IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 22, 2018, accepted April 25, 2018, date of publication April 30, 2018, date of current version June 5, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2831667

A Data Analytics Approach to the Cybercrime Underground Economy

JUNGKOOK AN AND HEE-WOONG KIM
Graduate School of Information, Yonsei University, Seoul 03722, South Korea

Corresponding author: Hee-Woong Kim (kimhw@yonsei.ac.kr)

This work was supported in part by the Ministry of Education of South Korea and the National Research Foundation of Korea under Grant NRF-2015S1A3A2046711 and in part by the Barun ICT Research Center, Yonsei University, under Grant 2018-22-0003.

ABSTRACT Despite the rapid escalation of cyber threats, there has still been little research into the foundations of the subject or methodologies that could serve to guide information systems researchers and practitioners who deal with cybersecurity. In addition, little is known about crime-as-a-service (CaaS), a criminal business model that underpins the cybercrime underground. This research gap and the practical cybercrime problems we face have motivated us to investigate the cybercrime underground economy by taking a data analytics approach from a design science perspective. To achieve this goal, we: (1) propose a data analysis framework for analyzing the cybercrime underground; (2) propose CaaS and crimeware definitions; (3) propose an associated classification model, and (4) develop an example application to demonstrate how the proposed framework and classification model could be implemented in practice. We then use this application to investigate the cybercrime underground economy by analyzing a large data set obtained from the online hacking community. By taking a design science research approach, this paper contributes to the design artifacts, foundations, and methodologies in this area. Moreover, it provides useful practical insights to practitioners by suggesting guidelines as to how governments and organizations in all industries can prepare for attacks by the cybercrime underground.

INDEX TERMS Crimeware-as-a-Service, crimeware, underground economy, hacking community, machine learning, design science research.

I. INTRODUCTION

As the threat posed by massive cyberattacks (e.g., ransomware and distributed denial of service attacks (DDoS)) and cybercrimes has grown, individuals, organizations, and governments have struggled to find ways to defend against them. In 2017, ransomware known as WannaCry was responsible for nearly 45,000 attacks in almost 100 countries [1]. The explosive impact of cybercrime has put governments under pressure to increase their cybersecurity budgets. United States President Barack Obama proposed spending over $19 billion on cybersecurity as part of his fiscal year 2017 budget, an increase of more than 35% since 2016 [2].

Global cyberattacks (such as WannaCry and Petya) are executed by highly organized criminal groups, and organized or national-level crime groups have been behind many recent attacks. Typically, criminal groups buy and sell hacking tools and services on the cybercrime black market, wherein attackers share a range of hacking-related information. This online underground market is operated by groups of attackers, and it in turn supports the underground cybercrime economy [3]. The cybercrime underground has thus emerged as a new type of organization that both operates black markets and enables cybercrime conspiracies to flourish.

Because organized cybercrime requires an online network to exist and to conduct its attacks, it is highly dependent on closed underground communities (e.g., Hackforums and Crackingzilla). The anonymity these closed groups offer means that cybercrime networks are structured differently than traditional Mafia-style heirarchies [4], which are vertical, concentrated, rigid, and fixed. In contrast, cybercrime networks are lateral, diffuse, fluid, and evolving. Since cyberspace is a network of networks [5], the threat posed by the rise of highly professional network-based cybercrime business models, such as Crimeware-as-a-Service (CaaS), remains mostly invisible to governments, organizations, and individuals.

Even though Information Systems (IS) researchers and practitioners are taking an increasing interest in cybercrime, due to the critical issues arising from the rapid increase in

cyber threats, few have attempted to put this new interest on a solid foundation or develop suitable methodologies. Previous studies have not analyzed the underground economy behind cybercrime in depth. Furthermore, little is known about CaaS, one of the primary business models behind the cybercrime underground. There is an overall lack of understanding, both in research and practice, of the nature of this underground and the mechanisms underlying it.

This research gap, and the practical problems faced by cybercriminals, motivates our study. We take a data analytics approach and investigate the cybercrime economy from a design science perspective. To achieve this goal, we (1) propose a data analysis framework for analyzing the cybercrime underground to guide researchers and practitioners; (2) define CaaS and crimeware to better reflect their features from both academic research and business practice perspectives; (3) use this to build a classification model for CaaS and crimeware; and (4) build an application to demonstrate how the proposed framework and classification model could be implemented in practice. We then evaluate this application by applying it in a case study, namely investigating the cybercrime economy by analyzing a large dataset from the online hacking community.

This study takes a design science research (DSR) approach. Design science ''creates and evaluates information technology artifacts intended to solve identified problems'' [6]. DSR involves developing a range of IT artifacts, such as decision support systems, models, frameworks, tools, methods, and applications [7]. Where behavioral science research seeks to develop and justify theories that explain or predict human or organizational phenomena, DSR seeks to extend the boundaries of human and organizational capabilities by creating new and innovative artifacts [6]–[8]. DSR's contribution is to add value to the literature and practice in terms of ''design artifacts, design construction knowledge (e.g., foundations), and/or design evaluation knowledge (e.g., methodologies),'' [7].

This study follows these DSR guidelines and contributes design artifacts, foundations, and methodologies [7]. In particular, DSR must demonstrate that design artifacts are ''implementable'' in the business environment to solve an important problem [7], so we provide an implementable framework rather than a conceptual one. We also create a front-end application as a case example to demonstrate how the proposed framework and classification model could be implemented in practice. In addition, this study contributes to design theory [9], [10].

As for foundations, DSR should have a creative development of constructs, models, methods, or instantiations that extend the design science knowledge base [7]. This study therefore adds to the knowledge base by providing foundational elements such as constructs (definitions, frameworks, and applications), a model (classification model), a method (analysis), and instantiations (applications).

As for methodologies, the creative development and use of evaluation methods provide DSR contributions [7]. Accordingly, this study uses dynamic analysis to conduct an ex-ante evaluation of the classification model. It also conducts an ex-post evaluation of a front-end application using observational methods (case examples). From a practical perspective, this study also provides practitioners with useful insights by making suggestions to guide governments and organizations in all industries in solving the problems they face when preparing for attacks from the cybercrime underground.

II. CONCEPTUAL BACKGROUND

A. CYBERCRIME UNDERGROUND BUSINESS MODEL

Cybercrime has undergone a revolutionary change, going from being product-oriented to service-oriented because the fact it operates in the virtual world, with different spatial and temporal constraints, differentiates it from other crime taking place in the physical world [11]. As part of this change, the cybercrime underground has emerged as a secret cybercrime marketplace because emerging technological changes have provided organized cybercriminal groups with unprecedented opportunities for exploitation [12].

The cybercrime underground has a highly professional business model that supports its own underground economy [5]. This business model, known as CaaS, is ''a business model used in the underground market where illegal services are provided to help underground buyers conduct cybercrimes, such as attacks, infections, and money laundering in an automated manner,'' [3]. Thus, CaaS is referred to as a do-it-for-me service, unlike crimeware which is a do-it-yourself product.

Because CaaS is designed for novices, its customers do not need to run a hacking server or have high-level hacking skills. Consequently, the CaaS business model can involve the following roles: writing a hacking program, performing an attack, commissioning an attack, providing an attack server (infrastructure), and laundering the proceeds. Sood and Enbody [3] have suggested that crimeware marketplaces have three key elements, namely actors (e.g., coders, operators, or buyers), value chains, and modes of operation (e.g., CaaS, pay-per-install, crimeware toolkits, brokerage, or supplying data). Periodic monitoring and analysis of the content of cybercrime marketplaces could help predict future cyber threats [3].

B. ROUTINE ACTIVITY THEORY

In criminology, routine activity theory (RAT) is used to explain the causes of crime, both general criminal activity and cybercrime [13], [14]. According to this theory, three elements are necessary for crimes to be committed: (1) a likely offender, (2) a suitable target, and (3) the absence of capable guardians against crime. In a cybercrime context, the ''likely offenders'' are motivated sellers and potential buyers in the underground market, and the ''suitable targets'' are the targeted vulnerable organizations. The ''absence of capable guardians against crime'' is due to organizations failing to take preventive measures against cybercrime.

Two types of product or service are available in the cybercrime underground. The first can be either CaaS or crimeware that are related to attack strategy, for example, phishing, brute force, or DDoS attacks, or can be used for spamming or creating botnets, exploits, ransomware, rootkits, or Trojans. Attack strategies often exploit system vulnerabilities such as application loopholes. In addition, social engineering attacks exploit human vulnerabilities [15]. The most well-known example of such an attack is the use of a ''secret question'' for password recovery: attackers check into the user's background to guess the secret question and hence steal the account. However, because social engineering is one of the oldest account hacking techniques, most account holders are now aware of it. In addition, social engineering-related products and services are rarely traded underground, although a few sellers have been known to sell tutorials. As a result, we have not included ''social engineering services'' as a CaaS type.

The second type of product or service available neutralizes organizations' preventive measures, such as anti-virus programs. These are based on programs designed to evade anti-virus software to either cause mischief or be left behind for later activation. Examples include encryption and virtual private network (VPN) services, crypters, and proxies.

From the perspective of RAT, the likely offenders are attackers motivated to attack organizations or products that constitute a suitable target. If such targets are attacked, however, both the targets and those who supply their cybersecurity products become aware of the vulnerabilities that made the attack possible, leading them to apply security updates to their software. These updates can be seen as capable guardians against crime, and the preventive measures taken can be identified by looking through each program's version history.

However, this is not the end of the matter, because the attackers will then develop and sell new versions of their hacking tools to combat the guardians, thus re-establishing the third RAT condition, the absence of capable guardians against crime. Such events can also be identified by the version numbers of the hacking tools sold on the black market: since it is an online marketplace, attackers must give detailed explanations to retain their customers' confidence. This cycle will continue as long as attackers can find vulnerabilities in organizations or products.

From this perspective, the cybercrime underground black market is essentially a market economy, ruled by supply and demand, with the preventive measures taken by organizations being the key drivers of demand. Ironically, attackers can only sell new tools because of their target organizations' ongoing preventive measures, which serve to make the black market more viable. Unlike criminals in general, attackers regard capable guardians against crime as a necessary evil, because cybercrime tends to adhere faithfully to market economy principles. Therefore, to get at the fundamental cybercrime issues, we need to understand the mechanisms underlying the cybercrime underground from an RAT perspective.

III. CLASSIFICATION AND DEFINITION OF CRIMEWARE PRODUCTS AND SERVICES

Although both academics and practitioners have recently started to devote more attention to CaaS, its fast-growing nature has prevented them from reaching consensus on how to define different types of CaaS and crimeware. As a result, most of the academic research has borrowed the definitions used by the business practice literature, leading to widely varying interpretations in different disciplines. Given this ambiguity, we approach categorizing CaaS and crimeware from an RAT perspective (considering vulnerabilities as suitable targets and preventive measures as capable guardians against crime) in a cybercrime underground context. In addition, we redefine CaaS and crimeware based on the definitions used in existing research and practice.

A. CLASSIFICATION OF CRIMEWARE SERVICES AND PRODUCTS

Table 1 lists the definitions of CaaS and crimeware used in the academic and business practices literature, which form a basis for our classification model, suitable for the IS field. We reclassify CaaS and crimeware in terms of the suitable targets (attack strategy/mode) and absence of capable guardians (preventive measures) in a cybercrime underground context.

The different attack strategies/modes in Table 1 are associated with RAT's suitable targets because vulnerable organizations, products, and services may suffer from attacks using a variety of strategies. In contrast, preventive measures are associated with RAT's absence of capable guardians because encryption and VPN services, crypters, and proxies are intended to neutralize preventive measures by bypassing anti-virus and log monitoring software.

B. DEFINITION OF CRIMEWARE SERVICES AND PRODUCTS

We now need to review the definitions used in both the research and business practice literature. This study extends the IS literature by facilitating a conceptual understanding of the CaaS business models used by the cybercrime underground. Drawing upon prior research and business practice literature, we propose definitions of CaaS and crimeware that better reflect the features of CaaS in both of these areas.

1) CRIMEWARE-AS-A-SERVICE

- Account Hacking Services: Previous academic research has defined account hacking as ''a crime which originated as a type of theft specific to digital environments where users create personal digital profiles and store valuable personal information such as passwords, bank account numbers, and ID numbers,'' [16]. In digital environments, such as cloud computing platforms, account hacking is one of the main cybersecurity threats. The most common account hacking methods are phishing and brute force attacks. With an emphasis on selling this as a service, we define an *account hacking service* as *a service that offers to gain unauthorized access*

TABLE 1. Classification of crimeware products and services. Phishing and brute force attack services are subsets of account hacking service.

Classification			Academic Literature	Business Practice Literature
Crimeware-as-a-Service (Service)	**Attack Strategy/ Mode**	**Account hacking**	Rakitianskaia et al. [16]	Goncharov [20]
		• **Phishing***	van der Merwe et al. [17] Volonino et al. [18]	Bezmalyi [21] Ng [22]
		• **Brute Force attack***	Álvarez et al. [19]	Shankdhar [23]
		DDoS attack	Mirkovic et al. [24] Singh and Juneja [25]	Goncharov [20] McMillen [26]
		Spamming	Cunningham et al. [27] Gyongyi and Garcia-Molina [28]	Zaharia [29]
	Preventive Measure	**Crypting services**	Tasiopoulos and Katsikas [30]	Goncharov [20]
		VPN services	Venkateswaran [31]	Goncharov [20]
Crimeware (Product)	**Attack Strategy/ Mode**	**Drive-by download**	Sood et al. [32]	Glassberg [33]
		• **Botnet**	Wang et al. [34] Zeidanloo and Manaf [35]	McMillen [26]
		• **Exploit**	Shahriari and Jalili [36]	Amaya [37]
		• **Ransomware**	Gazet [38] O'Gorman and McDonald [39]	Khanse [40] Turkel [41]
		• **Rootkit**	Zhu et al. [42] Luo et al. [43]	Kassner [44]
		• **Trojan**	Tehranipoor and Wang [45] Colarik and Janczewski [46]	Ortiz [47]
	Preventive Measure	**Crypter**	Tasiopoulos and Katsikas [30]	Goncharov [20]
		Proxy	Waldo [48]	Goncharov [20]

to a target's account by obtaining account information (e.g., username and password) or extra security information (e.g., security questions and answers).

Phishing Services: Phishing has been defined in the business practice literature in the last few years because it has become increasingly sophisticated and is one of the most common techniques used by cybercriminals. Phishing is defined as ''masquerading as a trustworthy source in an attempt to bait a user to surrender sensitive information such as a username, password, and credit card number,'' [22]. Volonino *et al.* [18] defined phishing as ''sending an e-mail to a user falsely claiming to be a legitimate enterprise in an attempt to scam the user.'' The term ''phishing'' is a portmanteau of ''password'' and ''fishing,'' where the latter refers to catching fish using bait or a lure. We thus define a *phishing service* as *a service that hacks accounts by pretending to be a reliable source, such as a bank or card service*.

Brute Force Attack Services: A brute force attack is an attempt to log in to an account and steal it by repeatedly trying random passwords. Such attacks often target less specific targets than phishing or social engineering. For example, an attacker may try to log in using one of the system's default usernames (e.g., ''root'' or ''admin'') by systematically trying all possible passwords. We thus define a *brute force attack service* as *a service that hacks accounts by trying all possible passwords*.

- DDoS Attack Services: In the research literature, a DDoS attack is defined as ''an attack which makes resources unavailable to its legitimate users,'' [25]. In the business practice literature, it is defined as ''an attack involving an enormous number of spurious requests from a large number of computers worldwide that flood a target server,'' [16]. DDoS botnet attacks can cause serious damage: for example, the Gameover Zeus attack stole online banking credentials, resulting in a $100 million loss [26]. However, the above definitions are not precise and do not encompass all the definitions used in research and practice. We thus define a *DDoS attack service* as *a service that makes one target service*

unavailable by flooding it with traffic from multiple compromised sources.

- Spamming Services: Over the last decade, spamming has been defined in a variety of ways in the literature. The academic literature defines spam as "unsolicited and unwanted e-mail from a stranger that is sent in bulk to large mailing lists, usually with some commercial objective," [27]. Likewise, Gyongyi and Garcia-Molina [28] defined spamming as "any deliberate human action that is meant to trigger an unjustifiably favorable relevance or importance of some web page considering the page's true value." Based on these characteristics, we define a *spamming service* as *a service that sends out unsolicited emails to a large number of people (e.g., mailing lists) using automated software*.
- Crypting Services: Crypter encrypt programs or source code to avoid detection and tracking and thus bypass anti-virus software [30]. Like other hacking services, encryption is sold as a service because crypters require a certain level of skill to use. The goal of such a service is to neutralize the preventive measures put in place by organizations and anti-virus software, preventing hacking programs from being caught or allowing them to be left behind to collect information. We define an *crypting service* as *a service that encrypts malicious code by using a crypter to bypass anti-virus software*.
- VPN Services: Networks connect different entities, and private networks only allow access by closed communities of authorized users [31]. The most secure way to access the Internet is using a VPN, because it hides all user information (e.g., identity and IP address). Because attackers use VPN services to avoid tracking or IP blocks, they are categorized as CaaS-related preventive measures. We thus define a *VPN service* as *a service that provides a secure connection to the Internet via a virtual private network*.

2) CRIMEWARE PRODUCTS

Crimeware itself is not considered to be CaaS, and comes in several different forms, as follows.

- Bootnet: Botnets are networks of compromised (or "zombie") computers controlled by "bot masters," and have become the most common cyberattack vector over the past few years [34], [35]. We define a *botnet* as *a network of infected devices, typically used for DDoS attacks*.
- Exploit: In the business practice field, an exploit is defined as "a program created specifically to exploit a vulnerability, in other words—simply trying to take advantage of an error in the design or programming of a system or application," [37] and is used to obtain administrator privileges on a system. We thus define an *exploit* as *a program or script that exploits vulnerabilities in applications, servers, or clients*.
- Ransomware: Ransomware is a type of malicious software that disables the functionality of a computer in some way [38]. We thus define *ransomware* as*malicious software that encrypts a victim's data to extort money from them*.
- Rootkit: The business practice literature defines a rootkit as "a program that allows someone to obtain root-level access to the computer," [44]. We thus define a *rootkit* as *a piece of malicious software that enables administrator-level access to an operating system or computer network*.
- Trojan: Trojans are defined by Colarik and Janczewski [46] as malicious programs that perform a legitimate function but also engage in unknown and/or unwanted activity. We thus define a *Trojan* as *a piece of malware that provides unauthorized remote access to a victim's computer*.
- Drive-by download: All these crimeware products are used in drive-by download attacks, which have become one of the primary types of cyberattack worldwide. Such attacks target victims through their Internet browsers, installing malware their computers as soon as they visit an infected website [33]. We thus define a *drive-by download attack* as *an attack that installs malware when the victim visits a malicious webpage*.
- Crypter: Crypters can encrypt programs or source code to avoid detection and tracking by bypassing anti-virus software [30], and can also be offered as a service. We thus define a *crypter* as *a piece of encryption software that helps an intruder to bypass security programs*.
- Proxy: Proxies are used for a variety of purposes, such as accelerating data transmission and filtering traffic [20]. We thus define a *proxy* as *a server that enables anonymous Web browsing*.

IV. ANALYTICAL FRAMEWORK AND METHODS

The constructs used in DSR are entity representations [10] that provide the vocabulary and symbols needed to define problems and solutions [7]. Accordingly, the design elements used in this study are the cybercrime underground, criminal items (CaaS and crimeware), classifications, and front-end system applications, and the artifacts are based on these constructs. These artifacts are evaluated in two stages [49]: ex-ante (classification evaluation) and ex-post (case example). Because DSR should be tentative, this ex-post evaluation is essential to the search process used by iterative DSR, which comprises search, design, ex-ante evaluation, construction, artifact, ex-post evaluation, and research [49]. Based on this, we propose the data analysis framework shown in Fig. 1.

Because cybercrime differs from general crime in many ways, we need to conduct a variety of analyses using a large dataset. A previous study [50] proposed a data mining framework for crime, dividing crimes harmful to the general public into eight categories: traffic violations, sex crime, theft, fraud, arson, gang/drug offenses, violent crime, and cybercrime.

