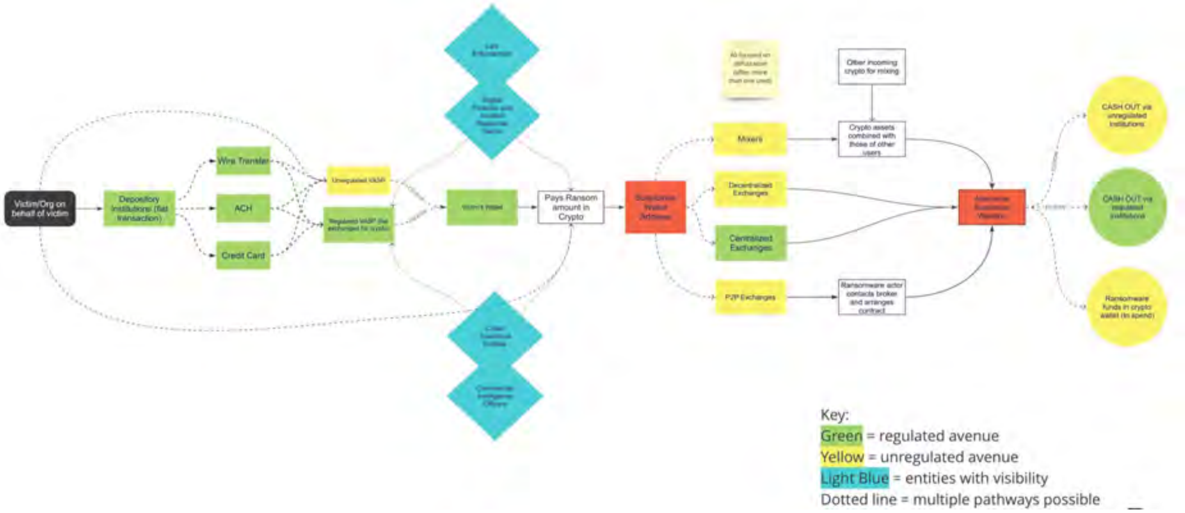
There are additional legislative opportunities that could encourage voluntary information sharing. One path forward is to leverage safe harbors for victims who engage in appropriate due diligence. For victims of ransomware attacks, decisions about whether or not to pay ransoms and report incidents are stressful and time constrained. Even when victims feel they have done their due diligence before making a payment, many organizations fear enforcement actions, reputational impact, and other delays caused by reporting incidents. Providing safe harbor for these victims, in exchange for a commitment to report the incident and cooperate with law enforcement for the duration of any resulting investigation, would provide a carrot in an environment full of sticks.

A second path forward could be to implement the Cyberspace Solarium Commission recommendation for the creation of a "joint collaborative environment." The Commission recommended that this environment be established to share threat information across the federal government and the private sector. In addition to enabling the sharing and fusing of threat information, insights, and other relevant data, the environment could enhance opportunities for disruptive action.

As the Committee's Majority and Minority reports have recently noted, ransomware became and remains a significant risk to critical infrastructure and thus to our national security. The actors are going to continue to press at the seams of our public-private collaboration. Now is the time to prioritize the urgency of action, equip organizations with better information to protect themselves and respond to the threat, and leverage our collective capabilities to be best positioned for the future.

Conclusion

Members of the Committee, thank you for the opportunity to participate in today's hearing. As the convener of the Ransomware Task Force, IST appreciates this Committee's leadership in combating ransomware and stands ready to continue to collaborate with you in the years ahead. I look forward to your questions.


Victim/Org on behalf of victim
Depository Institutions (fiat transaction)
Wire Transfer
ACH
Credit Card
Unregulated VASP
Regulated VASP (fiat exchanged for crypto)
Victim's Wallet
Law Enforcement
Digital Forensics and Incident Response Teams
Cyber Insurance Entities
Pays Ransom amount in Crypto
Suspicious Wallet Address
Mixers
Decentralized Exchanges
Centralized Exchanges
P2P Exchanges
Other incoming crypto for mixing
Crypto assets combined with those of other users
Ransomware actor contacts broker and arranges contract
CASH OUT via unregulated institutions
CASH OUT via regulated institutions
Ransomware funds in crypto wallet (to spend)

Key:
🟩 Green = regulated avenue
🟨 Yellow = unregulated avenue
🟦 Light Blue = entities with visibility
Dotted line = multiple pathways possible

Diagram Sources:

- https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf
- https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Witness%20Testimony_Walden_OI_2021.07.20.pdf
- http://ewfs.org/wp-content/uploads/2022/01/228_01.pdf
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf
- https://research.csiro.au/blockchainpatterns/general-patterns/blockchain-payment-patterns/escrow-2/

Prepared Written / Oral Testimony of Bill Siegel, CEO and Co-Founder of Coveware Inc.

Committee on Homeland Security and Governmental Affairs

Rising Threats: Ransomware Attacks and Ransom Payments
Enabled by Cryptocurrency

Tuesday, June 7th 2022

Mr. Chairman, Ranking Member Portman, and members of the Committee, thank you for the opportunity to share Coveware's perspective on ransomware attacks and the role of cryptocurrency in ransom payments.

My testimony today is derived from Coveware's experience which spans thousands of ransomware incidents over the last few years. During a given incident, we interact with the victim of the attack, privacy attorneys, forensic investigators, restoration firms, cyber insurance companies, and the law enforcement agencies that investigate these attacks. Throughout the incident, we collect data first hand, and the aggregated learnings from this data, and our experience gives us a unique perspective on this problem. We collect and organize this data, because like any problem, you can't solve it until you understand it. The analogy we use is that you can't build safe cars without studying lots of car crashes first. In addition to analysis, our firm has voluntarily and proactively reported subsets of our data to law enforcement from every attack we have ever worked on since inception of our firm. This data is used by law enforcement to augment active investigations into the criminal groups that carry out these attacks.

We are grateful for the work that Chairman Peters, and Ranking Member Portman along with the committee staff have already completed in the publishing the staff report "CASE STUDIES IN RANSOMWARE ATTACKS ON AMERICAN COMPANIES" and the Majority Staff report "Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns."

Both of these reports highlight acute issues and we are grateful that this committee is collaborating with public and private industry and the committee members are pursuing new legislation.

I'd like to quickly address the two primary areas of focus in these reports:

First with regards to cryptocurrency: Financially motivated cyber criminals almost universally denominate ransom demands in crypto-currency. The popularity of cryptocurrency with cyber criminals is rooted in the relative ease with which those criminals can protect ransom proceeds from seizure by law enforcement. The percentage of a ransom that finds its way to the cyber criminal's pockets is substantially higher when cryptocurrency is used vs. other currencies or stores of value. This is clear when looking at the recovery rates between two types of cyber crime, wire fraud and ransomware. If reported within 72 hours, illegitimate wires can typically be reversed and recovered. No such mechanism exists with crypto currency.

It is important to note that unlike financial theft, ransomware is much more akin to a kidnap and ransom incident. There are a number of variables that can prevent a ransom from being recovered once paid. Victims may not want their funds reclaimed out of fear that the criminals will not reciprocate with decryption keys, critical to restore an organization's business. Reclaiming a ransom also requires that the victim make a timely report to the correct branch of law enforcement. Moreover, for a trace and seizure to be successful the end destination of the cryptocurrency must be within the reach or western law enforcement. Most of the time, one or several of these variables inhibit a trace or seizure from even being started, let alone successful. It is also important to note that some form of currency, whether it be physical fiat, digital, or cryptocurrency has always been used for lots of different types of extortion. Ransomware existed before the advent of crypto-currency, and will persist if cryptocurrency were to ever disappear. As long as ransomware attacks are profitable to carry out against organizations with weak cyber security, cyber criminals will continue to proliferate these attacks. This brings us to the second topic of today's hearing, mandatory reporting.

Coveware has been vocal in our support for mandatory reporting for some time. Our hope is that reporting requirements will eventually be extended to all victims of ransomware, not just organizations under the oversight of CISA.

As with any new law the efficacy lies in its implementation. This hearing is uniquely timed to allow policy makers to understand the dynamics of reporting, and ensure that final rules achieve the targeted impact. We believe there will be two primary impacts to mandatory reporting:

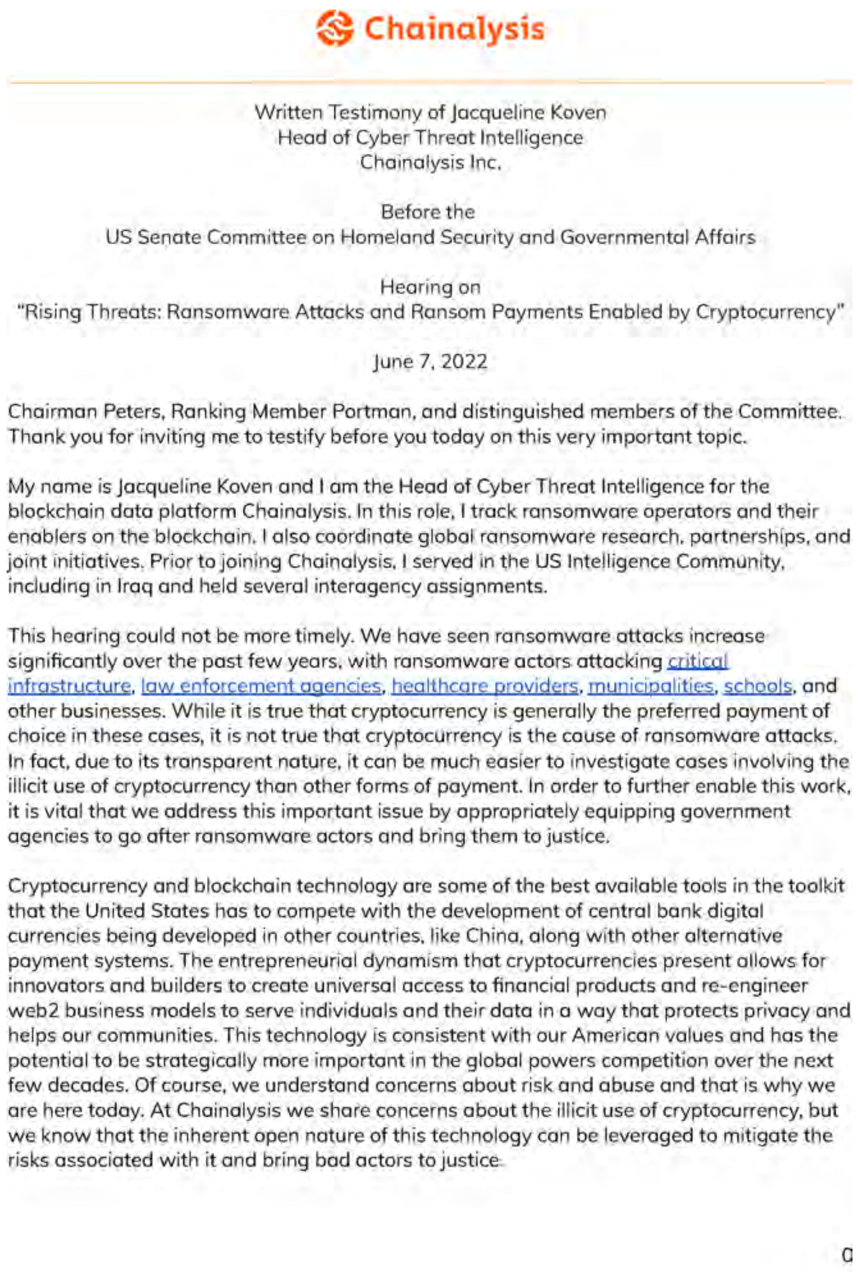
First, the US government will gain clarity on the scope of the problem. As was clearly documented in the Majority Staff Report, the variance between privately reported ransomware statistics and agency reported statistics is cavernous. Collecting accurate statistics is step number one and table stakes if new legislation or proposed solutions to solve this problem are to be taken seriously. Gaining clarity will allow agencies to more confidently resource their responses. We are encouraged to see that the Cyber Incident Reporting Act authored by Chairman Peters and Ranking Member Portman has begun to outline a clear path for reporting and unique agency responsibility.

The second impact will be in providing greater clarity on what to do about the problem. Gaining this clarity will hinge on WHAT information CISA collects, and IF CISA or other regulatory / law enforcement agencies are able to scalable digest the information reported to them. This new legislation has the potential to answer major questions, and enable CISA, the FBI, DHS and other agencies to make meaningful progress on this problem.

If not implemented correctly, however, the new legislation also has the potential to completely bury these agencies with unstructured data that cannot be parsed or analyzed at scale. This would render this new legislation completely ineffectual. Great care and focus should be applied to WHAT information is collected, and HOW this information is organized so that the velocity of analysis, recommendations and actions can achieve maximum efficacy.

Thank you very much Mr. Chairman. I look forward to answering the

Committee’s questions.



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.

Chainalysis

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.

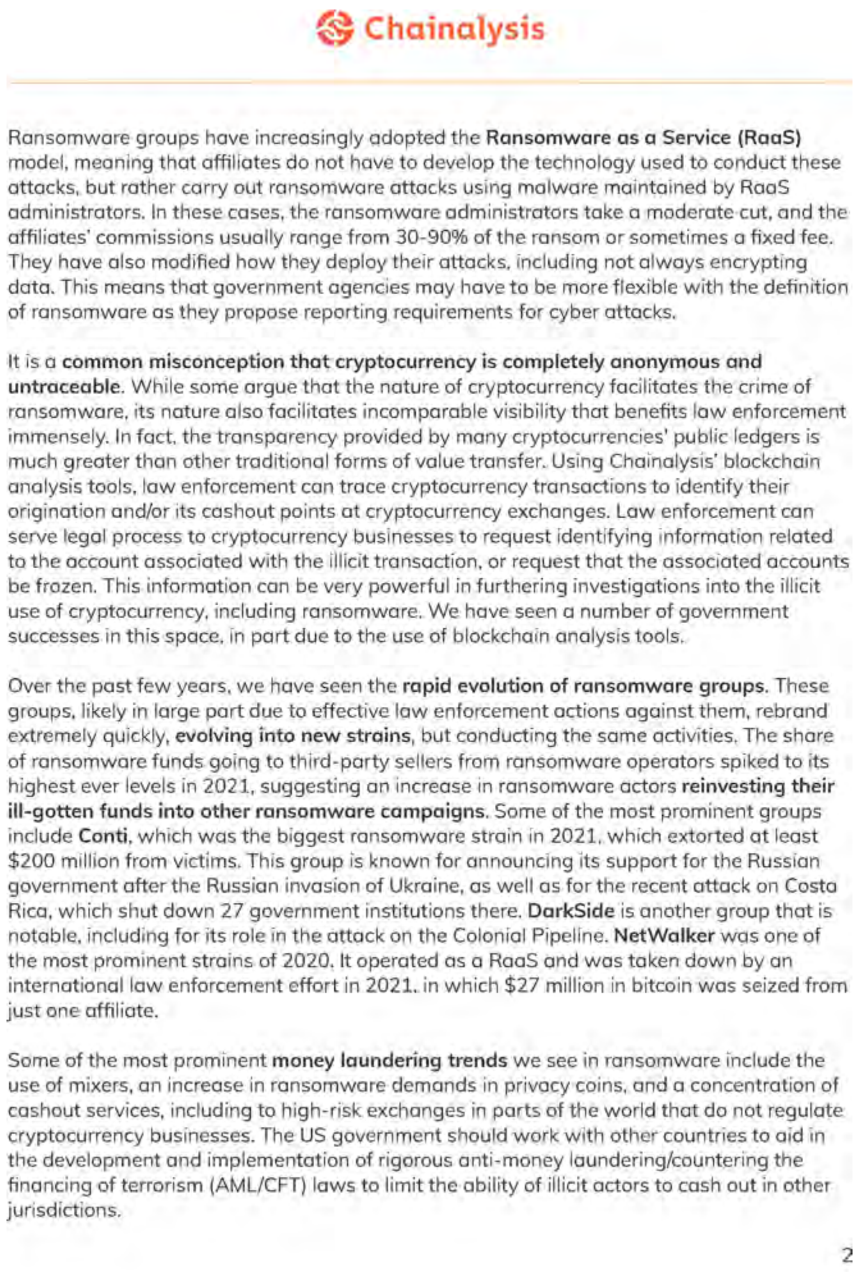
Executive Summary

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.



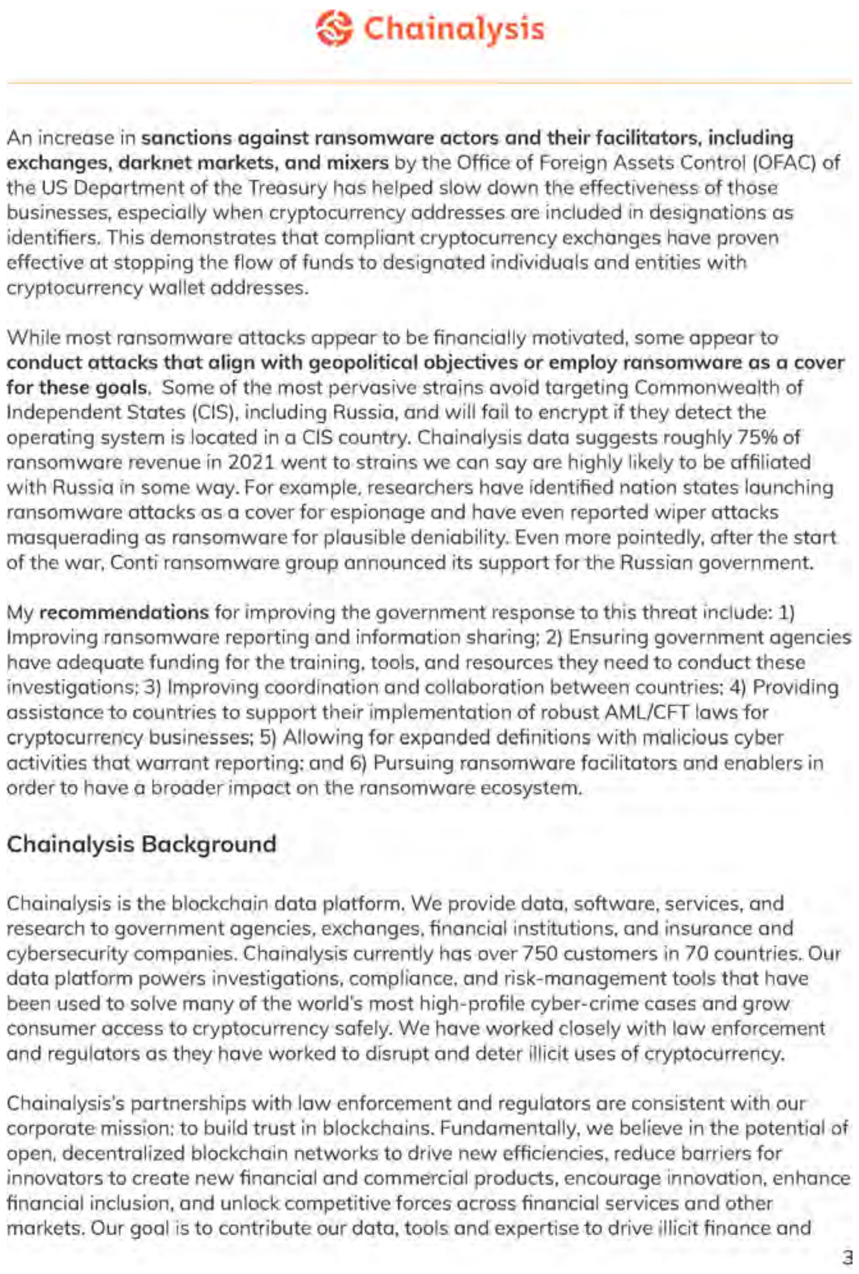
Chainalysis

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.

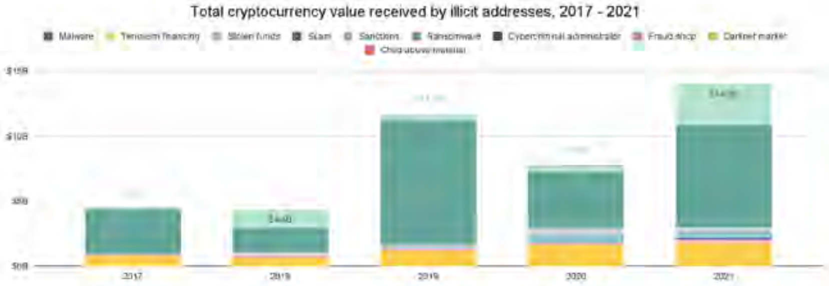
Chainalysis Background

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.

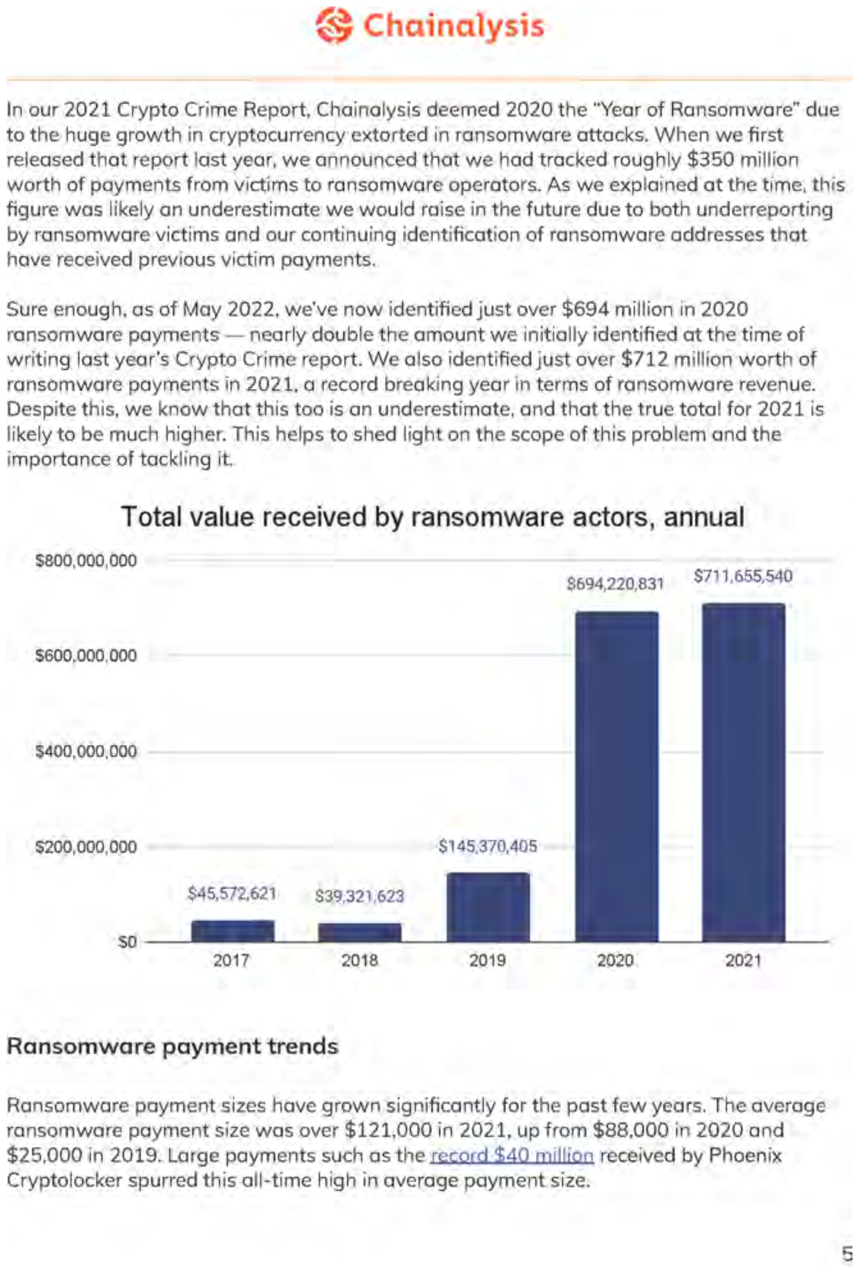
Chainalysis's data powers both investigative and compliance tools. Our investigative tool, Reactor, enables government agencies and investigative teams to trace the illicit uses of cryptocurrency, including money laundering, theft, scams, and other criminal activities. Our compliance tool, KYT (Know 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



Chainalysis

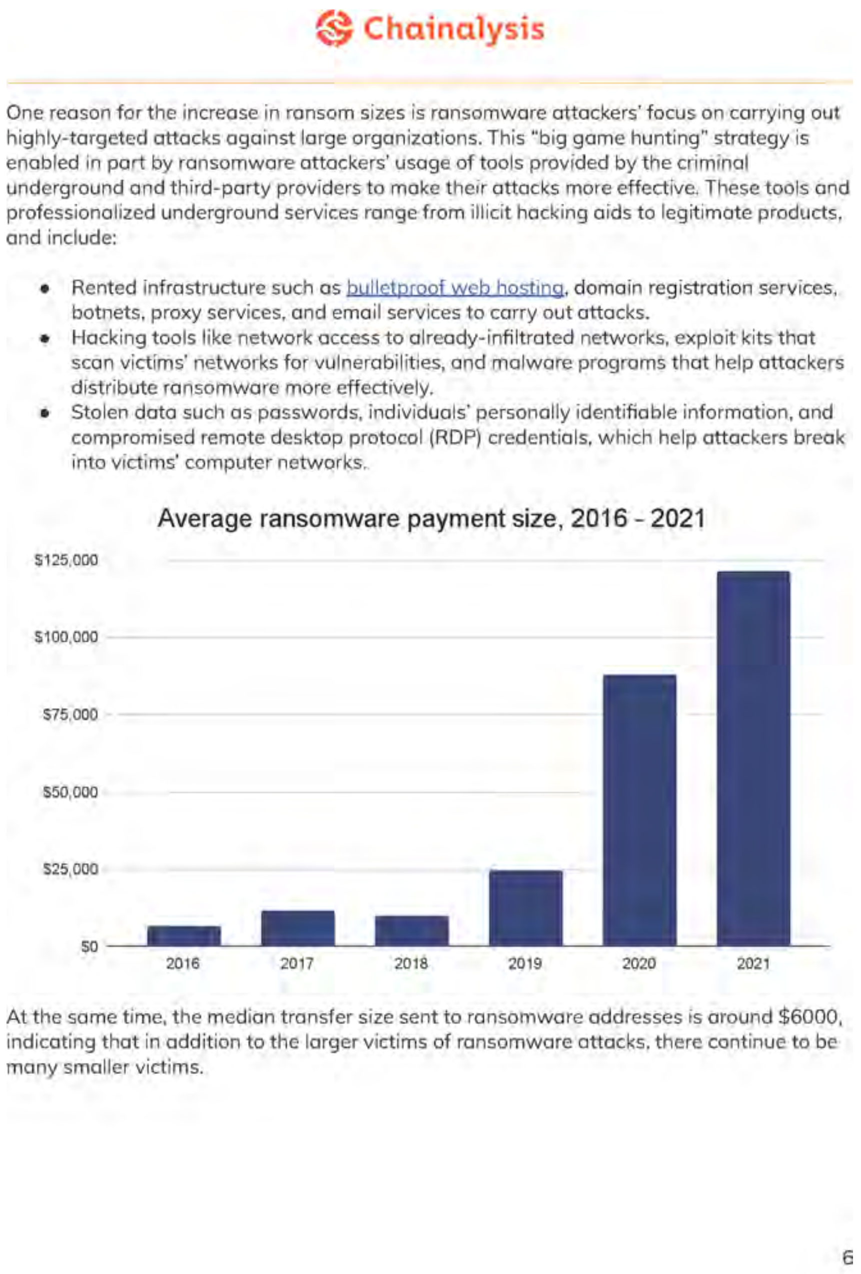
In our 2021 Crypto Crime Report, Chainalysis deemed 2020 the "Year of Ransomware" due to the huge growth in cryptocurrency extorted in ransomware attacks. When we first released that report last year, we announced that we had tracked roughly $350 million worth of payments from victims to ransomware operators. 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.

Total value received by ransomware actors, annual

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.



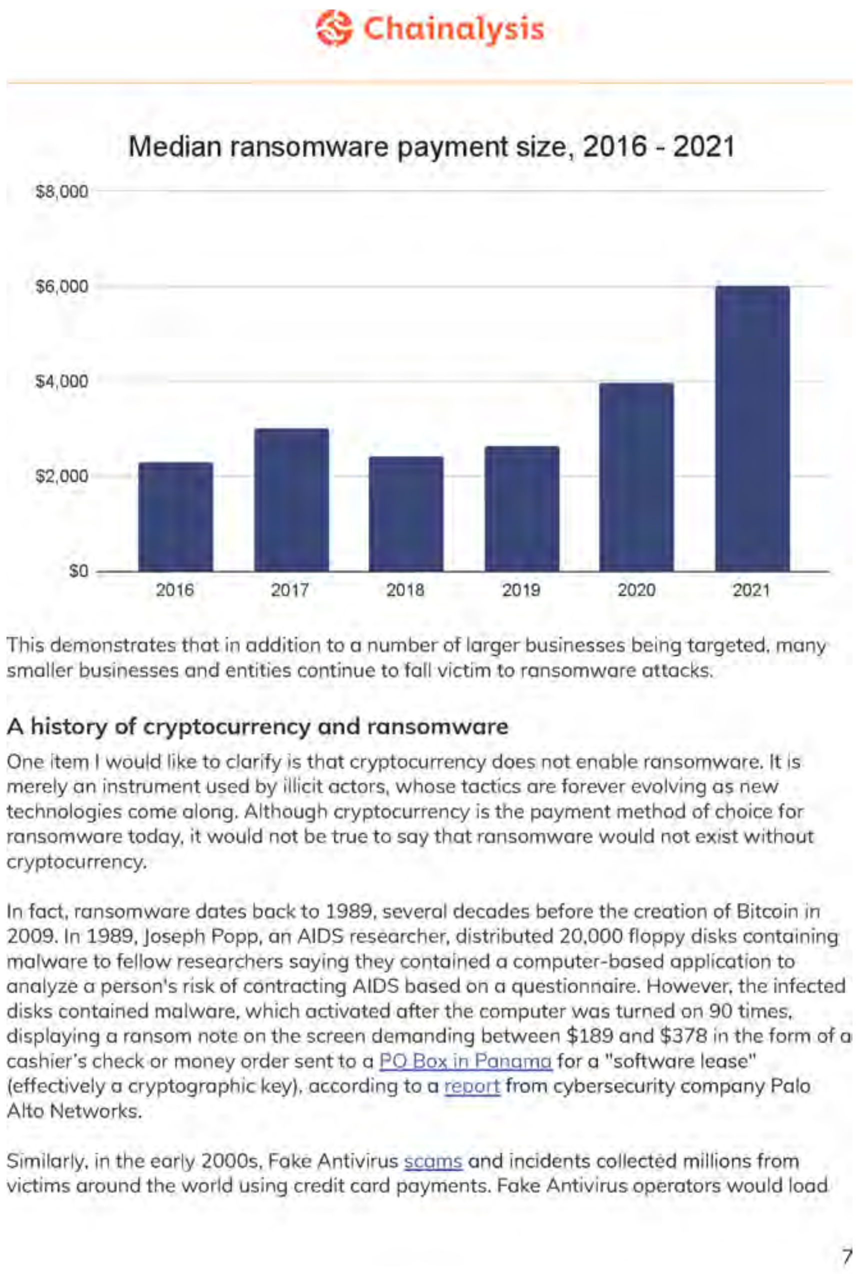
Chainalysis

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.

Average ransomware payment size, 2016 - 2021

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.



Median ransomware payment size, 2016 - 2021

$8,000
$6,000
$4,000
$2,000
$0
2016
2017
2018
2019
2020
2021

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.

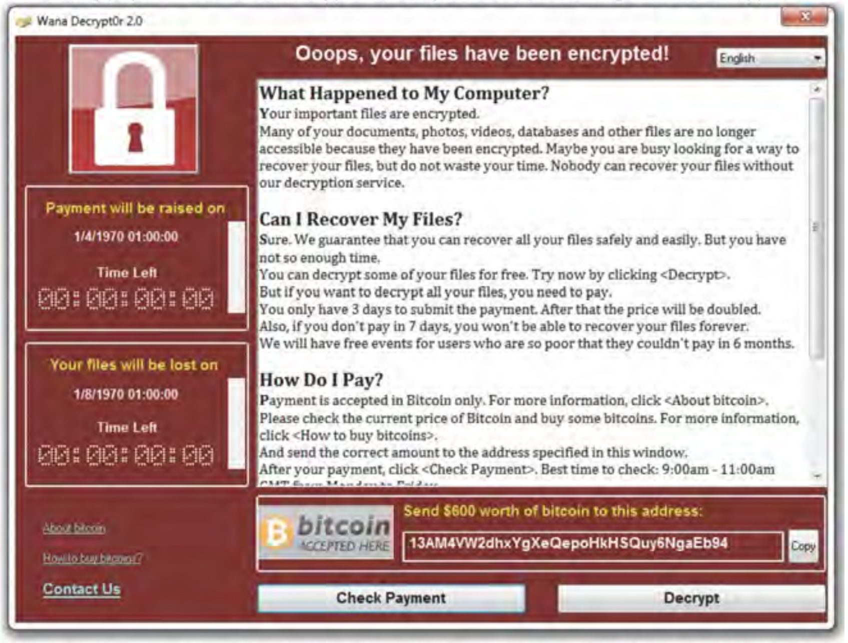
A history of cryptocurrency and ransomware

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.



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.

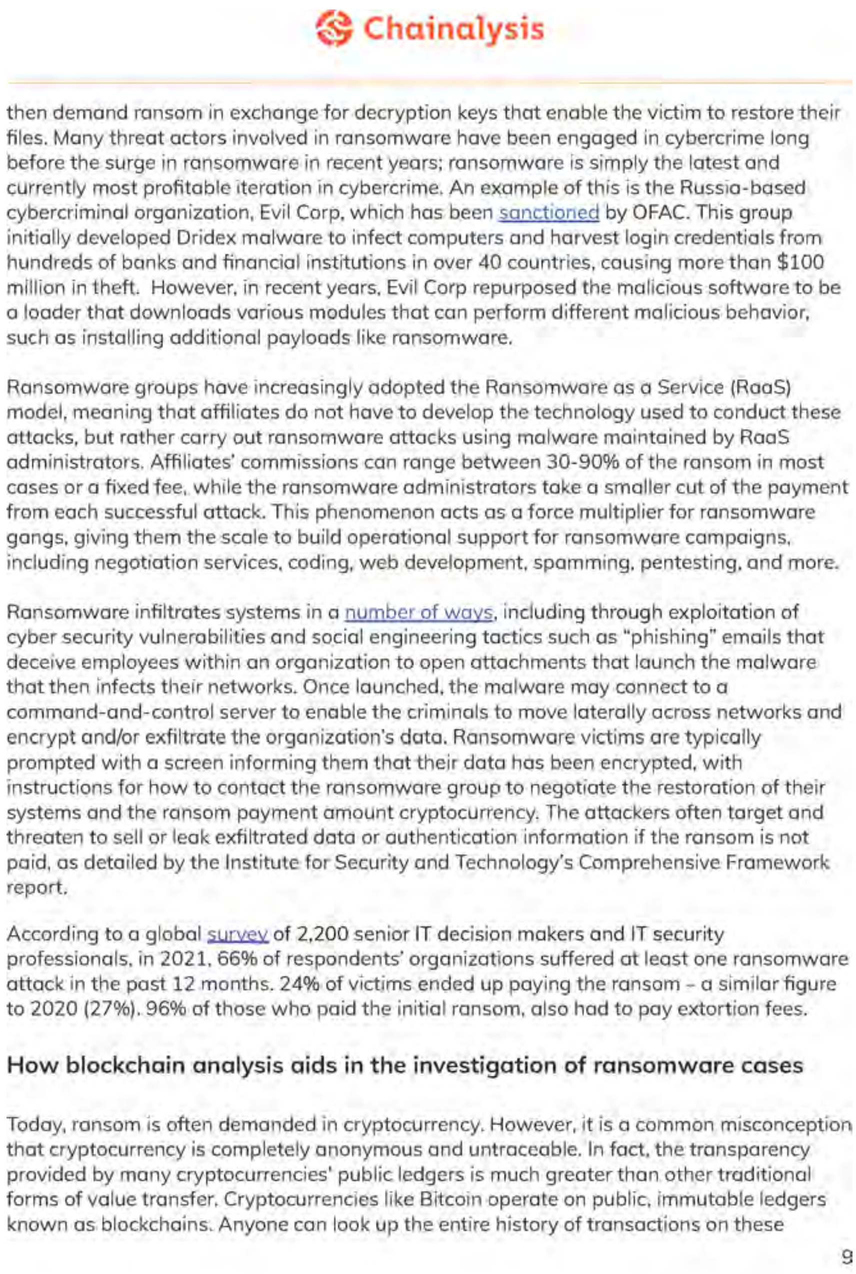
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

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.

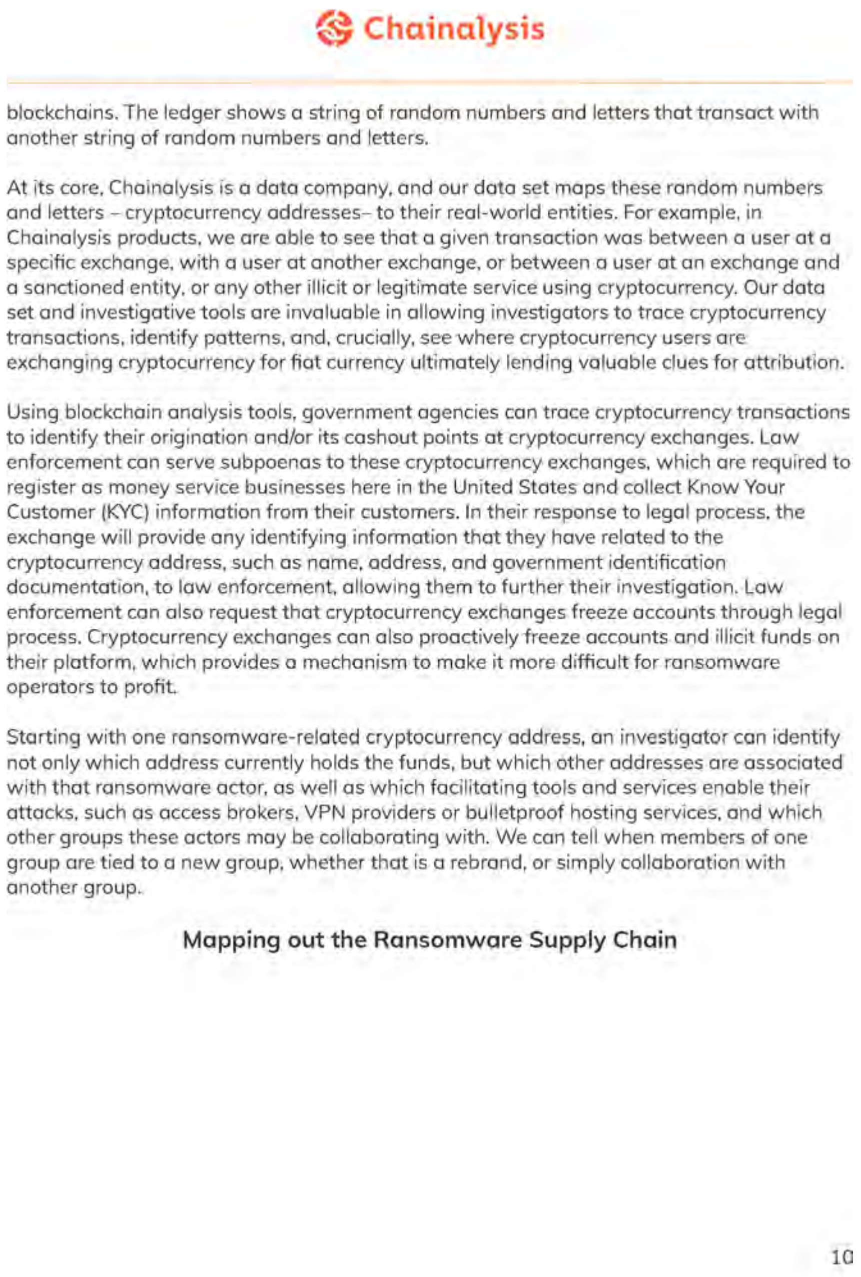
Ransomware groups have increasingly adopted the Ransomware as a Service (RaaS) model, meaning that affiliates do not have to develop the technology used to conduct these attacks, but rather carry out ransomware attacks using malware maintained by RaaS administrators. Affiliates' commissions can range 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



Chainalysis

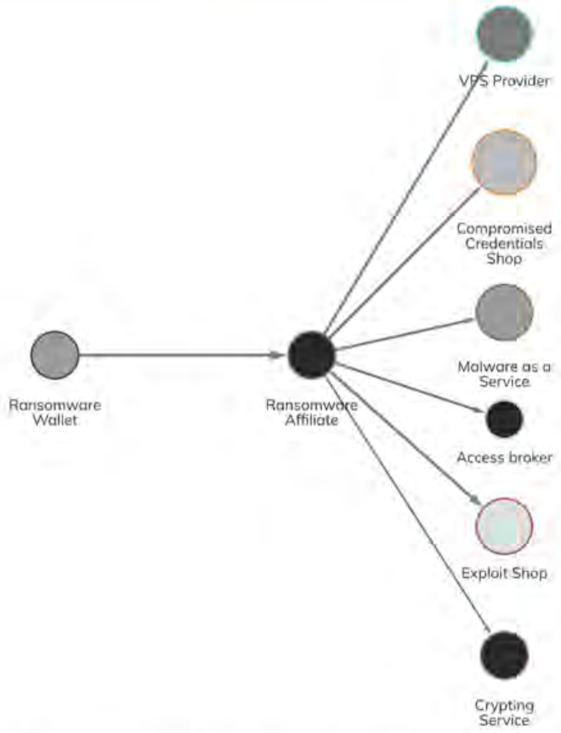
blockchains. The ledger shows a string of random numbers and letters that transact with another string of random numbers and letters.

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.

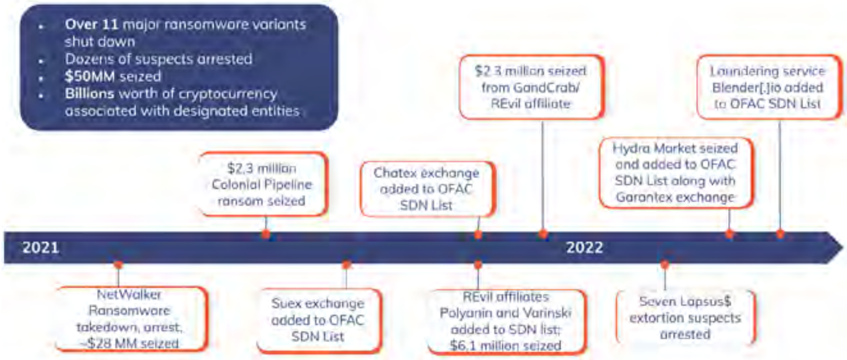
Mapping out the Ransomware Supply Chain



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.

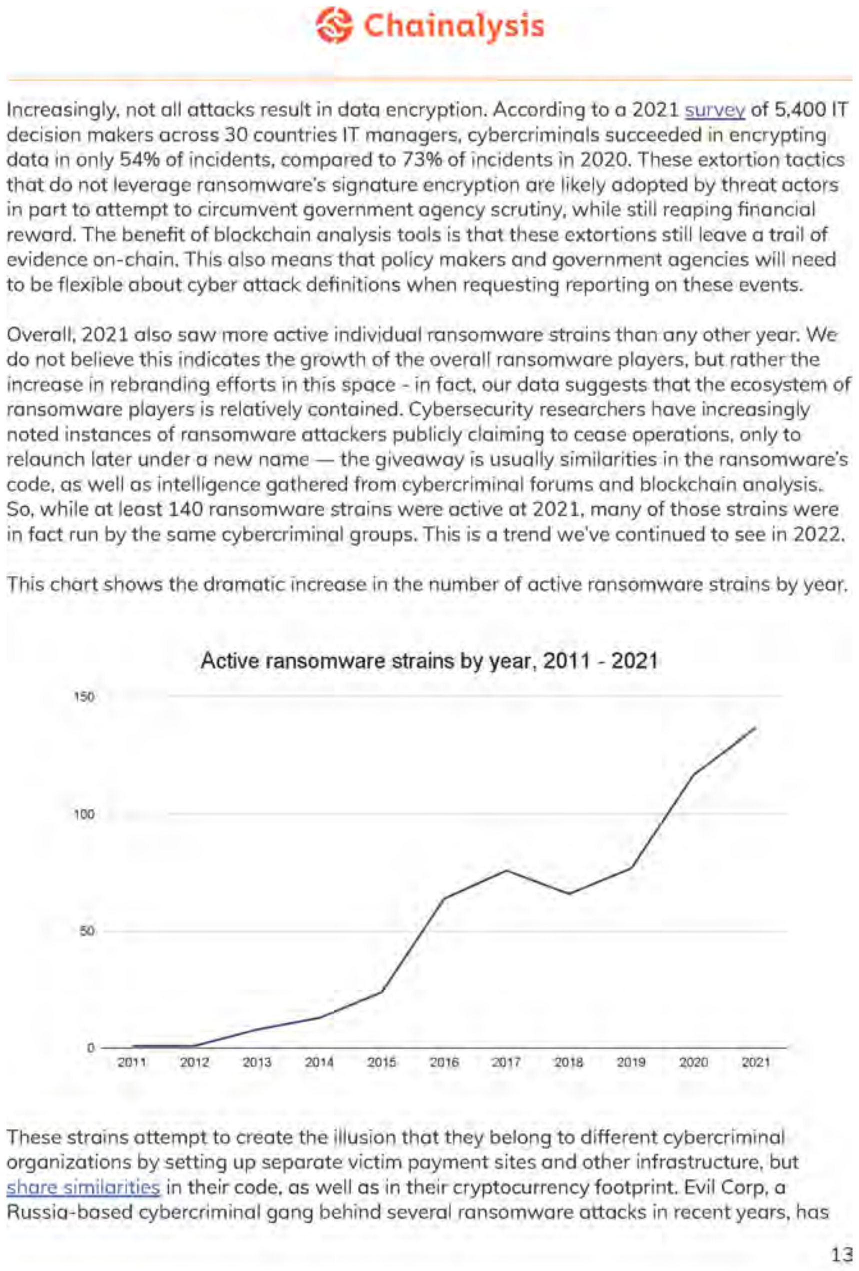
2021-2022 Highlights


- **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.



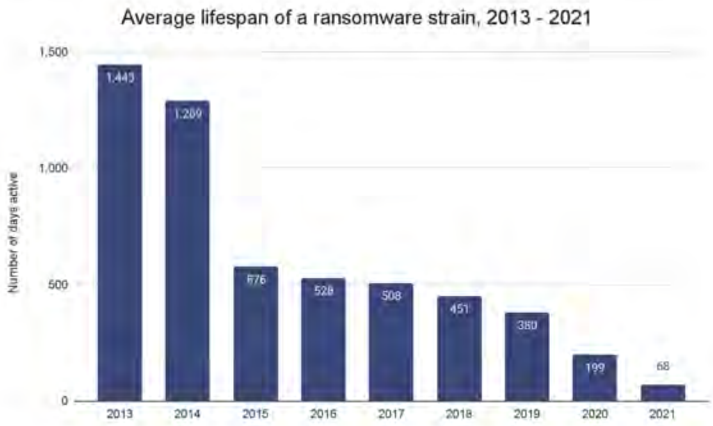
Increasingly, not all attacks result in data encryption. According to a 2021 survey of 5,400 IT decision makers across 30 countries IT managers, cybercriminals succeeded in encrypting data in only 54% of incidents, compared to 73% of incidents in 2020. These extortion tactics that do not leverage ransomware's 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.

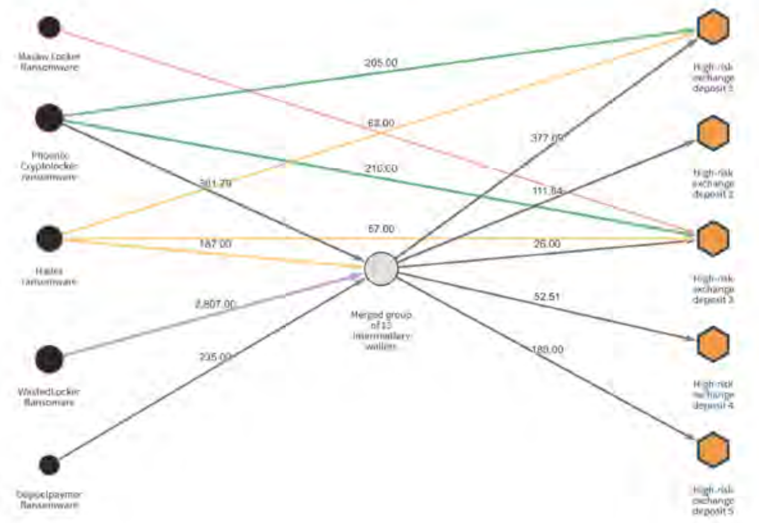
This chart shows the dramatic increase in the number of active ransomware strains by year.

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.


Average lifespan of a ransomware strain, 2013 - 2021

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.

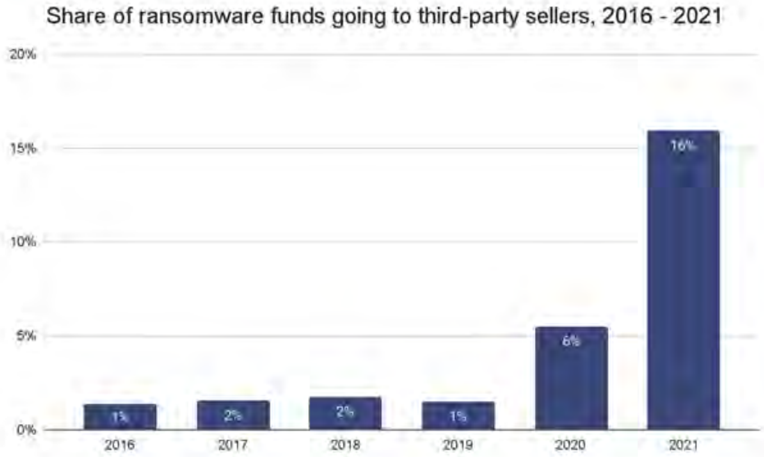

Macaw Locker Ransomware
Phoenix Cryptolocker ransomware
Hades ransomware
WastedLocker Ransomware
Doppelpaymer Ransomware
205.00
63.00
377.09
210.00
301.79
111.84
67.00
187.00
26.00
2,807.00
52.51
235.00
180.00
Merged group of 13 intermediary wallets
High-risk exchange deposit 1
High-risk exchange deposit 2
High-risk exchange deposit 3
High-risk exchange deposit 4
High-risk exchange deposit 5

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.



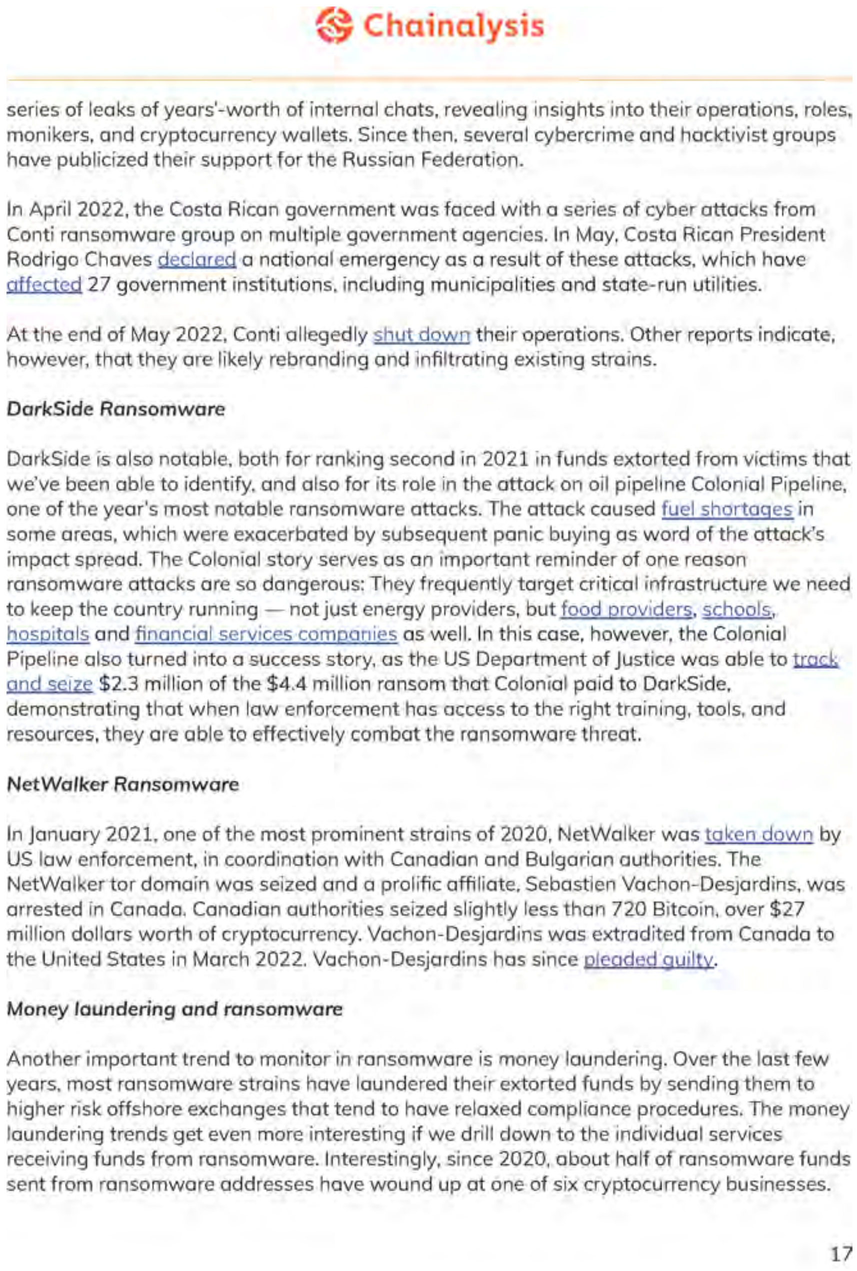
In 2021, 16% of all funds sent by ransomware operators were spent on tools and services used to enable more effective attacks, compared to 6% in 2020. While it's possible some of that activity constitutes money laundering rather than the purchase of illicit services, we believe that increasing use of 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



Chainalysis

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

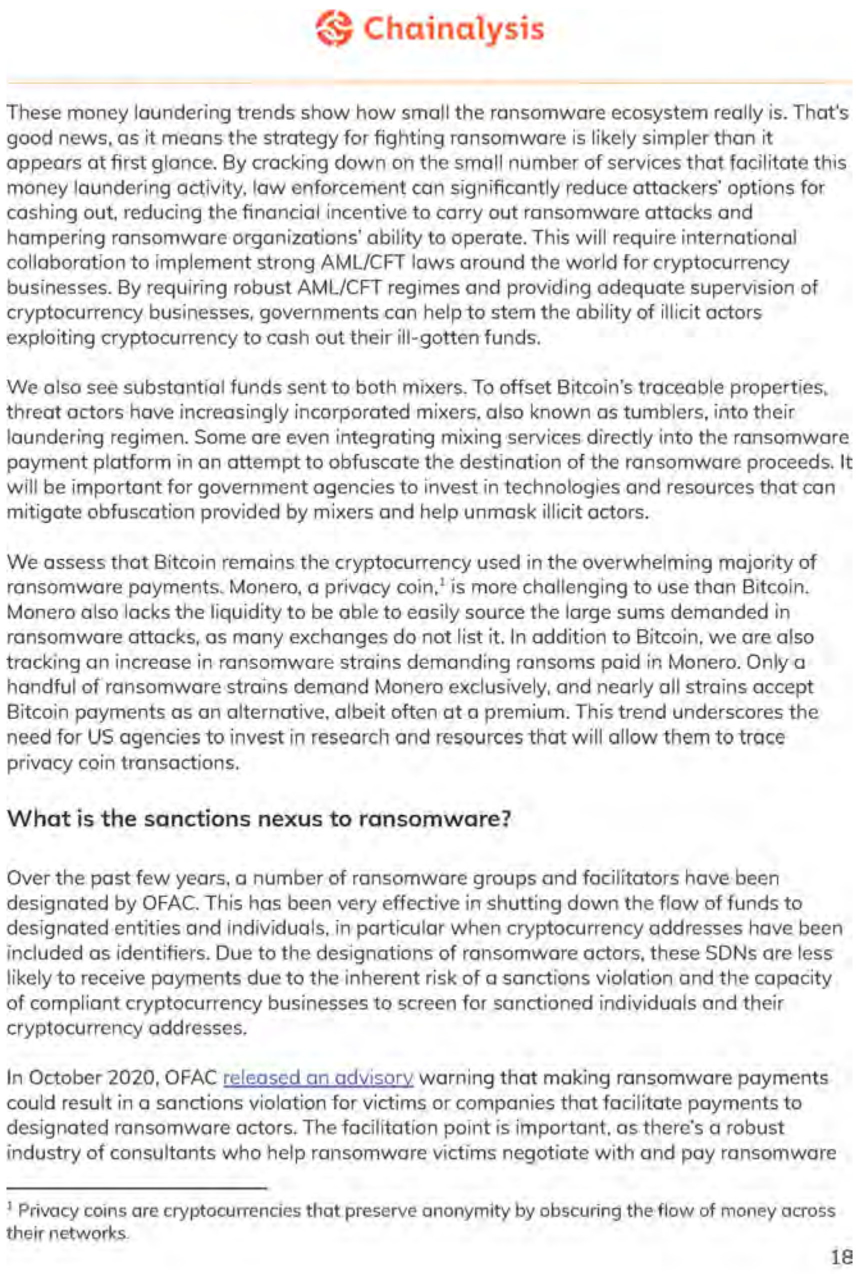
DarkSide is also notable, both for ranking second in 2021 in funds extorted from victims that we've been able to identify, and also for its role in the attack on oil pipeline Colonial Pipeline, one of the year's most notable ransomware attacks. The attack caused fuel shortages in some areas, which were 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.

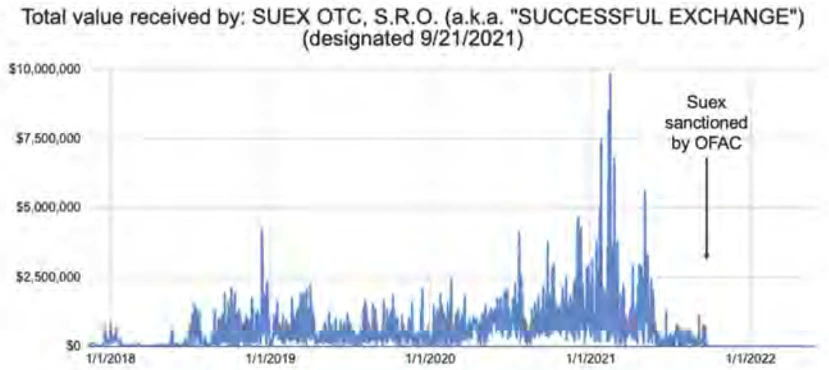
In October 2020, OFAC released an advisory warning that making ransomware payments could result in a sanctions violation for victims or companies that facilitate payments to designated ransomware actors. The facilitation point is important, as there's a robust industry of consultants who help ransomware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

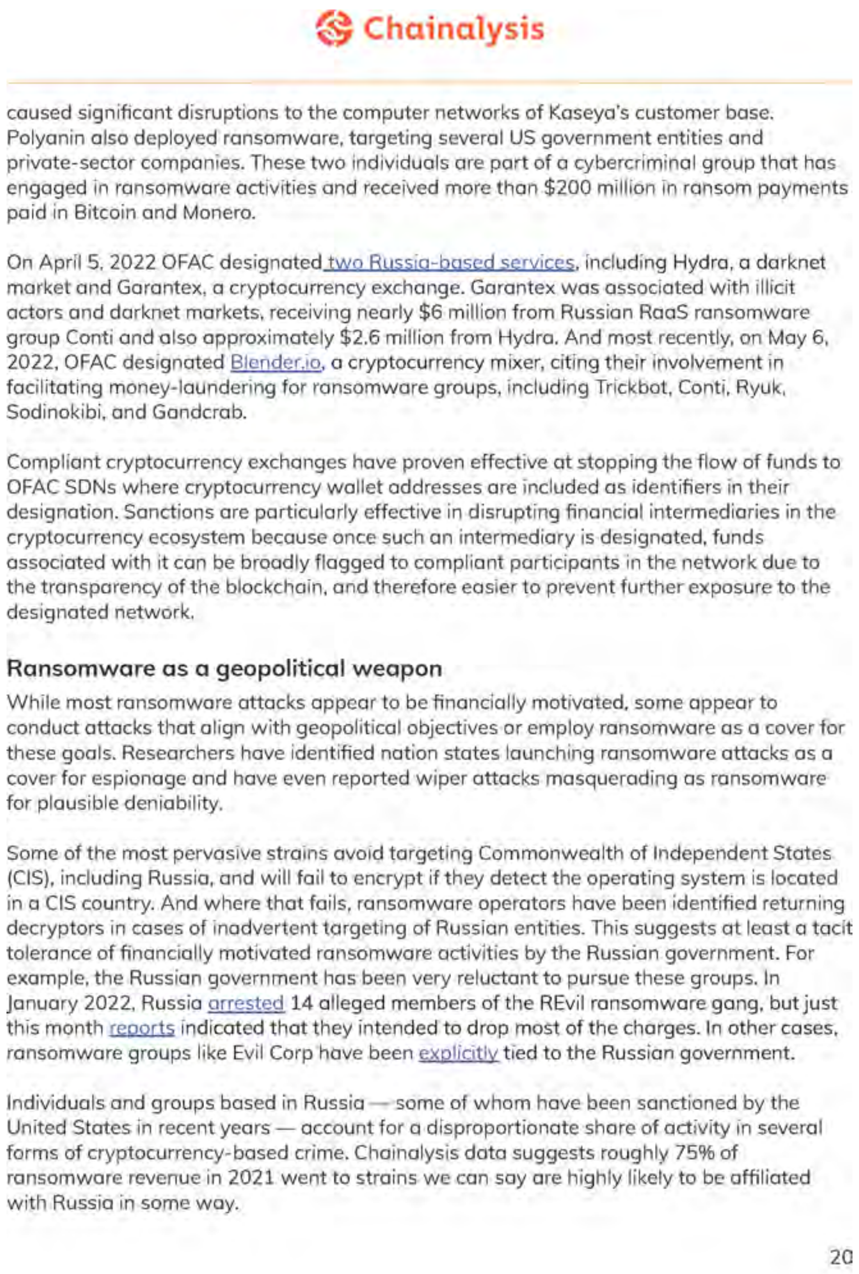
More recently, OFAC has designated several cryptocurrency businesses that were known for facilitating money laundering for ransomware groups and other illicit actors. This approach of going after not just bad actors but their facilitators helps to limit and cut off their cash out points.

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.



Total value received by: SUEX OTC, S.R.O. (a.k.a. "SUCCESSFUL EXCHANGE") (designated 9/21/2021)

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



Chainalysis

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.

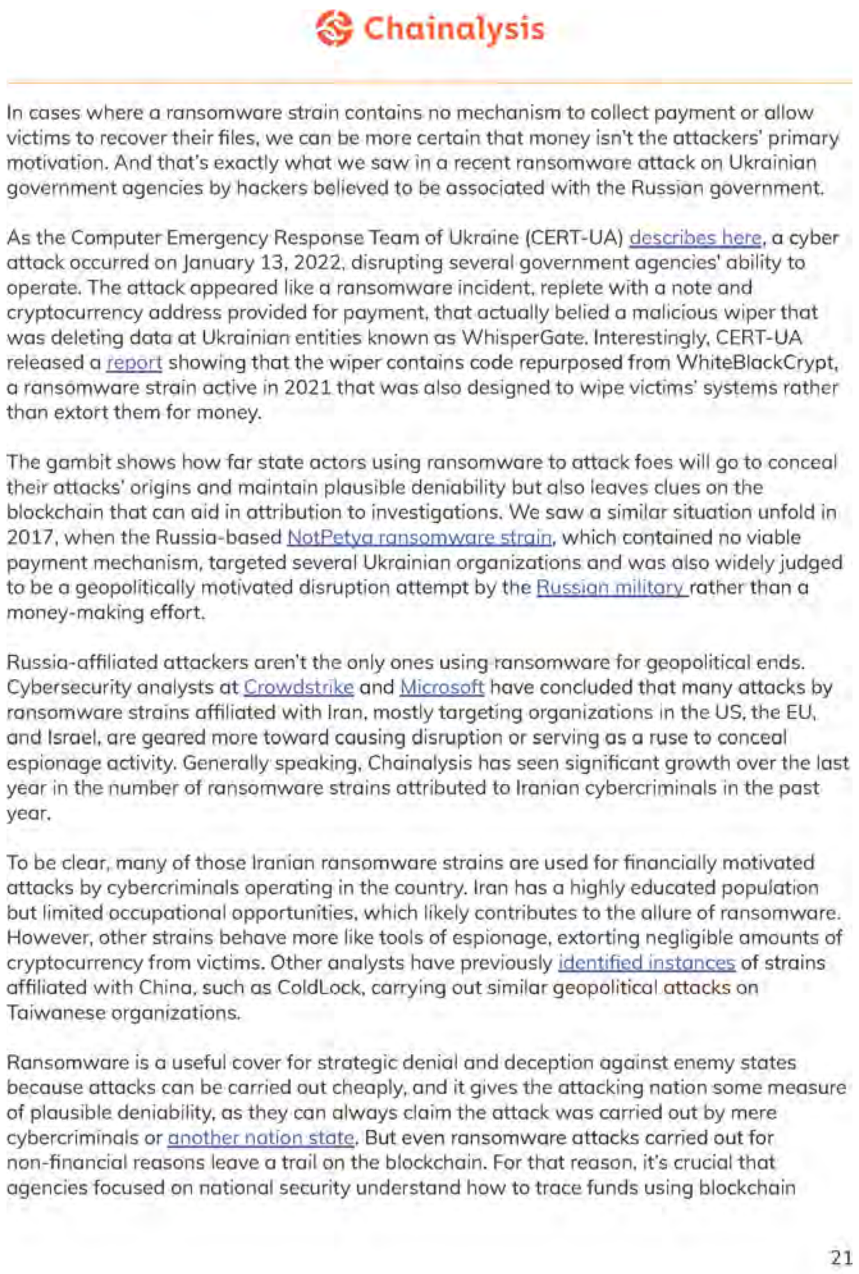
Compliant cryptocurrency exchanges have proven effective at stopping the flow of funds to OFAC SDNs where cryptocurrency wallet addresses are included as identifiers in their designation. Sanctions are particularly effective in disrupting financial intermediaries in the cryptocurrency ecosystem because 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

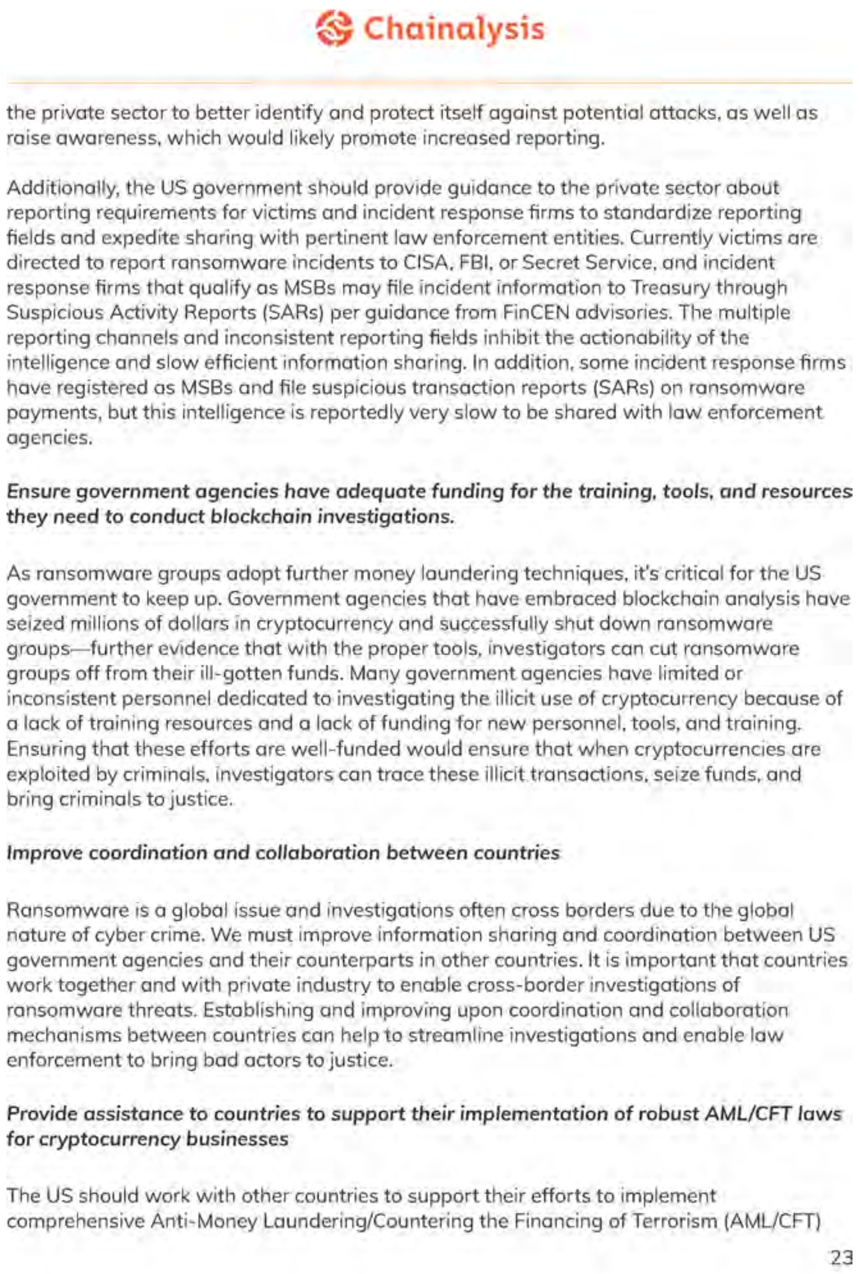
Given the recent increase in ransomware attacks, as well as their potentially devastating impacts, Chainalysis believes it is important to enact meaningful policies to deter, detect, and disrupt ransomware. We support the numerous on-going ransomware initiatives and believe the foundation of US policies 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.

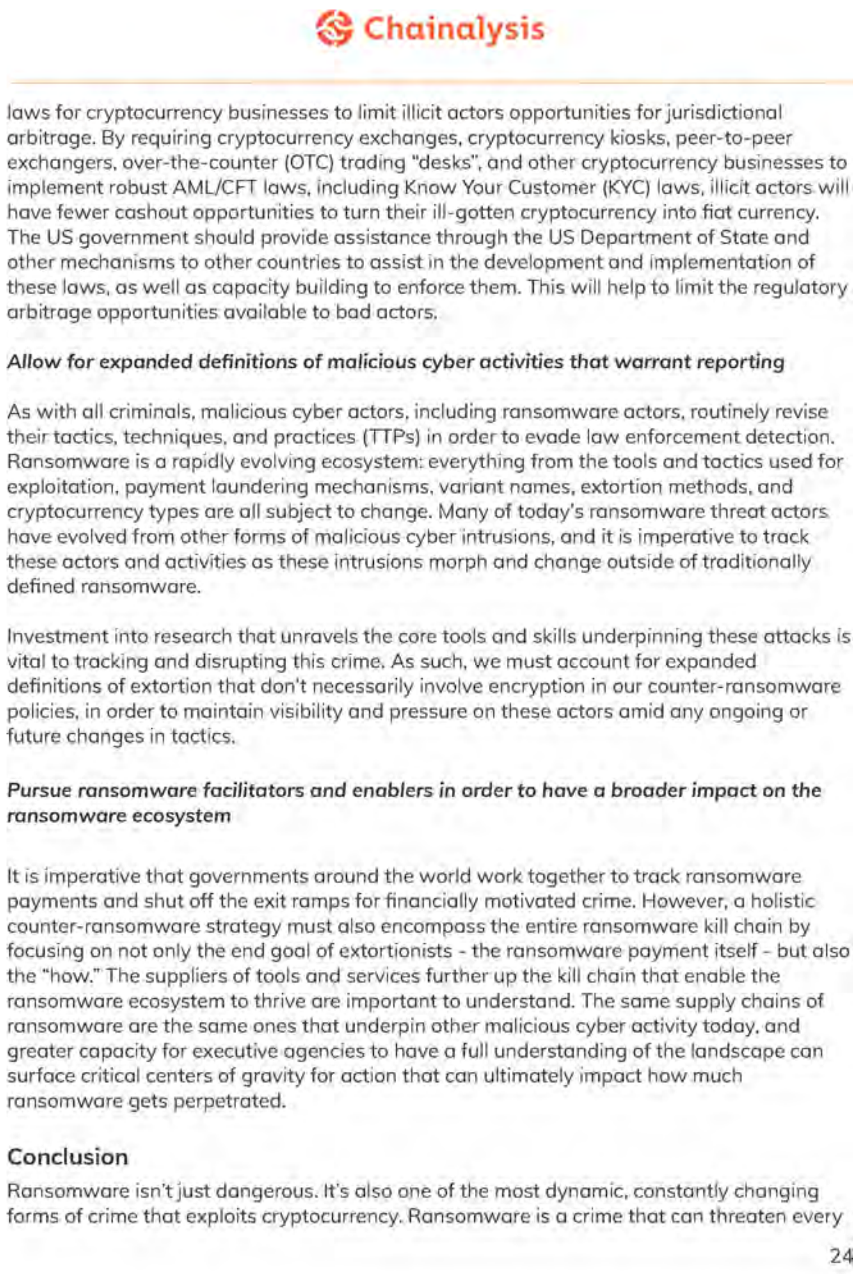
As ransomware groups adopt further money laundering techniques, it's critical for the US government to keep up. Government agencies that have embraced blockchain analysis have seized millions of dollars in cryptocurrency and successfully shut down ransomware groups—further evidence that with the proper 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.

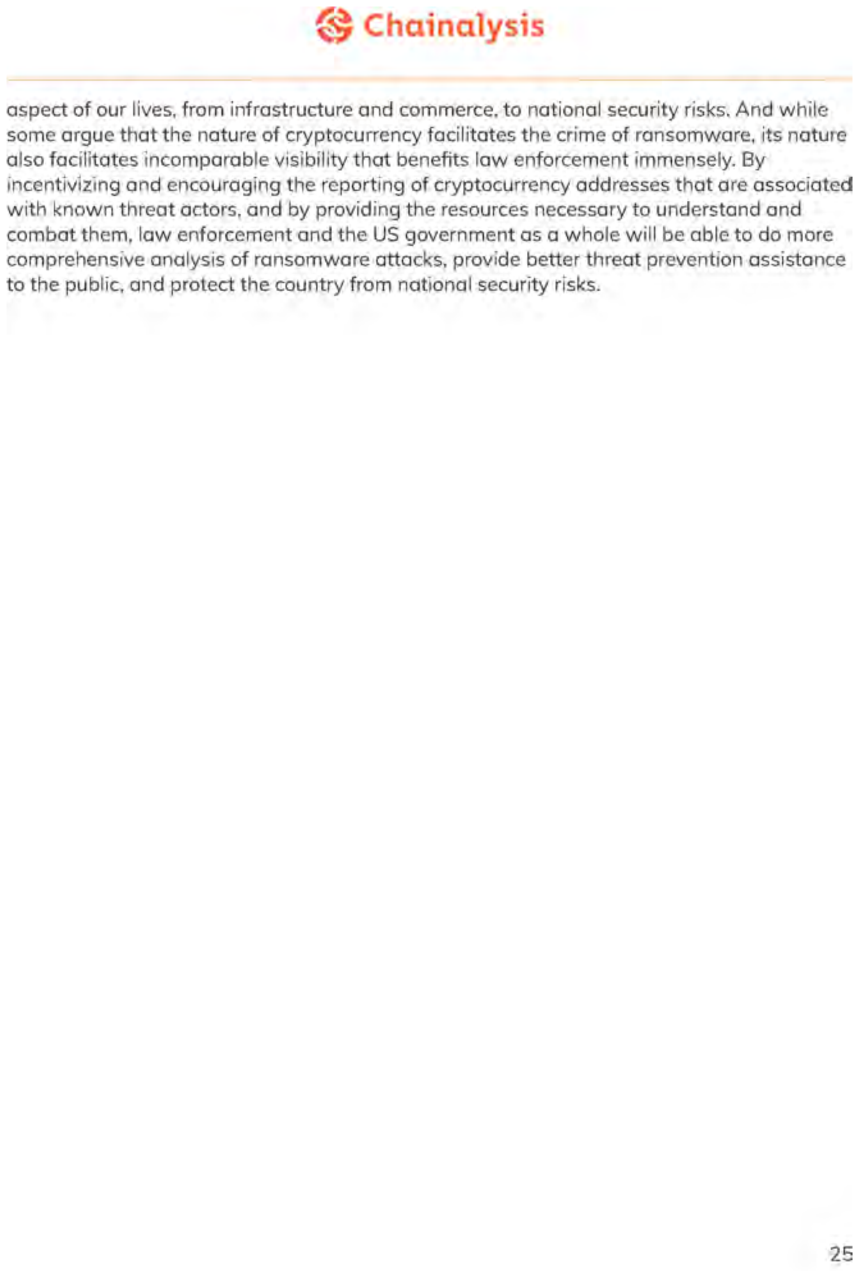
Investment into research that unravels the core tools and skills underpinning these attacks is vital to tracking and disrupting this crime. As such, we must account for expanded definitions of extortion that don't necessarily involve encryption in our counter-ransomware policies, in order to maintain 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

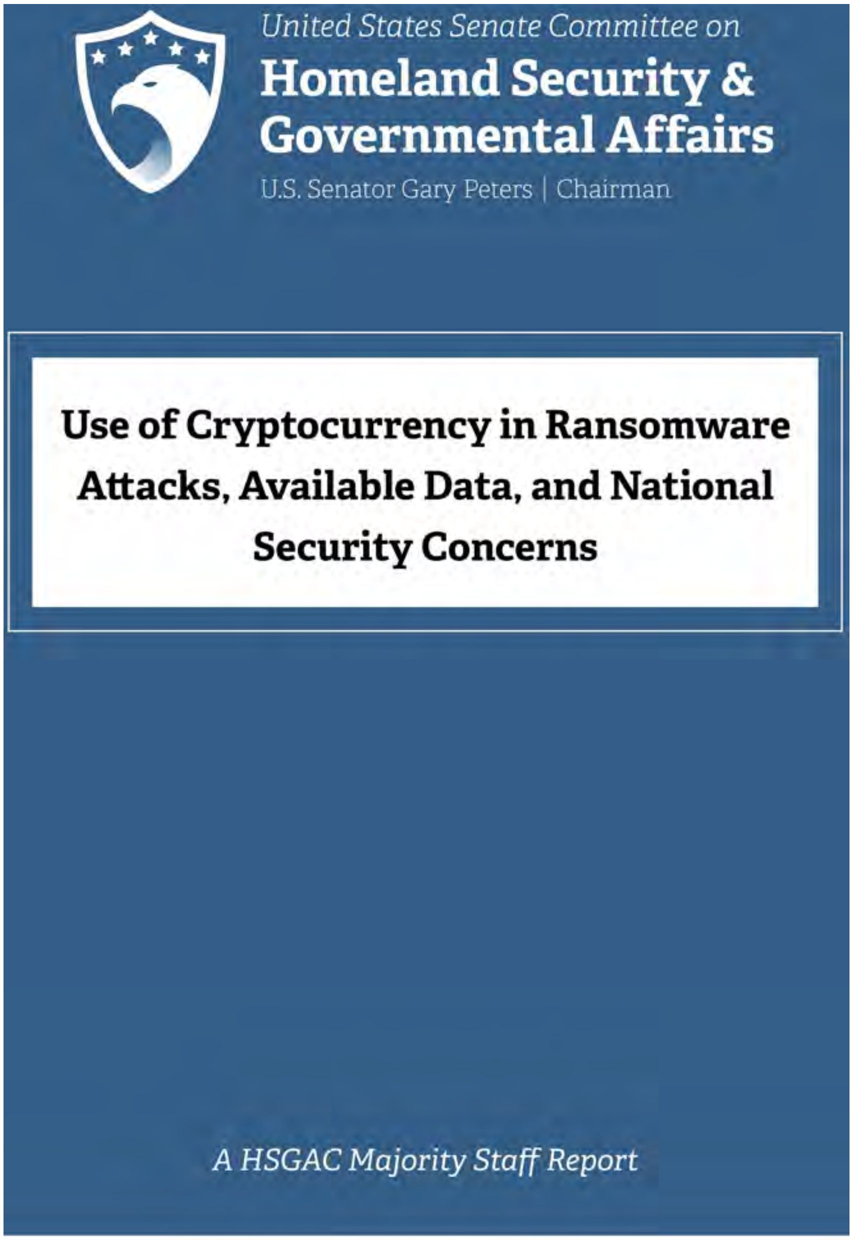
It is imperative that governments around the world work together to track ransomware payments and shut off the exit ramps for financially motivated crime. However, a holistic counter-ransomware strategy must also encompass the entire ransomware kill chain by focusing on not only the end goal of extortionists - 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.



United States Senate Committee on

Homeland Security & Governmental Affairs

U.S. Senator Gary Peters | Chairman

Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns

A HSGAC Majority Staff Report

Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Ransomware is a dangerous form of cyber-attack where threat actors prevent access to computer systems or threaten to release data unless a ransom is paid. It has the power to bankrupt businesses and cripple critical infrastructure – posing a grave threat to our national and economic security. The use of cryptocurrencies has further enabled ransomware attacks, particularly because cryptocurrency is decentralized and distributed and illicit actors can take steps to obscure transactions and make them more difficult to track.

In recent years, ransomware attack victims have included hospitals, school systems, local, state, and federal government agencies, as well as other critical infrastructure, including the water and energy sectors. In 2021, ransomware attacks impacted at least 2,323 local governments, schools, and healthcare providers in the United States. According to the World Economic Forum, ransomware attacks increased by 435 percent in 2020 and "are outpacing societies' ability to effectively prevent or respond to them."

Many of these attacks generated significant losses and damages for victims. A three-year comparison of the number of complaints of ransomware submitted to the Federal Bureau of Investigation (FBI) between 2018 and 2020, demonstrates a 65.7 percent increase in victim count and a staggering 705 percent increase in adjusted losses. In 2021, the agency received 3,729 ransomware complaints with adjusted losses of more than $49.2 million.

However, even these figures likely drastically underestimate the actual number of attacks and ransom payments made by victims and related losses. In fact, the FBI acknowledges that its data is "artificially low." Further evidence of this under-reporting is that the government data is significantly lower than several private sector estimates. For instance, Chainalysis, a blockchain data and analysis company that works with financial institutions, insurance and cybersecurity companies, and as a contractor for the U.S. government, reports that in 2020, malign actors received at least $692 million in cryptocurrency extorted as part of ransomware attacks, up from $152 million in 2019, close to a 300 percent increase over a two-year period. A separate study by the anti-malware company Emsisoft found that there were at least 24,770 ransomware incidents in the U.S. in 2019 and estimated their costs (including costs of downtime) at just under $10 billion.

To better understand this growing threat, U.S. Senator Gary Peters, Chairman of the Senate Homeland Security and Governmental Affairs Committee, announced in July 2020 an investigation into the role of cryptocurrency in incentivizing and enabling ransomware attacks, and the resulting harm of such attacks to victims. As a part of this ten-month investigation, Committee staff conducted interviews with federal law enforcement and regulatory agencies as well as private companies that assist ransomware victims with ransom demands. While not exhaustive, this report addresses key pieces of the larger landscape of the increasing national security threat from ransomware attacks and the use of cryptocurrency for ransom payments. The report details recommendations to address current gaps in information on ransomware attacks and use of cryptocurrency as ransom payments in these attacks.

The report finds that there is a lack of comprehensive data on the amount of ransomware attacks and use of cryptocurrency as ransom payments in these attacks. While multiple federal agencies are taking steps to address the increasing threat of ransomware attacks, more data is needed to better understand and combat these attacks. In interviews with Committee staff, federal officials and private sector companies each acknowledged the need for more compliance and data (*e.g.*, reporting of incidents and ransom payments). When more data is collected, the federal government will be in a better position to assist existing and potential cybercrime victims with prevention, detection, mitigation, and recovery. Such information also facilitates more efficient investigation and prosecution of illicit actors.

To address the current lack of information regarding the breadth and depth of the ransomware threat, Chairman Peters and Ranking Member Portman introduced the Cyber Incident Reporting Act of 2021, which passed the Senate as part of the Strengthening American Cybersecurity Act of 2022. The incident reporting provisions later became law as the Cyber Incident Reporting for Critical Infrastructure Act of 2022 in the Consolidated Appropriations Act of 2022 in March 2022. The new reporting mandates in the law will begin to address this problem. Nevertheless, as indicated by the findings in the report, the Administration and Congress must remain vigilant against this growing threat.

Almost 40 million Americans – including approximately three-in-ten Americans age 18 to 29 – have engaged in some form of investment, trade, or other legitimate use of cryptocurrencies according to a November 2021 estimate by the nonpartisan Pew Research Center. The global market value of all cryptocurrencies reached $3 trillion in 2021, up from $14 billion in 2016.

However, according to multiple agencies interviewed by Committee staff, cryptocurrency, typically Bitcoin, has become a near universal form of ransom payment in ransomware attacks, in part, because cryptocurrency enables criminals to extort huge sums of money from victims across diverse sectors with incredible speed. The payment structure's decentralized nature, as well as irregular regulatory compliance by some entities within the space and new anonymizing techniques contribute to the challenges law enforcement faces when seeking to arrest criminal actors, particularly foreign-based actors. High profile attacks, such as Colonial Pipeline, demonstrate ransomware attackers' threat to national security. The FBI's recovery of over half of the ransom paid by Colonial Pipeline, however, shows that with access to the right information, law enforcement can leverage cryptocurrency's unique features as well as other investigative techniques to track down cyber criminals and recover stolen funds.

Unfortunately, data reporting and collection on ransomware attacks and payments is fragmented and incomplete. Two federal agencies claim to host the government's one stop location for reporting ransomware attacks – the Cybersecurity and Infrastructure Agency (CISA) StopRansomware.gov website and the FBI's IC3.gov. These two websites are separate and, while the agencies state that they share data with each other, in discussions with Committee staff, ransomware incident response firms questioned the effectiveness of such communication channels' impact on assisting victims of an attack.

Many federal regulators have taken steps to address the rising threat of ransomware attacks by issuing new, and expanding existing, regulations and guidance. Generally, with respect to cryptocurrency, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) has clarified that "money service businesses", *e.g.*, persons that accept and transmit "value that substitutes for currency", are subject to key financial regulations. Over the past few years, the Securities and Exchange Commission (SEC), Internal Revenue Service (IRS), and FinCEN have each issued new guidance and regulations subjecting cryptocurrency to additional oversight. In 2021, the Department of Justice (DOJ), SEC, and the Treasury Department's Office of Foreign Assets Control (OFAC), among other agencies, also issued guidance recognizing the need for more ransomware incident reporting.

On March 9, 2022, the Biden Administration issued an Executive Order outlining a "whole-of-government" approach to examining the risks associated with the sharp increase in use of cryptocurrencies. Among other key policy priorities, the Administration recognizes that cryptocurrencies have "facilitated sophisticated cybercrime-related financial networks and activity, including through ransomware activity." The data needed to support these initiatives, among other agency efforts to tackle ransomware and cryptocurrency ransom payments, however, is fragmented and incomplete.

This limited collective understanding of the ransomware landscape and the cryptocurrency payment system blunts the effectiveness of available tools to protect national security and limits private sector and federal government efforts to assist cybercrime victims. As Russia's invasion of Ukraine continues and Russia seeks to find ways around the international finance system, the need to address these shortfalls grows. Approximately 74 percent of global ransomware revenue in 2021 went to entities either likely located in Russia or controlled by the Russian government. Further, CISA and other federal agencies have warned that Russia's invasion of Ukraine could lead to additional malicious cyber activity, including ransomware attacks, in the United States. Therefore, as the report finds, prioritizing the collection of data on ransomware attacks and cryptocurrency payments is critical to addressing increased national security threats.

I. FINDINGS OF FACT AND RECOMMENDATIONS

FINDINGS OF FACT

1. **The federal government lacks comprehensive data on ransomware attacks and use of cryptocurrency in ransom payments.** The government largely relies on voluntary reporting of ransomware attacks and cyber extortion demands, which only captures a fraction of the attacks that occur. As of July 2021, the Cybersecurity and Infrastructure Security Agency (CISA), which was created in 2018 specifically to reduce risk to the nation's cyber and physical infrastructure, estimated that only about one quarter of ransomware incidents were reported.

2. **Current reporting is fragmented across multiple federal agencies.** Data on ransomware attacks is reported to numerous federal agencies including CISA, the FBI, and the Treasury Department's FinCEN, among others. These agencies do not capture, categorize, or publicly share information uniformly.

3. **Lack of reliable and comprehensive data on ransomware attacks and cryptocurrency payments limits available tools to guard against uational security threats.** The lack of data on ransomware attacks and cryptocurrency ransom payments blunts the effectiveness of available tools for fighting ransomware attacks including U.S. sanctions, law enforcement efforts, and international partnerships, among other tools.

4. **Curreutly available data on ransomware attacks and cryptocurrency payments limits both private sector and federal government efforts to assist cybercrime victims.** The private sector and the federal government are not able to fully and effectively assist victims to prevent or recover from ransomware attacks without a comprehensive dataset on ransomware attacks, ransom demands, and payments. Such a dataset does not currently exist.

RECOMMENDATIONS

1. **The Administration should swiftly implement the new ransomware attacks and ransom payments reporting mandate.** CISA should complete the required rulemaking as soon as possible to implement the requirements in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 signed into law as part of the Consolidated Appropriations Act of 2022, which mandates incident reporting of substantial cyber-attacks and ransomware payments against critical infrastructure. Federal agencies should implement the requirement in the law to share all cyber incident reports with CISA to enable a consolidated view of incidents from across different sectors and reported under different regulatory regimes.

2. **The federal government should standardize existing federal data on ransomware incidents and ransom payments to facilitate comprehensive analysis.** Agencies should standardize how data from existing reporting requirements for ransomware incidents and ransom payments is organized and formatted across federal government agencies to enable more comprehensive information sharing and analysis.

3. **Congress should establish additional public-private initiatives to investigate the ransomware economy.** The federal government should promote public-private partnerships to research the ransomware economy, in particular, the interrelationships between cybercriminals who conduct or facilitate ransomware attacks and the financial structures facilitated by cryptocurrencies that sustain cybercriminals' illicit activities, including privacy coins. These partnerships should also examine ransomware infrastructure to help design and promote effective countermeasures.

4. **Congress should support information sharing regarding ransomware attacks and payments including crowdsourcing initiatives.** Congress and relevant agencies should consider ways to support partners within the private, nonprofit, and academic sectors seeking to expand the collection and organization of information on ransomware attacks including by examining federal funding options and sharing anonymized data regarding ransomware attacks and payments. In addition, government agencies should collaborate with partners to identify viable crowdsourcing initiatives to pool information regarding ransomware attacks and extortion payments.

II. BACKGROUND

On July 20, 2021, U.S. Senator Gary Peters, Chairman of the Senate Homeland Security and Governmental Affairs Committee, announced an investigation into the role that cryptocurrency plays in facilitating ransomware attack payments and the consequent escalation of ransomware attacks.[1] As a part of this investigation, staff conducted interviews with federal law enforcement and regulatory agencies as well as private companies that assist ransomware victims with ransom demands. Both federal agencies and private companies raised concerns regarding the lack of visibility into the full scope of ransomware threats and cryptocurrency ransom payments. Each of the interviewees advocated for increased data collection regarding illicit actors' methods and ransom payments to better understand the ever-evolving landscape of ransomware attacks and illicit uses of cryptocurrency.

A. Ransomware Attacks and Use of Cryptocurrency as Payment

Ransomware is an increasingly threatening and continually evolving form of cryptocurrency-enabled crime.[2] The origins of ransomware can be traced to the late 1980s.[3] By 2006, near universal access to the internet and online cash-equivalent instruments enabled increased anonymity and a more global reach, thereby creating new opportunities for profitable cybercrime. Geographic limitations tied to payment mechanisms and financial regulations, however, made it difficult to generate significantly large proceeds from ransomware attacks.[4] At the time, threat actors primarily used online payment systems such as Western Union and PayPal, among other methods, to receive ransom payments.[5] Although an alternative to banks, these payment systems engaged traditional depository financial institutions to facilitate the ransom payment transfer. In countries with anti-money laundering rules, *e.g.*, the United States,

[1] Senate Homeland Security and Governmental Affairs Committee, *Peters Announces Investigation Into Rise of Ransomware Attacks and How Cryptocurrencies Facilitate Cybercrimes* (July 20, 2021).

[2] Chainalysis, *The 2022 Crypto Crime Report* (Feb. 2022) (go.chainalysis.com/2022-Crypto-Crime-Report.html) (hereinafter "*The 2022 Crypto Crime Report*").

[3] Kaveh Waddell, *The Computer Virus That Haunted Early AIDS Researchers*, Atlantic (May 10, 2016) (https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/). In 1989, 20,000 AIDS researchers received floppy disks infected with the AIDS Trojan, *a.k.a.* PC Cyborg virus, disguised as a questionnaire to "help determine patients' risk of contracting AIDS." The ransom note demanded that a payment be made to a P.O. Box in Panama to retrieve access to files that were encrypted after use. *Id.*

[4] *See* Bart Custers, Jan-Jaap Oerlemans, and Ronald Pool, *Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies*, European Journal of Crime, Criminal Law and Criminal Justice (2020) (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3694282) and D. Y. Huang, et al., *Tracking Ransomware End-to-end*, IEEE Symposium ou Security and Privacy (2018) (ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8418627).

[5] Bart Custers, Jan-Jaap Oerlemans, and Ronald Pool, *Laundering the Profits of Ransomware*, European Journal of Crime, Criminal Law and Criminal Justice (2020) (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3694282).

regulated financial institutions are generally required to notify authorities of suspicious transactions and conduct background screenings to detect potentially illicit transactions.[6]

In 2009, Bitcoin, a type of cryptocurrency, was released and its eventual use by cybercriminals as a preferred form of ransom payment drastically transformed the ransomware business model.[7] This decentralized monetary system was designed to remove barriers to the transfer of value and allow "online payments to be sent directly from one party to another without going through a financial institution."[8] The foundational technology of cryptocurrency—blockchain—consists of a distributed ledger that is managed by its users through a peer-to-peer system. Once a Bitcoin cryptocurrency transaction is authorized by network participants, the amount of funds transferred, a timestamp, and the bitcoin addresses are stored on the blockchain and made publicly available.[9] The public ledger makes available an exact and transparent order of events which is designed to enhance trust between participants and promote security. Thus, any individual can join the network and view a history of transactions.[10]

Starting in 2012, as the use of Bitcoin and other cryptocurrencies became more widespread, ransomware encryption techniques also grew along with expansion of the digital black market.[11] This further enabled the modern wave of ransomware attacks that rely on payment via cryptocurrencies.[12]

[6] 31 U.S.C. § 5311 – 5330; *see also* Bart Custers, Jan-Jaap Oerlemans, and Ronald Pool, *Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies*, European Journal of Crime, Criminal Law and Criminal Justice (2020) (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3694282); Paypal, *PayPal Anti-Money Laundering and Counter-Terrorist Financing Statement* (May 11, 2009) (www.paypal.com/us/webapps/mpp/ua/aml-full) (explaining that "PayPal has robust policies and procedures to detect, prevent and report suspicious activity" and conducts background screenings to comply with OFAC (Office of Foreign Asset Control) requirements, and global sanctions).

[7] Bitcoin is spelled with a capital letter when referring to the software and community, and with a lower letter when referring to the unit of currency.

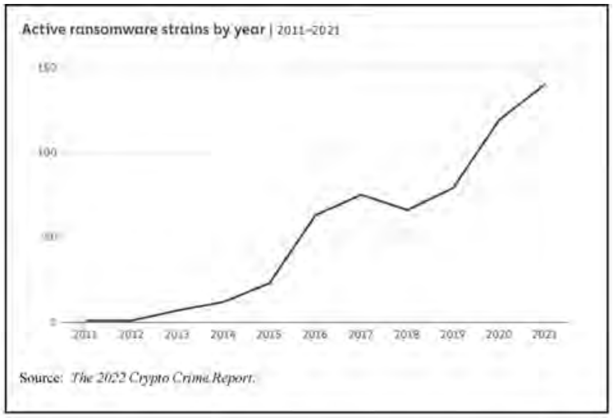
[8] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (bitcoin.org/bitcoin.pdf).

[9] Other cryptocurrency transactions make public similar information.

[10] *How to Read a Blockchain Transaction History*, Ledger (blog) (Sept. 11, 2020) (https://www.ledger.com/academy/how-to-read-a-blockchains-transaction-history).

[11] *See History of Ransomware*, CrowdStrike (June 21, 2021) (www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/); Aamir Lakhani, *Analyzing the History of Ransomware Across Industries*, Fortinet (blog) (May 17, 2021) (www.fortinet.com/blog/industry-trends/analyzing-the-history-of-ransomware-across-industries). *See also* Kurt Thomas, et al., *Framing Dependencies Introduced by Underground Commoditization*, Workshop on Economics of Information Security (2015) (elie.net/static/files/framing-dependencies-introduced-by-underground-commoditization/framing-dependencies-introduced-by-underground-commoditization-paper.pdf).

[12] *See History of Ransomware*, CrowdStrike (June 21, 2021) (www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/). *See also* Elie Bursztein, Luca Invernizzi, and Kylie McRoberts, *Unmasking the ransomware kingpins*, Elie (blog) (Oct. 2017) (https://elie.net/blog/security/unmasking-the-ransomware-kingpins/).



Source: *The 2022 Crypto Crime Report*.

Several characteristics of cryptocurrency, and particularly Bitcoin, make it one of the current ransom payment methods of choice for threat actors: large sums can be transferred more or less instantaneously worldwide; the system is decentralized and largely unregulated; it has a high level of flexibility; and the technology enables innovative approaches to maximize anonymity and make it increasingly harder for law enforcement agencies and regulators to track. In conversations with Committee staff, officials from the Department of Justice (DOJ) and the Treasury Department's Financial Crimes Enforcement Network (FinCEN) confirmed the correlation between cryptocurrency and the rise of modern ransomware attacks. As officials from DOJ told the Committee, "before cryptocurrency, ransomware attacks were difficult to monetize. With the availability of virtual currencies, however, criminals can collect ransoms much more easily. In addition, cryptocurrency payments are irreversible."[13]

The transparent nature of blockchain, however, also enables law enforcement agencies in some instances to track and interpret the flow of illicit cryptocurrency assets, to identify threat actors, and hold them accountable.[14] To make or receive a payment in bitcoin, a user must first create a Bitcoin wallet – a set of keys created using a device or program that sends and receives cryptocurrency, similar to a traditional wallet.[15] Each Bitcoin wallet contains a public key, used

[13] Letter from Peter Hyun, Acting Assistant Attorney General, Department of Justice, Letter to Chairman Peters (Apr. 29, 2022) (hereinafter "DOJ Letter"). In an interview with Committee staff, FinCEN also indicated that the agency had seen a correlation between the ease of being able to use and understand cryptocurrency, the speed of transactions, and the rise of ransomware attacks. Kevin O'Connor, Chief of Virtual Assets and Emerging Technology Section, Financial Crimes Enforcement Network, Interview with Senate Committee on Homeland Security and Governmental Affairs (July 20, 2021) (hereinafter "FinCEN O'Connor Interview").

[14] FinCEN O'Connor Interview.

[15] Jake Frankenfield, Amilcar Chavarria, and Katrina Munichiello, *Bitcoin Wallet*, Investopedia (Jan. 13 2022) (www.investopedia.com/terms/b/bitcoin-

to receive transactions, and a private key, used to sign and send Bitcoin transactions, giving the user control over the bitcoins in that address. Bitcoin wallets do not need to be registered or associated with the person who creates them – thus making it difficult to identify the owner or user of any particular wallet. Ransomware actors will often create one cryptocurrency wallet per victim; wallets can be easily generated and are "fresh and new" for most ransomware victims.[16] Although hidden, the identity of cryptocurrency wallet address holders may sometimes be deduced by tracing the transfer of ransom payments across the blockchain.[17] Oftentimes, key information can be deduced from the point where traditional currency is used to purchase cryptocurrency—the "on-ramp"—and the final destination where the illicit cryptocurrency is converted back to traditional currency— the "off ramp".[18]

Threat actors regularly operate on the darknet, an encrypted network on the internet that has its own social networks, search engines, sites, forums and other platforms for communication and file transfer.[19] To access the darknet, users must use specific browsers, such as Tor browser, as this part of the web is inaccessible via traditional search engines, such as Google.[20] A key difference between the darknet and the part of the web that is visible to the average user, *i.e.*, the surface web or clearnet, is the degree of anonymity. Whereas sites and social networks on the clearnet may be able to establish the identity of a user as well as their IP address, the darknet is designed to be more anonymous and conceals IP addresses, making it difficult for internet activity to be traced back to the user.[21] Online black markets and underground web-forums where illicit actors connect with each other are often utilized to purchase and sell tools for cyber-attacks, including ransomware attacks.[22] These same markets and forums are also used to recruit ransomware actors, and are typically located on the darknet.[23]

wallet.asp#:~:text=A%20Bitcoin%20wallet%20is%20a,Bitcoin%20addresses%20and%20send%20transactions) (noting that "instead of storing physical currency, the wallet stores the cryptographic information used to access bitcoin addresses and send transactions").

[16] Kurtis Minder, Chief Executive Office, GroupSense, Interview with Senate Committee on Homeland Security and Governmental Affairs (Mar. 31, 2022) (hereinafter "Minder Interview").

[17] Bill Siegel, Chief Executive Officer, Coveware, Interview with Senate Committee on Homeland Security and Governmental Affairs (Dec. 2, 2021) (hereinafter "Siegel Interview").

[18] *See generally Crypto On and Off-Ramps – How and Where?*, Ledger (Jan. 19, 2022) (www.ledger.com/academy/crypto-on-and-off-ramps-say-what). Traditional currency is also referred to as fiat currency, real currency, or national currency. *Id.*

[19] Congressional Research Service, *Dark Web* (R44101) (Mar. 10. 2017).

[20] *Id.* Tor or "The Onion Router" is an anonymity network designed to obfuscate communications. *Id.*

[21] Kyle Chivers, *What does an IP address tell you and how it can put you at risk*, Norton (Apr. 23, 2021) (us.norton.com/internetsecurity-privacy-what-does-an-ip-address-tell-you.html). An Internet Protocol address (IP address) is a unique identifier that typically reveals the geolocation, *e.g.*, city, zip code, or area code, of the nearest internet service provider (ISP). The IP address changes each time a device is connected to a different Wi-Fi network or router. *Id.*

[22] *See* Department of Justice, *Department of Justice Launches Global Action Against NetWalker Ransomware* (Jan. 27, 2021) (www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware).

[23] Anthony M. Freed, *What is the Dark Web Ransomware Marketplace?*, Cybereason (Oct. 19, 2021) (www.cybereason.com/blog/what-is-the-dark-web-ransomware-marketplace).

Cryptocurrency is the primary method of payment and money transmission in online black markets, to include those operating on the clearnet, as well as the darknet.[24] According to publicly available information from the U.S. Secret Service (hereinafter "Secret Service"), the widespread use of cryptocurrency enables transnational cybercrime, including ransomware for the following reasons:

> it provides a ready means for transnational criminals to convert to and from fiat currencies as well as transfer and launder proceeds of cyber-enabled crimes. Cyber criminals have additionally developed substantial networks of money mules and various digital money laundering services, such as over-the-counter brokers or exchange services and other unlicensed money services, to launder illicitly obtained funds.[25]

In conversations with Committee staff, FinCEN emphasized, "the law enforcement perspective is that we have had ransomware issues for years and we have serious issues with crimes on the darknet where cryptocurrency is really the only form of payment."[26] According to the Secret Service, cryptocurrency is increasingly almost exclusively the required method of payment demanded by ransomware attackers.[27]

B. Anatomy of a Ransomware Attack

Ransomware is a subset of malware—"an umbrella term for any malicious code or program that gives a threat actor explicit control over a system."[28] CISA describes ransomware

[24] Congressional Research Service, *Dark Web* (R44101) (Mar. 10. 2017); Email from United States Secret Service, Criminal Investigative Division, to Senate Committee on Homeland Secnrity and Governmental Affairs (Apr. 14, 2022).

[25] United States Secret Service, *U.S. Secret Service Launches Cryptocurrency Awareness Hub* (Feb. 18, 2022) (www.secretservice.gov/newsroom/releases/2022/02/us-secret-service-launches-cryptocurrency-awareness-hub). "Money mules" refer to individuals who move illicit funds on someone's behalf typically to facilitate the laundering of illicit proceeds. *Money Mules Don't Be a Mule: Awareness Can Prevent Crime*, Federal Bureau of Investigation (accessed on Mar. 30, 2022) (www.fbi.gov/scams-and-safety/common-scams-and-crimes/money-mules). Over the counter (OTC) trades involve brokers acting on behalf of private parties who are seeking to trade immense volumes of cryptocurrency with enhanced privacy and anonymity. *See* Connor Dempsey, *How does crypto OTC actually work?*, Medium (Mar. 25, 2019) (medium.com/circle-research/how-does-crypto-otc-actually-work-e2215c4bb13). *See also* Rihonna Scoggins, *What an FBI Section Chief Has Learned Investigating Virtual Currencies*, Fraud Conference News (Nov. 17, 2021) (www.fraudconferencenews.com/home/2021/11/15/what-you-need-to-understand-about-virtual-currencies-nbsp) (stating that a majority of cryptocurrency transactions are facilitated through OTC desks); *see generally* Congressional Research Service, *Dark Web* (R44101) (Mar. 10. 2017) (discussing how bitcoin is used and preferred on the Dark Web).

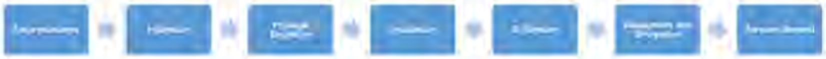
[26] FinCEN O'Connor Interview.

[27] Email from United States Secret Service, Criminal Investigative Division, to Senate Committee on Homeland Security and Governmental Affairs (Apr. 14, 2022).

[28] Andy Patrizio, *Malware vs. ransomware: What's the difference?*, TechTarget (July 13, 2021) (whatis.techtarget.com/feature/Malware-vs-ransomware-Whats-the-difference#:~:text=Malware%20is%20an%20umbrella%20term,system%20and%20encrypts%20the%20data).

as "a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption."[29] An archetypal ransomware attack is described below and will resemble the diagram in Figure 1.[30]

Figure 1. Anatomy of a Ransomware Attack



Compiled by Senate Homeland Security and Governmental Affairs Committee, Majority.

1. **Reconnaissance**. The threat actor, often a third party affiliate, analyzes the victim's assets for weaknesses.

2. **Infiltration**. The ransomware infiltrates the victim's computer system via an attack vector, *e.g.*, social engineering tactics such as phishing or known vulnerabilities.

3. **Privilege escalation**. After gaining entry, the threat actor may attempt to escalate privileges on the device or pivot to other internal company systems with more sensitive data.

4. **Installation**. Once the threat actor has sufficient permissions, the ransomware is installed on the victim's computer to gain access to its files and systems.

5. **Exfiltration**. In some ransomware attacks, the threat actor "exfiltrates" or steals, the data in a process known as double extortion.[31] The threat actor then transfers the stolen data to storage servers accessible by the attacker.[32]

6. **Deployment and Encryption**. The threat actor then deploys the ransomware, executing malicious code to encrypt the victim's data.[33]

[29] Cybersecurity and Infrastructure Security Agency, Stop Ransomware (accessed on Feb. 21, 2022) (www.cisa.gov/stopransomware).

[30] *Ransomware vs. malware*, Box Communications (blog) (Oct. 27, 2021) (blog.box.com/ransomware-vs-malware).

[31] Janus Agcaoili, Miguel Ang, Earle Earnshaw, et. al., *Ransomware Double Extortion and Beyond: REvil, Clop, and Conti*, Trend Micro (June 15, 2021) (https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti).

[32] *Id.* While some ransomware attacks exfiltrate data (and may extort payment to prevent the release of that data), many of these attacks only encrypt the data. *Id.*

[33] McAfee, *What Is Ransomware?* (accessed Mar. 28, 2022) (www.mcafee.com/enterprise/en-us/security-awareness/ransomware.html).

7. **Ransom Demand**. After encryption is complete, the victim will see a message from attackers demanding a ransom (usually in cryptocurrency) in exchange for the decryption key to decrypt and allow access to the victim's files.[34] The ransomware often establishes a specific time frame during which victims must pay the ransom in order to decrypt the files, *e.g.* 24 to 48 hours, after which it threatens to either increase the ransom amount, destroy the files, or delete the decryption key. If the attack is a double extortion attack, the ransom demand would be, in addition to the decryption key, in exchange for the attacker deleting the exfiltrated files, under threat of making the files public in the event the ransom is not paid.[35]

While to date, ransom payments are most commonly made in Bitcoin, ransomware attackers also may demand payment in other cryptocurrencies such as Monero, a privacy coin. Such coins are cryptocurrencies that preserve additional anonymity beyond Bitcoin and other older cryptocurrencies "by obscuring the flow of money across their networks."[36]

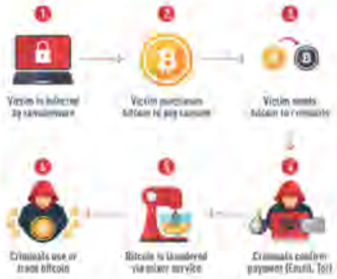
[34] *Id.* Certain types of ransomware will leak a portion of stolen data prior to contacting the victim as a sort of ransom. *Id.*

[35] Coveware, *Quarterly Report: Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues* (Nov. 4, 2020) (https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report).

[36] Robert Stevens, *What Are Privacy Coins and Are They Legal?*, CoinDesk (accessed Jan. 10, 2022) (www.coindesk.com/learn/what-are-privacy-coins-and-are-they-legal).

After illicit actors gain access to a victim's computer system, the parties will typically follow the payment transaction steps depicted in Figure 2 and described below.[37]

Figure 2. Cyberextortion payment transactions


1
Victim is infected by ransomware
2
Victim purchases bitcoin to pay ransom
3
Victim sends bitcoin to criminals
4
Criminals confirm payment (Email, Tor)
5
Bitcoin is laundered via mixer service
6
Criminals use or trade bitcoin

Source: *Spotlight on ransomware: Ransomware payment methods*, Emsisoft (blog) (Aug. 15, 2017).

1. Demand for ransom is made.

2. Victim may attempt to negotiate with the actors or refuse to make the payment.

3. If a victim decides to pay the ransom, they use traditional currency to purchase the demanded cryptocurrency, typically bitcoin.

4. Victim sends the ransom payment in cryptocurrency to the criminals at the digital wallet address specified in the ransom note or on a payment portal (often located on the darknet).

5. Criminals typically either "cash out", *i.e.*, exchange the cryptocurrency for traditional currency, or launder the cryptocurrency through cryptocurrency mixing services before "cashing out".

[37] Ransomware Task Force, *Combating Ransomware*, Institute for Security and Technology (Apr. 2021) (securityandtechnology.org/ransomwaretaskforce/report/).

C. U.S. Regulations, Illicit Uses of Cryptocurrency, and Ransomware Attacks

In the United States, cryptocurrency transactions are regulated under a patchwork of federal and state laws and regulations. No one regulatory agency has direct authority over virtual currencies. Further, there is no uniform definition for "cryptocurrency" under U.S. law. "Cryptocurrency" is often referred to as "virtual currency," "digital assets," "digital tokens," "cryptoassets," or "crypto."

Generally, at the federal level, the Securities and Exchange Commission (SEC) regulates the issuance of any digital asset that constitutes a security; the Commodity Futures Trading Commission (CFTC) exercises general anti-fraud and manipulation enforcement authority over cryptocurrency cash markets as a commodity in interstate commerce; the Internal Revenue Service (IRS) deems virtual currency to be property for tax purposes; the Office of the Comptroller of the Currency (OCC) regulates crypto-related activities in the banking industry; and FinCEN regulates certain uses of cryptocurrency in connection with money laundering and related financial crimes. The Bank Secrecy Act (BSA) and implementing regulations issued by FinCEN, discussed in more detail below, are the key anti-money laundering statutes and rules applicable to both traditional and virtual currency.

1. Bank Secrecy Act and Implementing Regulations

In 1970, Congress enacted the Currency and Foreign Transactions Reporting Act, commonly known as the BSA, to confront the threat of money laundering and related crimes.[38] The law establishes specific requirements for recordkeeping and reporting by private individuals, banks, and non-banking financial institutions to prevent malign actors from using U.S. financial institutions to obscure illicit funds. Subsequent laws enhanced and amended the BSA to provide additional tools to combat money laundering and to counter terrorism financing.[39]

In 2011, FinCEN, the federal agency that administers the BSA, issued regulations that have since been used to impose anti-money laundering requirements on the cryptocurrency industry.[40] In 2013, FinCEN issued interpretive guidance to clarify the applicability of the BSA and its implementing regulations to persons "creating, obtaining, distributing, exchanging,

[38] Pub. L. No. 91-508.

[39] *Id.* The BSA has been amended by the Title III of the USA PATRIOT Act of 2001 and the Anti-Money Laundering Act of 2020. *Id.* The USA PATRIOT Act—the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001" was enacted to enhance law enforcement investigatory tools to deter and punish terrorist acts in the United States and around the world. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, Pub. L. No. 107-56 (2001). In the 2021 National Defense Authorization Act (NDAA), Congress included significant reforms to the U.S. anti-money laundering (AML) regime. The NDAA includes the Anti-Money Laundering Act of 2020 (AMLA) and, within the AMLA, the Corporate Transparency Act (CTA). William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283 (2021).

[40] Pub. L. No. 91-508, as amended and 31 CFR § 1010.100(ff) (formerly 31 CFR § 103.11(uu)). *See also* 31 U.S.C. 310 (establishing FinCEN and requiring it to implement the recordkeeping, reporting, and other requirements of the BSA).

accepting, or transmitting virtual currencies."[41] The regulations clarify that "administrators" and "exchangers" are regulated as money service businesses.[42]

Pursuant to the BSA, a "money service business" (MSB) includes "money transmitters"— individuals and entities engaged in the transfer of funds, including the transmission of "value that substitutes for currency" to another location or person.[43] Per FinCEN guidance issued in May 2019, "value that substitutes for currency" includes convertible virtual currency (CVC) such as Bitcoin.[44] In 2020, the Cyber-Digital Task Force within DOJ published a cryptocurrency enforcement framework in which it reiterates that,

> [i]n the United States, individuals and entities that offer money transmitting services involving virtual assets, such as cryptocurrency exchanges and kiosks, as well as certain issuers, exchangers, and brokers of virtual assets, are considered MSBs.[45]

Thus, MSBs that engage in the transfer of cryptocurrency payments subject to U.S. jurisdiction must establish and maintain an anti-money laundering program, comply with suspicious activity and currency transaction reporting rules, among other BSA requirements for MSBs.[46] With few exceptions, they must also register with FinCEN.[47]

Note, however, certain business models involving CVC transactions can be exempt from "money transmitter" status and therefore are not subject to BSA anti-money laundering

[41] Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (FIN-2013-G001) (Mar. 18, 2013).

[42] *Id.* (defining "exchanger" as "a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency" and defines "administrator" as "a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency").

[43] Pub. L. No. 91-508, as amended and 31 CFR § 1010.100(ff) (formerly 31 CFR § 103.11(uu)). *See also* 31 U.S.C. 310 (establishing FinCEN and requiring agency to implement the recordkeeping, reporting, and other requirements of the BSA, as well as disseminating information to appropriate law enforcement agencies)

[44] Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (FIN-2019-G001) (May 9, 2019) (defining CVCs as a "type of virtual currency that either has an equivalent value as currency, or acts as a substitute for currency").

[45] Department of Justice, *Cryptocurrency: Enforcement Framework* (Oct. 2020).

[46]*See* 31 CFR § 1022.210 (requiring for MSBs to establish and maintain an anti-money laundering program); 31 CFR § 1022.310 (requiring for MSBs to file Currency Transaction Reports); 31 CFR § 1022.320 (requirement for MSBs to file Suspicious Activity Reports, other than for check cashing); 31 CFR § 1010.415 (requiring certain MSBs to verify the identity of the customer and create and maintain a record of each currency purchase between $3,000 and $10,000, inclusive); 31 CFR § 1010.410(e) and (f) (making rules applicable to certain transmittals of funds). *See also* Financial Crimes Enforcement Network, *BSA Requirements for MSBs* (accessed on May 3, 2022) (https://www.fincen.gov/bsa-requirements-msbs).

[47] *See* 31 CFR 1022.380. *See also* Financial Crimes Enforcement Network, Money Services Business (MSB) Registration (accessed Mar. 31, 2022).

requirements.[48] For instance, an individual or an entity that merely provides the "delivery, communication, or network access services used by a money transmitter to support money transmission services" is not subject to BSA regulatory requirements.[49] Under this exemption, CVC trading platforms that merely enable buyers and sellers to connect with each other are not subject to BSA rules.[50] Additionally, under the "integral services" exemption, businesses that provide services other than money transmission services, and which accept and transmit CVC as an integral part of providing such services, do not generally have to meet the BSA anti-money laundering requirements.[51] Ultimately, whether a person is a money transmitter under the BSA depends on the "facts and circumstances" of each case.[52]

Importantly, foreign-based MSBs that conduct activities within the United States must register with FinCEN as an MSB, and comply with anti-money laundering program, recordkeeping, monitoring, and reporting requirements. This is true even if the MSB does not have a physical presence in the U.S.[53] FinCEN specifically noted that this rule seeks to address the globalized nature of the internet, "the Internet and other technological advances make it increasingly possible for persons to offer MSB services in the United States from foreign locations."[54] Thus, foreign-located MSBs that provide services to persons in the United States such as sending virtual currency to, or receiving virtual currency from, third parties through the MSB, must comply with the BSA.[55]

[48] 31 CFR § 1010.100(ff)(5)(ii). *See also* Financial Crimes Enforcement Network, *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform* (FIN-2014-R011) (Oct. 27, 2014).

[49] 31 CFR § 1010.100(ff)(5)(ii)(A). *See also* Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (FIN-2019-G001) (May 9, 2019).

[50] The trading platform becomes a money transmitter if it also facilitates trades as an intermediary. Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (FIN-2019-G001) (May 9, 2019).

[51] Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (FIN-2019-G001) (May 9, 2019). *See also* 2011 MSB Final Rule, 76 FR at 43594 (stating "persons that sell goods or provide services other than money transmission services, and only transmit funds as an integral part of that sale of goods or provision of services, are not money transmitters").

[52] 31 CFR § 1010.100(ff)(5)(ii); Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (FIN-2019-G001) (May 9, 2019).

[53] Financial Crimes Enforcement Network, *Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses*, 76 FR 43585 (July 21, 2011) (final rule); Financial Crimes Enforcement Network, *Foreign-Located Money Service Businesses* (FIN-2019-A001) (Feb. 15, 2012). The 2011 rule revised FinCEN regnlations such that an entity qualifies as an MSB based on its activity within the United States, not its physical presence. The final rule states that the definition of an MSB includes, "[a] person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States." *Id.*

[54] Financial Crimes Enforcement Network, *Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses*, 76 Fed. Reg. 43585 (Jnly 21, 2011) (final rule).

[55] Financial Crimes Enforcement Network, *Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses*, 76 Fed. Reg. 43585 (Jnly 21, 2011) (final rule).

2. Federal Reporting Requirements for Transmitters of Virtual Currency

Administrators and exchangers, as defined by the FinCEN regulations, of virtual currency become money transmitters when they either exchange "traditional currency to cryptocurrency" or exchange "one cryptocurrency to another cryptocurrency."[56] Like brick and mortar financial institutions, such money transmitters must collect, keep, and report to authorities details regarding certain transactions involving cryptocurrency under the BSA.[57] This is true regardless of whether the money transmitter is operating in traditional currency, nonanonymized CVC, or anonymity-enhanced CVC (AEC). According to FinCEN, "a money transmitter cannot avoid its regulatory obligations because it chooses to provide money transmission services using anonymity-enhanced CVC" or with an "added feature of concealing the source of the transaction."[58]

The BSA's reporting requirements provide law enforcement and regulators with a certain degree of visibility into suspicious transactions and certain transactions involving more than $10,000 in currency. Specifically, money transmitters that handle cryptocurrency pursuant to the BSA must meet the following reporting requirements:

- **Suspicious Activity Reports**: Money transmitters that handle virtual currency must file "Suspicious Activity Reports" (SARs) for "suspicious" transactions that involve or aggregate funds of $2,000 or more.[59] A transaction is "suspicious" where the individual or entity "knows, suspects, or has reason to suspect that a transaction" (or a pattern of transactions) either: i) "involves funds derived from illegal activity"; ii) is designed to evade any BSA regulations; iii) has no "business or apparent lawful purpose"; or iv)

[56] Department of Justice, *Cryptocurrency: Enforcement Framework* (Oct. 2020); *see* Bank Secrecy Act, 31 U.S.C. 5311-5330 (1970). FinCEN regulations apply to exchangers regardless of whether they are directly brokering transactions or are parties to transactions; Financial Crimes Enforcement Network, *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System* (FIN-2014-R012) (Oct. 27, 2014); Financial Crimes Enforcement Network, *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform* (FIN-2014-R011) (Oct. 27, 2014).

[57] *See generally* 31 C.F.R. Part 1022 (identifying BSA requirements applicable to MSBs) and Department of Justice, *Cryptocurrency: Enforcement Framework* (Oct. 2020). Note unlike banking financial institutions, MSBs are not required to implement "Know Your Customer" programs (KYC) under the BSA. However, MSBs must implement an anti-money laundering compliance program that is "reasonably designed to prevent the [MSB] from being used to facilitate money laundering and the financing of terrorist activities." The program must be "commensurate with the risks posed by the location and size of, and the nature aud volume of the financial services provided…." 31 CFR §1022.210; *see also* Letter from Charles P. Rettig, Department of the Treasury, Internal Revenue Service to Senator Margaret Wood Hassan (Dec. 21, 2021) (https://www.hassan.senate.gov/imo/media/doc/crypto.pdf).

[58] Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (FIN-2019-G001) (May 9, 2019).

[59] *See* 31 CFR Chapter X; Financial Crimes Enforcement Network, *Money Services Business (MSB) Suspicious Activity Reporting* (accessed on Mar. 30, 2022) (www.fincen.gov/money-services-business-msb-suspicious-activity-reporting).

"involves the use of the financial institution to facilitate criminal activity."[60] To comply with the BSA, the MSB must have an adequate SAR program that "requires identifying a business purpose for the subject transactions and a legitimate source of funds."[61] Financial institutions are not limited to the circumstances above and may voluntarily file a report alerting FinCEN of a possible violation of any law or regulation in connection with a suspicious transaction.[62]

- **Currency Transaction Reports**: Money transmitters that handle virtual currency must file "Currency Transaction Reports" (CTRs) on transactions involving more than $10,000 in currency conducted by, or on behalf of, one person in a single day.[63] This includes multiple transactions that aggregate to more than $10,000. The report must include personal identification information regarding the individual conducting the transaction. Note CTR requirements are triggered only by physical transfers of currency exceeding $10,000.[64] Accordingly, a ransomware payment may trigger a CTR filing if the victim used more than $10,000 in physical cash to obtain cryptocurrency for the payment. Similarly, cashing out of illicit ransom proceeds of more than $10,000 at a cryptocurrency kiosk may trigger the CTR requirement.

3. Application of BSA and FinCEN Regulations Within the Context of Ransomware Attacks

[60] 31 CFR §1022.320. *See* Financial Crimes Enforcement Network, *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments* (FIN-2020-A006) (Oct. 1, 2020) (providing a list of ransomware-related financial red flag indicators to assist financial institutions in detecting suspicious transactions associated with ransomware attacks). *See also* Financial Crimes Enforcement Network, *FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws* (April 18, 2019) (www.fincen.gov/news/news-releases/fincen-penalizes-peer-peer-virtual-currency-exchanger-violations-anti-money).

[61] Letter from Charles P. Rettig, Department of the Treasury, Internal Revenue Service to Senator Margaret Wood Hassan (Dec. 21, 2021) (www.hassan.senate.gov/imo/media/doc/crypto.pdf)

[62] Financial Crimes Enforcement Network, *FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Instructions* (Oct. 2012) (https://www.fincen.gov/sites/default/files/shared/FinCEN%20SAR%20ElectronicFilingInstructions-%20Stand%20Alone%20doc.pdf) and Fiuancial Crimes Enforcement Network, *Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021* (June 30, 2021) (www.fincen.gov/sites/default/files/shared/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf).

[63] 31 CFR § 1010.330; *see also* Financial Crimes Enforcement Network, *FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws* (Apr. 18, 2019) (www.fincen.gov/news/news-releases/fincen-penalizes-peer-peer-virtual-currency-exchanger-violations-anti-money); Financial Crimes Enforcement Network, *Notice to Customers: A CTR Reference Guide* (accessed on Apr. 1, 2022) (www.fincen.gov/sites/default/files/shared/CTRPamphlet.pdf). "Currency" is defined as, "[t]he coin and paper money of the United States or any other country, which is circulated and customarily used and accepted as money." Financial Crimes Enforcement Network, *FinCEN Form 104: Currency Transaction Report* (Mar. 2011) (https://www.irs.gov/pub/irs-tege/fin104_ctr.pdf#page=3).

[64] Transfers by means of bank check, bank draft, wire transfer, or other written orders do not trigger CTR obligations. Financial Crimes Enforcement Network, *FinCEN Form 104: Currency Transaction Report* (Mar. 2011) (https://www.irs.gov/pub/irs-tege/fin104_ctr.pdf#page=3).

With respect to pursuing ransomware attackers, FinCEN told the Committee that the BSA reporting requirements are critical for assisting law enforcement:

> The requirements of the BSA — registration with FinCEN, maintaining an effective AML program, and meeting recordkeeping and reporting requirements — help shed light on where transactions may originate and where they are, or are likely to be, cashed out. This assists law enforcement pursue ransomware attackers. Ultimately, ransomware actors have to cash out, and the BSA establishes rules for the financial institutions that facilitate these transactions.[65]

The following table illustrates how anti-money laundering regulations apply to certain cryptocurrency business models and other businesses that ransomware attackers and/or victims may use to convert, send, receive, or cash out, traditional or virtual currency in connection with a ransom payment.[66] Specifically, the table identifies which entities meet the definition of an MSB and thus, are subject to FinCEN rules for money laundering prevention, *e.g.*, implementation of a risk-based AML program, registration with FinCEN, SAR & CTR reporting, and recordkeeping. Whether a party is regulated pursuant to the BSA, however, depends on the "facts and circumstances" of a particular case. The information below is general in nature and is provided to illustrate the complexity and myriad of players that may be involved in a ransom payment process.

[65] FinCEN O'Connor Interview.

[66] The information in the table was compiled by Majority staff on the Senate Homeland Security and Governmental Affairs Committee.

BUSINESS / TRADING PLATFORM	DESCRIPTION	RANSOMWARE-RELATED EXAMPLE(S)	MSB (Y/N)
CVC Exchange	- Acts as middleman between buyers and sellers - Enables trade of fiat-to-crypto or crypto-to-crypto	Victim sets up account, transmits real currency to the account to purchase CVC and requests that the exchange send the ransom in CVC to perpetrator's digital wallet address	MSB: Y (may be exempt if merely connects buyers and sellers)
Peer-to-Peer (P2P) Exchanger	- Individual operates as a P2P exchange "whether or not on a regular basis" - Engages in money transmission	Victim uses P2P exchanger to obtain and send large CVC amount to settle ransom or attacker uses P2P exchanger to launder illicit ransom proceeds	MSB: Y (may be exempt if trades are conducted on an infrequent basis and not for profit)
Wallet Host	- Third-party, *e.g.*, CVC exchange, hosts users' digital currency wallet - Host has control over private keys and trades funds on behalf of user	Victim requests that wallet host send the demanded ransom amount in CVC from hosted wallet to perpetrator's address	MSB: Y
Unhosted Wallet	- Individual self-hosts digital wallet on personal device - Typically used in P2P exchanges	Attacker uses unhosted wallets to quickly and covertly transfer large sums of money	MSB: N (if used for personal purchases without third-party authorization) Rule proposed in Dec. 2020 would create specific rules for banks and MSBs involved in unhosted wallets transactions; scheduled for Sept. 2022 if FinCEN follows through
Digital Forensic Incident Response (DFIR) Firm	- Assists victims with responding to cyber-attacks - May facilitate ransom payments to perpetrators	DFIR firm handles the conversion of client's real currency to CVC and transfers CVC to perpetrator's designated account	MSB: Y (must receive and transmit value) (integral exemption may apply)
Over-the-counter (OTC) Desk	- Engages in purchase and sale of CVC on behalf of party without middleman - Enables transfer of large CVC amounts with added anonymity	Victim uses OTC platform to exchange significant sums of real currency for CVC to pay ransom or attacker uses noncompliant OTC platform to launder illicit proceeds	MSB: Y
Virtual Currency Kiosk / ATM	- Standalone machine in retail stores - Used by owner to accept fiat from a customer and transmit the same value in CVC (or vice versa)	Attacker uses kiosk known to have weak customer identification standards or a noncompliant kiosk to cash out illicit funds	MSB: Y (kiosk owner qualifies; not required to report kiosk's location or specific kiosks)
Transmitter of Anonymity-enhanced CVC (AEC)	Transmits: a) CVC payment structured to conceal public information or b) CVC specifically engineered to prevent tracing	Attacker demands payment in Monero	MSB: Y
Mixer / Tumbler	Provides CVC anonymizing services and are in the business of transmitting money	Attacker uses service to launder illicit funds	MSB: Y (if transacting CVC exchanges)

Foreign-based MSB	Conducts business within the U.S. and likely does not have a U.S. location	Attacker uses MSB located in foreign country with little or no AML requirements to retrieve ransom from U.S.-based victim	MSB: Y
Darknet Marketplace	Marketplaces that facilitate CVC transactions	Facilitates ransomware purchase in CVC	MSB: Y

The following provides examples of scenarios where existing BSA regulations enable financial regulators and law enforcement to have visibility into a ransomware attack, in order of likelihood. These scenarios focus on the application of the BSA regulations to ransomware attacks and do not take into account an attack being reported in public sources, an attack being made public through litigation, state incident or breach reporting with public disclosures, law enforcement authorities to investigate and identify cyber-crimes, national security capabilities to identify foreign threats, or other regulatory regimes where victims are required to report cybersecurity incidents, including ransomware attacks.[67]

- **Most likely**. A ransom payment transaction of more than $2,000 is made and at least one entity involved in the transaction is regulated pursuant to the BSA. The regulated entity chooses to comply with FinCEN regulations. The entity correctly identifies the transaction as suspicious and files a SAR.[68]

- **Less likely**. A ransom payment transaction of more than $2,000 is made. The mode of transfer used to facilitate the transaction either is not regulated by the BSA or the counterparties and/or regulated entities choose not to comply with anti-money laundering regulations. The likelihood also decreases if the accounts used throughout the ransom payment process are primarily unhosted or a regulated entity fails to identify suspicious transactions. In this case, law enforcement or regulators may not become aware of the ransomware attack or ransom payment.

- **Least likely**. No ransom payment transaction occurs or a ransom payment transaction totaling less than $2,000 is made. The likelihood that law enforcement or regulators will become aware of the attack is highly unlikely based solely on BSA regulations.

[67] Different critical infrastructure sectors require the reporting of cybersecurity incidents at various thresholds, as does the SEC for publicly traded companies. *E.g.*, Transportation Security Administration, *Security Directive: Enhancing Pipeline Cybersecurity* (Security Directive Pipeline-2021-01) (May 28, 2021) (expiring on May 28, 2022) and Department of Homeland Security, *Ratification of Security Directive*, 86 Fed. Reg. 38209 (July. 20, 2021) (ratification of directive) and 17 CFR § 229, 249 (requiring public companies to report material cybersecurity risks and incidents that trigger disclosure obligations).

[68] *See* Financial Crimes Enforcement Network, *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments* (FIN-2020-A006) (Oct. 1, 2020) (providing a list of ransomware-related financial red flag indicators to assist financial institutions in detecting suspicious transactions associated with ransomware attacks).

4. U.S. Sanctions Policy

Ransomware victims (or agents working on their behalf) that decide to make a ransom payment in cryptocurrency must comply with U.S. sanctions laws and regulations.[69] The Department of Treasury's Office of Foreign Assets Control (OFAC) generally prohibits U.S. persons from engaging in business with individuals and entities on the agency's Specially Designated Nationals and Blocked Persons List (SDN List). Additionally, in most sanctions programs, any transaction, including by a non-U.S. person, that causes a U.S. person to violate the sanctions prohibitions, is also prohibited. Accordingly, parties must screen cryptocurrency transactions against OFAC's SDN list and undertake appropriate steps to prevent the transfer of CVC to sanctioned persons or jurisdictions.[70]

On September 21, 2021, OFAC issued an updated advisory to highlight the sanctions risks associated with ransomware payments and the proactive steps companies that assist victims of ransomware can take to mitigate such risks.[71] The guidance emphasizes that a person subject to U.S. jurisdiction may be held liable even if they did not have reason to know that the transaction was prohibited.[72]

D. Compliance

Due to the level of real or perceived regulatory and law enforcement scrutiny associated with compliant, regulated financial institutions, criminals frequently opt to enlist the services of financial institutions that do not conduct any meaningful anti-money laundering checks.[73] This continues to be the case in the cryptocurrency space. In particular, the ever-increasing demand for criminals to convert or cash out their illicitly acquired cryptocurrency – especially in the context of ransomware payments – has resulted in the rise of a host of exchanges, OTC brokers, unlicensed MSBs, and professional laundering platforms that conduct little to no inquiries into transactions or transactional counterparties and therefore are criminal in design.[74]

In an interview with Committee staff, Kevin O'Connor, Chief of Virtual Assets and Emerging Technology Section at FinCEN, stressed that the key to addressing the use of cryptocurrency in money laundering is ensuring compliance with BSA requirements for regulated entities. O'Connor told the Committee,

[69] *See* Department of Treasury, Questions on Virtual Currency (accessed May 16, 2022) (https://home.treasury.gov/policy-issues/financial-sanctions/faqs/560); Office of Foreign Assets Control, *Sanctions Compliance Guidance for the Virtual Currency Industry* (Oct. 2021) (https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf).

[70] Financial Crimes Enforcement Network, *Advisory on Illicit Activity Involving Convertible Virtual Currency* (FIN-2019-A003) (May 9, 2019).

[71] Department of Treasury, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Sep. 21, 2021) (home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf).

[72] *Id.*

[73] Email from United States Secret Service, Criminal Investigative Division, to Senate Committee on Homeland Security and Governmental Affairs (Apr. 14, 2022).

[74] *Id.*

> I think that is one of the reasons it is important to ensure that financial institutions, like virtual asset service providers, comply with the BSA because they are required to verify customer identity and maintain records and information. If financial institutions do not comply with these requirements it will make identifying illicit activity and disrupting bad actors more difficult. When you start looking at decentralized finance, you have to ask how U.S. law enforcement and regulators are going to collect and obtain the same information under the existing regulatory scheme.[75]

O'Connor highlighted compliance concerns with respect to peer-to-peer transactions, foreign-located MSBs, and professional money laundering services, stating that,

> Three examples where we see a greater degree of noncompliance are individual Peer-to-Peer exchangers, foreign-located MSBs, and cryptocurrency mixing services. FinCEN has observed that individual Peer-to-Peer exchangers are less likely to be registered with FinCEN and less likely to meet recordkeeping and reporting requirements under the BSA. We also see noncompliance with foreign-located MSBs that do business in whole or substantial part in the United States. FinCEN has been clear that these financial institutions have obligations under the BSA and its implementing regulations. For example, FinCEN—in coordination with law enforcement—took action against BTC-e, a Russia-based virtual asset service provider that did business in the U.S. and was cashing out 95 percent of ransomware proceeds at the time according to open source reporting. With respect to professional money laundering services like mixers and tumblers, FinCEN's enforcement action against the mixing service Helix highlighted the existing requirements currently imposed on these types of entities as financial institutions under the BSA. The good news is that, overall, we are seeing greater compliance by virtual asset service providers and as a result, more suspicious activity reports being filed with FinCEN.[76]

Similarly, senior staff at SEC's Strategic Hub for Innovation and Financial Technology (FinHub), told the Committee that Bitcoin markets will typically register with FinCEN and states for anti-money laundering purposes. However, many secondary trading platforms are not in compliance.[77] When a business fails to register with the proper regulatory authority, the SEC

[75] FinCEN O'Connor Interview.

[76] *Id. See also* Financial Crimes Enforcement Network, *In Matter of: BTC-e a/k/a Canton Business Corporation and Alexander Vinnik Citation* (No. 2017-03) (July 26, 2017) (assessment of Civil Money Penalty); Catalin Cimpanu, *95% of All Ransomware Payments Were Cashed out via BTC-e Platform*, Bleeping Computer (July 27, 2017) (https://www.bleepingcomputer.com/news/security/95-percent-of-all-ransomware-payments-were-cashed-out-via-btc-e-platform/); Financial Crimes Enforcement Network, *In the Matter of: Larry Dean Harmon d/b/a Helix* (No. 2020-2).

[77] Strategic Hub for Innovation and Financial Technology, Securities and Exchange Commission, Interview with Senate Committee on Homeland Security and Governmental Affairs (Sept. 9, 2021).

interviewee emphasized that there is a "huge gap in oversight."[78] In terms of anti-money laundering regulation and enforcement, the interviewee further stated, under these circumstances "the most serious issues are no recordkeeping and reporting" which means that "sometimes [it's impossible to] figure out who is running the platform."[79] This concern is particularly growing as transactions move into the decentralized financial (DeFi) space, an emerging financial technology that builds upon and expands the decentralized nature of Bitcoin and its blockchain.[80]

Cryptocurrencies' global nature, decentralized structure, speed of payment transfers and irreversibility, as well as opportunities for enhanced privacy and anonymity can be used in multiple ways by threat actors to facilitate non-compliance. According to FinCEN, some CVCs "appear to be designed with the express purpose of circumventing anti-money laundering/countering the financing of terrorism controls."[81] In other cases, unregistered entities may misrepresent the nature of their business to conceal their money transmission activity and avoid compliance.[82] As described by FinCEN above, many foreign-located MSBs that are subject to the BSA fail to adhere to anti-money laundering requirements and frequently facilitate payments in and out of the United States for illicit actors.[83] OFAC has also taken action against certain individuals for violating OFAC regulations and exchanging cryptocurrencies into traditional currency on behalf of ransomware actors.[84]

E. Recent Ransomware Attacks

In recent years, ransomware attack victims have increasingly targeted critical infrastructure, including hospitals, school systems, local, state, and federal government agencies, as well as major utilities including the water and energy sector. In 2021, ransomware attacks impacted at least "2,323 local governments, schools and healthcare providers" in the United States.[85] As detailed below, this number likely drastically underestimates the actual number of

[78] *Id.*

[79] *Id.*

[80] *Id.*

[81] Financial Crimes Enforcement Network, *Advisory on Illicit Activity Involving Convertible Virtual Currency* (FIN-2019-A003) (May 9, 2019).

[82] *Id.*

[83] *See In the matter of BTC-E a/k/a Canton Business Corporation and Alexander Vinnik*, Financial Crimes Enforcement Network (2017-03) (July 26, 2017). In January 2017, FinCEN assessed civil money penalties against BTC-e (a.k.a. Canton Business Corporation), a foreign-located money transmitter conducting business in the United States, and its alleged owner and operator, Alexander Vinnik, for failure to comply with anti-money laundering regulations. The MSB "attracted and maintained a customer base that consisted largely of criminals who desired to conceal proceeds from crimes such as ransomware." *Id.*

[84] Department of Treasury, *Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses* (Nov. 28, 2018) (home.treasury.gov/news/press-releases/sm556). On November 28, 2018, OFAC designated two Iranian individuals on the SDN list for exploiting illicit finance vulnerabilities in the cyber space and weak anti-money laundering controls. The individuals assisted with the exchange of bitcoin ransom payments into Iranian rial on behalf of Iranian ransomware attackers. *Id.*

[85] Emsisoft Malware Lab, *The State of Ransomware in the US: Report and Statistics 2021*, Emsisoft (blog) (Jan. 18, 2022) (blog.emsisoft.com/en/40813/the-state-of-ransomware-in-the-us-report-and-statistics-2021/).

attacks.[86] Victims also included police departments and manufacturing facilities, among many others.[87]

Ransomware attacks may generate significant losses and damages for victims by causing widespread system outage, economic loss, and reputational damage. Ransomware attackers have increasingly targeted supply chains, including those within critical infrastructure. In some cases, the attacks resulted in supply chain paralysis, causing collateral damage to businesses and customers and creating significant national security risks. Recent attacks include:

- **Education Sector**: In 2020, there were 50 documented instances of publicly reported ransomware attacks against U.S. public K-12 school districts across 25 different states.[88] Certain attackers took sensitive data, such as personal data of students and educators, and threatened to release the data if their ransom demands were not met. The attackers exposed personal information of at least 560,000 students and 56,000 staff in seven school districts. Reports claim that certain extortion demands exceeded $1 million.[89] Fifteen school districts across 13 states had closures and class cancellations as a result of ransomware attacks, a figure that was three times as high as in 2019.[90]

- **Health and Public Health Sector**: In 2021, malign actors targeted at least 68 healthcare providers including multiple hospitals and multi-hospital health systems. The impacted organizations operated a total of 1,203 sites.[91] These attacks can significantly impact patient care, such as preventing use of electronic health records, preventing staff from knowing which patients were scheduled for appointments, delaying surgeries, or forcing cancer patients to go elsewhere for radiation treatment.[92]

[86] Emsisoft Malware Lab, *The State of Ransomware in the US: Report and Statistics 2021*, Emsisoft (Blog) (Jan. 18, 2022) (blog.emsisoft.com/en/40813/the-state-of-ransomware-in-the-us-report-and-statistics-2021/). The estimated attacks "do not take into account attacks on third party service and solution providers that impacted the public sector," among other attacks. *Id.*; *see also* Tara Seals, *Kronos Ransomware Outage Drives Widespread Payroll Chaos*, threatpost (blog) (Dec. 13, 2021) (threatpost.com/kronos-ransomware-outage-payroll-chaos/176984/).

[87] Senate Committee on the Judiciary, Testimony Submitted for the Record of Executive Assistant Director for Cybersecurity Eric Goldstein, Cybersecurity and Infrastructnre Agency, *Hearing on America Under Cyber Siege: Preventing and Responding to Ransomware Attacks*, 117th Cong. (July 27, 2021) (S. Hrg. 117-XX).

[88] Douglas A. Levin, *The State of K-12 Cybersecurity: 2020 Year in Review*, K-12 Cybersecurity Resource Center and the K12 Security Information Exchange (Mar. 10, 2021) (k12cybersecure.com/wp-content/uploads/2021/03/StateofK12Cybersecurity-2020.pdf).

[89] *Id.*

[90] *Id.*

[91] Emsisoft Malware Lab, *The State of Ransomware in the US: Report and Statistics 2021*, Emsisoft (blog) (Jan. 18, 2022) (blog.emsisoft.com/en/40813/the-state-of-ransomware-in-the-us-report-and-statistics-2021/); *see also* HHS Cybersecurity Program, *Ransomware Trends 2021* (June 3, 2021) (www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf).

[92] Stacy Weiner, *The growing threat of ransomware attacks on hospitals*, Association of American Medical Colleges (July 20, 2021) (https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals).

- **Colonial Pipeline**: On May 7, 2021, Colonial Pipeline, which supplies close to half of all fuel consumed on the East Coast, including gasoline, diesel, and jet fuel, was the victim of a ransomware attack that prompted the operator to shut the pipeline down for five days.[93] Colonial Pipeline paid a ransom of 75 bitcoin (about $4.4 million) to obtain a decryption key from the hackers which was expected to help restore access to its systems. However, the decryption tool was exceedingly slow, forcing the company to rely on its business continuity planning tools to bring back operational capacity. It is believed that the attackers also threatened to release 100 gigabytes of stolen data had the ransom not been paid.[94] On June 7, 2021, DOJ, in collaboration with private industry, retrieved 63.7 bitcoins of the original ransom payment, approximately $2.3 million.[95]

- **Kaseya Virtual System Administrator ("Kaseya VSA")**: On July 2, 2021, a sophisticated supply chain ransomware attack leveraged a vulnerability in Kaseya VSA software, which is used by managed IT service providers with a large amount of small- to medium-sized businesses. Attackers exploited a vulnerability in the VSA software to distribute malicious updates containing ransomware to customers, resulting in service outages for an estimated 800 to 1,500 companies. As publicly reported, Kaseya obtained a decryption key from the FBI that successfully recovered access to files that were encrypted during the ransomware attack.[96] The company did not pay the demanded $70 million ransom.

[93] Sara Morrison, *How a major oil pipeline got held for ransom*, Vox Recode (June 8, 2021) (www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices). Colonial Pipeline was concerned that the ransomware attackers might have obtained information allowing for future attacks to be launched against vulnerable parts of the pipeline. The closures were aimed at preventing the spread of ransomware to other parts of the systems. *Id.*

[94] *Hackers Breached Colonial Pipeline Using Compromised* Password, Bloomberg (June 4, 2021) (www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password).

[95] Sara Morrison, *How a major oil pipeline got held for ransom*, Vox Recode (June 8, 2021) (www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices); *Hackers Breached Colonial Pipeline Using Compromised* Password, Bloomberg (June 4, 2021) (www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password); Department of Justice, *Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside* (June 7, 2021) (www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside).

[96] The FBI had obtained a decryption key to restore access to the victims' locked computers; however, the agency waited three weeks prior to providing the key to Kaseya. Certain analysts estimate that the victims, which included schools, hospitals and a small town in Maryland, could have saved millions of dollars in recovery costs with earlier access to the decryption key. According to public reports, the FBI withheld the key, with the agreement of other federal agencies, because it was planning to carry out an operation to disrupt the hackers, a group known as REvil, and the bureau did not want to tip them off. *FBI had a key to help Kaseya ransomware victims but delayed using* it, Washington Post (Sep. 21, 2021) (www.washingtonpost.com/politics/2021/09/21/fbi-had-key-help-kaseya-ransomware-victims-delayed-using-it/). *See also* Department of Justice, *Ukrainian Arrested and Charged with Ransomware Attack on Kaseya* (Nov. 8, 2021) (www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya) and Department of Justice, *Sodinokibi/REvil Ransomware Defendant Extradited to United States and Arraigned in Texas* (Mar. 9, 2022) (www.justice.gov/opa/pr/sodinokibirevil-ransomware-defendant-extradited-united-states-and-arraigned-texas).

Ransomware actors reap astounding profits from victims' losses. Chainalysis, a cryptocurrency analysis contractor for the U.S. government by spending, reports that in 2020, malign actors received at least $692 million in cryptocurrency extorted in ransomware attacks, up from $152 million in 2019.[97] According to DigitalMint, a company that facilitates acquisition of cryptocurrency on behalf of ransomware victims to resolve ransom demands, such figures are likely understated. DigitalMint estimates that the total amount of cryptocurrency ransomware payments likely reached closer to $1 billion in 2020.[98] According to one estimate, the average ransomware payment size in 2021 reached $118,000, up from $88,000 in 2020 and $25,000 in 2019.[99] At least 140 ransomware families received payments from victims in 2021—a new all-time high.[100]

In addition, victims' losses often include costs associated with business interruption, remediation, and rebuilding. In addition, organizations can face exposure to reliant third-party claims "if their computer systems remain inoperable or their data is lost."[101] Victims may also be subject to significant reputational damage. In interviews with Committee staff, both the private sector and law enforcement reiterated the severe threat ransomware attacks can create for small to medium-sized businesses stating that "one ransomware attack may be enough to cause small-to-medium sized companies to go out of business."[102]

Ransomware actors are increasingly highly adept at using more sophisticated methods shifting tactics to avoid detection. Available data has shown that the threat of ransomware attacks is growing.[103] The World Economic Forum found that ransomware attacks increased by

[97] *The 2022 Crypto Crime Report*; Danny Nelson, *Inside Chainalysis' Multimillion-Dollar Relationship With the US Government*, CoinDesk (Feb. 10, 2020) (www.coindesk.com/business/2020/02/10/inside-chainalysis-multimillion-dollar-relationship-with-the-us-government/). By 2019, Chainalysis had government contracts with ten federal agencies, departments and bureaus including CFTC, U.S. Drug Enforcement Agency (DEA), FBI, U.S. Immigration and Customs Enforcement (ICE), IRS, SEC, and the Transportation Security Administration (TSA), among other agencies. More recently, in 2021, Chainalysis held 21 contracts with six different agencies, including for software licenses, training, and blockchain analysis. USA Spending, Spending by Prime Award (accessed May 2, 2022) (www.usaspending.gov/search/?hash=89319dae3b34df861a7e06dc84dc8d60).

[98] MacKenzie Sigalos, *When ransomware strikes, this company helps victims make bitcoin payments*, CNBC (June 10, 2021) (www.cnbc.com/2021/06/10/digitalmint-helps-ransomware-victims-make-bitcoin-payments.html#:~:text=Since%20January%202020%2C%20DigitalMint%20says,a%20median%20payment%20of%20%24800%2C000).

[99] *The 2022 Crypto Crime Report*. Estimates of average ransom payments vary by source. For instance, Palo Alto reported that the average ransomware payment was $312,000 in 2020 and had reached $850,000 in the first quarter of 2021. John Davis, *Palo Alto Networks Leads Efforts to Combat Ransomware*, paloalto networks (blog) (May 14, 2021) (www.paloaltonetworks.com/blog/2021/05/policy-rtf-combating-ransomware/?utm_source=ransomware.org&utm_medium=link).

[100] *The 2022 Crypto Crime Report*.

[101] Oliver Sepulveda, *Third-Party Liability for Ransomware Attacks, Are You Covered?*, Daily Business Review (Dec. 2, 2020) (https://www.shutts.com/news-Third-Party-Liability-for-Ransomware-Attacks-Are-You-Covered).

[102] DOJ Letter. *See also* Minder Interview.

[103] *See* Cybersecurity and Infrastructure Security Agency, *2021 Trends Show Increased Globalized Threat of Ransomware* (AA22-040A) (Feb. 9, 2022) (www.cisa.gov/uscert/ncas/alerts/aa22-040a).

435 percent in 2020 and "are outpacing societies' ability to effectively prevent or respond to them."[104]

In communications with Committee staff, DOJ confirmed this threat. Whereas previously ransomware actors would primarily conduct large scale random attacks against consumers, more recently, certain threat actors have conducted targeted, high-impact attacks against businesses. According to DOJ, attackers used to primarily "conduct a "Spray and Pray" attack, in which they would send a spam link to multiple recipients," and then "the victim would click on the link, which installed malware onto the victim's machine."[105] As of recently, "ransomware attacks are more targeted, with attackers specifically researching victims, determining how to enter specific systems, and assessing what they will do once they gain access to the victim's system."[106] Attackers now also increasingly use the "tactic of not only encrypting a victim's only copy of information but also exfiltrating sensitive data from victims and threatening to release that information to the public if a ransom is not paid."[107] This technique is called a double extortion attack.[108]

Similarly, since 2020, cybercriminals have shown a growing preference for Monero, a form of cryptocurrency that grants more privacy than Bitcoin and claims to be untraceable.[109] Cybersecurity companies which assist clients with detection, mitigation, and prevention of cybersecurity risks as well as ransomware incident response firms, such as Coveware and LMG Security, have also seen an increase in ransom demands made in Monero, or other privacy coins.[110] With respect to the federal government, the IRS has had to develop new partnerships with private companies to attempt to develop a tool or solution for tracing Monero transactions.[111] In conversations with Committee staff, regulators expressed concern over the use of privacy coins, noting that there is a "substantial difference between more transparent cryptocurrency and more opaque transactions."[112] Law enforcement and regulators face issues

[104] World Economic Forum, *The Global Risks Report 2022* (2022) (www.weforum.org/reports/global-risks-report-2022).

[105] DOJ Letter.

[106] *Id.*

[107] *Id.*

[108] Janus Agcaoili, Miguel Ang, Earle Earnshaw, et. al., *Ransomware Double Extortion and Beyond: REvil, Clop, and Conti*, Trend Micro (June 15, 2021) (https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti).

[109] Andrew Hayward, *IRS Dishes Out $1.25 Million for Data Firms to Crack Monero*, Decrypt (Sep. 30, 2020) (decrypt.co/43451/irs-1-million-contracts-data-firms-crack-monero).

[110] Siegel Interview; Sherri Davidoff, Chief Executive Officer, LMG Security, Interview with Senate Committee on Homeland Security and Governmental Affairs (Nov. 5, 2021) (hereinafter "Davidoff Interview"). LMG Security noted that while cyber criminals prefer privacy coins, ransom payments are seldom, if ever, made in privacy coins. Rather, cyber criminals may subsequently exchange a ransom paid in bitcoin to a privacy coin via a P2P exchange in the hopes of preventing the payment from being traced via the bitcoin public ledger. Davidoff Interview.

[111] Andrew Hayward, *IRS Dishes Out $1.25 Million for Data Firms to Crack Monero*, Decrypt (Sep. 30, 2020) (decrypt.co/43451/irs-1-million-contracts-data-firms-crack-monero).

[112] FinCEN O'Connor Interview.

concerning cryptocurrency "with anonymity built into them" as it "becomes increasingly difficult to trace" transactions involving such virtual currencies.[113]

Further, ransomware actors are continuously testing new methods of attack that have the potential to increase the ransomware threat and maximize profits.[114] For instance, in November 2021, FBI warned private industry that ransomware actors are targeting firms involved in time-sensitive financial events, such as mergers and acquisitions.[115] The FBI determined that ransomware attackers research publicly available information such as a victim's stock valuation, as well as material nonpublic information, which they threaten to disclose if victims do not pay a ransom quickly.[116] One ransomware group that is known for experimenting with novel tactics encouraged stock traders to contact the threat actor in order to obtain insider information so that "they can short sell [the ransomware victim's] stock before any data is leaked and the news goes public."[117]

F. National Security Threat

1. Professionalization of Ransomware Actors and the Rise of Digital Black Markets

According to cybersecurity authorities in the United States, Australia, and the United Kingdom, many ransomware attacks are executed by well-organized groups, with the market continually becoming more professionalized.[118] Jeremy Sheridan, Assistant Director of the Office of Investigations at Secret Service, testified before Congress in July 2021 that,

> [t]oday's ransomware gangs employ a vast array of specialists, from malware developers to human resources departments to public relations teams. They

[113] *Id.*

[114] For instance, since the summer of 2021, certain ransomware gangs appear to have been recruiting insiders, *i.e.*, rogue employees, to help them gain corporate network access in return for a significant fee. *See* Bill Toulas, *Ransomware gangs increase efforts to enlist insiders for attacks*, BleepingComputer (Jan. 24, 2022) (www.bleepingcomputer.com/news/security/ransomware-gangs-increase-efforts-to-enlist-insiders-for-attacks/).

[115] Federal Bureau of Investigation, *Ransomware Actors Use Significant Financial Events and Stock Valuation to Facilitate Targeting and Extortion of Victims* (20211101-001) (Nov. 1, 2021) (www.ic3.gov/Media/News/2021/211101.pdf). *See also Ransomware Attackers Begin to Eye Midmarket Acquisition Targets*, Wall Street Journal (Mar. 1, 2022) (www.wsj.com/amp/articles/ransomware-attackers-begin-to-eye-midmarket-acquisition-targets-11646130601) (suggesting a correlation between ransomware attacks and merger and acquisition deals).

[116] Federal Bureau of Investigation, *Ransomware Actors Use Significant Financial Events and Stock Valuation to Facilitate Targeting and Extortion of Victims* (20211101-001) (Nov. 1, 2021) (www.ic3.gov/Media/News/2021/211101.pdf).

[117] Bradley Barth, *Ransomware gang offers traders inside scoop on attack victims so they can short sell their stocks*, SC Media (Apr. 23, 2021) (www.scmagazine.com/news/security-news/ransomware/ransomware-gang-offers-traders-inside-scoop-on-attack-victims-so-they-can-short-sell-their-stocks).

[118] Cybersecurity and Infrastructure Security Agency, *2021 Trends Show Increased Globalized Threat of Ransomware* (AA22-040A) (Feb. 9, 2022) (www.cisa.gov/uscert/ncas/alerts/aa22-040a).

> meticulously gather information on victim organizations and set extortion prices based on the information they collect.[119]

Ransomware actors also employ "independent services to negotiate payments, assist victims with making payments, and arbitrate payment disputes between themselves and other cyber criminals."[120] In addition, facilitated by the ease of cryptocurrency, the proliferation of ransomware contributed to the growth of an online black market where novice threat actors can access tools needed to conduct a ransomware attack.

The development of Ransomware-as-a-Service (RaaS) over the last decade has been a key factor in facilitating the professionalization of ransomware attackers. RaaS "is a business model between ransomware operators and affiliates in which affiliates pay to launch ransomware attacks developed by operators." [121] Ransomware operators typically provide affiliates with technology and support for ransomware attacks in exchange for a fee and/or a cut of the ransom proceeds depending on the revenue model.[122] Ransomware operators sometimes even develop RaaS kits, which "may include 24/7 support, bundled offers, user reviews, forums," and even assist affiliates "to develop their own ransomware variant."[123] As a result of its success, the RaaS market is competitive and incorporates traditional business practices, such as marketing campaigns, white papers, and a social media presence. Attackers can be "highly professionalized, leveraging expert third-party partnerships, an internal division of labor that mirrors the way legitimate businesses are organized, and economies of scale to grow their margins."[124] RaaS has significantly lowered the technical barrier of entry into the ransomware economy.

Digital black markets continue to expand in large part due to the consistently high payments in cryptocurrency from ransom victims combined with the low costs and developed infrastructure and networks that facilitate ransomware attacks. Notably, costs for ransomware tools range from $5 to more than $100 depending on the ransomware family, or may instead be based on a cut of proceeds.[125] Public information on profits from reported ransomware attacks

[119] Senate Committee on the Judiciary, Testimony Submitted for the Record of Jeremy Sheridan, Office of Investigations, United States Secret Service, U.S. Department of Homeland Security, *Hearing on Responding to Ransomware*, 117th (July 27, 2021) (S. Hrg. 117-XX) (www.secretservice.gov/sites/default/files/reports/2021-07/USSS-Testimony-AD-Jeremy-Sheridan-7-27-2021.pdf).

[120] Cybersecurity and Infrastructure Security Agency, *2021 Trends Show Increased Globalized Threat of Ransomware* (AA22-040A) (Feb. 9, 2022) (www.cisa.gov/uscert/ncas/alerts/aa22-040a).

[121] Kurt Baker, *Ransomware As A Service (RAAS) Explained*, CrowdStrike (Feb. 7, 2022) (www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/).

[122] *Id.*

[123] *Id.*

[124] Horizon2.ai, *The ransomware threat landscape has changed: here's how defenders must adapt*, Cybersecurity Dive (Dec. 6, 2021) (https://www.cybersecuritydive.com/spons/the-ransomware-threat-landscape-has-changed-heres-how-defenders-must-adap/610815/).

[125] Anthony M. Freed, *What is the Dark Web Ransomware Marketplace?*, Cybereason (Oct. 19, 2021) (www.cybereason.com/blog/what-is-the-dark-web-ransomware-marketplace). *See also* Mayra Rosario Fuentes,

suggest that certain ransomware groups have amassed budgets that are likely comparable with the budgets of nation-state organizations.[126] These criminal organizations use illicit gains to expand operations, specialize, and improve products, similar to legitimate businesses. More effective ransomware reinforces the organizations' business model and attracts more bad actors. It has also resulted in attacks that are less expensive and easier to conduct.[127]

2. Money Laundering Facilitation

After receiving ransom payments from victims, certain illicit actors will take advantage of the cryptocurrency payment structure to launder their profits.[128] Traditionally, money laundering follows three steps: 1) placement, 2) layering, and 3) integration.[129] Within the context of cryptocurrency, placement occurs when actors receive the ransomware payment and place it in a laundering tool; layering occurs within the laundering tool where illicit and legitimate funds are combined; and integration occurs when the funds are removed and appear to have been legally obtained.[130] Andrew Winerman, Acting Associate Director, Strategic Operations Division at FinCEN explained in conversations with Committee staff how ransomware actors make use of certain aspects of the cryptocurrency payment structure to launder ransom payments,

> [ransomware] [a]ttackers will try and launder what they obtain, they will receive funds in unhosted wallets and then they go to town with every technique to try and cash it out at a foreign exchange that isn't tracking.[131]

Specific laundering tools unique to the cryptocurrency ecosystem render it more difficult for authorities to trace payments back to the ransomware actors under investigation.[132] These laundering tools include mixers, also known as tumblers. In the most basic terms, these services attempt to combine cryptocurrency from a variety of sources, including ransom payments with transactions involving unrelated parties and / or "clean" cryptocurrency in order to obscure the

Shifts in Underground Markets, Past, Present, and Future, TrendMicro (2020) (documents.trendmicro.com/assets/white_papers/wp-shifts-in-the-underground.pdf).

[126] Microsoft, *Microsoft Digital Defense Report* (Oct. 2021) (query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi?id=101738).

[127] *Id.*

[128] Lavender Baj, *What the Heck Is a Crypto Tumbler And Is It Even Legal?*, Gizmodo (June 28, 2021) (www.gizmodo.com.au/2021/06/cryptocurrency-tumblers-mixers-explained/).

[129] Financial Crimes Enforcement Network, History of Anti-Money Laundering Laws (accessed on Mar. 16, 2022) (www.fincen.gov/history-anti-money-laundering-laws#:~:text=Money%20laundering%20is%20the%20process,into%20the%20legitimate%20financial%20system).

[130] *Bitcoin Money Laundering: How Criminals Use Crypto*, Elliptic (blog) (Sept. 18, 2019) (www.elliptic.co/blog/bitcoin-money-laundering).

[131] Andrew Winerman, Acting Associate Director, Strategic Operations Division, Financial Crimes Enforcement Network, Interview with Senate Committee on Homeland Security and Governmental Affairs (July 20, 2021).

[132] Email from United States Secret Service, Criminal Investigative Division, to Senate Committee on Homeland Security and Governmental Affairs (Apr. 14, 2022).

source and intended destination of a given transactional counterparty (individual or institution).[133] Such techniques pose serious risks and threats when used for illicit activity as they aim to render transactions increasingly anonymous.[134] Similarly, the lucrative nature of ransomware has resulted in an increased demand by criminals for mixing / tumbling services.[135]

According to DOJ, a major concern with the international nature of cryptocurrency is a lack of compliance with anti-money laundering laws across jurisdictions.[136] Some international jurisdictions even have a "complete absence of such regulation and supervision."[137] Inconsistent application of these laws leaves gaps in regulation and enforcement. This inconsistency also negatively impacts law enforcement's "ability to investigate, prosecute, and prevent criminal activity involving or facilitated by" cryptocurrency.[138]

Mr. Winerman from FinCEN explained in conversations with Committee staff the growing anti-money laundering threat created by jurisdictional arbitrage,

> [w] hile we think regulations are in a good place, there is clearly a lot of ransomware activity going on with cashing out in foreign exchanges in jurisdictions that aren't doing a great job at regulating.[139]

He further stated, "[i]n [the] future…improved ways to launder money and decentralized finance" would enhance the threat created by ransomware and cryptocurrency ransom payments.[140]

3. Russia/Ukraine Conflict

As Russia's attack on Ukraine continues, ensuring that policymakers have a comprehensive understanding of the ransomware threat is critical to defend against cyber-attacks by cybercriminals operating in or supported by the Russian government or other malign countries. On March 7, 2022, FinCEN issued an alert providing examples of red flags to assist CVC exchangers and administrators as well as other financial institutions in identifying

[133] *Id.*

[134] *Id.*

[135] *Id.*

[136] Department of Justice, *Cryptocurrency: Enforcement Framework* (Oct. 2020) (www.justice.gov/archives/ag/page/file/1326061/download).

[137] *Id.*

[138] *Id.*

[139] Andrew Winerman, Acting Associate Director, Strategic Operations Division, Financial Crimes Enforcement Network, Interview with Senate Committee on Homeland Security and Governmental Affairs (July 20, 2021).

[140] *Id.*

suspected Russian sanctions evasion activity by both state actors and oligarchs.[141] The alert warns financial institutions of the dangers posed by Russian-related ransomware campaigns, stating that the institutions may "observe attempted or completed transactions tied to CVC wallets or other CVC activity associated with sanctioned Russian, Belarusian, and other affiliated persons."[142] Further, according to public reports, one ransomware group has specifically expressed support for the Russian invasion of Ukraine and have warned of possible attacks against "enemies of the Kremlin if they respond to Russia's invasion."[143]

III. DATA COLLECTION ON RANSOMWARE ATTACKS AND PAYMENTS IS FRAGMENTED AND INCOMPLETE

U.S. laws, regulations and guidance have been issued to require, or strongly encourage, cyber incident reporting. Historically, federal agencies have had to rely on voluntarily reported information from victims and the private sector to gain a better understanding of the threat of ransomware and cryptocurrency ransom payments. For instance, in interviews with Committee staff, Bill Siegel, Chief Executive Officer (CEO) for Coveware, a ransomware incident response firm, explained that they regularly share with FBI, and other local, state, and federal law enforcement, aggregated data obtained from their clients' cases.[144] To address the current lack of comprehensive information regarding the breadth and depth of the ransomware threat, Chairman Peters and Ranking Member Portman introduced the Cyber Incident Reporting Act of 2021, which passed the Senate as part of the Strengthening American Cybersecurity Act of 2022. The incident reporting provisions of this bill recently were signed into law as the Cyber Incident Reporting for Critical Infrastructure Act of 2022 within the Consolidated Appropriations Act of 2022. The new reporting mandates for critical infrastructure in the law will begin to address this problem, however the law provides CISA time to complete a regulatory rulemaking process and therefore have not yet been implemented at the time of this report.

