A Tale of Two Markets: Investigating the Ransomware Payments Economy

Oosthoek, Kris; Cable, Jack; Smaragdakis, Georgios

DOI
10.1145/3582489

Publication date
2023

Document Version
Final published version

Published in
Communications of the ACM

DOI:10.1145/3582489

A data-driven, follow-the-money approach to characterize the ransomware ecosystem uncovers two parallel ransomware criminal markets: commodity ransomware and Ransomware as a Service (RaaS).

BY KRIS OOSTHOEK, JACK CABLE, AND GEORGIOS SMARAGDAKIS

A Tale of Two Markets: Investigating the Ransomware Payments Economy

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,[18] empty supermarket shelves in the Netherlands,[2] the closing of 800 supermarkets in Sweden,[35] and gasoline shortages in the U.S.[33] In a recent report, the European Union Agency for Cybersecurity (ENISA) ranked ransomware as the "prime threat for 2020–2021."[36] 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."[1] Other governments, including the U.K.,[25] Australia,[28] Canada,[29] and law enforcement agencies, such as the FBI[31] and Europol,[32] have 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 predators and prey, 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 2021, the "vast majority" of reported ransomware payments were made in Bitcoin.[30] However, sig-

» key insights

- **This research effort collects and analyzes 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.**
- **Analysis of the evolving ransomware ecosystem shows that there are two parallel ransomware markets: commodity and RaaS.**
- **Analysis of more than 13,000 transfers shows striking differences in laundering time, use of exchanges, and other means to cash out ransom payments.**
- **Defending against professionally operated RaaS is challenging; the authors propose ways to trace back RaaS cryptocurrency activity.**

nificant 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 compiled a dataset of 7,321 Bitcoin addresses that received ransom payments, which we used to shed light on the structure and state of the ransomware ecosystem.

Our contributions are as follows:

- We collected and analyzed the largest public dataset of ransomware activity to date, including 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 two parallel ransomware markets exist: 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 13,000 transfers shows striking differences in laundering time, use of exchanges, and other means to cash out ransom payments.
- We discuss difficulties in defending against professionally operated RaaS and we propose ways to trace 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.[7]

IMAGE BY ANDRIJ BORYS ASSOCIATES. USING SHUTTERSTOCK

The Ransomware Ecosystem

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

Commodity ransomware. In the early years of ransomware, the majority of ransomware that spread can be characterized as commodity ransomware, distinguishable 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; they often copy and modify leaked or shared source code, causing the formation of ransomware *families*. Historically, most commodity ransomware campaigns used 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 more than 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 the proper backup and contingency plan was thought to defend against ransomware. The initial philosophy was that an ability to quickly 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 and widespread forms of ransomware.

Ransomware as a Service. While the first reports of RaaS emerged in 2016, it was not 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.

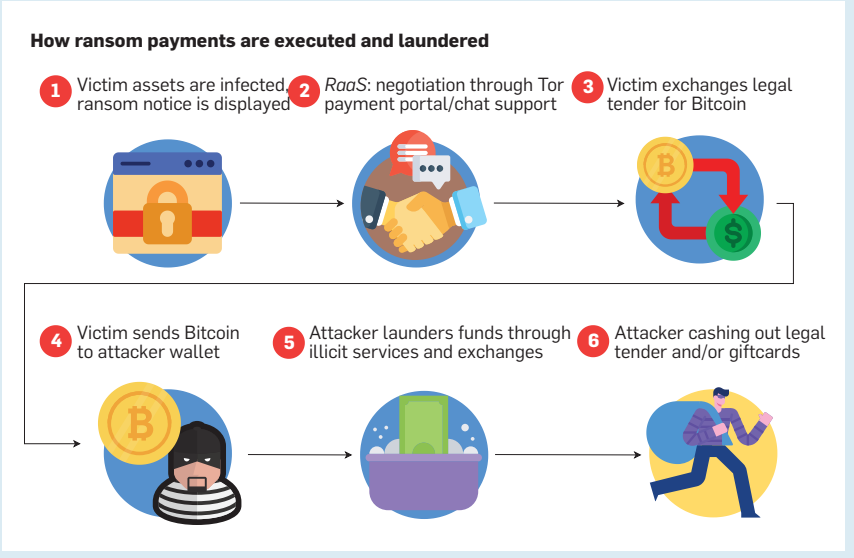
The rise of RaaS has enabled existing criminal groups to shift to a lucrative new business model where lower-skilled affiliates can access exploits and techniques previously reserved for more highly skilled criminals. This was exemplified by a leaked playbook from the RaaS group Conti, which enables novice actors to compromise enterprise networks.[22] RaaS affiliates can greatly differ 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.[17] 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.[23]

