INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 05, May 2023, pp : 931-934

e-ISSN : 2583-1062

Impact Factor : 5.725

DATA ANALYTICS APPROACH TO THE CYBER CRIME UNDERGROUND ECONOMY

Aakash Kumar[1], Rinki Kumari[2], Meghana S[3], Shweta Kumari[4], Dr. K. Balakrishnan[5]

[1,2,3,4]Student, Dept. of CSE, Sambhram Institute of Technology, Bangalore, Karnataka, India

[5]Associate Professor, Dept. of CSE, Sambhram Institute of Technology, Bangalore, Karnataka, India

DOI: https://www.doi.org/10.58257/IJPREMS31294

ABSTRACT

The rapid growth of technology and widespread use of the internet have led to the emergence of a thriving cyber crime underground economy. By analyzing large volumes of data collected from diverse sources, including open web monitoring, dark web crawling and law enforcement intelligence, this project aims to uncover cyber crime underground economy. Moreover, the study aims to detect emerging cyber threats, anticipate new attack vectors, and understand the dynamics of the illicit marketplace, including pricing mechanisms and product/service offerings. The implications of this project extend beyond law enforcement and cybersecurity domains. Organizations and individuals concerned about their digital security can benefit from the insights gained by understanding the underground economy. This project offers a valuable contribution to the broader efforts aimed at creating a safer digital environment by addressing the root causes of cybercrime and strengthening cyber resilience.

Keywords: Underground Economy, Analyzing, Web Monitoring, Cyber Threats

1. INTRODUCTION

The cybercrime underground economy refers to the covert network of individuals and groups engaged in unlawful activities on the internet. It operates beyond the confines of the legal system and encompasses a broad spectrum of illegal endeavors, such as hacking, identity theft, fraud, data breaches, drug trafficking, weapon sales, and more. Global cyber assaults, like Petya and WannaCry, are executed by highly organized criminal syndicates, and even nation-state crime groups have been implicated in numerous recent attacks. Typically, criminal organizations buy and sell hacking tools and services on the illicit cybercrime marketplace, where attackers exchange a range of hacking-related information. The same clandestine online marketplace is operated by groups of assailants and thereby sustains the subterranean cybercrime economy. Consequently, the cybercrime underground has emerged as a novel form of organization that conducts illicit operations and enables cybercrime conspiracies to flourish.

2. METHODOLOGY

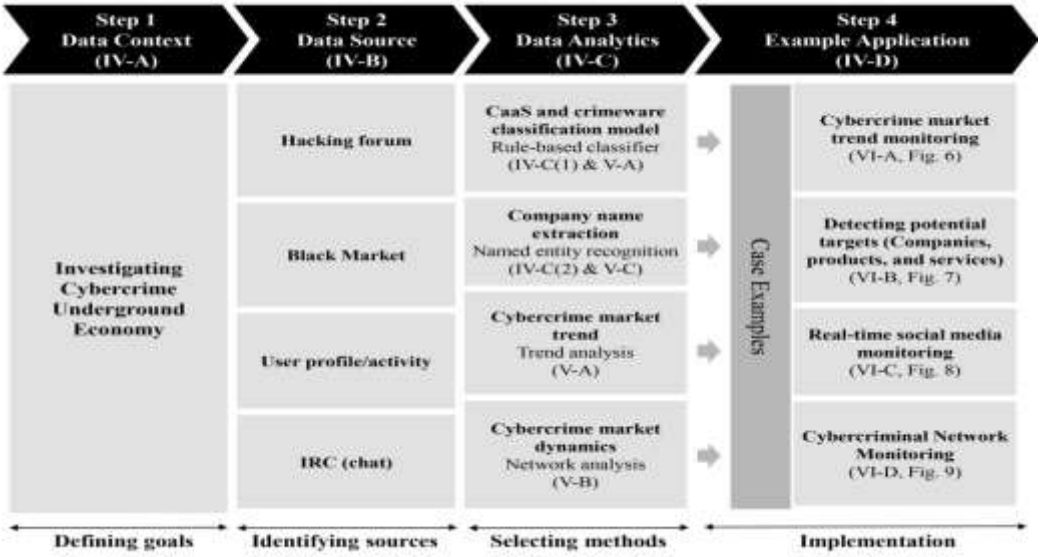

Figure 1: Proposed Data Analytical Framework

Step 1: Defining Goals: The initial stage involves determining the conceptual extent of the analysis. Precisely, this stage pinpoints the analysis framework, including the objectives and aims. To acquire a comprehensive comprehension of the existing CaaS research, we explored the hidden realm of cybercrime, functioning as an exclusive community. Hence, the primary objective of the suggested framework is to " investigate the cybercrime underground economy".

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 05, May 2023, pp : 931-934

e-ISSN : 2583-1062

Impact Factor : 5.725

Step 2: Identifying Sources: The subsequent stage involves determining the data origins, guided by the objectives established in Step 1. This stage necessitates considering the required data and its potential sources. Given that the aim of this research is to examine the clandestine cybercrime network, we focus on procuring data pertaining to the underground cybercrime community. Consequently, we obtained such data by directly engaging with the community itself, while also acquiring a malware database from a prominent global cybersecurity research organization. Since cybercriminals frequently alter their IP addresses and employ anti-crawling measures to obscure their communications, we employed a custom-designed crawler equipped to overcome obstacles and circumvent anti-crawling scripts, thereby enabling us to gather the necessary data. **Step3: Selecting analytical methods:** A wide array of commodities are traded within the realm of cybercrime, varying in terms of the level of associated jeopardy. In this research, our primary emphasis was placed on items of utmost importance to hacking. To begin, we sifted through the messages to exclusively isolate those bearing substantial risks.

Step4: Implementing an application: Despite organizations highlighting the actions they undertake to counteract cybercrime, the tangible efficacy of these measures remains unverified in real-world scenarios. In the final phase of our framework, we substantiate the application of the suggested CaaS and crimeware definitions, classification model, and analysis framework.

3. MODELING AND ANALYSIS

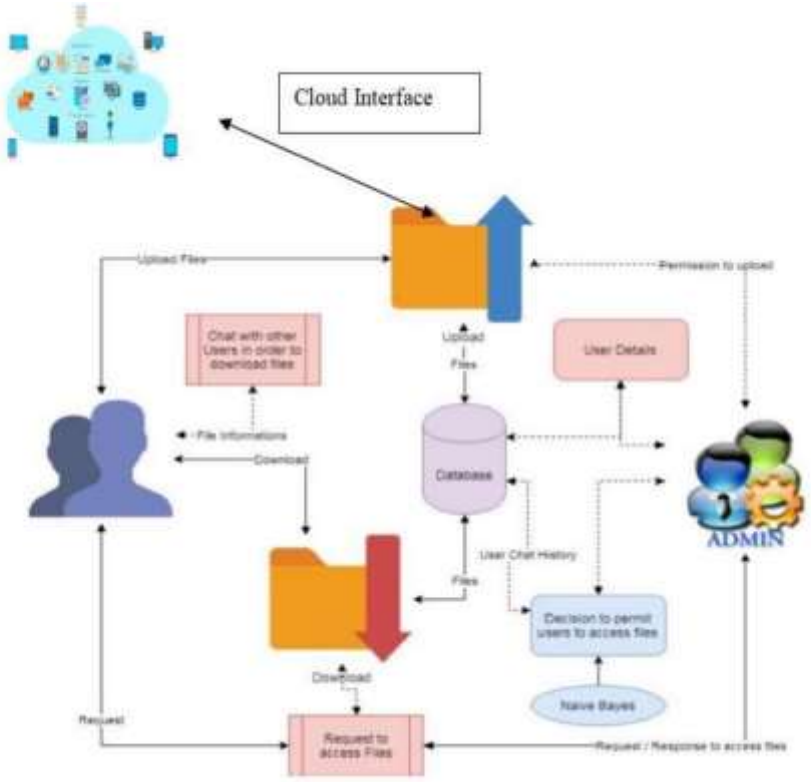

Figure 2: Architecture Model

Modules in the system architecture

Files to Upload: Users are granted authorization to upload files bearing the designated tags. Upon file submission, it is subject to scrutiny by the administrator for approval prior to publication or visibility to other users. The submitted materials may assume various formats, encompassing documents, music, and video, while executable (.exe) files are prohibited.

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.

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.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 05, May 2023, pp : 931-934

e-ISSN : 2583-1062

Impact Factor : 5.725

Graphic Representations: The approvals and disapprovals are used to compute the analyses of proposed systems. This can be quantified using graphical notations. The data can be presented in a dynamical format.

4. RESULTS AND DISCUSSION

Figure 3: Login Page

Figure 4: Request Page

Admin can go to the user request page to see all the requests and click on the chat button to analyze chat to see if the chat is malicious or not.

Figure 5: Negative Chat

Figure 6: Positive Chat

If the chat is malicious, the result will show up as positive.

If the chat is not malicious, the result will show up as negative.

Figure 7: Feedback page

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 05, May 2023, pp : 931-934

e-ISSN : 2583-1062

Impact Factor : 5.725

Figure 8: Data Analysis using graph

5. CONCLUSION

Analyzing the CaaS and crimeware trends, our findings reveal a significant presence of botnets, which are crimeware tools used for launching attacks. Notably, technology companies emerge as the most frequent potential targets, accounting for 28% of the cases, followed by content (22%), finance (20%), e-commerce (12%), and telecommunication (10%) companies. This signifies that attackers are expanding their scope to target organizations across various industries, exploiting their increased dependence on technology. Conducting regular surveillance and analysis of cybercrime marketplaces' content could aid in forecasting future cyber threats

6. REFERENCES

[1] https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8352813 Ganesh Kumar and P.Vasanth Sena, "Novel Artificial Neural Networks and Logistic Approach for Detecting Credit Card Deceit," International Journal of Computer Science and Network Security, Vol. 15, issue 9, Sep. 2015, pp. 222-234

[2] K.-K. R. Choo, "Organised crime groups in cyberspace: A typology," Trends Organized Crime, vol. 11, no. 3, pp. 270– 295, 2008.

[3] https://www.ijraset.com/research-paper/data-analytics-approach-to-the-cyber-crime-underground-economy

[4] A.K.Sood and R.J.Enbody," Crimeware-as-aservice– A survey of commoditized crimeware in the underground market," Int.J.Crit.Infr.Prot., vol.6, no.1, pp. 28–38, 2013.

[5] R.Venkateswaran, 2001. Crimeware as a service Survey of commoditized crimeware in the underground market. [6] FACT SHEET: Cyber security National Action Plan, Ed: The White House, 2016.