INFORMATION SHARING IN THE RANSOMWARE PAYMENT ECOSYSTEM

EXPLORING THE DELTA BETWEEN BEST PRACTICES AND EXISTING MECHANISMS

ZOË BRAMMER

IST Institute for SECURITY + TECHNOLOGY

Information Sharing in the Ransomware Payment Ecosystem:
Exploring the Delta Between Best Practices and Existing Mechanisms

Author: Zoë Brammer
Contributors: David Aaron, Silas Cutler, Matt Georgy, James Gulak, Adam Hickey, Trevaughn Smith, Megan Stifel

April 2024

IST

Table of Contents

Acknowledgments

Introduction

On January 6, 2023, the U.S. Department of Justice released a statement outlining a months-long disruption campaign against the Hive ransomware group. The statement described how, over a period of seven months, the Federal Bureau of Investigation (FBI) "penetrated Hive's computer networks, captured its decryption keys, and offered them to victims worldwide, preventing victims from having to pay $130 million in ransom demanded."[1] The disruption was the culmination of a quiet, strategic, sprawling, sequenced operation, and highlights what can be achieved when governments, law enforcement, security researchers, and the private sector share information and collaborate with victims to combat the ransomware threat.

The operation against Hive serves as an example that governments, law enforcement, and the private sector should aim to replicate at scale and look to build upon over time. It remains, however, an exception to the norm. Operations of this nature require a robust information environment, intense public/private collaboration, readily available intelligence information, voluntary information sharing, trust between stakeholders, and respect for processes that protect the identity of sources and the sensitive information they provide.

Operations like the Hive disruption rely on a foundation of strategic information sharing. Shortcomings in existing information sharing practices lead to information silos that result in a murky information environment, making it difficult for governments and industry to work together to combat ransomware at scale. As part of our effort to improve the information environment, the Institute for Security and Technology (IST)'s Ransomware Task Force (RTF) published *Mapping the Ransomware Payment Ecosystem: A Comprehensive Visualization of the Process and Participants* in the fall of 2022. This map and the subsequent Mini-Pilot are tools that can be leveraged by governments, researchers, and the private sector to gain visibility into the ecosystem, design disruptive opportunities, and ultimately blunt the ability of criminal and other malicious actors to profit from ransomware attacks. These tools also offer insight into the information produced at each point in the ransom payment process and the entities that may be able to achieve technical visibility into these pieces of information.

This report first describes in detail a ransomware attack scenario exercise conducted by IST's RTF Payments Working Group. Next, it compares the results of this exercise with recent collaborative operations, including the Hive disruption operation, the Emotet botnet takedown, and the Colonial Pipeline ransom payment recovery. This report in turn outlines existing formal federal information sharing mechanisms in the United States, maps these mechanisms atop

---

1   "U.S. Department of Justice Disrupts Hive Ransomware Variant," U.S. Department of Justice Office of Public Affairs, press release, January 26, 2023, https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant.

the ransomware payment ecosystem map, and identifies gaps that, if addressed, could clarify the information environment and help scale disruptive operations. Finally, this report delineates steps that the United States and its partner governments can take to bolster information sharing with the private sector to help scale existing best practices.

Ransomware Task Force Attack Scenario Exercise

IST's RTF Payments Working Group includes representatives from blockchain analytics companies, cyber insurance companies, financial institutions, digital forensic and incident response firms, international law enforcement, security researchers, and the U.S. government. The working group recently conducted a ransomware attack scenario exercise, walking through a ransomware attack from its identification within a victim organization, assuming a ransom payment was made, and stepping through the ransom payment process and subsequent incident investigation. The working group identified the entities involved in ransom payments and recoveries and the mechanisms by which these entities share information about incidents as they unfold. Ultimately, the exercise highlighted the fact that information sharing practices vary dramatically depending on the specific incident and outlined the ways in which victims, their lawyers, incident responders, cyber insurance companies, and governments manage the information they collect and share about incidents.

BASIC TIMELINE OF EVENTS IN A RANSOMWARE ATTACK

Ransom negotiation

Ransomware attack

Victim or organization on their behalf reports incident through a formal channel.

Victim or organization on their behalf reports payment through a formal channel.

Victim contacts cyber insurer and digital forensics and incident response firm.

Victim pays ransom.

Ransomware actors obfuscate, reinvest, and cash out.

| 0 hours | 1 day | 2 days | 3 days | 4 days | 5 days | 6 days | 7 days |

TIME SINCE ATTACK

Summary of Attack Scenario Exercise

This exercise revealed that after an attack, victims with the resources to do so generally contact their cyber insurer–if they have one–and identify an incident response company or team to help manage the ransom negotiation and payment. Many incident response companies encourage their clients to report ransomware incidents to the government via some combination of the FBI's Internet Crime Complaint Center (IC3) portal,[2] the Cybersecurity and Infrastructure Security Agency (CISA)'s incident reporting system,[3] and/or the U.S. Department of Homeland Security (DHS)'s suspicious activity reporting center,[4] among others, but there is currently no reporting mandate for the majority of entities. As of December 2023, publicly traded companies are required to disclose "material" cybersecurity incidents to the U.S. Securities and Exchange Commission (SEC), and companies that are subject to regulatory oversight may be required to report the incident to their regulator as well.[5]

In most cases, the victim or their representative conducts significant due diligence on the relevant ransomware family to ensure the payment does not go to a sanctioned or designated entity, as determined by the Office of Foreign Assets Control (OFAC). In cases where the victim and their representative determine payment is lawful and necessary, the victim or an organization on their behalf then negotiates the ransom and contacts a depository institution, like a bank, to facilitate the transfer of fiat currency to cryptocurrency, usually via a cryptocurrency business. The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) guidance advises money service businesses (MSBs) like banks and cryptocurrency businesses to file suspicious activity reports (SARs) if they become aware of a ransom payment.[6] According to the website, FinCEN guidance, while not legally binding, has a "persuasive precedential effect."[7] MSBs are also required to file SARs in cases where suspicious transactions total over $10,000. However, our working group indicated that, in most ransomware payment cases, victims do not notify their banks that the transaction is a ransom payment, in

2   "Internet Crime Complaint Center (IC3)," Federal Bureau of Investigation, accessed November 16, 2023, https://www.ic3.gov/.

3   "Incident Reporting System," Cybersecurity and Infrastructure Security Agency, accessed November 16, 2023, https://www.cisa.gov/forms/report.

4   "CISA Cyber Threat Indicator and Defensive Measure Submission System," Cybersecurity and Infrastructure Security Agency, accessed November 16, 2023, https://www.cisa.gov/forms/share-indicators.

5   Erik Gerding, "Cybersecurity Disclosure," U.S. Securities and Exchange Commission, December 14, 2023, https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214#:~:text=In%20July%20of%20this%20year,management%2C%20strategy%2C%20and%20governance.

6   Department of the Treasury Financial Crimes Enforcement Network, *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*, November 8, 2021, https://www.fincen.gov/sites/default/files/advisory/2021-11-08/Advisory%20Ransomware%20FINAL%20508_2020%20rescinded.pdf.

7   "Regulatory Releases," Department of the Treasury Financial Crimes Enforcement Network, accessed November 16, 2023, https://www.fincen.gov/regulatory-releases.

part due to concerns over liability, data privacy, cyber insecurity, and the potential for negative publicity around the incident that might tarnish the victim's reputation. In instances where victims do not notify their banks of ransom payments, bank telemetry will not necessarily reveal this fact. As a result, banks do not always have the evidence or even the suspicion necessary to file SARs in ransom-related payment cases.

Once a victim or their representative acquires sufficient cryptocurrency to pay the ransom, the victim often sends a test payment and, if successful, proceeds to transfer the full payment from their cryptocurrency wallet to the attacker's wallet or wallets. In many cases, the cryptocurrency business used to source the payment will file a SAR, but this is not guaranteed. SARs are collected and investigated by FinCEN, who then generally distributes relevant information to law enforcement and other U.S. government agencies. During the payment process, under FinCEN guidance, at least one entity acts as a money service business, even if not legally registered as such, because assets are exchanged from fiat to cryptocurrency and transferred from the victim to the attacker.[8]

Once the victim pays the ransom, the victim and their incident response team loses visibility into the path the ransom payment takes, except in cases in which the incident response firm elects to use blockchain analytics to monitor the payment. In addition, in cases where victims report attacks, law enforcement, intelligence teams supporting the incident response team, and blockchain analytics companies are often able to gain on-chain visibility, track payments, and ideally seize funds as threat actors obfuscate, cash out, and reinvest their ill-gotten assets. However, in instances where law enforcement and other government agencies are not notified of a ransom payment, it becomes time and resource-intensive, and sometimes impossible, to identify payments as attackers obfuscate, cash out, and/or reinvest the assets.