RaaS families often rely on spear phishing over the mass phishing mails used by commodity ransomware groups. They also exploit recently disclosed vulnerabilities, taking advantage of vulnerable remote and virtual desktop services.[37] 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 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 before seen. In this article, 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 unnecessary. With RaaS, attackers usually run chat-based services to interact with victims and negotiate the final ransom amount (step

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



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) to obfuscate ownership and reduce the risk of de-anonymization before cashing out (step 6).

Methodology

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

Addresses involved in ransom payments. We obtained 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.

To seed the dataset, we collected data from several public sources. We imported addresses from Paquet-Clouston et al.,[27] which 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.[3]

Members of the public may submit reports at Ransomwhere.[6] We received 99 reports containing 198 addresses over a six-month period between June and 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. To verify reports, the reporter must include the relevant Bitcoin addresses and the associated ransomware family. They also 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—for example, addresses involved in extortion scam emails.

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

Table 2. Composition of the dataset.

Source	Total USD	# BTC Addr.
Ransomwhere reports[6]	$87M	198
Paquet-Clouston et al.[32]	$10M	7,222
AlienVault OTX[1]	$4M	37
Total	*$101M*	*7,457*

All reported ransom addresses were Bitcoin addresses. Due to Bitcoin's transparent nature, 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[12] 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 two addresses belonging to a cache of Bitcoin seized by the U.S. Department of Justice after the closing of the Silk-Road dark Web market,[38] 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, see Table 1. Table 2 provides an overview of the sourcing of Bitcoin addresses in the dataset.

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,[9] we tracked the destination of outgoing transactions—that is, transfers. To estimate addresses' potential for illicit use, Crystal Blockchain uses clustering heuristics such as one-time change address and common-input-ownership,[5] which allow discovery of additional addresses controlled by an actor based on their use in a transaction. When filtering for potential false positives, heuristics and their outcomes are reliable.[21] On top of this, Crystal Blockchain manually collects off-chain data from various cryptocurrency services, in addition to scraping 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, we have only studied the direct destination of ransom payments (first hop). Based on the characterization of involved addresses across the path, we can study the laundering strategies of ransomware groups as well as the time needed to wash out the money.

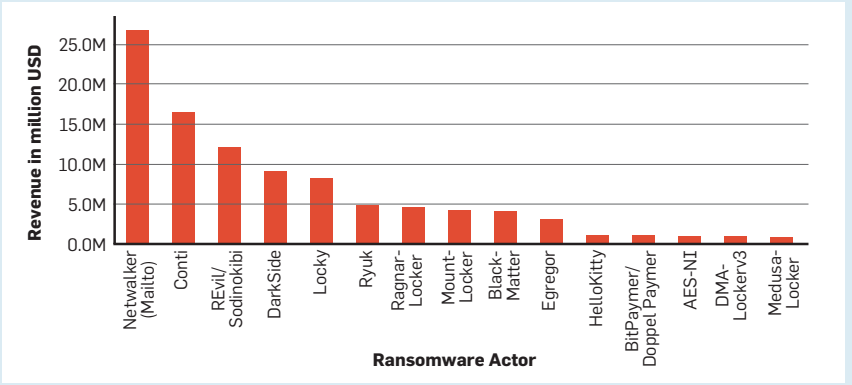
Ransomware actors. We obtained addresses and labeled families, and

Table 3. Ransomware families in the dataset.

