IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 7, July 2023

DOI: 10.17148/IARJSET.2023.10779

Cracking the Digital Underworld: A Data-Backed Investigation into Cybercrime and the Underground Economy

Prof. Vidya S[1*], Soujanya Mounesh Kerur[2]

Assistant Professor, Department of Master of Computer Application, BIT Bengaluru[1]

Soujanya Mounesh Kerur, PG Student, Department of Master of Computer Application, BIT Bengaluru[2]

Abstract: The escalating complexity of cybercrime poses challenges to traditional law enforcement methods. To combat this threat, data analytics has emerged as a promising approach. This paper explores the application of data analytics techniques to analyse the cybercrime underground economy. It examines data sources like publicly available information, dark web data, and cybersecurity incidents. Various methodologies, including machine learning, natural language processing, and anomaly detection, are discussed to identify trends and predict threats. Ethical considerations and successful case studies are also explored. The study highlights data analytics as a valuable tool in understanding cybercrime and devising proactive strategies for threat mitigation, emphasizing the need for collaboration among stakeholders.

Keywords: crimeware-as-a-service, crimeware, hacking, machine learning.

INTRODUCTION

In response to the escalating threat posed by major cyberattacks like ransomware and distributed denial of service (DDoS), individuals, governing bodies, and governments have been actively working to develop countermeasures and strategies. In 2017, the Wanna Cry ransomware was the cause of around 45,000 attacks across nearly 100 nations [1]. Leadership has increased its top-secret spending as a result of the growing impact of cybercrime. The cybercrime underground has evolved into a distinct ecosystem where highly organized criminal gangs conduct global cyberattacks, including infamous instances like WannaCry and Petya. Recent incidents have indicated involvement from organized crime groups at national levels. Within this underground network, attackers exchange various hacking-related data, while criminal organizations actively engage in the buying and selling of hacking equipment and services on the black market, solidifying its distinctive nature.

Figure 1: Cyber economy solutions

LITERATURE SURVEY

The evolution of cybercrime has led to a paradigm shift from a product-oriented approach to a service-oriented one. This transformation is a result of its virtual nature, which introduces distinct spatial and temporal constraints, setting it apart from traditional physical-world crimes.[8]. The emergence of the cybercrime underground as a covert marketplace can be attributed to the rise of advanced technologies, which have presented organized cybercriminal groups with unparalleled opportunities for exploitation. [9].The cybercrime underground operates with a remarkably professional business model, sustaining its own hidden economy. [10]. The business model, commonly referred to as CaaS (Cybercrime as a Service), entails the provision of illicit services to assist underground buyers in carrying out automated cybercrimes, including attacks, infections, and money laundering. [11]. Unlike crimeware, which involves a do-it-yourself approach, CaaS is

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 7, July 2023

DOI: 10.17148/IARJSET.2023.10779

characterized as a do-it-for-me service. Unlike the technical expertise required for crimeware, CaaS is specifically designed for novices, eliminating the need for customers to operate a hacking server or possess advanced hacking skills. According to Sood and Enbody, the CaaS business model encompasses several roles, which include creating a hacking program, executing the attack, hiring someone to carry out the attack, supplying the attack server infrastructure, and handling the money laundering process. [11] Sood and Enbody have proposed that crimeware marketplaces consist of three essential components: actors (coders, operators, or buyers), value chains, and modes of operation (such as CaaS, pay-per-install, crimeware toolkits, brokerage, or data supply). They suggest that regular monitoring and analysis of cybercrime marketplaces' content could aid in anticipating potential future cyber threats. [11].

METHODOLOGY

Our data analysis aimed to conduct a thorough examination of the hidden aspects of cybercrime, encompassing every stage of the data analysis process, from inception to conclusion. The process consists of four steps. The initial three stages involve defining objectives, identifying sources, and selecting appropriate analytical methods, followed by the implementation of the chosen approach. Step 1 involves setting clear goals for the analysis. Identifying the conceptual range of the investigation is the first stage. This stage specifically describes the context of the analysis, including the objectives and aims. We conducted an in-depth investigation of the exclusive cybercrime community to gain comprehensive insights into the current research on CaaS (Crime-as-a-Service). Consequently, Step 2 involves identifying relevant resources within the cybercrime underground economy. The subsequent step involves implementing our data analysis methodology with the objective of conducting a thorough examination of the cybercrime underground, encompassing all stages of data analysis from initiation to conclusion.Four steps make up this structure: Step 1 involves defining the objectives, where the primary focus is on identifying the conceptual scope of the investigation within the cybercrime underground. The subsequent steps include locating sources, selecting analytical methods, and executing the application.This stage specifically describes the context of the analysis, including the objectives and aims. In our pursuit of gaining a comprehensive understanding of current CaaS research, we examined the clandestine cybercrime underground community. Consequently, our proposed approach is geared towards investigating the cybercrime underground economy, with Step 2 focusing on identifying relevant sources
. The following action is to We mainly concentrated on components essential to hacking. First, we narrowed down the communications to only those that posed serious threats. Implementing an application is step four. Although businesses highlight the steps they take to combat cybercrime, their general efficacy has not yet been experimentally shown in real-world situations. The final phase of our approach showcases the practical application of the suggested CaaS and crimeware definitions, classification model, and analysis framework.

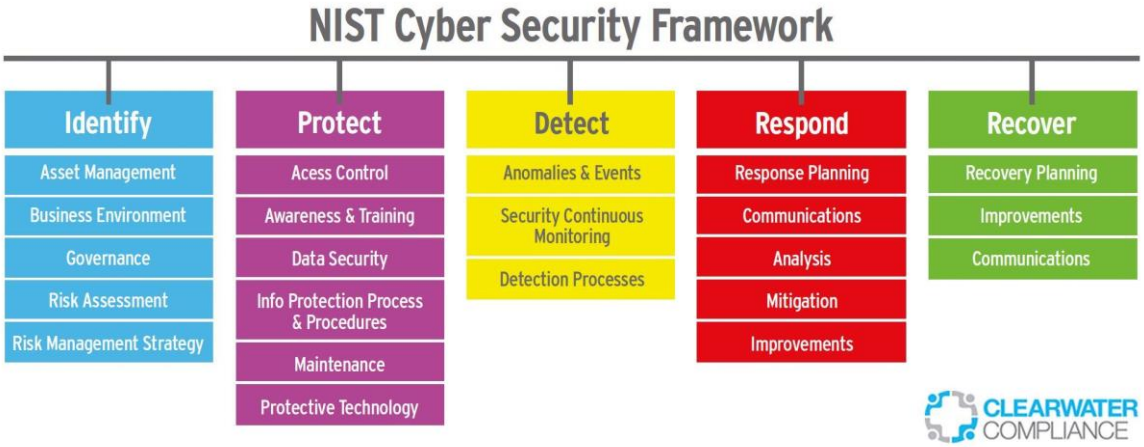

Figure 2: NIST Cyber Security Framework

MODULES IN THE SYSTEM ARCHITECTURE

1. uploading files Users may upload files using the designated tags. Before a file may be posted, published, or made accessible to other users, the admin must authorize it. Documents, music files, and videos of any kind may be submitted, however executable (.exe) files cannot.
2. Conversation Observation the ability to communicate between users is available. The administrator may keep an eye on this. The data is frequently threatened by the malicious conversion. To safeguard against cybercrime and stop

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 7, July 2023

DOI: 10.17148/IARJSET.2023.10779

the emergence of a cybercrime community. The classification algorithm known as naive Bayes classification can help with this.

3. Download documents The files can be requested, and if the administrator has accepted them, they can then be downloaded. The discussion amongst users can be used to decide which files to approve. The administrator decides which items to download and which people are approved. Additional actions are permitted for the users based on the users.

4. Visual Illustrations On the basis of the approvals and rejections, the analyses of suggested systems are determined. Graphical representations such as pie charts, bar charts, and line charts can be employed for quantitative analysis. The data can be presented dynamically, allowing for real-time updates and insights.

CONCLUSION

This DSR study focuses on developing and evaluating artifacts related to Crime-as-a-Service (CaaS) and criminal ware, specifically Remote Access Trojans (RATs). The research proposes a categorization model and a data analysis framework. It introduces definitions for various types of crimeware and CaaS offerings. The study highlights the significance of RATs in comprehensively analysing the cybercrime underground. The prevalence of botnets and VPNs increased in 2017, indicating attackers' consideration of security measures and weaknesses in various industries, making technology organizations the most prospective targets (28%), followed by content, banking, e-commerce, and telecommunications businesses.

REFERENCES

[1] 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.

[2] K.-K. R. Choo, “Organised Crime Groups in Cyberspace: a Typology,” Trends in Organized Crime, vol. 11, no. 3, pp. 270–295, 2008.

[3] RUPESH, M. K., & RAJASEKHAR, M. A. “A DATA ANALYTICS APPROACH TO THE CYBERCRIME UNDERGROUND ECONOMY”.

[4] Ramasubramanian, M. A DATA ANALYTICS APPROACH TO THE CYBER CRIME UNDERGROUND ECONOMY.

[5] VANISRI, M., & GUPTA, B. S. A DATA ANALYTICS APPROACH TO THE CYBERCRIME UNDERGROUND ECONOMY.

[6] Rao, S.K., Kumar, B.R. and Manjunath, B.E., Data Analysis Framework with an Associated Classification Model for Analyzing Cybercrime Underground Economy.

[7] Pastrana, Sergio, Alice Hutchings, Andrew Caines, and Paula Buttery. "Characterizing eve: Analysing cybercrime actors in a large underground forum." In *Research in Attacks, Intrusions, and Defenses: 21st International Symposium, RAID 2018, Heraklion, Crete, Greece, September 10-12, 2018, Proceedings 21*, pp. 207-227. Springer International Publishing, 2018.

[8] Kumar, M. K., & Bhargavi, D. K. (2020).”An Effective Study on Data Science Approach to Cybercrime Underground Economy”, Data. *Journal of Engineering, Computing and Architecture*, vol.*10*(1), pageNo.148-158.

[9] Avinash, G. R., Scholar, P., & Rao, M. V. (2020). “Data Analytics Approach To The Cybercrime, Underground Economy”. *Complexity International*, *24*(01).

[10] K. Hughes, “Entering the world-wide web,” ACM SIGWEB Newsl., vol. 3, no. 1, pp. 4–8, 1994.

[11] 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