RESEARCH ARTICLE OPEN ACCESS

The Cyber Crime Under Ground Economy Data Approach

Mr.V.TataRao [1], Mr.B.S.Venkata Reddy [2]

Dept. of CSE

Raghu Engineering College(Autonomous)

Andhra Pradesh -India

ABSTRACT

Despite the rapid escalation of cyber threats, there has yet been little inquiry into the fundaments of the study or methodologies that could do 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 look into the cybercrime underground economy by choosing a data analytics approach from a design science perspective. To accomplish this end, we propose (1) a data anaalysis framework for analyzing the cybercrime underground, (2) CaaS and crimeware definitions, and (3) an associated classification model. In summation, we (4) develop an example application to show how the proposed framework and classification model could be enforced in practice. We then utilize this application to investigate the cybercrime underground economy by examining a large dataset obtained from the online hacking community. By submitting a design science research approach, this work leads to the design artifacts, institutions, and methodologies in this field. Moreover, it offers useful practical insights to practitioners by suggesting guidelines as to how governments and governing bodies in all industries can prepare for attacks by the cybercrime underground.

Keywords:- Crimeware-as-a-Service, crimeware, underground economy, hacking community, machine learning.

I. INTRODUCTION

As the menace presented by massive cyberattacks (e.g., ransomware and distributed denial of service attacks (DDoS)) and cybercrimes have grown, individuals, governing bodies, and governments have scrambled to determine ways to fight back against them. In 2017, ransomware known as Wanna Cry was responsible for about 45,000 attacks in almost 100 countries [1]. The explosive impact of cybercrime has put command under anxiety to increase their supersecret budgets.

Global cyberattacks (such as Wanna Cry and Petya) are performed by highly organized criminal groups, and organized or national level crime groups have been behind many recent attempts. In general, criminal groups buy and sell hacking tools and services on the cybercrime black market, wherein attackers share a range of hacking-related data.

The cybercrime underground has thus issued as a novel type of organization that both operates black markets and enables cybercrime conspiracies to flourish.

Because well thought-out cybercrime requires an online network to exist and to conduct its attacks, it is highly dependent on closed antiestablishment 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, resolute, rigid, and fixed. In disparity, cybercrime networks are lateral, diffuse, fluid, and evolving. Since internet is a web of networks [5], the threat presented by the wage increase of highly professional network-based cybercrime business models, such as Crimeware-as-a-Service (CaaS), remains mostly invisible to governments, governing bodies, and people.

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

Former surveys have not studied the antiestablishment 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 sympathy, both in research and practice, of the nature of this underground and the mechanisms underlying it.

This research gap, and the matter-of-fact problems faced by cybercriminals, motivate our study. We need a data analytics approach and look into the cybercrime economy from a design science perspective. To accomplish this goal, we (1) propose a data psychotherapy framework for analyzing the cybercrime antiestablishment to guide researchers and connoisseur; (2) define CaaS and crimeware to better reflect their features from both academic research and business practice perspective; (3) use this to build a cataloging model for CaaS and crimeware; and (4) build an application to demonstrate how the proposed framework and classification model may perhaps be implemented in practice. We then assess this application by giving it in a case study, namely investigating the cybercrime economy by examining a large dataset from the online hacking community.

This study takes a propose 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 build up and justify theories that explain or predict human or organizational phenomena, DSR seeks to expand the limits of human and organizational capabilities by producing fresh and innovative artifacts [6] –[8]. DSR's contribution is to add value to the journalism and practice in terms of "design artifacts, design, fabricate knowledge (e.g., foundations), and/or design evaluation knowledge (e.g., methodologies)," [7].

This work follows these, DSR guidelines and contributes design artifacts, institutions, and methodologies [7]. In particular, DSR must demonstrate that design artifacts are "implementable" in the business environment to work out an important problem [7], so we provide an implementable framework rather than a conceptual one. We also make a front-end application as a case example to show how the proposed framework and classification model could be enforced in practice.

As for practicalities, DSR should have a creative development of constructs, model, methods, or instigations that extend the design science knowledge base [7]. This study, therefore adds to the knowledge base by providing initial 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 utilization of valuation methods provide DSR offerings [7]. Consequently, this study uses dynamic analysis to conduct an ex-ante evaluation of the cataloging model. It also takes an ex-post evaluation of a front-end application using observational methods (case examples). From a practical perspective, this work also provides practitioners with useful insights by making propositions to run governments and governing bodies in all industries in resolving the troubles they face when training 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 slanting because the fact it operate in the fundamental world, with different spatial and temporal constraints, differentiates it from other crime taking place in the physical world [11].