Although the previous study explained how data mining techniques could be applied to crime analysis, it did not consider the specific features of cybercrime. Furthermore, it

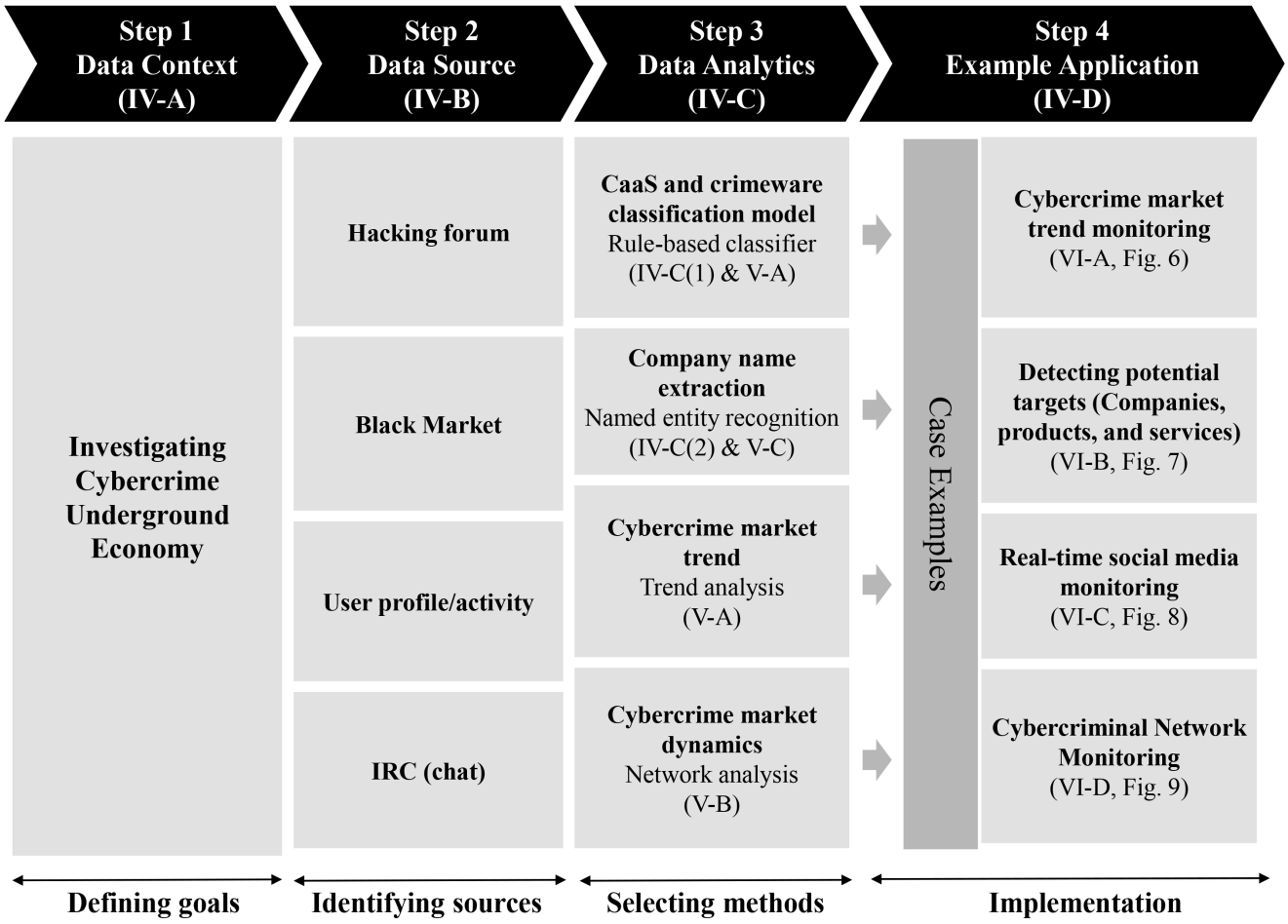


FIGURE 1. Proposed data analytical framework. Sections are in parentheses.

only explained the data mining techniques briefly, rather than presenting a broad overview of the framework [50]. In contrast, the goal of our data analysis framework is to conduct a big-picture investigation of the cybercrime underground by covering all phases of data analysis from the beginning to the end (see Fig. 1). This framework comprises four steps: (1) defining goals; (2) identifying sources; (3) selecting analytical methods; and (4) implementing an application.

Because this study emphasizes the importance of RAT for analyzing the cybercrime underground, the proposed RAT-based definitions are critical to this framework: Steps 1–4 all contain the RAT elements, as Fig. 1 shows.

A. STEP 1: DEFINING GOALS

The first step is to identify the conceptual scope of the analysis. Specifically, this step identifies the analysis context, namely the objectives and goals. To gain an in-depth understanding of the current CaaS research, we investigated the cybercrime underground, which operates as a closed community. Thus, the goal of the proposed framework is to ''investigate the cybercrime underground economy.''

B. STEP 2: IDENTIFYING SOURCES

The second step is to identify the data sources, based on the goals defined by Step 1. This step should consider what data is needed and where it can be obtained. Since the goal of this study is to investigate the cybercrime underground, we consider data on the cybercrime underground community. We therefore collected such data from the community itself and obtained a malware database from a leading global cybersecurity research firm.

Because cybercimimals often change their IP addresses and use anti-crawling scripts to conceal their communications, we used a self-developed crawler that can resolve captchas and anti-crawling scripts to gather the necessary data. We collected a total of 2,672,091 posts selling CaaS or crimeware, made between August 2008 and October 2017, from a large hacking community site (www.hackforums.net) with over 578,000 members and more than 40 million posts. We also collected 16,172 user profiles of sellers and potential buyers, based on their communication histories, as well as prices and questions and answers about the transactions.

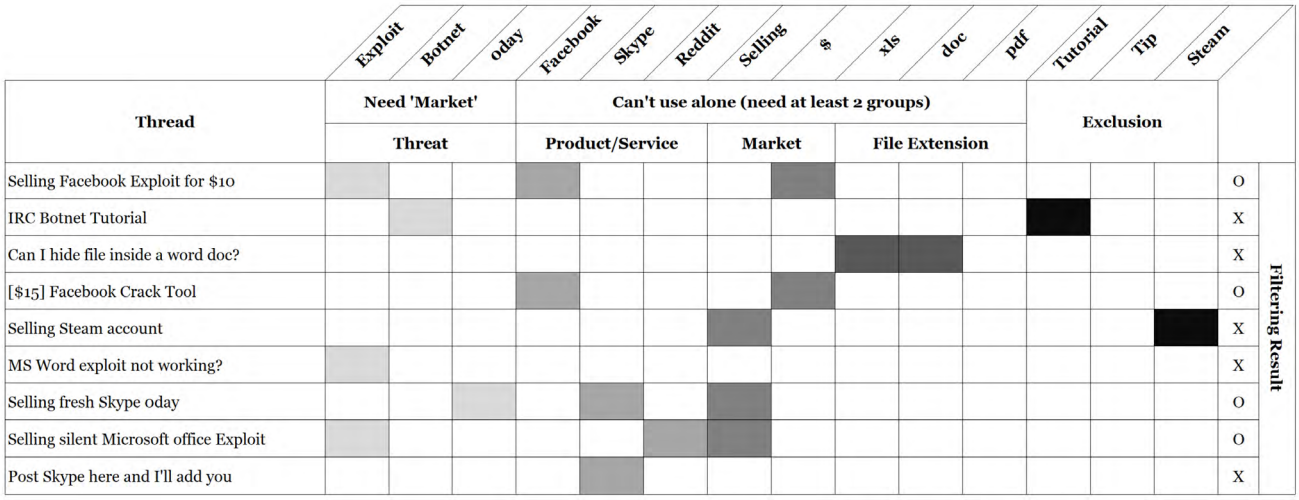


FIGURE 2. Rule-based matrix used for content filtering.

The black market uses traditional forum threads (e.g., bulletin boards) instead of typical e-commerce platforms (e.g., eBay, and Amazon). For example, sellers create threads in marketplace forums to sell items, and potential buyers comment on these threads. One of the most significant challenges was therefore converting this unstructured data into structured data. Since the product features, prices, and descriptions were explained within longer texts, we used a variety of text mining techniques to extract the important features: for example, we used named entity recognition to extract company names (see Section IV-C(2)). Since these texts included many typographic errors and jargon terms, we had to create a dictionary for use during a preprocessing step.

In addition, we obtained a malware database from a cybersecurity firm containing over 53,815 entries covering cybercrimes between May 11, 2010 and January 13, 2014. This unique dataset strengthened our study by providing real-world evidence from a different viewpoint.

C. STEP 3: SELECTING ANALYTICAL METHODS

1) CAAS AND CRIMEWARE CLASSIFICATION MODEL

A diverse range of items are sold in the cybercrime underground, with different degrees of associated risk. For this study, we focused mainly on items critical to hacking. We first filtered the messages to select only those that carried significant risks, and then divided them into the categories shown in Table 1.

To determine if a given message is dangerous, our classification model checks whether it falls into one of the following five categories: Threat, Product/Service, File Extension, Market, and Exclusion. Fig. 2 shows a simplified example to clarify this rule-based approach. We used a dictionary consisting of 1,191 keywords spread across five categories, built using data obtained from the cybersecurity research firm, anti-virus vendors, Wikipedia, and forums.

To be classified as a dangerous Threat, for example, a message must also contain Market-related keywords. Messages containing both Threat- and Market-related keywords are considered more dangerous (e.g., ''Selling silent Microsoft Office exploit'') than messages with only Threat-related keywords (e.g., ''Can I hide a file inside a word doc?''). Likewise, messages related to the Product/Service, Market, and File Extension categories are not identified as dangerous if they only contain keywords related to one category. In addition, messages containing Exclusion-related keywords (e.g., ''tutorials'' or ''tips'') are not identified as a dangerous (see Fig. 2).

To classify messages correctly, we also use keywords related to CaaS and crimeware. This classification step is applied after the messages have been filtered as above, so many keywords are not needed and the criteria are simpler. However, when a message fits into multiple categories, this overlap is recorded so as to derive additional insights from the later analysis and applications. The types of keyword used for the proposed classification model are as follows.

- Threat: keywords directly related to threats or cyberattacks (e.g., ''exploit'' or ''botnet'').
- Product/Service: keywords related to products or services (e.g., ''Facebook'' or ''Skype'').
- File Extension: keywords related to software or add-ons (e.g., ''doc'' or ''ppt'').
- Market: keywords related to markets or transactions (e.g., ''selling'' or ''$'').
- Exclusion: keywords that are not related to malware (e.g., ''tutorial'' or ''tips'').

To improve the quality of the training data, we referred to the malware database obtained from the cybersecurity research firm. Since this database contained labeled black market communications by cybersecurity professionals, it provided an appropriate guide for building the training dataset.

However, the database was a little out of date (May 11, 2011 to January 13, 2014), so we also referred to more recent data from anti-virus vendors' websites. Four undergraduate students (two groups of two) with cybersecurity backgrounds assisted in validating this data. Before creating the training dataset, we presented the participants with a set of guidelines and procedures based on the malware dataset. After they had fully understood and discussed these, we used them to create the training data. When two students disagreed, someone from the other group discussed the matter with them to help reconcile the disagreement. The inter-rater reliability score was 82%. This is above the suggested reliability minimum (80%), and so was considered adequate [51].

We employ the naïve Bayes algorithm, a probabilistic classification algorithm [52], [53] that addresses probabilistic reasoning under uncertainty, because it is the simplest approach for text classification [54]. Its predictions self-correct as new information is encountered, so they become more accurate with more data. The conditional probability is given by Bayes' theorem:

$$P(C_i \mid d) = \frac{P(d \mid C_j)P(C_j)}{P(d)} \tag{1}$$

Here, $P(C_j)$ and $P(C_i|d)$ are the prior and posterior probabilities of class C_i, while $P(d)$ and $P(d|C_i)$ are the prior and posterior probabilities of the predictor d. The dependent feature vector is $x = (x_1, x_2, \ldots, x_n)$ and Bayes' theorem gives us the following.

$$C_i = argmax\ P(x_1, x_2, x_3, x_4, \ldots, x_n \mid C)P(C_i) \tag{2}$$

$$C_i = \text{argmax} \prod_{i=1}^{n} P(x_n \mid C_i)P(C_i) \tag{3}$$

$$P(x_i) = \frac{Number\ of\ x_i\ in\ documents\ of\ class\ C}{Number\ of\ words\ in\ documents\ of\ class\ C} \tag{4}$$

Basing the probabilistic classifier on the naïve Bayes model simplifies the conditional independence assumptions for the CaaS and crimeware classes. The sentences in a document are tokenized into words, which are classified as relating to either CaaS or crimeware. The likelihood of the document having feature x_i can then be computed by dividing "the number of features x_i in documents of class C" by "the number of words in documents of class C" (Equation 4).

2) COMPANY NAME EXTRACTION

Named entity recognition is an information extraction technique that classifies named entities based on a predefined dictionary. We used the Open Calais API to recognize company and personal names. For example, Fig. 3 shows that "Apple" is recognized as referring to the company rather than the fruit. We use named entity recognition to identify the company names mentioned in the cybercrime underground, which we consider as potential targets (e.g., RAT suitable targets) [13], [14].

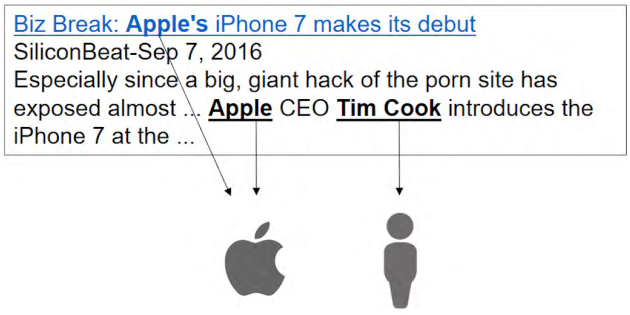


FIGURE 3. Named entity recognition.

D. STEP 4: IMPLEMENTING AN APPLICATION

Although organizations emphasize the measures they take to prevent cybercrime, their overall effectiveness has yet to be empirically demonstrated in practice. In the last step of our framework, we demonstrate the use of the proposed CaaS and crimeware definitions, classification model, and analysis framework. The resulting application implements all the data analysis methods explained in Section IV and aims to demonstrate how our proposed framework can deliver insights to end users.

V. DATA ANALYSIS AND RESULTS

The data analysis step of the proposed framework involves four steps. Here, we report the data analysis results: CaaS and crimeware classification and market trends, cybercrime market dynamics, and potential hacking targets.

A. CaaS AND CRIMEWARE CLASSIFICATION AND MARKET TRENDS

Here, we evaluate the accuracy of the proposed classifications. Specifically, we analyze the CaaS and crimeware trends between 2008 and October 2017 based on these classifications.

As Fig. 4 illustrates, the most common classes overall were botnets (17%) and exploits (17%). The most popular classes in 2017 were botnets (33%), VPN services (20%), exploits (13%), and brute force attack services (7%). In RAT terms, this indicates that attackers are interested in both attack strategy/mode (suitable targets) and preventive measures (capable guardians against crime).

To validate our classification model, we used a confusion matrix, a common method of calculating classifier output accuracy [55]. The training and testing datasets comprised 300 and 700 items, respectively. This gave an accuracy of 82.6% with a 95% confidence interval of (70.74%, 81.24%) for identifying the risks posed by CaaS- and crimeware-related messages. There were 92 true positives and 488 true negatives, so the precision, sensitivity, and specificity were 0.561, 0.638, and 0.871, respectively.

The CaaS and crimeware classification accuracy was 76.7%, with a 95% confidence interval of (75.32%, 72.28%). In addition, the precision and sensitivity were both 0.767, and the specificity was 0.971.

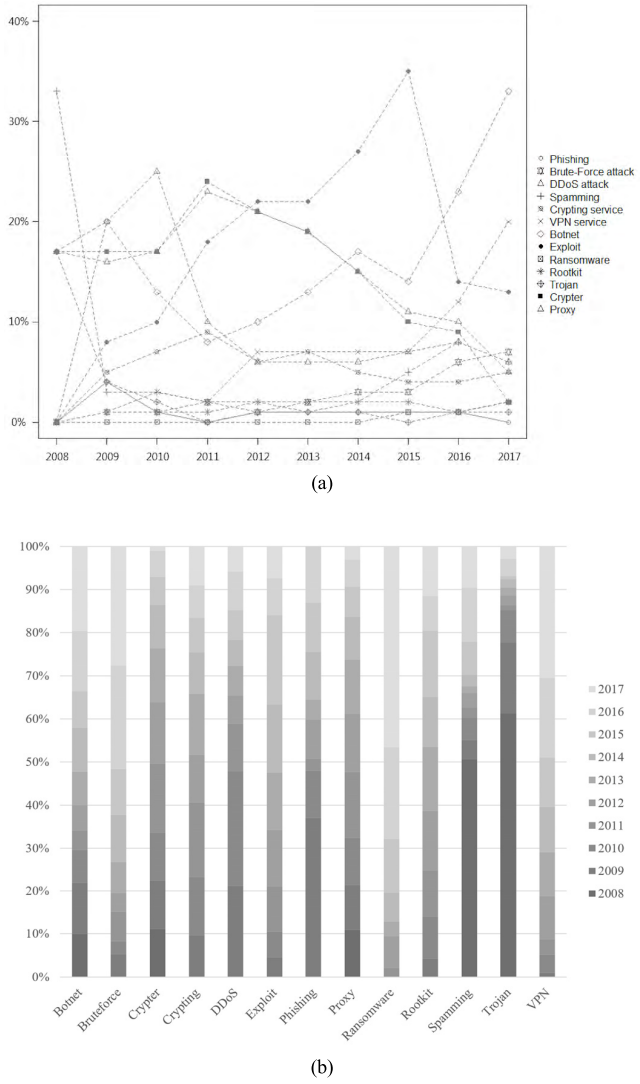


FIGURE 4. Dynamic trends of cybercrime underground market (2008-2017.10): (a) Comparison among categories. (b) Category self-comparison by year.

B. CYBERCRIME MARKET DYNAMICS

Marketplaces involve heterogeneous consumer demands that necessitate product differentiation, therefore social network analysis can be used to discover threats in hacker communities in the cybercrime underground context. In this regard, data visualization gives us new insights into the data and its structure by intuitively expressing relationships that cannot be seen directly from the data itself.

On the market supply side, Fig. 5 shows what the CaaS and crimeware sellers were attempting to sell. We considered four time spans, namely 2008–2010, 2011–2013, 2014–2017/10, and 2008–2017/10 to explore how the items for sale have evolved.

We created networks where the nodes represented sellers and illegal items. To focus on the types of criminal item, the seller information was masked. As Fig. 5 shows, DDoS attacks were the most common items between 2008–2010, but their prevalence has decreased over time because the range of items available has changed. Exploits have become more popular since 2011, and there have been corresponding increases for items related to preventing them, such as proxies and crypters. This can be interpreted as evidence that attackers are always aware of RAT's capable guardians against crime [13], [14].

C. POTENTIAL HACKING TARGETS: INDUSTRIES AND COMPANIES

In this section, we use cybercrime underground data to analyze the list of potential target organizations (see Section III-B); this is further demonstrated in Section V-A as a monitoring platform. These potential targets are related to RAT's suitable targets [13], [14].

Table 2 shows (in alphabetical order) the companies mentioned by the hacking community since 2008. According to the proposed framework (Fig. 1), the data context was the cybercrime underground, and named entity recognition (see Section IV-C(2)) was used to extract company names from the discussion. The companies' Standard Industrial Classification (SIC) codes were used to categorize them by industry. To confirm the company and industry names, we manually investigated all the companies' official websites.

Table 2 summarizes the results, which indicate that the technology (28%), content (22%), and finance (20%) industries were the ones most targeted by cyber threats. The technology industry includes many software, hardware, and automobile companies, while the majority of the companies in the content industry were related to social networking, Internet services, or news. The financial targets were made up of banks and online payment companies. Interestingly, 10% of the companies were telecommunications-related (e.g., smartphone makers and service providers). These results help us to better understand what attackers in the cybercrime underground are most interested in.

VI. EXAMPLE APPLICATIONS

This section demonstrates how our proposed framework can be implemented and customized for researchers and practitioners according to the DSR guidelines [6], [7]. Specifically, we present four example applications to evaluate the implementation process from a DSR perspective. We have developed an interactive Web platform for these applications, which can used by companies in a range of industries, such as finance, technology, services, manufacturing, and health, as well as by governments.

A. CYBERCRIME MARKET TREND MONITORING

This section describes how to monitor cybercrime market trends, based on the CaaS and crimeware classification model (see Section IV-C(1)) and the classification results (see Section V-A). The goal of this example application is to effectively monitor the cybercrime market by monitoring the number of times each CaaS and crimeware item is mentioned each day. Because CaaS and crimeware are related either to