Private entities, among other third parties, collect most of the publicly available data in this field. These cybersecurity entities include software companies, like Microsoft; computer security companies, such as McAfee and Emsisoft; cryptocurrency analysis and blockchain data platforms, like Chainalysis; cyberinsurance companies, such as Resilience Insurance; and sector-specific organizations, like the K-12 Cybersecurity Resource Center.[145] These companies and

[141] FinCEN, *FinCEN Provides Financial Institutions with Red Flags on Potential Russian Sanctions Evasion Attempts* (Mar. 7, 2022) (www.fincen.gov/news/news-releases/fincen-provides-financial-institutions-red-flags-potential-russian-sanctions).

[142] *Id.*

[143] Christopher Bing, *Russia-based ransomware group Conti issues warning to Kremlin foes*, Reuters (Feb. 25, 2022) (www.reuters.com/technology/russia-based-ransomware-group-conti-issues-warning-kremlin-foes-2022-02-25/).

[144] Siegel Interview.

[145] Microsoft, Our company (accessed Mar. 8, 2022) (www.microsoft.com/en-us/about/company); Emsisoft, Why Emsisoft (accessed Mar. 8, 2022) (www.emsisoft.com/en/company/about/); McAFee, About McAfee (accessed Mar. 8, 2022) (www.mcafee.com/en-us/consumer-corporate/about.html); Chainalysis, What we do (accessed Mar. 8, 2022) (www.chainalysis.com/company/); Resilience Insurance, About (accessed Mar. 8, 2022) (www.resilienceinsurance.com/about/); The K-12 Cybersecurity Resource Center, About (accessed Mar. 8, 2022) (k12cybersecure.com/about/).

organizations generally rely on voluntarily reported client data or publicly available information. As such, there are significant gaps in private sector data on the threat of ransomware attacks and the extent to which cryptocurrency ransom payments fuel the ransomware economy.

A. Data Collection by U.S. Government Agencies

Although there is significant coordination between regulatory and law enforcement agencies on open ransomware cases, to date, data on ransomware attacks and cryptocurrency ransom payments is not accessible and searchable across government agencies. In discussions with the Committee, the agencies interviewed (DOJ, SEC, and FinCEN) emphasized their close collaboration with federal regulatory and international counterparts on open cases.[146]

In interviews with the Committee, one company explained that they began collecting data on ransomware trends and aggregating statistics on ransomware payments and attack vectors to fill this void.[147] Coveware's CEO told the Committee in interviews,

> [W]e were found[ed] in 2018 because we felt like this was a very large problem with very little data collected on it and that struck us as odd that there was a large problem with little firsthand data. There was no go-to centralized data out there about what happens during these attacks. It took us a couple of months, and we meandered our way into a gap in incident response services.[148]

Government agencies collect data on cyber incidents, including ransomware, under a patchwork of laws, regulations, and guidance. These efforts seek to protect homeland security and critical infrastructure, facilitate and protect law enforcement actions, and promote foreign policy goals, among other purposes, while protecting victim privacy rights.[149] For instance, pursuant to the Anti-Money Laundering Act of 2020 (AMLA), FinCEN must publish threat

[146] *See* DOJ Letter; FinCEN O'Connor Interview; Division of Enforcement, Securities and Exchange Commission, Interview with Senate Committee on Homeland Security and Governmental Affairs (Sept. 9, 2021).

[147] Siegel Interview.

[148] Siegel Interview.

[149] *See* 45 CFR 164.308(a)(6); Department of Health and Human Services, Office of Civil Rights, *Fact Sheet: Ransomware and HIPAA* (accessed Mar. 28, 2022) (www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html); Federal Bureau of Investigation, *Ransomware Victims Urged to Report Infections to Federal Law Enforcement* (Sept. 15, 2016) (www.ic3.gov/Media/Y2016/PSA160915); Department of the Treasury, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Sept. 21, 2021) (home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf).

pattern and trend information with respect to incidents of cybercrime including ransomware affecting regulated financial institutions.[150] The data is collected from SARs.

Law enforcement and certain regulatory agencies encourage victims of ransomware to report attacks. Key federal contacts for reporting ransomware attacks include:

1. CISA
    - StopRansomware.gov – This website allows victims to report ransomware attacks and presents itself as "the U.S Government's official one-stop location for resources to tackle ransomware more effectively" and offers victims the option of reporting an attack.[151]

    - CISA Incident Reporting System – The CISA Incident Reporting System provides a secure web-enabled means of voluntarily reporting computer security incidents to CISA, including ransomware attacks.[152]

    - As of July 2021, CISA, which was created in 2018 specifically to reduce risk to the nation's cyber and physical infrastructure, estimated that only about one quarter of ransomware incidents were reported.[153]

    - Pursuant to the newly-passed Cyber Incident Reporting for Critical Infrastructure Act, critical infrastructure entities, as defined through a CISA rulemaking, will have to report within 72 hours of having a reasonable belief that a substantial cyber incident (also defined in the rulemaking) has occurred, and within 24 hours of making a ransomware ransom payment.[154]

2. FBI
    - IC3.gov – IC3.gov allows victims and third parties to report any cyber-attack, including ransomware attacks.[155] This portal enables the FBI to build a narrow

[150] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, Sec. 6001-6511 (2021). *See also* Financial Crimes Enforcement Network, *Financial Trend Analysis Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021* (June 30, 2021).

[151] Cybersecurity and Infrastructure Security Agency, Stop Ransomware (accessed on Mar. 3, 2022) (StopRansomware.gov).

[152] Cybersecurity and Infrastructure Security Agency, CISA Reporting System (accessed on Mar. 3, 2022) (us-cert.cisa.gov/forms/report). *See also* Cybersecurity and Infrastructure Security Agency, Report Incidents, Phishing, Malware, or Vulnerabilities (Mar. 3, 2022) (www.cisa.gov/uscert/report).

[153] Gerrit De Vynck, *Many ransomware attacks go unreported. The FBI and Congress want to change that.*, Washington Post (July 27, 2021) (https://www.washingtonpost.com/technology/2021/07/27/fbi-congress-ransomware-laws/).

[154] Consolidated Appropriations Act of 2022, Pub. L. No. 117-103, Sec. 2242 (2022).

[155] Federal Bureau of Investigation, Internet Crime Compliance Center (accessed on Feb. 25, 2022) (IC3.gov).

data universe on ransomware attacks for further analysis and future use.[156] FBI claims that IC3 is "the central point" for internet crime reporting.[157]

- Local FBI field offices – Ransomware victims can also report ransomware incidents to local FBI field offices as opposed to IC3.gov.[158] If local FBI field offices compile victim complaints of ransomware incidents, this information does not appear to be publicly available.

Public agencies at the state level also collect limited data on cyber incidents. Generally, mandatory reporting requirements are limited to data breaches involving personally identifiable information.[159] All 50 states, as well as D.C., Puerto Rico, and the Virgin Islands, have laws addressing applicability, definitions, notice requirements, and exemptions in connection with such reporting requirements.[160] In 2021, 45 states considered legislation relating to cybersecurity and reporting requirements.[161] Three of those states, Indiana, Louisiana, and North Dakota, have passed and implemented legislation requiring public entities to report ransomware attacks.[162] Entities in states with general cyber incidents reporting legislation may also need to report ransomware attacks depending on the state's requirements.[163]

B. Artificially Low Reporting

Based on the submissions made via FBI's IC3.gov website, the agency publishes an annual "Internet Crime Report" compiling data on the number of internet crimes (including ransomware) and losses reported annually. In 2020, FBI received 791,790 cybercrime complaints, a 69 percent increase from 2019.[164] Of these, 2,474 complaints constituted

[156] DOJ Letter.

[157] Internet Crime Compliance Center, *Internet Crime Report 2020*, Federal Bureau of Investigation (2020) (www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf).

[158] *See* Federal Bureau of Investigation, *Ransomware Victims Urged to Report Infections to Federal Law Enforcement* (Sep. 15, 2016) (www.ic3.gov/Media/Y2016/PSA160915).

[159] National Conference of State Legislatures, *Security Breach Notification Laws* (Apr. 15, 2021) (www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx).

[160] *Id.*

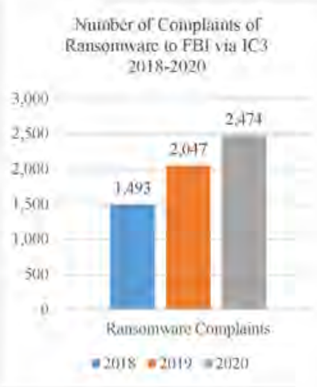
[161] *Id.*

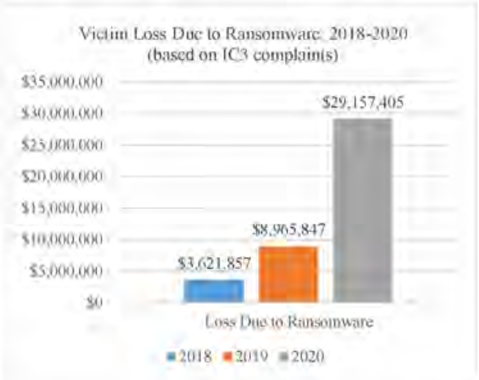
[162] National Conference of State Legislatures, *Computer Crime Statutes* (May. 4, 2022) (https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx).

[163] National Conference of State Legislatures, *Computer Crime Statutes* (May. 4, 2022) (https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx) (stating that North Carolina requires reporting of cyber incidents generally (which may include ransomware attacks).

[164] Federal Bureau of Investigation, *Internet Crime Report 2020* (Mar. 17, 2021) (https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf).

ransomware incidents with adjusted losses of over $29.1 million.[165] A three-year comparison of the number of complaints of ransomware submitted to IC3 demonstrates a 65.7 percent increase in victim count and a staggering 705 percent increase in adjusted losses.[166]





The report notes, however, that the ransomware data is "artificially low" because the data only considers attacks reported through IC3, excluding reports to FBI field offices. In addition, the information "does not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by a victim."[167] The report also notes that "in some cases, victims do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate."[168]

Security and privacy experts have noted that IC3 ransomware data is a "subset of a subset" of data.[169] Some argue that the figures are "incredibly low" and "inconsistent" due to the fact that victims will generally report an incident to their local field office.[170] The FBI's figures on ransomware may also be low due to lack of awareness on the part of victims regarding when and how ransomware incidents should be reported.[171] Despite FBI initiatives designed to

[165] Federal Bureau of Investigation, *Internet Crime Report 2020* (Mar. 17, 2021) (https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf).

[166] *Id.*

[167] Federal Bureau of Investigation, *Internet Crime Report 2020* (Mar. 17, 2021) (https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf).

[168] *Id.*

[169] Alexander Culafi, *FBI IC3 report's ransomware numbers are low*, TechTarget (Mar. 18, 2021) (www.techtarget.com/searchsecurity/news/252498133/FBI-IC3-reports-ransomware-numbers-are-low-experts-say).

[170] *Id.*

[171] Kyle Johnson and Mike O. Villegas, *Best practices for reporting ransomware attacks*, Tech Target (Mar. 2021) (www.techtarget.com/searchsecurity/answer/What-are-some-best-practices-for-reporting-ransomware-attacks).

educate potential victims regarding the reporting process, organizations may remain hesitant to voluntarily report the occurrence of an attack for a myriad of reasons including concerns regarding brand damage, regulatory oversight, civil legal actions, and loss of revenue.[172]

Further evidence of this under-reporting is that the numbers reported by FBI are drastically lower than several private sector estimates. For instance, one private sector study found that there were at least 24,770 ransomware incidents in the U.S. in 2019 and estimated their costs (including costs of downtime) at just under $10 billion.[173]

The FBI has since made improvements in its data collection process. In June 2021, the IC3 began tracking reported ransomware incidents in the critical infrastructure sector, specifically.[174] For instance, in the most recent version of the Internet Crime Report published on March 22, 2022, the FBI identified that IC3 received 649 complaints from organizations belonging to a critical infrastructure sector.[175] The report breaks down critical infrastructure into 16 different sectors.[176] Of those 16 sectors, "IC3 reporting indicated 14 sectors had at least 1 member that fell victim to a ransomware attack in 2021."[177] In addition, the FBI indicated that IC3 had received 3,729 ransomware complaints with adjusted losses of more than $49.2 million in 2021.[178] In another improvement over the 2020 annual report, the FBI also discusses the evolution of ransomware tactics and techniques and provides general recommendations for protecting computer systems against ransomware attacks.[179] Still, the agency acknowledges that the overall ransomware loss rate is "artificially low" due to the reasons described above, notably

[172] Alexander Culafi, *FBI IC3 report's ransomware numbers are low* (Mar. 18, 2021) (www.techtarget.com/searchsecurity/news/252498133/FBI-IC3-reports-ransomware-numbers-are-low-experts-say); *see* Federal Bureau of Investigation, Infragard (accessed on Feb. 22, 2022) (www.infragard.org/Application/Account/Login).

[173] Alexander Culafi, *FBI IC3 report's ransomware numbers are low*, TechTarget (Mar. 18, 2021) (www.techtarget.com/searchsecurity/news/252498133/FBI-IC3-reports-ransomware-numbers-are-low-experts-say). Emsisoft conducted a study that derives the number of reported incidents from submissions to ransomware identification service ID Ransomware. Every submission to this service represents a confirmed incident. In 2019, there was a total of 452,151 submissions. According to Emsisoft, at least 24,770 of these submissions were ransomware incidents in the U.S. Note, however, Emsisoft estimates that only approximately 25 percent of public and private sector organizations affected by ransomware use the "ID Ransomware" website. *See* Emsisoft Malware Lab, *Report: The cost of ransomware in 2020. A country-by-country analysis*, Emsisoft (blog) (Feb. 11, 2020) (blog.emsisoft.com/en/35583/report-the-cost-of-ransomware-in-2020-a-country-by-country-analysis/). *See also* Malware Hunter Team, *ID Ransomware* (access Mar. 3, 2022) (id-ransomware.malwarehunterteam.com/index.php).

[174] Federal Bureau of Investigation, *Internet Crime Report 2021* (Mar. 22, 2022) (https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf).

[175] *Id.*

[176] *Id. See also* Cybersecurity and Infrastructure Security Agency, Critical Infrastructure Sectors (accessed May 16, 2022) (https://www.cisa.gov/critical-infrastructure-sectors).

[177] Federal Bureau of Investigation, *Internet Crime Report 2021* (Mar. 22, 2022) (https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf).

[178] *Id.*

[179] Federal Bureau of Investigation, *Internet Crime Report 2021* (Mar. 22, 2022) (https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf).

lack of data from FBI field offices and insufficient data from victims on losses, among other reasons.[180]

C. Impact of Irregular Reporting on Law Enforcement Agencies and the Private Sector

DOJ emphasized that "victim reporting is essential in ransomware attack investigations. Learning about each ransomware attack helps the Department create an overall picture of the actions of the ransomware actors and protect against future attacks."[181] In discussing tracking cryptocurrency ransom payments that are being laundered, FinCEN added that "the best thing is to have the financial information, we could have more actionable data through improved reporting."[182]

Similarly, when speaking with Committee staff, Sherri Davidoff, the CEO of LMG Security, a cybersecurity consulting, research and training firm, explained that a lack of reporting requirements and incentives results in underreporting, which causes experts in this area to "not have a clear understanding of the problem and inhibits development of effective solutions."[183] Coveware has close to 100 percent of its clients proactively reporting ransomware incidents to law enforcement, oftentimes to FBI field offices.[184] However, since the agencies collect a standard subset of incident data during the initial reporting, law enforcement often needs to reconnect with the victim in order to collect further statements and evidence in the proper format necessary for investigating, securing indictments, and prosecuting cases.[185] When law enforcement attempts to re-contact the victims to gather more information, the company estimates 25 percent or less of clients engage.[186] This can make it very difficult to complete the investigation and indictment process.

With respect to reporting, instructions on both the FBI and CISA websites suggest that victims of cybercrimes need only submit one complaint to ensure that law enforcement within multiple agencies will be notified of the attack. However, these instructions lack clarity. The CEO of LMG Security told Committee staff that there is not a clear responsibility for victims to report incidents.[187] Generally, LMG Security emphasized that the process for victims who are seeking to "do the right thing" is confusing and expensive which works against U.S. national security interests.[188] Coveware's CEO, Bill Siegel, told Committee staff that, while their clients

[180] *Id.*

[181] DOJ Letter.

[182] FinCEN O'Connor Interview.

[183] Davidoff Interview (adding that the lack of detection capabilities throughout the U.S. contributes to the epidemic of cyber extortion attacks).

[184] Siegel Interview.

[185] *Id.*

[186] *Id.*

[187] Davidoff Interview.

[188] *Id.*

almost unanimously proactively share data with law enforcement, reporting is made more difficult when it is unclear which agency a victim should report to or when dealing with an inexperienced government contact. According to Coveware's CEO,

> [a ransomware victim] could contact the wrong branch of law enforcement and that could be a distraction. The right branch would know they can't take up all the company's attention when they are trying to save their business.[189]

Similarly, the majority of victims that work with GroupSense, a digital risk protection services company, regularly choose to report an incident to either CISA and/or the FBI. When reporting to law enforcement, GroupSense's CEO, Kurtis Minder, and his team provide all relevant information including cryptocurrency wallets included in ransom notes.[190] In some cases, the FBI claimed that they would return the ransom money. According to Mr. Minder however, the FBI's efforts have been unfruitful suggesting that threat actors are finding ways to move money without using a major exchange subject to FBI jurisdiction or otherwise accessible by the FBI.[191]

With more comprehensive data on ransomware attacks, ransom payments, and the role of cryptocurrency, law enforcement and CISA would be able to better track and share trends and tactics used by bad actors. Ransomware actors rarely employ novel, never-before-seen techniques. Testifying before Congress, Jeremy Sheridan, Assistant Director for the Office of Investigations at Secret Service, said "many new ransomware strains built upon those that came before them, adding layers of encryption and obfuscation, making defense and mitigation efforts far more challenging."[192]

In communications with Committee staff, DOJ confirmed that data from reported incidents can shed light on the techniques of an attack which is critical for helping identify ransomware actors, monitoring BSA compliance, and prosecuting wrongdoers. DOJ explained that "increased data on ransom payments and instructions from ransomware actors can further assist law enforcement agencies with monitoring Bank Secrecy Act compliance, prosecuting wrongdoers, and identifying potential loopholes" in anti-money laundering regulations in the cyberspace.[193] As of July 2021, DOJ had 40 different ransomware investigations and prosecutions that were open.[194] DOJ also explained, however, that existing means to gather data

[189] Siegel Interview.

[190] Minder Interview.

[191] *Id.*

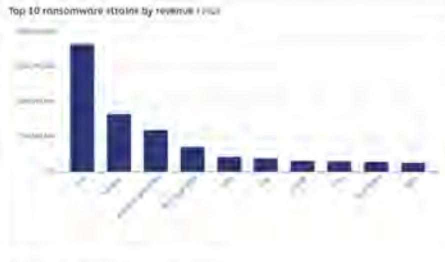
[192] Senate Committee on the Judiciary, Testimony Snbmitted for the Record of Jeremy Sheridan, Office of Investigations, United States Secret Service, U.S. Department of Homeland Security, *Hearing on Responding to Ransomware*, 117th (July 27, 2021) (S. Hrg. 117-XX) (www.secretservice.gov/sites/default/files/reports/2021-07/USSS-Testimony-AD-Jeremy-Sheridan-7-27-2021.pdf).

[193] DOJ Letter.

[194] *Id.* The 40 cases represent investigations and prosecutions being handled by the Computer Crime and Intellectual Property Section of Criminal Division at the Department of Justice alone. The cases are broken down by ransomware variant. Of the 40 cases, "each case represents more than one ransomware attack, and one case may

from certain foreign countries that host threat actors combined with the borderless nature of cryptocurrency can make it particularly difficult to capture illicit actors.

Further, reports have shown that ransomware attackers tend to rebrand themselves and launch new ransomware strains in order to evade law enforcement and continue pursuing ransom opportunities. Thus, a small number of ransomware groups appear to be behind a large number of ransomware attacks. For example, on May 19, 2022, reports identified that the Conti ransomware gang, a group that the U.S. government considers one of the most threatening, had officially terminated their operations. They were reported to now have partnered with other smaller ransomware gangs to continue conducting attacks.[195]



Source: *The 2022 Crypto Crime Report.*

Similarly, data regarding the ransomware actors' money laundering practices suggest that only a handful of cryptocurrency businesses receive funds from ransomware wallet addresses. One study found that between 2020 and 2021, 56 percent of funds sent from ransomware wallet addresses were transferred to only six cryptocurrency businesses — three large international exchanges, one high-risk exchange based in Russia, and two mixing services.[196] When speaking with Committee staff, GroupSense's CEO, Kurtis Minder, shared that ransomware actors continue to develop new tactics to avoid detection. For instance, he shared that threat actors now may move and store illicit funds on the darknet for an extended period of time before resurfacing to the clearnet to cash out. This tactic seeks to "wait out" cybersecurity companies and victims until they move on.

With more information, law enforcement will also be able to better understand ransomware actors and can alert victims when they are attacked by terrorist or criminal

involve hundreds of victims that involve every federal district." As cases proceed, in some instances, the investigative team determines that certain variants are deployed by the same individuals and the cases may be merged. *Id.*

[195] *See* Lawrence Abrams, *Conti ransomware shuts down operation, rebrands into smaller units*, BleepingComputer (May 19, 2022) (www.bleepingcomputer.com/news/security/conti-ransomware-shuts-down-operation-rebrands-into-smaller-units/) (announcing that Conti had partnered with numerous well-known ransomware operations enabling the cybercrime syndicate to "gain[…] mobility and greater evasion of law enforcement by splitting into small 'cells,' all managed by central leadership"). *See also* Sergiu Gatlan, *US offers $15 million reward for info on Conti ransomware gang*, BleepingComputer (May 7, 2022) (www.bleepingcomputer.com/news/security/us-offers-15-million-reward-for-info-on-conti-ransomware-gang/) (stating that the U.S. Department of State is offering up to $15 million for information regarding the leadership and co-conspirators of the Conti ransomware gang).

[196] *The 2022 Crypto Crime Report.*

organizations.[197] In an interview with the Committee, Bill Siegel from Coveware reiterated that "[t]here is a clear need for enhanced coordination between the government and industry, particularly as it relates to information sharing and incident reporting."[198] In his testimony before Congress in July 2021, Assistant Director Sheridan testified that,

> [t]he U.S. Government needs access to timely, actionable information. If victim companies fail to report ransomware attacks early, or if they fail to report them at all, it hinders law enforcement's ability to assist them with asset recovery or to prevent future incidents.[199]

Similarly, also testifying before Congress in July 2021, Eric Goldstein, Executive Assistant Director for CISA, stated,

> CISA must work with all possible partners to gain increased visibility into national risks. With increased visibility, we can better identify adversary activity across sectors, which allows us to produce more targeted guidance, understand the degree to which adversary activity across sectors is increasing risk, and identify particular incidents requiring a specialized CISA response team. Our partnership with [the Transportation Security Agency] to develop two Security Directives requiring reporting of cybersecurity incidents to CISA is an important step and an example of such collaboration. We look forward to working with Congress to further encourage reporting of cybersecurity incidents to the federal government in order to further enable this essential visibility.[200]

Incomplete reporting on ransomware attacks and cryptocurrency ransom payments obscures the vast disparity in victims' experiences and challenges with recovering from an attack. Aggregated and anonymized data from increased incident reporting could help inform policies regarding potential federal assistance for excessively burdened ransomware victims. Increased reporting may also shed light on the specific burdens faced by small- and medium-sized businesses, such as inability to access high cost prevention methods and the drastic economic consequences of these attacks.[201] In an interview with Committee staff, Mr. Minder from GroupSense, suggested that Congress consider providing assistance to small and medium-

[197] Siegel Interview (explaining that Coveware keeps its own, more comprehensive, list of cryptocurrency wallets associated with terrorist or criminal organizations, created from data they collect from their clients in light of perceived inadequacies with existing government data).

[198] *Id.*

[199] Senate Committee on the Judiciary, Testimony Submitted for the Record of Jeremy Sheridan, Office of Investigations, United States Secret Service, U.S. Department of Homeland Security, *Hearing on Responding to Ransomware*, 117th (July 27, 2021) (S. Hrg. 117-XX) (www.secretservice.gov/sites/default/files/reports/2021-07/USSS-Testimony-AD-Jeremy-Sheridan-7-27-2021.pdf).

[200] Senate Committee on the Judiciary, Testimony Submitted for the Record of Executive Assistant Director for Cybersecurity Eric Goldstein, Cybersecurity and Infrastructure Agency, *Hearing on America Under Cyber Siege: Preventing and Responding to Ransomware Attacks*, 117th Cong. (July 27, 2021) (S. Hrg. 117-XX).

[201] Minder Interview.

sized businesses impacted by ransomware attacks in light of the disproportionate burden on such companies.[202]

D. Evolving Federal Response to Increase Incident Reporting and Expand Available Data on Ransomware Attacks and Cryptocurrency Ransom Payments

Agencies have recently taken steps – both regulatory and law enforcement centered – that recognize the national security risk of ransomware and/or that seek to address information deficiencies in connection with such attacks. However, certain challenges have limited agencies' progress to date.

FinCEN. As described above, pursuant to the AMLA, FinCEN periodically publishes threat pattern and trend information with respect to incidents of cybercrime in financial institutions.[203] The information is derived from financial institutions' SARs, as described above. FinCEN's experience with SARs reporting demonstrates the benefit of clearer reporting incentives and intelligence sharing among relevant agencies, such as a more comprehensive threat assessment and better deployment of resources.[204] These reports also help to develop appropriate risk management strategies to identify, report, and mitigate cyber-events and cyber-enabled crime and to reveal additional patterns of suspicious behavior and identify suspects.[205]

However, the dataset is far from comprehensive due to lack of compliance and the fact that entities subject to FinCEN regulations are only required to file reports when they observe suspicious activity, among other limitations. Thus, it is highly likely that significant money laundering activity remains unreported.

OFAC. OFAC imposes sanctions on malicious cyber actors and others who "materially assist, sponsor, or provide financial, material, or technological support" for ransomware attacks.[206] In its 2020 Guidance on threats posed by ransomware attacks, OFAC warns companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and

[202] *Id.*

[203] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, Sec. 6001-6511 (2021). *See also* Financial Crimes Enforcement Network, *Financial Trend Analysis Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021* (June 30, 2021).

[204] Financial Crimes Enforcement Network, *Financial Trend Analysis Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021* (June 30, 2021).

[205] *Id.*

[206] Department of the Treasury, *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Oct. 1, 2020) aud Department of the Treasury, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Sept. 21, 2021). In 2013, for example, "a ransomware variant known as Cryptolocker was used to infect more than 234,000 computers, approximately half of which were in the United States. OFAC designated the developer of Cryptolocker, Evgeniy Mikhailovich Bogachev, in December 2016." *Id.*

incident response, that they may risk violating OFAC regulations if such transactions have a sanctions nexus, such as involvement of a sanctioned party or property.[207]

In discussions with Committee staff, however, LMG Security said that victims and third party agents face difficulties identifying which cryptocurrency wallets may be subject to U.S. sanctions. According to LMG Security, while OFAC keeps a list of sanctioned wallets, the OFAC Sanctions List Search Tool is not built to allow easy cryptocurrency address lookups, creating a barrier to victims seeking to access this information so that they can remain in compliance with OFAC sanctions.[208] LMG Security also explained that criminals routinely create brand new cryptocurrency wallets that have not previously been used, and then launder the funds, making it hard for OFAC to have a complete list of wallets associated with criminal organizations and terrorist groups.[209] Coveware, an incident response firm that assists victims with settling ransom demands, told the Committee that OFAC's list is not updated as sanctioned ransomware threat actors change their brands and tactics. Therefore, Coveware created its own list of threat actor groups.[210]

DOJ. On June 3, 2021, DOJ issued a memorandum to all federal prosecutors entitled, "Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion."[211] The DOJ guidance instructs U.S. attorney's offices across the country to coordinate ransomware investigations with the recently formed Ransomware and Digital Extortion Task Force.[212] The internal guidance states,

> [t]o ensure we can make necessary connections across national and global cases and investigations, and to allow us to develop a comprehensive picture of the national and economic security threats we face, we must enhance and centralize our internal tracking of investigations and prosecutions of ransomware groups and the infrastructure and networks that allow these threats to persist.[213]

According to DOJ, the procedures outlined in the guidance indicate that the agency has elevated investigations of ransomware attacks to a similar priority as terrorism.[214] Accordingly, all U.S

[207] Department of the Treasury, *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Oct. 1, 2020).

[208] *See* Davidoff Interview. *See also* Office of Foreign Assets Control, Sanctions List Search (accessed May 2, 2022) (https://sanctionssearch.ofac.treas.gov).

[209] Davidoff Interview.

[210] Siegel Interview.

[211] Department of Justice, Office of the Deputy Attorney General, *Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion* (June 3, 2021).

[212] Department of Justice, Office of the Deputy Attorney General, *Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion* (June 3, 2021).

[213] *Id.*

[214] Christopher Bing, *Exclusive: U.S. to give ransomware hacks similar priority as terrorism*, Reuters (June 3, 2021) (www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/) (quoting John Carlin, principal associate deputy attorney general at DOJ, " 'We've used this model around terrorism before but never with ransomware' ".

attorney's offices are now expected to file "urgent reports" with DOJ headquarters in "**every** instance" in which a U.S. attorney's office "learns of either a new ransomware or digital extortion attack in its District, or an attack believed to be related to an ongoing ransomware or digital extortion investigation or case it is conducting" that meets certain conditions.[215]

CISA. To address the current lack of information regarding the ransomware threat, Chairman Peters and Ranking Member Portman introduced the Cyber Incident Reporting Act of 2021, which passed the Senate as the Strengthening American Cybersecurity Act of 2022, of which its incident reporting provisions recently became law as the Cyber Incident Reporting for Critical Infrastructure Act of 2022 on March 15, 2022.[216] Critical infrastructure entities, as defined through a CISA rulemaking, will have to report within 72 hours of having a reasonable belief that a substantial cyber incident (also defined in the rulemaking) has occurred. A substantial cyber incident may include a ransomware attack. The same entities will have to report within 24 hours of making a ransomware payment, regardless of whether the ransomware attack met the threshold of a substantial cyber incident. CISA has two years after passage of the Act to issue the notice of proposed rulemaking, and another 18 months to issue the final rule.

SEC. The SEC requires public companies to report material cybersecurity risks and incidents that trigger disclosure obligations.[217] However, on March 9, 2022, SEC proposed a new rule to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies.[218] The proposal came after findings that current disclosure practices are inadequate. According to the SEC, certain disclosures may "contain insufficient detail" and staff has found that current reporting "is

[215] Department of Justice, Office of the Deputy Attorney General, *Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion* (June 3, 2021) (stating that urgent reports should be filed for an attack believed to be related to an ongoing investigation that is "(a) a major development in the case; (b) a law enforcement emergency; or (c) an event affecting the Department that is likely to generate national media or Congressional attention") (emphasis in original).

[216] Consolidated Appropriations Act of 2022, Pub. L. No. 117-103, Sec. 2242 (2022).

[217] 17 CFR § 229, 249. *See also* U.S. Securities and Exchange Commission, *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* 83 FR 8166 (Feb. 26, 2018) (Interpretation) (outlining SEC's views with respect to cybersecurity disclosure requirements under the federal securities laws as they apply to public operating companies) and Division of Corporation Finance, *CF Disclosure Guidance: Topic No. 2 – Cybersecurity* (Oct. 13, 2011) (https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm) (stating that certain disclosure requirements may impose an obligation to disclose cybersecurity risks and incidents, *e.g.*, when necessary to make other required disclosures not misleading, even if the requirements do not explicitly refer to cybersecurity matters).

[218] U.S. Securities and Exchange Commission, *SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies* (Mar. 9, 2022) (www.sec.gov/news/press-release/2022-39) and U.S. Securities and Exchange Commission, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* 87 FR 16590 (Mar. 23, 2022) (Proposed Rule). *See also* U.S. Securities and Exchange Commission, *Cybersecurity Risk Management for Investment Advisers Registered Investment Companies, and Business Development Companies* 87 FR 13524 (Mar. 9, 2022) (Proposed Rule) (proposing rule to "require advisers to report significant cybersecurity incidents affecting the adviser, or its fund or private fund clients, to the Commission on a confidential basis").

inconsistent, may not be timely, and can be difficult to locate."[219] The proposed rules recognize that cybersecurity is an emerging risk for public companies and that both companies and investors need to evaluate public companies' cybersecurity practices and incident reporting.[220]

SEC staff told the Committee that they have been looking at the policies and procedures of issuers and investment advisers to determine whether they are acting sufficiently to protect individuals when ransomware incidents occur. The agency is considering how to address victims within its jurisdiction that fail to take steps to develop proper controls and policies as well as those that fail to disclose ransoms that have been paid.[221]

Transportation Security Administration. Following the May 2021 ransomware attack against Colonial Pipeline, the Department of Homeland Security's Transportation Security Administration issued two security directives to address the cybersecurity threat to pipeline systems and associated infrastructure. Security Directive Pipeline-2021-01, effective May 28, 2021, requires TSA-specified owners and operators to report cybersecurity incidents resulting in operational disruption, among other incidents, to CISA within 12 hours after the incident is identified.[222] On July 3, 2021, the Transportation Security Oversight Board issued a notification of ratification of the directive in which it stated that the directive is set to expire on May 28, 2022.[223]

Office of the Comptroller of the Currency, Federal Reserve System, and Federal Deposit Insurance Corporation. In November 2021, the OCC, Federal Reserve System, and Federal Deposit Insurance Corporation issued a final rule imposing computer-security incident notification requirements on banking organizations and their bank service providers. Effective April 1, 2022, a banking organization is required to notify its primary federal regulator of any

[219] U.S. Securities and Exchange Commission, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* 87 FR 16590 (Mar. 23, 2022) (Proposed Rule) (indicating that staff observed that certain companies failed to report publicly disclosed cyber incidents and that smaller reporting companies generally provide less cybersecurity disclosure than larger registrants). *See also* Moody's Investors Service, *Research Announcement, Cybersecurity disclosures vary greatly in high-risk industries* (Oct. 3, 2019) (www.moodys.com/research/Moodys-Cybersecurity-disclosures-vary-greatly-in-high-risk-industries--PBC_1196854) (stating that corporate cyber disclosures can vary greatly among companies in high-risk sectors which makes it more difficult to analyze a company's cyber posture and could hurt investor confidence as cyberattacks increase in frequency).

[220] U.S. Securities and Exchange Commission, *SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies* (Mar. 9, 2022) (www.sec.gov/news/press-release/2022-39).

[221] SEC Interview. *See also* Travis Brennan, Ryan C. Wilkins, and Katie Beaudin, *As Ransomware Attacks Increase, The SEC Takes Notice* (Sep. 10, 2020) (www.lexology.com/library/detail.aspx?g=732a036d-86cf-4c89-84f1-a8db50470cb9) (stating that some ransomware attacks are publicly known but are not disclosed in SEC filings).

[222] Transportation Security Administration, *Security Directive: Enhancing Pipeline Cybersecurity* (Security Directive Pipeline-2021-01) (May 28, 2021).

[223] Department of Homeland Security, *Ratification of Security Directive*, 86 Fed. Reg. 38209 (July. 20, 2021) (ratification of directive).

"computer-security incident" that rises to the level of a "notification incident" within 36 hours.[224] Bank service providers are required to notify each affected banking organization customer once it is determined that the incident caused, or is reasonably likely to cause, a material service disruption or degradation. The rule is expected to "help promote early awareness of emerging threats to banking organizations and the broader financial system."[225] Increased early awareness is intended to help "agencies react to these threats before they become systemic."[226]

IV. LACK OF COMPREHENSIVE OR CONSOLIDATED DATA ON RANSOMWARE ATTACKS AND CRYPTOCURRENCY RANSOM PAYMENTS LIMITS TOOLS AVAILABLE TO GUARD AGAINST NATIONAL SECURITY THREAT

The lack of consolidated data regarding the universe of ransomware attacks and the role that cryptocurrency plays in facilitating illicit acts limit the tools available to guard against national security threats. The United Nations and the U.S. have recently observed nations using cryptocurrencies to evade sanctions.[227] According to public reports, "hacking techniques like ransomware could help Russians [extort] digital currencies and make up revenue lost to sanctions."[228] In light of the ongoing invasion of Ukraine by Russia, a comprehensive understanding of illicit cryptocurrency use and ransomware is critical to ensure compliance with U.S. sanctions policy and mitigate damaging cybercrime.

Criminal groups in Russia are well-experienced in executing ransomware attacks. According to a 2022 Chainalysis study, about 74 percent of global ransomware revenue, or more than $400 million worth of cryptocurrency, went to ransomware strains that are "highly likely to be affiliated with Russia."[229] Russia is also at the center of cryptocurrency-based money laundering associated with cybercrimes, including ransomware. Chainalysis found that most of the funds extorted from ransomware attacks are "laundered through services primarily catering to Russian users."[230] Taking further action to increase the federal government's collective awareness of the ransomware landscape and associated uses of cryptocurrency, could provide

[224] Office of the Comptroller General, *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*, 86 Fed. Reg. 223 (Nov. 23, 2021) (final rule).

[225] *Id.*

[226] *Id.*

[227] *Russia Could Use Cryptocurrency to Blunt the Force of U.S. Sanctions*, New York Times (Feb. 23, 2022) (www.nytimes.com/2022/02/23/business/russia-sanctions-cryptocurrency.html?partner=slack&smid=sl-share). Reports indicate that Russian entities are finding workarounds to make up revenue lost due to U.S. sanctions such as developing its own central bank digital currency. *Id.*

[228] *Id.*

[229] *The 2022 Crypto Crime Report.*

[230] *The 2022 Crypto Crime Report.*

lawmakers with more information when deliberating measures to enhance the government's ability to target Russian cybercriminals.

As barriers to the deployment of ransomware lower with pre-designed ransomware tools and RaaS, and cryptocurrency obfuscation tools and techniques become enhanced, ransomware attacks will likely continue to grow, and continue to threaten U.S. national security.[231] For instance, ransomware toolkits are readily available for purchase on the darknet, which RaaS operators can lease to affiliates who conduct attacks. Certain exchanges, namely nested exchanges are known to conduct lax anti-money laundering checks, or none at all, and to provide cryptocurrency trading services through a regulated exchange to avoid attention from law enforcement in connection with illicit transactions. Such exchanges oftentimes "support money laundering, scammers, and ransomware payments."[232] Providing analysts the ability to access and query data held by all federal agencies tracking ransom payments and the wallets being used to receive ransom payments, within the bounds of privacy and security rules, would likely improve analysts' ability to track the evolution of cryptocurrency platforms that support cybercriminal activity.

[231] Yaya J. Fanusie, *Cryptocurrency Laundering Is a National Security Risk*, Lawfare (Mar. 27, 2021) (www.lawfareblog.com/cryptocurrency-laundering-national-security-risk).

[232] *What Are Nested Exchanges and Why Should You Avoid Them?* Binance Academy (Dec. 2021) (academy.binance.com/en/articles/what-are-nested-exchanges-and-why-should-you-avoid-them). *See also Russia Could Use Cryptocurrency to Blunt the Force of U.S. Sanctions*, New York Times (Feb. 23, 2022) (www.nytimes.com/2022/02/23/business/russia-sanctions-cryptocurrency.html?partner=slack&smid=sl-share) (identifying "nesting" as a potential money-laundering technique that Russia could use to evade U.S. sanctions).

CONCLUSION

The majority of ransomware attacks go unreported and ransoms based in cryptocurrency continue to be paid against FBI guidance.[233] The continuing flow of ransom payments has encouraged illicit actors and contributed to a growing threat to businesses, the public, and to national security. The lack of comprehensive data on these attacks prevents the U.S. government from developing a full picture of cyber threats.

The Administration states that it has made countering ransomware attacks a priority. In October 2021, it brought together representatives from 30 countries to discuss how to disrupt "the financial systems that make ransomware profitable" and "the ransomware ecosystem," among other ways to fight back against ransomware attacks.[234] On March 9, 2022, the Biden Administration issued an Executive Order outlining a "whole-of-government" approach to examining the risks associated with the sharp increase in use of cryptocurrencies.[235] Among other key policy priorities, the Administration recognizes that cryptocurrencies have "facilitated sophisticated cybercrime-related financial networks and activity, including through ransomware activity."[236] The Executive Order also recognizes that cryptocurrencies present "heighten[ed] risks of crimes such as money laundering, terrorist and proliferation financing, fraud and theft schemes, and corruption."[237] Among other requirements, President Biden is directing federal agencies to develop coordinated plans to address "digital-asset-related illicit finance and national security risks."[238]

The data needed to support these initiatives, among other agency efforts to tackle ransomware and cryptocurrency ransom payments, remains fragmented and incomplete. The lack of comprehensive ransomware incident and ransom payment reporting contributes to a lack of data on matters that are priorities in the Biden Administration's national security agenda. Further, this limited collective understanding of the ransomware landscape and the cryptocurrency payment system blunts the effectiveness of available tools to protect national security. As Russia's invasion of Ukraine continues and Russia seeks to find ways around the international finance system, the need to address these shortfalls grows.

[233] Federal Bureau of Investigation, Ransomware (accessed Mar. 3, 2022) (www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware#:~:text=The%20FBI%20does%20not%20support,this%20type%20of%20illegal%20activity) and *see also* Sarah N. Lynch, *FBI Director Wray Urges companies to stop paying ransoms to hackers*, Reuters (June 23, 2021) (www.reuters.com/technology/fbi-director-wray-urges-companies-stop-paying-ransoms-hackers-2021-06-23/) (quoting FBI Director Chris Wray, "[i]n general, we would discourage paying the ransom because it encourages more of these attacks, and frankly, there is no guarantee whatsoever that you are going to get your data back").

[234] *See* White House, *Fact Sheet: Ongoing Public U.S. Efforts to Counter Ransomware* (Oct. 13, 2021) (www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/).

[235] Exec. Order No. 14067, 87 FR 14143 (Mar. 14, 2022).

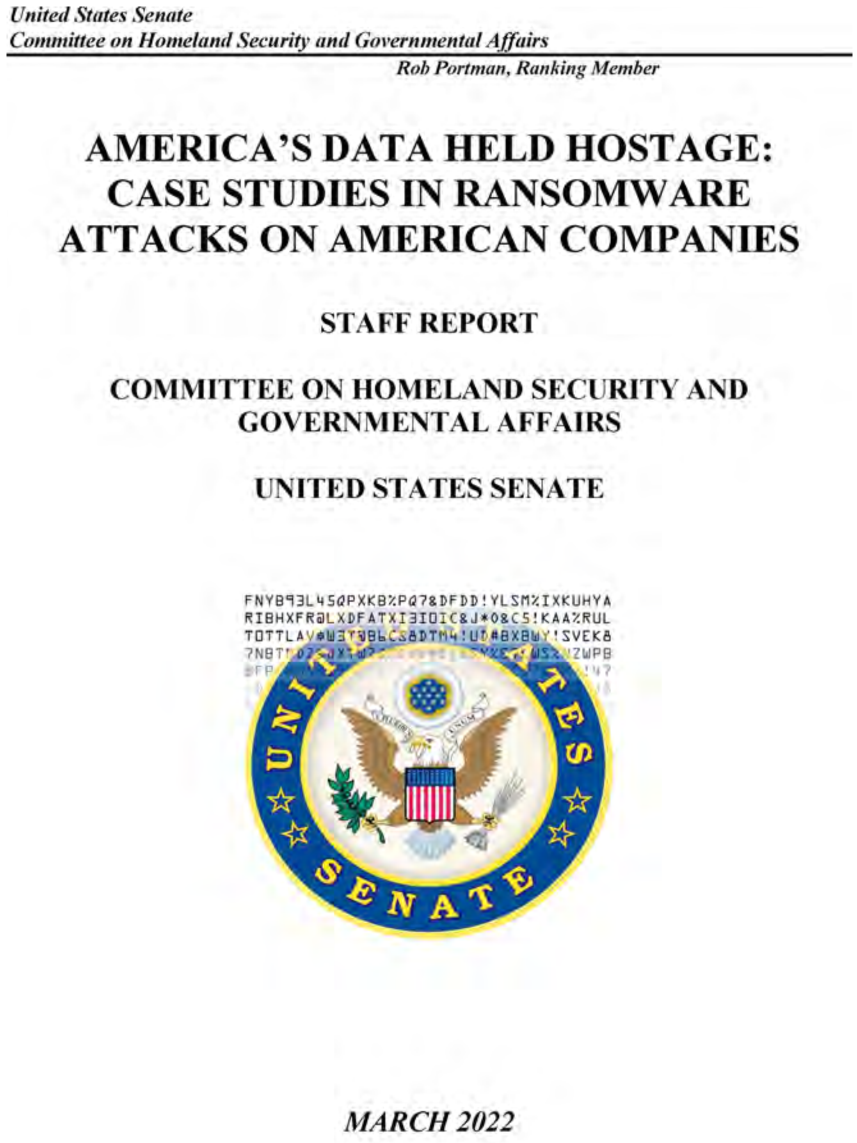
[236] *Id.*

[237] *Id.*

[238] *Id.*

To address the lack of understanding of the true scope of the problem and the size of the ransomware market, Chairman Peters and Ranking Member Portman introduced the Cyber Incident Reporting Act of 2021, which passed the Senate as part of the Strengthening American Cybersecurity Act of 2022, of which its incident reporting provisions recently became law as the Cyber Incident Reporting for Critical Infrastructure Act on March 15, 2022. The Administration should prioritize timely implementation of the new law's reporting requirements. The rules implementing the reporting process should be standardized and easily understood such that victims under the duress of an attack are not unduly burdened by the reporting process.

To ensure that the potential influx of ransomware attack-related data is used effectively, Congress should consider exploring whether federal agencies responsible for processing the data have sufficient resources to do so in a timely and effective manner and assess the level of resources that would be needed, if not. Further, given the extent to which the federal government relies on partnerships with the private, nonprofit, and academic sectors at home and abroad, Congress should consider effective ways for federal agencies to share data on ransomware attacks and payments. Finally, in light of ransomware threat actors' growing technological capabilities, any actions aimed at increasing government datasets on the ransomware ecosystem and cryptocurrency ransom payments must be done in conjunction with efforts to track and circumvent ransomware attackers' attempts to conduct increasingly sophisticated attacks.



United States Senate
Committee on Homeland Security and Governmental Affairs
Rob Portman, Ranking Member

AMERICA'S DATA HELD HOSTAGE: CASE STUDIES IN RANSOMWARE ATTACKS ON AMERICAN COMPANIES

STAFF REPORT

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

UNITED STATES SENATE

MARCH 2022

AMERICA'S DATA HELD HOSTAGE: CASE STUDIES IN RANSOMWARE ATTACKS ON AMERICAN COMPANIES

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

More than ever before, cyber criminals have the ability to disrupt Americans' lives from anywhere in the world. Over time, attackers' tactics have evolved and improved and cyberattacks now have the potential to paralyze entire industry sectors. Organizations are racing to update their systems and improve their defenses to counter this threat. The proliferation of ransomware attacks is a primary example of this challenge.

Ransomware is a type of malware that encrypts victims' computer systems and data, rendering the systems unusable and the data unreadable. Perpetrators then issue a ransom demand—often in cryptocurrency—allowing remote and anonymous payment to attackers. If the victim pays, hackers *may* provide the victim with a key to decrypt their systems and data. But there is no guarantee. In a new trend, called double extortion, attackers first steal sensitive data from a victim before deploying the ransomware. Then, cyber criminals threaten to release the stolen data if the victim refuses to pay the ransom—so even ransomware victims who are able to restore their data without paying the ransom are at risk.

Ransomware is on the rise. While the first recorded instance of ransomware was in 1989, the frequency of these attacks has increased exponentially, at least in part because of the establishment of cryptocurrencies. One cybersecurity firm estimated there were 623.3 million attempted ransomware attacks worldwide in 2021 alone—an average of 20 attempted attacks every second. The United States suffered the most ransomware attempts at 421.5 million, a 98 percent increase from 2020. Americans have become all too familiar with the real-world impact of high-profile ransomware attacks like those on Colonial Pipeline, America's largest fuel pipeline, and JBS, the world's largest beef producer.

* * * * * * * * * *

This report details the attacks by Russia-based ransomware group REvil on three American companies, and the experiences of those companies during the incident response. The goal of this report is to provide information companies and agencies can use to prepare for and respond to ransomware attacks.

REvil targeted entities of all sizes and sophistication. The three companies have little in common in terms of business model, purpose, or number of employees. Entity A is a global multi-sector Fortune 500 company with roughly 100,000 employees. Entity B is a global manufacturing company with several thousand employees. Entity C is a technology firm with only 50 employees. Nevertheless, all three were targeted by the same ransomware group. This underscores the broad threat ransomware presents and the proactive steps all organizations must take to implement cyber best practices.

Ransomware criminals often use phishing attacks to gain initial access. Cybercriminals gained access to Entity A's networks by compromising a known vulnerability on a legacy server of one of its vendors. Attackers then impersonated that vendor, and sent an unsuspecting Entity A employee an email attachment corrupted with ransomware.

A phishing attack—a malicious email disguised as a legitimate email—was also the entry point for REvil's ransomware attack on Entity B. REvil compromised Entity B when a mid-level employee opened a phishing email disguised as a message from their bank. Even organizations with sophisticated cybersecurity protections are susceptible to a single employee falling victim to a well-crafted phishing email.

Offline backups and well-defined incident response plans helped ransomware victims mitigate successful ransomware attacks. All three entities interviewed by the Committee had established incident response plans when REvil attacked them. This proactive measure allowed each entity to take quick remedial action, onboard third-party experts, and in the case of Entity B cut off the attacker's access before they encrypted its networks with ransomware.

In addition to restoring access to their critical data, backups permitted these three entities to resume normal business operations, like payroll. As a result, these entities avoided the attacks' worst effects, including the need to pay the ransom.

Two victim companies reported little help from the Federal Government. All three companies reported their incidents to the Federal Government. Of these, one company did not need the Government's help. The other two companies reported they got little help. They told the Committee that the Federal Bureau of Investigation (FBI) prioritized its investigative efforts into REvil's operations over protecting the companies' data and mitigating damage. Both companies also indicated they did not receive advice on best practices for responding to a ransomware attack or other useful guidance from the Federal Government.

Because there is no central repository to collect information on and provide insight into the ransomware attacks taking place across the United States, CISA and the National Cyber Director should work quickly with other appropriate agencies like FBI to implement recently enacted legislation requiring critical infrastructure owners and operators to report cyber incidents and ransomware payments to CISA. This law will enhance the Federal Government's ability to combat cyberattacks, mount a coordinated defense, hold perpetrators accountable, and prevent and mitigate future attacks through information sharing.

II. FINDINGS AND RECOMMENDATIONS

Findings of Fact

(1) All organizations, regardless of size and sophistication, are susceptible to ransomware attacks.

(2) Ransomware groups often use phishing attacks to gain initial access to victim networks.

(3) In past ransomware attacks, multifactor authentication, zero trust principles, and network segmentation helped prevent attackers from gaining or increasing access to sensitive data in a victim's networks.

(4) Maintaining offline backups and a well-defined incident response plan helped victims resume critical operations quickly without paying a ransom, when attackers did get in.

(5) The laws and regulations at the time discouraged victims from sharing information with other potential victims that could prevent future ransomware attacks.

(6) In two cases reviewed in this report, the FBI prioritized its investigative and prosecutorial efforts to disrupt attacker operations over victims' need to protect data and mitigate damage.

(7) Until recently, there was no Federal agency charged with collecting and tracking reports of cyber incidents to prevent and mitigate future attacks.

REvil Findings

(8) REvil monetized access to victim networks and sold that access to other REvil affiliates.

(9) Before encrypting victim organization networks, REvil used double extortion methods to first steal sensitive data from victims and then publish that data on REvil's public blog.

(10) REvil harassed victim company employees via email and telephone in an attempt to coerce the companies into paying ransoms.

Recommendations

(1) **CISA should immediately share all incident reports received under the Cyber Incident Reporting for Critical Infrastructure Act with the FBI.** The FBI and CISA should also strengthen their partnership to assist ransomware victims. Close coordination between these two entities will best position the FBI to investigate those responsible for ransomware attacks while also allowing CISA to provide the technical assistance victims need to recover.

(2) **FBI should ensure it considers ransomware victim priorities like protecting data and mitigating damage.** This will preserve FBI's constructive working relationship with the private sector and provide it with the information necessary to hold attackers accountable.

(3) **CISA and the National Cyber Director should work quickly with other appropriate agencies like FBI to implement recently enacted legislation requiring critical infrastructure owners and operators to report cyber incidents and ransomware payments to CISA.** This legislation will enhance the Federal Government's ability to combat cyberattacks, mount a coordinated defense, hold perpetrators accountable, and prevent and mitigate future attacks through the sharing of timely and actionable threat information.

(4) **Increase costs for attackers by eliminating low hanging fruit.** Organizations can increase the difficulty for ransomware criminals by patching vulnerabilities, implementing multi-factor authentication, maintaining accurate device and software inventories, and instituting complex password requirements. Adhering to these cyber best practices will increase the likelihood that attackers move on to less prepared targets.

(5) **Organizations should implement a defensive posture that assumes the organization has been breached.** Sophisticated cyber adversaries with near unlimited resources can compromise most networks if given enough time. Employing zero trust networking (continuous authentication and monitoring) with need-to-know access privileges will give organizations critical time to detect attackers and cut off their access before they exfiltrate or encrypt sensitive data. Flat networks and enterprise-wide shared drives give users more access than they need, allowing hackers to do more damage if they compromise one of those accounts.

(6) **Have a cyber incident response plan in place before an attack occurs.** When a cyber incident inevitably takes place, organizations should know in advance who needs to be notified and when. Incident response plans should detail explicit processes for notifying the Government and retaining an incident response provider. Entities should also determine which systems are most critical to its operations and how long those systems can be offline before business operations suffer significant impacts. For critical infrastructure owners and operators, organizations should go a step further to determine how long systems can be offline before there are regional or national effects.

(7) **Maintain offline backups and encrypt sensitive data when stored and in transit.** These two solutions can help mitigate the otherwise debilitating impact of ransomware attacks. With offline backups, organizations can reconstitute impacted systems without having to pay a ransom for the decryption key. Encrypting sensitive data addresses the second half of double extortion attacks because the data is unreadable. Together, offline backups and encryption of sensitive data are the most effective ways to mitigate the damage and cost associated with a successful ransomware attack.

III. BACKGROUND

Ransomware is a critical national security threat that can affect the daily lives of all Americans. During ransomware attacks, criminals deploy malicious software that encrypts a victims' files and renders its systems unusable.[1] In 2021, there were 623.3 million attempted ransomware attacks globally.[2] This was a 105 percent increase from 2020.[3] The United States was the top target for attempted ransomware attacks globally in 2021, increasing 98 percent from the prior year.[4] Of the 623.3 million attempted ransomware attacks in 2021, the United States had 421.5 million—accounting for over 67 percent of all attacks globally.[5]

Ransomware's rapid growth is problematic not only for the private sector but also for government.[6] During the first six months of 2021, there were more ransomware attack attempts on government than any other industry, and three times the number of attacks seen in 2020.[7] Testifying before the Senate Homeland Security and Governmental Affairs Committee, Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly summarized the ransomware threat saying, "incidents like Colonial Pipeline, JBS Foods and the scourge of ransomware attacks . . . on our schools and hospitals and small businesses illustrate how cybersecurity impacts our daily lives."[8]

A. Evolution of Ransomware

Encrypting files in attempt to prevent user access is an attack technique that dates back to the late 1980s.[9] The first ransomware attack on record is the AIDS Trojan deployed by floppy disk in 1989.[10] Roughly 20,000 malware-corrupted floppy disks were distributed to attendees of the World Health Organization's

[1] *Ransomware 101*, Cybersecurity & Infrastructure Sec. Agency, https://www.cisa.gov/stopransomware/ransomware-101.

[2] SonicWall, 2022 SonicWall Cyber Threat Report 29 (2022), https://www.sonicwall.com/medialibrary/en/white-paper/2022-sonicwall-cyber-threat-report.pdf.

[3] *Id.*

[4] *Id.* at 31.

[5] *Id.*

[6] *Alert (AA22-040A): 2021 Trends Show Increased Globalized Threat of Ransomware*, Cybersecurity & Infrastructure Sec. Agency (Feb. 10, 2022), https://www.cisa.gov/uscert/ncas/alerts/aa22-040a.

[7] SonicWall, Mid-Year Update: 2021 SonicWall Cyber Threat Report 11 (2021), https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2021-cyber-threat-report.pdf.

[8] *National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 117th Cong. (2021) (testimony of Jen Easterly, Director, CISA).

[9] Symantec, The Evolution of Ransomware 7 (2015).

[10] *Id.*

international AIDS conference that year in Stockholm.[11] To restore access to their files, victims were instructed to send $189 to a P.O. Box in Panama.[12]

AIDS Trojan Floppy Disk
Source: Andrada Fiscutean, A history of ransomware: The motives and methods behind these evolving attacks, *CSO (Jul. 27, 2020), https://www.csoonline.com/article/3566886/a-history-of-ransomware-the-*

A Belgian-based information technology (IT) professional impacted by the malware recalled he quickly determined it was not sophisticated and only took him ten minutes to restore all of his files.[13] The malware failed to encrypt file contents to prevent user access, and only changed file names to random characters.[14]

An American evolutionary biologist named Dr. Joseph Popp developed the AIDS Trojan.[15] Popp was arrested and charged with blackmail before being declared mentally unfit to stand trial.[16]

[11] Anthony M. Freed, *A Brief History of Ransomware Evolution*, CYBEREASON (Nov. 30, 2021), https://www.cybereason.com/blog/a-brief-history-of-ransomware-evolution.
[12] *Id.*
[13] Andrada Fiscutean, *A history of ransomware: The motives and methods behind these evolving attacks*, CSO (Jul. 27, 2020), https://www.csoonline.com/article/3566886/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html.
[14] *Id.*
[15] Anthony M. Freed, *A Brief History of Ransomware Evolution*, CYBEREASON (Nov. 30, 2021), https://www.cybereason.com/blog/a-brief-history-of-ransomware-evolution.
[16] Andrada Fiscutean, *A history of ransomware: The motives and methods behind these evolving attacks*, CSO (Jul. 27, 2020), https://www.csoonline.com/article/3566886/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html.

Modern ransomware arrived in 2005 with malware called PGPCoder.[17] This virus encrypted all files with extensions such as .doc, .html, and .jpg.[18] It also created "!_READ_ME_!.txt" files in each folder instructing victims to pay several hundred dollars to an e-gold or Liberty Reserve account to decrypt their files.[19]

While viruses like PGPCoder ushered in the modern ransomware construct, these attacks remained uncommon because payment collection was difficult.[20] At the time, hackers had few reliable options for collecting anonymous payments, free from law enforcement scrutiny.[21] Cryptocurrencies like Bitcoin changed this dynamic by streamlining the ransom collection process and providing some degree of anonymity.[22]

Ransomware continued to proliferate through the early 2010s, but hackers had yet to perfect using cryptocurrencies for ransom payments.[23] During this timeframe, cryptocurrencies remained a foreign concept to many, and so non-tech-savvy victims struggled to pay the ransoms.[24] As a result, some cybercriminals set up call centers to help victims purchase Bitcoin, a cryptocurrency often used to pay ransom demands.[25] This helped ensure payment, but was also expensive and time consuming for hackers.[26]

Cryptocurrency exchanges allowed cybercriminals to receive instant and anonymous payments outside of traditional financial institutions. [27] Armed with this newfound convenience and anonymity, cybercriminals realized they could make

[17] SYMANTEC, THE EVOLUTION OF RANSOMWARE 9 (2015).

[18] Andrada Fiscutean, *A history of ransomware: The motives and methods behind these evolving attacks*, CSO (Jul. 27, 2020), https://www.csoonline.com/article/3566886/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html.

[19] *Id.* Liberty Reserve was a money transfer business that only required a valid email address to open an account. Brian Krebs, *Reports: Liberty Reserve Founder Arrested, Site Shuttered*, KREBS ON SECURITY (May 25, 2013), https://krebsonsecurity.com/2013/05/reports-liberty-reserve-founder-arrested-site-shuttered/. In 2013, the U.S. Department of Justice shut down Liberty Reserve alleging the service processed $6 billion in criminal proceeds. Brian Krebs, *A Light at the End of Liberty Reserve's Demise?*, KREBS ON SECURITY (Feb. 14, 2020), https://krebsonsecurity.com/2020/02/a-light-at-the-end-of-liberty-reserves-demise/.

[20] CROWDSTRIKE, THE EVOLUTION OF RANSOMWARE: HOW TO PROTECT AGAINST NEW ADVERSARY TRENDS AND METHODS 2 (2021).

[21] SYMANTEC, THE EVOLUTION OF RANSOMWARE 22 (2015).

[22] *Id.* at 22–23.

[23] *History of Ransomware*, CROWDSTRIKE (Jun. 21, 2021), https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/.

[24] *Id.*

[25] CROWDSTRIKE, THE EVOLUTION OF RANSOMWARE: HOW TO PROTECT AGAINST NEW ADVERSARY TRENDS AND METHODS 2 (2021).

[26] *History of Ransomware*, CROWDSTRIKE (Jun. 21, 2021), https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/.

[27] SYMANTEC, THE EVOLUTION OF RANSOMWARE 22–23 (2015).

millions in just a few weeks.[28] Once someone sets up a Bitcoin wallet linked to an exchange, transactions to and from that wallet are not easily traceable to a specific person.[29] A digital currency wallet is a software application that allows a user to hold, store, and transfer digital currency.[30]

CrowdStrike, a prominent cybersecurity firm, conducted a survey in 2020 of 2,200 senior IT leaders and security professionals from organizations with 250 or more employees that revealed 56 percent of participating organizations experienced a ransomware attack in the last year.[31] The same survey found 54 percent of participating IT professionals now rank ransomware among the most concerning cyber threats facing their organizations.[32]

B. Recent Ransomware Trends

In recent years, ransomware criminals have improved their techniques to increase the pressure on victims to pay ransoms. As these techniques evolve over time, several recent trends have emerged. These include: (1) stealing and threatening to release sensitive victim data in what are called "double extortion attacks"; (2) targeting high-value organizations and data; (3) rebranding to evade law enforcement; and (4) using ransomware services-for-hire affiliate structures.

1. Double Extortion Attacks

Double extortion refers to hackers making an additional threat to release stolen victim data on top of encrypting its systems if the victim does not pay.[33] In double extortion attacks, hackers exfiltrate files from victims before encrypting their host systems.[34] This allows hackers to threaten to publish the stolen victim data to further coerce victims into making a ransom payment as shown in the REvil

[28] Andrada Fiscutean, *A history of ransomware: The motives and methods behind these evolving attacks*, CSO (Jul. 27, 2020), https://www.csoonline.com/article/3566886/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html.

[29] Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 85 Fed. Reg. 83,842 (Dec. 23, 2020) (codified at 31 C.F.R. pt. 1010, 1020, 1022).

[30] *Questions on Virtual Currency*, U.S. DEP'T OF TREASURY (Oct. 15, 2021), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/559.

[31] CROWDSTRIKE, 2020 CROWDSTRIKE GLOBAL SECURITY ATTITUDE SURVEY: INSIGHTS INTO SECURITY TRANSFORMATION AND PREVALENT ATTACK VECTORS IN A WORK-FROM-ANYWHERE WORLD 3 (2020), https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CSGlobalSecurityAttitudeSurveyReport.pdf.

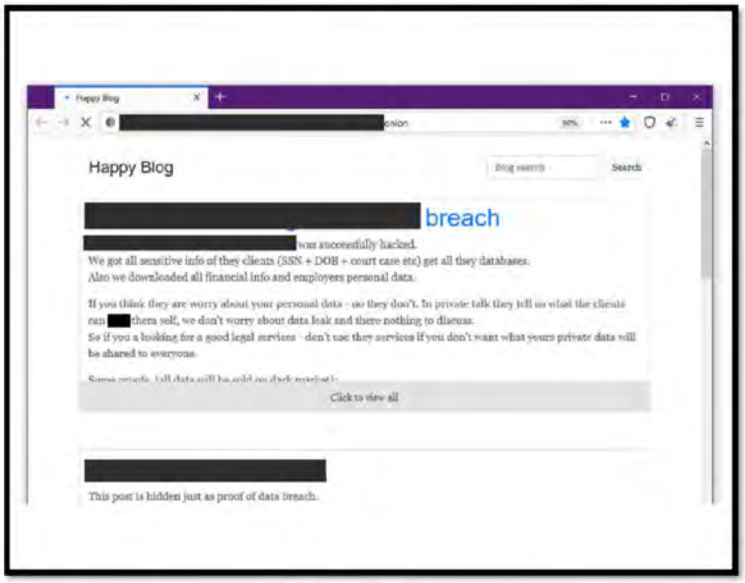
[32] *Id.* at 4.

[33] U.S. DEP'T OF TREASURY, FINANCIAL TREND ANALYSIS: RANSOMWARE TRENDS IN BANK SECRECY ACT DATA BETWEEN JANUARY 2021 AND JUNE 2021 3 (2021); IVANTI, RANSOMWARE: THROUGH THE LENS OF THREAT AND VULNERABILITY MANAGEMENT 38 (2022).

[34] U.S. DEP'T OF TREASURY, FINANCIAL TREND ANALYSIS: RANSOMWARE TRENDS IN BANK SECRECY ACT DATA BETWEEN JANUARY 2021 AND JUNE 2021 3 (2021).

"Happy Blog" screenshot below.[35] Ransomware operators use these websites called "leak sites" to post screenshots of a victim's directory structure to prove they possess and are prepared to release the victim's sensitive files.[36]

Tactics like double extortion have emboldened attackers, who now issue ransom demands larger than ever before. For example, during the first half of 2021, financial institutions reported $590 million in ransomware payments, exceeding the amount reported for all of 2020.[37] This was a 42 percent increase from the $416 million total reported in 2020.[38]



Happy Blog

[redacted] breach

[redacted] was successfully hacked.
We got all sensitive info of they clients (SSN + DOB + court case etc) get all they databases.
Also we downloaded all financial info and employers personal data.

If you think they are worry about your personal data - no they don't. In private talk they tell us what the clients can [redacted] them self, we don't worry about data leak and there nothing to discuss.
So if you a looking for a good legal services - don't use they services if you don't want what yours private data will be shared to everyone.

Some proofs (all data will be sold on dark market):

Click to view all

[redacted]

This post is hidden just as proof of data breach.

REvil Happy Blog Post

Source: Catalin Cimpanu, REvil ransomware group returns following Kaseya attack, RECORDED FUTURE (Sept. 7, 2021), https://therecord.media/revil-ransomware-group-returns-following-kaseya-attack/.

[35] *Id.*; Catalin Cimpanu, *REvil ransomware group returns following Kaseya attack*, RECORDED FUTURE (Sept. 7, 2021), https://therecord.media/revil-ransomware-group-returns-following-kaseya-attack/.
[36] PALO ALTO NETWORKS: UNIT 42, 2021 RANSOMWARE THREAT REPORT 5 (2021).
[37] U.S. DEP'T OF TREASURY, FINANCIAL TREND ANALYSIS: RANSOMWARE TRENDS IN BANK SECRECY ACT DATA BETWEEN JANUARY 2021 AND JUNE 2021 1 (2021).
[38] *Id.* at 3.

In 2021, the manufacturing industry experienced the most double extortion leaks, followed by professional and legal services and construction.[39] The double extortion tactic is prevalent in the Americas, accounting for 62 percent of victim data posted on leak websites.[40] Forty-seven percent of those victims were in the United States.[41] Late in 2021, ransomware criminals sometimes added an additional layer, called "triple extortion", where attackers also notify a ransomware victim's partners, shareholders, and suppliers of the incident.[42]

2. High-Value Target Attacks

Another trend in ransomware is high-value target attacks, sometimes referred to as "big game hunting" (BGH).[43] With this strategy, hackers target specific organizations with substantial financial resources or sensitive information.[44] BGH is so prevalent that CrowdStrike referred to it as "one of the most prominent trends" affecting digitally perpetrated crimes like ransomware.[45]

BGH also includes targeting entities important to the United States economy, like those in the industrial and manufacturing sectors.[46] Because disruption in day-to-day operations affect the core business of these sectors, these entities are more likely to pay a ransom to resume normal operations.[47] In some critical infrastructure sectors, regulations prescribe reliability and restrict downtime, providing further incentive to pay ransoms and restore service quickly.[48] For example, the Federal Energy Regulatory Commission, which regulates electric utilities, in some cases will fine electric utilities for violating reliability standards when a blackout occurs.[49] The attack on Colonial Pipeline, which is the largest refined products pipeline in the United States,[50] is an example of this.[51]

[39] Palo Alto Networks: Unit 42, 2021 Ransomware Threat Report 8 (2021).

[40] *Id.* at 6.

[41] *Id.*

[42] *Alert (AA22-040A): 2021 Trends Show Increased Globalized Threat of Ransomware*, Cybersecurity & Infrastructure Sec. Agency (Feb. 10, 2022), https://www.cisa.gov/uscert/ncas/alerts/aa22-040a.

[43] CrowdStrike, 2021 Global Threat Report 6 (2021).

[44] *History of Ransomware*, CrowdStrike (Jun. 21, 2021), https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/.

[45] *Id.*

[46] CrowdStrike, 2021 Global Threat Report 21 (2021).

[47] *Cf.* CrowdStrike, 2021 CrowdStrike Global Threat Report 21 (2021).

[48] *E.g.*, *Orders, Reliability Enforcement Orders*, Fed. Energy Reg. Commission (2020), https://www.ferc.gov/industries-data/electric/industry-activities/orders-reliability-enforcement-orders.

[49] *Id.*

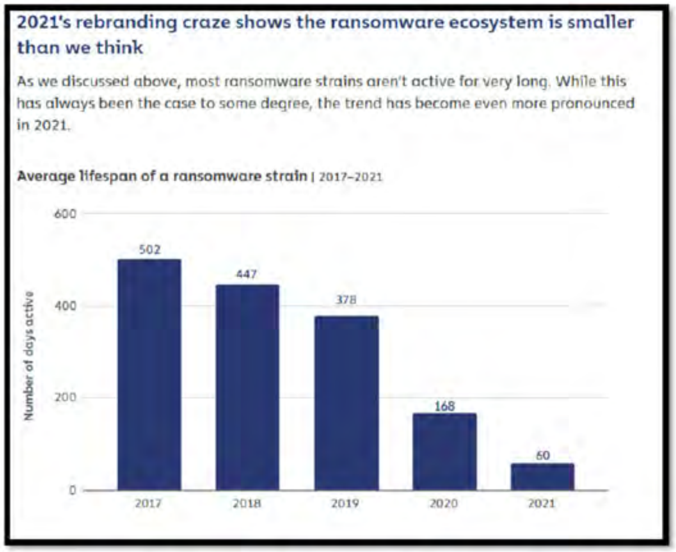
[50] *About Us/Our Company*, Colonial Pipeline, https://www.colpipe.com/about-us/our-company.

[51] *See generally Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 117th Cong. (2021) (testimony of Joseph Blount, President & Chief Executive Officer, Colonial Pipeline Company):

By the middle of 2021, and after high-profile attacks like Colonial Pipeline and JBS Foods, the FBI observed some ransomware threat actors shifting their efforts to mid-size victims to reduce scrutiny.[52] This shift also follows U.S. authorities disrupting several ransomware groups around the same time.[53]

3. Rebranding

Rebranding is a third trend where ransomware groups claim retirement only to reemerge shortly thereafter under a new name.[54] With this deceptive tactic, cybercriminals attempt to distract or evade law enforcement and continue normal operations.[55] This includes setting up new victim payment sites and other attack infrastructure.[56]



2021's rebranding craze shows the ransomware ecosystem is smaller than we think

As we discussed above, most ransomware strains aren't active for very long. While this has always been the case to some degree, the trend has become even more pronounced in 2021.

Rebranding Frequency and Short Lifespan of Ransomware Stains in 2021
Source: CHAINALYSIS, THE 2022 CRYPTO CRIME REPORT 45 (2022).

Cyberattack halts fuel movement on Colonial petroleum pipeline, U.S. ENERGY INFORMATION ADMIN. (May 11, 2021), https://www.eia.gov/todayinenergy/detail.php?id=47917.

[52] *Alert (AA22-040A): 2021 Trends Show Increased Globalized Threat of Ransomware*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Feb. 10, 2022), https://www.cisa.gov/uscert/ncas/alerts/aa22-040a.

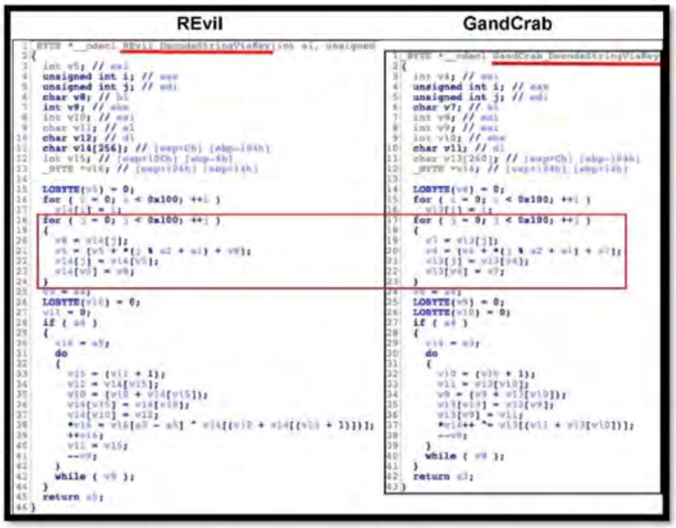
[53] *Id.*

[54] CHAINALYSIS, THE 2022 CRYPTO CRIME REPORT 45 (2022).

[55] *Id.* at 47.

[56] *Id.* at 46.

As an example, some consider REvil a rebrand of GandCrab, which announced its retirement in 2019.[57] GandCrab claimed to extort over $2 billion from victims and boasted "we are living proof that you can do evil and get off scot-free."[58] Below is a screenshot depicting the near identical code used by both REvil and GandCrab.



REvil

```
BYTE *__cdecl REvil_DecodeStringViaKey(int a1, unsigned
{
  int v5; // esi
  unsigned int i; // eax
  unsigned int j; // edi
  char v8; // bl
  int v9; // ebx
  int v10; // esi
  char v11; // al
  char v12; // dl
  char v14[256]; // [esp+Ch] [ebp-104h]
  int v15; // [esp+10Ch] [ebp-4h]
  _BYTE *v16; // [esp+124h] [ebp+14h]

  LOBYTE(v5) = 0;
  for ( i = 0; i < 0x100; ++i )
    v14[i] = i;
  for ( j = 0; j < 0x100; ++j )
  {
    v8 = v14[j];
    v5 = (v5 + *(j % a2 + a1) + v8);
    v14[j] = v14[v5];
    v14[v5] = v8;
  }
  v9 = a4;
  LOBYTE(v10) = 0;
  v11 = 0;
  if ( a4 )
  {
    v16 = a5;
    do
    {
      v15 = (v11 + 1);
      v12 = v14[v15];
      v10 = (v10 + v14[v15]);
      v14[v15] = v14[v10];
      v14[v10] = v12;
      *v16 = v16[a3 - a5] ^ v14[(v12 + v14[(v15 + 1)])];
      ++v16;
      v11 = v15;
      --v9;
    }
    while ( v9 );
  }
  return a5;
}
```

GandCrab

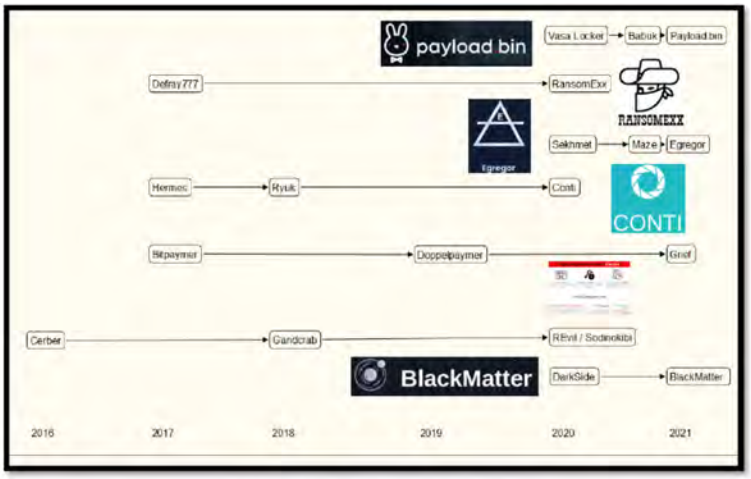
```
_BYTE *__cdecl GandCrab_DecodeStringViaKey
{
  int v4; // esi
  unsigned int i; // eax
  unsigned int j; // edi
  char v7; // bl
  int v8; // edi
  int v9; // esi
  int v10; // ebx
  char v11; // dl
  char v13[260]; // [esp+Ch] [ebp-104h]
  _BYTE *v14; // [esp+124h] [ebp+14h]

  LOBYTE(v4) = 0;
  for ( i = 0; i < 0x100; ++i )
    v13[i] = i;
  for ( j = 0; j < 0x100; ++j )
  {
    v7 = v13[j];
    v4 = (v4 + *(j % a2 + a1) + v7);
    v13[j] = v13[v4];
    v13[v4] = v7;
  }
  v8 = a4;
  LOBYTE(v9) = 0;
  LOBYTE(v10) = 0;
  if ( a4 )
  {
    v14 = a3;
    do
    {
      v10 = (v10 + 1);
      v11 = v13[v10];
      v9 = (v9 + v13[v10]);
      v13[v10] = v13[v9];
      v13[v9] = v11;
      *v14++ ^= v13[(v11 + v13[v10])];
      --v8;
    }
    while ( v8 );
  }
  return a3;
}
```

Similar Code Used by Both REvil and GandCrab
Source: DEP'T OF HEALTH & HUMAN SERVICES, *REVIL/SODINOKIBI RANSOMWARE VS. THE HEALTH SECTOR* 7 (2021), *https://www.hhs.gov/sites/default/files/revil-update-tlpwhite.pdf.*

Rebranding is a process ransomware gangs undertake with relative ease. The graphic below shows the rebrandings of several prominent ransomware gangs over just the last few years. At least one reason for rebranding is to avoid scrutiny and sanctions—ransomware groups can change their name, create a new website, and resume operations under the new name.[59]

[57] DEP'T OF HEALTH & HUMAN SERVICES, REVIL/SODINOKIBI RANSOMWARE VS. THE HEALTH SECTOR 4 (2021), https://www.hhs.gov/sites/default/files/revil-update-tlpwhite.pdf.
[58] *Id.* at 4–5.
[59] CHAINALYSIS, THE 2022 CRYPTO CRIME REPORT 47 (2022); *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, U.S. DEP'T OF TREASURY (Oct. 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.



Ransomware Group Rebranding Timeline
Source: Brian Krebs, Ransomware Gangs and the Name Game Distraction, KREBS ON SECURITY (Aug. 5, 2021), https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/.

4. Ransomware-as-a-Service

Over the last year, ransomware groups have professionalized their operations using a business model often called ransomware-as-a-service (RaaS).[60] Under this configuration, ransomware developers sell or deliver their malware to separate individuals or groups who have illicit access to a target victim network.[61] The two parties then enter into a profit sharing arrangement where the initial developer receives a percentage of all ransoms paid by victims.[62] Examples of RaaS groups include REvil, DarkSide, and Conti.[63]

[60] *Alert (AA22-040A): 2021 Trends Show Increased Globalized Threat of Ransomware*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Feb. 10, 2022), https://www.cisa.gov/uscert/ncas/alerts/aa22-040a.

[61] *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*, U.S. DEP'T OF TREASURY (Nov. 8, 2021), https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf.

[62] *Id.*

[63] DEP'T OF HEALTH & HUMAN SERVICES, REVIL/SODINOKIBI RANSOMWARE VS. THE HEALTH SECTOR 3 (2021), https://www.hhs.gov/sites/default/files/revil-update-tlpwhite.pdf; *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*, U.S. DEP'T OF TREASURY (Nov. 8, 2021), https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf; *Alert (AA21-265A): Conti Ransomware*, CYBERSECURITY AND INFRASTRUCTURE AGENCY (Mar. 9, 2022), https://www.cisa.gov/uscert/ncas/alerts/aa21-265a.

C. Role of the Private Sector in Ransomware Incident Response

Complex cyber attacks, including ransomware, make it difficult for victims to respond alone—often requiring specific technical and legal experts companies may not have on their payroll. As a result, third-party experts play a significant role in shaping ransomware incident response efforts. Examples of third-party experts include cyber insurers, law firms, cyber incident response firms, and ransomware negotiators. The high cost of retaining these experts can make responding to a ransomware attack difficult for all but the most well-financed businesses. According to a recent IBM report, the average total cost of a ransomware attack is $4.62 million.[64]

1. Cyber Insurance

The growth in ransomware attacks has caused a corresponding growth in cyber insurance. Companies can select standalone policies exclusively covering cyber risk or broader liability policies that also cover cyber incidents, like ransomware attacks.[65] As of 2020, United States domiciled insurers reported roughly $1.62 billion in direct written premiums for standalone cyber insurance policies, and $1.13 billion in direct written premiums for cyber coverage as part of broader insurance policies.[66] During 2020 alone, standalone cybersecurity insurance direct written premiums increased by 28.1 percent.[67]

Cyber insurance policies cover risk categories including liability for suffering a data breach, breach remediation costs, and coverage for legal or regulatory penalties.[68] In particular, this often covers costs associated with: business interruption, notifying consumers after a breach, providing credit monitoring services, and restoring or replacing impacted systems.[69] Costs associated with ransomware attacks are also covered by many cyber insurance policies.[70] Also, as discussed in the next subsection, cyber insurance policies often cover the cost of retaining outside legal counsel.[71]

Because coverage determinations and premiums are based on risk, cyber insurance can also incentivize better cyber hygiene and adherence to practices that

[64] IBM, 2021 COST OF A DATA BREACH REPORT 8 (2021).
[65] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 21-477, CYBER INSURANCE: INSURERS AND POLICYHOLDERS FACE CHALLENGES IN AN EVOLVING MARKET 4 (2021).
[66] NAT'L ASS'N INS. COMMISSIONERS, REPORT ON THE CYBERSECURITY INSURANCE MARKET 7 (2021).
[67] *Id.* at 5.
[68] *See* Adrejia Boutte Swafford, *Cyber Risk Insurance: Law Firms Need It, Too*, 67 LA. B. J. 326, 328 (2020).
[69] Adrejia Boutte Swafford, *Cyber Risk Insurance: Law Firms Need It, Too*, 67 LA. B. J. 326, 329 (2020).
[70] *Ransomware*, NAT'L ASS'N OF INSURANCE COMMISSIONERS (Aug. 25, 2021), https://content.naic.org/cipr_topics/topic_ransomware.htm.
[71] *See generally* Part III.C.2.

reduce the risk of ransomware attacks.[72] These include discouraging policyholders from configuring their networks in ways that expose them to unnecessary risk.[73] Policyholders have a significant interest in trying to implement these measures because doing so demonstrates to insurers that the policyholder has an effective cybersecurity program that reduces cyber risk, thereby reducing insurance premiums.[74] Nonetheless, cyber insurance may also incentivize ransomware attackers by assuring payment of the ransom.[75] As discussed below, some ransomware attackers will even seek out cyber insurance policy information to aid in their negotiations with victims.