Name	Address #	Name (cont'd.)	Address #
Locky	7,037	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 one address each. RaaS actors are highlighted.*

Figure 2. Revenue per ransomware actor.



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 no comprehensive public list of RaaS groups exists, 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.

Limitations. Our dataset of Bitcoin addresses is the largest public collection of ransomware payment addresses to date, based on total USD value. While this allows for a unique view of 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 them. 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 situation 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.[7]

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 one address are excluded from Table 3. The 10 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.[7]

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.

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 ac-

tive, 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.[13] 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 from individual victims. One example is an $11 million payment from Brazilian meat-processing company JBS to REvil/Sodinokibi on June 1, 2021.[6]

Locky had 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. One notable aspect about Locky, apart from its high revenue, is its address usage. The actors behind Locky issued new addresses to each victim, a novelty at the time.[19] This is evident in our analysis, with many addresses having only two or three incoming transactions. According to French court documents, Locky's developer is the same individual who owned BTC-e, a fraudulent exchange.[8] 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.

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 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 number of payments to a single address is 697 to AES-NI, followed by 496 to SynAck and 441 to File-Locker. While these 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. 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' investigation into NetWalker.[39]

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 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. Forty-six 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 functional-

Figure 3. USD revenue for commodity and RaaS.

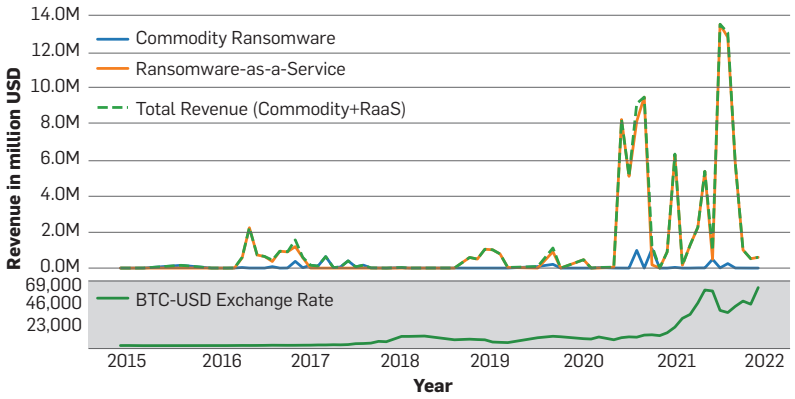
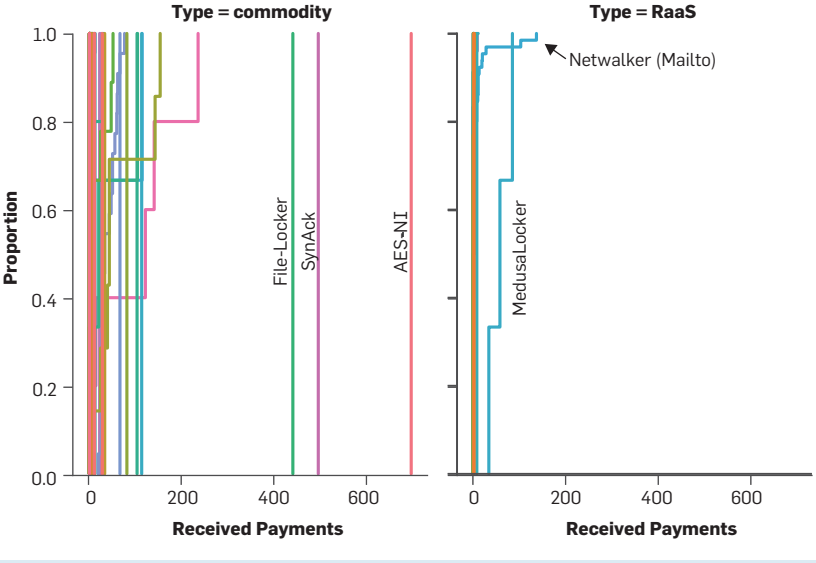


Figure 4. ECDF of payments per address for commodity ransomware and RaaS actors.



ity to increase security, such as timelocks 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 are not usually 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.

