Computers & Security 92 (2020) 101762

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

# The Ransomware-as-a-Service economy within the darknet

Per Håkon Meland[a,b,*], Yara Fareed Fahmy Bayoumy[a], Guttorm Sindre[a]

[a] *Department of Computer Science, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway*
[b] *Department of Software Engineering, Safety and Security, SINTEF Digital, NO-7034 Trondheim, Norway*

ARTICLE INFO

*Article history:*
Received 28 November 2019
Revised 30 January 2020
Accepted 18 February 2020
Available online 29 February 2020

*Keywords:*
Ransomware
RaaS
Malware
Darknet
Marketplace
Netnography

ABSTRACT

Ransomware is an epidemic that adversely affects the lives of both individuals and large companies, where criminals demand payments to release infected digital assets. In the wake of the ransomware success, Ransomware-as-a-Service (RaaS) has become a franchise offered through darknet marketplaces, allowing aspiring cybercriminals to take part in this dubious economy. We have studied contemporary darknet markets and forums over a period of two years using a netnographic research approach. Our findings show that RaaS currently seems like a modest threat relative to popular opinion. Compared to other types of illegal digital goods, there are rather few RaaS items offered for sale in darknet marketplaces, often with questionable authenticity. From our data we have created a value chain and descriptions of the actors involved in this economy.

## 1. Introduction

The darknet is an unregulated *Wild West* of the Internet, cyber crime's safe haven for communication and exchange of illegal goods and services. It is easily accessible, and with the help of anonymisation technology and modern-day digital currencies, a full-fledged economy takes place on a global scale right under the nose of impaired law enforcement agencies. An estimated USD 1 billion has been spent here during the first nine months of 2019 (Europol, 2019).

We have been especially interested in ransomware, which enables extortion of victims by taking control of their digital assets. On the darknet markets, *Ransomware-as-a-Service* (RaaS) is being offered as a franchise model that allows people without programming skills to become active attackers and take part in the ransomware economy. This is a way of democratising crime, giving ordinary people and smaller players an easier way into the criminal market (Jaishankar, 2008; Naylor, 2000), while reducing the risk of exposure for the ones on top of the value chain. For instance, a dissatisfied employee might decide to partner up with a RaaS developer to effectively infect an organisation from the inside and then splitting the profit.

### 1.1. Objective

In order to devise effective countermeasures against RaaS, it is helpful to understand the intricate relationships of people operating within the opaque darknet markets (Thomas et al., 2015). Currently, the relationships between organised crime and the Internet is under-investigated (Lavorgna, 2015). This research gap can be narrowed down by looking at the motivations and incentives of the people involved, and Waldrop (2016) suggests that this can be accomplished by embracing behavioural science and economics as part of the research. The research objective of our work has been to obtain a better understanding of the darknet market for RaaS as we have tried to address the following research questions:

1. How severe is the RaaS threat?
2. What are the value chains related to this market?

The answers to these questions are of significance when estimating the current impact of RaaS and the participating actors, and to guide further research both for academic and commercial purposes.

### 1.2. Scope

We have studied RaaS within popular contemporary darknet markets and forums over a period of two years (fall of 2017 to fall of 2019) using a netnographic research approach. Our observations have been complemented with historical data found in archives and published interviews with stakeholders involved in darknet operations. Our study has been limited to English-speaking spaces

* Corresponding author at: Department of Software Engineering, Safety and Security, SINTEF Digital, Strindvegen 4, NO-7034 Trondheim, Norway.
*E-mail address:* per.h.meland@sintef.no (P.H. Meland).

https://doi.org/10.1016/j.cose.2020.101762

not residing behind walls requiring pay-for-access or other unethical contributions.

### 1.3. Outline

In Section 2 we present background information about the environment in which we have conducted the study. Section 3 gives an overview of related research that we have built our knowledge on. Section 4 details our methodological approach and data sources, including the ethical issues we had to consider. Section 5 summarises our most important results, which are discussed in the following Section 6. Finally, Section 7 concludes the paper.

## 2. Background information

### 2.1. The darknet and dark web

The term *darknet* is commonly associated with hidden networks on the Internet, and most prominently, *The Onion Router* (TOR), originally developed by the US Naval Research Laboratory to protect communication with agents stationed abroad but later made open to anyone who wants to anonymously interact with others. Another darknet example is the *Invisible Internet Project* (I2P), but it currently has fewer users and is thus considered less anonymous than TOR.

The collection of websites that reside on the secret space of the darknet is commonly referred to as the *dark web*. The dark web can also be thought of as a subset of the *deep web* (aka *invisible* or *hidden web*). What distinguishes any website in the deep web from what we refer to as the *surface web, lightnet,* or *clearnet*, is that it is not indexed, and therefore, cannot be found by the everyday search engines most people use. Though most of the deep web content is perfectly legitimate, the story is quite different when it comes to dark web. A study by Moore and Rid (2016) gave a conservative estimate that 57% of the TOR websites facilitated criminal activities related to drugs, arms, murder and child pornography.

### 2.2. Marketplaces and forums

Both within the surface web and darknets there are websites similar in structure to online shopping sites that facilitate the illegal transactions. These websites go by the name of *darknet markets/marketplaces, underground markets* or *cryptomarkets*. For the sake of simplicity, the rest of this paper will refer to them as darknet markets.

The pioneering Adamflowers/Farmer's Market started out as a surface web market in 2006 but transitioned to TOR in 2010. It had been selling illegal drugs to more than 34 countries before it was eventually shut down by law enforcement agencies in 2012 (Vaas, 2012). Learning from the mistakes of the Farmer's Market, Silk Road became the first darknet market that used cryptocurrency for payment in 2011. The business model of Silk Road was very successful, and its administrators were making a living off vendor fees and commissions. It was shut down by the FBI in 2013, but a multifold of markets emerged in its wake using similar models.

Sometimes darknet marketplaces are shut down for other reasons than law enforcement. Money stored in escrow has on several occasions been stolen from or by the administrators, so-called *exit scams.* The Sheep Marketplace is a well-known example, where one of the vendors exploited a site vulnerability and took off with 54 000 bitcoins in 2013, while the administrator shut down the site and stole 40 000 bitcoins for himself in 2015 (DIVIDEDBY0, 2017).

Most darknet markets are accompanied with a discussion forum. Such forums help the users tackle uncertainties related to the quality of the offered goods and services (Yip et al., 2013). For instance, vendor review is a common discussion topic. This helps identify potential *scammers*, i.e., vendors that actively manipulate their own product reviews.