The cybercrime underground has a highly professional business model that holds its own underground economy [5]. This commercial enterprise model, known as CaaS, is "a business model utilized in the underground market where illegal services are supplied to help underground buyers conduct cyber crimes, such as attacks, infections, and money laundering in an automated fashion," [3].

Because CaaS is designed for novice, its regulars do not need to run a hacking server or have high-level hack skills. Therefore, the CaaS business model can involve the following roles:writing a hacking program, performing an attack, commission an attack, providing an attack server (infrastructure), and rinse 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 criminals, routine activity theory (RAT) is applied to explain the causes of crime, both genusl criminal activity and cybercrime [13], [14]. According to this theory, three elements are necessary for crimes to be unswerving: (1) a likely offender, (2) a suitable target, and (3) the absence of capable guardians against crime.

The "absence of capable guardians against crime" is due to organizations failing to adopt prophylactic measures against cybercrime.

Two types of product or service are existing in the cybercrime antiestablishment. The first can be either CaaS or somewhere that relate to attack strategy, for example, phishing, brute violence, or DDoS attacks, or can be utilized for spamming or creating potents, exploit, ransoming, rootkits, or Trojans. Attack strategy often exploit system vulnerabilities such as application loophole. In increase, social engineering attacks exploit human vulnerabilities [15]. Still, because social engineering is one of the oldest account hacking techniques, most account holders are directly cognizant of it. In increase, social engineering-related merchandise and services are rarely traded underground, although a few vendors have been known to sell tutorials. As a termination, we experience not included "social engineering services" as a CaaS type.

The second type of product or service available countercheck organizations' preventive measures, such as antivirus programs. These are based on programs designed to evade antivirus software to either cause mischief or be left behind for later activation. Examples include encryption and virtual private network (VPN) services, crypters, and placeholders. From the position of the RAT, the likely offenders are attackers motivated to attack organizations or products that constitute a worthy mark. If such targets are attacked, however, both the targets and those who supply their cybersecurity products become aware of the accountableness 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.

Nevertheless, this is not the conclusion of the issue, because the attackers will then produce and sell new versions of their hacking tools to battle the guardians, thus re-setting up the third RAT condition, the absence of capable guardians against crime. This round will go on as long as attackers can detect 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.

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]	Bezmalyi [21]
		• Brute Force attack*	Volonino et al. [18] Alvarez et al. [19]	Ng [22] 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]

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

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.

Crimeware-as-a-Service

- Initiated as a case of theft specific to digital environments where users make personal digital profiles and store valuable personal data 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 to a target's account by obtain account information (e.g., username and password) or extra security information (e.g., security questions and answers).

Phishing Services: Phishing has been determined in the business practice literature in the final few years because it has become increasingly sophisticated and is one of the most common techniques applied by cybercriminals. Phishing is defined as "masquerading as a dependable source in an attempt to entice a user to surrender sensitive in sequence such as a username, password, and credit card number," [22]. leonine et al. [18] defined phishing as "sending an e-mail to a user falsely claiming to be a unlawful enterprise in an attempt to scam the user." The term "phishing" is a valise 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 specified in a assortment of ways in the literature. The intellectual literature defines spam as "unsolicited and unwanted e mail from a stranger that is sent in bulk to large mail lists, usually with some money-making objective," [27]. Likewise, Gyongyi and Garcia-Molina[28]defined seaming as "any deliberate human action that is meant to trigger an unjustifiably favorable relevance or importance of some web page making an allowance for 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.*

- Scripting Services: Crypter encrypt programs or source code to avoid catching and tracking and thus bypass anti-virus software [30]. Like other hacking services, encryption is sold as a service because crofters require a certain level of skill to use. The goal of such a service is to counterbalance the preventive measures put in place by organization and anti-virus software, prevent 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 community of authorized users [31]. The most dependable way to access the Internet is using a VPN, because it hides all user data (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 character 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 squeeze money from them.

- Rootkit: The business practice literature defines a rootkit as "a course of study that permits individual to obtain root-level access to the computer," [44]. We therefore define a rootkit as a bit of malicious software that enables administrator-level access to an in commission system or computer network.

- Trojan: Trojans are defined by clack and jounciest [46] as malicious programs that perform a legitimate function but also engage in unknown and/or unwanted activity. We therefore define a Trojan as a bit 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 main types of cyberattack worldwide. Such attacks target victims through their Internet browsers, installing malware their computers as soon as they see an infected web site [33]. We therefore define a drive-by download attack as an attack that installs malware when the victim visits a malicious web page.

- Scripture: Crypters can encrypt programmed or source code to avoid catching and tracking by depart from anti-virus software [30], and can likewise be provided as a service. We therefore define a scripture as a bit of encryption software that helps an intruder to bypass security programs.

- Proxy: Proxies are used for a assortment of uses, such as accelerating data transmission and filtering traffic [20]. We therefore determine a proxy as a host that enables anonymous Web browsing.

IV.ANALYTICAL FRAMEWORK AND METHODS

The constructs used in DSR are entity representations [10] that provide the glossary and symbols required 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.

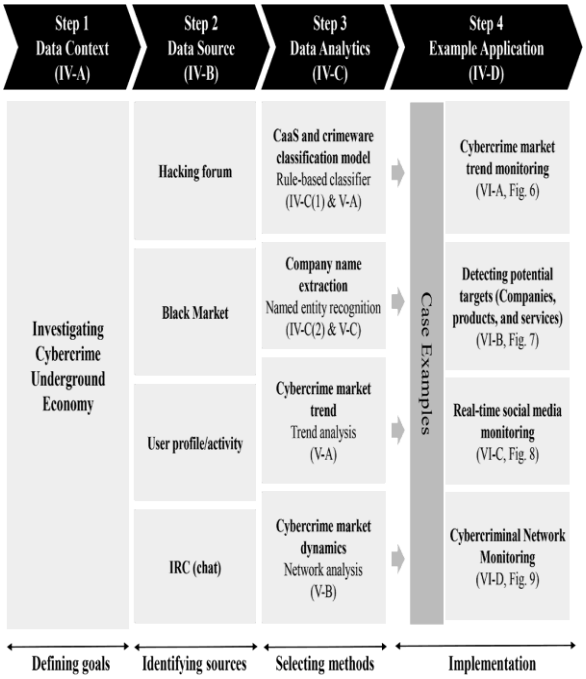


FIGURE 1. Proposed data analytical framework. Sections are in parentheses.

Because cybercrime differs from general crime in many ways, we need to take a variety of analyses utilizing a big data set.

Although the previous study explained how data mining techniques could be applied to crime analysis, it did not look at the specific features of cyber crime.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 contains four steps: (1) defining goals; (2) identifying sources; (3) selecting analytical methods; and (4) implementing an application.

Because this work underscores the consequence of RAT for

analyzing the cybercrime antiestablishment, the proposed RAT- based definitions are vital to this framework: Steps 1–4 all contain the RAT elements, as Fig. 1 shows.

A. Step 1: Defining Goals

The foremost stride is to distinguish the conceptual scope of the psychoanalysis. Specifically, this step identifies the analysis context, namely the objectives and destinations.

Step 2: Identifying Sources

The second stride is to identify the information authors, grounded on the goals defined by Step 1. Since the goal of this work is to give the impression of being into the cybercrime underground, we consider data on the cybercrime underground community. We therefore collected such data from the community itself and received a malware database from a leading global cybersecurity research firm.

Because cybercimimals often change their IP addresses and use anti-crawling scripts to hold in their communications, we employed a self-developed crawler that can resolve captchas and anti-crawling scripts to collect the necessary information. We picked up 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 places.

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 convert 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 topographies errors and jargon terms, we had to create a dictionary for use during a prepossessing step. In summation, we received a malware database from a cybersecurity firm containing over 53,815 entries covering cyber crimes between May 11, 2010 and January 13, 2014.

B. Step 3: Selecting Analytical Methods

1) CaaS AND CRIMEWARE CLASSIFICATION MODEL

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

To find out if a given message is serious, our cataloging model checks whether it flows 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.

To be classed as a dangerous Threat, for example, a message must also contain Market-linked keywords. Messages containing both Threat and Market interrelated keywords are well thought-out 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 given after the messages have been filtered as above, so many keywords are not demanded and the standards are simpler. However, when a message fits into multiple pigeonhole, this overlap is recorded so as to derive additional sageness from the later analysis and applications.

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").

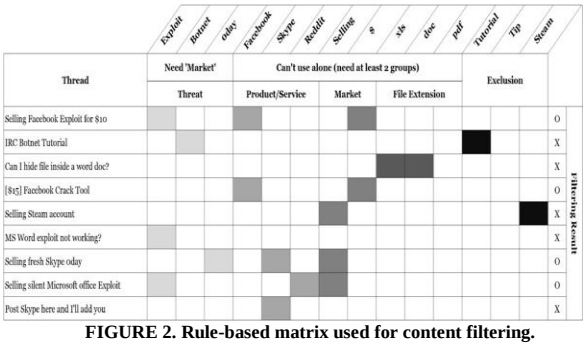


FIGURE 2. Rule-based matrix used for content filtering.

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

P(Ci|d) □ P(d | Cj)P(Cj) P(d) .(1)

$$C_i = argmax\, P(x_1, x_2, x_3, x_4, \dots, x_n |\, C)\, P(C_i)\ (2)$$

$$C \square \arg\max \prod P(x \ |C\ )P(C\ )\ (3)$$

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

As Fig. 4 illustrates, the most common curriculum 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 pin down 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

Basing the more cabalistic classifier on the naïve Bayes model simplifies the conditional independence as sumptions for the CaaS and crimeware classes. The judgment of convictions in a document are tokenized into words, which are classified as pertaining to either CaaS or crimeware.

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 know companies and personal names. For example, see Fig. 3 indicates that "Apple" is recognized as bringing up to the society rather than the yield. We use named entity recognition to identify the company names noted in the cybercrime underground, which we regard as likely objects (e.g., RAT suitable targets) [13], [14].

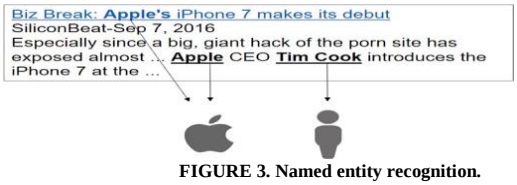


FIGURE 3. Named entity recognition.

C. Step 4: Implementing an Application

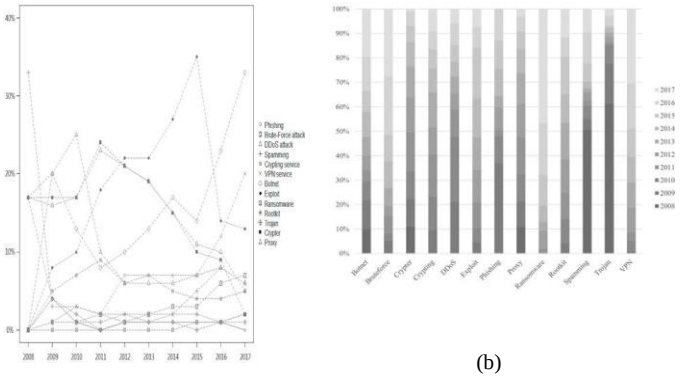
Although organizations emphasize the steps they need to prevent cybercrime, their overall effectiveness has yet to be empirically established in practice.In the last step of our framework, we demonstrate the use of the proposed CaaS and crimeware definitions, classification model, and analysis framework. The resulting application implements all the data analysis methods explained in Section IV and aims to prove 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 scrutiny 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.



(a) (b)

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.

B. Cybercrime Market Dynamics

Market places involve assorted consumer demands that impose product discrimination, therefore social network analysis can be used to discover threats in hacker neck of the woods in the cybercrime underground context. In this regard, data visualization gives us fresh insights into the data and its structure by without needing to ask expressing relationships that cannot be unwavering directly from the information itself.

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

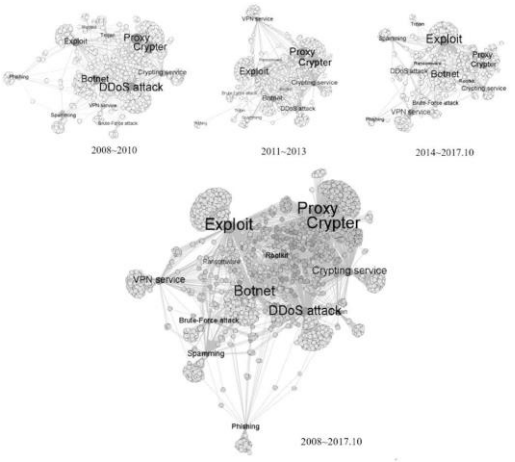


FIGURE 5. Dynamic networks between sellers and cybercriminal items.

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 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).

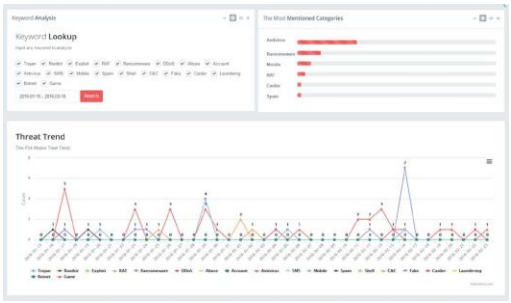


FIGURE 6. CaaS and crimeware trend monitoring system.

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 since2008. Analyzing the hacking tool trends may allow organizations to discover which ones they should focus on protecting themselves against.

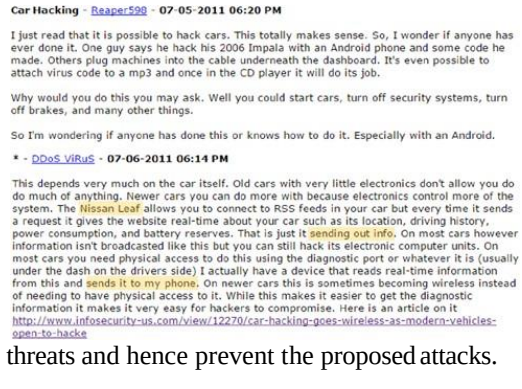
These results can be intuitively understood, enhancing our understanding of how CaaS and crimeware change over time. First, bar graphs show which of the selected keywords were most used within the given period. Second, daily trend graphs show the frequencies with which particular CaaS and

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 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 monitor the potential threats and hence prevent the proposed attacks.


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


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.

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 MediaMonitoring

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 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).

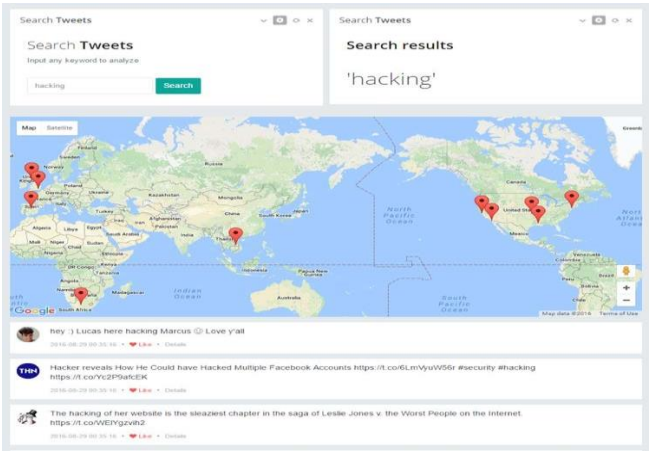


FIGURE 8. Twitter monitoring system.

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 NetworkMonitoring

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.

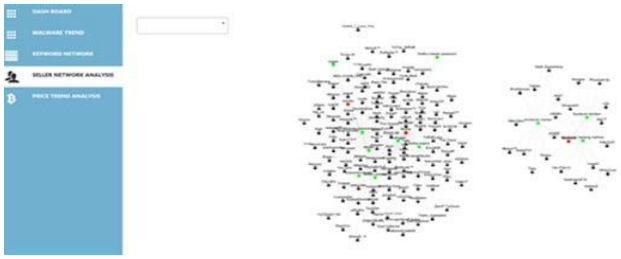


FIGURE 9. Buyers and sellers network analysis

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.

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.

B. Implications for Research

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 itto 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.

C. 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 subnational 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. (2017, May 12). *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," ed: The White House, 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. Infr. Prot.*, vol. 6, no. 1, pp. 28–38, 2013.

[4] S. W. Brenner, "Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships," *N. C. J. Law & Technol.*, vol. 4, no. 1, pp. 1-50, 2002.

[5] K. Hughes, "Entering the world-wide web," *ACM SIGWEB Newsl.*, 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," *Aust. J. Inf. Syst.*, vol. 10, no. 1, pp. 14–22, 2002.

[10] S. Gregor and D. Jones, "The Anatomy of a Design Theory," *J. the 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 in 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," *Am. Sociol. Rev.*, vol. 44, pp. 588–608, 1979.

[14] M. Felson, "Routine Activities and Crime Prevention in the Developing Metropolis," *Criminol.*, 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. Security*, vol. 55, 114–127, 2015.
[16] A. S. Rakitianskaia, M. S. Olivier, and A. K. Cooper, "Nature and Forensic Investigation of Crime in Second Life," in *10th Annual Inf. Security South Afr. Conf.*, 2011.
[17] A. van der Merwe, M. Loock, and M. Dabrowski, "Characteristics and Responsibilities Involved in a Phishing Attack," in *Proc., 4th Int. Symp. on information and communication technologies*, 2005, pp. 249–254: Trinity College Dublin.
[18] L. Volonino, R. Anzaldua, and J. Godwin, *Computer Forensics: Principles and Practices*. Prentice-Hall, Inc., 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. (2014, Oct. 1). *Why Phishing Works and How to Avoid It*. [Online]. Available: https://blog.kaspersky.com/how-to-avoid-phishing/6145/
[22] C. Ng. (2014, May 21). *What's the Difference between Hacking and Phishing?* [Online]. Available: https://blog.varonis.com/whats- difference-hacking-phishing/
[23] P. Shankdhar. (2017, May 29). *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 *Second IEEE Int. Symp. on Network Computing and Applications, 2003. NCA 2003.*, 2003, pp. 171–178: IEEE Comput. Soc.
[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. (2016, Mar. 24). *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," *Workshop on Long-Lived CBR Systems (ICCBR'03),* 2003.
[28] Z. Gyongyi and H. Garcia-Molina, "Web Spam Taxonomy," in *First Int. Workshop on Adversarial Information Retrieval on the Web (AIRWeb 2005)*, 2005.
[29] A. Zaharia. (2015, Nov. 14). *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. on Informatics - PCI '14*, New York, New York, USA, 2014, pp. 1–2: ACM Press.
[31] R. Venkateswaran, "Virtual private networks," *IEEE Potentials*, vol. 20, no. 1, pp. 11–15, 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. 2017.
[33] Glassberg, J. (2016, Apr. 7). *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. Dependable and Secure Comput.*, vol. 7, no. 2, pp. 113–127, 2010.
[35] H. R. Zeidanloo and A. B. A. Manaf, "Botnet Detection by Monitoring Similar Communication Patterns," *International J. Computer Science and Inf. Security*, 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. (2014, Oct.). *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 Corporation, 2012.
[40] A. Khanse. (2013, Dec. 18). *How to Protect Against and Prevent Ransomware Attacks & Infections*. [Online]. Available: http://www.thewindowsclub.com/prevent-ransomware-windows
[41] D. Turkel. (2015, Dec. 16. *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 *2012 Int. Conf. Graph. Image Proc.*, 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," 2004: DTIC Document.

[44] M. Kassner. (2008, Sep. 17). *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*. Springer Science & Business Media, 2011.

[46] L. J. Janczewski and A. M. Colarik, *Cyber Warfare and Cyber Terrorism* (Information Science Reference). Hershey, New York: IGI Global, 2007.

[47] J. Ortiz. (2015, Nov. 30). *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. on design science research in information systems and technology*, 2009.

[50] H. Chen, W. Chung, J. J. Xu, G. Wang, Y. Qin, and M. Chau, "Crime Data Mining: A General Framework and Some Examples," *Comput.*, vol. 37, no. 4, pp. 50–56, 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 *Proceedings of the Tenth international conference on Uncertainty in artificial intelligence*, ed: Morgan Kaufmann Publishers Inc., 1994, pp. 399–406.

[53] P. Langley, W. Iba, and K. Thompson, "An Analysis of Bayesian Classifiers," *Aaai*, vol. 90, pp. 223–228, 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 Recogn. Lett.*, vol. 27, no. 8, pp. 861–874, 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 Strateg. Aff.*, 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

AUTHORS DETAILS

Mr. B. S. Venkata Reddy working as Assistant Professor in the Department of Computer Science and Engineering, Raghu Engineering College(Autonomous),Visakhapatnam, Andhrapradesh. His research interest is on Data Science, Big Data and Business Analytics, Cyber security, Social Media Marketing. He is pursuing part time Ph.D from AMET, Cheinnai. In connection with NGOs, Startups , Training Institutions, Colleges ,etc., he has certified various Technical Courses and Trained more than 10,000 students from 1998 to till date . He has membership in various organizations. He has a zeal to work for the development of the community with various innovative, creative and unique activities and Programs. His basic motto is to serve the nation through the people of the community.

Mr. V.TataRao working as Assistant Professor(Ratified Faculty by JNTUK) in the Department of Computer Science and Engineering, Raghu Engineering College (Autonomous), Visakhapatnam, Andhrapradesh. His research interest on Network security and Cyber security. He has obtained his B.Tech(CSE) from JNTUH, M.Tech(CSE) from JNTUK.