Money-Laundering Analysis

In the previous section, we investigated ransom payments by victims to ransomware actors. In this section, we investigate 13,097 laundering transactions in our dataset (see Table 1) to shed light on how these actors liquidate their illicit earnings. For this analysis, we use the methodology introduced in the previous "Ransom Payments and Laundering" section.

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 (FileLocker, SynAck, and AES-NI) also 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 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 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 sug-

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

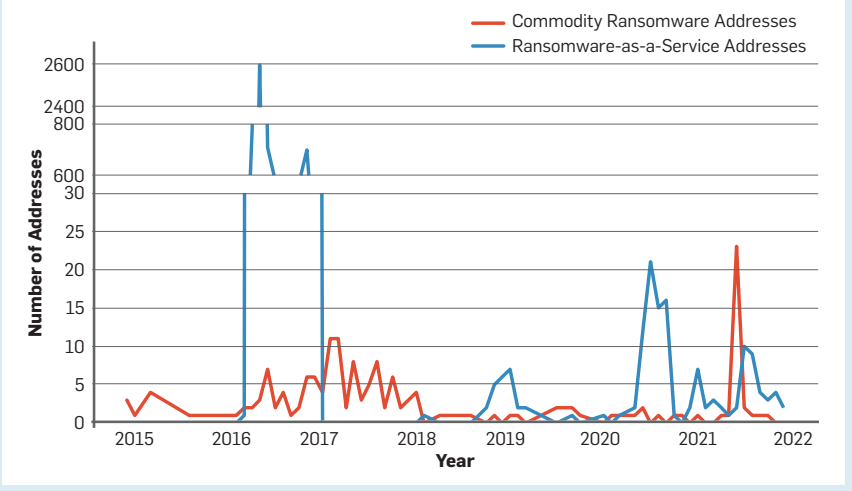
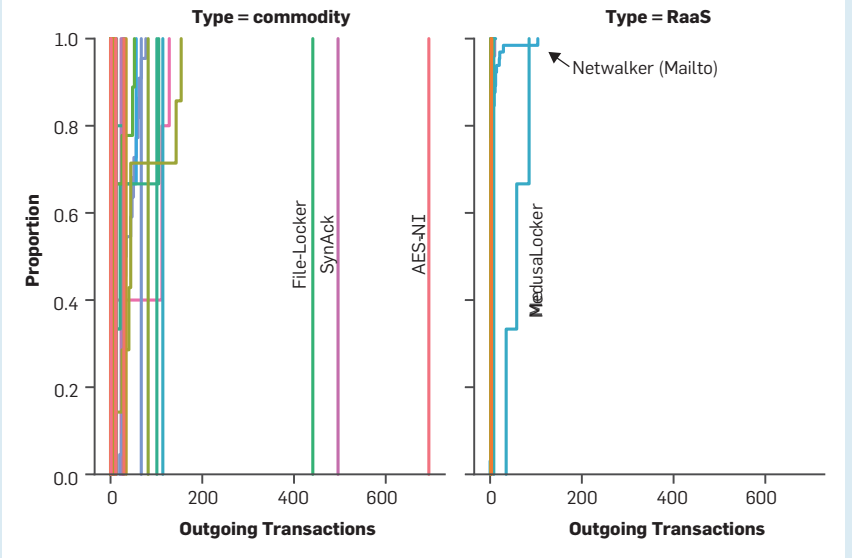


Figure 6. Transfer transactions per address for commodity and RaaS actors.



gests 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 unable 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,[13] with WannaCry under heavy monitoring and most of the laundering failed.[42]

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, such platforms are subject to Know Your Customer (KYC) regulations, which require 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. Law enforcement use blockchain-analysis tools in such anti-money laundering (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—that is, the first transfer transaction. This is the service to which actors transfer funds directly after receiving them from victims. 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 that they trust the service, at least enough not to disclose their identity.

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

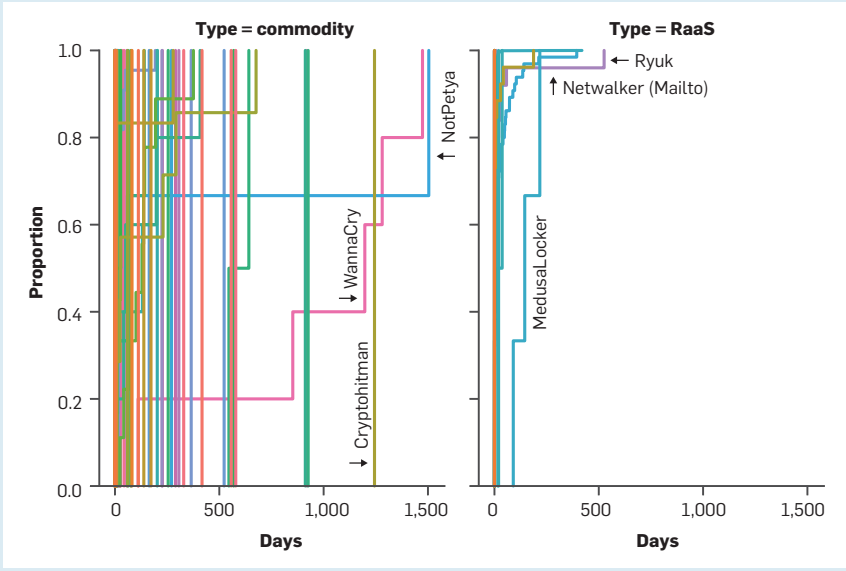


Table 4. Laundering entities overview.

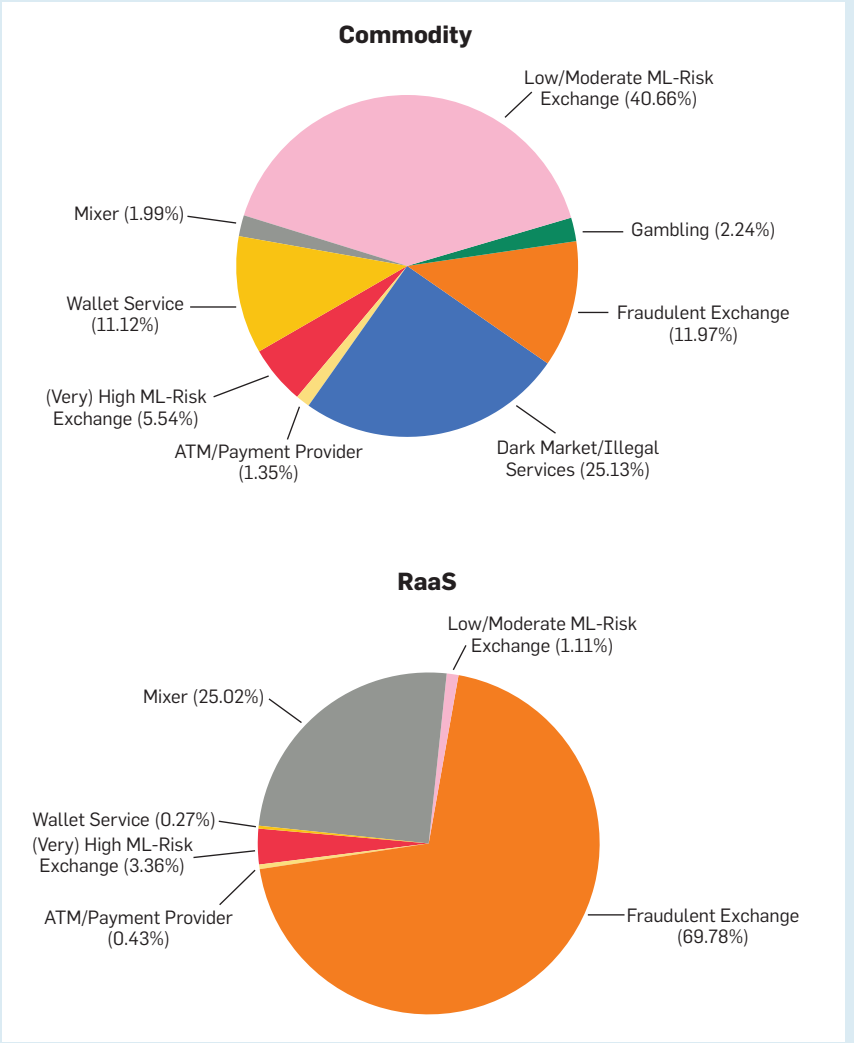
Entity	Description	Evidence
ATM/Payment Provider	Payment gateways for physical/online merchants or ATMs, usually used to launder small amounts.	See U.S. Dept. of Justice[29]
Dark Market/Illegal Services	Illegal services available on Tor or other Internet services, used to buy illegal server hosting and so on.	See Europol[11]
Fraudulent Exchange	Exchange platforms officially sanctioned by the U.S. Office of Foreign Assets Control (OFAC).	See Cimpanu[7]
Gambling	Online casinos and gambling platforms, used to launder small amounts anonymously.	See *Financial Times*[38]
Low/Moderate ML-Risk Exchange	Exchanges with strict AML/KYC policies might still be used for laundering criminal funds.	See *Reuters*[34]
Mixers	These services take and 'mix' Bitcoin from various parties to obfuscate ownership.	See U.S. Dept. of Justice[28]
(Very) High ML-Risk Exchange	Exchanges with lax or no AML/KYC implementations are popular for money laundering.	See Poulsen[33]
Wallet Service	Custodial/online wallets, some might also have privacy features such as mixers.	See *Financial Times*[38]