### 2.3. Ransomware and Ransomware-as-a-Service

Gallo and Liska (2016) define *ransomware* as *"a blanket term used to describe a class of malware that is used to digitally extort victims into payment of a specific fee"*. Typically, malicious code makes specific files or a whole system unavailable to the victim through encryption or change of usage rights. After a limited time, the ransom fee must be payed, or the damage becomes permanent. In most cases (65%) (Hernandez-Castro et al., 2017), the system is recovered after the ransom has been payed.

The first ransomware, known as AIDS, was observed in the wild already in 1989, spreading through the exchange of floppy disks (O'Kane et al., 2018). In the years to follow, ransomware was not a serious threat. Studies by O'Gorman and McDonald (2012) and Kharraz et al. (2015) have shown that the number of ransomware families was quite low for more than two decades, especially the ones with sophisticated destructive capabilities. However, this all changed with the introduction of stronger encryption schemes in the ransomware code and especially the availability of cryptocurrency as a payment method difficult to track by law enforcement (Young and Yung, 2017). Ransomware has been recognized as one of the fastest growing cybercrimes in recent history (Grobman and Cerra, 2016), and even though the overall number of infections started to decline in 2018, the current trend is that businesses are becoming the primary targets, whereas regular citizens are to a lesser extent being hit (Symantec, 2019).

In the wake of the ransomware success, *ransomware-as-a-service* (RaaS) has become an entry point for criminals with little programming skills to participate and earn money from ransomware (O'Kane et al., 2018). Contacting ransomware service providers using darknet markets, the criminals can cheaply obtain tailor-made ransomware ready to be used on their prospective victims. In addition to the creation fee, the service providers may take a 20–30% cut of the ransom as well. RaaS can have different formats, such as source code that the buyer compiles himself, pre-compiled binaries or an interface where the buyer inputs information about the victims. This collaborative strategy is a way of achieving a faster rate of infections with a lower risk of getting caught.

## 3. Related research

### 3.1. Marketplace and forum research

The vast body of research on darknet markets is related to illegal drugs, while there is limited literature focusing solely on ransomware markets. However, if we glance towards the broader category of digital goods and services, we find many studies that are of relevance to ransomware. Ablon et al. (2014) published a book describing structures, types of participants, products of open and closed black markets. Though their focus was mostly on botnets and zero-day vulnerabilities, they also show the price development for exploit kits and the evolution of markets over time. The year after, Thomas et al. (2015) surveyed existing research in order to systematize the community's understanding of the underground economy and develop a taxonomy of profit and support centres for reasoning about the flow of capital. Broadhurst et al. (2018) wrote a research review of malware trends on darknet markets. In their own six-month study (Sep 17 - Feb 18), they were able to observe increasing interaction between cybercriminals and state or quasi-state cybersecurity actors. Their analysis of the Dream market product listing in this period showed that ransomware only constituted 0.73% of the offered goods, while compromised accounts and credit cards represented 72% of the listed products.

Van Wegberg et al. (2018) carried out a six-year longitudinal study tracking the evolution of commoditization on eight marketplaces, spanning from Silk Road to Alphabay. Within the malware category, the ransomware clusters around the Stampado and Philadelphia stood out as the most prominent. However, they also claim that there has been limited growth due to bottlenecks in outsourcing critical parts of the criminal value chain. This can be seen in relation to the exploratory darknet study by Cusack and Ward (2018). Based on observations from the business processes and technologies associated with ransomware, their opinion is that over time, erosion of trust will render the ransomware crime model economically infeasible.

### 3.2. Stakeholders, roles and value chains

The stakeholders involved in the underground economy have different responsibilities and expose themselves to different types of risks. Several research papers have modelled value chains that illustrate the roles involved and the direction of communication and responsibility. Zhuge et al. (2009) have modelled the underground economy in China, with an emphasis on online games. They defined several roles, including *virus writers, website masters/crackers, envelope* (account) *stealers, virtual asset stealers* and *sellers and players* (buyers). Yip (2010) compared the Chinese cybercrime underground with the West and added other types of roles for faux website design. In another stakeholder classification, Cárdenas et al. (2009) identified the *malware distributors* role. O'Kane et al. (2018) have described *mixers* and *tumblers* involved in the money laundering services. A report by the security company Carbon Black (2017) defined three core economic tiers for the ransomware supply chain; *author, RaaS* and *distributor*.

Yip et al. (2013) examined the structure of organised cybercrime and sources of uncertainty given the masked identities of the traders and presence of undercover agents. Rossy and Décary-Hétu (2017) further examined trust issues as vendors often face the threat of identity theft by people who want to take advantage of their established reputation. Holt et al. (2012) identified network structures for information sharing amongst *malware writers* and other members of the community. della Torre (2018) analysed the strategic dynamics of vendors in the darknet markets, discovering that the fittest and richest vendors focus on a limited subset of products (3–5) with little updates. Kwon and Shakarian (2018) studied information sharing between actors during takedowns, finding examples of both collaboration for alterative economic routes and distrustful communication during such events.

For a thorough overview of the contemporary cybercrime ecosystem and its developments, we refer to Broadhead (2018).

### 3.3. Economics of ransomware

There have been many papers that analyse the economics of ransomware as seen from the offender's and victim's point of view. Economic incentives from developing and distributing ransomware are high, simply because the revenue is high, whereas the costs of resources and probability of apprehension are low. Hernandez-Castro et al. (2017) put forth an economic model based on the victim's willingness to pay. Here, the amount for a single ransomware variant can either be a fixed price for all victims, or fluctuating based on a set of factors (*price discrimination*). Laszka et al. (2017) proposed a game-theoretic model of the ransomware ecosystem, including backup and recovery investments, and incentives to pay the ransom. Lee and Lee (2017) observed that the cost of acquiring ransomware was determined by complexity of the vulnerability the malware is exploiting. Aurangzeb et al. (2017) have done a literature survey on ransomware families including their payment methods.

Another category of studies has tried to *follow the money*, analysing the cryptocurrency transaction logs associated with ransomware. For instance, Huang et al. (2018) do this from the time victims acquire bitcoins to pay the ransom and through to the time ransomware operators cash them out. Paquet-Clouston et al. (2019) have a similar approach. They found that this market is highly skewed with a low number of players and that the total amount of ransom is relatively low compared to the hype surrounding the issue. The analysis by Anderson et al. (2018) of ransom payments on the blockchain indicated that substantial ransom sums may have been mixed in and obfuscated with drug transactions. Conti et al. (2018) have conducted a longitudinal study on twenty ransomwares and how they have impacted the economy of bitcoin payments.

Within academic publications, there has been less research focusing on the economy of ransomware-as-a-service. However, a few security companies have published reports on this franchise model. For instance, Check Point and IntSight (2016) disclose the business operation of the Cerber RaaS from end-to-end, and Carbon Black (2017) describe how novice criminals are included to minimize the risk of the ransomware authors.

## 4. Methodological approach

*Netnography* is a research approach centred on the study of *online traces*, which are various types of data people make available online to anonymous or networked others (Kozinets, 2019). In this sense, they also represent social information on which research can be done. We answer to Kozinets' four defining elements by having a *cultural focus* on ransomware trade, *social media data* that primarily stem from darknet marketplaces and forums, an *immersive engagement* through actively learning and reflecting on the focal phenomenon by members of the research team, and finally a *praxis* that follows particular netnographic research procedures.

As an initial *movement*, we decided upon the ethical concerns related to this research. Online traces such as archived data are publicly available and should technically be regarded as published open content. However, the personal identities of the people involved are secret, and they operate behind pseudonyms. Connecting data and giving them unwanted exposure could lead to retributive actions, e.g., towards the researchers or affiliated organisations. To reduce such risks, we decided to avoid direct interaction with subjects creating or selling ransomware. This is stressed by Martin and Christin (2016) for two main reasons. Firstly, the research after publication will not be pertinent to any proof for prosecution against any individual. Secondly, there will be no need to ask for permissions or consent. The pseudonyms we recorded in our field notes are either altered or not included in this paper, hence no data linked to the user's identity or personal background are exposed. To avoid supporting illegal activities, we have not purchased anything. Finally, we have not tried to deceive, intimidate or confuse people within this research space.

Our study spanned over two years with four phases of data collection further described below.

### 4.1. Phase 1: pre-study

This initial phase was a pre-study of contemporary darknet markets and forums performed during the fall of 2017. Following the recommendations of Kozinets et al. (2014) we found it best to start the investigation with a small number of sites to gain a cultural sense of "what is going on" in that particular social space. Our sample was selected using DNStats (2019), which at that time offered links to the most popular darknet websites along with uptime and availability. We chose the *Dream* and *Wallstreet* markets, being the two most prominent markets dealing with ransomware, and the discussion forum *Intel Exchange*, which was the only open market that allowed members to promote ransomware services (aka *vending*). By searching for "ransom" and manual inspection we collected RaaS item price listings and descriptions in our field notes, as well as vendor profiles and ratings/reviews/comments from buyers. Within forums we also used the search keyword "ransom" and recorded relevant discussions, e.g., related to the process of buying and partner search for development or distribution.

### 4.2. Phase 2: expansion

We expanded our research sample in the spring of 2018, covering additional contemporary sites, historical data and published interviews with stakeholders. These were selected using *DNStats*, (2019), *Reddit* (2019), *DeepDotWeb* (2017) and *Darknet Markets* (DNetX, 2019). Prior to 22nd of March 2018, Reddit offered several subreddits with posts concerning darknet markets and activity, but these were all banned to shut out illegal activities. DeepDotWeb provided news and an overview of the top darknet markets and forums based on ratings and uptime status. Darknet Markets provided news and a directory listing of active and dead sites.

In addition to the previous marketplaces from phase 1, we chose to include the *Berlusconi* market, which was growing quickly at that time. We identified historical archives by Branwen et al. (2015), containing scraped data of 89 different marketplaces and 37 forums between 2013–2015, McKenna and Goode's archive (2017) of *Alphabay* between 2016–2017, and Lewis' (2017) item listings and buyer feedback from the *Hansa* and *Valhalla* markets from October and December 2016. Additional forums were the top ranked *OnionLand, HUB,* and *HiddenAnswers*. Both Onionland and HUB were taken down in the beginning of 2018.

We gained insight into the thoughts and opinions of darknet community stakeholders by studying interviews published on DeepDotWeb, covering marketplace administrators (*TheRealDeal, Alphabay* and *German Plaza*), a marketplace platform developer, a forum moderator, a forum vendor, a money launderer, and a ransomware developer.

### 4.3. Phase 3: iteration

During the Winter of 2018/2019 we revisited the contemporary marketplaces and forums to capture the latest trends and developments with respect to RaaS. We included the *Tochka* (aka *Point*) market due to its then high ranking at Darknet Markets and DeepDotWeb, the *Empire* market, which had emerged in February 2018 to become one of the fastest growing markets, and the *Dread* forum, which had become a popular discussion site on the darknet after the subreddit crackdowns. For our stakeholder analysis, we included additional published interviews with the administrators of *Valhalla, Outlaw, Minerva, Oasis* and *Tochka* found on DeepDotWeb, as well as one with the *Empire* market administrator found in a *Dark Web News* article by C.M. (2018).

### 4.4. Phase 4: a new line-up

By Fall 2019, several of our previous data sources were debunked or shut down (*Dream, WallStreet, IntelExchange*). As *DeepDotWeb* had also been seized by law enforcement, the identification of marketplaces relied on *DarknetLive* (2019), which we found to have the most up-to-date index of marketplace links, supplemented by *TheDarkWebLInks* (2019) and *DNStats*. From the living marketplaces we found RaaS in the following sample: *Apollon, Berlusconi, Darkbay, Empire, Grey* and *Samsara* (successor of Dream). Berlusconi went offline around September 22nd, right after we had completed our observations, possibly due to an exit scam or takedown. We excluded *Tochka* since there were no RaaS items there anymore.

## 5. Results

We have integrated the collected data from each phase and made an incarnation showing phenomena related to vendor resilience despite of marketplace takedowns, that there is a strong decline in the availability of RaaS items, that there is a high risk of buying fraudulent items, what kind of buyers/distributors the vendors are targeting, and finally, a larger picture of the RaaS economy and its actors.

### 5.1. Vendor resilience

Our first study phase started right after the takedown of the dominant darknet markets Alphabay and Hansa as a part of Operation Bayonet (Europol, 2017). This led to a rapid growth of the Dream userbase also observed by Van Wegberg et al. (2017), both when it came to vendors and buyers. We believe that one of the reasons that Dream succeeded in taking this business was its relatively high uptime and performance compared to its competitors at the time. Another reason could be related to a rapid establishment of trust between the actors. We observed that Dream had a specific feature that allowed vendors to present their previous rating from Alphabay and Hansa on their profile page. This let them maintain their existing reputation and buyers could base their trust on trade ratings from dead markets. This phenomenon reappeared in phase 4 after the death of Dream, as Empire allowed vendors to display their sales stats from Dream. This is an example of resilience in a volatile environment where people are anonymous, and trust is a great market advantage.