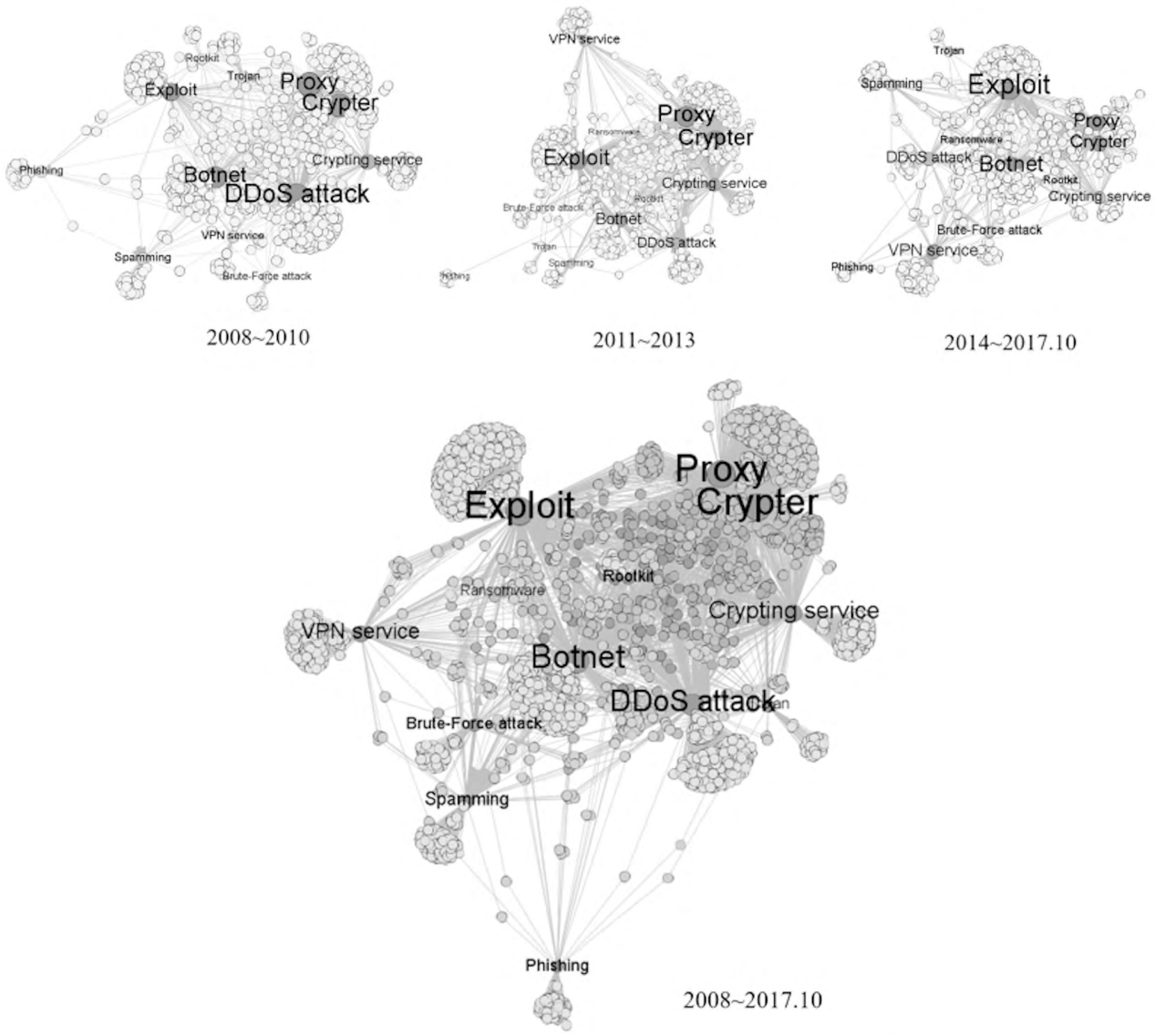


FIGURE 5. Dynamic networks between sellers and cybercriminal items.

attack strategy/mode or to preventive measures (see Table 1), this can be interpreted in terms of RAT's suitable targets (attack strategy/mode) and capable guardians against crime (preventive measures).

As Fig. 6 illustrates, the application allows users to search for CaaS and crimeware trends in the cybercrime underground data (see Section IV-B). The data used here were collected from the "Premium Sellers Section." This application can show the CaaS and crimeware trends since 2008. Analyzing the hacking tool trends may allow organizations to discover which ones they should focus on protecting themselves against.

These results can be intuitively understood, enhancing our understanding of how CaaS and crimeware change over time. First, bar graphs show which of the selected keywords were most used within the given period. Second, daily trend graphs show the frequencies with which particular CaaS and crimeware items are mentioned. These both serve to highlight the changes in cybercrime market trends over time. Although this application is based on the proposed classifications, it also allows new CaaS and crimeware items to be added that have not yet been classified. This scalability is an important part of DSR's search process and its emphasis on tentative study [49].

B. DETECTING POTENTIAL TARGETS (COMPANIES, PRODUCTS, AND SERVICES)

This section describes an application that relies on extracting company names (see Section IV-C(2)) and potential hacking targets (see Section V-C). The goal of this example application is to identify potential target companies, products, and services. The analysis in Fig. 7 is based on using the named

TABLE 2. Company names mentioned in cybercrime underground. Names are in alphabetical order.

Industry	Company	%
Technology (e.g., software, automobiles)	3M, Adobe, BMW, CISCO, EA, Exino Inc., GE, GlobalScape, HP, IDC Research Inc., Intel Corp., KDDI Japan, LG, Microsoft, Oracle, Panasonic, Panda Security, Philips, Samsung, Scania, Simba, Softbank Korea, Sony, Sybase, Sycore Business Solutions Corp., SynLan Technologies, Western Digital, Yamaha	28%
Content (e.g., social network services, Internet, news)	ABC, AOL, Baidu, Bang Bros, CBS, Craigslist, Facebook, Google, IMDB, Instagram, Justin.tv, Last.FM, LinkedIn, LiveJournal, MSN, NBC, SoundCloud, Twitter, Warner Bros, Yahoo, YouTube, Zynga	22%
Finance (e.g., banking, investing, and payments)	AlertPay, American Express, AMP, Personal Banking, Bank of America, Blackrock, Canadian Bank, Clickbank, Digital River, Goldman Sachs, iBank, Indian Bank, IP Capital, Kidd, Liberty Reserve, Moneybookers, PayPal, PlaySpan, Polish Bank, State Bank of India, Tradestation, Western Union	20%
E-commerce (e.g., products and services)	Amazon, Best Buy, Dope, eBay, GameStop, GoDaddy, Groupon, Netflix, Nike, Staples, Uber, Walmart	12%
Tele Comm. (e.g., smartphones and service providers)	Apple, AT&T, HTC, KT Freetel, MetroPCS, Nokia, Sprint, Swisscom, T-Mobile, Verizon Wireless	10%
Others	Airsoft Gun, Ajanta Pharmaceuticals, ARMA International, FedEx, Green Leaf Technology, UPS, USG Corp.	8%

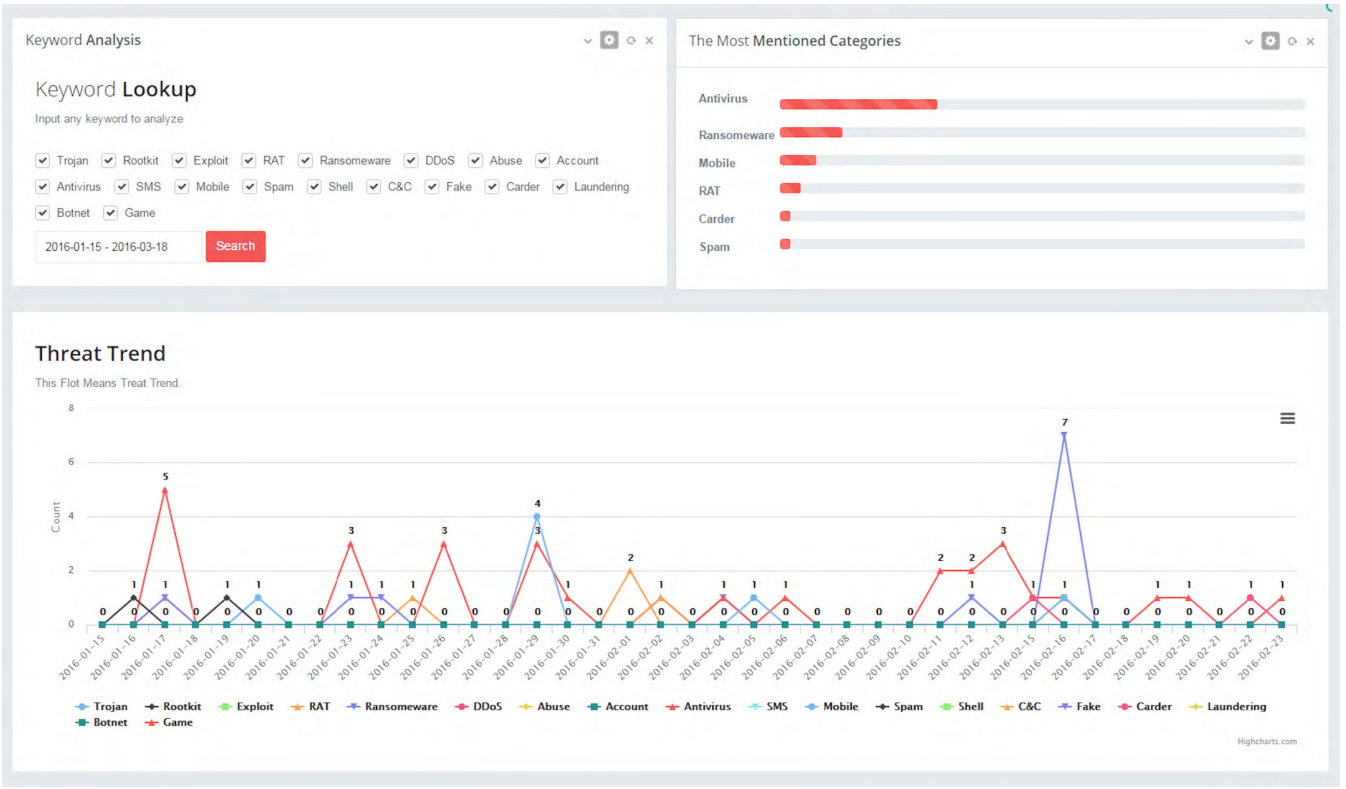
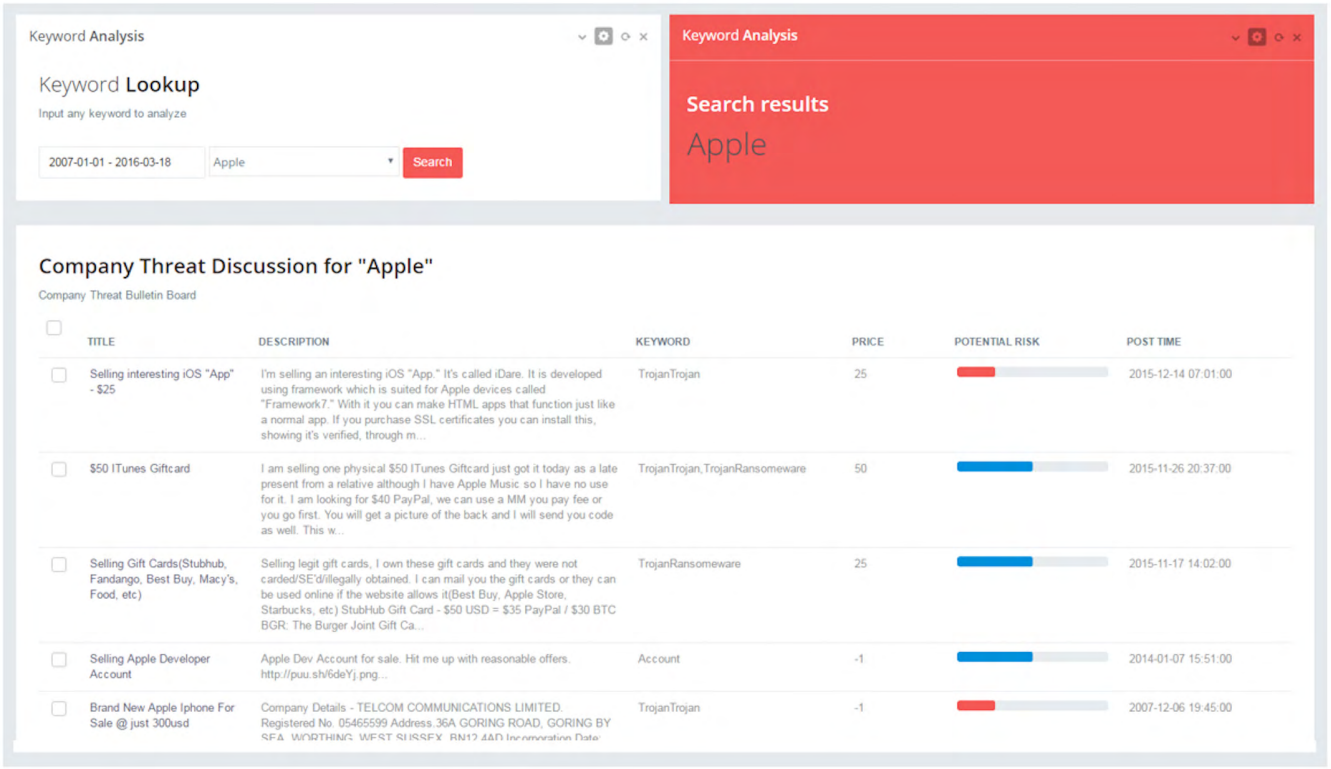


FIGURE 6. CaaS and crimeware trend monitoring system.

entity recognition algorithm to extract company names from both "Hacks, Exploits, and Various Discussions" and "Premium Sellers Section" in the cybercrime community forum. The companies' SIC codes are used to categorize them by industry.

