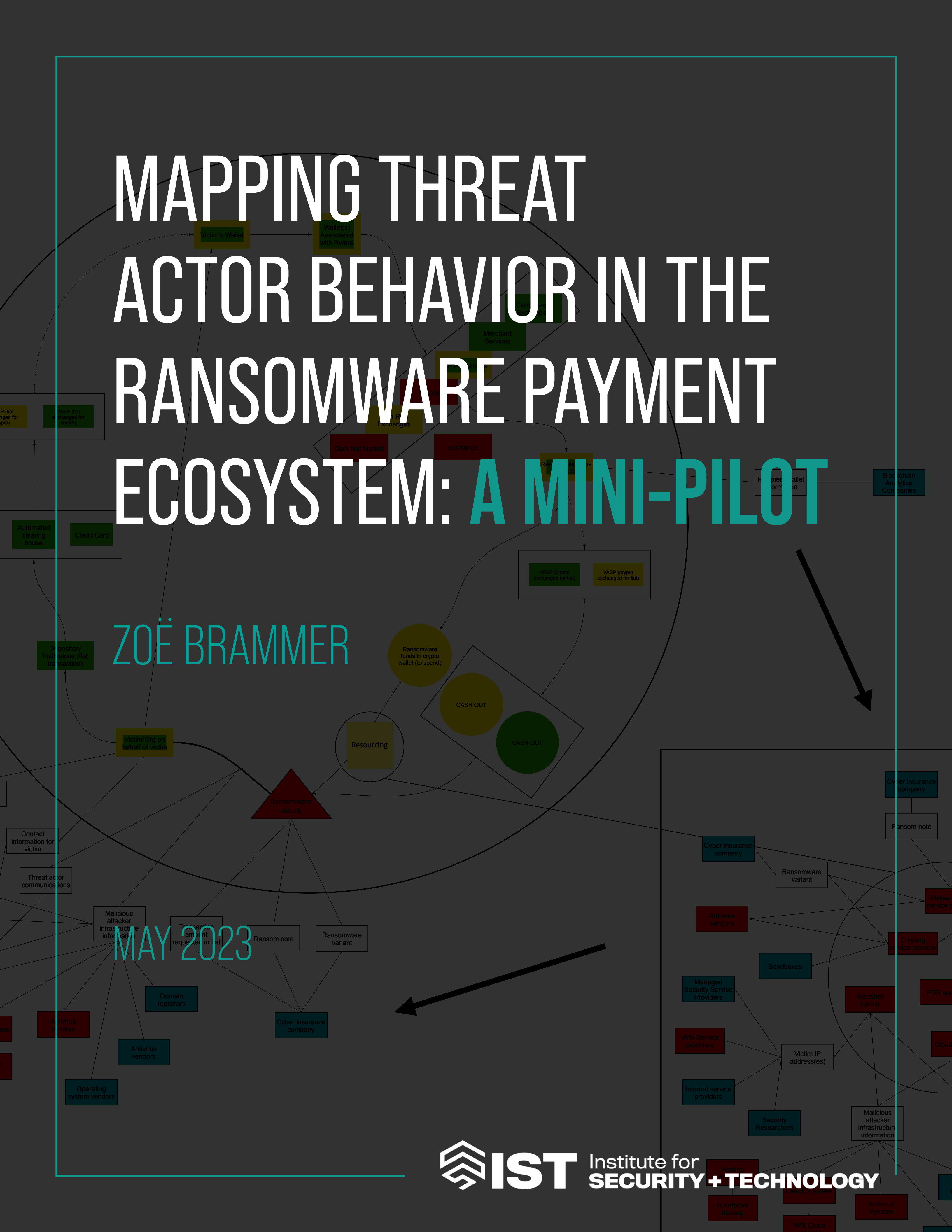

Victim's Wallet
Wallet(s) Associated with Rware
Merchant Services
Dark Net Market
Exchange
VASP (fiat exchanged for crypto)
Automated clearing house
Credit Card
Depository Institutions (fiat transaction)
Blockchain Analytics Companies
VASP (crypto exchanged for fiat)
VASP (crypto exchanged for fiat)
Ransomware funds in crypto wallet (to spend)
CASH OUT
CASH OUT
Resourcing
Victim/Org on behalf of victim
Ransomware Attack
Contact information for victim
Threat actor communications
Malicious attacker infrastructure information
Ransom note
Ransomware variant
Domain registrars
Antivirus vendors
Antivirus vendors
Operating system vendors
Cyber insurance company
Cyber insurance company
Ransom note
Cyber insurance company
Ransomware variant
Antivirus vendors
Crypting service provider
Sandboxes
Managed Security Service Providers
Webshell vendor
VPN Service providers
Victim IP address(es)
Internet service providers
Security Researchers
Malicious attacker infrastructure information
Bulletproof hosting
Antivirus Vendors

MAPPING THREAT ACTOR BEHAVIOR IN THE RANSOMWARE PAYMENT ECOSYSTEM: A MINI-PILOT

ZOË BRAMMER

MAY 2023

IST Institute for SECURITY + TECHNOLOGY

Mapping Threat Actor Behavior in the Ransomware Payment Ecosystem: **A Mini-Pilot**

May 2023
Author: Zoë Brammer

IST may provide information about third-party products or services, including security tools, videos, templates, guides, and other resources included in our cybersecurity toolkits (collectively, “Third-Party Content”). You are solely responsible for your use of Third-Party Content, and you must ensure that your use of Third-Party Content complies with all applicable laws, including applicable laws of your jurisdiction and applicable U.S. export compliance laws.

Table of Contents

Background

The 2021 Ransomware Task Force Report called for the disruption of the ransomware business model to decrease criminal profits from ransomware attacks as a critical avenue to mitigate the ransomware threat. In the fall of 2022, IST published Mapping the Ransomware Payment Ecosystem, providing a comprehensive visualization of the process and participants involved in ransomware payments. The map was the first step in understanding the sources of available information to help disrupt the ransomware business model. The ultimate goal is for experts to use the map to take actions that disincentivize threat actors from carrying out attacks.

In late 2022, IST staff began work on a mini-pilot, an exercise that tests the map against four cases of ransomware attacks. The mini-pilot seeks to identify which kinds of disruption could be the most effective and where to apply them in the payment process. This briefing paper discusses the methodology employed in developing the mini-pilot and presents the mini-pilot results, key findings, and proposed next steps.

To conduct the mini-pilot, IST selected four case studies and overlaid ransomware threat actor behavior onto our payment ecosystem map. Although this exercise does not capture every ransomware actor or attack, it aggregates many of the entities threat actors commonly leverage to carry out ransomware attacks, including but not limited to antivirus vendors, cloud service providers, hosting providers, cryptocurrency exchanges, and tooling providers.

We present the cases in a series of maps. Each case map 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/non-compliant (yellow). Some entities can be both unregulated and non-compliant, indicated by their yellow and green color coding. The circle of white boxes identifies types of information produced at 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 results of this mini-pilot indicate additional entities to include in the existing map, and reveal a “resourcing” phase where threat actors develop attacker infrastructure and perfect their tools before carrying out an attack.

Data and Methods

A number of Ransomware Task Force stakeholders made this mini-pilot possible by sharing data they routinely collect about threat actor behavior with the author of this report. Given the sensitivity of this data, references to specific organizations and other entities have been anonymized and generalized where needed. Most of the data we received was already anonymized; in instances without prior anonymization, IST staff removed all references to specific ransomware groups and other identified entities, for example by replacing entity names with the type of entity.

By overlaying threat actor behavior drawn from the anonymized data atop the original ransomware payment ecosystem map, IST staff were able to trace threat actor behavior as they prepared for and carried out attacks. Each type of entity that the actor came into contact with is highlighted in red on the map. IST staff produced five maps based on these case studies: four unique maps that trace specific ransomware threat actor behavior, and a fifth, composite map aggregating all four cases.

Cases 1, 2, and 3 are drawn from raw data provided to us by a blockchain analysis firm. Each case describes a unique threat group or actor and identifies the entities consistently leveraged by the group/actor to successfully carry out an attack. Case 4 is drawn from a combination of publications, outlining common ransomware actor tactics, techniques, and procedures (TTPs), specifically those required to make an attack possible.[1,2] These results were cross-referenced with a case study focused on a single threat group provided by an incident response organization. The caption associated with each figure includes additional details. The composite map aggregates the findings from all four cases to render overall conclusions about the map's counter-ransomware applications.

[1] John Dwyer and Camille Singleton, "Understanding the Adversary: How Ransomware Attacks Happen," *SecurityIntelligence*, IBM, November 30, 2021, https://securityintelligence.com/posts/how-ransomware-attacks-happen/.

[2] John Dwyer, "Detections That Can Help You Identify Ransomware," *SecurityIntelligence*, IBM, October 20, 2021, https://securityintelligence.com/posts/detections-help-identify-ransomware/.

Case 1

A ransomware group leverages a crypting service provider, malware-as-a-service provider, bulletproof hosting provider, VPN service provider, darknet market, cryptocurrency mixer, and cryptocurrency exchange to carry out a ransomware attack.

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:

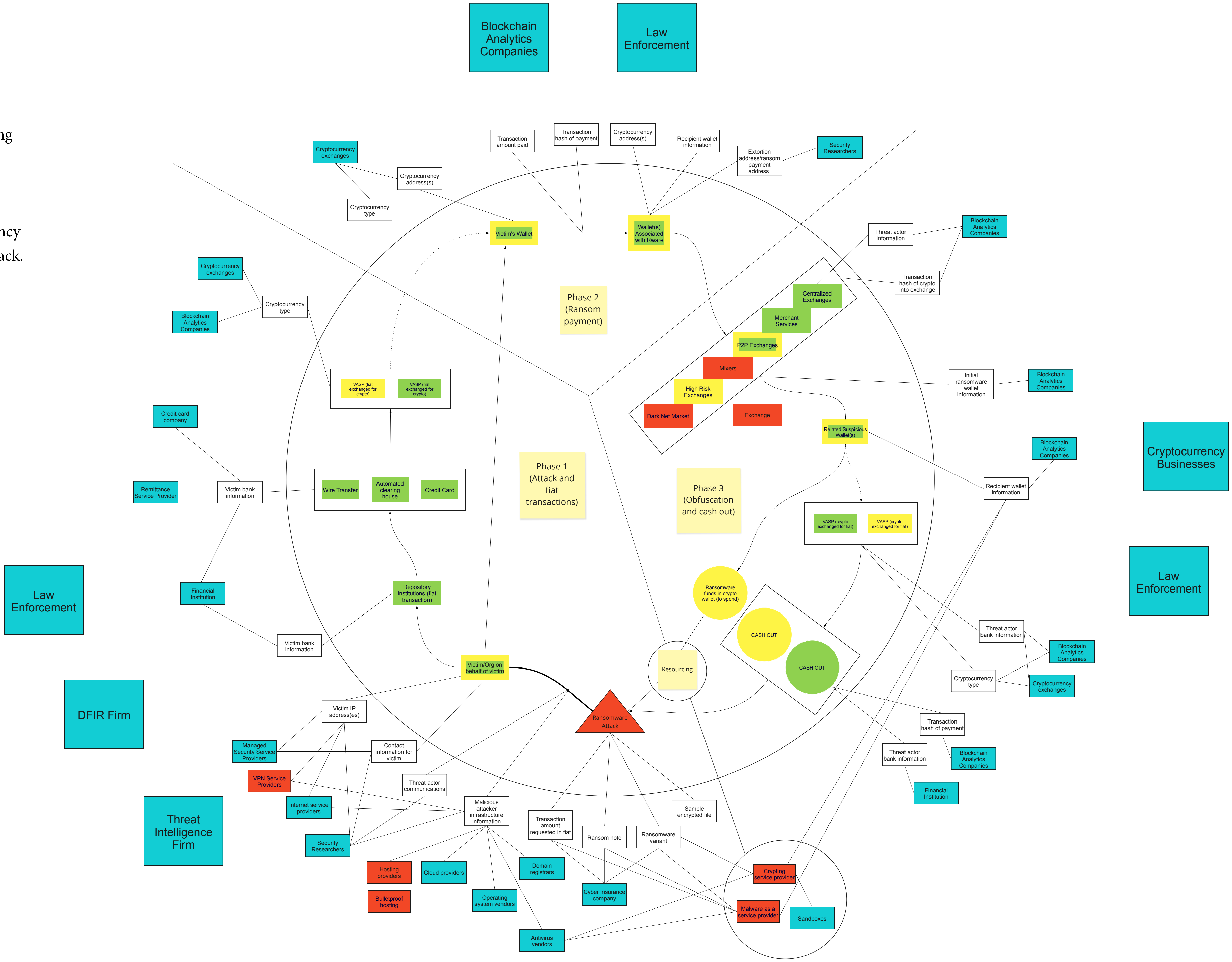
🟩 Regulated avenue

🟨 Unregulated or noncompliant avenue

🟦 Entities with visibility

🟥 Entities leveraged by threat actors to carry out a ransomware attack

----- Escrow



Blockchain Analytics Companies
Law Enforcement
Cryptocurrency exchanges
Cryptocurrency address(s)
Cryptocurrency type
Transaction amount paid
Transaction hash of payment
Cryptocurrency address(s)
Recipient wallet information
Extortion address/ransom payment address
Security Researchers
Victim's Wallet
Wallet(s) Associated with Rware
Threat actor information
Blockchain Analytics Companies
Transaction hash of crypto into exchange
Cryptocurrency exchanges
Blockchain Analytics Companies
Cryptocurrency type
Phase 2 (Ransom payment)
Centralized Exchanges
Merchant Services
P2P Exchanges
Mixers
High Risk Exchanges
Dark Net Market
Exchange
Initial ransomware wallet information
Blockchain Analytics Companies
VASP (fiat exchanged for crypto)
VASP (fiat exchanged for crypto)
Credit card company
Related Suspicious Wallet(s)
Blockchain Analytics Companies
Cryptocurrency Businesses
Remittance Service Provider
Victim bank information
Wire Transfer
Automated clearing house
Credit Card
Phase 1 (Attack and fiat transactions)
Phase 3 (Obfuscation and cash out)
Recipient wallet information
VASP (crypto exchanged for fiat)
VASP (crypto exchanged for fiat)
Law Enforcement
Law Enforcement
Financial Institution
Depository Institutions (fiat transaction)
Ransomware funds in crypto wallet (to spend)
CASH OUT
Threat actor bank information
Blockchain Analytics Companies
Victim bank information
CASH OUT
Resourcing
Cryptocurrency type
Cryptocurrency exchanges
Victim/Org on behalf of victim
DFIR Firm
Victim IP address(es)
Ransomware Attack
Transaction hash of payment
Managed Security Service Providers
Contact information for victim
Threat actor bank information
Blockchain Analytics Companies
VPN Service Providers
Threat actor communications
Financial Institution
Internet service providers
Malicious attacker infrastructure information
Sample encrypted file
Threat Intelligence Firm
Transaction amount requested in fiat
Ransom note
Ransomware variant
Security Researchers
Hosting providers
Cloud providers
Domain registrars
Crypting service provider
Bulletproof hosting
Operating system vendors
Cyber insurance company
Malware as a service provider
Sandboxes
Antivirus vendors

Case 2

A ransomware group leverages a hash decryption service, cloud provider, VPS cloud server, antivirus vendor, and VPN service provider to carry out a ransomware attack.

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:

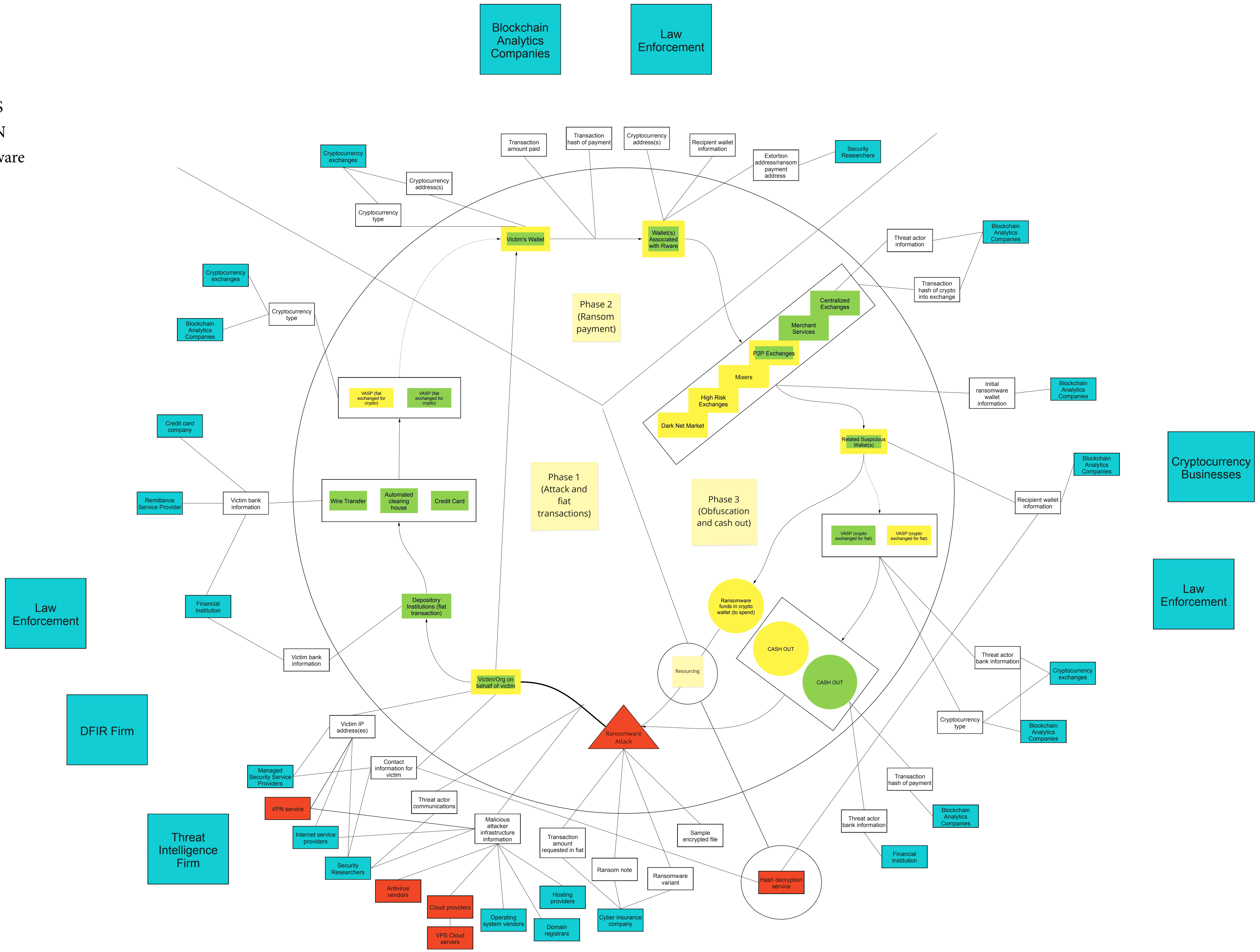
🟩 Regulated avenue

🟨 Unregulated or noncompliant avenue

🟦 Entities with visibility

🟥 Entities leveraged by threat actors to carry out a ransomware attack

----- Escrow



Blockchain Analytics Companies
Law Enforcement
Cryptocurrency exchanges
Cryptocurrency address(s)
Cryptocurrency type
Transaction amount paid
Transaction hash of payment
Cryptocurrency address(s)
Recipient wallet information
Extortion address/ransom payment address
Security Researchers
Victim's Wallet
Wallet(s) Associated with Rware
Threat actor information
Blockchain Analytics Companies
Transaction hash of crypto into exchange
Cryptocurrency exchanges
Blockchain Analytics Companies
Cryptocurrency type
Phase 2 (Ransom payment)
Centralized Exchanges
Merchant Services
P2P Exchanges
Mixers
High Risk Exchanges
Dark Net Market
Initial ransomware wallet information
Blockchain Analytics Companies
VASP (fiat exchanged for crypto)
VASP (fiat exchanged for crypto)
Related Suspicious Wallet(s)
Blockchain Analytics Companies
Recipient wallet information
Cryptocurrency Businesses
Credit card company
Remittance Service Provider
Victim bank information
Wire Transfer
Automated clearing house
Credit Card
Phase 1 (Attack and fiat transactions)
Phase 3 (Obfuscation and cash out)
VASP (crypto exchanged for fiat)
VASP (crypto exchanged for fiat)
Law Enforcement
Financial Institution
Depository Institutions (fiat transaction)
Ransomware funds in crypto wallet (to spend)
CASH OUT
CASH OUT
Victim bank information
Resourcing
Threat actor bank information
Cryptocurrency exchanges
Victim/Org on behalf of victim
DFIR Firm
Ransomware Attack
Cryptocurrency type
Blockchain Analytics Companies
Victim IP address(es)
Contact information for victim
Managed Security Service Providers
VPN service
Threat actor communications
Transaction hash of payment
Threat actor bank information
Blockchain Analytics Companies
Malicious attacker infrastructure information
Transaction amount requested in fiat
Sample encrypted file
Internet service providers
Threat Intelligence Firm
Security Researchers
Ransom note
Ransomware variant
Financial Institution
Antivirus vendors
Hosting providers
Hash decryption service
Cloud providers
Operating system vendors
Domain registrars
Cyber insurance company
VPS Cloud servers

Case 3

A ransomware group leverages a crypting service provider, hash decryption service, webshell vendor, bulletproof hosting provider, VPN service provider, and dark net market to carry out a ransomware attack.

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:

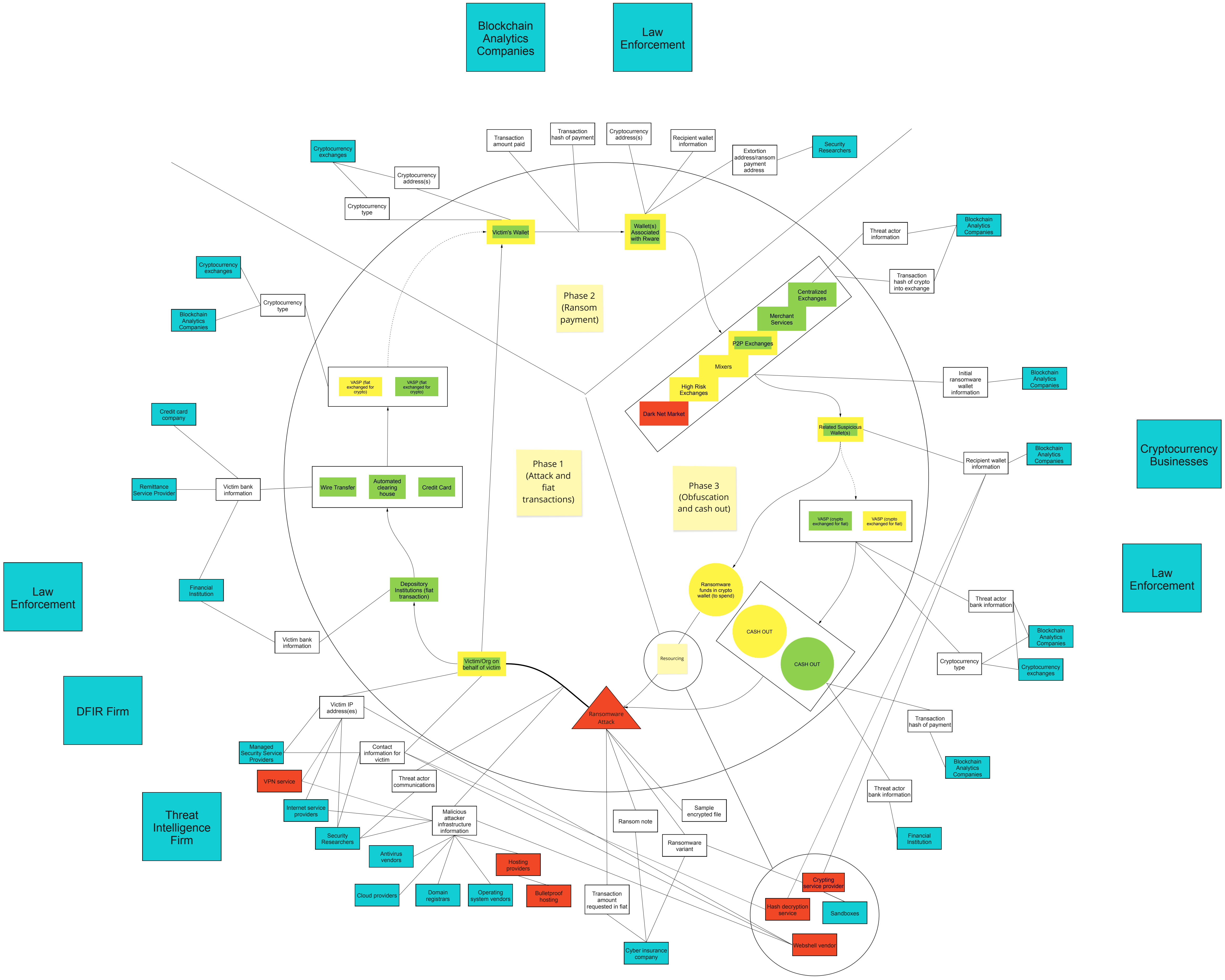
🟩 Regulated avenue

🟨 Unregulated or noncompliant avenue

🟦 Entities with visibility

🟥 Entities leveraged by threat actors to carry out a ransomware attack

----- Escrow


Blockchain Analytics Companies
Law Enforcement
Transaction amount paid
Transaction hash of payment
Cryptocurrency address(s)
Recipient wallet information
Extortion address/ransom payment address
Security Researchers
Cryptocurrency exchanges
Cryptocurrency address(s)
Cryptocurrency type
Victim's Wallet
Wallet(s) Associated with Rware
Threat actor information
Blockchain Analytics Companies
Transaction hash of crypto into exchange
Cryptocurrency exchanges
Cryptocurrency type
Blockchain Analytics Companies
Phase 2 (Ransom payment)
Centralized Exchanges
Merchant Services
P2P Exchanges
Mixers
High Risk Exchanges
Dark Net Market
VASP (fiat exchanged for crypto)
VASP (fiat exchanged for crypto)
Initial ransomware wallet information
Blockchain Analytics Companies
Credit card company
Related Suspicious Wallet(s)
Recipient wallet information
Blockchain Analytics Companies
Cryptocurrency Businesses
Remittance Service Provider
Victim bank information
Wire Transfer
Automated clearing house
Credit Card
Phase 1 (Attack and fiat transactions)
Phase 3 (Obfuscation and cash out)
VASP (crypto exchanged for fiat)
VASP (crypto exchanged for fiat)
Law Enforcement
Financial Institution
Depository Institutions (fiat transaction)
Ransomware funds in crypto wallet (to spend)
Threat actor bank information
Blockchain Analytics Companies
Victim bank information
CASH OUT
CASH OUT
Cryptocurrency type
Cryptocurrency exchanges
Victim/Org on behalf of victim
Resourcing
Ransomware Attack
DFIR Firm
Victim IP address(es)
Transaction hash of payment
Blockchain Analytics Companies
Managed Security Service Providers
Contact information for victim
VPN service
Threat actor communications
Threat actor bank information
Sample encrypted file
Internet service providers
Malicious attacker infrastructure information
Ransom note
Threat Intelligence Firm
Security Researchers
Ransomware variant
Financial Institution
Antivirus vendors
Hosting providers
Crypting service provider
Cloud providers
Domain registrars
Operating system vendors
Bulletproof hosting
Transaction amount requested in fiat
Hash decryption service
Sandboxes
Webshell vendor
Cyber insurance company

Case 4

Ransomware groups leverage tooling providers, cloud providers, EDR vendors, domain registrars, and antivirus vendors to prepare for a ransomware attack.

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:

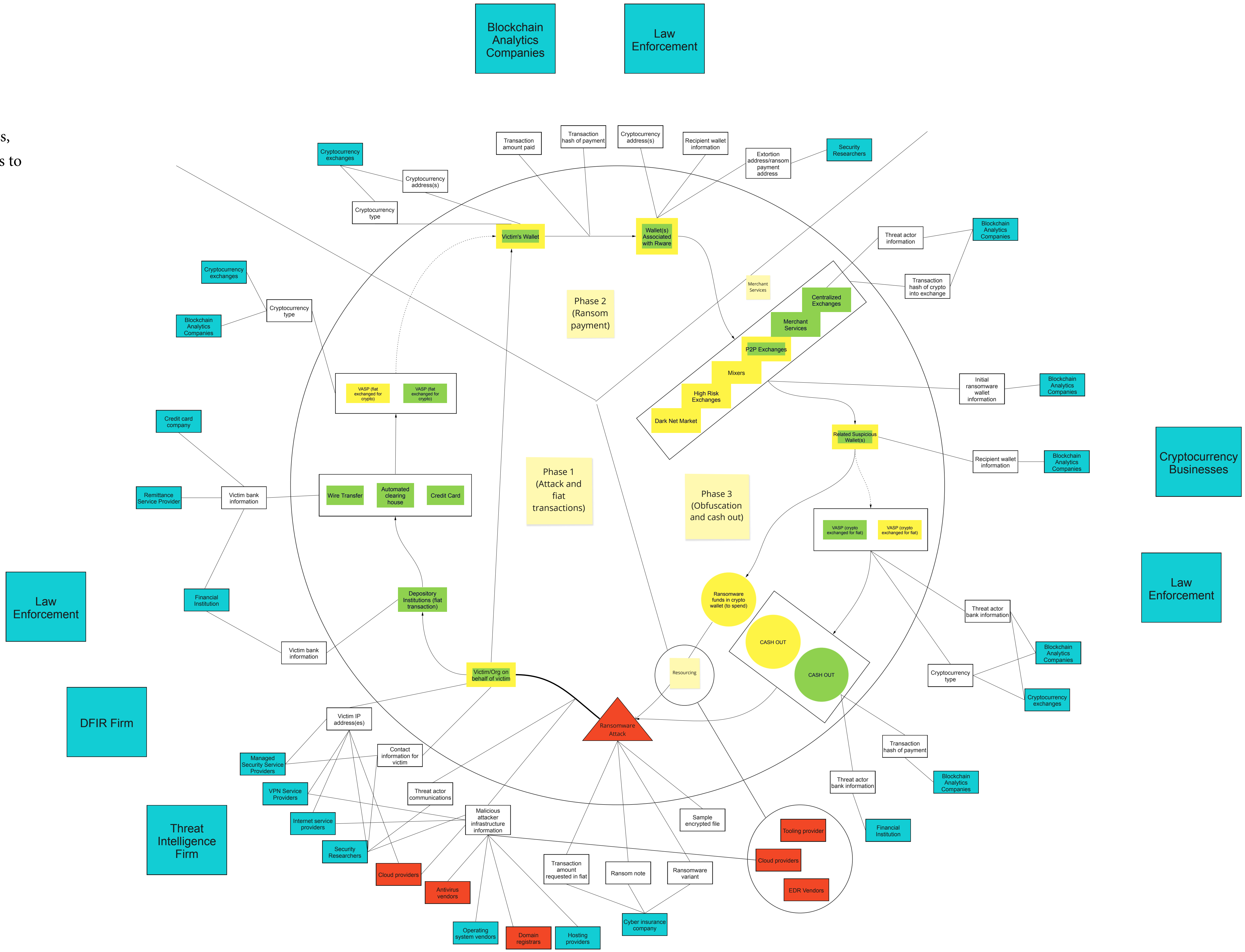
🟩 Regulated avenue

🟨 Unregulated or noncompliant avenue

🟦 Entities with visibility

🟥 Entities leveraged by threat actors to carry out a ransomware attack

----- Escrow



Blockchain Analytics Companies
Law Enforcement
Cryptocurrency exchanges
Cryptocurrency address(s)
Cryptocurrency type
Transaction amount paid
Transaction hash of payment
Cryptocurrency address(s)
Recipient wallet information
Extortion address/ransom payment address
Security Researchers
Victim's Wallet
Wallet(s) Associated with Rware
Cryptocurrency exchanges
Blockchain Analytics Companies
Cryptocurrency type
Phase 2 (Ransom payment)
Merchant Services
Threat actor information
Blockchain Analytics Companies
Transaction hash of crypto into exchange
Centralized Exchanges
Merchant Services
P2P Exchanges
Mixers
High Risk Exchanges
Dark Net Market
VASP (fiat exchanged for crypto)
VASP (fiat exchanged for crypto)
Initial ransomware wallet information
Blockchain Analytics Companies
Credit card company
Related Suspicious Wallet(s)
Recipient wallet information
Blockchain Analytics Companies
Cryptocurrency Businesses
Remittance Service Provider
Victim bank information
Wire Transfer
Automated clearing house
Credit Card
Phase 1 (Attack and fiat transactions)
Phase 3 (Obfuscation and cash out)
VASP (crypto exchanged for fiat)
VASP (crypto exchanged for fiat)
Law Enforcement
Financial Institution
Depository Institutions (fiat transaction)
Ransomware funds in crypto wallet (to spend)
Threat actor bank information
Law Enforcement
Victim bank information
CASH OUT
CASH OUT
Blockchain Analytics Companies
Victim/Org on behalf of victim
Resourcing
Cryptocurrency type
Cryptocurrency exchanges
DFIR Firm
Victim IP address(es)
Ransomware Attack
Managed Security Service Providers
Contact information for victim
Transaction hash of payment
Threat actor bank information
Blockchain Analytics Companies
VPN Service Providers
Threat actor communications
Malicious attacker infrastructure information
Sample encrypted file
Threat Intelligence Firm
Internet service providers
Tooling provider
Financial Institution
Security Researchers
Cloud providers
Cloud providers
Transaction amount requested in fiat
Ransom note
Ransomware variant
Antivirus vendors
EDR Vendors
Cyber insurance company
Operating system vendors
Domain registrars
Hosting providers

Composite Map

Aggregates the data from cases 1-4.

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:

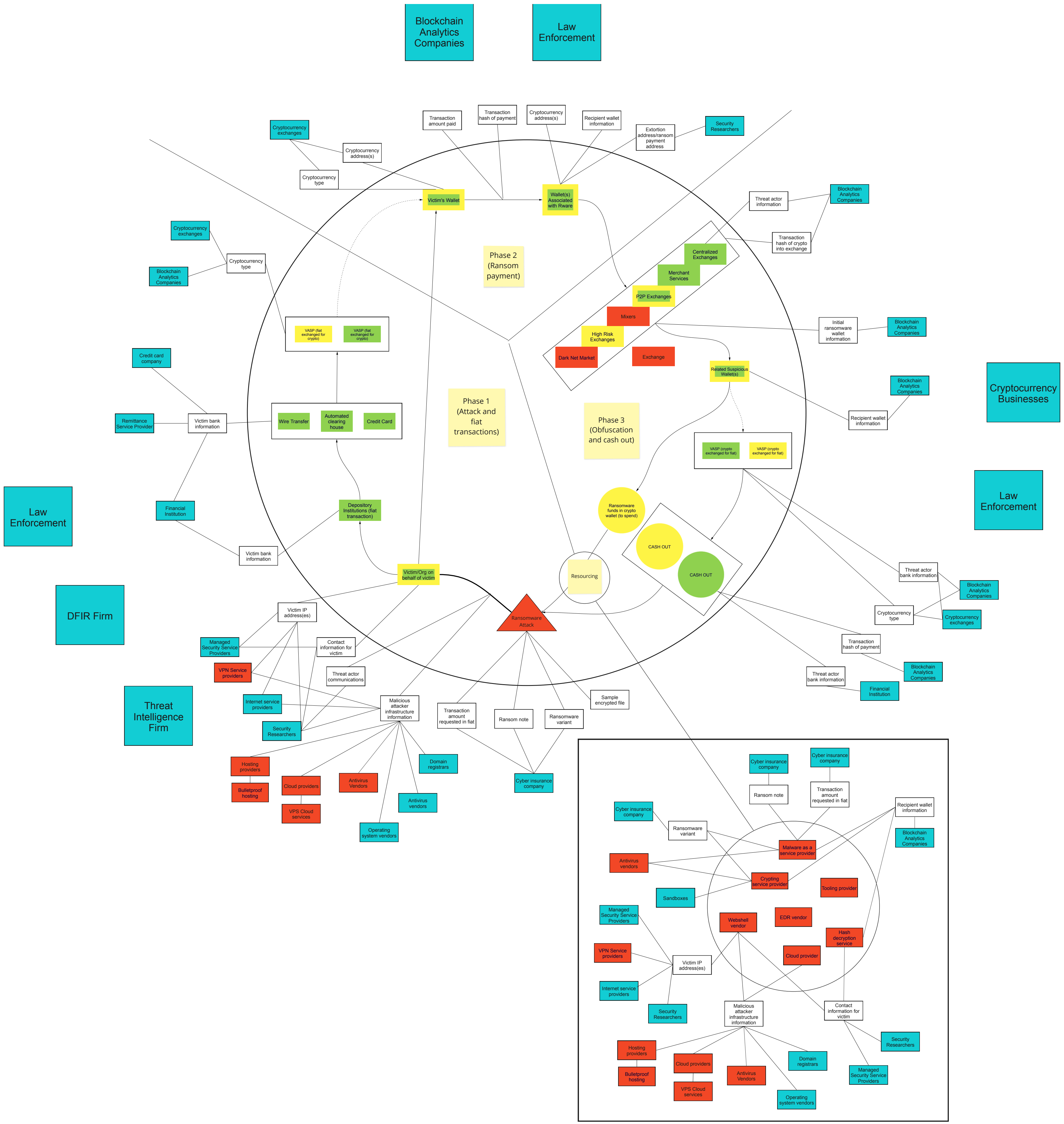
🟩 Regulated avenue

🟨 Unregulated or noncompliant avenue

🟦 Entities with visibility

🟥 Entities leveraged by threat actors to carry out a ransomware attack

----- Escrow



Blockchain Analytics Companies
Law Enforcement
Transaction amount paid
Transaction hash of payment
Cryptocurrency address(s)
Recipient wallet information
Extortion address/ransom payment address
Security Researchers
Cryptocurrency exchanges
Cryptocurrency address(s)
Cryptocurrency type
Victim's Wallet
Wallet(s) Associated with Rware
Threat actor information
Blockchain Analytics Companies
Transaction hash of crypto into exchange
Cryptocurrency exchanges
Cryptocurrency type
Blockchain Analytics Companies
Phase 2 (Ransom payment)
Centralized Exchanges
Merchant Services
P2P Exchanges
Mixers
High Risk Exchanges
Dark Net Market
Exchange
VASP (fiat exchanged for crypto)
VASP (fiat exchanged for crypto)
Initial ransomware wallet information
Blockchain Analytics Companies
Related Suspicious Wallet(s)
Blockchain Analytics Companies
Cryptocurrency Businesses
Recipient wallet information
Credit card company
Remittance Service Provider
Victim bank information
Wire Transfer
Automated clearing house
Credit Card
Phase 1 (Attack and fiat transactions)
Phase 3 (Obfuscation and cash out)
VASP (crypto exchanged for fiat)
VASP (crypto exchanged for fiat)
Law Enforcement
Law Enforcement
Financial Institution
Depository Institutions (fiat transaction)
Ransomware funds in crypto wallet (to spend)
CASH OUT
CASH OUT
Victim bank information
Victim/Org on behalf of victim
Resourcing
Threat actor bank information
Blockchain Analytics Companies
Cryptocurrency type
Cryptocurrency exchanges
DFIR Firm
Victim IP address(es)
Ransomware Attack
Managed Security Service Providers
Contact information for victim
Transaction hash of payment
VPN Service providers
Threat actor communications
Threat actor bank information
Blockchain Analytics Companies
Financial Institution
Threat Intelligence Firm
Internet service providers
Malicious attacker infrastructure information
Transaction amount requested in fiat
Ransom note
Ransomware variant
Sample encrypted file
Security Researchers
Hosting providers
Bulletproof hosting
Cloud providers
VPS Cloud services
Antivirus Vendors
Domain registrars
Antivirus vendors
Operating system vendors
Cyber insurance company
Cyber insurance company
Cyber insurance company
Ransom note
Transaction amount requested in fiat
Cyber insurance company
Ransomware variant
Recipient wallet information
Blockchain Analytics Companies
Malware as a service provider
Antivirus vendors
Crypting service provider
Tooling provider
Sandboxes
Managed Security Service Providers
Webshell vendor
EDR vendor
Hash decryption service
VPN Service providers
Cloud provider
Victim IP address(es)
Internet service providers
Security Researchers
Malicious attacker infrastructure information
Contact information for victim
Security Researchers
Hosting providers
Cloud providers
Antivirus Vendors
Domain registrars
Managed Security Service Providers
Bulletproof hosting
VPS Cloud services
Operating system vendors

Results

The results of this mini-pilot indicate several additional entities (blue tiles) to include in the map, as well as a new "resourcing" phase (in the "magnified" circle in the bottom right quadrant of each map), where threat actors develop attacker infrastructure and perfect their tools before carrying out an attack.

The mini-pilot identifies entities previously left off the map that are directly and tangentially related to ransomware payments. In the innermost circle, the data indicates that cryptocurrency mixers, cryptocurrency exchanges, and dark net markets are commonly used to launder payments. The majority of the entities identified by this mini-pilot, however, are only tangentially related to ransomware payments. In other words, while they are not directly involved in paying ransoms, obfuscating cryptocurrency, or the cash out process, threat actors use the tools and services they provide to carry out attacks. This distinction could present the opportunity for a number of avenues to disrupt the payment ecosystem and thereby meaningfully impact the ongoing use of ransomware for financial gain.

As a result of this mini-pilot, IST staff highlight two distinct types of entities that ransomware threat actors leverage to carry out attacks. Some entities that threat actors use exist for precisely this type of malicious activity and are not generally used by the public. This group includes:

- Crypting service providers
- Cryptocurrency mixers
- Darknet markets
- Hash decryption services
- Malware-as-a-service providers
- Webshell vendors

Threat actors also consistently leverage legitimate entities:

- Antivirus vendors
- Cloud service providers and VPS Cloud services
- Cryptocurrency exchanges
- EDR vendors
- Hosting providers, especially bulletproof hosting
- Tooling providers
- VPN service providers

The results of this mini-pilot suggest that each entity illustrated in the original ransomware payment ecosystem map may have an opportunity to help add friction to the ecosystem, regardless of their direct involvement in ransom payments.

A Note on Changes to the Original Ransomware Payment Ecosystem Map

In developing this mini-pilot, IST staff, in collaboration with RTF members, identified two inaccuracies in the original ransomware payment ecosystem map. First, upon noting that threat actors frequently use VPN service providers to leverage their attacks we elected to add this entity to the original ransomware payment ecosystem map. Second, members of the RTF identified that merchant services, which enable customers to send and receive currency and are included in the obfuscation section of the map, are usually regulated. To reflect this characteristic, this tile is now green.

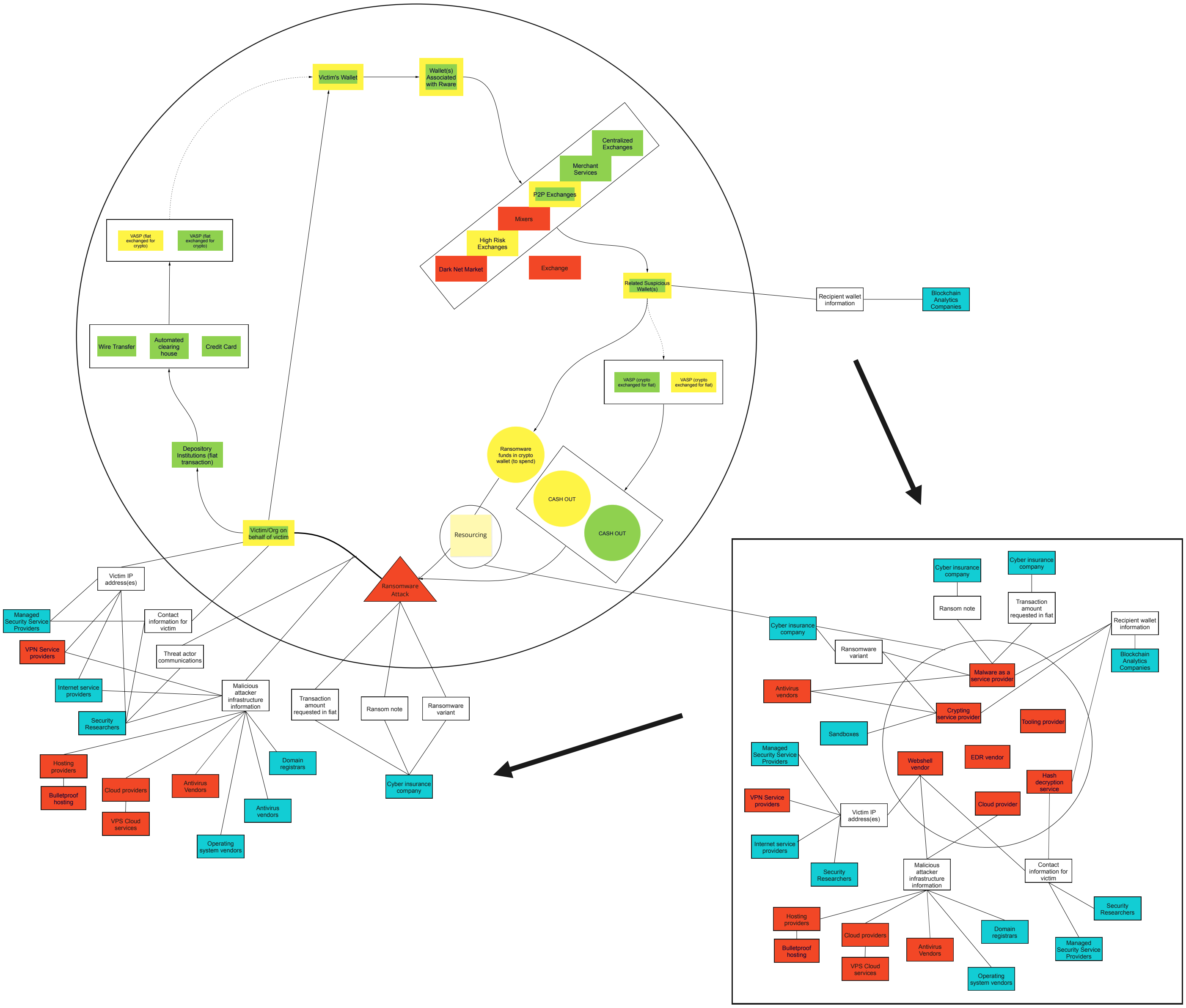
Next Steps

The results of this mini-pilot suggest at least three potentially impactful opportunities to disrupt ransomware attacks.

First, some entities employed by threat actors, like malware-as-a-service providers, crypting service providers, and webshell vendors, among others, exist precisely for malicious activity. In future work, IST staff and the Ransomware Task Force will explore opportunities to curb the proliferation of these types of entities. Among other opportunities, enhanced information sharing about these entities among stakeholders included in the map could be impactful. Encouraging information sharing could require additional incentives, such as regulation or other governmental action.

Second, threat actors at times use legitimate entities, like cloud service providers, VPN providers, and antivirus vendors, for purposes that are not benign. The use of these entities occurs primarily in the resourcing phase and phase one of the ransomware payment ecosystem map–after a ransomware attack occurs but before the ransom is paid. This suggests the possibility of information sharing opportunities that could, if structured appropriately, provide vital indicators to law enforcement and others with the ability to intervene in the attacks, thereby adding friction for threat actors.

Finally, the inclusion of the resourcing phase illustrates the cyclical nature of the ransomware ecosystem. As shown in the graphic below, this mini-pilot suggests that, in some cases, threat actors pay for tools and services to develop attacker infrastructure using cryptocurrency wallets associated with prior attacks. This points to the possibility that, with enough contextual information, entities like blockchain analytics companies and cryptocurrency businesses, among others, might be able to share cryptocurrency wallet information with law enforcement and other relevant stakeholders. This could help identify illicit proceeds as they move through the payment process and prevent future attacks by those same threat actors.


Victim's Wallet
Wallet(s) Associated with Rware
Centralized Exchanges
Merchant Services
P2P Exchanges
Mixers
High Risk Exchanges
Dark Net Market
Exchange
Related Suspicious Wallet(s)
Recipient wallet information
Blockchain Analytics Companies
VASP (fiat exchanged for crypto)
VASP (fiat exchanged for crypto)
Wire Transfer
Automated clearing house
Credit Card
Depository Institutions (fiat transaction)
VASP (crypto exchanged for fiat)
VASP (crypto exchanged for fiat)
Ransomware funds in crypto wallet (to spend)
CASH OUT
CASH OUT
Resourcing
Victim/Org on behalf of victim
Ransomware Attack
Victim IP address(es)
Managed Security Service Providers
Contact information for victim
VPN Service providers
Threat actor communications
Internet service providers
Malicious attacker infrastructure information
Transaction amount requested in fiat
Ransom note
Ransomware variant
Security Researchers
Hosting providers
Bulletproof hosting
Cloud providers
VPS Cloud services
Antivirus Vendors
Domain registrars
Antivirus vendors
Operating system vendors
Cyber insurance company
Cyber insurance company
Cyber insurance company
Ransom note
Transaction amount requested in fiat
Recipient wallet information
Blockchain Analytics Companies
Cyber insurance company
Ransomware variant
Malware as a service provider
Antivirus vendors
Crypting service provider
Tooling provider
Sandboxes
Managed Security Service Providers
Webshell vendor
EDR vendor
Hash decryption service
VPN Service providers
Victim IP address(es)
Cloud provider
Internet service providers
Security Researchers
Malicious attacker infrastructure information
Contact information for victim
Security Researchers
Hosting providers
Bulletproof hosting
Cloud providers
VPS Cloud services
Antivirus Vendors
Domain registrars
Operating system vendors
Managed Security Service Providers

The arrows indicate that threat actors often reuse cryptocurrency wallets, and pay for tools and services required to carry out ransomware attacks using wallets associated with prior attacks. This highlights the cyclical nature of the ransomware cycle.

Conclusion

In the coming months, using this mini-pilot as a launching point, IST staff and RTF working groups will identify potential opportunities to disrupt the ransomware payment ecosystem and subvert the profitability of this crime. In particular, the group will focus on testing how key barriers and enablers could prompt change in the ecosystem and identifying hot spots in the payment ecosystem where disruption might have an outsized effect on threat actors, as some tools and services are easier to replace or replicate than others. This mini-pilot indicates that there may be a range of opportunities to add friction for all entities depicted in the ransomware payment ecosystem map, and that disrupting this ecosystem requires not just a multistakeholder approach but a strategic one. By centering threat actor behavior, it may be possible not only to disrupt the ecosystem, but to predict where these actors will move as the ecosystem tightens its grip on illicit activity.

INSTITUTE FOR SECURITY AND TECHNOLOGY
www.securityandtechnology.org

info@securityandtechnology.org