Although more companies now have cyber insurance policies, there is still significant cost uncertainty in this market.[76] More attacks mean more demand for cyber insurance, but also higher premiums as insurers take on more risk.[77] During the last quarter of 2020 alone, a survey of insurance brokers showed a 10 to 30 percent increase in cyber insurance prices.[78] In a similar way, the attack frequency and severity has caused insurers to scale back cyber coverage for at-risk sectors like healthcare and education.[79]

To minimize risk, many cyber insurance providers now rely on reinsurance.[80] Reinsurance allows insurers to mitigate risk by insuring the policy they are providing to a customer with a third-party insurer in return for a percentage of the premiums.[81] Outsized risk for insurers could cause significant changes to the cyber insurance products offered to customers or even a decline in the number of insurers offering cyber policies altogether.[82] According to one cyber insurer, this scenario

[72] *Cf.* CARNEGIE ENDOWMENT FOR INT'L PEACE, ADDRESSING THE PRIVATE SECTOR CYBERSECURITY PREDICAMENT: THE INDISPENSABLE ROLE OF INSURANCE 11 (2018).

[73] *Id.*

[74] *See* Tristan Hinsley & Holden Wegner, *The rising tide of cyber insurance premiums in the age of ransomware*, SECURITY MAGAZINE (Nov. 18, 2021), https://www.securitymagazine.com/articles/96549-the-rising-tide-of-cyber-insurance-premiums-in-the-age-of-ransomware.

[75] *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, U.S. DEP'T OF TREASURY (Oct. 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

[76] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 21-477, CYBER INSURANCE: INSURERS AND POLICYHOLDERS FACE CHALLENGES IN AN EVOLVING MARKET 8 (2021).

[77] *Id.*

[78] NAT'L ASS'N INS. COMMISSIONERS, REPORT ON THE CYBERSECURITY INSURANCE MARKET 6 (2021).

[79] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 21-477, CYBER INSURANCE: INSURERS AND POLICYHOLDERS FACE CHALLENGES IN AN EVOLVING MARKET 8 (2021).

[80] Tristan Hinsley & Holden Wegner, *The rising tide of cyber insurance premiums in the age of ransomware*, SECURITY MAGAZINE (Nov. 18, 2021), https://www.securitymagazine.com/articles/96549-the-rising-tide-of-cyber-insurance-premiums-in-the-age-of-ransomware.

[81] *Id.*

[82] Tom Johansmeyer, *Cybersecurity Insurance Has a Big Problem*, HARVARD BUS. REV. (Jan. 11, 2021), https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem.

would remove a valuable risk management strategy for organizations with substantial cyber exposure.[83]

2. Outside Legal Counsel

One way companies constrain liability after ransomware attacks is by retaining outside counsel immediately after a cyber incident is confirmed.[84] According to a recent CrowdStrike report, 49 percent of the company's incident response engagements were referred to CrowdStrike by third-party counsel.[85]

By retaining outside counsel, victims may be able to protect some details of its investigation from disclosure under the attorney-client privilege.[86] It is common for victims to delegate their incident response efforts to outside counsel.[87] The outside counsel then retains third-party experts to help respond to the incident, including cybersecurity response firms.[88] As a result, organizations often assert the attorney-client privilege and work-product doctrine to shield documents and opinions of third-party firms retained by the outside counsel from discovery.[89] Organizations bear the burden of demonstrating those communications were for the purpose legal counsel or the documents were prepared in reasonable anticipation of litigation.[90]

The issue of whether third-party investigative documents were prepared for the purpose of legal advice or in anticipation of litigation, and thus shielded from discovery, is complicated and often the subject of litigation.[91] Target's 2013 data breach is an example of when a court determined the attorney-client privilege protected third-party investigative documents.[92] After Target discovered the breach, the company launched a dual-track investigation.[93] On the first track, Target retained Verizon to conduct a non-privileged investigation examining how

[83] *Id.*
[84] *See* infra section 2; *see also* Robert Lemos, *Breach Response Shift: More Lawyers, Less Cyber-Insurance Coverage*, DARK READING (Jan. 10, 2022), https://www.darkreading.com/attacks-breaches/changes-to-breach-response-more-lawyers-less-cyber-coverage.
[85] CROWDSTRIKE, CROWDSTRIKE SERVICES CYBER FRONT LINES REPORT 15 (2021).
[86] Brian Mund & Leonard Bailey, *Privilege in Data Breach Investigations*, 69 DOJ J. FED. L. & PRAC. 39, 41 (2021).
[87] *Id.*
[88] *Id.*
[89] *Id.* at 43, 45.
[90] *Id.*
[91] Todd Presnell & Benjamin William Perry, *A Tale of Two Functions: Weighing Business and Legal Considerations in the Wake of a Data Breach to Preserve Attorney-Client Privilege and Work Product Protections*, NAT. L. REV. (Mar. 9, 2022), https://www.natlawreview.com/article/tale-two-functions-weighing-business-and-legal-considerations-wake-data-breach-to.
[92] *In re Target Corp. Customer Data Security Breach Litigation*, MDL No. 14–2522, 2015 WL 6777384, at 2–3 (D. Minn. Oct. 23, 2015).
[93] *Id* at 2.

the breach occurred and to develop an appropriate response.[94] With the second track, Target created its own "Data Breach Task Force" and according to a Target court filing engaged a separate Verizon team "to enable counsel to provide legal advice to Target, including legal advice in anticipation of litigation and regulatory inquiries."[95] Target only asserted privilege for documents created during the second track investigation.[96]

The plaintiffs suing Target argued none of the investigative documents prepared by Verizon should be protected by attorney-client or work product privilege.[97] The plaintiffs claimed the assertion of privilege was improper because "Target would have had to investigate and fix the data breach regardless of any litigation to appease its customers and ensure continued sales, discover its vulnerabilities, and protect itself against future breaches."[98] The court sided with Target holding "the Data Breach Task Force was focused not on the remediation of the breach, as Plaintiffs contend, but on informing Target's in-house and outside counsel about the breach so that Target's attorneys could provide the company with legal advice and prepare to defend the company in litigation."[99]

Marriott's 2018 breach is another example of the attorney-client and work product privilege protecting third-party investigative documents. When Marriott identified the breach, the company retained the law firm BakerHostetler to investigate the incident.[100] BakerHostetler then entered a new statement of work with IBM on behalf of Marriott "to assist BakerHostetler in providing legal advice to Marriott."[101]

The plaintiffs suing Marriott claimed all documents generated during the investigation were not privileged because IBM and Marriott had a pre-existing business relationship and the "the services IBM provided after the breach were the same kind of services IBM provided before the breach."[102] The court rejected the plaintiffs' claims reasoning "that the post-November 2018 work yielded a result or results similar to the work done before that date cannot negate the universal agreement of the witnesses that Marriott had retained IBM for a specific purpose—to aid [BakerHostetler] in [its] defense of Marriott."[103]

[94] *Id.*

[95] *Id.* at 1 (internal quotation marks omitted).

[96] *Id.*

[97] *Id.*

[98] *Id.*

[99] *Id.* at 3; *In re Target Corp. Customer Data Security Breach Litigation*, MDL No. 14–2522, 2015 WL 6777384, at 3 (D. Minn. Oct. 23, 2015).

[100] *In re Marriott International Inc. Customer Data Security Breach Litigation*, MDL No. 19-MD-2879, 2021 WL 2660180, at 3 (D. Md. Jun. 29, 2021).

[101] *Id.* at 5.

[102] *Id.* at 3.

[103] *Id.* at 6.

Unlike Target and Marriott, healthcare insurance company Premera was unable to assert the attorney-client or work product privileges to protect third-party investigative documents after its breach in 2015. Before discovering the breach, Premera hired Mandiant in October 2014 to review its data management system.[104] After the breach in February 2015, Premera hired outside counsel in anticipation of litigation.[105] The next day, Premera amended its existing statement of work with Mandiant and shifted supervision over Mandiant from the company to outside counsel.[106] This amended statement of work "did not otherwise change the scope of Mandiant's work from what was described in the Master Services Agreement between Mandiant and Premera entered into on October 10, 2014."[107]

The court distinguished Premera from Target saying "[w]ith Premera . . . there was only one investigation, performed by Mandiant, which began at Premera's request."[108] Although supervision was later shifted to outside counsel, this "by itself, is not sufficient to render all of the later communications and underlying documents privileged or immune from discovery as work product."[109]

Moreover, unlike Marriott, Premera did not articulate a separate and distinct purpose for the post-breach investigative work.[110] Concluding privilege did not apply, the court ruled "the amended statement of work did not change the scope of work and there is no evidence that Mandiant changed its scope or purpose at the direction of outside counsel."[111]

3. Cyber Incident Response Firms

As discussed in the case law above, cyber incident response firms help victim companies understand the impact of cyber incidents and devise an effective response. Assistance from these firms is necessary for most victims because it is difficult to know the appropriate investigative procedures, data collection, reporting requirements, and legal precautions a victim must take to understand an incident.[112]

Once retained, cyber firms provide several services to mitigate incident impact. Among other things, these services include dispatching on-site experts to

[104] *In re Premera Blue Cross Customer Data Security Breach Litigation*, 296 F. Supp. 3d 1230, 1245 (D. Or. 2017).
[105] *Id.*
[106] *Id.*
[107] *Id.*
[108] *Id.*
[109] *Id.*
[110] *Id.* at 1246.
[111] *Id.*
[112] CTR. FOR INTERNET SEC., CIS CONTROL 17: INCIDENT RESPONSE MANAGEMENT (2022), https://controls-assessment-specification.readthedocs.io/en/stable/control-17/.

triage the incident response.[113] These experts then conduct an investigation to identify the relevant threat vector, neutralize escalation, and work to maintain victim business continuity.[114] To achieve this, incident response professionals often stand up around the clock security operations centers to monitor threats.[115]

For companies seeking a more proactive approach, cyber incident response firms offer their services on a retainer basis.[116] Retainer services help companies optimize "remediation measures with advanced planning, forward-deployed capabilities and on-demand resources for incident response."[117] Pre-deploying cyber defense capabilities can help shorten incident response times when attacks do occur.[118]

Incident response firms not only help victims remediate and contain incidents, but also make recommendations for how victims can implement more resilient cyber defenses.[119] Recommendations often include cyber best practices like offline backups, endpoint detection, behavior-based detection, and multi-factor authentication.[120]

4. Ransomware Payment Negotiators

Ransomware created a new niche market for ransom negotiators that did not exist a few years ago.[121] There are now roughly a half-dozen ransomware negotiation companies who help victims "navigate the world of cyber extortion."[122] As more victims rely on these experts, some have criticized ransom negotiators for facilitating payments to criminal hackers.[123]

[113] *See, e.g., Modern Ransomware and Incident Response Solutions*, MANDIANT, https://www.mandiant.com/resources/modern-ransomware.

[114] *Modern Ransomware and Incident Response Solutions*, MANDIANT, https://www.mandiant.com/resources/modern-ransomware.

[115] *Id.*

[116] *See, e.g., Rapid Response Retainer,* VERIZON (2022), https://www.verizon.com/business/products/security/incident-response-investigation/rapid-response-retainer/?_ga=2.114554183.1531745227.1644877823-843136888.1644877823.

[117] *Rapid Response Retainer,* VERIZON (2022), https://www.verizon.com/business/products/security/incident-response-investigation/rapid-response-retainer/?_ga=2.114554183.1531745227.1644877823-843136888.1644877823.

[118] *Id.*

[119] *See, e.g.,* CROWDSTRIKE, CROWDSTRIKE SERVICES CYBER FRONT LINES REPORT 23 (2021).

[120] CROWDSTRIKE, CROWDSTRIKE SERVICES CYBER FRONT LINES REPORT 23–24 (2021).

[121] Rachel Monroe, *How to Negotiate with Ransomware Hackers*, NEW YORKER (May 31, 2021), https://www.newyorker.com/magazine/2021/06/07/how-to-negotiate-with-ransomware-hackers.

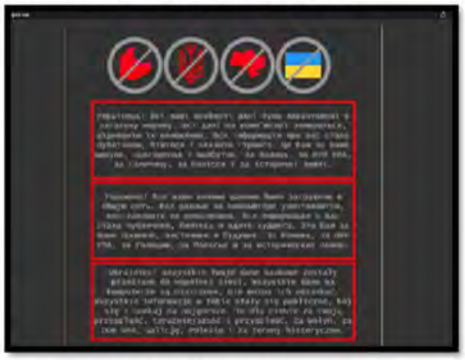
[122] *Id.*

[123] *Id.*

Negotiations with ransomware gangs often take place over a short time period using instant messaging platforms.[124] Because many hackers are not native English speakers, "one-sentence messages from the hackers in broken English is the norm."[125] Entire negotiations sometimes conclude after only ten to fifteen exchanges with attackers.[126]

Experienced ransomware negotiators give victim companies an edge at the bargaining table because they have detailed profiles on ransomware groups they have dealt with in the past.[127] The profiles detail standard threat actor operations, including past ransom demand patterns.[128] This allows victims to enter negotiations with a clear strategy and avoid expensive mistakes with hackers.[129]

These mistakes include aggressive negotiation tactics and quickly offering to increase ransom demand counteroffers which signals to adversaries that there is more money on the table.[130] Ransomware groups have also begun stealing victims' cyber insurance policies so they know the deductible and coverage limits of their victims—key information in the negotiation.[131]



Example of Defaced Ukrainian Government Website
Source: Nick Biasini et. al, Ukraine Campaign Delivers Defacement and Wipers, in Continued Escalation, CISCO TALOS *(Jan. 21, 2022), https://blog.talosintelligence.com/2022/01/ukraine-campaign-delivers-defacement.html*

D. Russian Cyber Aggression

Well before its unlawful and unprovoked invasion of Ukraine, Russia executed several coordinated cyberattack campaigns against Ukraine and other

[124] Brian Fung & Clare Sebastian, *What it's really like to negotiate with ransomware attackers*, CNN (Jul. 13, 2021), https://www.cnn.com/2021/07/13/tech/ransomware-negotiations/index.html.
[125] *Id.*
[126] *Id.*
[127] *Id.*
[128] *Id.*
[129] *Id.*
[130] Rachel Monroe, *How to Negotiate with Ransomware Hackers*, NEW YORKER (May 31, 2021), https://www.newyorker.com/magazine/2021/06/07/how-to-negotiate-with-ransomware-hackers.
[131] Brian Fung & Clare Sebastian, *What it's really like to negotiate with ransomware attackers*, CNN (Jul. 13, 2021), https://www.cnn.com/2021/07/13/tech/ransomware-negotiations/index.html.

eastern European countries.[132] Indeed, researchers and government agencies have attributed dozens of debilitating attacks on eastern European countries to Russia since 2007.

In April 2007, Russia orchestrated a Denial of Service (DDOS) attack against Estonia.[133] The attack impacted Estonian government websites, parliament, banks, ministries, newspapers, and broadcasters.[134] Russia executed another DDOS attack against Georgia in August 2008 impacting 54 Georgian websites and 90 percent of state institution websites.[135] The attack left the Georgian government barely able to communicate on the Internet.[136] In 2009, Russia launched DDOS attacks against Kyrgyzstan's two primary internet servers for the country's websites and email.[137] The attack came on the same day Russia was pressuring Kyrgyzstan to cut off United States access to Manas Air Base.[138]

Following anti-government protests in March 2014, Russia likely deployed "snake" malware against the Ukrainian Prime Minister's Office and several Ukrainian embassies.[139] According to a subsequent report by BAE Systems, the snake malware provided full remote access and was difficult to detect because of its ability to remain inactive for several days.[140] In March 2015, another likely Russian malware campaign—Operation Potao Express—targeted the Ukrainian government, military, and one major Ukrainian news agency.[141] In December 2015, Russia used malware to compromise three Ukrainian power companies causing

[132] *See, e.g.*, Press Release, Ukraine Ministry of Digital Transformation, Russia Intends to Reduce Trust in the Government with Fakes About the Vulnerability of Critical Information Infrastructure and the "Drain" of Ukrainian Data (Jan. 16, 2022), https://thedigital.gov.ua/news/rosiya-mae-namir-zniziti-doviru-do-vladi-feykami-pro-vrazlivist-kritichnoi-informatsiynoi-infrastrukturi-ta-zliv-danikh-ukraintsiv (translated to English); *see also, e.g.*, Brad Smith, *Digital technology and the war in Ukraine*, Microsoft (Feb. 28, 2022), *https*://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/; Robert Falcone, Mike Harbison, & Josh Grunzweig, *Threat Brief: Ongoing Russia and Ukraine Cyber Conflict*, Palo Alto Networks (Jan. 20, 2022), https://unit42.paloaltonetworks.com/ukraine-cyber-conflict-cve-2021-32648-whispergate/

[133] U.S. Dep't of State, Integrated Country Strategy: Estonia 3 (Jan. 2021), https://www.state.gov/wp-content/uploads/2021/01/ICS_EUR_Estonia_Public-Release.pdf.

[134] Eur. Union Inst. for Sec. Studies, Hacks, leaks, and disruptions: Russian cyber strategies 18–19 (Oct. 2018), https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf.

[135] *Id.* at 59.

[136] Stephen W. Korns & Joshua E. Kastenberg, *Georgia's Cyber Left Hook*, U.S. Army War College (2008), https://apps.dtic.mil/sti/pdfs/ADA636632.pdf.

[137] Maj. William C. Ashmore, *Impact of Alleged Russian Cyber Attacks*, U.S. Army Command & Gen. Staff College (2009), https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-027.pdf.

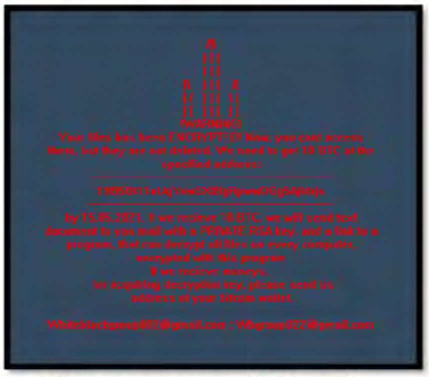
[138] *Id.*

[139] Chester Wisniewski, *Cyberthreats during Russian-Ukrainian tensions: what can we learn from history to be prepared?* Sophos (updated Mar. 7, 2022), https://news.sophos.com/en-us/2022/02/22/cyberthreats-during-russian-ukrainian-tensions-what-can-we-learn-from-history-to-be-prepared/.

[140] BAE Systems, The Snake: Cyber Espionage Toolkit 33 (2014).

[141] ESET, Operation Potao Express: Analysis of a cyber-espionage toolkit 2, 14 (2015), https://www.welivesecurity.com/wp-content/uploads/2015/07/Operation-Potao-Express_final_v2.pdf.

power outages for roughly 225,000 customers.[142] These campaigns reportedly include defacing websites as shown in the adjacent graphic. Other examples related to the subject of this report include deploying wiper malware disguised as ransomware that targets and deletes startup files and user data.[143] According to analysis by Ukraine's State Service of Special Communication and Information Protection (SSCIP), the malware, dubbed "WhisperKill," masquerades as ransomware.[144] Both SSCIP and Cisco's Talos Cyber Intelligence Group identified WhisperKill as similar and likely a modification of previously seen ransomware, WhiteBlackCrypt (encrypt3d).[145] When deployed, it encrypts the contents of the Master Boot Record (MBR) and C:\ partition of the system, likely in a false-flag attempt to disguise its true origins and intent. [146] WhisperKill's fake ransom note contained a trident—also part of the Ukrainian coat of arms—



!WARNING!

Your files has been ENCRYPTED! Now, you cant access them, but they are not deleted. We need to get 10 BTC at the specified address:

19BSBt11aUqYnwSXBgRpwwDGg5Ajirbjn

by 15.05.2021. If we recieve 10 BTC, we will send text document to you mail with a PRIVATE RSA key, and a link to a program, that can decrypt all files on every computer, encrypted with this program.
If we recieve moneys,
for acquiring decryption key, please send us
address of your bitcoin wallet.

Whiteblackgroup002@gmail.com ; Wbgroup022@gmail.com

Fake ransom message presented by WhisperKill.
Source: Ukraine State Service of Special Communications & Information Protection, Information on the Possible Provocation (Jan. 26, 2022), https://cip.gov.ua/services/cm/api/attachment/download/44480

[142] *ICS Alert (IR-ALERT-H16-056-01: Cyber-Attack Against Ukrainian Critical Infrastructure*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (revised Jul. 20, 2021), https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01.

[143] Ukraine State Service of Special Communication and Information Protection (SSCIP), Information on the Possible Provocation (Jan. 26, 2022), https://cip.gov.ua/services/cm/api/attachment/download/44480; Nick Biasini et. al, Ukraine Campaign Delivers Defacement and Wipers, in Continued Escalation, CISCO TALOS (Jan. 21, 2022), , https://blog.talosintelligence.com/2022/01/ukraine-campaign-delivers-defacement.html.

[144] Ukraine State Service of Special Communication and Information Protection (SSCIP), Information on the Possible Provocation, https://cip.gov.ua/services/cm/api/attachment/download/44480 (Jan. 26, 2022 13:35).

[145] Ukraine State Service of Special Communication and Information Protection (SSCIP), Information on the Possible Provocation (Jan. 26, 2022), https://cip.gov.ua/services/cm/api/attachment/download/44480; Nick Biasini et. al, Ukraine Campaign Delivers Defacement and Wipers, in Continued Escalation, CISCO TALOS (Jan. 21, 2022), , https://blog.talosintelligence.com/2022/01/ukraine-campaign-delivers-defacement.html.

[146] A false-flag is the fabrication of pretext to justify an invasion. Press Release, U.S. Dep't of Defense, Pentagon Press Secretary John F. Kirby Holds a Press Briefing (Feb. 3, 2022), https://www.defense.gov/News/Transcripts/Transcript/Article/2922998/pentagon-press-secretary-john-f-kirby-holds-a-press-briefing/. Ukraine State Service of Special Communication and Information Protection (SSCIP), Information on the Possible Provocation (Jan. 26, 2022), https://cip.gov.ua/services/cm/api/attachment/download/44480; Nick Biasini et. al, Ukraine Campaign Delivers Defacement and Wipers, in Continued Escalation, CISCO TALOS (Jan. 21, 2022), , https://blog.talosintelligence.com/2022/01/ukraine-campaign-delivers-defacement.html.

bolstering SSCIP's assessment this was a false flag attack.[147]

In short, WhisperKill was disguised to be motivated by financial or ideological considerations, instead of a destructive Russian-sponsored attack.[148] Unlike ransomware, however, WhisperKill deletes the decryption key after completing the encryption operation, making it impossible to decrypt the data, even if the victim pays the ransom. [149] This makes WhisperKill a useless tool for ransomware attackers because victims will never pay the ransom. From the user's perspective, all their data is deleted irrecoverably.

WhisperKill is not Ukraine's first experience with wiper malware masquerading as ransomware. In June 2017, Ukraine was hit with an aggressive wiper malware called NotPetya, with similar characteristics to WhisperKill, including masquerading as ransomware and destroying the MBR.[150] The White House, publicly attributed the NotPetya attack to the Russian military, describing it as "the most destructive and costly cyber-attack in history . . . causing billions of dollars in damage" and "part of the Kremlin's ongoing effort to destabilize Ukraine and demonstrat[ing] ever more clearly Russia's involvement in the ongoing conflict."[151] The statement went on to call it "a reckless and indiscriminate cyber-attack that will be met with international consequences."[152] The following month, in response to Russia's "significant efforts to undermine U.S. cybersecurity," the United States imposed sanctions against Russian intelligence agencies and officials.[153]

Both Ukraine and the United States have warned that U.S. agencies and critical infrastructure could be Russia's next target in retaliation for our unwavering support of Ukraine.[154]

[147] Ukraine State Service of Special Communication and Information Protection (SSCIP), Information on the Possible Provocation (Jan. 26, 2022), https://cip.gov.ua/services/cm/api/attachment/download/44480 (translated to English).

[148] *Id.*

[149] *Id.*

[150] Release, White House, Statement from the Press Secretary (Feb. 15, 2018), https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/; Nick Biasini et. al, Ukraine Campaign Delivers Defacement and Wipers, in Continued Escalation, CISCO TALOS (Jan. 21, 2022), , https://blog.talosintelligence.com/2022/01/ukraine-campaign-delivers-defacement.html.

[151] Release, White House, Statement from the Press Secretary (Feb. 15, 2018), https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/.

[152] *Id.*

[153] Fact Sheet, White House, President Donald J. Trump is Standing Up To Russia's Malign Activities (Apr. 6, 2018), https://trumpwhitehouse.archives.gov/briefings-statements/president-donald-j-trump-standing-russias-malign-activities/.

[154] Ukraine Ministry of Digital Transformation, Russia Intends to Reduce Trust in the Government with Fakes About the Vulnerability of Critical Information Infrastructure and the "Drain" of Ukrainian Data (Jan. 16, 2022), https://thedigital.gov.ua/news/rosiya-mae-namir-zniziti-doviru-do-vladi-feykami-pro-vrazlivist-kritichnoi-informatsiynoi-infrastrukturi-ta-zliv-danikh-ukraintsiv

E. Notable Known Ransomware Attacks

In the last year, several ransomware attacks caused substantial disruptions to critical industry sectors. Three examples include the attacks on Colonial Pipeline, JBS Foods, and Kaseya. Each is profiled in greater detail below.

1. Colonial Pipeline

Based in Georgia, Colonial Pipeline (Colonial) operates the largest refined fuel pipeline in the United States.[155] Spanning more than 5,500 miles, Colonial provides roughly half of the transportation fuel consumed on the East Coast and provides energy to more than 50 million Americans.[156] The United States Senate Committee on Homeland Security and Government Affairs held a hearing on the attack on June 8, 2021 with Colonial Pipeline Chief Executive Officer (CEO) Joseph Blount.[157]

Colonial detected its attack in the early morning of May 7, 2021 after an employee discovered the ransom note.[158] To contain the attack, Colonial initiated the shutdown process soon after discovery.[159] In just over an hour, Colonial shut down operations for all 5,500 miles of the pipeline.[160] It total, Blount testified that it took Colonial "fifteen minutes to close down the conduit, which has about 260 delivery points across 13 states and Washington, D.C."[161]

(translated to English); *Shields Up*, CYBERSECURITY & INFRA. SEC. AGENCY, https://www.cisa.gov/shields-up.

[155] *About Us/Our Company*, COLONIAL PIPELINE, https://www.colpipe.com/about-us/our-company.

[156] *Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 117th Cong. (2021) (testimony of Joseph Blount, President & Chief Executive Officer, Colonial Pipeline Company).

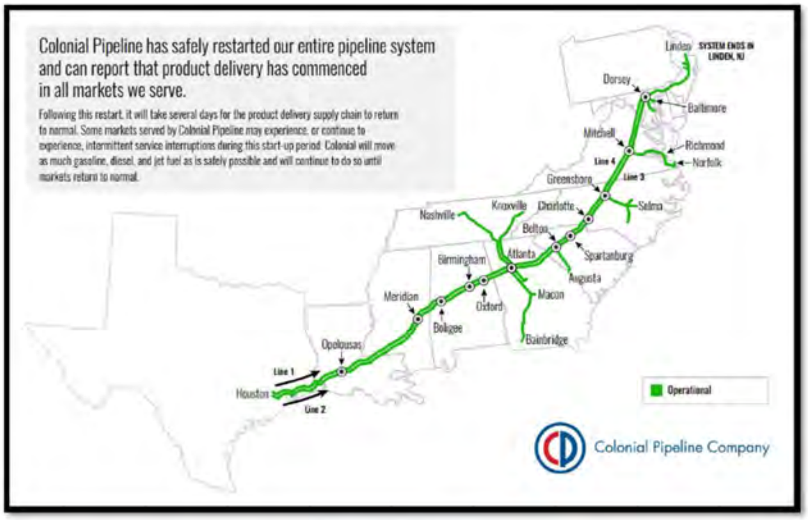
[157] *See generally Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 117th Cong. (2021).

[158] *Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 117th Cong. (2021) (written testimony of Joseph Blount, President & Chief Executive Officer, Colonial Pipeline Company).

[159] *Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 117th Cong. (testimony of Joseph Blount, President & Chief Executive Officer, Colonial Pipeline Company).

[160] *Id.*

[161] *Id.*



Colonial Pipeline has safely restarted our entire pipeline system and can report that product delivery has commenced in all markets we serve.

Following this restart, it will take several days for the product delivery supply chain to return to normal. Some markets served by Colonial Pipeline may experience, or continue to experience, intermittent service interruptions during this start-up period. Colonial will move as much gasoline, diesel, and jet fuel as is safely possible and will continue to do so until markets return to normal.

Colonial Pipeline Map
Source: Press Release, Colonial Pipeline, Media Statement Update: Colonial Pipeline System Disruption (May 17, 2021), https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption.

By the evening of May 7th, Blount made the decision to negotiate with the attackers and paid a $4.4 million ransom the next day.[162] Blount called this "one of the hardest decisions I have had to make in my life," but believed "restoring critical infrastructure as quickly as possible, in this situation, was the right thing to do for the country."[163] Colonial's shutdown led to the highest gas prices in six and a half years and left thousands of East Coast gas stations without fuel.[164] On May 17th, Colonial issued a press release saying its normal operations were restored and it was "transporting refined products at normal levels."[165]

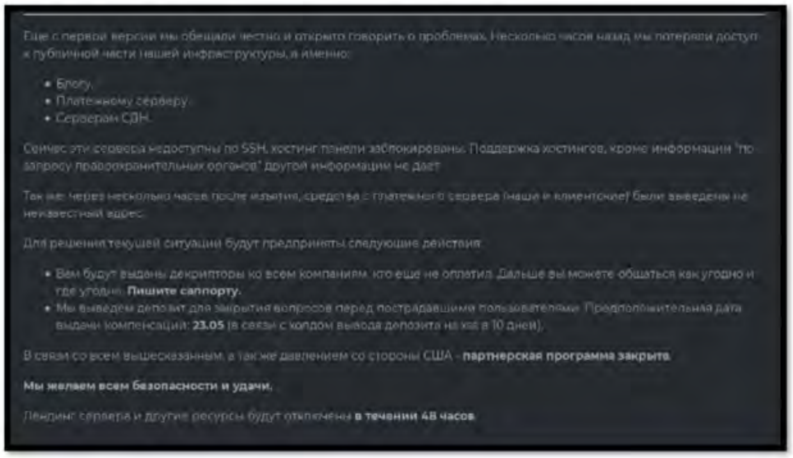
[162] *Id.*

[163] *Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 117th Cong. (2021) (written testimony of Joseph Blount, President & Chief Executive Officer, Colonial Pipeline Company).

[164] Collin Eaton & Dustin Volz, *Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom*, WALL ST. J. (May 19, 2021), https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636.

[165] Press Release, Colonial Pipeline, Media Statement Update: Colonial Pipeline Systems Disruption (May 17, 2021), https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption.

The FBI attributed the attack on Colonial to a criminal gang based in Russia, known as DarkSide.[166] On May 13th, just days after Colonial discovered the attack, DarkSide announced it lost access to its attack infrastructure and discontinued all operations.[167] A screenshot of the message DarkSide sent to its affiliates is pictured below. Translated to English, the message says "due to pressure from the U.S., the affiliate program is closed. Stay safe and good luck."[168]



Еще с первой версии мы обещали честно и открыто говорить о проблемах. Несколько часов назад мы потеряли доступ к публичной части нашей инфраструктуры, а именно:

- Блогу.
- Платежному серверу.
- Серверам CDN.

Сейчас эти сервера недоступны по SSH, хостинг панели заблокированы. Поддержка хостингов, кроме информации "по запросу правоохранительных органов" другой информации не дает.

Так же, через несколько часов после изъятия, средства с платежного сервера (наши и клиентские) были выведены на неизвестный адрес.

Для решения текущей ситуации будут предприняты следующие действия:

- Вам будут выданы декрипторы ко всем компаниям, кто еще не оплатил. Дальше вы можете общаться как угодно и где угодно. **Пишите саппорту.**
- Мы выведем депозит для закрытия вопросов перед пострадавшими пользователями. Предположительная дата выдачи компенсации: **23.05** (в связи с холдом вывода депозита на ххх в 10 дней).

В связи со всем вышесказанным, а так же давлением со стороны США - **партнерская программа закрыта.**

Мы желаем всем безопасности и удачи.

Лендинг сервера и другие ресурсы будут отключены **в течении 48 часов.**

DarkSide Closure Message to Affiliates
Source: The moral underground? Ransomware operators retreat after Colonial Pipeline hack, INTEL 471 (May 14, 2021), https://intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime.

In June, the Department of Justice (DOJ) recovered roughly $2.3 million of Colonial's initial ransom payment.[169] After paying the ransom to DarkSide, Colonial sent the FBI the Bitcoin address where the company transmitted the

[166] Press Release, Fed. Bureau of Investigation, FBI Statement on Compromise of Colonial Pipeline Network (May 10, 2021), https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks; Press Release, FBI Deputy Director Paul M. Abbate's Remarks at Press Conference Regarding the Ransomware Attack on Colonial Pipeline (Jun. 7, 2021), https://www.fbi.gov/news/pressrel/press-releases/fbi-deputy-director-paul-m-abbates-remarks-at-press-conference-regarding-the-ransomware-attack-on-colonial-pipeline.

[167] *The moral underground? Ransomware operators retreat after Colonial Pipeline hack*, INTEL 471 (May 14, 2021), https://intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime.

[168] *Id.*

[169] Press Release, U.S. Dep't of Justice, Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (Jun. 7, 2021), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

payment.[170] Investigators then traced the funds through several addresses before landing at a specific address for which the United States Government had a private key allowing it to seize the illicit funds.[171]

2. JBS Foods

JBS Foods (JBS) is the world's largest beef producer and a leading chicken and pork supplier in the United States.[172] JBS has operations around the world, including in the United States, Australia, United Kingdom, Mexico, Brazil, and Canada.[173]

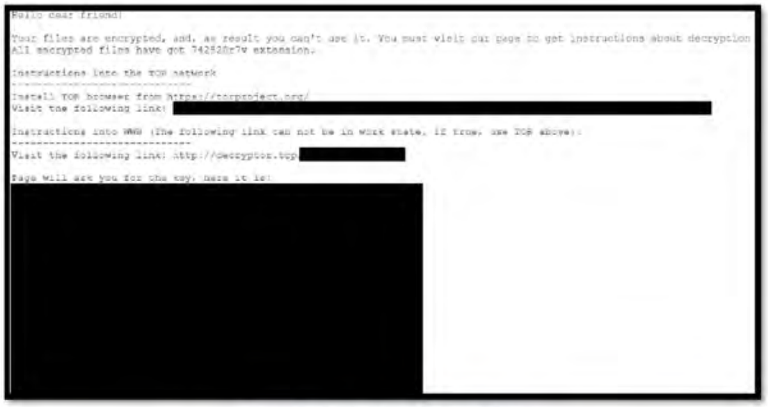
Closed JBS Plant on June 1, 2021
Source: Derek B. Johnson, Ransomware, SolarWinds forced cybersecurity into public's consciousness, says CISA chief, SC MEDIA (Nov. 10, 2021), https://www.scmagazine.com/analysis/policy/ransomware-solarwinds-forced-cybersecurity-into-publics-consciousness-says-cisa-chief?es_p=13943087.

On May 30, 2021, JBS's American subsidiary, JBS USA, announced it "determined that it was the target of an organized cybersecurity attack, affecting

[170] Aff. In Support of App. for a Seizure Warrant at ¶28, June 7, 2021, 3:21-mj-70945-LB, https://www.justice.gov/opa/press-release/file/1402056/download.
[171] *Id.* at ¶¶ 29–34; Press Release, U.S. Dep't of Justice, Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (Jun. 7, 2021), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside. Private keys allow users to make digital currency transfers. *Questions on Virtual Currency*, U.S. DEP'T OF TREASURY (Oct. 15, 2021), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/559.
[172] *Our Business*, JBS FOODS, https://jbsfoodsgroup.com/our-business.
[173] *Id.*

some of the servers supporting its North American and Australian IT systems."[174] After discovery, JBS reported it shut down all affected systems, notified relevant authorities, and retained third-party IT experts to resolve the situation.[175] JBS's announcement also added "the company's backup servers were not affected, and it is actively working with an [i]ncident [r]esponse firm to restore its systems as soon as possible."[176]

JBS's initial announcement did not explicitly mention a ransomware attack, but the FBI attributed the incident to the notorious Russia-based ransomware group REvil on June 2nd.[177] On June 9th, JBS made an $11 million ransom payment to REvil saying, "this decision had to be made to prevent any potential risk for our customers."[178] Public reports indicate REvil's initial ransom demand was $22.5 million.[179] Below is an example of an REvil ransom note.



```
Hello dear friend!

Your files are encrypted, and, as result you can't use it. You must visit our page to get instructions about decryption
All encrypted files have got 742520r7v extension.

Instructions into the TOR network
-----------------------------
Install TOR browser from https://torproject.org/
Visit the following link: [redacted]

Instructions into WWW (The following link can not be in work state, if true, use TOR above):
-----------------------------
Visit the following link: http://decryptor.top[redacted]

Page will ask you for the key, here it is:
[redacted]
```

Example of REvil Ransomware Note
Source: Email from U.S. Senate Sergeant at Arms to Committee staff (Mar. 11, 2022) (on file with the Committee).

[174] Press Release, JBS USA, LLC, Media Statement: JBS USA Cybersecurity Attack (May 31, 2021), https://www.globenewswire.com/news-release/2021/05/31/2239049/17532/en/Media-Statement-JBS-USA-Cybersecurity-Attack.html.

[175] *Id.*

[176] *Id.*

[177] Press Release, Fed. Bureau of Investigation, FBI Statement on JBS Cyberattack (Jun. 2, 2021), https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-jbs-cyberattack.

[178] Press Release, JBS USA, LLC, JBS USA Cyberattack Media Statement-June 9 (Jun. 9, 2021), https://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-june-9.

[179] Lawrence Abrams, *JBS paid $11 million to REvil ransomware, $22.5M first demanded*, BLEEPING COMPUTER (Jun. 10, 2021), https://www.bleepingcomputer.com/news/security/jbs-paid-11-million-to-revil-ransomware-225m-first-demanded/.

The attack shuttered several of the largest meat plants in the United States, including JBS facilities in Colorado, Iowa, Pennsylvania, Minnesota, Nebraska, and Texas compounding existing food supply chain strains from labor shortages and high transportation costs.[180] The U.S. Department of Agriculture issued a statement urging JBS competitors to ramp up their production to offset JBS's shutdown.[181]

3. Kaseya

Kaseya is a Miami-based software company that provides network management services.[182] Founded in 2000, more than 40,000 organizations use Kaseya's products globally, and its services help customers "efficiently manage, secure, and backup IT."[183]

Kaseya Headquarters
Source: Alex Marquardt, Ransomware group demands $70 million for Kaseya attack, CNN (Jul. 5, 2021), https://www.cnn.com/2021/07/05/business/ransomware-group-payment-kaseya/index.html.

Hackers targeted Kaseya's virtual systems administrator (VSA) software used by managed service providers to track and distribute software updates.[184] On July 3, 2021, Kaseya announced "a potential attack against the VSA that has been

[180] Jacob Bunge, *Meat Buyers Scramble After Cyberattack Hobbles JBS*, WALL ST. J. (Jun. 2, 2021), https://www.wsj.com/articles/meatpacker-jbs-hit-by-cyberattack-affecting-north-american-australian-operations-11622548864?mod=article_inline.

[181] Press Release, U.S. Dep't of Agric., Statement from the U.S. Department of Agriculture on JBS USA Ransomware Attack (Jun. 1, 2021), https://www.usda.gov/media/press-releases/2021/06/01/statement-us-department-agriculture-jbs-usa-ransomware-attack.

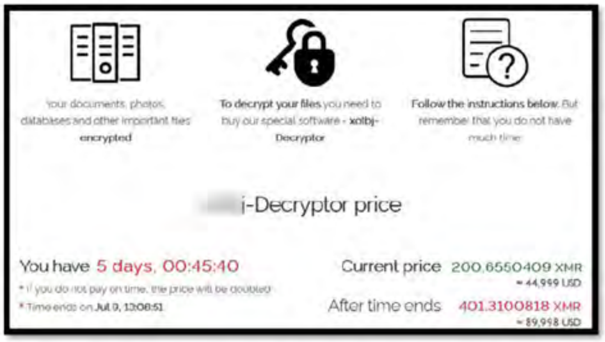
[182] *Contact Us*, KASEYA, https://www.kaseya.com/contact-us/; *We are Kaseya*, KASEYA, https://www.kaseya.com/company/.

[183] *We Are Kaseya*, KASEYA, https://www.kaseya.com/company/.

[184] *VSA*, Kaseya, https://www.kaseya.com/products/vsa/;Press Release, Continued Advisory, Kaseya (Jul. 4, 2021), https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689.

limited to a small number of on-premises customers."[185] After further investigation, the company announced its "VSA product has unfortunately been the victim of a sophisticated cyberattack."[186] Compromising this software allowed hackers to distribute ransomware through corrupted updates to Kaseya's broad customer base.[187] The attack was attributed to REvil, but Kaseya did not pay a ransom or communicate with the attackers.[188]

Kaseya estimates this supply chain attack compromised 60 direct customers and impacted roughly 1,500 downstream non-customers.[189] REvil issued a $70 million ransom demand to decrypt all impacted systems, but made demands between $25,000 and $5 million for individual victims to unlock their networks.[190] Below is a screenshot of one such demand.