By analyzing the attackers' conversations, the application can extract the names of the companies, products, and services that they mention and therefore their likely targets (see Fig. 7). This analysis of RAT's suitable targets [13], [14] allows security managers to



(a)

Car Hacking - Reaper598 - **07-05-2011 06:20 PM**

I just read that it is possible to hack cars. This totally makes sense. So, I wonder if anyone has ever done it. One guy says he hack his 2006 Impala with an Android phone and some code he made. Others plug machines into the cable underneath the dashboard. It's even possible to attach virus code to a mp3 and once in the CD player it will do its job.

Why would you do this you may ask. Well you could start cars, turn off security systems, turn off brakes, and many other things.

So I'm wondering if anyone has done this or knows how to do it. Especially with an Android.

* - DDoS ViRuS - **07-06-2011 06:14 PM**

This depends very much on the car itself. Old cars with very little electronics don't allow you do do much of anything. Newer cars you can do more with because electronics control more of the system. The Nissan Leaf allows you to connect to RSS feeds in your car but every time it sends a request it gives the website real-time about your car such as its location, driving history, power consumption, and battery reserves. That is just it sending out info. On most cars however information isn't broadcasted like this but you can still hack its electronic computer units. On most cars you need physical access to do this using the diagnostic port or whatever it is (usually under the dash on the drivers side) I actually have a device that reads real-time information from this and sends it to my phone. On newer cars this is sometimes becoming wireless instead of needing to have physical access to it. While this makes it easier to get the diagnostic information it makes it very easy for hackers to compromise. Here is an article on it http://www.infosecurity-us.com/view/12270/car-hacking-goes-wireless-as-modern-vehicles-open-to-hacke

(b)

Nissan Leaf electric cars hack vulnerability disclosed

By Leo Kelion
Technology desk editor

24 February 2016 | Technology

BBC

Some of Nissan's Leaf cars can be easily hacked, allowing their heating and air-conditioning systems to be hijacked, according to a prominent security researcher.

Troy Hunt reported that a flaw with the electric vehicle's companion app also meant data about drivers' recent journeys could be spied on.

Mr Hunt said he gave the firm a month to fix the issue before he decided to make it public.

Nissan said there was no safety threat.

The problem remains unresolved but Mr Hunt said car owners could protect themselves by disabling **their Nissan CarWings account**. Those who have never signed up are not at risk.

(c)

FIGURE 7. Hacking vulnerability disclosed and the earlier signal from the underground: (a) Monitoring system. (b) Relevant result (July 6, 2011). (c) BBC news (Feb. 24, 2016).

monitor the potential threats and hence prevent the proposed attacks.

Figs. 7(b) and (c) illustrate a real-world example. On February 24, 2016, BBC News reported that a ''Nissan Leaf electric cars hack vulnerability has been disclosed'' and explained that the vehicle's app could be spied on (see Fig. 7 (c)). Interestingly, this vulnerability had already been discussed in the underground community, on July 5, 2011 (4.5 years earlier). This shows that monitoring the activity of the underground community can enable vulnerabilities to be discovered before companies formally disclose them.

C. REAL-TIME SOCIAL MEDIA MONITORING

Cyberattacks are unpredictable and damaging, but those who have not taken precautions against such attacks suffer the most. The most effective way to reduce the damage is to respond in real time. This section therefore focuses on

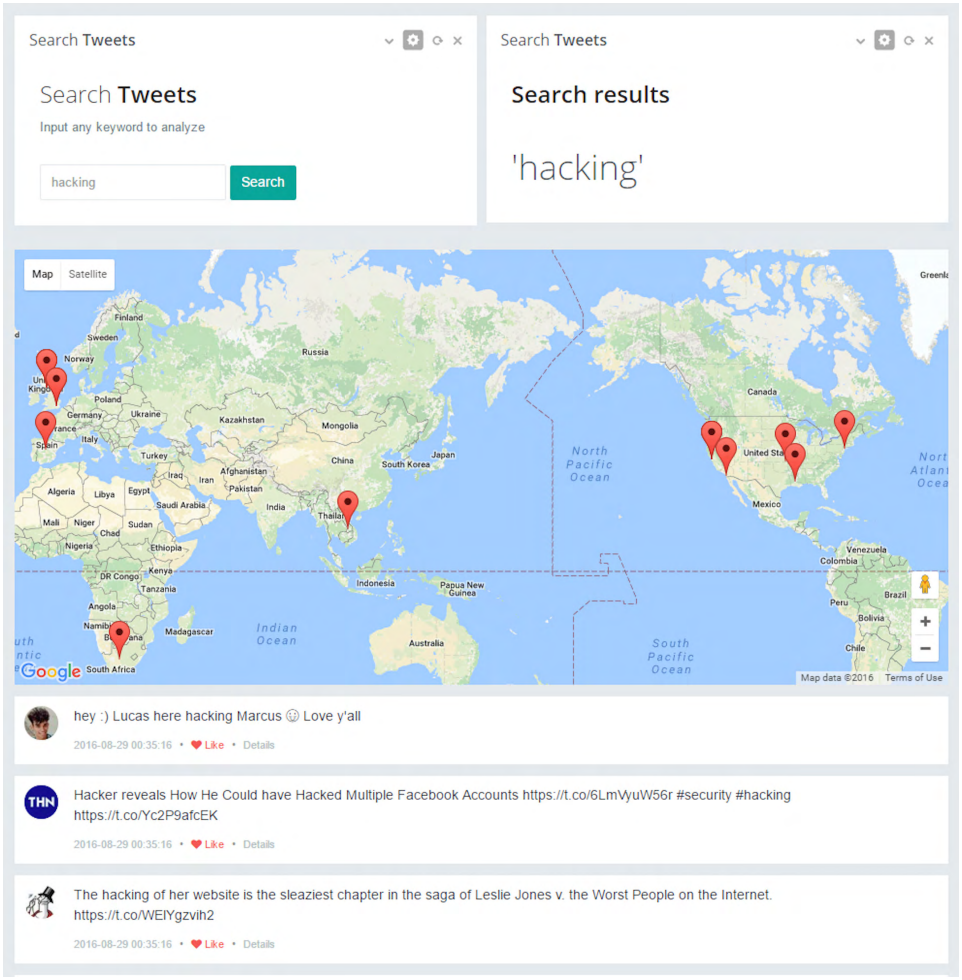


FIGURE 8. Twitter monitoring system.

a real-time monitoring application that aims to monitor cybercrime-related discussions on social networks. Unlike Sections VI-A and VI-B, this application may reflect different RAT views, depending on who is tweeting, such as an attacker (motivated offender) or anti-virus vendor (guardian against crime), and on what topic (e.g., suitable targets or preventive measures).

Fig. 8 shows that the ''hacking'' keyword was mentioned in a range of different places. The application presents real-time global search results visually, allowing users to identify the new trends and meaningful discussions contained in Twitter messages. It can locate the authors of tweets containing specific keywords immediately. The application thus yields insights into the original languages, locations, and hashtags associated with given keywords. In most cybercrime cases, it is critically important that organizations take immediate action, so this monitoring helps organizations to react immediately to the use of specific keywords.

D. CYBERCRIMINAL NETWORK MONITORING

Now, we apply the methods discussed in Section V-B to analyze the relationships between potential buyers and sellers in the underground market. This application aims to identify the potential buyers and sellers of CaaS and crimeware, using data collected from the forums at www.hackforums.net. In this case, we visualize the data using a network whose nodes represent potential buyers and sellers and whose edges represent forum threads and replies. This allows us to assess their relationships in terms of the degrees of connectivity and centrality, based on the numbers of edges connected to particular nodes (see Fig. 9). This enables the application to identify the most influential users as well as any patterns in the network.

This feature is also a potentially useful tool for monitoring behavior associated with money laundering. Because money laundering involves more than one transaction, it is of vital importance to monitor and detect patterns of interaction among community members. It also enables end users to keep an eye on the most influential players in the market. By defining particular attributes based on activity-related information, additional analyses, such as impact, clustering, and homophily analyses, can be used to monitor noteworthy attackers and profile criminals.

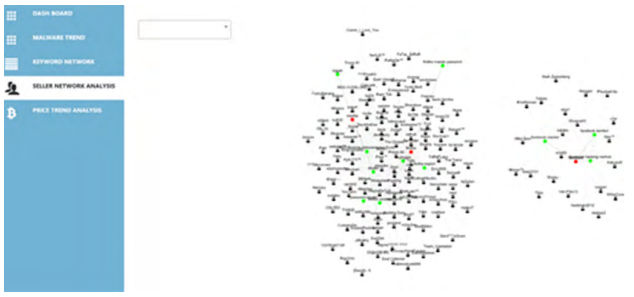


FIGURE 9. Buyers and sellers network analysis.

VII. DISCUSSION AND IMPLICATIONS

A. DISCUSSION

Because this study takes a DSR approach, we have focused mainly on building and evaluating artifacts rather than on developing and justifying theory: actions are usually considered to be the main focus of behavioral science [7]. We have therefore proposed two artifacts: a data analysis framework and a classification model. We have also conducted an ex-ante evaluation of our classification model's accuracy and an ex-post evaluation of its implementation using example applications. In line with the initiation perspective of DSR [6], [7], these four example applications demonstrate the range of potential practical applications available to future researchers and practitioners.

Unlike previous studies [12], [56], [57] that have presented general discussions of a broad range of cybercrime, our study has focused primarily on CaaS and crimeware from an RAT perspective. We have also proposed sets of definitions for different types of CaaS (phishing, brute force attack, DDoS attack, spamming, crypting, and VPN services) and crimeware (drive-by download, botnets, exploits, ransomware, rootkits, Trojans, crypters, and proxies) based on definitions taken from both the academic and business practice literature. Based on these, we have built an RAT-based classification model [13], [14]. This study emphasizes the importance of RAT for investigating the cybercrime underground, so these RAT-based definitions are critically important parts of our framework.