Conclusion

In sum, the existing information sharing structure around ransomware incidents is almost entirely voluntary. While some victims, incident response firms, and cyber insurers may choose to employ best practices and share information with law enforcement, governments, and other actors, they are generally not required to do so. Further, legal teams concerned with liability around data privacy and cyber insecurity, and the potential for negative publicity around the incident that might tarnish the victim's reputation often discourage voluntary information sharing. Without a significant shift in regulatory and incentive structures around ransomware incidents, the information environment will remain murky and ransomware actors will continue to carry out attacks.

---

8   Department of the Treasury Financial Crimes Enforcement Network, *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments,* November 8, 2021, https://www.fincen.gov/sites/default/files/advisory/2021-11-08/Advisory%20 Ransomware%20FINAL%20508_2020%20rescinded.pdf.

This report builds on IST's work to map the ransomware payment ecosystem and identify opportunities for disruption, and the inaugural RTF report, "Combating Ransomware: A Comprehensive Framework for Action," which highlights a range of recommendations targeting the ransomware information environment.

RANSOMWARE TASK FORCE RECOMMENDATIONS TARGETING THE RANSOMWARE INFORMATION ENVIRONMENT

Action 2.1.1	Develop new levers for voluntary sharing of cryptocurrency payment indicators.
Action 2.1.3	Incentivize voluntary information sharing between cryptocurrency entities and law enforcement.
Action 2.1.4	Centralize expertise in cryptocurrency seizure, and scale criminal seizure processes.
Action 2.1.7	Establish an insurance-sector consortium to share ransomware loss data and accelerate best practices around insurance underwriting and risk management.
Action 2.3.1	Increase government sharing of ransomware intelligence.
Action 4.1.4	Clarify United States Treasury guidance regarding ransomware payments.
Action 4.2.2	Create a standard format for ransomware incident reporting.
Action 4.2.3	Encourage organizations to report ransomware incidents.
Action 4.2.4	Require organizations and incident response entities to share ransomware payment information with a national government prior to payment.

Enabling Success: Information Sharing Case Studies

A number of historical cases outline victim, security researcher, law enforcement, and government information sharing practices that have helped to enable successful operational collaboration. In what follows, this report outlines three such cases, each providing unique insights into effective information sharing strategies. Broadly speaking, these case studies share two main variables. First, in all three cases, victims, security researchers, and private sector entities shared critical information with the U.S. government in a timely, specific, and detailed manner. Second, in all three cases and with help from security researchers and private sector entities, law enforcement was able to gain access to attacker infrastructure. While both of these variables are subject at least in part to chance, the case study outcomes indicate that information sharing plays a key role determining success. Stakeholders should therefore aim to create an information sharing environment that promotes these practices at scale across the ecosystem.

Information Sharing Best Practices in RaaS Disruptive Operations: Disrupting the Hive Ransomware Gang

Governments, industry, and security researchers viewed the FBI's 2023 Hive operation as a success due to the number of victims aided by law enforcement through strategic information sharing.[9] For the purpose of this report, we focus on the operational strategy employed by the FBI, global law enforcement partners, and the private sector in particular, and note that the actual disruption of the Hive ransomware gang's infrastructure could have been more impactful by deepening engagement with security researchers in order to have more enduring impact and advance ongoing projects.

---

9   "U.S. Department of Justice Disrupts Hive Ransomware Variant," U.S. Department of Justice Office of Public Affairs, press release, January 26, 2023, https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant.

The Hive Ransomware Gang

Beginning around June 2021, the Hive ransomware gang employed a double-extortion model to attack victims. Using a ransomware-as-a-service model (RaaS), the group targeted victims over the course of a two year period, causing major disruptions in victim operations and affecting responses to the COVID-19 pandemic. In one case outlined by the FBI, "a hospital attacked by Hive ransomware had to resort to analog methods to treat existing patients and was unable to accept new patients immediately following the attack."[10]

The Hive Disruption Operation

In July 2022, after a flurry of victims reporting Hive-related ransomware incidents, the FBI's Tampa Field Office gained clandestine, persistent access to Hive's control panel. In a January 2023 speech, Deputy Attorney General (DAG) Lisa Monaco described how the FBI "lawfully infiltrated Hive's network and hid there for months—repeatedly swiping decryption keys and passing them to victims to free them from ransomware."[11] FBI Director Christopher Wray said in a statement that this access was the result of "technical expertise…human sources, and our other investigative tradecraft."[12] The FBI's Tampa Field Office led the operation assisted by the Cyber Division team at FBI Headquarters and other field office personnel across the country, relying heavily on "FBI personnel stationed around the world, who led the collaboration with our foreign law enforcement partners…the German Reutlingen Police Headquarters, the German Federal Criminal Police, the Netherlands National High Tech Crime Unit, and Europol."[13]

Critically, after gaining access to Hive infrastructure, the FBI quietly sat in the group's servers for a period of seven months and was able to identify Hive victims and generate over 300 ransomware decryption keys.[14] Simultaneously, the FBI coordinated with global law enforcement partners to notify Hive victims who reported attacks and those with IP addresses identified on malicious servers and assisted in sharing decryption keys, enabling victims to recover their data

---

10   "U.S. Department of Justice Disrupts Hive Ransomware Variant."

11   "Deputy Attorney General Lisa O. Monaco Delivers Remarks on the Disruption of Hive Ransomware Variant," U.S. Department of Justice Office of Public Affairs, speech, January 26, 2023, https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-disruption-hive-ransomware-variant.

12   "Director Christopher Wray's Remarks at Press Conference Announcing the Disruption of the Hive Ransomware Group," Federal Bureau of Investigation, speech, January 26, 2023, https://www.fbi.gov/news/speeches/director-christopher-wrays-remarks-at-press-conference-announcing-the-disruption-of-the-hive-ransomware-group.

13   "Director Christopher Wray's Remarks at Press Conference Announcing the Disruption of the Hive Ransomware Group."

14   Dina Temple-Raston and Gabriela Glueck, "Knocking down Hive: How the FBI Ran Its Own Ransomware Decryption Operation," *The Record*, May 16, 2023, https://therecord.media/hive-ransomware-decryptors-fbi-bryan-smith-interview-click-here#:~:text=The%20FBI%20sat%20in%20the,systems%20without%20paying%20a%20ransom.

and avoid paying ransoms. Over the course of this seven month period, the FBI assisted 1,300 victims in decrypting their data, saving victims an estimated $130 million as a result.[15]

FBI Director Christopher Wray said of the operation, "the coordinated disruption of Hive's computer networks, following months of decrypting victims around the world, shows what we can accomplish by combining a relentless search for useful technical information to share with victims with investigation aimed at developing operations that hit our adversaries hard."[16] While this operation was undoubtedly a success, Director Wray also noted that "only about 20% of Hive's victims reported potential issues to law enforcement."[17] In a January 2023 statement on the Hive operation, DAG Monaco acknowledged the importance of information sharing through incident reporting, highlighting that successful operations "require the creative use of civil and criminal authorities, and they require partnerships–among law enforcement to be sure–but also with victims…Whether you own a small business, run a Fortune 500 company, oversee a school district, or manage a hospital—we can work with you to counter ransomware, mitigate harm, prevent losses, and strike back at the bad guys."[18]

Notably, this "hack the hackers'' RaaS disruption model saw success again in December 2023, when the Department of Justice announced their disruption of the ALPHV/Blackcat ransomware strain. In a statement, the Department of Justice explains that the "FBI developed a decryption tool that allowed FBI field offices across the country and law enforcement partners around the world to offer over 500 affected victims the capability to restore their systems," saving multiple victims from ransom demands totaling approximately $68 million.[19]

Conclusion

The Hive case is an example of how government agencies and law enforcement can leverage operational collaboration and victim notification to disrupt threat actors. It also highlights the power of information sharing by exposing how a lack of critical information sharing between

---

15   "Director Christopher Wray's Remarks at Press Conference Announcing the Disruption of the Hive Ransomware Group," Federal Buerau of Investigation, speech, January 26, 2023, https://www.fbi.gov/news/speeches/director-christopher-wrays-remarks-at-press-conference-announcing-the-disruption-of-the-hive-ransomware-group.

16   "U.S. Department of Justice Disrupts Hive Ransomware Variant," U.S. Department of Justice Office of Public Affairs, press release, January 26, 2023, https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant.

17   "Director Christopher Wray's Remarks at Press Conference Announcing the Disruption of the Hive Ransomware Group," Federal Buerau of Investigation, speech, January 26, 2023, https://www.fbi.gov/news/speeches/director-christopher-wrays-remarks-at-press-conference-announcing-the-disruption-of-the-hive-ransomware-group.

18   "Deputy Attorney General Lisa O. Monaco Delivers Remarks on the Disruption of Hive Ransomware Variant," U.S. Department of Justice Office of Public Affairs, speech, January 26, 2023, https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-disruption-hive-ransomware-variant.