Your documents, photos, databases and other important files **encrypted**

To decrypt your files you need to buy our special software - **xolbj-Decryptor**

Follow the instructions below. But remember that you do not have much time

[redacted]i-Decryptor price

You have 5 days, 00:45:40

* If you do not pay on time, the price will be doubled

* Time ends on **Jul 9, 13:08:51**

Current price 200.6550409 XMR
≈ 44,999 USD

After time ends 401.3100818 XMR
≈ 89,998 USD

REvil Ransom Demand to Kaseya Ransomware Victim
Source: Lawrence Abrams, REvil is increasing ransoms for Kaseya ransomware attack victims, BLEEPING COMPUTER (Jul. 4, 2021), https://www.bleepingcomputer.com/news/security/revil-is-increasing-ransoms-for-kaseya-ransomware-attack-victims/.

According to public reporting, the FBI had a decryption key obtained by accessing REvil's internal servers, but did not share the key with Kaseya victims for

[185] Press Release, Continued Advisory, Kaseya (Jul. 3, 2021), https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689.
[186] Press Release, Continued Advisory, Kaseya (Jul. 6, 2021), https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689.
[187] *Incident Overview & Technical Details*, KASEYA (2021), https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961.
[188] Press Release, Continued Advisory, Kaseya (Jul. 26, 2021), https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689.
[189] *Incident Overview & Technical Details*, KASEYA (2021), https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961.
[190] Robert McMillan, *Ransomware Hackers Demand $70 Million to Unlock Computers in Widespread Attack*, WALL ST. J. (Jul.5, 2021), https://www.wsj.com/articles/ransomware-hackers-demand-70-million-to-unlock-computer-in-widespread-attack-11625524076?mod=article_inline.

several weeks while the FBI planned an operation to disrupt REvil's criminal activity.[191] REvil's platform went offline before the FBI could execute this plan.[192]

The total number is unknown, but several Kaseya victims made ransom payments before the decryption key became available.[193] These payments reportedly ranged from $40,000 to $220,000.[194] Other impacted companies restored their systems from backups—a time consuming and expensive process.[195] Regardless, the downstream impact was substantial. For example, one downstream Kaseya victim, Swedish grocery store chain Coop closed 700 stores for six days, likely costing millions in lost revenue.[196]

F. REvil Arrests

Over the past year, several REvil hackers have been arrested. This includes the individuals allegedly responsible for the Kaseya and JBS attacks. One hacker, Yaroslav Vasinskyi, was arrested in Poland and extradited to the United States. In January 2022, Russian authorities claimed to arrest fourteen others.

1. Yaroslav Vasinskyi

On October 8, 2021, Polish authorities detained Yaroslav Vasinskyi as he crossed the border from Ukraine.[197] Vasinskyi, 22, is a Ukrainian national allegedly responsible for orchestrating the Kaseya attack.[198] In August 2021, a Federal grand jury in the United States indicted him for his role in the incident.[199]

The Department of Justice charged Vasinskyi with "conspiracy to commit fraud and related activity in connection with computers, substantive counts of

[191] Ellen Nakashima & Rachel Lerman, *FBI held back ransomware decryption key from businesses to run operation targeting hackers*, WASH. POST (Sept. 21, 2021), https://www.washingtonpost.com/national-security/ransomware-fbi-revil-decryption-key/2021/09/21/4a9417d0-f15f-11eb-a452-4da5fe48582d_story.html.

[192] *Id.*

[193] *Id.*

[194] OFFICE OF THE CYBER EXEC., NAT'L COUNTERINTELLIGENCE & SEC. CTR., KASEYA VSA SUPPLY CHAIN RANSOMWARE ATTACK (Aug. 10, 2021), https://www.odni.gov/files/NCSC/documents/SafeguardingOurFuture/Kaseya%20VSA%20Supply%20Chain%20Ransomware%20Attack.pdf.

[195] Ellen Nakashima & Rachel Lerman, *FBI held back ransomware decryption key from businesses to run operation targeting hackers*, WASH. POST (Sept. 21, 2021), https://www.washingtonpost.com/national-security/ransomware-fbi-revil-decryption-key/2021/09/21/4a9417d0-f15f-11eb-a452-4da5fe48582d_story.html.

[196] *Id.*

[197] Press Release, U.S. Dep't of Justice, Ukrainian Arrested and Charge with Ransomware Attack on Kaseya (Nov. 8, 2021), https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya.

[198] *Id.*

[199] Indictment at 1, United States v. Vasinskyi, 3-21CR0366-S (N.D. Tex. 2021).

damage to protected computers, and conspiracy to commit money laundering."[200] If convicted on all counts, Vasinskyi could face up to 145 years in prison.[201] On March 9, 2022, the United States successfully extradited and arraigned Vasinskyi in the Northern District of Texas.[202]

At the same time the Department of Justice disclosed Vasinskyi's arrest, it also announced the seizure of $6.1 million from another REvil hacker named Yevgeniy Polyanin.[203] Polyanin is a Russian national linked to "3,000 ransomware attacks that netted $13 million in ransom from entities across the United States."[204] He was separately charged with the same crimes as Vasinskyi.[205] Polyanin remains at large.[206]

2. Russian Federal Security Service Arrests

On January 14, 2022, Russia's Federal Security Service (FSB) arrested 14 alleged REvil gang members, including the individual senior U.S. officials claim was responsible for the Colonial Pipeline attack.[207] This individual switched to work for REvil after his previous gang, DarkSide, disappeared after the Colonial attack.[208]

[200] Press Release, U.S. Dep't of Justice, Ukrainian Arrested and Charged with Ransomware Attack on Kaseya (Nov. 8, 2021), https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya.

[201] *Id.*

[202] Press Release, U.S. Dep't of Justice, Sodinokibi/REvil Ransomware Defendant Extradicted to United States and Arraigned in Texas (Mar. 9, 2022), https://www.justice.gov/opa/pr/sodinokibirevil-ransomware-defendant-extradited-united-states-and-arraigned-texas.

[203] Press Release, U.S. Dep't of Justice, Ukrainian Arrested and Charge with Ransomware Attack on Kaseya (Nov. 8, 2021), https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya; *See also generally* United States v. Vasinskyi, 3-21CR0366-S (N.D. Tex. 2021).

[204] Press Release, U.S. Dep't of Justice, Ukrainian Arrested and Charged with Ransomware Attack on Kaseya (Nov. 8, 2021), https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya; Ellen Nakashima & Dalton Bennett, *Ring of ransomware hackers targeted by authorities in United States and Europe*, WASH. POST (Nov. 8, 2021), https://www.washingtonpost.com/national-security/revil-ransomware-arrests-doj/2021/11/08/9432dfc2-409f-11ec-a88e-2aa4632af69b_story.html.

[205] Press Release, U.S. Dep't of Justice, Ukrainian Arrested and Charged with Ransomware Attack on Kaseya (Nov. 8, 2021), https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya.

[206] *Id.*

[207] Robyn Dixon & Ellen Nakashima, *Russia arrests 14 alleged members of REvil ransomware gang, including hacker U.S. says conducted Colonial Pipeline attack*, WASH. POST (Jan. 14, 2022), https://www.washingtonpost.com/world/2022/01/14/russia-hacker-revil/.

[208] *Id.*

REvil Hacker Arrested by Russian Authorities
Source: REvil ransomware gang arrested in Russia, *BBC NEWS (Jan. 14, 2022), https://www.bbc.com/news/technology-59998925.*

Russian authorities raided 25 addresses "seizing more than $1 million in U.S. currency, euros, Bitcoin, and rubles, as well as computer equipment and 20 luxury cars."[209] U.S. law enforcement provided FSB with information on the identity and criminal activities of REvil's leader.[210] The 14 individuals arrested will be prosecuted in Russia and will not be extradited to the United States.[211] Below is money the FSB seized during the arrests.

Money Seized Duirng FSB Arrests
Source: REvil ransomware gang arrested in Russia, *BBC NEWS (Jan. 14, 2022), https://www.bbc.com/news/technology-59998925.*

[209] *Id.*

[210] *Id.*

[211] *REvil ransomware gang arrested in Russia*, BBC NEWS (Jan. 14, 2022), https://www.bbc.com/news/technology-59998925.

IV. CASE STUDIES

The section below provides three REvil ransomware victim case studies. All three entities voluntarily cooperated with the Committee's requests for information and interviews. To protect the victim companies against any retaliation by ransomware criminals, the report does not reveal their identities and has not included certain information that could be used to identify them.

The entities discussed below are from different business sectors with significant differences in size and revenue. Despite these differences, all three fell victim to an REvil ransomware attack. This underscores the broad threat ransomware presents and the proactive steps all organizations must take to implement cyber best practices.

A. Entity A

Entity A is a global multi-sector Fortune 500 company with over 100,000 employees. Committee staff met with members of Entity A's senior leadership to discuss its REvil ransomware attack. Reflecting on the incident, one senior employee of Entity A remarked, that broadly speaking, U.S. companies are, "just sitting ducks" without more effective government and industry collaboration going forward.[212] As noted below, Entity A's state of cyber preparedness allowed it to effectively respond to the threat.

1. IT Structure and Incident Response Plan

IT Structure. Entity A has over 200 employees devoted to IT security, and dedicates approximately 10 percent of its overall IT budget to IT security.[213] Entity A has 146,000 total endpoints.[214]

Entity A analyzes cyber risks and threats on a continuous and on-going basis to ensure the confidentiality, integrity, and availability of its information systems.[215] As determined appropriate, Entity A supplements this analysis with

[212] Committee Briefing with Entity A (Apr. 4, 2021).

[213] Email from Entity A to Committee staff (Mar. 15, 2022) (on file with the Committee).

[214] *Id.* An endpoint is any remote device that communicates with a network. Examples include desktops, laptops, smartphones, tablets, and servers. *What is an Endpoint*, PALO ALTO NETWORKS (2022), https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint.

[215] Email from Entity A to Committee staff (Mar. 15, 2022) (on file with the Committee).

third-party cybersecurity products.[216] Entity A senior leadership receives regular briefings on security issues and no less than once per month.[217]

Incident Response Plan. Entity A had a formal incident response plan in place when the attack occurred.[218] Among other things, this plan specifies that Entity A implement network segmentation, disable business-to-business connections, implement aggressive endpoint controls, engage outside counsel and third-party response services, sever internet access, and perform forensic analysis.[219]

Entity A informed the Committee it adhered to its incident response plan during the attack.[220] Entity A continually updates this plan to address gaps and account for the constant changes in attacker techniques.[221]

2. Attack Background

According to Entity A, REvil compromised a known vulnerability on a legacy server of one of its vendors.[222] From there, attackers impersonated the vendor and sent an unsuspecting Entity A employee an email attachment corrupted with ransomware.[223] After opening the attachment, the ransomware encrypted Entity A's networks.[224]

After locking down Entity A's networks, REvil issued a $70 million ransom demand.[225] To assist with incident response, Entity A retained Microsoft's Detection and Response Team.[226] After forensic analysis, Entity A confirmed REvil was responsible and traced the Internet Protocol (IP) addresses back to servers in Amsterdam.[227]

3. Attack Impact

Entity A did not pay the ransom demanded by REvil.[228] After its networks were encrypted, Entity A shut down all impacted systems to protect data and was forced to rebuild several of these systems following the attack.[229] There is no

[216] *Id.*
[217] *Id.*
[218] *Id.*
[219] *Id.*
[220] *Id.*
[221] *Id.*
[222] Committee Briefing with Entity A (Apr. 4, 2021).
[223] *Id.*
[224] *Id.*
[225] *Id.*
[226] *Id.*
[227] *Id.*
[228] *Id.*
[229] *Id.*

indication REvil exfiltrated customer data or accessed any proprietary or classified information.[230]

During the incident response, Entity A observed the threat actors moving around its networks and the information they were attempting to access.[231] REvil did not demonstrate a particular interest in specific information held by Entity A, but instead moved around randomly trying to access whatever information they could.[232]

It took Entity A roughly a week to evict the hackers and secure its networks from subsequent attacks.[233] Entity A suggested it would have taken much longer to cut off hacker access without its vast resources and robust backups.[234] REvil claimed its motivation for the attack was purely financial and did not provide a more targeted explanation for selecting Entity A as a victim.[235] After Entity A declined to make a ransom payment, REvil started making threatening phone calls to leadership attempting to coerce a ransom payment.[236]

4. Federal Government Coordination and Lessons Learned

Federal Government Coordination. After confirming the attack, Entity A notified the FBI and other law enforcement agencies.[237] Overall, Entity A found the FBI to be unhelpful throughout the process. Entity A asked the FBI for best practices and other guidance documents, but did not receive helpful assistance when responding to the attack.[238] For example, the FBI offered their hostage negotiator who appeared to have little expertise in responding to ransomware attacks.[239] Entity A indicated the FBI prioritized investigating those responsible for the attack over helping Entity A respond and secure its network—the top priority for Entity A.[240] Entity A had no interaction with Department of Homeland Security or CISA during the incident.[241]

Lessons Learned. Entity A said its biggest takeaway is the sophistication of hostile actors and the financial means at their disposal.[242] Entity A has sophisticated cybersecurity, and yet it was unable to prevent this attack.[243] Entity

[230] *Id.*
[231] *Id.*
[232] *Id.*
[233] *Id.*
[234] *Id.*
[235] *Id.*
[236] *Id.*
[237] *Id.*
[238] *Id.*
[239] *Id.*
[240] *Id.*
[241] *Id.*
[242] *Id.*
[243] *Id.*

A recommended the Federal Government better coordinate its approach to responding and defending against such sophisticated and well-funded adversaries.[244] Entity A said it wished it could have shared more information with others about its experience with REvil, and that previous victims could have shared more information to help them.[245] According to Entity A, such information sharing continues to be penalized or discouraged under the current legal and regulatory framework.[246]

Finally, this incident solidified the importance of Entity A's IT backups.[247] Without viable offline backups after REvil's deployed its ransomware, Entity A told the Committee, it may have taken weeks to get its systems back online.[248] Such a disruption would almost certainly have caused serious national economic repercussions across several business sectors.[249]

B. Entity B

Entity B is a global manufacturing company with several thousand employees. Three members of Entity B's senior leadership met with Committee staff to discuss its REvil ransomware attack.

1. IT Structure and Incident Response Plan

IT Structure. Entity B has 170 employees in its IT department, roughly ten of whom are devoted to IT security.[250] Entity B's total annual IT budget is $65 million.[251] This includes all in-house software subscriptions.[252] Approximately eight percent of that $65 million is devoted to IT security, and this percentage has increased since the attack.[253] In total, Entity B has roughly 6,000 endpoints.[254]

Entity B employs traditional endpoint security, multi-factor authentication, anti-virus software, virtual private network (VPN), and single sign-on solutions.[255] Senior leadership is briefed on all significant cyber incidents, and the Chief

[244] *Id.*
[245] *Id.*
[246] *Id.*
[247] *Id.*
[248] *Id.*
[249] *Id.*
[250] Committee Briefing with Entity B (Jan. 6, 2022). Entity B also employs IT security professionals in other departments. *Id.*
[251] *Id.*
[252] *Id.*
[253] *Id.*
[254] *Id.*
[255] *Id.*

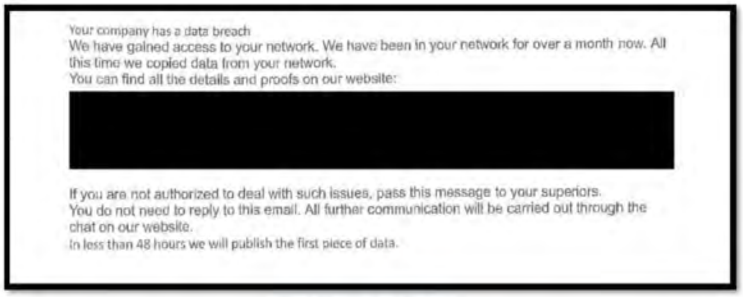
Information Officer (CIO) briefs the audit committee of the Board of Directors eight times a year.[256]

Incident Response Plan. Entity B had an established incident response plan at the time of the attack.[257] The incident response plan was implemented years before the attack, and was updated in the fall prior to the attack.[258] This plan provides that Entity B will keep external consultants on retainer and documents key points of contact in the event of a breach.[259] It also provides for annual table top exercises to test Entity B's cyber preparedness.[260]

Entity B told the Committee its incident response plan enabled Entity B's immediate ability to hire the external consultants necessary to understand the incident's impact.[261] Any gaps identified during the attack were in the company's cyber infrastructure and not the incident response plan.[262]

2. Attack Background

An IT security employee discovered the attack after noticing an unusual log-in to the company's Google cloud environment.[263] The CIO was notified of the incident immediately, and senior leadership including the General Counsel, CEO, and CFO were briefed within four days.[264]



Your company has a data breach
We have gained access to your network. We have been in your network for over a month now. All this time we copied data from your network.
You can find all the details and proofs on our website:

[redacted]

If you are not authorized to deal with such issues, pass this message to your superiors.
You do not need to reply to this email. All further communication will be carried out through the chat on our website.
In less than 48 hours we will publish the first piece of data.

REvil Message to Entity B
Source: Email from Entity B to Committee staff (Mar. 10, 2022) (on file with the Committee).

[256] *Id.*
[257] *Id.*
[258] *Id.*
[259] *Id.*
[260] *Id.*
[261] *Id.*
[262] *Id.*
[263] *Id.*
[264] *Id.*

After discovering the attack, Entity B initiated its incident response plan and sealed off its networks so its data could not be encrypted by REvil.[265] At this point, REvil made its initial ransom demand confirming Entity B was breached.[266]

REvil compromised Entity B's networks through an email phishing attack.[267] The email was opened by a mid-level employee who thought it was a legitimate email from their bank.[268] Following initial access, hackers spent a month trying to elevate privileges, but were limited to the one compromised employee's access.[269] After a month and a half, attackers elevated privileges and moved laterally across Entity B's networks.[270] After that lateral movement, there was a lull in activity while it is suspected the initial attackers sold their access to another REvil affiliate.[271] Entity B's forensic review seemed to confirm this theory, as they were able to observe two distinct attack vectors.[272] The second actor informed Entity B they were on its networks for about a month when they made their demand, and Entity B representatives told the Committee they did not uncover any evidence to the contrary.[273]

Kerberoasting explained.

Kerberoasting is an attack technique that exploits a Windows authentication protocol called Kerberos. The technique involves a hacker with low level access on a network obtaining a hashed password to a service account through the Kerberos authentication service. Service accounts often enjoy higher level access than regular users and have simple, infrequently changed passwords that make them easier to guess. As result, an attacker may be able to use the hashed password for the service account to guess the password to the service account, and escalate access on the network. (Attackers with access to a password hash can guess a simple password very quickly and automatically through a process called "brute forcing" and widely available software tools. These tools use a dictionary file of potential passwords to try thousands of different password combinations a second until they find the right one.)

See generally Steal or Forge Kerberos Tickets: Kerberoasting, MITRE (Oct. 20, 2020), https://attack.mitre.org/techniques/T1558/003/.

REvil attackers used a post-exploitation attack known as Kerberoasting to move laterally

[265] *Id.*
[266] *Id.*
[267] *Id.*
[268] *Id.*
[269] *Id.*
[270] *Id.*
[271] *Id.*
[272] *Id.*
[273] *Id.*

through Entity B's networks.[274] With this kind of attack, threat actors target domain administrator privileges in the hopes of gaining unrestricted access and control of the IT landscape.[275] At the time of the incident, Entity B did not have multi-factor authentication for its internal networks.[276] As a result, and because the compromised employee had already logged into the company's VPN, attackers could move freely around Entity B's networks.[277] When the breach occurred, Entity B did not have a zero trust architecture or segmented networks.[278]

REvil specifically accessed Entity B's on premises Windows drives.[279] Entity B started moving to Google Cloud several years before the attack for storage purposes, but not every employee successfully migrated.[280] REvil executed searches such as "finance" and "paycheck" and successfully stole large amounts of sensitive information.[281] All told, REvil exfiltrated about 1.5 terabytes of data from Entity B networks.[282]

REvil specifically exfiltrated Excel sheets, PowerPoints, and Word documents from company employee personal network Windows drives.[283] Attackers also obtained and posted certain employee pension information, personally identifiable information (PII), and Social Security Numbers (SSNs).[284] Entity B was most upset about the posting of employee PII.[285] No proprietary information was publicly released.[286]

[274] *Id.*
[275] *Id.*
[276] *Id.*
[277] *Id.*
[278] *Id.*
[279] *Id.*
[280] *Id.*
[281] *Id.*
[282] *Id.*
[283] *Id.*
[284] *Id.*
[285] *Id.*
[286] *Id.*

Monero.

Monero is a type of anonymity enhanced cryptocurrency (AEC) often called "privacy coins." AECs offer a greater degree of anonymity over their better-known cousin Bitcoin because they use non-public or private ledgers that make it more difficult to trace or attribute transactions.

U.S. DEP'T OF JUSTICE, REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE: CRYPTOCURRENCY ENFORCEMENT FRAMEWORK 4 (2020).

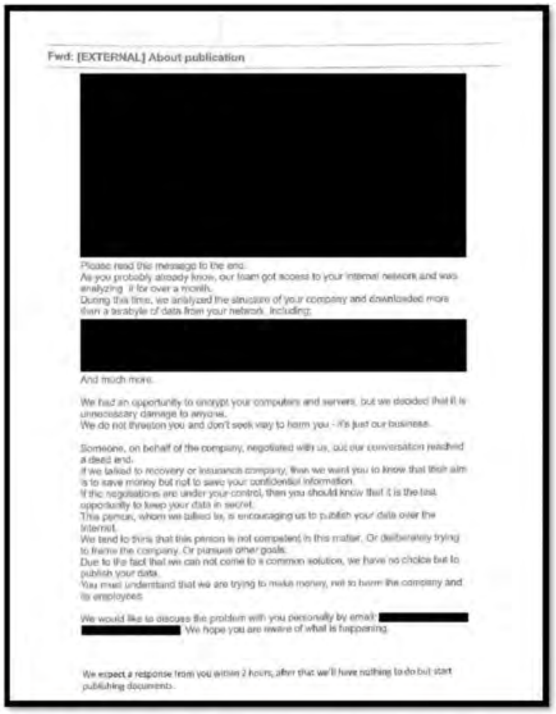
3. Attack Impact

It took about a month to understand the full impact of the breach and how much data was stolen.[287] REvil issued an initial $2 million ransom demand in Monero cryptocurrency.[288] This demand escalated to $10 million before a final demand of several hundred thousand dollars.[289]

As outlined in its response plan, Entity B retained an incident response firm, outside counsel, and a ransomware negotiator.[290] It also had cyber insurance to cover the costs of retaining these experts; however, its insurance premiums rose substantially after the breach.[291]

Entity B communicated with REvil through a third-party ransomware negotiation company.[292] These communications lasted for one month after which Entity B discontinued all communications with REvil.[293] A month later, REvil harassed Entity B employees via email saying the company was allowing their PII to be publicly released.[294] According to Entity B, this harassment was the most significant follow-on activity after discovery of the breach.[295]

[287] *Id.*
[288] *Id.*
[289] *Id.*
[290] *Id.*
[291] *Id.*
[292] *Id.*
[293] *Id.*
[294] *Id.*
[295] *Id.*



Fwd: [EXTERNAL] About publication

[redacted]

Please read this message to the end.
As you probably already know, our team got access to your internal network and was analyzing it for over a month.
During this time, we analyzed the structure of your company and downloaded more than a terabyte of data from your network. Including:

[redacted]

And much more.

We had an opportunity to encrypt your computers and servers, but we decided that it is unnecessary damage to anyone.
We do not threaten you and don't seek way to harm you - it's just our business.

Someone, on behalf of the company, negotiated with us, but our conversation reached a dead end.
If we talked to recovery or insurance company, than we want you to know that their aim is to save money but not to save your confidential information.
If the negotiations are under your control, then you should know that it is the last opportunity to keep your data in secret.
This person, whom we talked to, is encouraging us to publish your data over the Internet.
We tend to think that this person is not competent in this matter. Or deliberately trying to frame the company. Or pursues other goals.
Due to the fact that we can not come to a common solution, we have no choice but to publish your data.
You must understand that we are trying to make money, not to harm the company and its employees.

We would like to discuss the problem with you personally by email: [redacted] We hope you are aware of what is happening.

We expect a response from you within 2 hours, after that we'll have nothing to do but start publishing documents.

REvil Message to Entity B Threatening to Release Sensitive Data
Source: Email from Entity B to Committee staff (Mar. 10, 2022) (on file with the Committee).

Entity B did not make a ransom payment to REvil in part because it was able to cut off REvil's access before they encrypted Entity B's data.[296] An Entity B representative told the Committee attackers got greedy and tried to access its Google cloud environment.[297] When REvil did this, an IT security employee observed the unusual activity and sealed off Entity B's networks.[298] According to the representatives interviewed by the Committee, the incident did not impact any

[296] *Id.*
[297] *Id.*
[298] *Id.*

Entity B operational systems.[299] In addition, Entity B maintains backups and severed connection to those once the breach was identified.[300]

4. Federal Government Coordination and Lessons Learned

Federal Government Coordination. Entity B notified its local FBI Field Office within a week of detecting the incident.[301] Entity B recalled there was no "here's a playbook" discussions with the FBI regarding how to best respond.[302] The FBI did provide several contacts to help Entity B respond to the incident.[303] To assist with its investigation of REvil, Entity B submitted all relevant incident information to the FBI.[304] Entity B did not interact with CISA during the attack but does receive CISA's cybersecurity vulnerability alerts now.[305]

Lessons Learned. After the attack, Entity B acknowledged it needs to migrate to the cloud more aggressively, improve patching, and implement multi-factor authentication for its internal networks. Entity B has already improved its patching process and implemented multi-factor authentication for its internal networks.[306] In retrospect, one representative said Entity B should have forced employees to migrate to the cloud sooner, but they are able to "swing a bigger hammer" after the breach.[307] Overall, Entity B felt its incident response plan worked well, but the breach exposed gaps in its cyber architecture.[308]

C. Entity C

Entity C is a technology firm with approximately 50 total employees. Senior leadership from Entity C met with the Committee to discuss the impact of its REvil ransomware attack.

1. IT Structure and Incident Response Plan

IT Structure. Entity C has two employees devoted to IT and IT security.[309] Its overall IT budget is between $300,000 and $800,000 per year.[310] Entity C's representative did not know how much of that total budget is devoted to IT security

[299] *Id.*
[300] *Id.*
[301] *Id.*
[302] *Id.*
[303] *Id.*
[304] *Id.*
[305] *Id.*
[306] *Id.*
[307] *Id.*
[308] *Id.*
[309] Committee Briefing with Entity C (Jan. 27, 2022).
[310] *Id.*

or how many cyber incidents are reviewed on a daily basis.[311] In total, Entity C has roughly 55 endpoints.[312]

To protect its networks, Entity C employs endpoint detection, anti-virus software, and maintains offline network backups.[313] Senior leadership receives weekly briefings on cybersecurity matters.[314]

Incident Response Plan. Entity C had an established incident response plan at the time of the attack.[315] While one Entity C representative acknowledged its incident response plan only becomes relevant at the very end of preparedness, it allowed Entity C to respond and reconstitute its systems within a short timeframe.[316] For example, the company made payroll three days after the attack and sent invoices to customers within eight days.[317]

According to senior leadership, this incident exposed weaknesses in Entity C's incident response plan and specifically the processes for reconstituting impacted systems after an attack.[318] Following the incident, Entity C is working to implement data segregation, need-to-know access controls, and encryption.[319]

2. Attack Background

An employee discovered the attack after watching all of the files in an Entity C system get encrypted in real time.[320] IT staff received alerts of this malicious activity around the same time, and shortly thereafter, began severing internet connectivity as a risk reduction measure.[321]

Forensic analysis provided Entity C with significant evidence that hackers compromised its networks by exploiting a Microsoft vulnerability.[322] A few days after the incident, Entity C had evidence to conclude REvil was responsible for the attack.[323] Entity C does not have high confidence of precisely when its systems were breached.[324]

[311] *Id.*
[312] *Id.*
[313] *Id.*
[314] *Id.*
[315] *Id.*
[316] *Id.*
[317] *Id.*
[318] *Id.*
[319] *Id.*
[320] *Id.*
[321] *Id.*
[322] *Id.*
[323] *Id.*
[324] *Id.*

After the initial breach, the attackers were disjointed as they moved across Entity C's network.[325] Through either an effective set of human actors or automated processes, hackers identified several files and packaged them for exfiltration.[326] An Entity C representative indicated hackers spent a lot of time preparing to exfiltrate this information, but luckily never accessed Entity C's most sensitive information.[327] Attackers established persistence and moved laterally, but were cut off because Entity C discovered the breach at the same time.[328]

Entity C only knows what company data was exfiltrated based upon what REvil posted on their public blog.[329] An Entity C representative broadly described this information as PII.[330] It also included invoices for contracts, project descriptions, and payroll sheets containing full names and SSNs of Entity C employees.[331] None of the information exfiltrated by REvil was classified or proprietary.[332]

3. Attack Impact

Entity C informed the Committee the attack impact was significant during the first 24 hours, but lessened as it worked to bring its systems back online over the next six months.[333] Entity C understood the scope of the attack fairly quickly, but spent a lot of time searching for indicators of compromise that might go undetected with the help of an outside cyber forensics company.[334] In general though, REvil's tactics and activity on Entity C's networks were consistent with other ransomware attacks orchestrated by this organization.[335]

As mentioned above, REvil successfully encrypted several Entity C systems, requiring Entity C to acquire new hardware for a few of these systems.[336] Entity C had low confidence the encrypted systems could be securely reconstituted or otherwise had older firmware.[337] For the systems with older firmware, acquiring the new hardware had less to do with what the perpetrators did and more to do with desired level of confidence before they turned the systems back on.[338] The

[325] *Id.*
[326] *Id.*
[327] *Id.*
[328] *Id.*
[329] *Id.*
[330] *Id.*
[331] *Id.*
[332] *Id.*
[333] *Id.*
[334] *Id.*
[335] *Id.*
[336] *Id.*
[337] *Id.*
[338] *Id.*

decryption process for systems not requiring new hardware took between several days and three months.[339]

Entity C's offline backups helped it restore its systems following the attack.[340] Entity C did not experience any substantial or irregular financial costs as a result of the attack and only had to pay for the new hardware discussed above.[341]

While the financial costs were manageable, Entity C did experience the customary stress and inconvenience associated with a ransomware attack.[342] When discussing this inconvenience, an Entity C representative noted its cyber insurance policy covered most incident response costs, but added further, "if you want to talk about *** pain . . . that is different."[343]

Entity C's cyber insurance policy transferred the risk of handling the incident from Entity C to a law firm.[344] The law firm then selected all of the providers to assist Entity C with responding to the attack.[345] Because these service providers handled most issues during the incident response, Entity C had limited interaction with the perpetrators.[346] Entity C declined to discuss specific ransomware payments or demands, but did confirm REvil made its ransom demand in cryptocurrency.[347] When asked if insurance premiums have gone up, Entity C's representative replied, "everyone's will, it doesn't have anything to do with the fact that you were hacked."[348]

4. Federal Government Coordination and Lessons Learned

Federal Government Coordination. After confirming the incident, Entity C notified its contracting Federal agencies who then notified law enforcement including the FBI.[349] Entity C believes this was an opportunistic attack attributable to weaknesses in its internet-facing architecture, and not because of the information it holds.[350] Entity C preferred to respond to the attack on its own and, for the most part, the Federal Government allowed it to do so.[351] Nonetheless, Entity C said its contracting Federal agencies were helpful.[352] After the critical

[339] *Id.*
[340] *Id.*
[341] *Id.*
[342] *Id.*
[343] *Id.*
[344] *Id.*
[345] *Id.*
[346] *Id.*
[347] *Id.*
[348] *Id.*
[349] *Id.*
[350] *Id.*
[351] *Id.*
[352] *Id.*

incident response phase concluded, Entity C met with officials from the its contracting Federal agencies to share information relevant to the incident.[353] As a general matter, Entity C found the Federal Government's response teams were caught off guard by the idea that a group or entity would launch attacks like this on such a large scale in such a small time frame.[354]

Lessons Learned. When asked if they would have done anything differently, Entity C said they would have done more of "everything."[355] After the attack, Entity C is taking steps to ramp up its security protections with the goal of having all systems back online within 24 hours should another attack occur.[356]

V. CONCLUSION

The Committee's investigation and the case studies above demonstrate that ransomware is a significant threat for all organizations—regardless of size and sophistication. At the same time, the case studies also illustrate the steps an organization can take to lessen the worst impacts of a ransomware attack—like maintaining offline backups and encrypting sensitive data. To help address this threat and facilitate information sharing, CISA and the National Cyber Director should work with other appropriate agencies like FBI to implement recently enacted legislation requiring critical infrastructure owners and operators to report cyber incidents and ransomware payments to CISA. Implementing this legislation will enhance the Federal Government's visibility into cyberattacks taking place across the United States and enable a coordinated response against the hostile nation-states and criminal organizations responsible.

[353] *Id.*
[354] *Id.*
[355] *Id.*
[356] *Id.*

Statement for the Record of Bryan Palma, CEO, Trellix
Before the Senate Homeland Security & Governmental Affairs Committee
Hearing on Rising Threats: Ransomware Attacks and Ransom Payments Enabled by Cryptocurrency
342 Dirksen Senate Office Building
June 7, 2022

Chairman Peters, Ranking Member Portman, and distinguished members of the committee, thank you for giving me the opportunity to submit this statement for the record. I am Bryan Palma, CEO of Trellix, a cybersecurity company launched this year from the combination of McAfee Enterprise and FireEye. Trellix is a global company with over 40,000 business and government customers and a billion sensors in the market. This reach gives us unique insights into the challenges organizations face detecting, responding to and remediating today's threats.

Researchers at Trellix have continued to analyze ransomware and the payments accompanying it, which are predominately in cryptocurrency. Instances of ransomware attacks have been on the rise for several years now – particularly against critical infrastructures such as schools and healthcare facilities. While various task forces have addressed different aspects of the problem, the relationship of cryptocurrency to ransomware needs further exploration. To this end, the Senate Homeland Security & Governmental Affairs Committee recently released a well-researched report, Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns. The report's findings are an excellent start to what should be an ongoing investigation of the role of cryptocurrency in incentivizing and enabling ransomware attacks.

Cryptocurrency has become an almost universal form of payment in ransomware attacks, as it allows criminals to extort massive amounts of money from victims with rapid speed. As cryptocurrency is decentralized and distributed, illicit actors can intentionally obscure transactions and make them more difficult to track. In 2020, malicious actors extorted at least $692 million in cryptocurrency from ransomware attacks, up from $152 million in 2019, representing close to a 300 percent increase over a two-year period, the report finds. Yet more comprehensive data is still needed to assess the relationship between ransomware and cryptocurrency, a union that shows no signs of slowing down. Trellix's own research corroborates the report's findings that cryptocurrency has been a major factor in making ransomware perpetrators difficult to track.

For example, our Trellix Threat Labs group analyzed a ransomware-as-a-service known as Sodinokibi, or REvil, and were able to follow the money. The process was extremely complicated, as for the Sodinokibi ransomware, a unique bitcoin (BTC) wallet is generated for each victim, and then wallets are generated for affiliates of Sodinokibi as well. By linking underground forum posts with BTC transfer traces, we were able to uncover new information on the size of the campaign and associated revenue – even getting detailed insights into what the affiliates do with their earnings following a successful attack. The analysis shows that paying ransomware actors is not only keeping the ransom model alive but is also supporting other forms of crime.

In 2021, Europol credited us with providing research that helped lead to the arrest of five of Sodinokibi's affiliates, who had asked for more than 200 million euros in ransom. This action, coupled with a coordinated takedown of their infrastructure and internal disputes, led to Sodinokibi's exiting the stage as a major player, although it still exists. Center stage has been taken by Lockbit, Cuba and Conti Ransomware, where our researchers suspect a number of Sodinokibi's members have relocated. The Conti ransomware family uses multiple threads to encrypt files at a faster rate than others and contains command-line options to scan for local files as well as remote files over SMB (server message block) shares. Conti also uses the Windows Restart Manager to free up files that are open by various applications. The ransomware uses AES-256 encryption and requires the victim to email the threat actor for the decryption key. Variants of the malware will post stolen data from entities who refuse to pay the ransom.

In 2021, the Conti playbook was leaked, followed by the March 2022 leak of their chat messages. Currently we are investigating all wallets that were part of the Conti chat leaks to see if we can identify wallets that contain large amounts of cryptocurrencies. If we do, we will forward that intel to the appropriate U.S. authorities and help seize those wallets.

In another investigation, Trellix Threat Labs has been studying the Netwalker ransomware, initially known as Mailto, which was first detected in August 2019. Since then, new variants have been discovered, with a strong uptick noticed in March of this year. Using Trellix's billions of sensors around the world, we can show the global prevalence of the NetWalker ransomware. We have also seen it evolve to a more stable and robust ransomware-as-a-service model, and it appears the malware operators are targeting and attracting a broader range of technically advanced and enterprising criminal affiliates.

Our researchers also discovered a large sum of BTC linked to NetWalker, suggesting its extortion efforts are effective and that many victims have had no option other than to succumb to its criminal demands. As the BTC blockchain is a publicly accessible ledger, we can follow the money once more and see where the ransomware actors are transferring it.

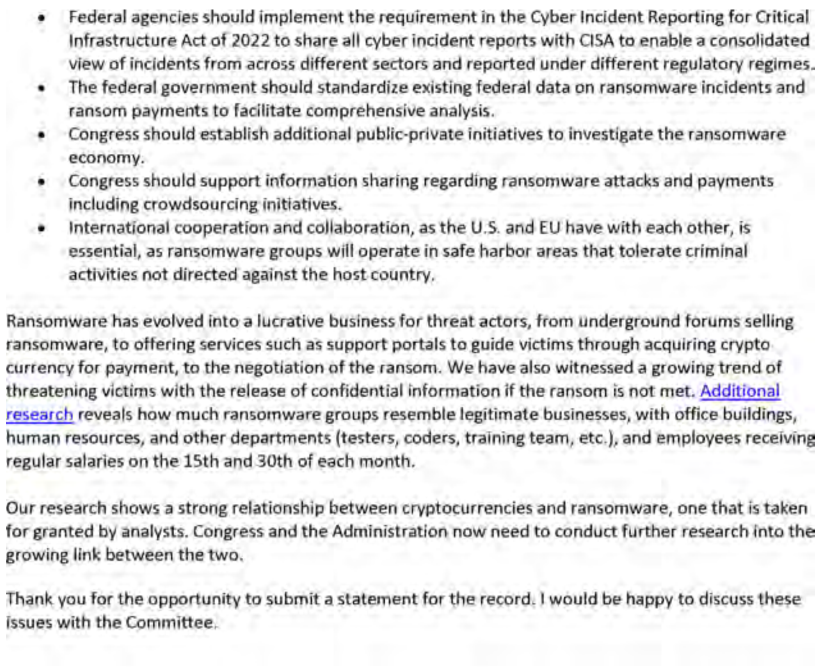
We also have noticed some interesting trends related to cryptocurrency:

- Mixing-services: Cybercriminals know that BTC transactions are public and use bitcoin-mixing services to attempt to hide their transaction into a multitude of transactions before it goes on to the next hop. This makes research complicated, especially if one doesn't have access to specialized services. Another trick is for criminals to use BTC for a certain number of transactions, then change to a less traceable cryptocurrency.

- Rogue crypto exchanges: In many countries, one needs to register, with a valid proof of identity, in order to buy or sell BTC or other cryptocurrency. However, not every crypto exchange follows this policy, particularly those considered suspect. We have often traced cryptocurrencies back to exchanges in the APAC region where the transactions ended, but where the jurisdiction cannot help to seize the stored amount or help find the next hops, i.e., where the money went.

While our threat researchers and their colleagues in other cybersecurity companies attempt to follow the money in many situations, the government has the resources and capabilities to make a real difference in this area. However, reporting of ransomware attacks and their associated payments is not centralized across federal agencies. This limits the effectiveness of agencies that are working hard to track and deter ransomware attacks. We agree with the recommendations in the Committee's report seeking to enhance the ransomware detection and response capabilities of the federal government, including:

- The Administration should swiftly implement the new ransomware attacks and ransom payments reporting mandate.



- Federal agencies should implement the requirement in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 to share all cyber incident reports with CISA to enable a consolidated view of incidents from across different sectors and reported under different regulatory regimes.
- The federal government should standardize existing federal data on ransomware incidents and ransom payments to facilitate comprehensive analysis.
- Congress should establish additional public-private initiatives to investigate the ransomware economy.
- Congress should support information sharing regarding ransomware attacks and payments including crowdsourcing initiatives.
- International cooperation and collaboration, as the U.S. and EU have with each other, is essential, as ransomware groups will operate in safe harbor areas that tolerate criminal activities not directed against the host country.

Ransomware has evolved into a lucrative business for threat actors, from underground forums selling ransomware, to offering services such as support portals to guide victims through acquiring crypto currency for payment, to the negotiation of the ransom. We have also witnessed a growing trend of threatening victims with the release of confidential information if the ransom is not met. Additional research reveals how much ransomware groups resemble legitimate businesses, with office buildings, human resources, and other departments (testers, coders, training team, etc.), and employees receiving regular salaries on the 15th and 30th of each month.

Our research shows a strong relationship between cryptocurrencies and ransomware, one that is taken for granted by analysts. Congress and the Administration now need to conduct further research into the growing link between the two.

Thank you for the opportunity to submit a statement for the record. I would be happy to discuss these issues with the Committee.