### 5.2. Market size perspectives

The most popular goods sold on open darknet markets are drugs. Where available, RaaS items are usually found under the *Digital Goods* or *Services* categories, but RaaS is rare in these inventories. The most popular digital goods or service is *carding* or *credit card fraud*. Fig. 1 shows an overview of items offered on *Dream*, the largest market in phase 2 and 3 of our study, comparing ransomware to *digital goods* and to *carding.*

Though the number of total items had increased about 38% between 2018 and 2019, the number of RaaS items declined 22%. In phase 3, RaaS items constituted about 0.15% of the total items available at *Dream*. We could not extend this trend analysis to phase 4 as *Dream* died before that, however the successor *Samsara* contained merely 3 RaaS items. In fact, the total number of ransomware items across the six remaining markets were now only 69. 65 of these items were sold from the markets *Apollon, Berlusconi, Empire* and *Grey*, which were the only ones that also stated the number of successful sales per item. Only 28 items had any sales at all, and the total number of successful sales from these were 359, constituting a total sales profit of approximately USD 2 202 based on the listed price per item.

### 5.3. No honour among thieves

The authenticity of RaaS items sold on the darknet markets was questioned throughout our research and we found several indications of scam. Firstly, most of the renowned RaaS vendors had gained their high rating from credit card gift cards or drug related sales in the past, and not because of RaaS. Secondly, the descriptive RaaS information tended to be copied from other RaaS items.

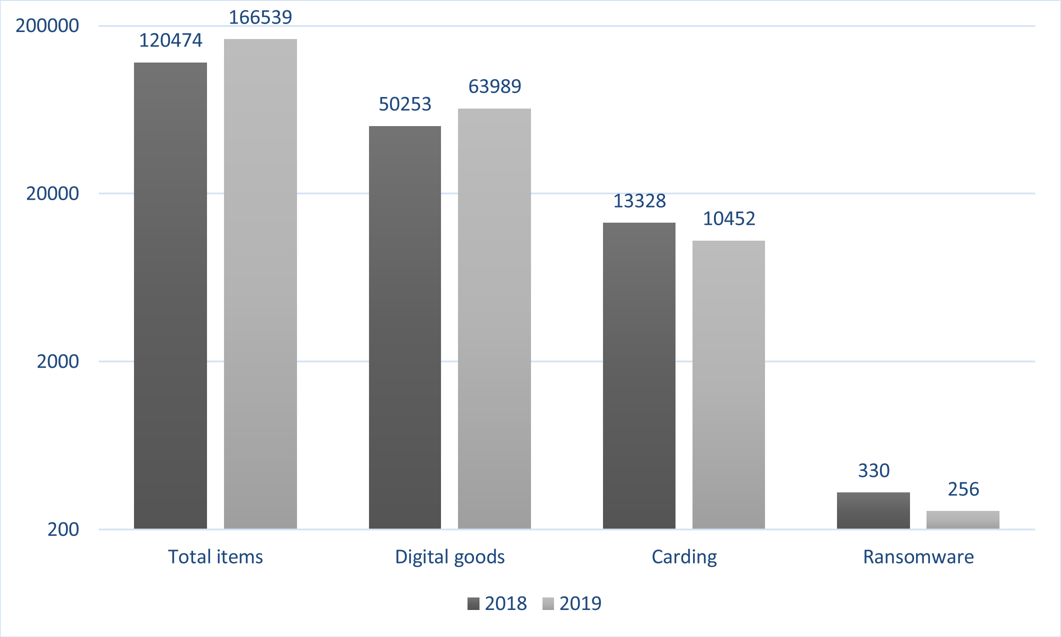

**Fig. 1.** Inventory excerpt from the Dream market shown with a logarithmic Y-axis scale.

Thirdly, a lot of the data in the feedback fields, which include obscured aliases and star ratings, seemed to be artificially created since they were identical and registered at the same time. Buyers using the free text fields tended to give negative feedback. Such observations lead us to believe that most of the RaaS items sold on the darknet markets are frauds, where the buyers either get rubbish or ransomware that redirects the whole payment somewhere else than the buyer's wallet. For instance, one of the most trusted RaaS vendors we found on *WallStreet* received this feedback comment:

> "…these files are all open source files found for free at github, and are old"

The fraud assumption was further supported by a question posted on the OnionLand forum, where a user questioned the validity of services offered by software dealers on the marketplaces:

> "Is there anyone or any vendor/market out there that isn't a scam)? I mean, seriously!!! I'm beginning to think this whole Darknet is just an urban legend!!"

The moderator of the forum responded as follows:

> "The public space is supposed to be filled with scams and stupid products, because you don't have to prove your worth to get into the public sphere. The only way to experience the inner workings is to be able to convince others that you should be allowed into invite-only spheres as mentioned."

Gaining access to such walled spaces can be a challenge if you do not already know someone on the inside. For instance, one of the most popular walled forums, named Hell, requested a payment of 0.01 Bitcoin or a trusted referral in order to get access. Additionally, users would need to prove their worth for the community. Upon an inspection of the Hell bitcoin wallet we could not see a substantial amount of transactions, which either means that there few members or they are invited by acquaintances.

### *5.4. RaaS target market*

In order to gain an understanding about the type of customers the vendors were targeting, we looked more closely at our gathered RaaS item descriptions. A common piece of information is the recommended level of technical expertise a buyer should have. During phase 1, we analysed the 20 items that provided such descriptions and found out that most of them (65%) targeted experts, while novice users should be able to use the other portion (35%). Moreover, popular items tended to include links to detailed guides and tutorial videos with step-by-step instructions on how to distribute and activate the ransomware, claim the ransom (or even give mercy to the victim).

We also analysed the anonymous social interactions that took place on the forums. During phase 2, we categorized the frequency of the RaaS topics that we found on HiddenAnswers, which was the oldest forum and had the highest number of posts concerning RaaS compared to OnionLand and HUB. Based on 79 posts in English, we created 8 different groups of Q&A as shown in Fig. 2.

The majority of these posts were about ransomware acquisition or development, indicating that this forum was dominated by non-experts. This was to be expected since experienced developers would rather stick to walled forums or IRC-channels.

### *5.5. Value chain*

Based on marketplace observations, forums posts, available interviews and literature we have created a simplified map of the value chain related to RaaS as depicted with blue arrows in Fig. 3. RaaS items follow the red arrows until they become ransomware infections at victims. The green arrow indicates a close coupling between marketplaces and forums. The stakeholders are briefly described in Table 1, where we have also tried to classify them according to the risk categories *high, medium, low* based on how likely it is that they will be exposed and possible consequences. Note that there are law enforcement agencies, security companies, researchers and neutral darknet bystanders entangled in this anonymised online community as well, but they are not directly involved in the economy.

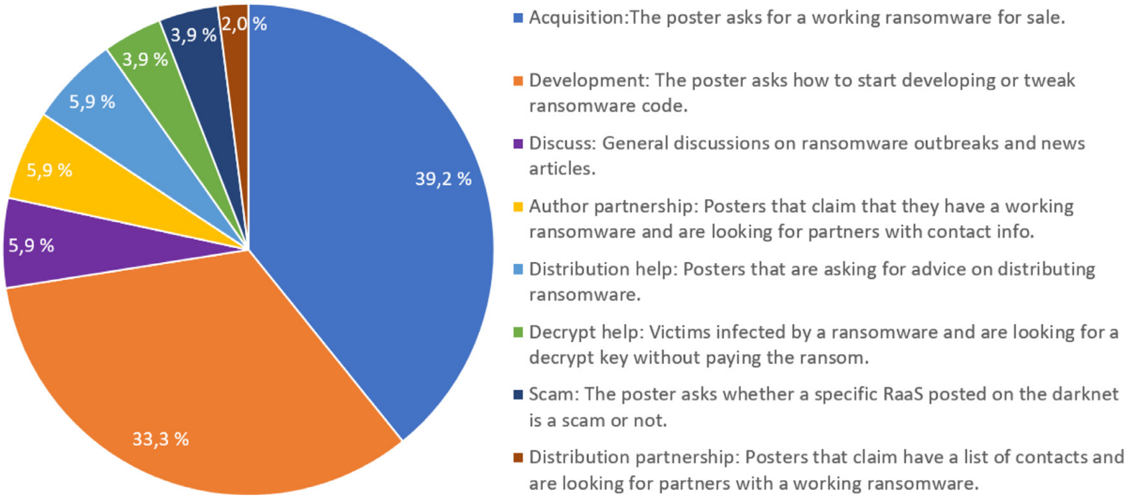

**Fig. 2.** Question categories related to ransomware in the Hidden Answers forum.

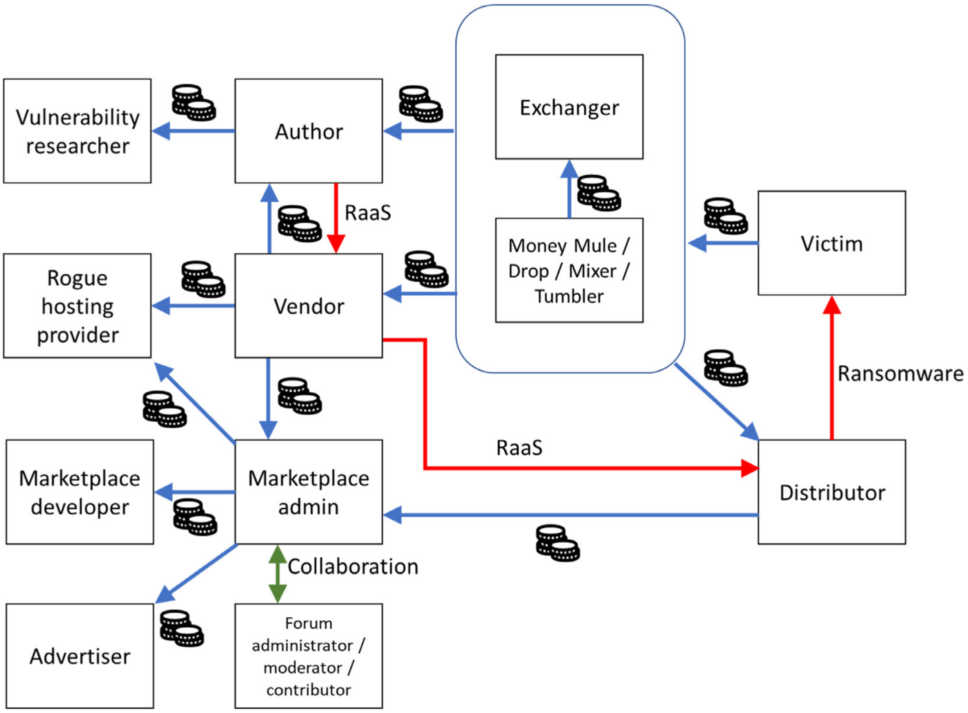

**Fig. 3.** Value chain for the RaaS economy.

## 6. Discussion

Netnography studies are useful for getting a better understanding of the activities taking place on the darknet. In our case, we narrowed the scope down to phenomena related to RaaS, but RaaS is often tied to other types of activities as well, such as a plethora of different infection methods and money laundering schemes. The size, unstructured nature and instability of our data sources have been a challenge in the data collection and analysis. However, this instability is a reality that the darknet community must deal with as well. On the surface web, we are all used to search engine functionality when looking for information, but on the darknet, links to markets, forums and websites are a commodity listed in market inventories. In addition, access to walled sites is seldom granted for free. When facing such research barriers, it is important to acknowledge that we will never get a complete picture of the social interactions and economy within this somewhat obfuscated world. However, we argue that through our research approach, we have been able to find clear indications, trends and examples of phenomena that contribute to the general knowledge of RaaS activities on the darknet.

Darknet markets, though constantly hunted by law enforcement agencies, have proven themselves to be quite resilient. In spite of numerous takedowns of high-profiled markets, vendors persist and quickly move on to other markets, using their PGP key to preserve their reputation. This is in accordance with Everton's (2008) general finding that *"covert and illegal* (i.e., *dark) networks are quick to adapt to changing environmental pressures"*.

A trend that Europol (2018) has documented, is an increasing number of smaller vendor shops and secondary markets catering to specific languages or nationalities. Smaller vendor shops are more difficult to come by, and were not within the scope of our study, so we cannot say if this is also the case for RaaS, but we observed that some of the most well-known RaaS items are provided

**Table 1**
Actor descriptions and risk categories.

| Actor | Description |
|---|---|
| Vulnerability researcher | Vulnerability researchers (Cárdenas et al., 2009) discover and sell information about zero-day vulnerabilities to others who can write the exploit code. They have high expertise in hardware and software, and a forum member mentioned that many of them were *sysadmins* in respected companies.<br>Risk category: Low, little exposure and minor consequences of getting caught. |
| Author | Authors are professional developers that create the malware that takes advantage of vulnerabilities, some of which are purchased from vulnerability researchers. There are authors offering services for signing ransomware with stolen code certificates to make the payload look legit (Abrams, 2016). As pointed out by Yip (2010), there can be fierce competition between malware authors.<br>Risk category: Low, authors seldom expose themselves on the darknet and rather outsource the risk taking to others while harvesting a significant portion of the ransom amount. |
| Vendor | Vendors do marketing and sales on marketplaces or on their own private website. Vendors can be authors, but the majority of darknet vendors have little programming knowledge and sell a wide range of products that are not necessarily digital goods. Some vendors offer technical support.<br>Risk category: Medium, can be compared to weapons dealers that facilitate crime, but do not directly take part in the offensive action. Highly exposed on the darknet. |
| Distributor | The distributors buy or get hold of RaaS and infect the devices of victims. Distributors can be observed on the darknet. They share experiences and feedback on ransomware purchases. Some distributors search for partnerships involving malware developers on forums and offer vulnerability information of their target system. As shown in earlier studies (Bayoumy et al., 2018), two levels of malware distributors can be defined; *novice* and *experienced.*<br>Risk category: High, severe consequences if they get caught (depending on different legal jurisdictions). |
| Victim | Victims suffer from ransomware infections and may lose their data or pay the ransom (or both). They may need the help of an exchanger to obtain the ransom amount in cryptocurrency.<br>Risk category: High, the main source of income for all other parties. |
| Marketplace admin | Provides a market platform that vendors and distributors can use for trade. Should be a trusted third party that governs the money transaction. There have been several examples of administrators running off with the money (exit scams).<br>Risk category: High, law enforcement agencies put a lot of effort in shutting down these services. High penalty when caught. Also, other marketplaces may try to get rid of competition. |
| Marketplace developer | Person with technical expertise that develops the marketplace platforms for the administrators. Requires a high security competence.<br>Risk category: Low, creating marketplace infrastructure is probably not a crime in itself. |
| Advertiser | Marketplace affiliate that posts darknet links on the surface web and receives kickback money when there are successful transactions originating from these. Example DeepDotWeb.<br>Risk category: Medium, high penalty when getting caught, but this does not happen often. |
| Forum admin/moderator / contributor | People responsible for managing the forum contents and membership access. Usually have a close relationship with the administrator of one or more marketplaces.<br>Risk category: Medium, forums are targeted by law enforcement agencies just as marketplaces, but probably a lesser penalty if they get caught. |
| Rogue hosting provider | Provide website hosting services on the darknet that reduces the risk of getting caught (Cárdenas et al., 2009).<br>Risk category: Low, difficult to prove that they are responsible for the website contents. |
| Money Mule / Drop / Mixer / Tumbler | Transactions received from victims are transferred through an intermediary, either a professional money launderer or someone who unknowingly forwards the money. Modern ransomware actors tend to immediately launder their gains through well-known bitcoin laundering operations, who take a fee (around 2.5%) for their services (Hernandez-Castro et al., 2017). A marketplace administrator (Empire) operating with Monero has said that tumblers are not needed due to the anonymity features of that cryptocurrency.<br>Risk category: High, unknowing mules can be traced and prosecuted even though they are innocent. New investigation techniques can better track cryptocurrency transactions. |
| Exchanger | Exchangers own verified accounts and use their immunity to offer currency exchange services to cybercriminals.<br>Risk category: Medium, as their actions can be investigated by authorities or financial institutions. |

from dedicated sites, and that several vendors were unhappy with the commission and vendor fees of the larger markets. Contrary to the findings by della Torre (2018), showing that the “best” vendors focused on few products, we have observed in the case of RaaS that the vendors deal with a large variety of products in several different categories.

What we can say with a large degree of certainty, is that RaaS constitutes a relatively small portion of the inventory for the major darknet markets. There have been reports from security companies that seem to be inaccurate or biased. For instance, one report from 2017 (CarbonBlack, 2017) claimed that there were 45,000 current listings, and that the sales of ransomware in the darknet increased by 2500% from 2016 to 2017. These estimates were based on measurements from a small sample that were extrapolated based on the assumed size of the darknet. Our latest observations showed that there were merely 69 ransomware related items for sale in the dominating markets after a strongly decreasing trend from 2018 to 2019. In addition, we saw indications many of these items were duplicates and frauds, leading us to believe that the real availability of RaaS seems exaggerated. Indeed, our assumptions regarding RaaS fraud support the findings of Wehinger (2011) and Cusack and Ward (2018) related to lack of trust and amount of fraud on the darknet. Compared to RaaS, carding services are more prevalent on the darknet, arguably since they require less technical skills and a different economic model where the buyers ask the vendor to deduct the price of the service from the total amount of money in the card instead of buying it in cryptocurrency. Unlike RaaS, the reviews on carding services are considered more authentic since they are more expressive and greater in number.

Open darknet forums allow members to share knowledge and eventually improve their skills and create partnerships with others. Getting into an invite-only forum requires a history with darknet activity, and this can be achieved through prolonged discussions on the open forums. This is in line with the *apprentice work ethics* phenomenon as reported by Mann and Sutton (1998). Holt et al. (2012) have presented a sociograph for connectivity and centrality of darknet members showing that low-skilled hackers have a lot less connections than the highly skilled, who are very much aware of their peers. This was evident in the forum activities we were able to observe as well. Those who openly want to acquire information are indeed low-skilled and publicly post on forums, putting them at the edge of the sociography, whereas the highly skilled are usually active in invite-only forums or have been assigned to be the moderator of the forum. This is in accordance with the two-tier model of Herley and Florêncio (2010); an open tier for inexperienced users and a more closed tier for experienced criminals.

Our study has been limited to English-speaking markets and forums. These are known to be more concerned with drug related items and carding services compared to, e.g., Russian sites. Leah (2019) has given an historical overview of Russian-specific darknet markets and forums that complements our study. According to her, Russian criminals are notorious for selling malicious software, while Russian authorities have *"historically turned a blind eye to online crimes"*. The most well-known darknet marketplace and forum, *RAMP*, was reportedly taken down in July 2017, but the vendors successfully moved to other key marketplaces. She also reports that digital goods markets such as *MEGA* and *Hydra* require direct communication between buyer and vendor before the transaction takes place. This mechanism is a way of increasing trust between the actors, and it will be interesting to see if the Western markets will implement the same strategy.

## 7. Conclusion and further work

Based on our own field notes from studying the darknet over two years and additional archival data going further back, the answer to our first research question is that the RaaS threat currently seems more modest than indicated in the media and reports from security companies. There are now relatively few RaaS items offered for sale in the most popular darknet marketplaces, and the number of successful sales does not indicate a large economy. Moreover, the authenticity of many items was questionable. In a virtual economy where people are anonymous and real trust is hard to come by, there are plenty of opportunists trying to make money of naïve cybercriminals. Retribution is difficult, and reporting RaaS fraud to the police is not viable for several reasons. There are professional RaaS vendors that ask for a share of the ransom revenue instead of an investment up front. They tend to host their merchandise in privately-owned websites, but these are difficult to find due to the limited search capabilities on the darknet, and the fact that advertisements are banned from most of the forums. However, it is important to remember that ransomware prevails as a serious threat when committed by experienced cybercriminals, and the forums may be considered a recruitment ground for their organisations. The value chain we have outlined to address our second research question can be useful when trying to break the underground economy behind ransomware and subsequently mitigate this cyber threat.

## Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## CRediT authorship contribution statement

**Per Håkon Meland:** Conceptualization, Investigation, Writing - original draft, Visualization, Resources, Data curation. **Yara Fareed Fahmy Bayoumy:** Conceptualization, Methodology, Investigation, Data curation. **Guttorm Sindre:** Supervision, Writing - review & editing.

## References

Ablon, L., Libicki, M.C., Golay, A.A., 2014. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*. Rand Corporation.

Abrams, L. (2016, February 23). CTB-Locker for websites: reinventing an old ransomware. Retrieved from https://www.bleepingcomputer.com/news/security/ctb-locker-for-websites-reinventing-an-old-ransomware/.

Anderson, R.J., Shumailov, I., Ahmed, M., Rietmann, A., 2018. Bitcoin redux. Paper presented at the Workshop on the Economics of Information Security (WEIS).

Aurangzeb, S., Aleem, M., Iqbal, M.A., Islam, M.A.Security, 2017. Ransomware: a survey and trends. J. Inf. Assur. 6 (2).

Bayoumy, Y., Meland, P.H., Sindre, G., 2018. A netnographic study on the dark net ecosystem for ransomware. Paper presented at the International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA).

Branwen, G., Christin, N., Décary-Hétu, D., Andersen, R.M., StExo, Presidente, E. ,..., Goode, S. (2015). Dark net market archives, 2013-2015. Retrieved from https://www.gwern.net/DNM-archives.

Broadhead, S., 2018. The contemporary cybercrime ecosystem: a multi-disciplinary overview of the state of affairs and developments. Comput. Law Secur. Rev. 34 (6), 1180–1196.

Broadhurst, R., Lord, D., Maxim, D., Woodford-Smith, H., Johnston, C., Chung, H.W.,..., Sabol, B. (2018). Malware trends on 'Darknet'Crypto-Markets: research review. Available at SSRN 3226758.

C.M. (2018). Interview: empire market admin talks DNM community, security, Crypto & Plans for Future. Retrieved from https://darkwebnews.com/darkwebmarkets/empire-market/empire-market-admin-interview/.

CarbonBlack. (2017). The ransomware economy: how and why the dark web marketplace for ransomware is growing at a rate of more than 2,500% per year. Retrieved from https://www.carbonblack.com/company/news/press-releases/dark-web-ransomware-economy-growing-annual-rate-2500-carbon-black-research-finds/.

Cárdenas, A., Radosavac, S., Grossklags, J., Chuang, J., Hoofnagle, C., 2009. An economic map of cybercrime. Paper presented at the Telecommunications Policy Research Conference (TPRC).

CheckPoint. (2016). CerberRing: an in-depth exposé on cerber Ransomware-as-a-Service. Retrieved from https://blog.checkpoint.com/2016/08/16/cerberring/.

Conti, M., Gangwal, A., Ruj, S., 2018. On the economic significance of ransomware campaigns: a Bitcoin transactions perspective. Computers & Security, 79 162–189.

Cusack, B., Ward, G., 2018. Points of failure in the ransomware electronic business model. Paper presented at the Twenty-fourth Americas Conference on Information Systems.

*DarknetLive*. (2019). Darknet markets. Retrieved from https://darknetlive.com/.

*DeepDotWeb*. (2017). DeepDotWeb. Retrieved from https://www.deepdotweb.com/.

della Torre, G.G., 2018. Business Strategies in Darknet Marketplaces: An attempt to Model Competition in the Framework of Economic Complexity. Politecnico di Torino. Retrieved from https://webthesis.biblio.polito.it/9063/.

DIVIDEDBY0. (2017). Sheep marketplace owner indicted and face years in prison. Retrieved from https://www.deepdotweb.com/2017/04/21/sheep-marketplace-owner-indicted-face-years-prison/.

DNetX. (2019). Darknet Markets. Retrieved from https://www.darknetmarkets.com/.

*DNStats*. (2019). Dark Market Tracker. Retrieved from https://dnstats.net/.

Europol. (2017, 20 July). Massive blow to criminal dark web activities after globally coordinated operation. Retrieved from https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

Europol. (2018). Internet Organised Crime Threat Assessment (IOCTA) 2018. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.

Europol. (2019). Internet Organised Crime Threat Assessment (IOCTA) 2019. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019.

Everton, S.S., 2008. Tracking, Destabilizing and Disrupting Dark Networks with Social Networks Analysis. The NPS Institutional Archive DSpace Repository Retrieved from Calhoun https://calhoun.nps.edu/handle/10945/34415.

Grobman, S., Cerra, A., 2016. The Second Economy: The Race for Trust, Treasure and Time in the Cybersecurity War. Apress.

Herley, C., Florêncio, D., 2010. Nobody sells gold for the price of silver: dishonesty, uncertainty and the underground economy. In: Economics of Information Security and Privacy. Springer, pp. 33–53.

Hernandez-Castro, J., Cartwright, E., & Stepanova, A. (2017). Economic analysis of ransomware. arXiv:1703.06660v1.

Holt, T.J., Strumsky, D., Smirnova, O., Kilger, M., 2012. Examining the social networks of malware writers and hackers. Int. J. Cyber Criminol. 6, 891.

Huang, D.Y., Aliapoulios, M.M., Li, V.G., Invernizzi, L., Bursztein, E., McRoberts, K., ... McCoy, D., 2018. Tracking ransomware end-to-end. Paper presented at the 2018 IEEE Symposium on Security and Privacy (SP).

Jaishankar, K., 2008. Space transition theory of cyber crimes. In: Schmalleger, F., Pittaro, M. (Eds.), Crimes of the Internet. Pearson, pp. 283–301.

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., Kirda, E., 2015. Cutting the gordian knot: a look under the hood of ransomware attacks. Paper presented at the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment.

Kozinets, R.V., 2019. Netnography: The Essential Guide to Qualitative Social Media Research. SAGE Publications Limited.

Kozinets, R.V., Dolbec, P.-Y., Earley, A., 2014. Netnographic analysis: understanding culture through social media data. In: The SAGE Handbook of Qualitative Data Analysis. SAGE, pp. 262–276.

Kwon, K.H., Shakarian, J., 2018. Black-Hat Hackers' crisis information processing in the Darknet: a case study of cyber underground market shutdowns. In: Networks, Hacking, and Media–CITA MS@ 30: Now and Then and Tomorrow. Emerald Publishing Limited, pp. 113–135.

Laszka, A., Farhang, S., Grossklags, J., 2017. On the economics of ransomware. Paper presented at the International Conference on Decision and Game Theory for Security.

Lavorgna, A., 2015. Organised crime goes online: realities and challenges. J. Money Launder. Control 18 (2), 153–168.

Leah, M. (2019). Russians on the darknet part II: marketplaces & forums. Retrieved fromhttps://www.darkowl.com/blog/2019/russians-on-the-darknet-marketplaces-amp-forums.

Lee, J., Lee, K., 2017. Spillover effect of ransomware: economic analysis of web vulnerability market. Res. Brief. Inf. Commun. Technol. Evolut. (ReBICTE) 3.

Lewis, S.J. (2017). Dark web data dumps. Github Repository. Retrieved from https://polecat.mascherari.press/onionscan/dark-web-data-dumps.

Liska, A., Gallo, T., 2016. Ransomware: Defending Against Digital Extortion. O'Reilly Media, Inc..

Mann, D., Sutton, M., 1998. »NETCRIME: more change in the organization of thieving. Br J Criminol 38 (2), 201–229.

Martin, J., Christin, N., 2016. Ethics in cryptomarket research. Int. J. Drug Policy 35, 84–91.

McKenna, M., & Goode, S. (2017). Alphabay crawl 20170128. Retrieved from https://www.dropbox.com/s/0w74dz4c83tzhar/20170128-alphabay.tar.xz.

Moore, D., Rid, T., 2016. Cryptopolitik and the darknet. Survival (Lond) 58 (1), 7–38.

Naylor, R.T., 2000. Expert Panel on Emerging Crimes: Hosted by the Department of Justice, Canada Retrieved from https://www.justice.gc.ca/eng/rp-pr/csj-sjc/crime/rr03_20/rr03_20.pdf.

O'Gorman, G., & McDonald, G. (2012). *Ransomware: a growing menace*. Retrieved from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf.

O'Kane, P., Sezer, S., Carlin, D., 2018. Evolution of ransomware. IET Networks 7 (5), 321–327.

Paquet-Clouston, M., Haslhofer, B., Dupont, B., 2019. Ransomware payments in the bitcoin ecosystem. J. Cybersecur. 5 (1) tyz003.

*Reddit*. (2019). The front page of the internet. Retrieved from https://www.reddit.com/.

Rossy, Q., Décary-Hétu, D., 2017. Internet traces and the analysis of online illicit markets. In: The Routledge International Handbook of Forensic Intelligence and Criminology. Routledge, pp. 249–263.

Symantec. (2019). Internet security threat report. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-executive-summary-en.pdf.

*TheDarkWebLInks*. (2019). Darkweb markets. Retrieved from https://www.thedarkweblinks.com.

Thomas, K., Huang, D., Wang, D., Bursztein, E., Grier, C., Holt, T.J., … Vigna, G., 2015. Framing dependencies introduced by underground commoditization. In: Paper presented at the Workshop on Economics of Information Security (WEIS).

Vaas, L. (2012, April 23). Tor-hidden online narcotics store, 'The farmer's market', brought down in multinational sting. Retrieved from https://nakedsecurity.sophos.com/2012/04/23/farmers-market-tor-narcotics/.

Van Wegberg, R., Tajalizadehkhoob, S., Soska, K., Akyazi, U., Gañán, C., Klievink, B., … Van Eeten, M., 2018. Plug and prey? measuring the commoditization of cybercrime via online anonymous markets. In: Paper presented at the Proceedings of the 27th USENIX Conference on Security Symposium. Baltimore, MD, USA.

Van Wegberg, R., Verburgh, T., Van den Berg, J., & Van Staalduinen, M. (2017). Alphabay exit, hansa-down: dream on? Retrieved from https://dws.pm/download/PUB/17-9099-factsheetbrochure-dws-05.pdf.

Waldrop, M.M., 2016. How to hack the hackers: the human side of cybercrime. Nature 533 (7602).

Wehinger, F., 2011. The dark net: self-regulation dynamics of illegal online markets for identities and related services. Paper presented at the European Intelligence and Security Informatics Conference (EISIC).

Yip, M., 2010. An investigation into Chinese cybercrime and the underground economy in comparison with the West (Master Thesis). University of Southampton.

Yip, M., Webber, C., Shadbolt, N., 2013. Trust among cybercriminals? Carding forums, uncertainty and implications for policing. Polic. Soc. 23, 516–539.

Young, A.L., Yung, M., 2017. On ransomware and envisioning the enemy of tomorrow. Computer 50 (11), 82–85.

Zhuge, J., Holz, T., Song, C., Guo, J., Han, X., Zou, W., 2009. Studying malicious websites and the underground economy on the Chinese web. In: Managing Information Risk and the Economics of Security. Springer, pp. 225–244.

**Per Håkon Meland** is a senior research scientist at the independent research institute SINTEF in Norway. He obtained his M.Sc. degree in Computer Science at the Norwegian University of Science and Technology in 2002, where he is also a Ph.D. fellow in the intertwined fields of threat modelling and security economics.

**Yara Fareed Fahmy Bayoumy** completed her Information Systems Master degree at the Norwegian University of Science and Technology in 2018. She earned a Bachelors Degree in Computer and Communication Engineering from Alexandria University in 2015.

**Guttorm Sindre** is a professor at the Department of Computer Science, Norwegian University of Science and Technology, and is also leader for the Excited Centre for Excellence in IT Education. He obtained his Ph.D. from the Norwegian Institute of Technology in 1990. His research interests are in requirements engineering, security requirements, and IT education and didactics.