In addition, unlike prior research that discussed the cybercrime underground economy without attempting to analyze the data [3], we have analyzed large-scale datasets obtained from the underground community.

Looking at the CaaS and crimeware trends, our results show that the prevalence of botnets (attack-related crimeware) and VPNs (preventive measures, related to CaaS) has increased in 2017. This indicates that attackers consider both the preventive measures taken by organizations and their vulnerabilities. The most common potential target organizations are technology companies (28%), followed by content (22%), finance (20%), e-commerce (12%), and telecommunication (10%) companies. This indicates that a wide variety of companies in a range of industries are becoming potential targets for attackers, having become more vulnerable due to their greater reliance on technology.

B. LIMITATIONS AND FUTURE RESEARCH

Although our study has made several significant findings, it nevertheless has several limitations that will need to be addressed in future studies. These will be able to add more analysis and significant further insights.

First, we only collected data from the largest hacking community and did not consider other hacking communities. Future studies will therefore need to generalize our findings by investigating a wider range of hacking communities.

Second, this study has focused on the CaaS and crimeware available in the cybercrime underground, but much in-depth analysis remains to be done on the configurations of cybercrime networks. Future research could cluster keywords and threats by industry to provide a deeper understanding of the potential vulnerabilities, and it could attempt to discover the network effects involved or the leaders of the cybercrime underground.

C. IMPLICATIONS FOR RESEARCH

This study contributes to the DSR literature in a broader IS context in several ways. Because it takes a DSR approach, it contributes to the design artifacts, foundations, and methodologies in this area [6]–[8]. First, by creating example front-end applications, we have demonstrated how our design artifacts (the proposed framework and classification model) can be implemented in practice. Despite the rapidly growing threat from cybercrime, there has been little research into practical frameworks for future cybersecurity researchers: the previous studies have not attempted to analyze the data or take a systematic modeling approach [3], [58]–[62]. In DSR, we must demonstrate that the artifacts can be implemented in a business environment for them to qualify as solving an important unsolved problem [7]. We have therefore provided an implementable framework, not just a conceptual one.

Second, this study adds to the emerging cybersecurity literature by providing a foundation on which to build [7]. We have investigated the cybercrime underground economy using our proposed analytical framework. Despite the importance of data analysis, scholars have had little guidance as to how to analyze and integrate data from different contexts. We have shown (see Section IV and Fig. 1) that large-scale datasets can be analyzed using a range of techniques within a single analytical framework.

A previous study [63] examined how data-driven document classification can help decision-making by improving data quality and model performance in IS. Our proposed framework, which can be used to effectively and systematically classify CaaS and crimeware, therefore provides opportunities for further research. This study also extends the prior research by proposing well-developed analytical strategies that can help in building empirical models.

In addition, there is currently a lack of good CaaS and crimeware definitions and classification models. This has limited progress in IS because researchers have had to rely on a broad range of potentially inadequate definitions borrowed from the business practice literature. Thus, our proposed

definitions and classification model will serve as a basis for further research.

Third, this study adds to the body of knowledge by demonstrating new approaches to the problems cybercrime and social media researchers face [7], [73]. Despite the increasing importance of data analysis, researchers have been slow to recognize the advantages of new and more powerful data-driven analysis methods. We have applied several modern techniques, such as machine learning, key phrase extraction, and natural language processing, in this area, thereby encouraging future research to be more systematic and empirical. In addition, our results suggest that combining natural language processing and machine learning approaches is a suitable way to study closed communities whose members frequently use jargon or obscure expert language.

Finally, this study adds to RAT [13], [14] by applying it to the cybercrime underground. The same three factors can be applied to cybercrime and general crimes, so we have classified CaaS and crimeware in the context of the cybercrime underground and analyzed them accordingly.

D. IMPLICATIONS FOR PRACTICE

From a RAT perspective, the practical implications of this study mainly affect the capable guardians against crime, because our results indicate how underground attackers perceive preventive measures. A previous review of the current status of legal, organizational, and technological efforts to combat cybercrime in different countries relied on a case study of the work being done in Taiwan [64]. It made four recommendations for governments, lawmakers, international organizations, intelligence and law enforcement agencies, and researchers: (1) regularly update existing laws; (2) enhance specialized task forces; (3) use civil resources; and (4) promote cybercrime research. The practical implications of our study are based on those of the previous study [64]. We have already discussed the fourth recommendation (''promote cybercrime research'') in the previous section, so we will now focus on the other three areas.

First, our study has implications for governments and lawmakers in that it recommends existing laws be regularly updated. The proposed CaaS and crimeware definitions and classification model may improve national defense and security by suggesting potential government roles and the adoption of particular regulatory policies. A previous study [65] suggested that governments and lawmakers should encourage security providers, such as anti-software vendors, to collaborate and share security-related information. For example, governments and companies could develop joint plans to stop the spread of cybercrime by tracking cyber threats [64]. Our study therefore suggests governments should actively encourage companies to invest in their cybersecurity infrastructures.

Second, the proposed data analysis framework can be used to enhance specialized task forces. This study suggests that organizations in all industries should attempt to gain a deeper understanding of the nature of the cybercrime underground. For example, they should be aware that there are cybercrime underground markets where hacking tools are sold. More importantly, these tools could be based on vulnerabilities in their organizations, products, and services. Governments and organizations therefore need to increase their technical capabilities when it comes to analyzing large-scale datasets of different types [66], [67]. Although the proposed framework and classification model are of particular use to companies mentioned specifically by the cybercrime underground, the framework can also be used to analyze more general types of issues commonly encountered in practice [68]. In this regard, legal and technical training is needed to reduce the impact of cyberattacks [64].

Third, this study calls for researchers, companies, anti-virus vendors, and governments to collaborate in the fight against cybercrime using civil resources. Rather than acting alone, these groups should unite to maximize their efficiency and effectiveness. Successful collaboration may enable stronger and better-coordinated responses to immediate cyber threats in risky environments [69]. For example, by sharing information, technology, and support, stronger defense systems can be built for everyone. Our study enables this by providing a framework, definitions, classification model, and applications that can be implemented by researchers, governments, organizations, and anti-virus vendors.

Finally, this study also has important implications for society. Over the last few years, the world has been facing cyberterrorism and cyberwar threats from nation-sponsored attackers [70]. Pollitt [71] defined cyberterrorism as ''the premeditated, politically motivated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by sub-national groups or clandestine agents.'' Unlike most cybercrime, which is primarily motivated by monetary gain [72], cyberterrorists are politically motivated. As a result, governments should, for example, strengthen their ability to protect their citizens in online virtual environments by enhancing their immediate responses to threats such as cyberespionage and cyberterrorism. This issue therefore has profound implications in terms of the need for a global cyber defense to maintain a cyber-safe environment.

REFERENCES

[1] J. C. Wong and O. Solon. (May 12, 2017). *Massive Ransomware Cyber-Attack Hits Nearly 100 Countries Around the World*. [Online]. Available: https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs
[2] *FACT SHEET: Cybersecurity National Action Plan*, The White House, Washington, DC, USA, 2016.
[3] A. K. Sood and R. J. Enbody, ''Crimeware-as-a-service—A survey of commoditized crimeware in the underground market,'' *Int. J. Crit. Infrastruct. Protect.*, vol. 6, no. 1, pp. 28–38, 2013.
[4] S. W. Brenner, ''Organized cybercrime-how cyberspace may affect the structure of criminal relationships,'' *North Carolina J. Law, Technol.*, vol. 4, no. 1, pp. 1–50, 2002.
[5] K. Hughes, ''Entering the World-Wide Web,'' *ACM SIGWEB Newslett.*, vol. 3, no. 1, pp. 4–8, 1994.
[6] S. Gregor and A. R. Hevner, ''Positioning and presenting design science research for maximum impact,'' *MIS Quart.*, vol. 37, no. 2, pp. 337–356, 2013.

[7] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quart.*, vol. 28, no. 4, pp. 75–105, 2004.
[8] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *J. Manag. Inf. Syst.*, vol. 24, no. 3, pp. 45–77, 2007.
[9] S. Gregor, "Design theory in information systems," *Austral. J. Inf. Syst.*, vol. 10, no. 1, pp. 14–22, 2002.
[10] S. Gregor and D. Jones, "The anatomy of a design theory," *J. Assoc. Inf. Syst.*, vol. 8, no. 5, pp. 313–335, 2007.
[11] M. Yar, "The novelty of 'Cybercrime': An assessment in light of routine activity theory," *Eur. J. Criminol.*, vol. 2, no. 4, pp. 407–427, 2005.
[12] K.-K. R. Choo, "Organised crime groups in cyberspace: A typology," *Trends Organized Crime*, vol. 11, no. 3, pp. 270–295, 2008.
[13] L. E. Cohen and M. Felson, "Social change and crime rate trends: A routine activity approach," *Amer. Sociol. Rev.*, vol. 44, no. 4, pp. 588–608, 1979.
[14] M. Felson, "Routine activities and crime prevention in the developing metropolis," *Criminology*, vol. 25, no. 4, pp. 911–932, 1987.
[15] F. Mouton, M. M. Malan, K. K. Kimppa, and H. S. Venter, "Necessity for ethics in social engineering research," *Comput. Secur.*, vol. 55, pp. 114–127, Nov. 2015.
[16] A. S. Rakitianskaia, M. S. Olivier, and A. K. Cooper, "Nature and forensic investigation of crime in second life," in *Proc. 10th Annu. Inf. Secur. South Africa Conf.*, 2011. [Online]. Available: http://dblp.uni-trier.de/rec/bibtex/conf/issa/RakitianskaiaOC11
[17] A. van der Merwe, M. Loock, and M. Dabrowski, "Characteristics and responsibilities involved in a phishing attack," in *Proc. 4th Int. Symp. Inf. Commun. Technol.*, 2005, pp. 249–254.
[18] L. Volonino, R. Anzaldua, and J. Godwin, *Computer Forensics: Principles and Practices*. Englewood Cliffs, NJ, USA: Prentice-Hall, 2006.
[19] G. Álvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalyzing a discrete-time chaos synchronization secure communication system," *Chaos, Solitons Fractals*, vol. 21, no. 3, pp. 689–694, 2004.
[20] M. Goncharov. (2014). *Russian Underground Revisited*. [Online]. Available: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf
[21] V. Bezmalyi. (Oct. 1, 2014). *Why Phishing Works and How to Avoid It*. [Online]. Available: https://blog.kaspersky.com/how-to-avoid-phishing/6145/
[22] C. Ng. (May 21, 2014). *What's the Difference Between Hacking and Phishing?* [Online]. Available: https://blog.varonis.com/whats-difference-hacking-phishing/
[23] P. Shankdhar. (May 29, 2017). *Popular Tools for Brute-force Attacks*. [Online]. Available: http://resources.infosecinstitute.com/popular-tools-for-brute-force-attacks
[24] J. Mirkovic, G. Prier, and P. Reiher, "Source-end DDoS Defense," in *Proc. 2nd IEEE Int. Symp. Netw. Comput. Appl. (NCA)*, Apr. 2003, pp. 171–178.
[25] A. Singh and D. Juneja, "Agent based preventive measure for UDP flood attack in DDoS attacks," *Int. J. Eng. Sci. Technol.*, vol. 2, no. 8, pp. 3405–3411, 2010.
[26] D. McMillen. (Mar. 24, 2016). *Why Botnets Remain the Go-To Weapon for Cybercriminals*. [Online]. Available: https://securityintelligence.com/why-botnets-remain-the-go-to-weapon-for-cybercriminals/
[27] P. Cunningham, N. Nowlan, S. J. Delany, and M. Haahr, "A case-based approach to spam filtering that can track concept drift," in *Proc. Workshop Long-Lived CBR Syst. (ICCBR)*, 2003, pp. 2003-1–2003-3.
[28] Z. Gyöngyi and H. Garcia-Molina, "Web spam taxonomy," in *Proc. 1st Int. Workshop Adversarial Inf. Retr. Web (AIRWeb)*, 2005, pp. 1–9.
[29] A. Zaharia. (Nov. 14, 2015). *Analysis: How Malware Creators Use Spam to Maximize Their Impact*. [Online]. Available: https://heimdalsecurity.com/blog/analysis-how-malware-creators-use-spam-to-maximize-their-impact/
[30] V. G. Tasiopoulos and S. K. Katsikas, "Bypassing antivirus detection with encryption," in *Proc. 18th Panhellenic Conf. Informat. (PCI)*, New York, NY, USA, 2014, pp. 1–2.
[31] R. Venkateswaran, "Virtual private networks," *IEEE Potentials*, vol. 20, no. 1, pp. 11–15, Feb. 2001.
[32] A. K. Sood, S. Zeadally, and R. Bansal, "Cybercrime at a scale: A practical study of deployments of HTTP-based botnet command and control panels," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 22–28, Jul. 2017.
[33] J. Glassberg, (Apr. 7, 2016). *What You Need to Know About, 'Drive-By' Cyber Attacks*. [Online]. Available: http://www.foxbusiness.com/features/what-you-need-to-know-about-drive-by-cyber-attacks
[34] P. Wang, S. Sparks, and C. C. Zou, "An advanced hybrid peer-to-peer botnet," *IEEE Trans. Depend. Sec. Comput.*, vol. 7, no. 2, pp. 113–127, Apr. 2010.
[35] H. R. Zeidanloo and A. B. A. Manaf, "Botnet detection by monitoring similar communication patterns," *Int. J. Comput. Sci. Inf. Secur.*, vol. 7, no. 3, pp. 36–45, 2010.
[36] H. R. Shahriari and R. Jalili, "Vulnerability take grant (VTG): An efficient approach to analyze network vulnerabilities," *Comput. Secur.*, vol. 26, no. 5, pp. 349–360, 2007.
[37] C. G. Amaya. (Oct. 2014). *Myths About Malware: An Exploit is the Same as Malware*. [Online]. Available: http://www.welivesecurity.com/2014/10/21/myths-about-malware-exploit-is-the-same-as-malware/
[38] A. Gazet, "Comparative analysis of various ransomware virii," *J. Comput. Virol.*, vol. 6, no. 1, pp. 77–90, 2010.
[39] G. O'Gorman and G. McDonald, "Ransomware: A growing menace," Symantec Corp., Mountain View, CA, USA, Tech. Rep., 2012. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf
[40] A. Khanse. (Dec. 18, 2013). *How to Protect Against and Prevent Ransomware Attacks & Infections*. [Online]. Available: http://www.thewindowsclub.com/prevent-ransomware-windows
[41] D. Turkel. (Dec. 16, 2015). *There Are Now Programs That Anyone Can Use to Extort Money From You*. [Online]. Available: http://www.businessinsider.com/ransomware-as-a-service-is-the-next-big-cyber-crime-2015-12/
[42] Y. Zhu, S. L. Liu, H. Lu, and W. Tang, "Research on the detection technique of bootkit," in *Proc. Int. Conf. Graph. Image Process.*, 2013, p. 876860.
[43] J. Luo, M. Li, A. Khashnobish, J. McDermott, and J. Froscher, *A Taxonomy of Software Deceptive Interpretation in the Linux Operating System*, document NRL/MR/5540–04-8841, DTIC, 2004.
[44] M. Kassner. (Sep. 17, 2008). *10+ Things You Should Know About Rootkits*. [Online]. Available: http://www.techrepublic.com/blog/10-things/10-plus-things-you-should-know-about-rootkits/
[45] M. Tehranipoor and C. Wang, *Introduction to Hardware Security and Trust*. New York, NY, USA: Springer, 2011.
[46] L. J. Janczewski and A. M. Colarik, *Cyber Warfare and Cyber Terrorism*. Hershey, PA, USA: IGI Global, 2007.
[47] J. Ortiz. (Nov. 30, 2015). *The CryptoLocker Legacy—Another Reason for Strong Data Protection*. [Online]. Available: https://storageswiss.com/2015/11/30/the-cryptolocker-legacy/
[48] J. Waldo, "The Jini architecture for network-centric computing," *Commun. ACM*, vol. 42, no. 7, pp. 76–82, 1999.
[49] R. Baskerville, A. Ga, J. Pries-heje, and J. Venable, "Soft design science methodology," in *Proc. 4th Int. Conf. Design Sci. Res. Inf. Syst. Technol.*, 2009, p. 9.
[50] H. Chen, W. Chung, J. J. Xu, G. Wang, Y. Qin, and M. Chau, "Crime data mining: A general framework and some examples," *Computer*, vol. 37, no. 4, pp. 50–56, Apr. 2004.
[51] J. R. Landis and G. G. Koch, "The measurement of observer agreement for categorical data," *Biometrics*, vol. 33, no. 1, pp. 159–174, 1977.
[52] P. Langley and S. Sage, "Induction of selective Bayesian classifiers," in *Proc. 10th Int. Conf. Uncertain. Artif. Intell.*, 1994, pp. 399–406.
[53] P. Langley, W. Iba, and K. Thompson, "An analysis of Bayesian classifiers," *Aaai*, vol. 90, pp. 223–228, Jul. 1992.
[54] J. Chen, H. Huang, S. Tian, and Y. Qu, "Feature selection for text classification with Naïve Bayes," *Expert Syst. Appl.*, vol. 36, no. 3, pp. 5432–5435, 2009.
[55] T. Fawcett, "An introduction to ROC analysis," *Pattern Recognit. Lett.*, vol. 27, no. 8, pp. 861–874, Jun. 2006.
[56] Y. Ben-Itzhak, "Organised cybercrime and payment cards," *Card Technol. Today*, vol. 21, no. 2, pp. 10–11, 2009.
[57] L. Tabansky, "Cybercrime: A national security issue?" *Military Strategic Affairs*, vol. 4, no. 3, pp. 117–136, 2012.
[58] W. Kim, O.-R. Jeong, C. Kim, and J. So, "The dark side of the Internet: Attacks, costs and responses," *Inf. Syst.*, vol. 36, no. 3, pp. 675–705, 2011.
[59] S. Gordon and R. Ford, "On the definition and classification of cybercrime," *J. Comput. Virol.*, vol. 2, no. 1, pp. 13–20, 2006.
[60] S. Philippsohn, "Trends in cybercrime—An overview of current financial crimes on the Internet," *Comput. Secur.*, vol. 20, no. 1, pp. 53–69, 2001.
[61] M. S. Gerber, "Predicting crime using Twitter and kernel density estimation," *Decision Support Syst.*, vol. 61, pp. 115–125, May 2014.
[62] S. B. Hoar, "Trends in cybercrime: The dark side of the Internet," *Criminal Justice*, vol. 20, pp. 4–13, 2005.

[63] D. Martens and F. Provost, "Explaining data-driven document classifications," *MIS Quart.*, vol. 38, no. 1, pp. 73–99, 2014.
[64] W. Chung, H. Chen, W. Chang, and S. Chou, "Fighting cybercrime: A review and the Taiwan experience," *Decision Support Syst.*, vol. 41, no. 3, pp. 669–682, 2006.
[65] S. H. Kim and B. C. Kim, "Differential effects of prior experience on the malware resolution process," *MIS Quart.*, vol. 38, no. 3, pp. 655–678, 2014.
[66] K. S. Wilson and M. A. Kiy, "Some fundamental cybersecurity concepts," *IEEE Access*, vol. 2, pp. 116–124, 2014.
[67] A. Sajid, H. Abbas, and K. Saleem, "Cloud-assisted IoT-based SCADA Syst. Security: A review of the state of the art and future challenges," *IEEE Access*, vol. 4, pp. 1375–1384, 2016.
[68] Z. Shi, G. M. Lee, and A. B. Whinston, "Toward a better measure of business proximity: Topic modeling for industry intelligence," *MIS Quart.*, vol. 40, no. 4, pp. 1035–1056, 2016.
[69] A. Majchrzak and S. L. Jarvenpaa, "Safe contexts for interorganizational collaborations among homeland security professionals," *J. Manag. Inf. Syst.*, vol. 27, no. 2, pp. 55–86, 2010.
[70] G. Giacomello, "Close to the edge: Cyberterrorism today," in *Understanding Terrorism*. Bingley, U.K: Emerald Group, 2014, pp. 217–236.
[71] M. M. Pollitt, "Cyberterrorism—Fact or Fancy?" *Comput. Fraud Secur.*, vol. 1998, no. 2, pp. 8–10, 1998. [Online]. Available: https://doi.org/10.1016/S1361-3723(00)87009-8
[72] I. P. L. Png, C.-Y. Wang, and Q.-H. Wang, "The deterrent and displacement effects of information security enforcement: International evidence," *J. Manag. Inf. Syst.*, vol. 25, no. 2, pp. 125–144, 2008.
[73] H. W. Kim, H. C. Chan, and S. Gupta, "Social media for business and society," *Asia–Pacific J. Inf. Syst.*, vol. 25, no. 2, pp. 211–233, 2015.

JUNGKOOK AN is currently pursuing the Ph.D. degree with the Graduate School of Information, Yonsei University, Seoul, South Korea. His research interests include big data analytics, cybersecurity, natural language processing, business intelligence, social media marketing, and brand engagement.

HEE-WOONG KIM was a Faculty Member with the Department of Information Systems and Analytics, National University of Singapore. He is currently a Professor with the Graduate School of Information, Yonsei University, Seoul, South Korea. He has served on the Editorial Boards for the *Journal of the Association for Information Systems* and the IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT.