A Data Analytics Approach To Cybercrime Underground Economy

Prithviraj[1], Sanjay B P[2], B R Vikas[3], Mr. Chethan Kumar B H[4]
[1, 2, 3] Dept of Information Science and Engineering
[4]Asst.Prof, Dept of Information Science and Engineering
[1, 2, 3, 4] East West Institute of Technology, Bangalore, 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 cybersecurity. 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 propose (1) a data analysis framework for analyzing the cybercrime underground, (2) CaaS and crimeware definitions, and (3) an associated classification model. In addition, we (4) 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- machine learning, crimeware, design science research

I. INTRODUCTION

As the threat posed by massive cyberattacks (e.g., ransomware and distributed denial of service attacks (DDoS)) and cybercrimes has grown, individuals, organizations, and governments have struggled to find ways to defend against them. In 2017, ransomware known as WannaCry was responsible for nearly 45,000 attacks in almost 100 countries [1]. The explosive impact of cybercrime has put governments under pressure to increase their cybersecurity budgets. United States President Barack Obama proposed spending over $19 billion on cybersecurity as part of his fiscal year 2017 budget, an increase of more than 35% since 2016 [2]. Global cyberattacks (such as WannaCry and Petya) are executed by highly organized criminal groups, and organized or national-level crime groups have been behind many recent attacks. