International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

An Effective Data Analytics Approach to Cybercrime Underground Economy Using Ml Methodologies

Dr. A. Swarupa Rani & G.Manasa
1.Associate Professor, Dept. of MCA, SIETK, Puttur, A.P.
2. PG Scholar, Dept. of MCA, SIETK, Puttur, A.P.

Abstract: *Despite the rapid escalation of digital threats, there has still been little research into the foundations of the subject or methodologies that could serve to manage Information Systems researchers and practitioners who deal with cyber security. In addition, little is referred to about Crime-as-a-Service (CaaS), a criminal plan of action that supports the cybercrime underground. This research gap and the practical cybercrime issues we face have motivated us to investigate the cybercrime underground economy by taking a data analytics approach from a design science point of view. To achieve this goal, we propose (1) a data analysis framework for analyzing the cybercrime underground, (2) CaaS and crime ware definitions, and (1) an associated classification demonstrate. In addition, we (1) build up an example application to demonstrate how the proposed framework and classification model could be actualized in practice. We at that point utilize this application to investigate the cybercrime underground economy by analyzing a large dataset obtained from the internet hacking community. By taking a design science research approach, this examination adds to the design of artifacts, foundations, and methodologies in this area. Additionally, it gives helpful practical bits of knowledge to practitioners by proposing rules as to how governments and organizations in all businesses can prepare for attacks by the cybercrime underground.*

Key-Words— Crimeware-as-a-Service, Crimeware, Underground Economy, Hacking Community, Machine Learning, Design Science-research

I.INTRODUCTION

THE Cybercrime, or computer-oriented crime, is the crime that involves a computer and a network.[1]The computer may have been used in the commission of a crime, or it may be the target.Cybercrimes can be defined as:

"Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms,

emails, notice boards and groups) and mobile-phones (Bluetooth/SMS/MMS)" Cybercrime may threaten a person or a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, Particularly those surrounding hacking, copyright infringement, unwarranted mass-surveillance, sextortion, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise. Debarati Halder and K. Jaishankar further define cybercrime from the perspective of gender and defined 'cybercrime against women' as "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones". Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Cybercrimes crossing international borders and involving the actions of at least one nation state is sometimes referred to as cyberwarfare.

Despite the fact that Information Systems (IS) researchers and practitioners are taking an increasing enthusiasm for cybercrime, because of the critical issues arising from the rapid increase in digital threats, few have attempted to put this new enthusiasm on a strong foundation or create suitable methodologies.Past investigations have not analyzed the underground economy behind cybercrime top to bottom. Besides, little is thought about CaaS, one of the primary plans of action 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 fundamental it.

This research gap and the practical issues faced by cybercriminals motivate our investigation. We take a data analytics approach and investigate the cybercrime economy from a design science point of view. To achieve this goal, we (1) propose a data analysis framework for analyzing the cybercrime underground to manage researchers and practitioners; (2) characterize CaaS and crimeware to more readily mirror their features from both academic research and business practice points of view; (1) utilize this to manufacture a classification show for CaaS and crimeware; and (1) assemble an application to demonstrate how the proposed framework and classification model could be actualized in practice. We at that point evaluate this application by applying it in a case think about, namely

investigating the cybercrime economy by analyzing a large dataset from the web-based hacking community.

This investigation takes design science research (DSR) approach. Design science "creates and evaluates information innovation artifacts planned to tackle recognized problems". DSR includes building up a range of IT artifacts, for example, choice emotionally supportive networks, models, frameworks, devices, strategies, and applications. Where behavioral science research tries to create and legitimize hypotheses that explain or anticipate human or organizational phenomena, DSR looks to expand the boundaries of human and organizational capabilities by creating new and innovative artifacts. DSR's commitment is to add value to the literature and practice as far as "design artifacts, design development information (e.g., foundations), and/or design evaluation learning (e.g., methodologies),".

This examination pursues these DSR rules and contributes design artifacts, foundations, and methodologies. In particular, DSR must demonstrate that design artifacts are "implementable" in the business condition to take care of an important issue, so we give 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 actualized in practice. In addition, this examination adds to the design hypothesis.

