iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VIII **Month of publication:** August 2022

DOI: https://doi.org/10.22214/ijraset.2022.45908

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VIII Aug 2022- Available at www.ijraset.com

A Data Analytics Approach to the Cyber Crime Underground Economy

K. Vinaya Padmaja[1], Kalyani. T[2], T. Rushalani[3], Dr. M. Ramasubramanian[4]
[1, 2, 3]*Students, Department Of CSE Engineering, SWEC, Hyderabad, Telangana, India*
[4]*Guide, Professor, Department Of CSE Engineering, SWEC, Hyderabad, Telangana, India*

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

Keywords: Crime ware-as-a-Service, crime ware, underground economy, hacking community, machine learning.

I. INTRODUCTION

As the threat posed by major cyber attacks (e.g., ransom ware and distributed denial of service (DDoS)) and cybercrime has risen, people, governing organizations, and governments have rushed to devise countermeasures. Want to Cry ransomware was responsible for about 45,000 assaults in nearly 100 countries in 2017 [1]. The growing impact of cybercrime has prompted leadership to boost its top-secret expenditures. Global cyber attacks (such as Want to Cry and Peaty) are carried out by highly organized criminal gangs, and many recent efforts have been carried out by organized or national level crime groups. In general, criminal groups use the cybercrime black market to acquire and sell hacking tools and services, and attackers share a variety of hacking-related data.

As a result, the cybercrime underground has emerged as an unique form of organization that both administers black marketplaces and facilitates cybercrime plots. Because well planned cybercrime necessitates the existence and operation of an internet network, it is heavily reliant on closed antiestablishment communities (e.g., Hack forums and Crackingzilla). Because of the secrecy provided by these closed groups, cybercrime networks are structured differently from conventional Mafia-style hierarchies [4], which are vertical, resolute, inflexible, and fixed. Cybercrime networks, in contrast, are lateral, diffuse, fluid, and dynamic. Because the internet is a web of networks [5,] the threat posed by the wage growth of highly professional network-based cybercrime business models such as Crime ware-as-a-Service (CaaS) is mostly unseen to governments, governing bodies, and the general public.

II. METHODOLOGY

Our data analysis framework's objective is to perform a big-picture examination of the cybercrime underground by encompassing all aspects of data analysis from start to finish. This structure is made up of four steps: (1) setting goals; (2) identifying sources; (3) deciding on analytical techniques; and (4) putting the application into action.

A. Step 1: Defining Goals

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

B. Step 2: Identifying Sources

The second step is to identify the data sources, based on the goals defined by Step 1. This step should consider what data is needed and where it can be obtained. Since the goal of this study is to investigate the cybercrime underground, we consider data on the cybercrime underground community. We therefore collected such data from the community itself and obtained a malware database from a leading global cyber security research firm. Because cybercriminals often change their IP addresses and use anti-crawling scripts to conceal their communications, we used a self-developed crawler that can resolve catches and anti- crawling scripts to gather the necessary data.

C. Step3: Selecting analytical methods

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

D. Step4: Implementing an application

Although organizations emphasize the measures they take to prevent cybercrime, their overall effectiveness has yet to be empirically demonstrated in practice. In the last step of our framework, we demonstrate the use of the proposed CaaS and crimeware definitions, classification model, and analysis framework.

III. MODELING AND ANALYSIS

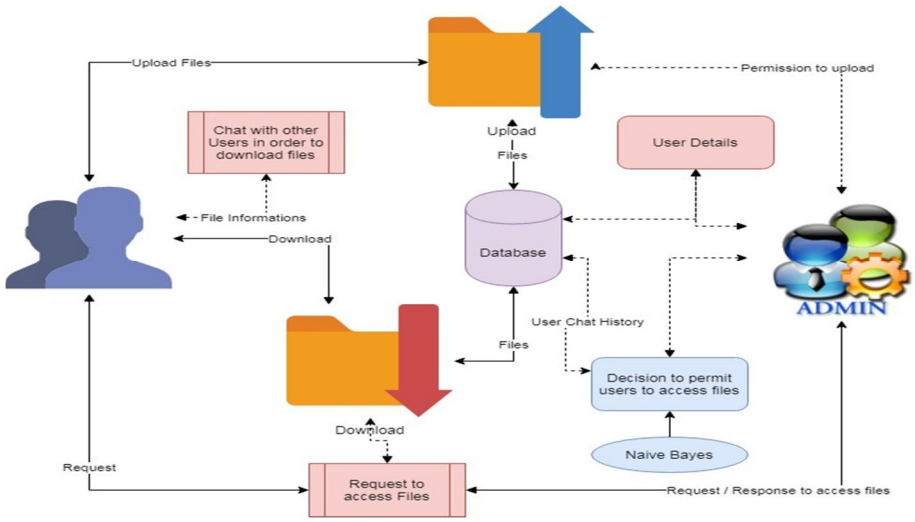


Fig1: System Architecture

A. Modules in The System Architecture

1) *Files to Upload:* Users are permitted to upload files with the specified tags. When a file is uploaded, it is forwarded to admin for approval before it can be published or seen by other users. These submitted materials can be in any format, including documents, music, and video, but executable (.exe) files are not permitted.
2) *Observation of Conversations:* Users are permitted to communicate with one another. The administrator could keep an eye on this. The malevolent conversion enjoys threatening the data. In order to defend cybercrime and prevent the formation of a cybercrime community. This is possible with the aid of a classification method known as naive Bayes classification.
3) *File Downloads:* The files may be downloaded by requesting them, and once authorised by the administrator, they can be downloaded. The choice to authorise files can be derived from the user discussion. The administrator takes action on download files and user approval status. Based on the users, further activities are permitted.
4) *Graphic Representations:* The approvals and disapprovals are used to compute the analyses of proposed systems. This can be quantified using graphical notations such as a pie chart, a bar chart, or a line chart. The data can be presented in a dynamical format.

IV. RESULTS AND DISCUSSION

This study adds to the body of knowledge by demonstrating new approaches to the problems cybercrime and social media researchers face 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.

Although our study has made several significant findings, it nevertheless has several limitations that will need to be addressed in future studies. These will be able to add more analysis and significant further insights. First, we only collected data from the largest hacking community and did not consider other hacking communities. Future studies will therefore need to generalize our findings by investigating a wider range of hacking communities. Second, this study has focused on the CaaS and crime ware available in the cybercrime underground, but much in depth analysis remains to be done on the configurations of cybercrime networks. Future research could cluster keywords and threats by industry to provide a deeper understanding of the potential vulnerabilities, and it could attempt to discover the network effects involved or the leaders of the cybercrime underground.

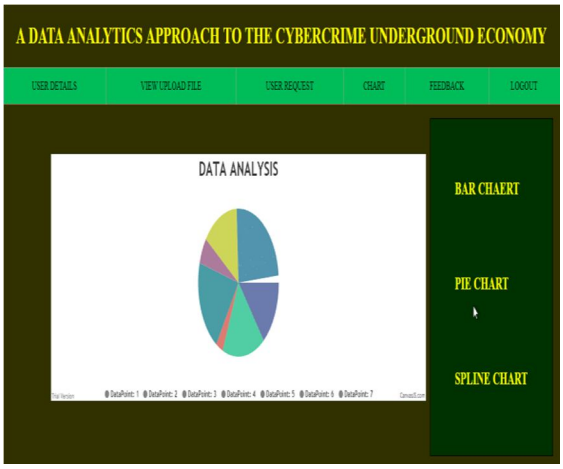


Fig2: Chart

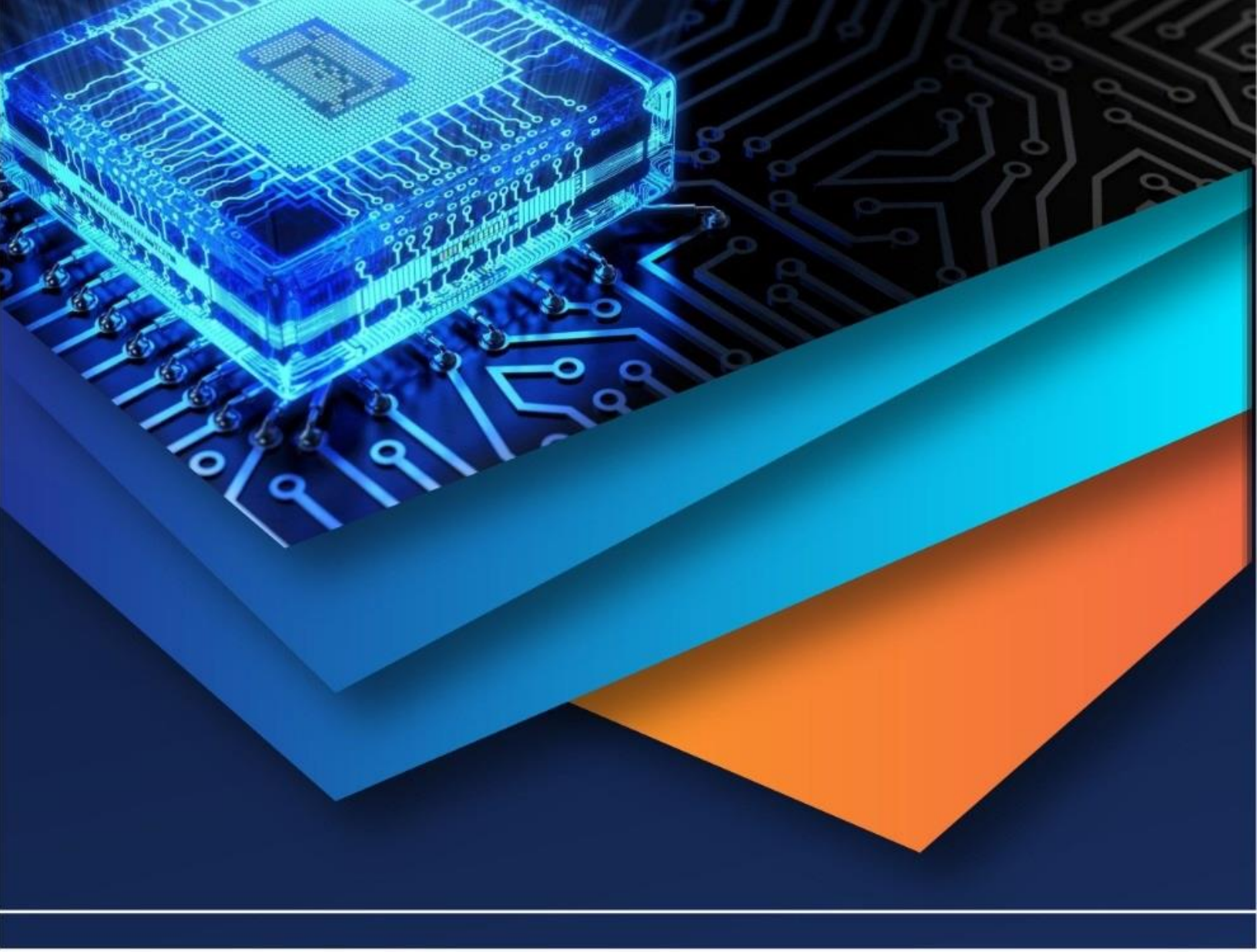
V. CONCLUSION

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 crime ware from an RAT perspective.

We have also proposed sets of definitions for different types of CaaS (phishing, brute force attack, DDoS attack, and spamming, creeping, and VPN services) and crime ware (drive-by download, botnets, exploits, ransom ware, root kits, Trojans, creepers, 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. 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 crime ware trends, our results show that the prevalence of botnets (attack-related crime ware) 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.

REFERENCES

[1] J. C. Wong and O. Solon, Massive Ransomware Cyber-Attack Hits Nearly 100 Countrie Around the World, May 2017, [online] Available: https://www.theguardian.com/technology/2017/may/12/global-cyber-attack- ransomware-nsa-uk-nhs.
[2] FACT SHEET: Cybersecurity National Action Plan, Washington, DC, USA, 2016.
[3] A. K. Sood and R. J. Enbody, "Crimeware-as-a-service—A survey of commoditized crimeware in the underground market", Int. J. Crit. Infrastruct. Protect., vol. 6, pp. 28-38, 2013.
[4] S. W. Brenner, "Organized cybercrime-how cyberspace may affect the structure of criminal relationships", North Carolina J. Law Technol., vol. 4, no. 1, pp. 1-50, 2002.
[5] K. Hughes, "Entering the World-Wide Web", ACM SIGWEB Newslett., vol. 3, no. 1, pp. 4-8, 2019.
[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.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY