MAPPING THE RANSOMWARE PAYMENT ECOSYSTEM

A COMPREHENSIVE VISUALIZATION OF THE PROCESS AND PARTICIPANTS

ZOË BRAMMER

IST Institute for SECURITY + TECHNOLOGY

Mapping the Ransomware Payment Ecosystem:
A Comprehensive Visualization of the Process and Participants

November 2022
Author: Zoë Brammer

IST

Table of Contents

Introduction

The Institute for Security and Technology's Ransomware Task Force (RTF) is working to illuminate the ransomware payment ecosystem as part of our efforts to improve the information environment and blunt the ability of criminal and other malign actors to profit from ransomware attacks.

Central to mitigating the threat of ransomware is the development of a common understanding of the actors, stakeholders, processes, and information, both required for and produced during the ransomware payment process. Yet, when we began this work, such a picture did not exist. IST undertook this effort to fill that gap.

With a clear picture of the ransomware payment ecosystem, a number of opportunities present themselves: first, the ability to identify where a particular incident is in the payment process, which can allow counter-ransomware efforts to disrupt that process; second, the identification of entities involved in the process who may have opportunities to gather information and/or take action; and third, the potential to bring together disparate entities to identify additional ways to add friction to and potentially disrupt the ransomware payment process, thereby complicating the ability of attackers to successfully profit from ransomware attacks.

This paper takes the first steps toward a more in-depth exploration of these opportunities. It presents a novel, comprehensive ransomware payment map and orients the reader to the actors and entities adapting to the ransomware threat. In future work, IST will analyze how each entity could leverage its position to observe the ransomware payment cycle. Future work will analyze the technical, regulatory and legal, and other requirements for these actors to access this information. IST will also outline ways each entity could add friction to the ongoing use of ransomware. Our goal is to enable changes in the economic incentive structure of ransomware attacks, reducing the use of ransomware overall.

Methodology

At its core, ransomware is a form of extortion, and we began our analysis with the ransomware payment process. IST staff searched existing literature, but could not identify a single, comprehensive depiction of the ransomware payment process from attack to cash-out.
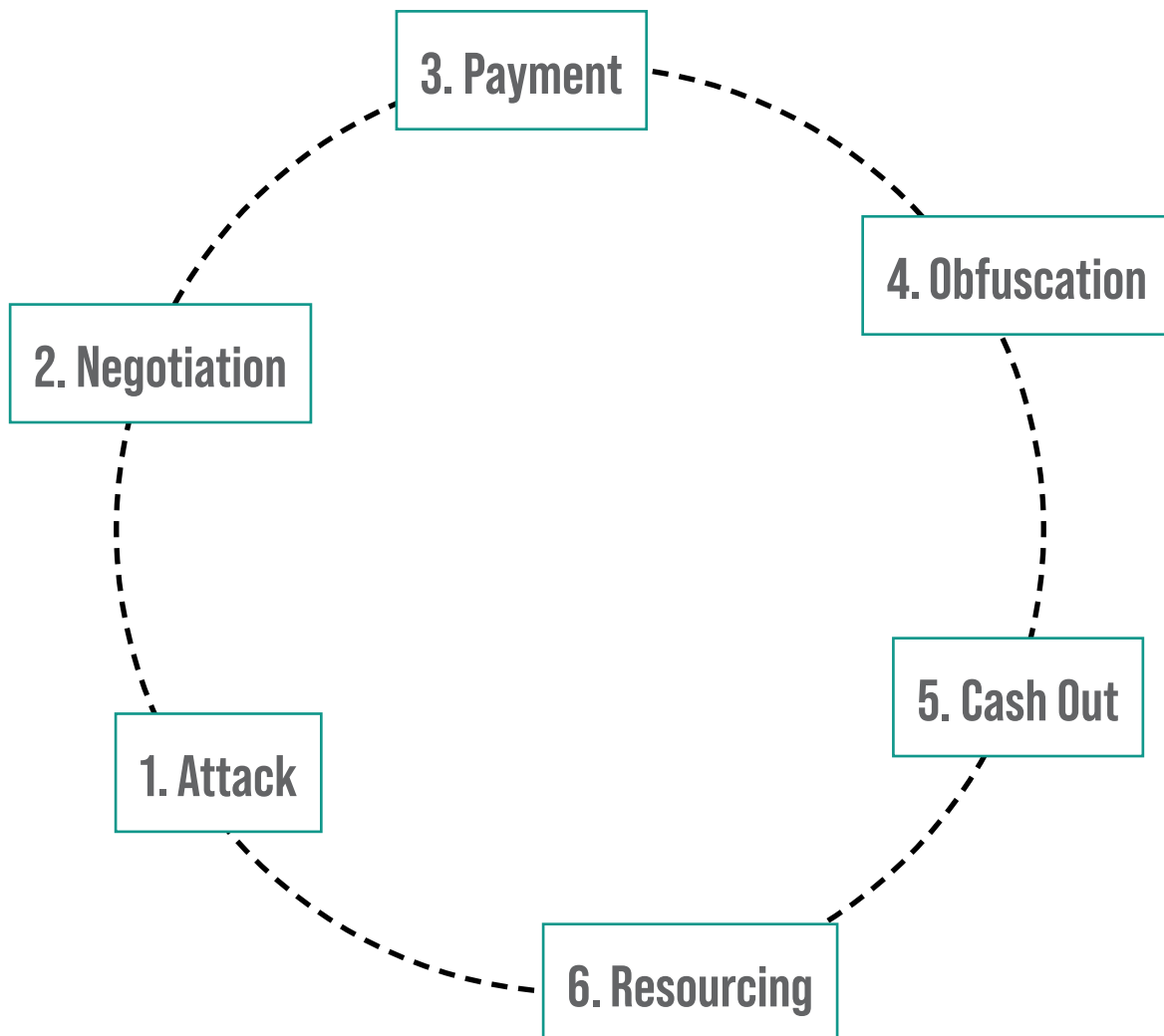
To develop the ransomware payment map, IST began by compiling and de-conflicting data from existing ecosystem maps, including FinCEN's map of convertible virtual currency (CVC) movement in ransomware incidents, a map included in congressional testimony, and maps developed by IST for the initial Ransomware Task Force report. Maps depicting more specific processes like currency mixing and escrow also aided in developing this visualization.

After developing the initial draft, IST staff conducted interviews with experts from law enforcement, blockchain analytics companies, cyber insurance firms, financial institutions, security researchers, threat intelligence providers, and other organizations to refine the map. IST also shared the map with Ransomware Task Force cryptocurrency, cyber insurance, and ransomware incident response network working groups to solicit feedback.

With the baseline ransomware payment map complete, IST staff began to research the types of information produced at each stage of the payment process and the entities and actors involved. At each stage of development, IST staff consulted relevant stakeholders and experts, primarily from within existing Ransomware Task Force membership, and iteratively refined the map with new information.

The Ransomware Payment Map

In the most general terms, the ransomware attack and payment process follows six steps or phases: 1) attack; 2) ransom negotiation; 3) ransom payment; 4) obfuscation of funds;[1] 5) cash out; and, 6) resourcing, where actors reinvest funds in new malware, personnel, and other tools to further their malign activity.

---

1   To learn more about obfuscation, see CipherTrace's webinar "Understanding Advanced Cryptocurrency Techniques": https://ciphertrace.com/advanced-crypto-obfuscation-techniques-webinar/.
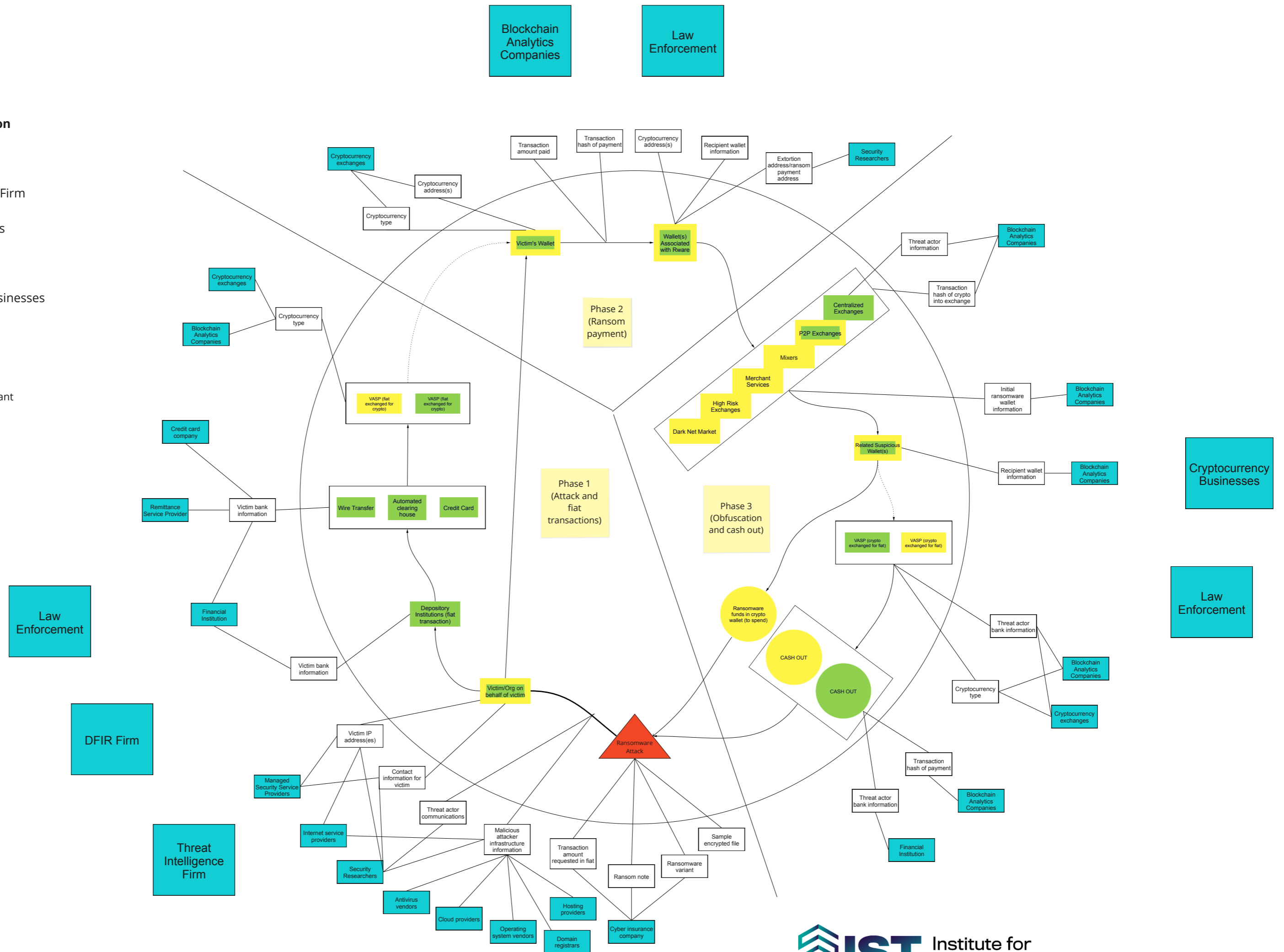
The above is an abstract simplification, intended to visualize a version of the ransomware payment process. On the following page, we present the complete payment map, a comprehensive visualization of the ransomware payment ecosystem. It depicts the ransomware payment process from attack to cash out in the innermost circle. As described in the key, the entities involved in the ransomware payment process are generally either regulated (green) or unregulated and/or non-compliant (yellow). Some entities can be both, indicated by their yellow and green color coding.

The 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. Subsequent IST analysis will unpack the extent to which these entities are actually able to access, collect, disseminate, and share this information, including through voluntary and mandatory reporting.

Entities with visibility into information in a given section

- Phase 1:
  - Law Enforcement
  - DFIR Firm
  - Threat Intelligence Firm
- Phase 2:
  - Blockchain analytics companies
  - Law Enforcement
- Phase 3:
  - Cryptocurrency Businesses
  - Law Enforcement

Key:
- Green = regulated avenue
- Yellow = unregulated or noncompliant avenue
- Light Blue = entities with visibility
- Dotted line = escrow

The map is broken down into three phases, marked by segmented lines and labeled with yellow "post-it notes" to orient the viewer. Following initial network and information access, attackers typically encrypt the victim's data and demand a ransom in exchange for decryption tools. At this point, the victim decides whether to pay the ransom. In making this decision, the victim can reach out to law enforcement or other resources such as No More Ransom, who might be able to identify a decryption key–although in the vast majority of cases decryption keys are not available.[2] If a decryption key cannot be located and the victim continues to decide not to pay the ransom, the victim will likely have to restore their systems from backups or rebuild them from scratch.

If the victim decides to pay and does not already have cryptocurrency assets in storage, the victim must obtain the cryptocurrency required for the ransom. Many victims choose to work with a firm specializing in ransomware incident response, such as a digital forensics and incident response (DFIR) or threat intelligence firm. The victim or an organization acting on behalf of the victim typically contacts the victim's depository institution to collect fiat currency equivalent to the amount of the negotiated ransomware payment. The victim's funds are then moved from their fiat currency depository institution via wire transfer, automated clearing house, or credit card either to a third party who specializes in ransom payments or directly to a cryptocurrency business like a virtual asset service provider (VASP). Finally, the cryptocurrency business exchanges fiat currency for cryptocurrency.

The second phase of the map depicts the ransom payment. The cryptocurrency business deposits the cryptocurrency in a wallet owned by the victim or an organization paying on behalf of a victim like a DFIR firm. The victim or the organization paying on its behalf then directs the payment of the ransom to a wallet or wallets owned by ransomware actors and/or their associates. Once the funds are received, the ransom is typically distributed to a number of wallets held by ransomware actors and/or their affiliates.

In the third phase of the map, ransomware actors, with the help of third party money launderers, work to obfuscate and launder the ransom funds and sometimes cash them out. The process of laundering is complex, and includes myriad options. Ransomware actors employ mixers to attempt obfuscation.[3] Because

---

2   Decryption keys are private cryptographic keys created as the second key in the public/private key pairing that allow ransomware actors to encrypt and hold victim data.

3   A cryptocurrency mixer (sometimes called a "tumbler") is a service that blends the cryptocurrencies of many

Bitcoin, Ethereum, and most other public blockchain transactions are generally traceable, obfuscation achieves a level of privacy that is otherwise hard to obtain. It is important to note that mixers are not inherently illicit. People may use mixers out of a preference or desire for privacy, but they are also employed by illicit actors to obfuscate funds.

Ransomware actors also employ merchant services, high risk and centralized exchanges, dark net markets, and peer-to-peer exchanges to launder illicit funds. Often, actors use a number of these methods simultaneously or sequentially to achieve as much anonymity as possible. They may also use the funds to make purchases on dark net markets or through merchant services.

At this point, the ransomware actors cash out their digital assets in a number of different ways. They may retain cryptocurrency assets, or they may exchange cryptocurrency for fiat currency using regulated, unregulated, or noncompliant cryptocurrency businesses.[4] Generally, actors use these resources to pay members of their team or affiliates and to reinvest in tools, techniques, and procedures (TTPs), as well as infrastructure to facilitate future ransomware attacks. Sometimes, ransomware actors use alternative cash-out methods, like staking funds, a concept similar to a high-yield savings account, where cryptocurrency assets are locked for a set period of time in exchange for interest in the form of additional cryptocurrency.[5] Other methods include trade-based money laundering and purchasing assets that hold value, like real estate or gold.[6]

This map is the first step in building a greater understanding of the ransomware payment ecosystem and the entities involved. With this information, analysts will be able to develop actions that frustrate the flow of funds to criminal actors, a concept referred to as "friction." Many of the elements of this map may be applicable to other types of cryptocurrency-facilitated criminal processes.

---

users together to obfuscate the origins and owners of the funds.

4   For the purposes of this paper, noncompliant refers to organizations not in compliance with regulations to which they appear subject based upon the activities they undertake.

5   For more information on staking funds, see Forbes' article on "Crypto Staking Basics": https://www.forbes.com/advisor/investing/cryptocurrency/crypto-staking-basics/.

6   Based on a report by the GAO, trade-based money laundering "is one of the primary mechanisms criminal organizations and others use to launder illicit proceeds, and the basic techniques involve the mis-invoicing of goods and services, such as through over- and under-invoicing." Read more: https://www.gao.gov/products/gao-22-447.

Who is Involved?

A primary goal of the ransomware payment map is to identify entities involved in the process. Not all entities involved are knowingly or voluntarily participating in a ransomware payment; some entities may not be aware of whether an individual transaction is related to ransomware. The map also reveals where some entities may be able to see certain types of information at each point in the payment process. Knowing the types of organizations involved and what information they may be able to gather can make it possible to identify potential friction points, as these entities are uniquely positioned to affect the ransomware payment process. This section will identify each type of entity included in the map and begin to outline the pieces of information about which they may have or are able to gain visibility. Future work will analyze the technical, regulatory and legal, and other requirements for these actors to access this information.

Cyber insurance companies may be involved in all phases of the payment process, but most victim organizations are not insured. Given their role, insurers often gain access to a great deal of information from insured victims during the claims process. Because some cyber insurers reimburse victims for their ransom payments and often conduct additional due diligence, including but not limited to asking for the ransom variant, they generally know the ransom demand and may have access to the ransom note. They can also usually tell which ransomware variant the attackers used, especially in extremely rare instances when the insurance company has access to the decryption key that would enable a victim company to avoid having to pay the ransom. Cyber insurance companies impact many of the decisions made in phase one of the payment map, including whether or not an insured victim should work with an incident response firm and which firm to use, as well as how the victim should respond to the attack. Further, they are often involved in all phases of the ransomware incident, including blockchain forensics and remediation.

Web hosting providers have access to domain registration information, and as a result, generally have access to information about malicious domains. This visibility may in some cases be achieved through engagement of the security researcher

community, abuse reports, and public reporting monitoring that identifies instances in which their infrastructure is used.

Operating system vendors, similar to hosting providers and antivirus vendors, may have access to information about malicious domains. This information may in some cases be gathered through system telemetry such as operating system crash reports and user reports, security researcher community engagement, and dedicated teams for tracking threats.

Antivirus software and endpoint detection and response (EDR) vendors, similar to hosting providers and operating system vendors, may have access to information about malicious domains. Typically, these entities receive telemetry from their software, including detections and remote capture of new copies of ransomware-related malware. Security researcher community engagement can also aid in this type of information gathering.

Security researchers may have visibility into public and non-public information, including information about malicious domains, certain threat actor communications, victim information, and victim IP addresses. While it is impossible to identify all avenues used by security researchers to gather information, some of those avenues include analysis of identified copies of malware, monitoring of known threat actor infrastructure, engagement with community and networks, and information sharing between researchers and the broader cybersecurity community.

Internet service providers (ISPs) may be able to see victim IP addresses and malicious domain information. This visibility may in some cases be established through network telemetry. Using network-based detections, ISPs may be able to identify both threat actor infrastructure and associated communications with victims.

Managed service providers (MSPs) are employed for a range of services, including for networks, applications, infrastructure, and security. As a result, MSPs may have access to victim information and IP addresses. Customers of most MSPs are typically asked to provide infrastructure addresses and contact information before services are initiated as part of basic due diligence.

Remittance service providers (RSPs), when used, may have insight into victim bank information, and may also have threat actor wallet addresses and other

information produced during ransom negotiations if they participate in processing the payment. This visibility may at times be achieved through communications with customers and internal knowledge management resulting from their work supporting victims of ransomware and other incidents.

Financial institutions, if notified by their customers, may have visibility into a ransom-related payment originating from a victim organization's bank account.

Credit card companies, if notified by their customers, may have visibility into ransom-related cryptocurrency payments originating from a victim organization's account.

Cryptocurrency exchanges can, when given necessary context, see the type of cryptocurrency used in ransom transactions and associated wallet addresses, and, when required to align with Know Your Customer/Anti-Money Laundering regulations, may also possess victim information. This visibility is generally established through blockchain review and transaction logs.

Digital forensics and incident response (DFIR) firms may have a range of visibility depending on their business model. In general, there are three aspects of incident response: forensic investigation, negotiation, and data restoration. While some firms engage in all aspects of the incident response process, others specialize in only one or two areas. As a result, while some DFIR firms have more visibility than others, many have visibility into all of phase one. In instances where the firm handles negotiations, they may have access to ransom demand amounts, cryptocurrency types, sample encrypted files, and actors' communications. Ransom variants and notes may at times be identified through system forensics and victim information may be compiled through customer logs.

Threat intelligence firms, depending on their clients' disclosures and the work of their researchers, may have visibility into all of phase one of the payment process. Because threat intelligence firms also sometimes handle incident response, they may access much of the information seen by DFIR firms. Further, these firms generally rely on information sharing with other parties like security researchers and incident responders, and human-enabled intelligence collection like sifting through cybercrime forums and talking to threat actors.

Blockchain analytics companies, with necessary context, may see all of phase two and most of phase three of the payment process. Blockchain analytics companies take publicly-available blockchain data–transaction data from blockchain ledgers– and map addresses and transactions to real-world services and entities. Blockchain companies sometimes partner with law enforcement, threat intelligence firms, and other companies to share information. Blockchain analytics tools can also often be used to map out illicit networks. Starting with one ransomware-related cryptocurrency address, an investigator may be able to identify not only which address currently holds the funds, but which other addresses are associated with that ransomware actor. They may also be able to identify which facilitating tools and services enable their attacks, such as access brokers, virtual private network (VPN) providers or bulletproof hosting services, and which other groups these actors may be collaborating with. This information is typically gleaned through blockchain data and analysis, and some blockchain companies employ their own security researchers, giving them broader information gathering capabilities.

Law enforcement may have insight into information produced in all three phases of the map as a result of victim self-reporting and involvement in incident response, as well as information obtained through the use of blockchain analysis tools and other techniques used in connection with investigations. Between visibility established through authorized law enforcement investigative techniques and the submission of incident reports such as the FBI's Internet Crime Complaint Center (IC3) form, law enforcement could be among the most exposed to information about ransomware attacks and other cyber crimes.

Cryptocurrency businesses may have visibility into most of phase three of the map. Because the term "cryptocurrency businesses" encapsulates a number of more specific services like blockchain analytics and cryptocurrency exchange, this visibility is primarily established through blockchain analytics and review, and customer information that can help identify victims and other actors.

Conclusion

Generating an accurate depiction of the ransomware payment process and ecosystem is a critical first step to disrupting the economic incentive structure that underpins the ransomware threat. The ransomware payment map presented here takes this foundational step. As further analysis of this ecosystem unfolds, we can identify opportunities for entities identified as part of the payment process to take action to increase costs for attackers. Further, while this map serves to illuminate the ransomware payment ecosystem, that ecosystem evolves frequently and this depiction should be updated regularly to reflect other potential and existing malign actors' use of cryptocurrencies.

The next steps for researchers are to further analyze the visibility of each entity identified here and to seek opportunities for those actors to gather useful and actionable information within their reach.

It is also important to understand what constraints each actor faces in gathering information and taking action. Future research needs to consider the complex systems of incentives, including but not limited to regulatory regimes and liability protections, that affect the other actors in the ecosystem. In the next phase of our research, IST will take on these important analytical tasks to examine and identify additional concrete actions that can add friction to the ransomware process.

INSTITUTE FOR SECURITY AND TECHNOLOGY
www.securityandtechnology.org

info@securityandtechnology.org