As for foundations, DSR should have a creative improvement of builds, models, techniques, or instantiations that broaden the design science learning base. This examination, accordingly, adds to the learning base by giving foundational components, for example, builds (definitions, frameworks, and applications), a model (classification display), a strategy (analysis), and instantiations (applications).

As for methodologies, the creative advancement and utilization of evaluation strategies give DSR commitments. Accordingly, this investigation utilizes a dynamic analysis to lead an ex-ante evaluation of the classification to demonstrate. It also directs an ex-post evaluation of a front-end application utilizing observational strategies (case examples). From a practical viewpoint, this investigation also furnishes practitioners with valuable bits of knowledge by making recommendations to direct governments and organizations in all ventures in taking care of the issues they

face while preparing for attacks from the Cybercrime underground.

II. Related Work

Think of the cybercriminal underground as a global marketplace full of anonymous buyers and sellers. It's composed of several smaller markets unique to each region. Currently, the most prominent are those in Russia, China, and Latin America.

CONCEPTUAL BACKGROUND

A. Cybercrime Underground Business Model

These virtual black markets mostly thrive in forums or chat rooms where numerous cybercriminals act as anonymous businessmen who trade goods and services to make profit. And much like typical businessmen, these cybercriminals adhere to specific business models:

- Commercial model: It's the most straightforward approach. Cybercriminals hawk goods like stolen user credentials, malware, exploits, and the like, and sell them to anyone who's interested.
- Organized crime model: This set-up involves several individuals or groups who work together to achieve certain targets. Each person in the chain serves their own unique function integral to the whole team's operations.
- Outsourcing model: This business model requires cybercriminals to partner with outside computer owners, whose network of machines they can rent as botnets for malicious schemes.
- Mentor-apprentice model: Those interested to advance their know-how in hacking creating malicious applications can hire more skilled cybercriminals to pass on what they know.

Whatever model cybercriminals choose to follow, one thing's for sure, if you're using the Internet, you, including your personal information and money, are prone to their schemes. Whether you're checking email, playing games, or connecting with friends on social media, cybercriminals are continuing to develop wares designed to piggyback on each of your activities. As long as cybercriminals have something to profit from, the cybercriminal underground is always open for business

B. Routine Activity Theory

Routine activity theory is a sub-field of crime opportunity theory that focuses on situations of crimes. It was first proposed by Marcus Felson and Lawrence E. Cohen in their explanation of crime rate change in

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

the United States 1947 - 1974.The theory has been extensively applied and has become one of the most cited theories in criminology. Unlike criminological theories of criminality, routine activity theory studies crime as an event, closely relates crime to its environment and emphasize its ecological process,there by diverting academic attention away from mere offenders.

The premise of routine activity theory is that crime is relatively unaffected by social causes such as poverty, inequality, and unemployment. For instance, after World War II, the economy of Western countries started to booming and the Welfare states were expanding. Despite this, crime rose significantly during this time. According to Felson and Cohen, the reason for the increase is that the prosperity of contemporary society offers more opportunities for crime to occur. For example, the use of automobile, on one hand, enables offenders to move more freely to conduct their violations and, on the other hand, provide more targets for theft. Other social changes such as college enrollment, female labor participation, urbanization, suburbanization, and lifestyles all contribute to the supply of opportunities and, subsequently, the occurrence of crime.

Fig 1: Physical convergence in time and space

Routine activity theory has its foundation in human ecology and rational choice theory. Over time, the theory has been extensively employed to study sexual crimes, robberies, cyber crimes, residential burglary and corresponding victimizations, among others. It is also worth noting that, in the study of criminal victimization, the routine activity theory are often regarded as "essentially similar" to lifestyle theory of criminology by Hinderlang, Gottfredson, and Garofalo (1978). More recently, routine activities theory has been repeatedly used in multilevel frameworks with social disorganization theory in understanding various neighborhood crimes.

2.2 CLASSIFICATION AND DEFINITION OF CRIMEWARE PRODUCTS SERVICES

Although the two academics and practitioners have as of late started to give more attention to CaaS, its fast-developing nature has kept them from reaching agreement on the best way to characterize distinctive sorts of CaaS and crimeware.

Subsequently, a large portion of the academic research has acquired the definitions utilized by the business practice literature, leading to generally varying interpretations in various orders. Given this ambiguity, we approach categorizing CaaS and crimeware from a RAT point of view (thinking about vulnerabilities as suitable targets and preventive measures as capable guardians against wrongdoing) in a cybercrime underground setting. In addition, we reclassify CaaS and crimeware based on the definitions utilized in existing research and practice.

A. Classification of Crimeware Services and Products

The meanings of CaaS and crimeware utilized in the academic and business practices literature, which shape a basis for our classification display, suitable for the IS field. We reclassify CaaS and crimeware as far as the suitable targets (attack strategy/mode) and the absence of capable guardians (preventive measures) in a cybercrime underground setting.

The diverse attack strategies/modes in Table 1 are associated with RAT's suitable targets because vulnerable organizatins, items, and services may experience the ill effects of attacks utilizing a variety of strategies. In contrast, preventive measures are associated with RAT's absence of capable guardians because encryption and VPN services, crypters, and intermediaries are planned to neutralize preventive measures by bypassing anti-infection and log checking software.

B. Meaning of Crimeware Services and Products

We presently need to survey the definitions utilized in both the research and business practice literature.

This examination expands the IS literature by facilitating a conceptual understanding of the CaaS plans of action utilized by the cybercrime underground. Drawing upon earlier research and business practice literature, we propose meanings of CaaS and crimeware that better mirror the features of CaaS in both of these areas.

1) Crimeware-as-a-Service

The Crimeware-as-a-Service (CaaS) model gives cybercriminals a way to automate their unauthorized and often illegal activities on the Internet. And they can earn a significant amount of money very quickly using CaaS. Recently, Cloud Threat Labs (CTL), now part of Symantec Corporation discovered that hackers are using Google Drive to host Facebook Phishing and Account hijacking tools.

Multiple versions of these tools were found on Google Drive.

Analysis**:** Generally, online scamming and phishing tools are used broadly to harvest credentials from target entities. In this case study, we will take a look into the "Facebook Hacking" tool, including multiple variants that are used by unauthorized actors to steal end-user credentials for nefarious purposes. In reality, this is not a real hacking tool that exploits vulnerabilities in Facebook, rather it's an online scamming tool that is sold as a service under the CaaS model exploiting novice individuals attempting to hack another person's Facebook account.

2) Crimeware Products

Crimeware is a set of programs or any computer program that has been designed to facilitate illegal activity online. Many spyware programs, keyloggers, and browser hijackers can be considered crimeware, although only those used illicitly. The phishing kit is one common type of crimeware that is a collection of tools assembled to make it easier for people with minimal technical skills to launch a phishing exploit. Typically, a phishing kit includes website development software, complete with graphics, coding, and content that can be used to produce convincing imitations of authorized sites, and spamming software to automate the mass mailing process. Phishing kits and several other types of crimeware are readily available on the Internet. **Harmful Effects Caused by Crimeware**

You will have to be worried about crimeware because of the following harmful effects:

- Identity Theft
- Intrusion of Privacy
- Annoying Pop-ups
- Private Data Theft
- Loss of productivity because of
- operating system errors, system slowdowns, etc.
- Saturation with unwanted advertising: pop-up windows, spam, etc.
- Financial losses because of the theft of passwords for accessing online services.
- Legal problems via the usage of the compromised computer by third parties for illicit activities.

III.PROPOSAL METHODOLOGY

We at that point utilize this application to investigate the cybercrime underground economy by analyzing a large dataset obtained from the internet hacking community. By taking a design science research approach, this examination adds to the design of artifacts, foundations, and methodologies in this area. it gives helpful

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

practical bits of knowledge to practitioners by proposing rules as to how governments and organizations inall businesses can prepare for attacks by the cybercrime underground.