19   "Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant," U.S. Department of Justice Office of Public Affairs, press release, December 19, 2023, https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant.

criminals using Hive RaaS products resulted in tremendous losses for the group. Despite the large number of failed attacks, Hive administrators appear to have been unaware that victims were gaining access to decryptors, thereby bypassing attacks. Feedback from security researchers highlights the need for more sharing of intermediary intelligence findings, such as server details and access lists, which can be used for mutual investigative support. The incident response community, including law enforcement, victims, and private sector actors facilitating collaboration, should aim to replicate the reciprocal information sharing that enabled the Hive operation.

Ultimately, the Hive operation was successful because:

» Victims reported Hive ransomware incidents to the FBI which, combined with security researcher's efforts to notify law enforcement, prompted an investigation into the group. This reporting aligns with *RTF Action 4.2.3*, encourage organizations to report ransomware incidents.

» The FBI and global law enforcement partners shared sensitive information about compromised IP addresses and notified and provided decryption keys to Hive victims who reported attacks and to those with IP addresses identified on malicious servers. Notably, the information shared by the FBI did not leak or interfere with their visibility. This information sharing aligns with *RTF Action 2.3.1*, increase government sharing of ransomware intelligence.

Information Sharing Best Practices in Takedown Operations: The Emotet Botnet Takedown

While the Hive case study illustrates a disruptive operation against a ransomware gang that the incident response community should aim to replicate, the case of the Emotet botnet illustrates an effective takedown operation. Unlike the case of Hive, the Working Group acknowledges Emotet is not a ransomware gang, but a botnet that operates by inserting unauthorized code into machines at scale with some degree of centralized control. However, given the extent to which ransomware threat actors leveraged its capacity and the fact that it operates similarly to ransomware, Emotet is a worthwhile example of successful information sharing to explore. The 2023 National Cybersecurity Strategy outlines the success of this operation, noting that the "2021 takedown of the Emotet botnet showed the potential of this collaborative approach, with Federal agencies, international allies and partners, and private industry cooperating to disrupt the botnet's operations."[20]

---

20   The White House, *National Cybersecurity Strategy*, March 1, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

The Emotet Botnet

Emotet is a modular malware implant designed to act as an initial point of access. After infecting a device, it can be used to further propagate or deploy ransomware tooling.[21] Emotet's developers designed it for broad use against a variety of targets and deployed it against critical industries worldwide, including banking, e-commerce, healthcare, academia, government, and the technology sector. Emotet malware primarily infects victim computers through spam email messages containing malicious attachments or hyperlinks. The Emotet botnet was a network of computers infected with Emotet malware and controlled by a group of malicious actors. According to an unsealed affidavit, foreign law enforcement agents working in coordination with the FBI identified the IP addresses of approximately 1.6 million computers worldwide that appeared to have been infected with Emotet malware between April 1, 2020 and January 17, 2021.[22] CISA estimates that Emotet infections cost local, state, tribal, and territorial governments up to $1 million per incident to remediate.[23]

The Emotet Botnet Takedown

In January 2021, the Department of Justice released a statement announcing its participation in a multinational operation to take down the Emotet botnet.[24] The monumental operation involved law enforcement, judicial authorities, and private sector partners in the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada, and Ukraine, with international activity coordinated by Europol and Eurojust.[25] Information shared among foreign law enforcement partners and the FBI included the IP addresses of infected systems and threat actor infrastructure information. Law enforcement likely used information derived from the IP addresses of infected systems to identify and notify victims and enumerated threat actor infrastructure information to plan for Emotet's seizure and takedown.

According to an affidavit, foreign law enforcement agents, working in coordination with the FBI and utilizing critical indicators provided by private sector entities, security researchers, and Emotet victims, gained access to Emotet servers, including a distribution server located overseas, and identified several other servers worldwide that were used to distribute the Emotet

21   "Emotet Malware: CISA," Cybersecurity and Infrastructure Security Agency, November 16, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-280a.

22   "AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means," United States District Court for the Middle District of North Carolina, January 25, 2021, https://www.justice.gov/file/1402221/download.

23   "Emotet Malware: CISA," Cybersecurity and Infrastructure Security Agency, November 16, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-280a.

24   "Emotet Botnet Disrupted in International Cyber Operation," U.S. Department of Justice Office of Public Affairs, press release, July 15, 2021, https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation.

25   "World's Most Dangerous Malware EMOTET Disrupted through Global Action," Eurojust, press release, January 27, 2021, https://www.eurojust.europa.eu/news/worlds-most-dangerous-malware-emotet-disrupted-through-global-action.

malware.[26] The FBI and foreign law enforcement agencies, with the help of the private sector, further identified the IP addresses of approximately 1.6 million infected computers worldwide, and notified a number of U.S.-based hosting providers of their compromised servers.[27] FBI Legal Attachés further notified authorities in more than 50 countries that providers in their jurisdictions hosted hundreds of additional compromised IP addresses.

In advance of the takedown, foreign law enforcement working in collaboration with the FBI replaced Emotet malware on servers located in their jurisdictions with a file created by law enforcement. Once downloaded, infected computers would download the replaced file during an already-programmed Emotet update. The law enforcement file prevented the administrators of the Emotet botnet from further communicating with infected computers, thereby halting the botnet's spread.

In January 2021, international law enforcement and judicial authorities gained control of Emotet botnet infrastructure and took it down from the inside.[28] Infected machines were redirected towards law enforcement-controlled infrastructure, enabling law enforcement to take control of the botnet while simultaneously providing alternative infrastructure for victims and security researchers. Using the botnet itself, law enforcement developed a module for Emotet that would uninstall it from infected systems. The widespread notification effort undertaken by law enforcement, combined with this re-routing approach, allowed for a relatively seamless takedown that preserved private sector infrastructure. This effort also minimized collateral damage to important ongoing security research, thereby enabling post-takedown continuity and preserving trust between public sector entities like government and law enforcement and their private sector counterparts.

Conclusion

The takedown of the Emotet botnet would not have been possible without strategic, scaled information sharing. In a signal of its success, the National Cybersecurity Strategy underscores the importance of effective information sharing in takedowns of this nature, saying "effective disruption of malicious cyber activity requires more routine collaboration between the private sector entities that have unique insights and capabilities and the Federal agencies that have the means and authorities to act…The Federal Government will rapidly overcome barriers to supporting and leveraging this collaboration model."[29]

26   "AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means," United States District Court for the Middle District of North Carolina, January 25, 2021, https://www.justice.gov/file/1402221/download.

27   "Emotet Botnet Disrupted in International Cyber Operation," U.S. Department of Justice Office of Public Affairs, press release, July 15, 2021, https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation.

28   "World's Most Dangerous Malware EMOTET Disrupted through Global Action," Eurojust, press release, January 27, 2021, https://www.eurojust.europa.eu/news/worlds-most-dangerous-malware-emotet-disrupted-through-global-action.

29   White House, *National Cybersecurity Strategy*, March 1, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/

Ultimately, the Emotet botnet takedown was successful because:

» The U.S. government and foreign law enforcement partners shared information about attacker infrastructure and access to servers across jurisdictions, thereby enabling an effective international operational strategy. This cooperation aligns with *RTF Action 2.3.1*, increase government sharing of ransomware intelligence.

» Reciprocal information sharing between international governments, law enforcement, and the private sector facilitated operational collaboration by enabling law enforcement authorities around the globe to notify victims and providers of compromised IP addresses and re-route infected machines toward law-enforcement controlled infrastructure. This cooperation aligns with *RTF Actions 2.3.1*, increase government sharing of ransomware intelligence, and *4.2.3*, encourage organizations to report ransomware incidents.

» Law enforcement effectively replaced Emotet malware on local servers to stop the botnet's spread, thereby avoiding collateral damage to private sector infrastructure, and ultimately uninstalled Emotet malware from infected systems.

Information Sharing Best Practices in Ransom Recovery: Colonial Pipeline Ransom Seizure

Stakeholders should aim to replicate the Hive operation and the Emotet takedown and look to expand disruptions from single strikes to sequenced actions that have broad and long-term impact. Ultimately, however, the profitability of ransomware is the driving force leading to these attacks. Ransomware attacks not only encrypt and sometimes wipe and/or expose confidential victim data to the public, but also impose payment and remediation costs that can financially cripple victims. Recovering ransom payments can both mitigate the financial harm to victims and reduce the benefit to bad actors. Recovery is therefore an important piece of disrupting the ransomware business model and ultimately the ransomware threat. For the third case study, this report focuses on the successful recovery of the ransom payment in the Colonial Pipeline attack.

The Colonial Pipeline Attack

In May 2021, the ransomware gang DarkSide accessed the Colonial Pipeline corporate network. In a two-hour window, DarkSide stole 100 gigabytes of data and infected Colonial Pipeline's IT network with ransomware, preventing the company from billing its customers and forcing it to shut down the pipeline.[30] Colonial Pipeline "is one of the largest and most vital oil pipelines

National-Cybersecurity-Strategy-2023.pdf.

30   Sean Michael Kerner, "Colonial Pipeline Hack Explained: Everything You Need to Know." *TechTarget*, April 26, 2022, https://www.

in the U.S.,"[31] supplying nearly half of the fuel for the East Coast. In the immediate aftermath of the attack, Colonial Pipeline reported to the FBI that DarkSide accessed its computer network, and that in response, it paid a ransom demand for approximately 75 Bitcoins or $3,496,500.[32] Mandiant, hired to help respond to the incident, worked with Colonial Pipeline to notify CISA, the U.S. Department of Homeland Security, and the U.S. Department of Energy about the attack.

The Colonial Pipeline Ransom Recovery

The Colonial Pipeline network attack was unique not only because of the scale of its impact and the widespread concern it caused, but also because of the unprecedented government response to the incident. In the immediate aftermath of the attack, the White House convened an interagency response group, conducted regular outreach to state and local officials, Members of Congress, and impacted companies and retailers, and worked with the FBI and DHS to provide guidance on securing critical infrastructure.[33]

The Colonial Pipeline ransom recovery is perhaps the most famous ransomware-related success story because of the collaborative nature of the response and the fact that law enforcement recovered an enormous sum of money from threat actors. The interagency response group enabled information sharing between the Department of Justice (including the FBI), the Department of Homeland Security (DHS) including the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Energy (DOE), the Department of Defense (DOD), the Department of Transportation (DOT), the Department of the Treasury, the Federal Energy Regulatory Commission, the Environmental Protection Agency (EPA), and the White House Office of Management and Budget.[34]

In June 2021, the U.S. Department of Justice announced that it seized 63.7 Bitcoins, valued at the time at approximately $2.3 million, from DarkSide.[35] A February 2022 Chainalysis publication outlines how cooperation between law enforcement and blockchain analytics companies enabled the ransom seizure. By reviewing the Bitcoin blockchain, Chainalysis

---

techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-everything-you-need-to-know.

31   Kerner, "Colonial Pipeline Hack Explained."

32   "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," Department of Justice Office of Public Affairs, press release, June 8, 2021, https://www.justice.gov/opa/pr/ department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

33   "Fact Sheet: The Biden-Harris Administration Has Launched an All-of-Government Effort to Address Colonial Pipeline Incident," The White House, May 11, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/11/ fact-sheet-the-biden-harris-administration-has-launched-an-all-of-government-effort-to-address-colonial-pipeline-incident/.

34   "Fact Sheet: The Biden-Harris Administration Has Launched an All-of-Government Effort"

35   "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," Department of Justice Office of Public Affairs, press release, June 8, 2021, https://www.justice.gov/opa/pr/ department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

identified a cryptocurrency wallet "address controlled by DarkSide's administrators, who then sent 63.7 Bitcoin—85% of Colonial's payment—to the affiliate who controlled the attack."[36] This Bitcoin represents proceeds traceable to a computer intrusion and property involved in money laundering and may be seized pursuant to criminal and civil forfeiture statutes."[37] Using this convertible virtual currency (CVC) wallet information, FBI investigators leveraged a 'private key,' or the rough equivalent of a password needed to access assets from the specific Bitcoin address, and ultimately seized the funds.

Conclusion

The Colonial Pipeline ransomware attack is undoubtedly unique in the scale of its impact, the publicity around the incident, and the speed of government response. While in this case the ransom recovery was enabled by a government task force, the operation was successful because:

» The U.S. government shared critical indicators with security researchers and the private sector. This action aligns with *RTF Action 2.3.1*, increase government sharing of ransomware intelligence.

» Security researchers and private sector entities worked closely with law enforcement to track transactions on the blockchain. This cooperation aligns with *RTF Actions 2.1.3*, incentivize voluntary information sharing between cryptocurrency entities and law enforcement, and *2.1.4*, centralize expertise in cryptocurrency seizure, and scale criminal seizure processes.

---

36   "Chainalysis In Action: How FBI Investigators Traced DarkSide's Funds Following the Colonial Pipeline Ransomware Attack," Chainalysis, February 10, 2022, https://www.chainalysis.com/blog/darkside-colonial-pipeline-ransomware-seizure-case-study/.

37   "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," Department of Justice Office of Public Affairs, press release, June 8, 2021, https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

Exploring the Delta: Existing Federal Information Sharing Mechanisms

The Hive, Emotet, and Colonial cases illustrate instances in which information sharing enabled successful outcomes. They are also exceptions to the norm. More commonly, the incentives, processes, and mechanisms in place to facilitate information sharing are inadequate to scale effective operational collaboration and achieve successful outcomes like those described above. Further, the number of existing reporting mechanisms can cause confusion for victims and can result in the siloing of information within a range of U.S. government agencies and between international governments. The remainder of this report explores existing information sharing mechanisms and the gap between information sharing practices as outlined in the RTF's attack scenario exercise and those outlined in the three case studies of successful information sharing.

Most information sharing today falls into one of two broad categories: formal, via governmental reporting mechanisms, and informal, via trust groups, non-profits, and peer-to-peer sharing. Governments generally facilitate formal information sharing. In the United States, formal information sharing includes incident reporting through the FBI's IC3, CISA, or DHS. Informal information sharing is generally facilitated by trust groups, including Information Sharing and Analysis Centers (ISACs) or Information Sharing and Analysis Organizations (ISAOs), nonprofits like the Cyber Threat Alliance, and informal bilateral organization-to-organization or researcher-to-researcher sharing. Critically, informal information sharing is entirely voluntary and predicated on trust, virtue, and reciprocity. U.S. law, namely the Cybersecurity Information Sharing Act of 2015, provides liability protection and other incentives that victims and researchers rely upon in reporting and sharing information about ransomware incidents. Whether these incentives are sufficient is outside the scope of this paper, but deserves further analysis as policymakers look at additional tools to leverage in reducing ransomware risk.

In order to better understand existing gaps in information sharing practices, IST staff overlaid formal, federal reporting mechanisms atop the ransomware payment ecosystem map, which comprehensively identifies the types of information produced at each point during the ransomware attack cycle and the entities with the potential to achieve technical visibility into each type of information. This mapping also highlights the entities required to report payments

through each mechanism and the information they should provide. We acknowledge and applaud victims who choose to report voluntarily, but these cases are not included in this mapping due to the individualized nature of voluntary reporting. In what follows, this report aims to illuminate gaps and inconsistencies in existing information sharing mechanisms.

Formal U.S. Government Information Sharing Mechanisms

There are a range of existing formal information sharing mechanisms by which the U.S. government collects information on cyber incidents. In this report, the RTF analyzes reporting mechanisms facilitated by the FBI, the Department of Treasury, and the Department of Homeland Security. This report explores each reporting mechanism and offers recommendations on how to improve the information environment within the U.S. government.

Reading the Information Sharing Mechanism Maps

For each existing information sharing mechanism, this paper includes a graphic. The underlying "map" is drawn from the ransomware payment ecosystem mini-pilot, published by IST in May 2023.

Each graphic depicts the ransomware payment process from attack to cash out in the innermost circle. The first concentric circle of white boxes identifies types of information produced along each point of the ransomware payment process. The second concentric circle of blue boxes depicts entities with potential access to these pieces of information. The black tiles in each graphic identify the entities required to report, the types of information required by a given reporting avenue and the associated points in the ransomware payment process when these pieces of information might become available.

For a complete explanation of the processes, information types, and entities included in the ransomware payment ecosystem map, we recommend reading *Mapping the Ransomware Payment Ecosystem: A Comprehensive Visualization of the Process and Participants*, published by IST in November 2022.

The Federal Bureau of Investigation (FBI) Internet Crimes Complaint Center (IC3)

The FBI collects information from victims primarily through their Internet Crimes Complaint Center (IC3) and shares this information with FBI field offices focused on specific cyber threats and other "federal, state, local, or international law enforcement or regulatory agencies for criminal, civil, or administrative action, as appropriate."[38] The FBI also often operates as a central node around which the government structures operational collaboration. Ultimately, however, we note that at this time there are no regulatory obligations for victims to report ransomware attacks or other forms of cybercrime to the FBI, and that in general the FBI does not guarantee the confidentiality of reports or give victims control over how the FBI utilizes the information shared in their disclosures.[39]

The FBI's IC3 portal requests a range of information in standard text format, including victim information like name and address, victim bank name, and affected account numbers; incident information like the transaction amount, a summary of the incident, and whether or not other agencies or stakeholders were notified about the incident; and suspect information like names and email addresses, recipient bank information, and IP addresses.

In order to further the FBI's capacity to share critical information, the FBI should consider collecting additional information about cryptocurrency transactions, in particular through the IC3 or direct contact. Technical indicators regarding cryptocurrency transactions such as the type of cryptocurrency requested, CVC wallet address of the victim and the recipient, and the transaction hash of the ransom payment can help law enforcement and blockchain analytics companies track ransoms as they are paid, obfuscated, cashed-out, and reinvested. Collecting and sharing this type of information can help facilitate ransom payment recoveries, as evidenced by the case of Colonial Pipeline.

The FBI should also consider collecting additional information about threat actors through its IC3 portal, especially those technical indicators that might shed light into the resourcing phase, where threat actors re-invest in their criminal enterprise by building infrastructure and procuring services. This could include indicators like malware hashes and malicious domain information, which could be shared with field offices and private sector entities working to disrupt threat groups. Collecting these technical indicators from service providers, security researchers,

38 "Internet Crime Complaint Center (IC3): Frequently Asked Questions," Federal Bureau of Investigation Internet Crime Complaint Center (IC3), accessed November 16, 2023, https://www.ic3.gov/.

39 "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)," Cybersecurity and Infrastructure Security Agency, accessed March 25, 2024, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.

and network telemetry and sharing them with law enforcement helped facilitate the Emotet botnet takedown by providing law enforcement with operational information regarding Emotet infrastructure that ultimately enabled the botnet's seizure and takedown.

It is also critical that the FBI conducts information sharing reciprocally. While it is extremely beneficial for victims to share incident information with the FBI, in order to disrupt the ransomware threat at scale it is equally important that the FBI selectively share relevant anonymized information like cryptocurrency wallet addresses, recovered threat actor details, and network indicators with private sector partners like blockchain analytics companies, security researchers, and service providers. Notably, it is exactly this type of reciprocal information sharing that allowed the FBI to assist so many victims in the Hive operation. Operational security will always be important to protect national security, law enforcement, and other interests, but the FBI should continue to seek opportunities to share information rather than find reasons to withhold it.

Mapping FBI / IC3 Information Sharing

Entities with visibility:

Phase 1:
– Law enforcement
– DFIR firm
– Threat intelligence firm

Phase 2:
– Blockchain analytics companies
  Law enforcement

Phase 3:
– Cryptocurrency businesses
– Law enforcement

Key:

☐ Information produced during the ransomware payment process

■ Entities required to report and information required by FBI/IC3 reporting mechanism

🟩 Regulated avenue

🟨 Unregulated or noncompliant avenue

🟦 Entities with visibility

🔺 Ransomware attack

----- Escrow

The U.S. Department of Treasury: Suspicious Activity Reports (SARs) and FinCEN Guidance

SAR Reporting

SARs, or Suspicious Activity Reports, are to be filed by financial institutions and/or digital forensics and incident response (DFIR) firms licensed as MSBs in cases where entities subject to the reporting requirement believe that they have processed ransom payments. Covered entities are required to file suspicious activity reports "no later than 30 calendar days after the date of initial detection of facts that may constitute a basis for filing a suspicious activity report,"[40] and must file in cases when cash transactions exceed $10,000 and in cases when suspicious activity might signal criminal activity. While FinCEN guidance establishes that ransom payments qualify as suspicious activity, banks and cryptocurrency businesses are not always aware that transactions they facilitate are ransom-related payments, and therefore may not report every instance.[41]

SARs focus primarily on collecting information about suspicious financial transactions and the actors carrying out suspected financial crimes, when available. They include victim bank information such as the affected account number(s), and threat actor information where available, such as the recipient cryptocurrency wallet address, malicious domain information, and forms of identification for the suspect, if possible. These types of information are critical in identifying ransom payments when they occur and enabling law enforcement and blockchain analytics companies to track ransoms as they move through the payment ecosystem.

It is notable that, although cryptocurrency MSBs are subject to reporting requirements and such information would likely be part of the pertinent details to include in a SAR filing, SARs do not explicitly require information about cryptocurrency transactions.[42]

---

40   "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," Federal Bureau of Investigation Financial Crime Enforcement Network, November 8, 2021, https://www.fincen.gov/sites/default/files/advisory/2021-11-08/Advisory%20Ransomware%20FINAL%20508_2020%20rescinded.pdf.

41   "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments."

42   "Suspicious Activity Report," U.S. Department of Treasury, accessed November 16, 2023, https://www.fdic.gov/formsdocuments/6710-06.pdf.

Mapping Suspicious Activity Reports (SARs)

Entities with visibility:

Phase 1:
- Law enforcement
- DFIR firm
- Threat intelligence firm

Phase 2:
- Blockchain analytics companies
  Law enforcement

Phase 3:
- Cryptocurrency businesses
- Law enforcement

Key:

- ☐ Information produced during the ransomware payment process
- ■ Entities required to report and information required by SAR reporting mechanism
- 🟩 Regulated avenue
- 🟨 Unregulated or noncompliant avenue
- 🟦 Entities with visibility
- 🔺 Ransomware attack
- ----- Escrow
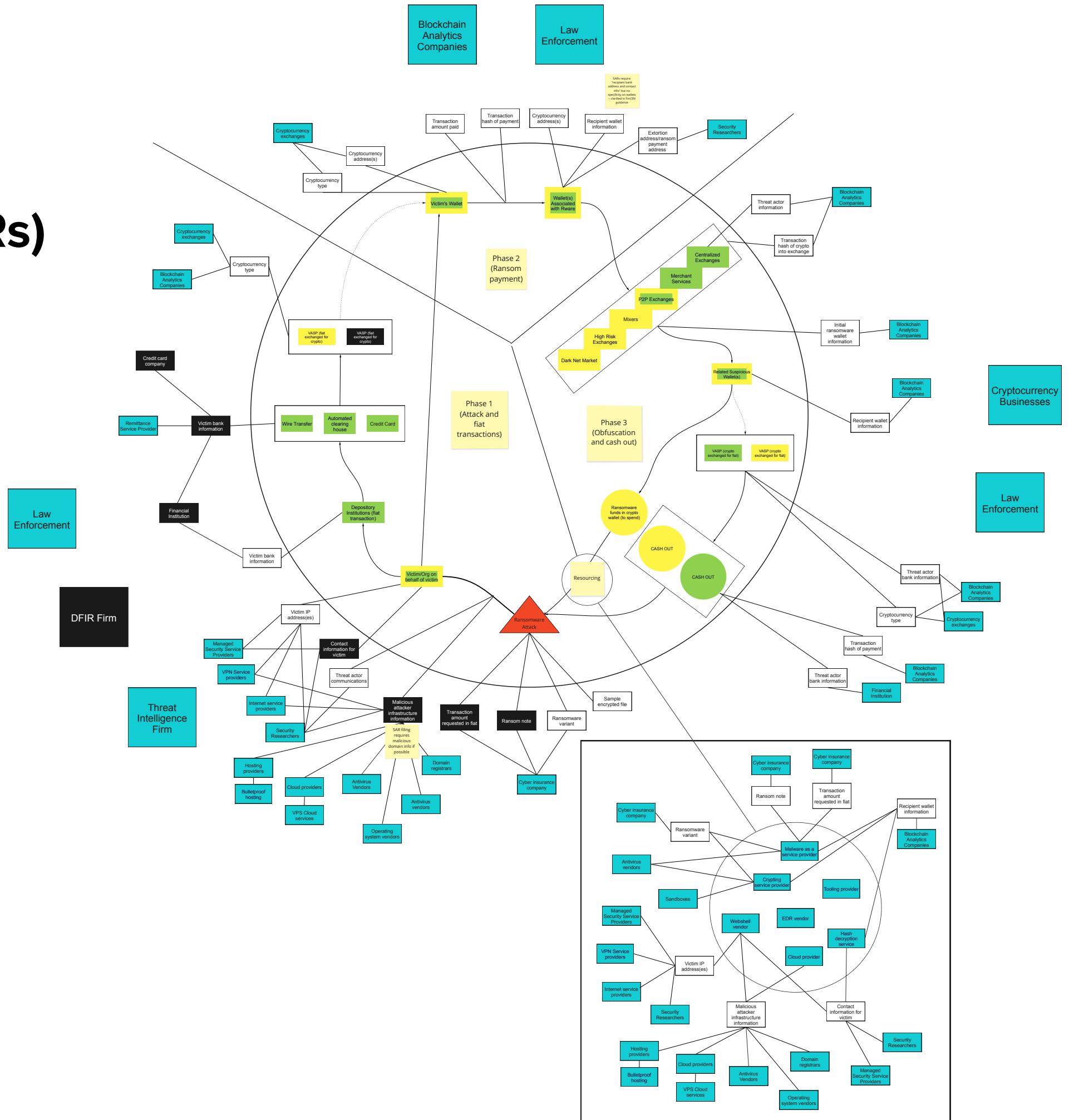
FinCEN Guidance

FinCEN guidance expands upon SAR filing requirements in two ways. First, some guidance expands the entities that may be subject to SAR reporting requirements, for example by outlining cases in which MSBs may also be required to file SARs. A November 2021 advisory, for example, states that "some DFIR companies and [cyber insurance companies] CICs, as well as some [money service businesses] MSBs that offer [convertible virtual currencies] CVCs, facilitate ransomware payments to cybercriminals, often by directly receiving customers' fiat funds, exchanging them for CVC, and then transferring the CVC to criminal-controlled accounts. Depending on the particular facts and circumstances, this activity could constitute money transmission."[43]

Second, FinCEN guidance emphasizes additional types of information that may be useful to report. As cryptocurrency is increasingly used to facilitate criminal activity, FinCEN guidance emphasizes the importance of sharing technical indicators like CVC wallet addresses, IP address, malware hashes, and mobile device information like IMEI numbers.[44] These indicators, especially when shared as soon as the victim is able, can be of critical importance to disruptive operations and broader operational collaboration, as illustrated by the Colonial Pipeline ransom recovery example. The Department of Treasury should work to circulate these technical indicators, in particular within the U.S. government, and more broadly with private sector partners like blockchain analytics companies and security researchers to enable these entities to block, or otherwise disrupt, malicious actors leveraging legitimate service providers for malicious purposes.

---

43   "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," Federal Bureau of Investigation Financial Crime Enforcement Network, November 8, 2021, https://www.fincen.gov/sites/default/files/advisory/2021-11-08/Advisory%20Ransomware%20FINAL%20508_2020%20rescinded.pdf.

44   "Advisory on Illicit Activity Involving Convertible Virtual Currency," Federal Bureau of Investigation Financial Crime Enforcement Network, May 9, 2019, https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf.

Mapping FinCEN Guidance

Entities with visibility:

Phase 1:
- Law enforcement
- DFIR firm
- Threat intelligence firm

Phase 2:
- Blockchain analytics companies
  Law enforcement

Phase 3:
- Cryptocurrency businesses
- Law enforcement

Key:

▭ (white box)	Information produced during the ransomware payment process
▮ (black box)	Entities required to report and information required by FinCEN reporting mechanism
▮ (green)	Regulated avenue
▮ (yellow)	Unregulated or noncompliant avenue
▮ (cyan)	Entities with visibility
▲ (red triangle)	Ransomware attack
- - - - -	Escrow
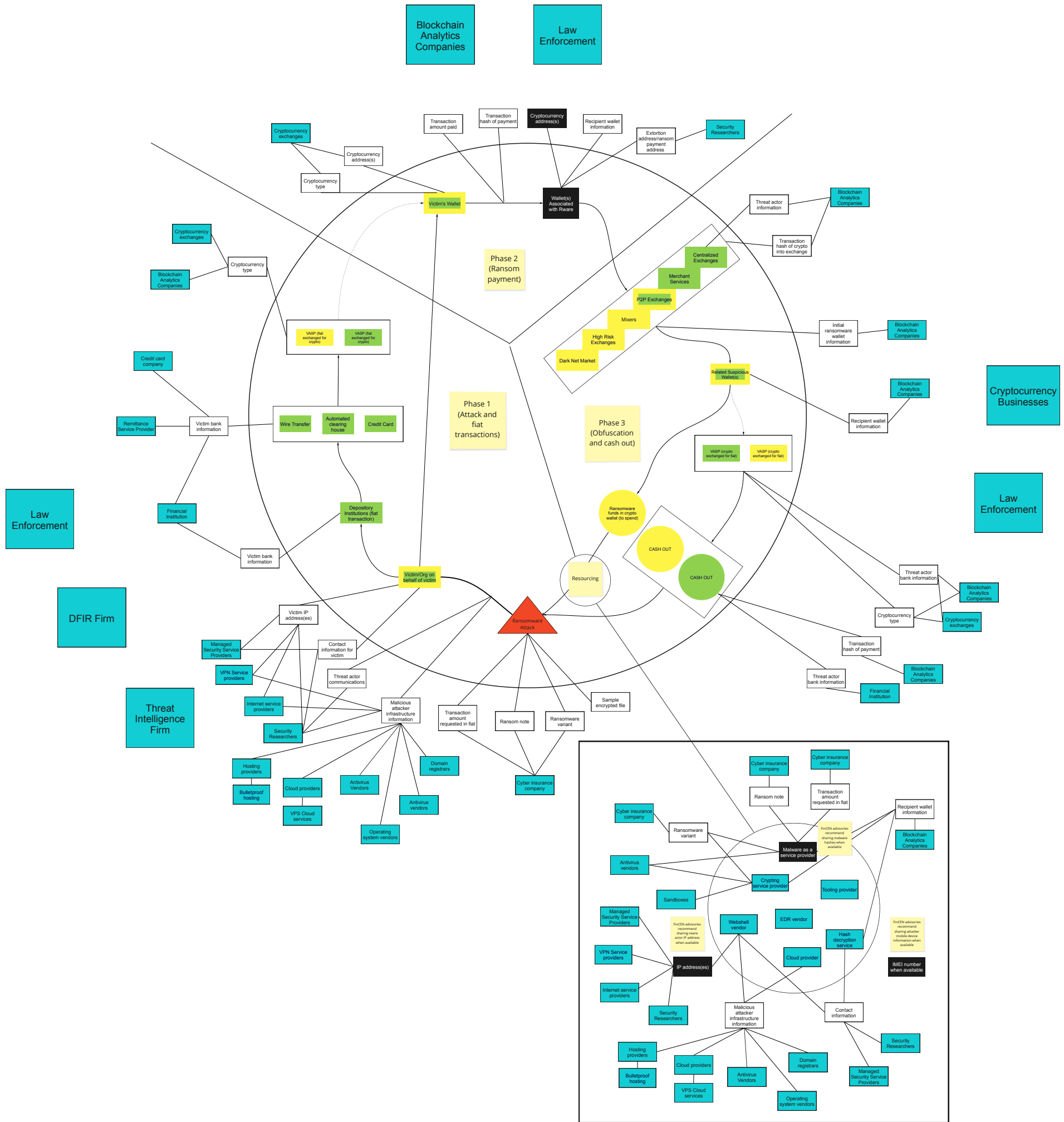
The U.S. Department of Homeland Security: CISA Reporting and the Cyber Threat Indicator and Defensive Measure Submission System

CISA Reporting

In March 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), paving the way for CISA to establish and implement regulations requiring critical infrastructure entities to report cyber incidents to CISA, including ransomware attacks. CIRCIA includes a number of requirements related to the reporting and sharing of covered cyber incidents,[45] to include:

» CISA must develop and issue regulations requiring covered entities to report to CISA any covered cyber incidents within 72 hours from the time the entity reasonably believes the incident occurred.

» Any federal entity receiving a report on a cyber incident after the effective date of the final rule must share that report with CISA within 24 hours. CISA will also have to make information received under CIRCIA available to certain federal agencies within 24 hours.

» The DHS must establish and Chair an intergovernmental Cyber Incident Reporting Council to coordinate, deconflict, and harmonize federal incident reporting requirements.

The CIRCIA final rule, set to be finalized, per the Notice of Proposed Rulemaking,[46] by 2025, will mark a significant step forward in information sharing from the private sector to the government, within the federal government, and from the government back to the private sector. The RTF Payments Working Group commends the stated goals of establishing a central repository for reporting through federal incident report sharing and a cyber incident reporting council to further centralize and harmonize federal incident reporting requirements. This type of interagency information sharing and harmonization helped facilitate all three of the success stories explored in this report.

---

45   "Cyber Incident Reporting for Critical Infrastructure Act of 2022 Fact Sheet," Cybersecurity and Infrastructure Security Agency, accessed November 16, 2023, https://www.cisa.gov/sites/default/files/publications/CIRCIA_07.21.2022_Factsheet_FINAL_508%20c. pdf.

46   "Notice of Proposed Rulemaking for Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)," Cybersecurity and Infrastructure Security Agency, March 27, 2024, https://public-inspection.federalregister.gov/2024-06526.pdf.

CIRCIA will significantly enhance the quantity and nature of the information reported to CISA. Until the final rule is enacted, CISA only collects reporting from those entities which voluntarily report to it. The current format of CISA's existing reporting mechanism is minimal, including fields for basic information about the victim organization, the date or date range of the incident, and a written description of the incident. While victims may decide to share detailed information about an incident in this unstructured narrative format, parsing the information is time consuming and slows information sharing processes. The graphic below illustrates what, in a minimum case, the victim would be prompted to provide.

Once CIRCIA is implemented, entities deemed critical infrastructure will likely be required to provide significantly more data.[47] This reporting mechanism will also be available on a voluntary basis to entities not deemed to be critical infrastructure resources, because implementation of CIRCIA will not extend mandatory reporting for all victims of ransomware and other cyber incidents.

As illustrated in the case studies explored in this report, in order for information sharing to truly foster operational collaboration, information gathered through reporting must also be shared reciprocally with the private sector. We encourage CISA and the U.S. government more broadly to prioritize working with the private sector to establish strategic, scalable strategies to improve the information environment, especially when these strategies are reciprocal.

---

47   For more insight into our recommended best practices for U.S. government reporting, see IST and the Cyber Threat Alliance's (CTA) Cyber Incident Reporting Framework, published November 2022, https://securityandtechnology.org/virtual-library/reports/cyber-incident-reporting-framework/. For more insight into our recommended best practices for sharing information internationally, see IST and CTA's Cyber Incident Reporting Framework: Global Edition, published March 2023, https://securityandtechnology.org/virtual-library/reports/cyber-incident-reporting-framework-global-edition/.

Mapping CISA Reporting

Entities with visibility:

Phase 1:

– Law enforcement

– DFIR firm

– Threat intelligence firm

Phase 2:

– Blockchain analytics companies
  Law enforcement

Phase 3:

– Cryptocurrency businesses

– Law enforcement

Key:

☐ Information produced during the ransomware payment process

■ Entities required to report and information required by CISA reporting mechanism

🟩 Regulated avenue

🟨 Unregulated or noncompliant avenue

🟦 Entities with visibility

🔺 Ransomware attack

----- Escrow
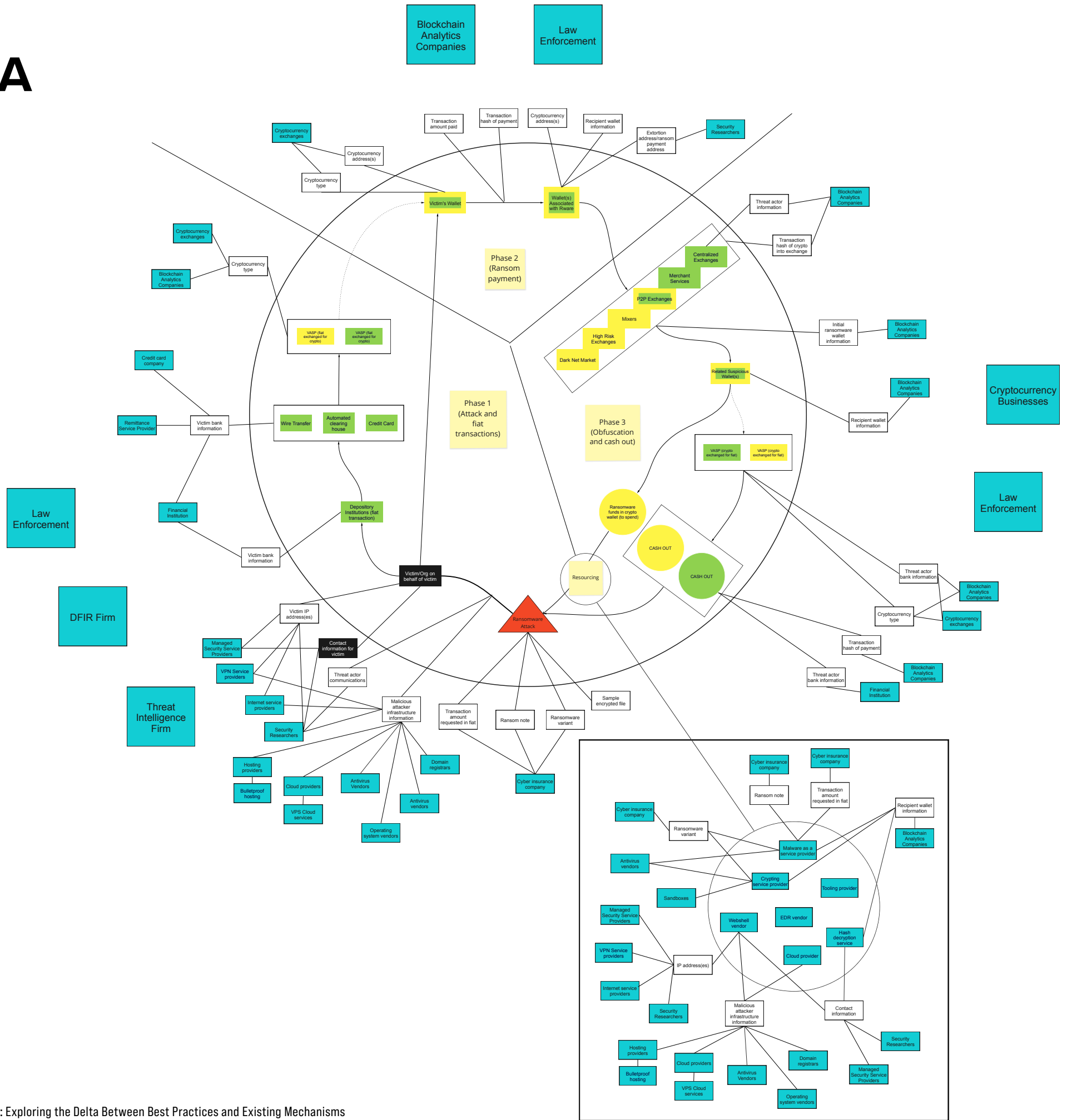
The Department of Homeland Security Cyber Threat Indicator and Defensive Measure Submission System

The Department of Homeland Security also hosts the Cyber Threat Indicator and Defensive Measure Submission System to collect technical indicators about cyber threats and associated actors to share with other U.S. government agencies and private sector entities.[48] This reporting mechanism explicitly requests much of the information that is missing in the existing CISA reporting avenue, namely by collecting indicators like IP addresses, malicious attacker infrastructure information, malware hashes, and malicious domain information.

Security researchers and other individuals working to disrupt criminal cyber activity often use the Cyber Threat Indicator submission system. Often, the information collected through this mechanism, while incredibly important, does not relate to ongoing incidents reported to CISA by victims, creating a potential disconnect between victim and researcher reporting. Sometimes, Digital Forensics and Incident Response (DFIR) firms or other incident response entities submit technical indicators through the Cyber Threat Indicator system on behalf of victims they are assisting, but this type of telemetry is usually only established long after attacks take place.

Ideally, the final CIRCIA ruling establishes a reporting framework that combines the non-technical information collected by CISA through its existing incident reporting platform and the technical indicators collected through the Cyber Threat Indicator submission system. By providing a centralized location to which victims and security researchers can submit reports of cybercriminal activity, U.S. government agencies are likely to more quickly identify connections between different reports and paint a better picture of the broader threat landscape.

---

48 "CISA Cyber Threat Indicator and Defensive Measure Submission System," Cybersecurity and Infrastructure Security Agency, accessed November 16, 2023, https://www.cisa.gov/forms/share-indicators.

Mapping DHS Security Cyber Threat Indicator and Defensive Measure Submission System


Entities with visibility:

Phase 1:
- Law enforcement
- DFIR firm
- Threat intelligence firm

Phase 2:
- Blockchain analytics companies
  Law enforcement

Phase 3:
- Cryptocurrency businesses
- Law enforcement

Key:

☐ (white box)	Information produced during the ransomware payment process
■ (black box)	Entities required to report and information required by DHS reporting mechanism
■ (green box)	Regulated avenue
■ (yellow box)	Unregulated or noncompliant avenue
■ (cyan box)	Entities with visibility
▲ (red triangle)	Ransomware attack
-----	Escrow

Information Sharing in the Ransomware Payment Ecosystem: Exploring the Delta Between Best Practices and Existing Mechanisms
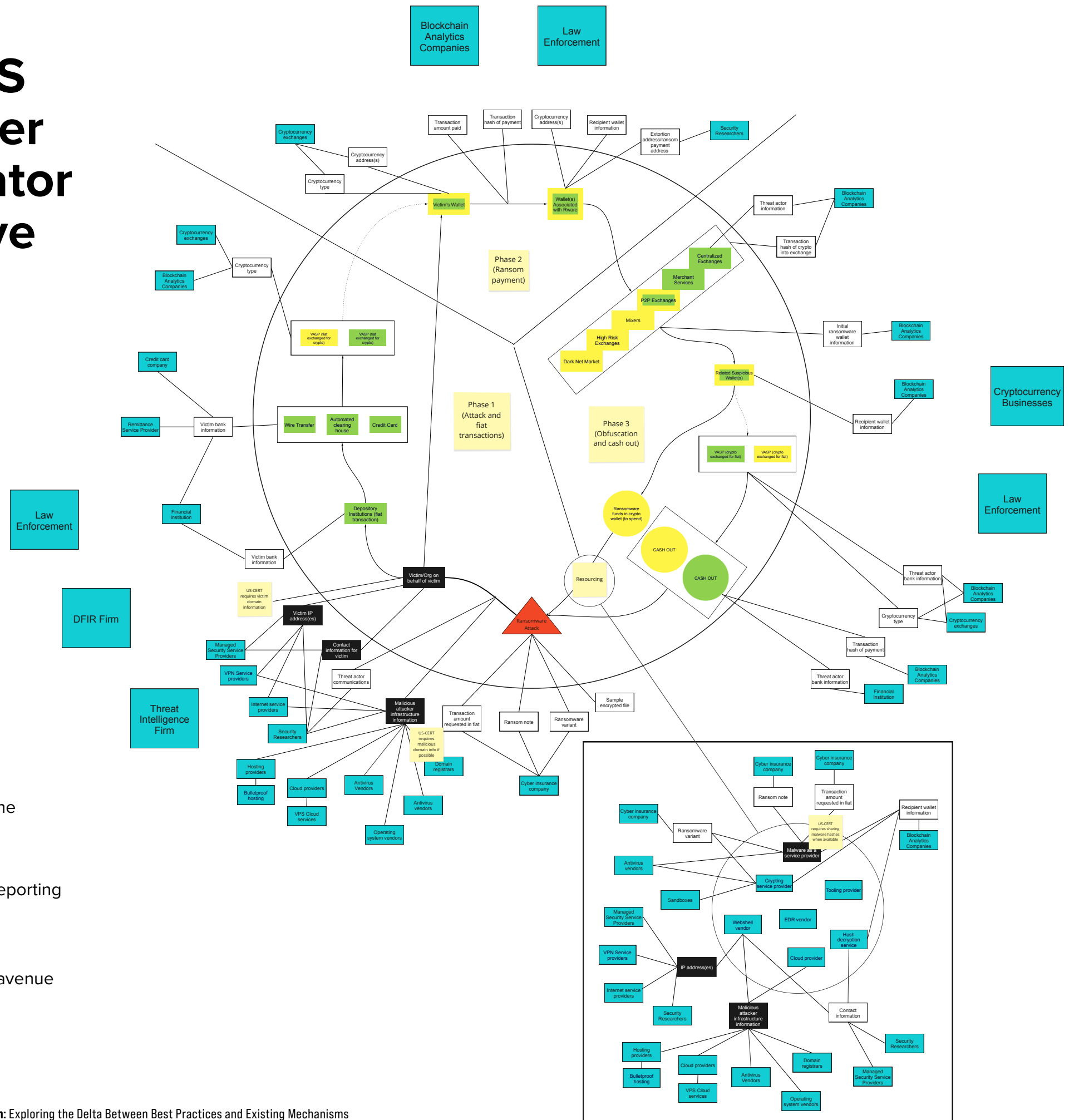
Conclusion

The three success cases outlined in this report have two main variables in common. First, victims, security researchers, and private sector entities shared critical information with the U.S. government in a timely, specific, and detailed manner. Second, law enforcement, with help from security researchers and private sector entities, gained access to attacker infrastructure. Information sharing plays a key role in determining success by facilitating the early identification of ransomware threats by governments, law enforcement, industry, and/or security researchers, and enabling cooperation through which to gain access and ultimately disrupt attacker infrastructure.

The FBI and U.S. Departments of Treasury and Homeland Security play unique roles in disrupting cyber threats, and each have their own formal incident reporting mechanisms collecting different types of information. There are three primary challenges associated with formal information sharing mechanisms: the number of existing reporting avenues, inconsistencies in the information collected through each avenue, and the voluntary nature of most reporting mechanisms. If remedied, information sharing might more closely enable the variables needed for successful disruptive outcomes at scale.

First, the number of existing reporting mechanisms can cause confusion for victims and results in the siloing of information within a range of U.S. government agencies. This can substantially hinder investigations. Even if the U.S. government does an excellent job of sharing this information between agencies, this distribution of information is ultimately inefficient, potentially resulting in information slipping through the cracks and/or slow government response times. Ideally, the U.S. government should create a single, unified reporting process. In lieu of this possibility, the U.S. government should, "[t]o the maximum extent possible…standardize incident reporting forms across departments and agencies to better aggregate data, analyze trends, and recover ransoms."[49] For a complete list of relevant types of information that the government should try to collect in the case of cyber incidents, see Section 3 of IST and CTA's *Cyber Incident Reporting Framework*.

Second, each reporting avenue or piece of guidance targets a different set of information. This can result in the U.S. government receiving multiple reports about a single incident and/ or widely varying types of information about a given incident. While this appears to be in part because of the different role each agency plays in incident response, in combination with the number of avenues, the result is often that each agency has a different understanding of not only each individual incident, but likely of the threat as a whole. We recommend that, in addition

---

49   "Cyber Incident Reporting Framework," Institute for Security and Technology, November 2022, https://securityandtechnology.org/
      virtual-library/reports/cyber-incident-reporting-framework/.

to centralizing reporting, the U.S. government reassess the information they prioritize collecting to ensure they are in the best possible position to respond to and remediate incidents.

Third, to date, the majority of these reporting avenues are voluntary, with the exception of SARs which MSBs are required to file when transactions exceed $10,000. It is clear that, to date, purely voluntary reporting mechanisms do not collect enough information to adequately facilitate operational collaboration or outline the state of the ransomware threat more broadly. We recommend that the U.S. government continue to encourage victims to report substantial cyber incidents, regardless of whether they are subject to mandatory reporting requirements.

The result of these challenges is a complex and interlocking system of reporting avenues that can confuse victims, and have not to date led to the operational collaboration and action needed to improve the cybersecurity of the ecosystem at scale, in large part because U.S. government cybersecurity experts do not have access to the most critical and relevant information about incidents with enough time to act.

The Path Forward

The ransomware information ecosystem remains murky, inhibiting effective operational collaboration at scale and playing a role in ransomware's proliferation. This report outlines a number of historical examples in which information sharing between governments, the private sector, security researchers, and victims led to effective outcomes: the Hive Ransomware operation, the Emotet Botnet takedown, and the Colonial Pipeline ransom recovery. Voluntary information sharing from victims, reciprocal information sharing between governments and the private sector, and the dissemination of information to relevant stakeholders in a timely manner predicted the success of all three cases.

In order to move the information sharing norm closer to the ideals outlined in this report, we recommend that:

» The U.S. government reassess the information it prioritizes collecting to ensure it is in the best possible position to respond to and remediate incidents;

» The U.S. government provide detailed guidance on when and how victims should share information in order to have the greatest impact, and how this information will be protected, disseminated, and acted upon, in line with *RTF Actions 2.1.1*, develop new levers for voluntary sharing of cryptocurrency payment indicators; *4.1.4*, clarify United States Treasury guidance regarding ransomware payments; *4.2.3*, encourage organizations to report ransomware incidents; and *4.2.4*, require organizations and

incident response entities to share ransomware payment information with a national government prior to payment;

» The U.S. government consolidate existing reporting avenues and automate or designate a single body to sort through the reports, share information with relevant government agencies and private sector entities, and delegate response efforts, in line with *RTF Action 4.2.2*, create a standard format for ransomware incident reporting;

» Law enforcement and the U.S. government prioritize reciprocal information sharing with the private sector, particularly security researchers, blockchain analytics companies, and entities with access to malicious attacker infrastructure information, in line with *RTF Action 2.3.1*, increase government sharing of ransomware intelligence;

» Law enforcement avoid disruptions of attacker infrastructure that risks collateral damage to private sector infrastructure, and work instead to seize attacker infrastructure and provide alternative infrastructure for victims and security researchers;

» Law enforcement work with the private sector to help notify victims of ransomware infections and compromised IP addresses;

» The U.S. government continue to encourage/require sanitized reporting by intermediaries like cyber insurers, cryptocurrency businesses, and digital forensics and incident response companies as early in the incident as possible, when victims lack the bandwidth to focus on reporting, in line with *RTF Actions 2.1.3*, incentivize voluntary information sharing between cryptocurrency entities and law enforcement; *2.1.7*, establish an insurance-sector consortium to share ransomware loss data and accelerate best practices around insurance underwriting and risk management; *4.2.3*, encourage organizations to report ransomware incidents; and *4.2.4*, require organizations and incident response entities to share ransomware payment information with a national government prior to payment;

» The U.S. government continue to encourage victims to report incidents, even if they are not required to do so, in line with *RTF Action 4.2.3*, encourage organizations to report ransomware incidents.

VASP (fiat exchanged for crypto)

VASP (fiat exchanged for crypto)

Hig
Exc

Dark Net Market

Phase 1
(Attack and fiat transactions)

(O
an

Wire Transfer

Automated clearing house

Credit Card

Depository Institutions (fiat transaction)

Victim bank information

Victim/Org on behalf of victim

Resourcing

S-CERT
res victim
omain
rmation

Victim IP address(es)

Ransomware Attack

Contact information for victim

Threat actor communications

Internet service providers

Security Researchers

Malicious attacker infrastructure information

Transaction amount requested in fiat

Ransom note

Ransomware variant

US-CERT requires malicious domain info if possible

e