International Journal for Innovative
Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IJIEMR Transactions, online available on 07th Jan 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=ISSUE-1

DOI: 10.48047/IJIEMR/V12/ISSUE 01/39

Title **The Use Of Data Science In Examining The Cybercrime Underground Market**

Volume 12, Issue 1, Pages: 446-454

Paper Authors

Mrs. S.Lalitha, B.Akshitha, Hanan Fatima, Summaiya Lateef

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

The Use Of Data Science In Examining The Cybercrime Underground Market

Mrs. S.Lalitha, Assistant professor, Dept. of Information Technology, Sridevi Women's Engineering College, Hyd. Shudulalalitha@gmail.com

B.Akshitha, B.Tech., Dept. of Information Technology, Sridevi Women's Engineering College, Hyd.

Hanan Fatima, B.Tech., Dept. of Information Technology, Sridevi Women's Engineering College, Hyd.

Summaiya Lateef, B.Tech., Dept. of Information Technology, Sridevi Women's Engineering College, Hyd.

ABSTRACT – However, little research has been done to pave the way for future academics and professionals in the area of information systems to follow despite the exponential increase of cyber threats. The public has little knowledge about CaaS, the hidden economic infrastructure of the cybercrime underground. Since there is a dearth of studies on cybercrime, we choose to investigate it using a data analytics approach informed by the discipline of design science. To that end, we first lay out a data processing framework for investigating the dark web, before moving on to discuss the nature of CaaS and crime ware and the classification algorithm that goes along with them. Finally, we sketch out a possible organisational structure for putting these ideas into practise. This programme is used to evaluate the cybercrime black market by first collecting a big dataset from the internet security community. Applying a design science approach, this study improves the field's design artefacts, underpinnings, and methods. More than that, it provides helpful guidance on how governments and businesses across a wide range of sectors should be ready for cybercrime attacks.

This umbrella word includes the terms Crime Ware, Criminal Ware, the Underground Economy, and the Hacker Community, all of which may be found in the Index Terms.

INTRODUCTION

Companies, companies, and other organisations are increasingly working to prepare for the threat of large-scale cyber attacks (including malware and DDoS). And wrongdoings. Almost 45,000 incidents in

2017 were traced back to WannaCry ransomware [1]. As the effects of cybercrime expand, authorities are under more pressure to increase their cyber security budget. More than $19 billion was allotted for network security in President Obama's proposed budget for fiscal year 2017, an increase of more than 35% over 2016. Attacks like WannaCry and Petya, as well as many others of late on a national or worldwide scale, were carried out by well-coordinated criminal gangs. Because of the nature of the underground black market in which hackers trade information about hacking attempts, most hacking operations and equipment are acquired by organised criminal groups. This online black market is managed by groups of cybercriminals, and it serves as a lifeline for the criminal underground [3]. It's a new kind of group that's emerged to handle cybercrime and illegal marketplaces. The cybercrime industry is highly dependent on shadowy criminal networks for both its survival and its assaults (e.g., Hack forums and Crackingzilla). Because of their need for secrecy, cyber security organisations are structured differently from traditional Mafia hierarchies [4] in that they are more vertically oriented, rigid, and stable. However, this is not the case for criminal networks engaged in cybercrime. Cybercrime is a collection of interrelated issues, therefore the rise of highly proficient online cybercriminals' marketing methods, such as Crimeware-as-a-Service (CaaS), goes mostly ignored by governments, corporations, and people. IS researchers and scientists are becoming more interested in cybercrime as a consequence of the serious issues presented by the exponential growth of cyber hazards; nevertheless, very few have attempted to provide a firm groundwork for this new interest or construct adequate techniques. Previous studies haven't delved far into the cybercrime "underground" economy. Cybercriminals rely heavily on the CaaS business model, yet little is known about it. Neither academics nor practitioners have a good grasp on the nature of this underworld or its underlying dynamics. The information vacuum and the real-world difficulties experienced by hackers sparked our research. Through the study of design theory and big data analysis, we examine the cybercrime economy. CaaS and crime ware are defined to accurately represent both educational research and commercial practise; a classification algorithm for CaaS and crime ware is built; (4) an application is built to illustrate how such suggested conceptual model and classifying concept might be implemented effectively in the real world of cybercrime. Applying a designing computational modelling (DSR) approach, it might be utilised to look into the ransomware ecosystem by first analysing large datasets gathered from the internet's technical community. The end result of design science is an IT artefact that was developed with the express purpose of addressing a particular issue. Some examples of the kinds of information technology (IT) artefacts created during DSR include recommendation systems, ideas, structures, platforms, techniques, and applications [6]. Whereas the aim of DSR is on finding and explaining methods by which human or organisational events may be understood or predicted, the focus of behavioural science is on developing and justifying theories that increase such abilities. DSR adds to the body of knowledge by expanding our understanding of "design artefacts, planning and construction learning (e.g. frameworks), and/or design evaluation understanding (e.g. methods). [7]. New design items, foundations, and procedures are created while still adhering to DSR standards. Since DSR must demonstrate that design objects are "implementable" in the economy to address a critical issue [7], we propose an efficient implementation approach rather than merely a theoretical one. A sample front-end application demonstrates the benefits and feasibility of using the suggested infrastructure and categorization strategy. The findings of this study thus add to the body of knowledge surrounding design theory [9, 10]. Producing novel ideas, theories, approaches, or applications is essential for expanding our understanding of design science [10]. This research adds to the body of knowledge by providing essential ingredients such as constructs (classifications, structures, and programmes), a modelling (complex implementation), an analytical approach, and instantiations (applications). It is in the creation and use of novel assessment processes that DSR has made significant contributions to methodology [12]. In light of this, the classification model was tested in this study using dynamic analysis. Additionally, an observational analysis of a front-end application is performed (case examples). Moreover, this study provides useful recommendations for addressing the difficulties encountered by government agencies and enterprises of all sizes and types in their efforts to prepare for cybercrimes.

I. RELATED WORK

A look at criminal software as a service that has emerged on the dark web.

The sale of crimeware using a "service" model, known as "crimeware as a service" (CaaS), is rapidly growing in the underground economy. In addition to seeking to make cyber assaults more structured, automated, and accessible to those who don't know much about computers, CaaS offers major contributions to this problem. This paper defines CaaS and explains how an underground economy has developed around it. In addition, the study discusses the many criminal software applications available on the dark web.

b. Does cybercrime have a structure? Possible Effects of the Internet on Criminal Collaboration

In this study, the authors speculate on how the nature of cybercrime may evolve in the future. The first part of the book examines criminal groups in the "real world." After establishing the meaning of "organised crime," the article examines the upsides of a well-structured criminal organisation. The essay continues by explaining why the two established forms of organised crime in the "actual world"—the "crime" approach and the hierarchies American Mafia model—are unlikely to catch on in the virtual one. Both of the aforementioned models, it is argued, originated from the limitations of accomplishing things in "real life," limitations that are seldom an issue in the virtual world. Next, the paper considers the possibility of a cyber manifestation of organised crime. For this purpose, it examines how the armed forces use Netware. The study concludes that cybercrime will be transient, horizontal, and fluid, in contrast to the permanent, hierarchical patterns of organisation seen in the "real world." The combination of these factors might make it difficult for law enforcement to apprehend criminals.

c. Categories of Online Criminal Organizations

There are three sorts of illegal meetings that are taking use of developments in modern information and communication technologies (ICT): There are three types of criminal organisations using ICT for criminal purposes: 1) traditional criminal gangs that use ICT to improve their illegal actions on land; 2) organised malicious cyber groups that only operate online; and 3) organisations of philosophically and politically driven people who use ICT to commit crimes. Because media technology is often at fault for the emergence of disputes or provides evidence for or against a dispute in court, police departments would benefit from a deeper understanding of cyber forensics principles, recommendations, processes, tools, but rather procedures, along with pro fundamentals, instructions, methods, devices, and strategies. There seems to be a need for more study and innovative approaches to combating organised crime in cyberspace.

II. METHODOLOGY

Ninety percent of people today rely on online services like banking, healthcare, and traffic information to go about their daily lives, but this has led to a rise in cases of cyber theft and attack. Malware developers can now detect data transmission in order to steal sensitive information or tamper with numbers, resulting in financial loss or malfunction of the customer's own mechanism. Passwords of users may be brute-forced, and BOT assaults can boost fake ratings. There is a wide range of cyber attacks on the web since software engineers may hire themselves out for Black Market cash to create them.

This paper describes a wide variety of attacks, and the researcher applies Naive Bayes to the data in order to determine which kind of cyber attacks are the most resource-intensive. Businesses targeted by hackers are being used to develop a categorization algorithm that uses signatures of key attacks like spamming and Code injection.

As a result of developing stress reactions, the project may now be carried out:

Dataset Upload and Analysis: During this time, we'll be tasked with loading a database, doing a variety of analyses (such counting cybercrimes), and finally cleaning the dataset by removing any outliers.

Dataset Processing & Analytical Techniques: Each kind of attacker would be assigned a numeric identifier, the database would be split into training and testing sections, and applications would use 80% of the dataset to teach the Naive Bayes algorithm and 20% to evaluate its prediction abilities.

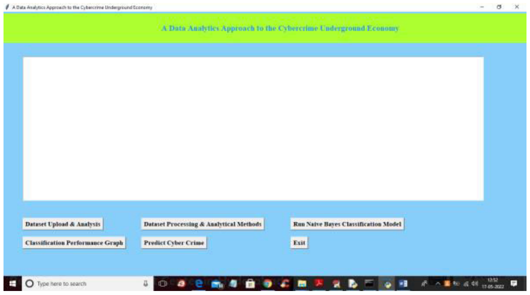
Naive Bayes Classification Model Execution: In this course, classification approaches would be trained on datasets with an accuracy rate of 80% or above, and a following methodology would be developed.

To evaluate the efficacy of the suggested approach, we will utilise this module to construct a classification performance graph with high accuracy and based on the Naive Bayes method.

Predict Cybercrime: We may use these modules to check whether a database of cybercrime networks has any indicators of cybercriminals by submitting it to a classification system.

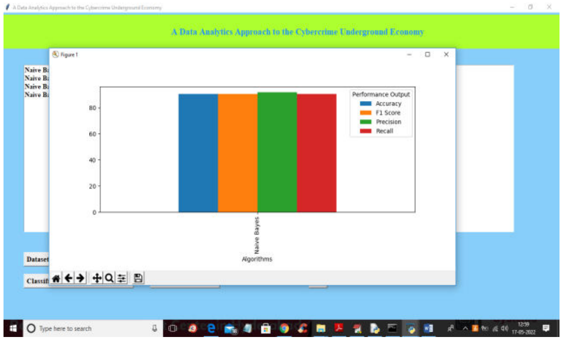
III. RESULTS AND DISCUSSION

There are four steps to the data analysis procedure proposed. In this part, we discuss the many types of CaaS, the current market for this kind of software, and the types of criminals that could be interested in hacking into this type of software. Double-clicking while sprinting. The following is the output from the.bat file:

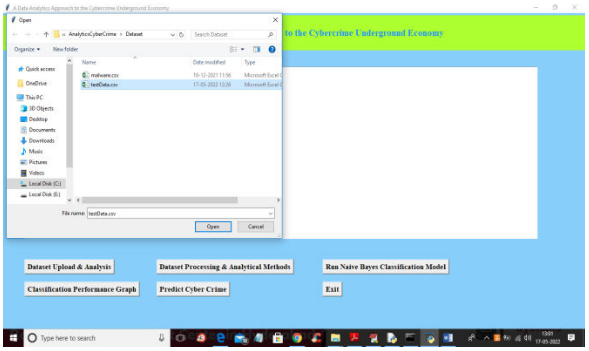

A Data Analytics Approach to the Cybercrime Underground Economy
A Data Analytics Approach to the Cybercrime Underground Economy
Dataset Upload & Analysis
Dataset Processing & Analytical Methods
Run Naive Bayes Classification Model
Classification Performance Graph
Predict Cyber Crime
Exit
Type here to search

Right-click the output, and choose "Dataset Upload & Analysis." From there, you may choose a location to save your uploaded datasets.

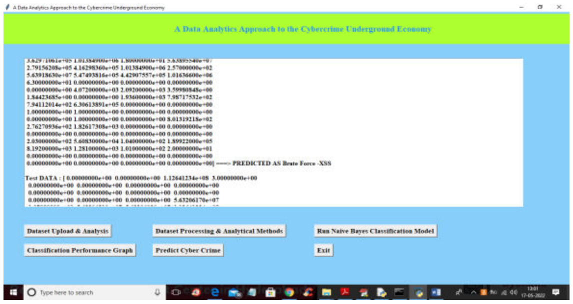
To see the graph, choose the 'Classification Techniques Graph' tab once Naive Bayes retraining has been completed and its prediction performance has been confirmed to be 90%.



In the aforementioned findings, each bar's hue corresponds to a unique metric, such as Accuracy, Quality, etc. All criteria are functioning at or above 90% as seen visually by selecting the "Predict Cyber Crime" button and inputting testing data.



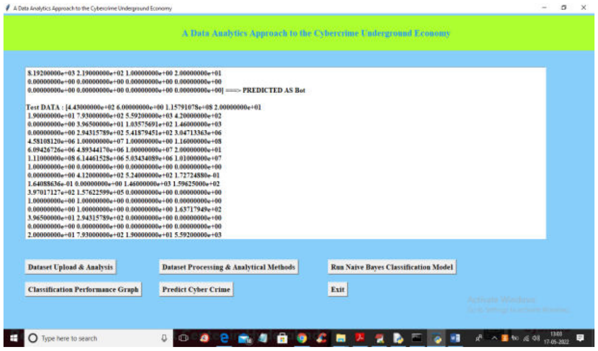
To see this result, load your dataset in the 'testData.csv' format by entering it and then selecting the 'open' button.


A Data Analytics Approach to the Cybercrime Underground Economy
A Data Analytics Approach to the Cybercrime Underground Economy
Dataset Upload & Analysis
Dataset Processing & Analytical Methods
Run Naive Bayes Classification Model
Classification Performance Graph
Predict Cyber Crime
Exit
Type here to search

```
3.62971061e+05 1.01384900e+06 1.80000000e+01 5.63895540e+07
2.79156208e+05 4.16298360e+05 1.01384900e+06 2.57000000e+02
5.63918630e+07 5.47493816e+05 4.42907557e+05 1.01636600e+06
6.30000000e+01 0.00000000e+00 0.00000000e+00 0.00000000e+00
0.00000000e+00 4.07200000e+03 2.09200000e+03 3.59980848e+00
1.84423685e+00 0.00000000e+00 1.93600000e+03 7.98717532e+02
7.94112014e+02 6.30613891e+05 0.00000000e+00 0.00000000e+00
1.00000000e+00 1.00000000e+00 0.00000000e+00 0.00000000e+00
0.00000000e+00 1.00000000e+00 0.00000000e+00 8.01319218e+02
2.76270936e+02 1.82617308e+03 0.00000000e+00 0.00000000e+00
0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00
2.03000000e+02 5.60830000e+04 1.04000000e+02 1.89922000e+05
8.19200000e+03 1.28100000e+03 1.01000000e+02 2.00000000e+01
0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00
0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00] ------> PREDICTED AS Brute Force -XSS

Test DATA : [ 0.00000000e+00  0.00000000e+00  1.12641234e+08  3.00000000e+00
 0.00000000e+00  0.00000000e+00  0.00000000e+00  0.00000000e+00
 0.00000000e+00  0.00000000e+00  0.00000000e+00  0.00000000e+00
 0.00000000e+00  0.00000000e+00  0.00000000e+00  5.63206170e+07
```

The above result displays Internet traffic data in parenthesis, and the projected variety of cybercriminal activity comes after the equal sign. Just scroll down to the very bottom of the page above to see our complete list of predicted cyber assaults.


A Data Analytics Approach to the Cybercrime Underground Economy
A Data Analytics Approach to the Cybercrime Underground Economy
Dataset Upload & Analysis
Dataset Processing & Analytical Methods
Run Naive Bayes Classification Model
Classification Performance Graph
Predict Cyber Crime
Exit
Type here to search
13:03
17-05-2022

```
8.19200000e+03 2.19000000e+02 1.00000000e+00 2.00000000e+01
0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00
0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00] ===> PREDICTED AS Bot

Test DATA : [4.43000000e+02 6.00000000e+00 1.15791078e+08 2.00000000e+01
1.90000000e+01 7.93000000e+02 5.59200000e+03 4.20000000e+02
0.00000000e+00 3.96500000e+01 1.03575691e+02 1.46000000e+03
0.00000000e+00 2.94315789e+02 5.41879451e+02 3.04713363e+06
4.58108120e+06 1.00000000e+07 1.00000000e+00 1.16000000e+08
6.09426726e+06 4.89344170e+06 1.00000000e+07 2.00000000e+01
1.11000000e+08 6.14461528e+06 5.03434089e+06 1.01000000e+07
1.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00
0.00000000e+00 4.12000000e+02 5.24000000e+02 1.72724880e-01
1.64088636e-01 0.00000000e+00 1.46000000e+03 1.59625000e+02
3.97017127e+02 1.57622599e+05 0.00000000e+00 0.00000000e+00
1.00000000e+00 1.00000000e+00 0.00000000e+00 0.00000000e+00
0.00000000e+00 1.00000000e+00 0.00000000e+00 1.63717949e+02
3.96500000e+01 2.94315789e+02 0.00000000e+00 0.00000000e+00
0.00000000e+00 0.00000000e+00 0.00000000e+00 0.00000000e+00
2.00000000e+01 7.93000000e+02 1.90000000e+01 5.59200000e+03
```

IV. CONCLUSION

Since activities are often assumed to be the primary goal of behavioural research, this study's emphasis has been on making and studying artefacts rather than developing and testing hypotheses. Both a model of the information processing flow and a technique for making predictions have been created. We have also undertaken retrospective analyses of the effectiveness of these classifiers and post-implementation analyses of their performance on sample programmes. These four stories illustrate the variety of DSR starting perspective industrial cases available to emerging academic institutions and businesses. Furthermore, there are substantial societal implications of this research. There has been a steady increase in the danger of cyber terrorism and cyber war in recent years, with many of the threats coming from groups with state backing. Cyber assaults are defined by Polite as "the premeditated, politically motivated attack on information, computer systems, computer programmers, and data that leads to crime against - anti aims by sub - national level organisations or covert agents." In contrast to the majority of cybercrime, which is motivated primarily by financial gain, cyberterrorism is driven by political goals. Governments may, for instance, improve their quick responses to threats like cyber espionage and cyber terrorism, which would assist strengthen their capacity to safeguard their population in online digital worlds. As a result, this problem significantly affects the effectiveness of any cyber security defence intended to maintain a secure online environment.

V. 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-cyberattack-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 Design Science 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. 75- 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. 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: a Typology," 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 the Developing 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.