ANALYTICAL FRAMEWORK AND METHODS

The builds utilized in DSR are element representations that give the vocabulary and images expected to characterize issues and arrangements. Accordingly, the design components utilized in this investigation are the cybercrime underground, criminal things (CaaS and crimeware), classifications, and front-end framework applications, and the artifacts are based on these builds. These artifacts are evaluated in two stage: ex-ante (classification evaluation) and ex-post (case example). Because DSR ought to be tentative, this ex-present evaluation is essential on the search procedure utilized by iterative DSR, which involves search, design, ex-ante evaluation, development, artifact, ex-post evaluation, and research . Based on this, we propose the data analysis framework appeared Fig.1.

Sections are in parentheses.

Because cybercrime varies from general wrongdoing from numerous points of view, we have to direct a variety of analyses utilizing a large dataset. A past report proposed a data digging framework for wrongdoing, separating violations harmful to the general open into eight categories: traffic violations, sex wrongdoing, burglary, fraud, arson, gang/sedate offenses, vicious wrongdoing, and cybercrime.

Although the past investigation explained how data mining methods could be applied to wrongdoing analysis, it didn't think about the particular features of cybercrime. Besides, it just explained the data mining methods quickly, rather than displaying a broad review of the framework .

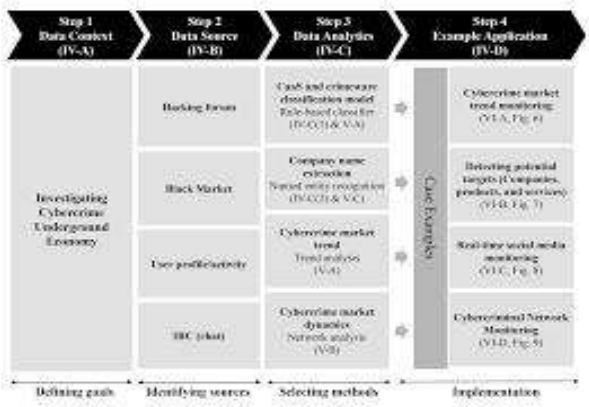

Figure2.Proposed data analytical framework.

In contrast, the goal of our data analysis framework is to lead a major picture investigation of the cybercrime underground by covering all phases of data analysis from the earliest starting point as far as possible (see Fig. 1). This framework includes four stages: (1) characterizing goals;(2) distinguishing sources; (3) choosing analytical strategies;

and (4) actualizing an application. Because this investigation emphasizes the importance of RAT for analyzing the cybercrime underground, the proposed RAT-based definitions are critical to this framework: Steps 1– 1 all contain the RAT components, as Fig. 1 appears.

A: Defining Goals

The initial step is to distinguish the conceptual extent of the analysis. Specifically, this progression recognizes the analysis setting, namely the targets and goals. To gain a top to bottom understanding of the momentum CaaS research, we investigated the cybercrime underground, which operates as a shut community. In this way, the goal of the proposed framework is to "investigate the cybercrime underground economy."

B: Identifying Sources

The second step is to recognize the data sources, based on the goals characterized by Step 1. This progression ought to think about what data is required and where it very well may be obtained. Since the goal of this examination is to investigate the cybercrime underground, we think about data on the cybercrime underground community. We, consequently, gathered such data from the community itself and obtained a malware database from a leading global cyber security research firm.

Because cybercriminals regularly change their IP addresses and utilize anti-crawling contents to conceal their communications, we utilized a self-created -crawling contents to gather the necessary data. We gathered a total of 2,172,091 posts moving CaaS or crimeware, made between August 2008 and October 2017, from a large hacking community site (www.hackforums.net) with more than 178,000 individuals and in excess of 10 million posts. We also gathered 16,172 client profiles of merchants and potential purchasers, based on their communication narratives, as well as costs and questions and answers about the transactions.

The black market utilizes traditional discussion threads (e.g., release boards) instead of typically web-based business platforms (e.g., eBay, and Amazon). Since these writings included many typographic mistakes and jargon terms, we had to create a dictionary for use amid a preprocessing step. In addition, we obtained a malware database from a cyber security firm containing more than 13,815 sections covering cybercrimes between May 11, 2010, and January 13, 2014. This exceptional dataset fortified our

investigation by giving real world proof from an alternate perspective.

C: Selecting Analytical Methods

1) CaaS AND CRIMEWARE CLASSIFICATION MODEL

A various range of things is sold in the cybercrime underground, with various degrees of associated hazard. For this examination, we concentrated mainly on things critical to hacking. We originally sifted the messages to choose just those that carried significant dangers and then isolated them into the categories.

To be classified as a dangerous Threat, for example, a message should also contain Market-related catchphrases. Messages containing the two Threats-and Market-related watchwords are viewed as increasingly dangerous (e.g., "Moving quiet Microsoft Office abuse") then messages with just Threat-related catchphrases (e.g., "Can I conceal a record inside a word doc?"). In like manner, messages related to the Product/Service, Market, and File Extension categories are not recognized as dangerous on the off chance that they just contain catchphrases related to one category. In addition, messages containing Exclusion-related catchphrases (e.g., "tutorials" or "tips") are not recognized as dangerous.

To classify messages accurately, we also use catchphrases related to CaaS and crimeware. This classification step is applied after the messages have been separated as above, so many watchwords are not required and the criteria are less complex. Be that as it may, when a message fits into numerous categories, this overlap is recorded in order to get additional experiences from the later analysis and applications. The sorts of the catchphrase utilized for the proposed classification show are as per the following.

- Threat: watchwords specifically related to threats or digital attacks (e.g., "misuse" or "botnet").
- Product/Service: watchwords related to items or services (e.g., "Facebook" or "Skype").
- File Extension: watchwords related to software or add-ons (e.g., "doc" or "ppt").
- Market: watchwords related to markets or transactions (e.g., "moving" or "$").
- Exclusion: watchwords that are not related to malware (e.g., "tutorial" or "tips").

To enhance the quality of the training data, we alluded to the malware database obtained from the cyber security research firm. Since this database contained labeled black market communications by cyber security professionals, it gave an

appropriate manual for building the training dataset.

Not with standing, the database was somewhat outdated (May 11, 2016, to January 13, 2018), so we also alluded to later data from anti-infection sellers' sites. Four undergraduate understudies (two gatherings of two) with cyber security backgrounds assisted in validating this data. Before creating the training dataset, we gave the participants a lot of rules and techniques based on the malware dataset. After they had completely comprehended and talked about these, we utilized them to create the training data. At the point when two understudies disagreed, somebody from the other gathering talked about the matter with them to help accommodate the disagreement. The between rater reliability score was 82%. This is above the proposed reliability least (80%), and so was viewed as adequate.

We utilize the naïve Bayes algorithm, a probabilistic classification algorithm that addresses probabilistic reasoning under uncertainty because it is the least difficult approach for content classification. machine learning we are often interested in selecting the best hypothesis (h) given data (d).

In a classification problem, our hypothesis (h) may be the class to assign for a new data instance (d).

One of the easiest ways of selecting the most probable hypothesis given the data that we have that we can use as our prior knowledge about the problem. Bayes' Theorem provides a way that we can calculate the probability of a hypothesis given our prior knowledge.

Bayes' Theorem is stated as:

P (h/d) = (P (d/h) * P (h)) / P (d)

Where

P(h|d) is the probability of hypothesis h given the data d. This is called the posterior probability.

P(d|h) is the probability of data d given that the hypothesis h was true.

P (h) is the probability of hypothesis h being true (regardless of the data). This is called the prior probability of h.

P (d) is the probability of the data (regardless of the hypothesis).

You can see that we are interested in calculating the posterior probability of P(h|d) from the prior probability p(h) with P(D) and P(d|h).

After calculating the posterior probability for a number of different hypotheses, you can select the hypothesis with the highest probability. This is the maximum probable hypothesis and may formally be called the maximum a posteriori (MAP) hypothesis.

This can be written as:

MAP (h) = max (P (d/h) * P (h)) / P (d))

The P (d) is a normalizing term which allows us to calculate the probability. We can drop it when we are interested in the most probable hypothesis as it is constant and only used to normalize. Back to classification, if we have an even number of instances in each class in our training data, then the probability of each class (e.g. P(h)) will be equal. Again, this would be a constant term in our equation and we could drop it so that we end up with:

MAP (h) = max (P (d/h))

The reliant feature vector is x =(x1, x2, x3….xn) and Bayes' hypothesis gives us the accompanying.

Ci=argmaxP(x1, x2, x3…….xn/C) P (Ci) ----------(2)

Ci= argmax∏[3] ( ) ( )----------

(3)

P (xi) = Number of x_i in document of Class C/Number of words in document of class C---------- (4)

Basing the probabilistic classifier on the naïve Bayes display streamlines the conditional freedom assumptions for the CaaS and crimeware classes. The sentences in a record are tokenized into words, which are classified as relating to either CaaS or crimeware. The probability of the report having feature xi can then be figured by partitioning "the quantity of features xi in archives of class C" by "the number of words in records of class C".

2) COMPANY NAME EXTRACTION

Named element acknowledgment is an information extraction system that classifies named substances based on a predefined dictionary. We utilized the Open Calais API to perceive the company and personal names. For example, Fig. 1 demonstrates that "Apple" is perceived as alluding to the company rather than the natural product. We use named substance acknowledgment to recognize the company names referenced in the cybercrime underground, which we consider as potential targets (e.g., RAT suitable targets) .

D: Implementing an Application

Although organizations emphasize the measures they take to avert cybercrime, their overall viability has yet to be empirically demonstrated in practice. In the last advance of our framework, we demonstrate the utilization of the proposed CaaS and crimeware definitions, classification model, and analysis framework. The subsequent application actualizes all the data analysis strategies explained in Section IV and aim to demonstrate how our proposed framework can convey bits of knowledge to end clients.

IV. CONCLUSION

A Data Analytics Approach to the Cybercrime Underground Economy, to wind up, malware's main objective is to deliver and hide malicious program, then to steal data and extort money. Now this black market has flourished that much that many cybercriminals are creating kits they can sell to new incomers in the underground economy of black market money. It helps all inexperienced new virus attackers with less technical knowledge to cause attacks without too much problem. It may continue to process itself in 2013 and even beyond to keep on one step further of the ever changing approaches, which businesses use technology.

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. Info. Prot., vol. 1, no. 1, pp. 28–18, 2013.

[4] S. W. Brenner, "Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships," N. C. J. Law & Technol., vol. 1, no. 1, pp. 1-10, 2002.

[5] K. Hughes, "Entering the world-wide web," ACM SIGWEB Newsl., vol. 1, no. 1, pp. 1–8, 1994.

[6] S. Gregor and A. R. Hevner, "Positioning and Presenting Design Science Research for Maximum Impact," MIS Quart., vol. 17, no. 2, pp. 17-156, 2013.

[7] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," MIS Quart., vol. 28, no. 1, pp. 15-105, 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. 1, pp. 15–17, 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. 1, pp. 1–15, 2007.

[11] M. Yar, "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory," Eur. J. Criminol., vol. 2, no. 1, pp. 107– 127, 2005.

[12] K.-K. R. Choo, "Organised Crime Groups in Cyberspace: a Typology," Trends in Organized Crime, vol. 11, no. 1, pp. 270–295, 2008.

[13] L. E. Cohen and M. Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach," Am. Social. Rev., vol. 14, pp. 188–108, 1979.

[14] M. Felson, "Routine Activities and Crime Prevention in the Developing Metropolis," Criminol., vol. 25, no. 1, pp. 911–92, 1987.

[15] F. Mouton, M. M. Malan, K. K. Kimppa, and H. S. Venter. "Necessity for ethics in social engineering research," Comput. Security, vol. 15, 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., 1th 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. 1, pp. 189–194, 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/1145/

[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.

About authors:

Dr.A.Swarupa Rani,
Associate Professor in Dept. of MCA,
SIETK, Puttur, Andhra Pradesh, India.
E-mail Id: swaruparani_kanta@yahoo.com

Ms. G.Manasa,
Dept. of MCA,
SIETK, Puttur, Andhra Pradesh, India.
E-mail Id: manasa141995@gmail.com