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.[41]

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 a service fee) back as a mix of other users' Bitcoin. Thus, it is harder 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

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



currency or other cryptocurrencies. It is, however, also known that cybercriminals have wound down the use of fraudulent exchanges.[26] 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, log-in 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 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 moment the payment is made.[14]

Discussion

Ransomware is a severe, growing threat plaguing our world, built on a cybercriminal business model which monetizes the insufficient security of many organizations. RaaS is the most potent form of ransomware yet, allowing cybercriminal actors to have a real-world impact on a scale not previously seen. In recent years, ransomware has increased in scale and frequency, and as seen in this article, attacker techniques are becoming increasingly sophisticated. Yet, as evidenced by recent law-enforcement actions, such as those against DarkSide and REvil, we are not without hope. RaaS actors are more resilient, but not immune, from law-enforcement action.

Nonetheless, failure to act now may make RaaS attackers even more successful. In particular, we highlight two areas crucial to preventing further success of ransom money laundering. First, we must rapidly develop infrastructure to report ransomware attacks and payments, which enables rapid tracing and seizure of ransomware payments. Second, privacy-preserving cryptocurrencies may allow ransomware actors to cover their tracks more effectively. New cryptocurrencies must be designed in a manner resilient to illicit activity while still ensuring privacy.

As evidenced by the Ransomwhere dataset, data on ransomware payments can be an indispensable tool to analyze ransomware threat actor activity. The sooner data can be shared, the greater chance law enforcement can recover ransom payments. As such, we encourage more reporting of ransomware attacks and associated payments. The Ransomwhere dataset likely represents a fraction of all ransomware attacks that occur, with most attacks going unreported. Various governments are considering mandatory reporting of ransomware attacks, with the U.S. having enacted legislation requiring critical infrastructure entities to report ransomware attacks and 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.

We note the increase of ransomware payment demands in privacy-preserving cryptocurrencies such as Monero.[30] Ransomware actors have indicated their preference for privacy-preserving cryptocurrency by accepting a lower payment in Monero than Bitcoin.[30] 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 developing cryptocurrencies to research mechanisms for preserving privacy while ensuring resilience against illicit activity to be traced; if not, ransomware actors may operate under greater impunity.

Conclusion

The research in this article represents 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 operating Ransomwhere, our open crowdsourced ransomware payment aggregator, to collect information from victims of ransomware attacks. Our analysis of 13,500 payments unveils that there are two symbiotic, parallel markets: commodity ransomware and (dominant since 2019) Ransomware as a Service (RaaS). The first is operated by individuals or a small group of programmers and the second by professional cybercriminals who offer 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 also generally more difficult to defend against, with Initial Access Brokers dedicating their time to obtaining access vectors. Their sophisticated pricing models consider factors such as access level, victims' annual revenue, and impact on critical infrastructure—incentivizing attackers to breach high-value targets.

Our analysis 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 levels 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 make it tougher for law-enforcement agencies to recover ransom payments.

By providing an extensive overview of ransomware payments and making our data available, we hope to provide insight into a cybercriminal economy that poses a severe threat to many organizations and societies, of which reporting is often fragmented.

Acknowledgments

The authors 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 Cybersecurity year in review. National Security Agency (2022); https://bit.ly/3NdXRj1.
2. Abrams, L. Dutch supermarkets run out of cheese after ransomware attack. *Bleeping Computer.* (2021); https://bit.ly/42nTrKS.
3. AT&T Alien Labs Open Threat Exchange. AT&T (2021); https://bit.ly/3qmsZ6V.
4. Berwick, A. and Wilson, T. Crypto giant Binance kept weak money-laundering checks even as it promised tougher compliance, documents show. *Reuters* (January 21, 2022); https://reut.rs/3OSHDgD.
5. Blockchain attacks on privacy. Bitcoin Wiki; https://en.bitcoin.it/wiki/Privacy.
6. Bunge, J. JBS paid $11 million to resolve ransomware attack. *The Wall Street Journal* (June 9, 2021); https://on.wsj.com/3qp5DOa.
7. Cable, J. Ransomwhere: A crowdsourced ransomware payment dataset (2022); https://bit.ly/3OSX9Jd.
8. Cimpanu, C. BTC-e founder sentenced to five years in prison for laundering ransomware funds. *ZDNet* (2021); https://zd.net/43FwSCq.
9. Crystal Expert. Crystal Blockchain (2021); https://bit.ly/42nyjEG.
10. Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). U.S. Cybersecurity and Infrastructure Security Agency (CISA), (2022); https://bit.ly/42nA1pA.
11. Darkmarket: World's largest illegal dark web marketplace taken down. Europol (2021); https://bit.ly/3qxoQx1.
12. Dark Web Monitor. CFLW Cyber Strategies; https://dws.pm/.
13. Department of Justice launches global action against NetWalker Ransomware. U.S. Department of Justice (2021); https://bit.ly/3oWJRAO.
14. Department of Justice seizes $2.3 million in cryptocurrency paid to the ransomware extortionists Darkside. U.S. Department of Justice (2021); https://bit.ly/3IZ1s29.
15. Greenberg, A. The untold story of NotPetya, the most devastating cyberattack in history. *Wired* (August 22, 2018); https://bit.ly/3NdwKEM.
16. Hern, A. WannaCry, Petya, NotPetya: How ransomware hit the big time in 2017. *The Guardian* (December 30, 2017); https://bit.ly/45L4bG1.
17. Hogan-Burney, A. How cyberattacks are changing according to new Microsoft Digital Defense Report. Microsoft (October 24, 2021); https://bit.ly/3Cb5vEL.
18. HSE cyber-attack: Irish health service still recovering months after hack. BBC (2021); https://bbc.in/3CcQwtL.
19. Huang, D.Y. et al. Tracking ransomware end-to-end. In *2018 IEEE Symposium on Security and Privacy*, IEEE, 618–631.
20. Individual arrested and charged with operating notorious darknet cryptocurrency mixer. U.S. Department of Justice (2021); https://bit.ly/43qsCa3.
21. Kalodner, H. et al. BlockSci: Design and applications of a blockchain analysis platform. In *USENIX Security Symposium* (2020).
22. Largent, W. Translated: Talos' insights from the recently leaked Conti ransomware playbook. Cisco Talos (2021); https://bit.ly/43HWIpr.
23. Loui, E. and Reynolds, J. CARBON SPIDER embraces big game hunting, Part 2. *Crowdstrike* (November 4, 2021); https://bit.ly/3NcWO2V.
24. McMillan R. and Poulsen, R. U.S. accuses Russian of money laundering for Ryuk Ransomware Gang. *The Wall Street Journal* (November 12, 2021); https://on.wsj.com/43renSw.
25. Mitigating malware and ransomware attacks. UK National Cyber Security Centre (2021); https://bit.ly/45GSiRz.
26. Oosthoek, K. and Doerr, C. Cyber security threats to Bitcoin exchanges: Adversary exploitation and laundering techniques. *IEEE Transactions on Network and Service Management 18*, 2 (2020), 1616–1628.
27. Paquet-Clouston, M., Haslhofer, B., and Dupont, B. Ransomware payments in the Bitcoin ecosystem. *J. of Cybersecurity 5*, 1 (2019).
28. Ransomware Action Plan. Australian Department of Home Affairs (2021); https://bit.ly/3qoQ1dv.
29. Ransomware. Canadian Centre for Cyber Security (2021); https://bit.ly/45PqCd0.
30. Ransomware trends in Bank Secrecy Act data between January 2021 and June 2021. U.S. Department of Treasury Financial Crimes Enforcement Network (2021); https://bit.ly/43FJTvM.
31. Ransomware. U.S. Federal Bureau of Investigation (2021); https://bit.ly/3CdYWRO.
32. Ransomware: What you need to know. Europol (2021); https://bit.ly/3OWxpM1.
33. Romo, V. Panic drives gas shortages after Colonial Pipeline ransomware attack. *NPR.* (May 11, 2021); https://n.pr/3qqYMUo.
34. Six charged with crimes related to virtual currency exchange business. U.S. Department of Justice (2021); https://bit.ly/3oLzEHB.
35. Swedish Coop supermarkets shut due to US ransomware cyber-attack. BBC (2021); https://bbc.in/3Cam4R0.
36. Threat Landscape Report 2021. European Union Agency for Cybersecurity (ENISA); https://bit.ly/3qrcoPz.
37. Top routinely exploited vulnerabilities. U.S. Cybersecurity and Infrastructure Security Agency (CISA), Alert (AA21-209A). (2021); https://bit.ly/43tllX9.
38. United States files a civil action to forfeit cryptocurrency valued at over one billion U.S. dollars. U.S. Department of Justice (2020); https://bit.ly/3MOiNMh.
39. Seret, T. et al. Take a "NetWalk" on the wild side. McAfee ATR Operational Intelligence Team (August 3, 2020); https://bit.ly/3MRAIS7.
40. The rise of crypto laundries: How criminals cash out of bitcoin. *Financial Times* (2022); https://on.ft.com/45OpsOZ.
41. Wang, K. et al. A large-scale empirical analysis of ransomware activities in Bitcoin. *ACM Transactions on the Web (TWEB) 16*, 2 (2021), 1–29.
42. Wannacry money laundering attempt thwarted. *BBC* (2017); https://bbc.in/42mMN7K.

Kris Oosthoek is a security researcher and holds a Ph.D. in Computer Science from Delft University of Technology (TU Delft), The Netherlands.

Jack Cable is a security researcher and holds a B.S. in Computer Science from Stanford University, USA.

Georgios Smaragdakis is professor of Cybersecurity at Delft University of Technology (TU Delft), The Netherlands.

Watch the authors discuss this work in the exclusive *Communications* video. https://cacm.acm.org/videos/investigating-ransomware-payments