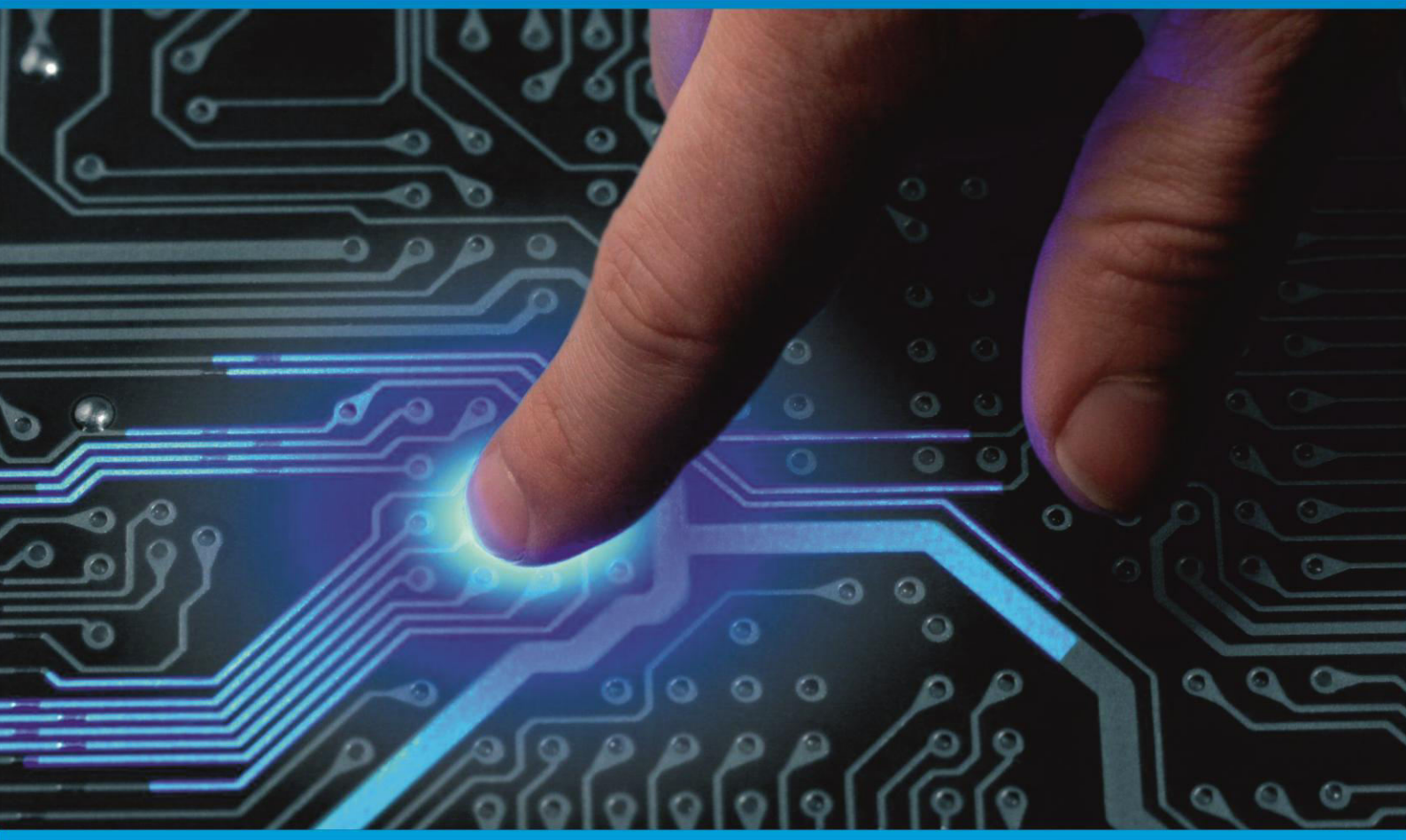
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905173 |

CAAS: A Framework for Cyber Crime Data Analytics

M A Basith Ahsen[1], Osama Abdul Basith[1], Dr. T Prem Chander[2]

B.E Students, Dept. of I.T., ISL Engineering College, Affiliated to Osmania University, Hyderabad, India[1]

Associate Professor, Dept. of I.T., ISL Engineering College, Affiliated to Osmania University, Hyderabad, India[2]

ABSTRACT: Notwithstanding the quick heightening of digital dangers, there has still been little examination into the establishments of the subject or procedures that could serve to direct Information Systems specialists and experts who manage network protection. Moreover, little is referred to about Crime-as-a-Service (CaaS), a criminal plan of action that supports the cybercrime underground. This examination hole and the pragmatic cybercrime issues we face have roused us to explore the cybercrime underground economy by adopting an information investigation strategy from a plan science point of view. To accomplish this objective, we propose (1) an information examination system for investigating the cybercrime underground, (2) CaaS and crime-ware definitions, and (3) a related order model. What's more, we (4) foster a model application to show how the proposed structure and characterization model could be executed by and by. We at that point utilize this application to research the cybercrime underground economy by breaking down an enormous dataset got from the web based hacking local area. By adopting a plan science research strategy, this examination adds to the plan antiquities, establishments, and procedures around here. In addition, it gives valuable reasonable experiences to professionals by recommending rules with regards to how governments and associations in everything businesses can plan for assaults by the cybercrime underground.

KEYWORDS: Cyber, Crime, Data Analytics, Economy, Security

I. INTRODUCTION

As the danger presented by gigantic cyberattacks (e.g., ransomware and appropriated forswearing of administration assaults (DDoS)) and cybercrimes has developed, people, associations, and governments have battled to discover approaches to protect against them. In 2017, ransomware known as WannaCry was liable for almost 45,000 assaults in very nearly 100 nations. The touchy effect of cybercrime has put governments compelled to build their network safety spending plans. US President Barack Obama proposed spending more than $19 billion on online protection as a component of his monetary year 2017 financial plan, an expansion of over 35% since 2016.

Worldwide cyberattacks (like WannaCry and Petya) are executed by exceptionally coordinated criminal gatherings, and coordinated or public level wrongdoing bunches have been behind numerous new assaults. Commonly, criminal gatherings purchase and sell hacking instruments and administrations on the cybercrime bootleg market, wherein assailants share a scope of hacking-related data. This online black market is worked by gatherings of aggressors and it thus upholds the underground cybercrime economy.

The cybercrime underground has subsequently arisen as another kind of association that both works illegal businesses and empowers cybercrime tricks to prosper. Since coordinated cybercrime requires an online organization to exist and to direct its assaults, it is profoundly subject to shut underground networks (e.g., Hackforums and Crackingzilla). The namelessness these shut gatherings offer implies that cybercrime networks are organized uniquely in contrast to conventional Mafia-style heirarchies, which are vertical, concentrated, unbending, and fixed. Conversely, cybercrime networks are sidelong, diffuse, liquid, and developing. Since the internet is an organization of organizations, the danger presented by the ascent of exceptionally proficient organization based cybercrime plans of action, like Crimeware-as-a-Service (CaaS), remains generally imperceptible to governments, associations, and people.

Despite the fact that Information Systems (IS) analysts and experts are taking an expanding interest in cybercrime, because of the basic issues emerging from the fast expansion in digital dangers, few have endeavored to put this new interest on a strong establishment or foster appropriate techniques. Past examinations have not dissected the underground economy behind cybercrime inside and out. Moreover, little is thought about CaaS, one of the essential plans of action behind the cybercrime underground. There is a general absence of understanding, both in examination

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905173 |

and practice, of the idea of this underground and the instruments hidden it. This exploration hole, and the functional issues looked by cybercriminals, rouses our investigation.

We adopt an information examination strategy and research the cybercrime economy from a plan science point of view. To accomplish this objective, we (1) propose an information examination structure for dissecting the cybercrime underground to direct analysts and professionals; (2) characterize CaaS and crimeware to all the more likely mirror their highlights from both scholastic exploration and business practice viewpoints; (3) utilize this to fabricate an arrangement model for CaaS and crimeware; and (4) form an application to show how the proposed system and grouping model could be executed by and by. We at that point assess this application by applying it for a situation study, to be specific exploring the cybercrime economy by breaking down an enormous dataset from the internet hacking local area. This investigation takes a plan science research (DSR) approach. Plan science "makes and assesses data innovation relics proposed to tackle distinguished issues". DSR includes fostering a scope of IT ancient rarities, for example, choice emotionally supportive networks, models, structures, devices, strategies, and applications. Where conduct science research tries to create and legitimize hypotheses that clarify or foresee human or authoritative wonders, DSR looks to broaden the limits of human and hierarchical capacities by making new and imaginative antiquities. DSR's commitment is to enhance the writing and practice as far as "plan relics, plan development information (e.g., establishments), or potentially plan assessment information (e.g., procedures)". This investigation follows these DSR rules and contributes plan curios, establishments, and techniques. Specifically, DSR should show that plan ancient rarities are "implementable" in the business climate to tackle a significant issue, so we give an implementable structure instead of a theoretical one. We additionally make a front-end application as a case guide to show how the proposed structure and order model could be executed by and by. Also, this examination adds to plan hypothesis. Concerning establishments, DSR ought to have an imaginative advancement of builds, models, techniques, or launches that expand the plan science information base. This investigation along these lines adds to the information base by giving essential components like builds (definitions, structures, and applications), a model (Classification model), a method(analysis), and launches (applications).

Related work

Cybercrime has gone through a progressive change, going from being item situated to support arranged on the grounds that the reality it works in the virtual world, with various spatial and fleeting requirements, separates it from other wrongdoing occurring in the actual world. As a component of this change, the cybercrime underground has arisen as a mysterious cybercrime commercial center on the grounds that arising mechanical changes have furnished coordinated cybercriminal bunches with remarkable freedoms for abuse. The cybercrime underground has a profoundly proficient plan of action that upholds its own underground economy. This plan of action, known as CaaS, is "a plan of action utilized in the black market where illicit administrations are given to help underground purchasers direct cybercrimes, like assaults, contaminations, and illegal tax avoidance in a mechanized way,". Hence, CaaS is alluded to as a do-it-for-me administration, not at all like wrongdoing product which is a DIY item. Since CaaS is intended for tenderfoots, its clients don't have to run a hacking worker or have undeniable level hacking abilities. Subsequently, the CaaS plan of action can include the accompanying jobs: composing a hacking program, playing out an assault, appointing an assault, giving an assault worker (foundation), and washing the returns. Sood and Enbody have recommended that crimeware commercial centers have three key components, specifically entertainers (e.g., coders, administrators, or purchasers), esteem chains, and methods of activity (e.g., CaaS, pay-per-introduce, crimeware toolboxs, financier, or providing information). Occasional observing and examination of the substance of cybercrime commercial centers could help foresee future digital dangers.

II. PROPOSED SYSTEM

Althoughthe two scholastics and professionals have as of late began to give more thoughtfulness regarding CaaS, its quickly developing nature has kept them from arriving at agreement on the most proficient method to characterize various kinds of CaaS and crimeware. Thus,

the majority of the scholarly exploration has acquired the definitions utilized by the business practice writing, prompting broadly shifting understandings in various orders. Given this vagueness, we approach arranging CaaS and crimeware from a RAT point of view (thinking about weaknesses as reasonable targets and preventive measures as able

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905173 |

watchmen against wrongdoing) in a cybercrime underground setting. Likewise, we rethink CaaS and crimeware dependent on the definitions utilized in existing exploration and practice.

CLASSIFICATION OF CRIMEWARE SERVICES AND PRODUCTS

The definitions of CaaS and crimeware used inthe academic and business practices literature, which form abasis for our classification model, suitable for the IS field.We reclassify CaaS and crimeware in terms of the suitabletargets (attack strategy/mode) and absence of capableguardians (preventive measures) in a cybercrimeunderground context.The different attack strategies/modes in Table 1 areassociated with RAT's suitable targets because vulnerableorganizations, products, and services may suffer from attacksusing a variety of strategies. In contrast, preventive measuresare associated with RAT's absence of capable guardiansbecause encryption and VPN services, crypters, and proxiesare intended to neutralize preventive measures by bypassinganti-virus and log monitoring software.

DEFINITION OF CRIMEWARE SERVICES AND PRODUCTS

We now need to review the definitions used in both theresearch and business practice literature. This study extendsthe IS literature by facilitating a conceptual understanding ofthe CaaS business models used by the cybercrimeunderground. Drawing upon prior research and businesspractice literature, we propose definitions of CaaS andcrimeware that better reflect the features of CaaS in both of these areas.

Crimeware-as-a-Service

Account Hacking Services: Previous academic research has defined account hacking as "a crime which originated as a type of theft specific to digital environments where users create personal digital profiles and store valuable personal information such as passwords, bank account numbers, and ID numbers,". 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 obtaining account information (e.g., username and password) or extra security information (e.g., security questions and answers). Phishing Services: Phishing has been defined in the business practice literature in the last few years because it has become increasingly sophisticated and is one of the most common techniques used by cybercriminals. Phishing is defined as "masquerading as a trustworthy source in an attempt to bait a user to surrender sensitive information such as a username, password, and credit card number,"Volonino et al. defined phishing as "sending an e-mail to a user falsely claiming to be a legitimate enterprise in an attempt to scam the user." The term "phishing" is a portmanteau of "password" and "fishing," where the latter refers to catching fish using bait or a lure. We thus define a phishing service as a service that hacks accounts by pretending to be a reliable source, such as a bank or card service. Brute Force Attack Services: A brute force attack is an attempt to log in to an account and steal it by repeatedly trying random passwords. Such attacks often target less specific targets than phishing or social engineering. For example, an attacker may try to log in using one of the system's default usernames (e.g., "root" or "admin") by systematically trying all possible passwords. We thus define a brute force attack service as a service that hacks accounts by trying all possible passwords.

DDoS Attack Services: In the research literature, a DDoS attack is defined as "an attack which makes resources unavailable to its legitimate users,". 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,". DDoS botnet attacks can cause serious damage: for example, the Gameover Zeus attack stole online banking credentials, resulting in a $100 million loss. 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.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

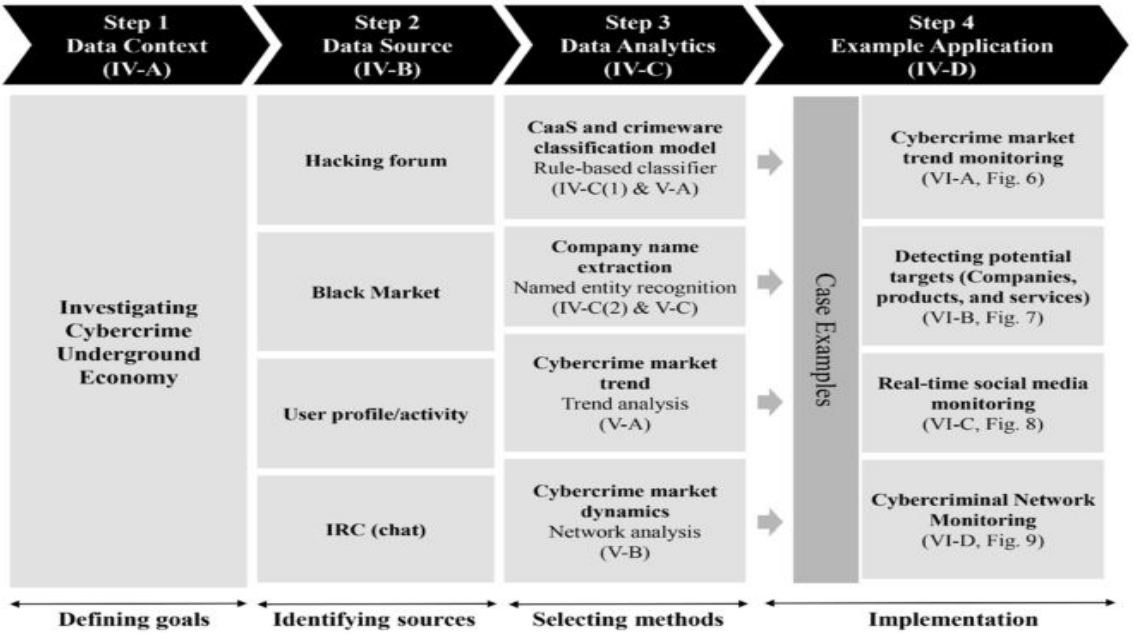
| DOI: 10.15680/IJIRCCE.2021.0905173 |

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," and is used to obtain administrator privileges on a system. We thus define an exploit as a program or script that exploits vulnerabilities in applications, servers, or clients.
- Ransomware: Ransomware is a type of malicious software that disables the functionality of a computer in some way. We thus define ransomware as malicious software that encrypts a victim's data to extort money from them.
- Rootkit: The business practice literature defines a rootkit as "a program that allows someone to obtain root-level access to the computer. We thus define a rootkit as a piece of malicious software that enables administrator-level access to an operating system or computer network.
- Trojan: Trojans are defined by Colarik and Janczewski as malicious programs that perform a legitimate function but also engage in unknown and/or unwanted activity. We thus define a Trojan as a piece of malware that provides unauthorized remote access to a victim's computer.
- Drive-by download: All these crimeware products are used in drive-by download attacks, which have become one of the primary types of cyberattack worldwide. Such attacks target victims through their Internet browsers, installing malware their computers as soon asthey visit an infected website. We thus define a drive-by download attack as an attack that installs malware when the victim visits a malicious webpage.
- Crypter: Crypters can encrypt programs or source code to avoid detection and tracking by bypassing anti-virus software, and can also be offered as a service. We thus define a crypter as a piece of encryption software that helps an intruder to bypass security programs.
- Proxy: Proxies are used for a variety of purposes, such as accelerating data transmission and filtering traffic. We thus define a proxy as a server that enables anonymous Web browsing.

PROPOSED SYSTEM ARCHITECTURE.

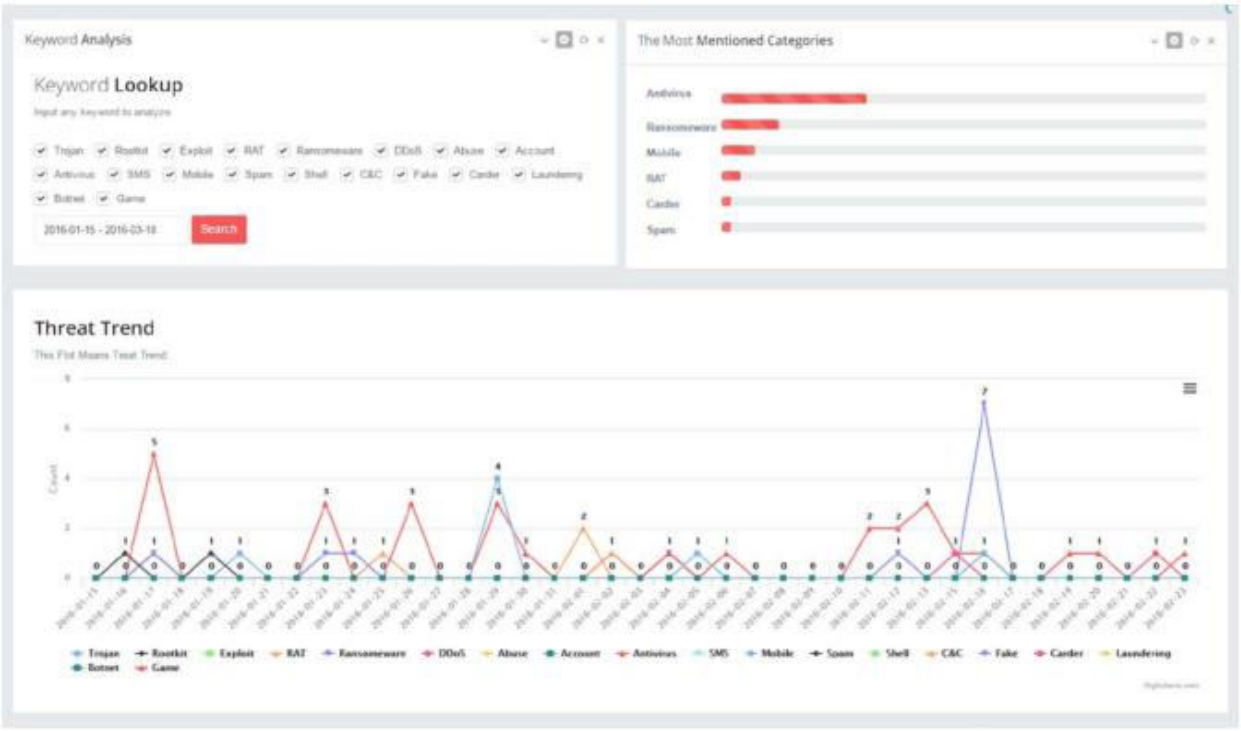


Proposed data analytical framework.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905173 |



CaaS and crimeware trend monitoring system.

III. RESULTS

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. 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, these four example applications demonstrate the range of potential practical applications available to future researchers and practitioners. Unlike previous studies 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, and 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 RATbased classification model.

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

IV. CONCLUSION AND FUTURE WORK

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

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905173 |

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. 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. In this regard, legal and technical training is needed to reduce the impact of cyberattacks.

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 DesignScience 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. 75105, 2004.
[8] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information SystemsResearch," 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: aTypology," 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 theDeveloping 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/cloudcontent/us/pdfs/securityintelligence/white-papers/wp-russian-underground-revisited.pdf

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details