A Tale of Two Markets: Investigating the Ransomware Payments Economy

Kris Oosthoek
Delft University of Technology

Jack Cable
Stanford University

Georgios Smaragdakis
Delft University of Technology

ABSTRACT

Ransomware attacks are among the most severe cyber threats. They have made headlines in recent years by threatening the operation of governments, critical infrastructure, and corporations. Collecting and analyzing ransomware data is an important step towards understanding the spread of ransomware and designing effective defense mechanisms. We report on our experience operating `Ransomwhere`, an open crowdsourced ransomware payment aggregator to collect information from victims of ransomware attacks. With `Ransomwhere`, we have gathered around 13.5 thousand ransom payments to more than 87 criminal ransomware actors with total payments of more than $101 million. Leveraging the transparent nature of Bitcoin, the cryptocurrency used for most ransomware payments, we characterize the evolving ransomware criminal structure and ransom laundering strategies. Our analysis shows that there are two parallel ransomware criminal markets: commodity ransomware and Ransomware as a Service (RaaS). We notice striking differences between the two markets in the way that cryptocurrency resources are utilized, revenue per transaction, and ransom laundering efficiency. Although it is relatively easy to identify choke points in commodity ransomware payment activity, it is more difficult to do the same for RaaS.

1 INTRODUCTION

Ransomware, a form of malware designed to encrypt a victim's files and make them unusable without payment, has quickly become a threat to the functioning of many institutions and corporations around the globe. In 2021 alone, ransomware caused major hospital disruptions in Ireland [3], empty supermarket shelves in the Netherlands [8], the closing of 800 supermarket stores in Sweden [4], and gasoline shortages in the United States [21]. In a recent report, the European Union Agency for Cybersecurity (ENISA) ranked ransomware as the "prime threat for 2020-2021" [14]. The U.S. government reacted to high profile attacks against U.S. industries by declaring ransomware a national security threat and announcing a "coordinated campaign to counter ransomware" [22]. Other governments, including the United Kingdom [38], Australia [23], Canada [13], and law enforcement agencies, such as the FBI [39] and Europol [12], have also launched similar programs to defend against ransomware and offer help to victims.

To the criminal actors behind these attacks, the resulting disruption is just 'collateral damage'. A handful of groups and individuals, with names such as NetWalker, Conti, REvil and DarkSide, have received tens of millions of dollars as ransom. But this is just the top of the food chain in an ecosystem with many grey areas, especially when it comes to laundering illicit proceedings. In this article, we will provide a closer look at the ecosystem behind many of the attacks plaguing businesses and societies, known as Ransomware as a Service (RaaS).

Cryptocurrency remains the payment method of choice for criminal ransomware actors. While many cryptocurrencies exist, Bitcoin is preferred due to its network effects, resulting in wide exchange options. Bitcoin's sound monetary features as a medium of exchange, unit of account and store of value make it as attractive to criminals as it is to regular citizens. According to the U.S. Department of Treasury, based on data from the first half of 2021, the "vast majority" of reported ransomware payments were made in Bitcoin [29]. However, significant discrepancies exist between total ransomware revenues reported by industry and government outlets. Law enforcement agencies have started to disrupt ransomware actors by obtaining personal information of threat actors from Bitcoin exchanges. This is realized through anti-money laundering regulations such as Know Your Customer (KYC), which require legal identity verification during registration with a given service. While cryptocurrencies such as Bitcoin enable ransomware, blockchain technology also offers unprecedented opportunities for forensic analysis and intelligence gathering. Using our crowdsourced ransomware payment aggregator, `Ransomwhere`, we compile a dataset of 7,321 Bitcoin addresses which received ransom payments, based on which we shed light on the structure and state of the ransomware ecosystem.

Our contributions are as follows:

- We collect and analyze the largest public dataset of ransomware activity to date, which includes 13,497

ransom payments to 87 criminal actors over the last five years, worth more than $101 million.
- We characterize the evolving ransomware ecosystem. Our analysis shows that there are two parallel ransomware markets: commodity and RaaS. After 2019, we observe the rapid rise of RaaS, which achieves higher revenue per address and transaction, and higher overall revenue.
- We also characterize ransom laundering strategies by commodity ransomware and RaaS actors. Our analysis of more than 13 thousand transfers shows striking differences in laundering time, utilization of exchanges, and other means to cash out ransom payments.
- We discuss difficulties in defending against professionally-operated RaaS and we propose potential manners of tracing back RaaS cryptocurrency activity.
- To enable future research in this area, we make our aggregator, `Ransomwhere`, and the underlying ransomware payments of our analysis publicly available at [6].

2 THE RANSOMWARE ECOSYSTEM

The ransomware ecosystem can be largely divided into two categories: commodity ransomware and ransomware as a service (RaaS).

2.1 Commodity Ransomware

In the early years of ransomware, the majority of ransomware that spread can be characterized as 'commodity' ransomware. Commodity ransomware is distinguished by widespread targeting, fixed ransom demands, and technically-adept operators. It usually targets a single device. Actors behind commodity ransomware are usually technically savvy, as most of the time it is developed and deployed by the same person. Commodity ransomware operators take advantage of preexisting work, often copying and modifying leaked or shared source code, causing the formation of ransomware *families*. Historically, most commodity ransomware campaigns utilized phishing emails as the primary delivery vector and exploited vulnerabilities in common word processing and spreadsheet software, if not directly via malicious executables. The modus operandi was mass exploitation, rather than targeting specific victims or corporations.

Exemplary are the WannaCry and NotPetya ransomware families, which over the course of only two months impacted tens of thousands of organizations in over 150 countries by exploiting a vulnerability allegedly stolen from the NSA [16]. By today's standards, both families were poorly coded and their payment systems were not ready for business (although allegedly this was on purpose with NotPetya [15]).

Applying the conventional advice of having proper backup and contingency plan was thought to defend against ransomware. The initial philosophy was that a quick ability to restore would make it unnecessary to pay, impairing the financial incentive of ransomware operators. But it turned out that what we now regard as a commodity was just a proving ground for more destructive, widespread forms of ransomware.

2.2 Ransomware as a Service (RaaS)

While the first reports of Ransomware as a Service (RaaS) emerged in 2016, it wasn't until 2019 that RaaS became widespread, rapidly capturing a large share of the ransomware market. We define RaaS as ransomware created by a core team of developers who license their malware on an affiliate basis. They often provide a payment portal (typically over Tor, an anonymous web protocol), allowing negotiation with victims and dynamic generation of payment addresses (most often Bitcoin). RaaS frequently employs a double extortion scheme, not only encrypting victims' data, but also threatening to leak their data publicly if a ransom is not paid.

The rise of RaaS has enabled existing criminal groups to shift to a lucrative new business model where lower-skilled affiliates can access exploits and techniques previously reserved for highly-skilled criminals. This was exemplified by a leaked playbook from the RaaS group Conti, which enables novice actors to compromise enterprise networks [35]. RaaS affiliates can differ markedly in their approaches. Some scan the entire internet and compromise any victims they can. Once they have identified the victim, they engage in price discrimination based on the victim company's size. Affiliates may even use financial documents obtained in the attack to justify higher prices [20]. Another strategy, known as *big game hunting*, targets big corporations that can afford to pay a high ransom. Darkside is one of most notable RaaS families whose affiliates practice big game hunting, including the notable Colonial Pipeline attack in 2021 [19].

RaaS families often rely on spear phishing over the mass phishing mails utilized by commodity ransomware groups. They also exploit recently disclosed vulnerabilities, taking advantage of vulnerable remote and virtual desktop services [9]. RaaS has lowered the barrier to entry into cyber-criminality, as it has removed the initial expenditure to develop effective ransomware. As a result, attacks can be performed with near zero cost. Combined with high ransom demands, this has led to a low-risk, high reward criminal scheme.

RaaS has effectively *weaponized* the unpatched internet-facing technology of many unwitting organizations. Such

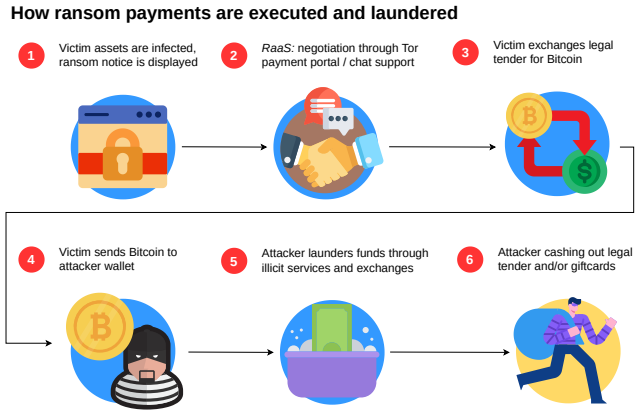

Figure 1: General course of a ransom payment and its laundering.

organizations have significant financial interest to have systems restored and get back to business after a ransomware attack. Cryptocurrencies enable ransomware actors to directly monetize these vulnerabilities at a scale never seen before. In this paper, we regard the functioning of ransomware actors through what is typically the last mile of the attack.

Figure 1 shows the general course of events after a ransomware infection, when the victim decides to pay the attacker (step 1). In the case of commodity ransomware families, the ransom demand price is fixed and negotiation with the attacker is not necessary. With RaaS, attackers usually run chat-based services to interact with victims and negotiate the final ransom amount (step 2). After this, a victim will usually exchange fiat legal tender for cryptocurrency such as Bitcoin at an exchange platform (step 3) and then send it to the attacker's wallet (step 4). The attacker will then usually launder the obtained Bitcoin through various services (step 5) in order to obfuscate ownership and reduce the risk of de-anonymization before cashing out (step 6).

3 METHODOLOGY

In this section, we describe how we collected data of ransom payments and ransomware actors in our study.

3.1 Addresses involved in Ransom Payments

We obtain ransomware Bitcoin addresses from our crowdsourced payment aggregator `Ransomwhere`. The `Ransomwhere` dataset contains Bitcoin addresses and associated families collected from open-source datasets and publicly-submitted crowdsourced reports. In total, the Ransomwhere dataset contains 7,457 Bitcoin addresses and their corresponding ransomware families.

Table 1: Ransomware Dataset Statistics

Data	Commodity	RaaS	Total
Unique Actors	71	16	87
Bitcoin Addresses	161	7,160	7,321
Received Transactions (Payments)	4,799	8,698	13,497
Transferred Transactions (Laundering)	4,557	8,540	13,097

To seed the dataset, we collected data from several public sources. We imported addresses from Paquet-Clouston et al. [31], who collected 7,222 addresses and labeled families representing approximately $12.7 million in payments. This dataset provides us with, among other ransomware families, 7,014 addresses belonging to Locky. We further collected 37 addresses and associated families from the AT&T Alien Labs Open Threat Exchange, an open threat intelligence sharing platform [1].

Members of the public may submit reports at our crowdsourced payment aggregator `Ransomwhere` [6]. We received 99 reports containing 198 addresses over a 6-month period from June 2021 to December 2021. While this is a lower number of addresses, they represent the majority of ransomware payment value in our dataset, as seen in Table 2. In order to verify reports, the reporter must include the relevant Bitcoin addresses and the associated ransomware family. In addition, they must provide evidence of the ransom demand, such as a screenshot of the ransom payment portal or a ransom message on an infected computer. Some addresses were involved in more than one report. All reports were manually reviewed before being added to the dataset. We did not accept reports that were inaccurate or were not related to ransomware (e.g., addresses involved in extortion scam emails).

All reported ransom addresses were Bitcoin addresses. Due to the transparent nature of Bitcoin it is possible to verify that the collected addresses indeed received payments. Using our own Bitcoin full node, we scraped all transactions for the addresses in our dataset. Overall, 7,323 out of 7,457 Bitcoin addresses were involved in at least one ransom payment. We discarded 134 addresses that did not receive any payment. We have queried Tor using a solution from a peer researcher [34] for all Bitcoin addresses in our dataset to rule out the chance of an address being used for cybercrime purposes other than ransomware. Based on this, we excluded 2 addresses belonging to a cache of Bitcoin seized by the U.S. Department of Justice after the closing of the SilkRoad

Table 2: Composition of the dataset

Source	Total USD	# BTC Addr.
Ransomwhere reports [6]	$87M	198
Paquet-Clouston et al. [31]	$10M	7,222
AlienVault OTX [1]	$4M	37
Total	***$101M***	***7,457***

darkweb market [24], which originally appeared in the Paquet-Clouston et al. dataset. After these steps, the final number of addresses considered for our analysis is 7,321. For a summary of our dataset we refer to Table 1. Table 2 provides an overview of the sourcing of Bitcoin addresses included in the dataset.

3.2 Ransom Payments and Laundering

The transparency of Bitcoin also allows us to collect information about ransom payments, including the amount of Bitcoin received. For each address, we collected the number of incoming (payments) and outgoing (transfers) transactions, their value in Bitcoin, and their timestamp. We calculated the USD value of each transaction using the BTC-USD daily closing rate on the day of the transaction. This serves as an approximate ransom payment and not the exact amount in USD the criminal actors requested or later profited. The total ransom paid to addresses in our dataset is $101,297,569. The lowest payment received is $1, and the highest is $11,042,163. The median payment value is $1,176.

In collaboration with Crystal Blockchain [5], we tracked the destination of outgoing transactions, i.e., transfers. In order to estimate addresses' potential for illicit use, Crystal Blockchain utilizes clustering heuristics such as one-time change address and common-input-ownership [41], as well as human collection of off-chain data from various cryptocurrency services. In addition to this, Crystal Blockchain scrapes online forums and other Internet services for Bitcoin addresses and their associated real-world entity. Based on this, it is possible to track payments several hops from the original deposit address. To have the most reliable view, in our analysis we have only studied the direct destination of ransom payments (first hop). Based on the characterization of the involved addresses across the path, we are able to study the laundering strategies of ransomware groups as well as the time needed to wash out the money (see Section 5).

3.3 Ransomware Actors

We obtained addresses and labeled families as described in Section 3.1. We categorized each ransomware family as used by either commodity ransomware or RaaS actors. Ransomware is generally categorized as RaaS due to the use of an affiliate structure, with the ransomware developer (operator) selling the ransomware to criminal actors either based on a commission for each ransom paid, or a flat monthly fee (*as a service*, like many subscription-based services). As there does not exist any comprehensive public list of RaaS groups, we have labeled a family as RaaS if a reliable industry or law enforcement source claims that a given ransomware is sold *as a service*. A list of commodity and RaaS families in our dataset is presented in Table 3.

Table 3: Ransomware families in the dataset

Name	#Addrs.	Name (contd.)	#Addrs.
Locky	7037	DarkSide	3
NetWalker	66	MedusaLocker	3
SamSam	48	NotPetya	3
Ryuk	40	GlobeImposter	3
Conti	27	ThunderCrypt	3
Qlocker	22	Nemucod	3
JigSaw	11	LockBit 2.0	2
CryptConsole	10	Globe v2	2
Egregor	9	EDA2	2
DMALocker v3	9	Flyper	2
Globe v3	7	Black Kingdom	2
REvil	7	CryptoLocker	2
CryptoTorLocker2015	7	AvosLocker	2
HC6/HC7	6	NoobCrypt	2
Globe	5	VenusLocker	2
WannaCry	5	XLocker v5	2
TeslaCrypt	5	Chimera	2
CTB-Locker	5	Badblock	2
Xorist	4	Other Groups/Families*	50

* 50 families with 1 address each. RaaS actors are highlighted.

3.4 Limitations

Our dataset of Bitcoin addresses is the largest public collection of ransomware payment addresses collected to date, based on total USD value. While this allows for a unique view on the ransomware financial ecosystem, it is not exhaustive. An inherent limitation of any research using adversary artifacts is its dependence on the availability of artifacts that bad actors have an interest to hide. Furthermore victims might have an interest to not report addresses, as they prefer keeping attacks undisclosed. We note that certain families, such as NetWalker, may be overrepresented in our dataset due to us having more complete data on these families. Despite this limitation, we believe that our dataset provides a valuable, if incomplete, representation of ransomware payments over many years. This broad view provides a better reflection of the state of affairs than simply focusing on a few families. We hope that this can lay the groundwork for further public data collection in the future, and encourage anyone to submit data at `Ransomwhere` [6].

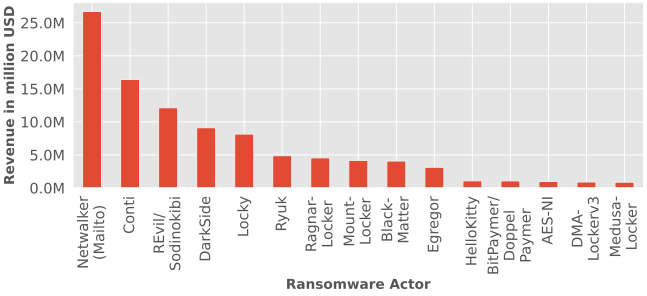

Figure 2: Revenue per ransomware actor.

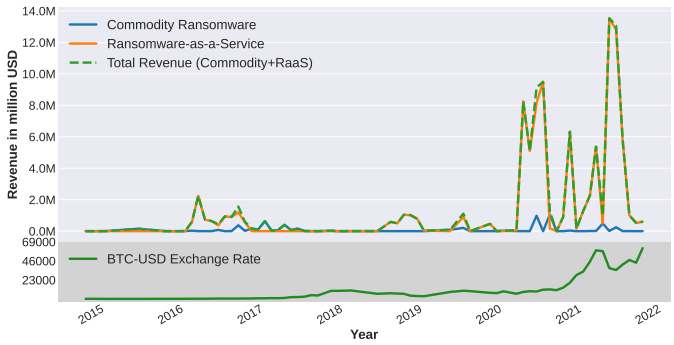

Figure 3: USD revenue for commodity and RaaS.

4 RANSOM PAYMENT ANALYSIS

In this section, we analyze 13,497 payments to the Bitcoin addresses in our dataset (see Table 1). A payment is a transaction received by an address in our dataset. Table 3 lists the ransomware families used by the actors in our dataset. Our dataset contains Bitcoin addresses associated with 87 commodity ransomware or RaaS actors. For reasons of brevity, families for which our dataset contains just 1 address are excluded from Table 3. The 16 actors that are classified as RaaS, highlighted in Table 3, account for 7,160 out of 7,321 addresses in our dataset. As mentioned previously, for full review our dataset is publicly available [6].

Ransomware victims typically create an account with a reputable exchange platform to buy Bitcoin with fiat currency. Then, victims perform a transaction (payment) to the address provided by the ransomware actor. In our dataset, payment transactions to ransomware addresses tend to originate one to two hops away from reputable exchange platforms, such as Coinbase and Kraken.

4.1 Ransomware Revenue

In Figure 2 we list the 15 ransomware families with the highest revenue. The top-grossing families are dominated by RaaS: NetWalker has the highest revenue, $26.7 million, followed by Conti ($16.4 million), REvil/Sodinokibi ($12.1 million), DarkSide ($9.1 million) and Locky ($8.1 million). Combined, commodity actors account for a total revenue of $5.5 million. Although the number of RaaS actors is significantly lower, they together earned $95.7 million.

Figure 3 shows the accumulated revenue of both commodity ransomware and RaaS actors. We see that, from 2015 until 2019, early RaaS actors, primarily Locky, were earning significant but still relatively low revenue. Commodity actors were also active, but with even lower revenue. As seen in Figure 3, RaaS revenue reached $8.2 million in April 2020. This can be primarily attributed to NetWalker, which actively targeted hospitals and healthcare institutions during the first COVID-19 lockdown in that period [25]. Other revenue peaks caused by RaaS groups are in May and June of 2021, with peaks of $13.5 million and $12.8 million respectively. These spikes are caused by large ransom payments by individual victims. One example of this is a payment to REvil/Sodinokibi on June 1st, 2021, accounting for $11 million. This is a payment by the Brazilian meat processing company JBS, which dominated headlines at the time [18].

Locky has a notorious reputation as one of the biggest ransomware strains in 2016-2017. It is also one of the earliest, if not the first, RaaS families. What stands out apart from its high revenue is its address usage. The actors behind Locky issued new addresses to each victim, a novelty at the time [17]. This is evident in our analysis, with many addresses having only 2 or 3 incoming transactions. According to French court documents, Locky's developer is the same individual who owned BTC-e, a fraudulent exchange [7]. Hence, the actor was able to set up a new address for each payment without raising compliance alarms. Locky is an early, less sophisticated example of a RaaS operation which would serve as an example for many cybercriminals to follow.

4.2 Ransomware Payment Characteristics

RaaS actors are not only more effective in terms of profits, but also in handling payments. They typically have higher revenue per address, while also generating unique addresses for victims. In Figure 4 we show the cumulative distribution of received payments between commodity and RaaS actors. Commodity ransomware actors typically use single wallet addresses to receive hundreds of ransom payments. The highest amount of payments to a single address is 697 to AES-NI, followed by 496 to SynAck and 441 to File-Locker. While these

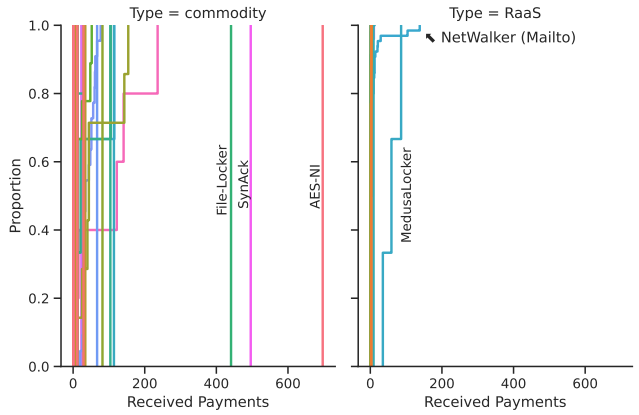

Figure 4: ECDF of payments per address for commodity ransomware and RaaS actors.

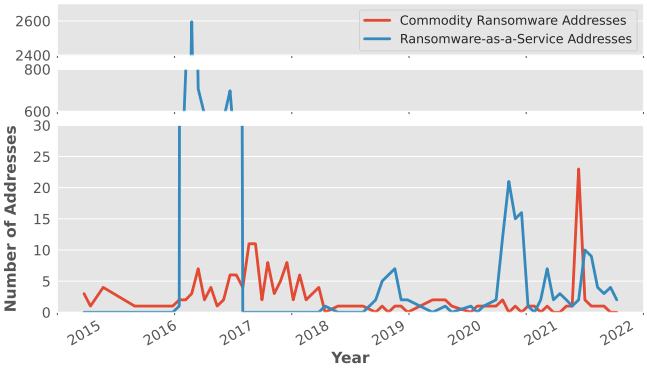

Figure 5: Number of unique payment addresses for commodity ransomware and RaaS.

are outliers, Figure 4 shows that using a single address to receive upwards of 100 payments is not unusual.

In contrast, RaaS actors almost exclusively use a new wallet address to receive each payment, as observed in Figure 4 (right). An outlier is an address associated with NetWalker which has received 138 payments. This address is likely an intermediate payment address, combining payments from many victims, discovered during McAfee Labs's investigation into NetWalker [36].

The distribution of unique addresses per commodity ransomware and RaaS actor over time is presented in Figure 5. In stark contrast to the revenue from ransom activities, presented in Figure 3, the number of addresses used in recent years are low, on the order of tens per month. We suspect that RaaS actors prefer to create new addresses for each new ransom payment in order to ensure their pseudo-anonymity, and thus make legal investigations and takedowns more difficult.

Moreover, our analysis shows that RaaS groups apply better operational security practices when using native Bitcoin functionality for wallets (payment addresses). Bitcoin uses Bitcoin Script to handle transactions between addresses. The script type used defines the wallet type. Pay-to-Public-Key-Hash (P2PKH) addresses have the prefix *1*. This is Bitcoin's legacy address format and the most common address format in our dataset with 7,339 addresses. 46 addresses in our dataset are Pay-to-Script-Hash (P2SH) formatted, recognized by the prefix *3*. To spend received payments in Bitcoin, the recipient must specify a redeem script matching the hash. The script can contain functionalities to increase security, such as time-locks or requiring co-signatures. We only observe this for select actors in our dataset: Qlocker, Netwalker, REvil, Ryuk and Phobos. This could mean that these groups have a specific interest in operational security, as transactions usually are not supported by exchange platforms. Another address format is Pay-to-Witness-Public-Key-Hash (P2WPKH), or Segregated Witness (SegWit) protocols, with prefix *bc1q*. In our dataset 72 addresses have this format, belonging to Conti, Netwalker, SunCrypt, DarkSide and HelloKitty. These are all RaaS actors, which could imply deliberate application of SegWit for additional security over traditional address formats.

5 MONEY LAUNDERING ANALYSIS

In the previous section, we investigated ransom payments by victims to ransomware actors. In the next section, we investigate 13,097 laundering transactions in our dataset (see Table 1) to shed light on how these actors liquidate their illicit earnings.

5.1 Laundering Strategies

To avoid exposing their identity, ransomware actors will usually launder their revenue. After routing funds through one or more services to obfuscate the money trail, it is cashed out as legal tender or monetized through the purchase of voucher codes or physical goods. In Figure 6 we show the number of transfer transactions per address. The number of transfer (outgoing) transactions provides insights into how actors prefer to initialize their laundering. In short, we see that RaaS actors mostly prefer to empty the deposit address in one transaction, whereas commodity actors prefer multiple smaller transactions – up to hundreds, in some cases more. Hence commodity ransomware actors are less sophisticated. For example, three commodity ransomware actors with the most payments per address (File-Locker, SynAck, AES-NI) also

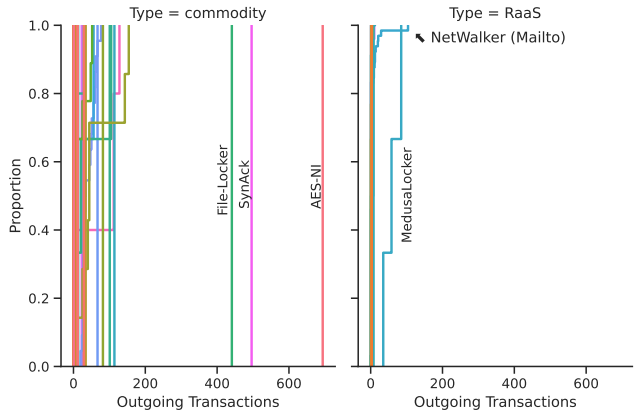

Figure 6: Transfer transactions per Address for commodity and RaaS actors.

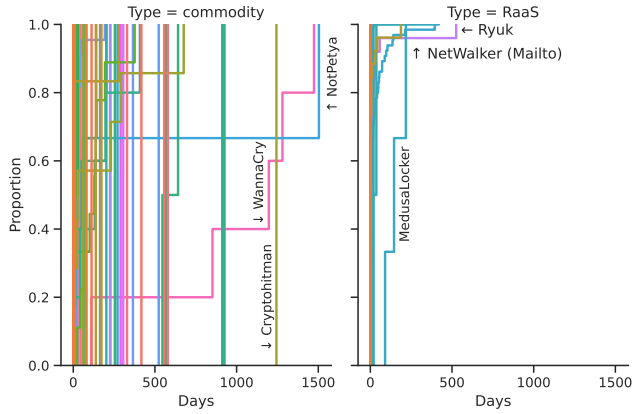

Figure 7: Collect-to-Laundry time for commodity ransomware and RaaS actors.

have the most outgoing transactions. While the motivation for this behavior remains unclear, given that law enforcement scrutiny was relatively low, it is likely that the commodity actors took advantage of the ability to cash out more frequently with little risk. This is further supported by their choice of laundering entities.

Almost all ransomware actors in our dataset launder their proceedings entirely. The speed by which this happens can be inferred from the time between the first incoming payment to and the last outgoing transaction from the deposit address. We define this time duration in which ransomware actors start laundering after having received the payment as *collect-to-laundry time*. Note that this is not the total duration of ransom cash-out, but rather the time spent between receiving the ransom payment and transferring the payment received. Figure 7 shows the ECDF of the collect-to-laundry time (in days) for the commodity ransomware and the RaaS actors in our dataset. RaaS actors have a significantly lower collect-to-laundry time compared to commodity actors. Typically, payments to RaaS actors are transferred away from the deposit address in the first minutes to hours after payment. The few outliers in RaaS are caused by NetWalker and individual addresses associated with actors for which we have multiple addresses in our dataset (Ryuk, Conti). As the illicit funds received by RaaS are washed out quickly and, typically, in full, this suggests that it is more difficult to track payments to RaaS, thus lowering the odds of recovery.

Only a small set of families still have significant portions of their proceedings on the original address. This is the case for NetWalker, which has 20.36% still on an address, MedusaLocker (7.98%) and WannaCry (7.92%). In this case, it is likely that the actor has lost the private key or is incapable to safely launder the ransom, for example due to law enforcement scrutiny. It is known that NetWalker's proceedings have been seized by law enforcement [25], with WannaCry under heavy monitoring and most of the laundering failed [2].

5.2 Challenges in Fighting Laundering

Contrary to popular belief, Bitcoin is not anonymous but pseudo-anonymous. Forensic analysis might link a Bitcoin address to a real-world identity, especially when an exchange platform is used to convert between fiat currency and Bitcoin. In most jurisdictions, legal entities behind such platforms are held to Know Your Customer (KYC) legislation, which requires them to verify the identity of every user signing up to their service. During an investigation, when known illicit Bitcoin is routed through an exchange that requires KYC, authorities have a chance to identify the culprit. Several industry players support law enforcement in such AML investigations, with technology based on clustering algorithms which can link addresses to a service such as an exchange. As seen in Figure 8, we have grouped the data we obtained through Crystal Blockchain in a select set of entities, which are described in Table 4.

Laundering can involve routing illicit funds through several hops before cashing out. As it is difficult to know where actual ownership has terminated after several hops, in this analysis we only study the first hop, i.e., the first transfer transaction. This is the service to which actors transfer funds directly after received them from the victim. As this has the closest link to the payment address, this is the first point of investigation for law enforcement. An actor choosing to use a service implies

Table 4: Laundering Entities Overview

Entity	Description	Evidence
ATM / Payment Provider	Payment gateways for physical/online merchants or ATMs, usually used to launder small amounts	[28]
Dark Market / Illegal Services	Illegal services available on Tor or other Internet services, used to buy illegal server hosting etc.	[11]
Fraudulent Exchange	Exchange platforms officially sanctioned by the US Office of Foreign Assets Control (OFAC)	[7]
Gambling	Online casinos and gambling platforms, used to launder small amounts anonymously	[37]
Low/Moderate ML-Risk Exchange	Exchanges with strict AML/KYC policies might still be used for laundering criminal funds	[33]
Mixers	These services take and 'mix' Bitcoin from various parties to obfuscate ownership	[27]
(Very) High ML-Risk Exchange	Exchanges with lax or no AML/KYC implementations are popular for money laundering	[32]
Wallet Service	Custodial/online wallets, some might have also have privacy features such as mixers.	[37]

that they trust the service, at least enough not to disclose their identity.

Figure 8 shows the proportion of estimated USD value of Bitcoin directly transferred (first hop) to the entities explained in Table 4 for commodity and RaaS actors. Due to limitations in reliably establishing (legal) entities behind an address, the direct transactions in our dataset account for a subset of the total revenue generated by the actors in our dataset. Hence we report using percentages, a best practice used with comparable datasets [40].

Our core observation is that commodity actors do not exhibit a specific laundering strategy, while RaaS actors primarily use fraudulent exchanges and mixers. Mixers are services which take in Bitcoin from cybercriminals or privacy-aware users and combine these in many transactions. This hinders the accurate tracking of Bitcoin, as every client gets their initial deposit (minus service fee) back as a mix of other users' Bitcoin. Thus, it is more difficult to trace the laundering activity of RaaS criminal actors.

When considering fraudulent exchanges together with low- and high-risk exchanges, commodity authors tend to prefer exchanges with a low to moderate risk of money-laundering, and thus perhaps cash out to fiat currency or other cryptocurrencies. It is however also known that cybercriminals have wound down the use of fraudulent exchanges [30]. In a sense, commodity actors do not partake in any systematic laundering at all, whereas RaaS actors use fraudulent (non-KYC) exchanges and mixers, a clear laundering strategy. Based on this, we hypothesize that the chances of recovering payments through law enforcement intervention are higher with commodity ransomware than with RaaS. The money laundering services they use logically leave more user traces (IP address, login session) than mixer services and fraudulent exchanges with obfuscation of ownership by design.

When an actor's collect-to-laundry time is high, a law enforcement investigation may be able to successfully recover the funds. However, in many such cases there is less incentive to intercept transactions due to the comparatively low ransom amounts. The speed by which

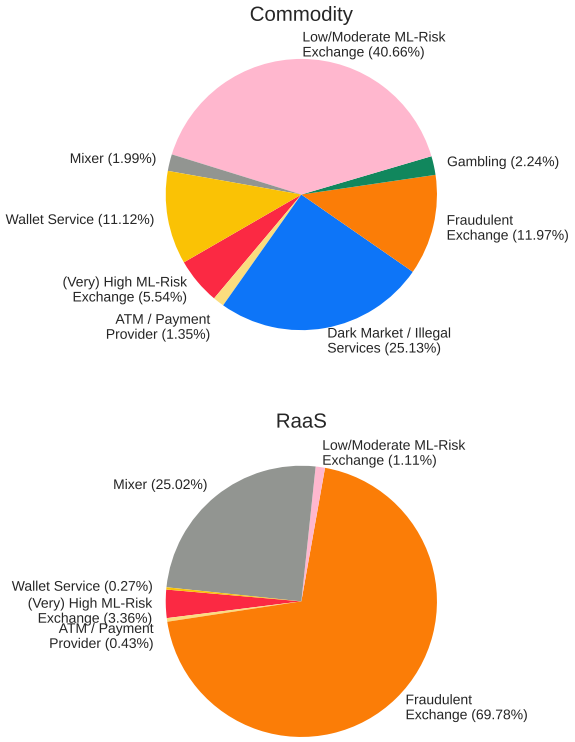

Figure 8: Pie chart of one-hop laundering entities.

RaaS groups transfer funds out suggests criminal sophistication, which is also reflected in their preferred means of laundering. Given this, it is difficult to intercept funds unless law enforcement is already involved at the very moment the payment is made [26].

6 CONCLUSION

Ransomware is a severe, growing threat plaguing our world, built on a cybercriminal business model which monetizes the insufficient security of many organizations.

In this paper, we take a data-driven, "follow the money" approach to characterize the structure and evolution of the ransomware ecosystem. To this end, we report on our

experience in operating `Ransomwhere`, our open crowdsourced ransomware payment aggregator to collect information from victims of ransomware attacks. Through the analysis of a corpus of over 13,500 ransom payments with a total revenue of more than $101 million, we shed light on the practices of these criminal actors over recent years. Our analysis unveils that there are two symbiotic, parallel markets: commodity ransomware actors, and (dominant since 2019) Ransomware as a Service (RaaS) actors. The first is operated by individuals or a small group of programmers, the second by professional cybercriminals who offer their malware on an affiliate basis to typically less technical criminal actors. Due to differences in their attack methods, RaaS can demand higher ransom amounts based on the victim at hand. RaaS is generally also more difficult to defend against, with Initial Access Brokers dedicating their time to obtaining access vectors. Their pricing models reflect factors such as access privilege level, company annual revenue and impact on public infrastructure - incentivizing persistence in breaching less accessible targets.

Our analysis of ransom payments shows that RaaS actors have adopted more sophisticated cryptographic techniques compared to commodity actors in their operation and typically generate one address per victim to hide their identity. This allows RaaS to generate more revenue and with higher level of protection, attracting more criminal groups to use RaaS to perform high profile attacks in recent years. RaaS actors are also more efficient at laundering ransom payments, as they move to launder funds within hours or days. Lastly, RaaS actors transfer revenue from ransom payments to mixers and other sophisticated laundering entities that increase the difficulty for law enforcement agencies to recover ransom payments. By providing an extensive overview of the ransomware economy and making our data available, we hope to provide insight into a cybercriminal economy that poses a severe threats to many organizations and societies, but of which reporting is often fragmented.

We conclude with a few takeaways based on the results of our paper. First, we note the increase of ransomware payment demands in privacy-preserving cryptocurrencies such as Monero [29]. Cybercriminals sometimes place incentivize this by accepting a lower payment in Monero than Bitcoin [29]. The same privacy-preserving properties that make these cryptocurrencies appealing to everyday consumers offer cybercriminals a mechanism to shield their illicit activity and evade law enforcement. While use of such cryptocurrencies is not yet widespread by ransomware actors, likely due to a lack of liquidity in those markets, we expect cybercriminals to further adopt privacy-preserving cryptocurrencies in the years to come. We urge those develop cryptocurrencies to research mechanisms for preserving privacy while still allowing illicit activity to be traced – if not, we may lose an effective mechanism of studying and combating cybercrime.

Second, we encourage more reporting of ransomware attacks and associated payments. We assume that the Ransomwhere dataset represents a fraction of all ransomware attacks that occur, with a majority of attacks going unreported. Various governments are considering mandatory reporting of ransomware attacks. This includes the United States government, which has required critical infrastructure owners and operators to report ransomware attacks, including ransom payments [10]. Further bolstering such reporting, and the public aggregation of payment data, will allow better insight into the business practices of ransomware actors and for more effective action to be taken against these cybercriminals.

ACKNOWLEDGEMENTS

The authors would like to thank Crystal Blockchain for providing data on the laundering of illicit proceedings in our dataset. This work was supported in part by European Research Council (ERC) Starting Grant ResolutioNet (ERC-StG-679158).

REFERENCES

[1] 2021. AT&T Alien Labs Open Threat Exchange. https://cybersecurity.att.com/open-threat-exchange.
[2] BBC. 2017. Wannacry money laundering attempt thwarted. https://www.bbc.com/news/technology-40826056
[3] BBC. 2021. HSE cyber-attack: Irish health service still recovering months after hack. https://www.bbc.com/news/world-europe-58413448.
[4] BBC. 2021. Swedish Coop supermarkets shut due to US ransomware cyber-attack. https://www.bbc.com/news/technology-57707530.
[5] Crystal Blockchain. 2021. Crystal Expert. https://crystalblockchain.com/crystal-expert/.
[6] Jack Cable. 2022. *Ransomwhere: A Crowdsourced Ransomware Payment Dataset.* https://doi.org/10.5281/zenodo.6512123
[7] Catalin Cimpanu. 2021. BTC-e founder sentenced to five years in prison for laundering ransomware funds. https://www.zdnet.com/article/btc-e-founder-sentenced-to-five-years-in-prison-for-laundering-ransomware-funds/
[8] Bleeping Computer. 2021. Dutch supermarkets run out of cheese after ransomware attack. https://www.bleepingcomputer.com/news/security/dutch-supermarkets-run-out-of-cheese-after-ransomware-attack/.
[9] U.S. Cybersecurity and Infrastructure Security Agency (CISA). 2021. Alert (AA21-209A): Top Routinely Exploited Vulnerabilities. https://www.cisa.gov/uscert/ncas/alerts/aa21-209a
[10] U.S. Cybersecurity and Infrastructure Security Agency (CISA). 2022. Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). https://www.cisa.gov/circia.

[11] Europol. 2021. darkmarket: world's largest illegal dark web marketplace taken down. https://www.europol.europa.eu/media-press/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down

[12] Europol. 2021. Ransomware: What you need to know. https://www.europol.europa.eu/publications-events/publications/ransomware-what-you-need-to-know.

[13] Canadian Centre for Cyber Security. 2021. Ransomware. https://cyber.gc.ca/en/ransomware.

[14] European Union Agency for Cybersecurity (ENISA). 2021. Threat Landscape report - 2021. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends.

[15] Andy Greenberg. 2018. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[16] The Guardian. 2017. WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017. https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

[17] Danny Yuxing Huang, Maxwell Matthaios Aliapoulios, Vector Guo Li, Luca Invernizzi, Elie Bursztein, Kylie McRoberts, Jonathan Levin, Kirill Levchenko, Alex C Snoeren, and Damon McCoy. 2018. Tracking ransomware end-to-end. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 618–631.

[18] The Wall Street Journal. 2021. JBS Paid $11 Million to Resolve Ransomware Attack. https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781.

[19] Eric Loui and Josh Reynolds. 2021. CARBON SPIDER Embraces Big Game Hunting, Part 2. https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-2/.

[20] Microsoft. 2021. How cyberattacks are changing according to new Microsoft Digital Defense Report. https://www.microsoft.com/security/blog/2021/10/11/how-cyberattacks-are-changing-according-to-new-microsoft-digital-defense-report/

[21] NPR. 2021. Panic Drives Gas Shortages After Colonial Pipeline Ransomware Attack. https://www.npr.org/2021/05/11/996044288/panic-drives-gas-shortages-after-colonial-pipeline-ransomware-attack.

[22] National Security Agency (NSA). 2022. 2021 Cybersecurity Year in Review. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/2921744/nsa-releases-2021-cybersecurity-year-in-review/.

[23] Australian Government Department of Home Affairs. 2021. Australia's Ransomware Action Plan. https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf.

[24] U.S. Department of Justice. 2020. United States Files A Civil Action To Forfeit Cryptocurrency Valued At Over One Billion U.S. Dollars. https://www.justice.gov/usao-ndca/pr/united-states-files-civil-action-forfeit-cryptocurrency-valued-over-one-billion-us.

[25] U.S. Department of Justice. 2021. Department of Justice Launches Global Action Against NetWalker Ransomware. https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware.

[26] U.S. Department of Justice. 2021. Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside. https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

[27] U.S. Department of Justice. 2021. individual arrested and charged with operating notorious darknet cryptocurrency mixer. https://www.justice.gov/opa/pr/individual-arrested-and-charged-operating-notorious-darknet-cryptocurrency-mixer

[28] U.S. Department of Justice. 2021. six charged with crimes related to virtual currency exchange business. https://www.justice.gov/usao-nh/pr/six-charged-crimes-related-virtual-currency-exchange-business

[29] U.S. Department of Treasury Financial Crimes Enforcement Network. 2021. Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021. https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf.

[30] Kris Oosthoek and Christian Doerr. 2020. Cyber Security Threats to Bitcoin Exchanges: Adversary Exploitation and Laundering Techniques. *IEEE Transactions on Network and Service Management* 18, 2 (2020), 1616–1628.

[31] Masarah Paquet-Clouston, Bernhard Haslhofer, and Benoit Dupont. 2018. Ransomware Payments in the Bitcoin Ecosystem. arXiv:1804.04080 [cs.CR]

[32] Robert Poulsen. 2021. U.S. Accuses Russian of Money Laundering for Ryuk Ransomware Gang. https://www.wsj.com/articles/u-s-accuses-russian-of-money-laundering-for-ryuk-ransomware-gang-11636741333

[33] Reuters. 2022. Crypto Giant Binance Kept Weak Money-Laundering Checks Even As It Promised Tougher Compliance, Documents Show. https://www.reuters.com/investigates/special-report/finance-crypto-currency-binance/

[34] Dark Web Solutions. 2022. Dark Web Monitor. https://dws.pm/.

[35] Cisco Talos. 2021. Translated: Talos' insights from the recently leaked Conti ransomware playbook. https://blog.talosintelligence.com/2021/09/Conti-leak-translation.html

[36] McAfee ATR Operational Intelligence Team. 2020. Take a "NetWalk" on the Wild Side. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/take-a-netwalk-on-the-wild-side/

[37] Financial Times. 2022. the rise of crypto laundries: how criminals cash out of bitcoin. https://www.ft.com/content/4169ea4b-d6d7-4a2e-bc91-480550c2f539.

[38] UK National Cyber Secuirty Centre. 2021. Mitigating malware and ransomware attacks. https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks.

[39] U.S. Federal Bureau of Investigation (FBI). 2021. Common Scams and Crimes: Ransomware. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware.

[40] Kai Wang, Jun Pang, Dingjie Chen, Yu Zhao, Dapeng Huang, Chen Chen, and Weili Han. 2021. A Large-scale Empirical Analysis of Ransomware Activities in Bitcoin. *ACM Transactions on the Web (TWEB)* 16, 2 (2021), 1–29.

[41] Official Bitcoin Wiki. 2021. Blockchain attacks on privacy. https://en.bitcoin.it/wiki/Privacy.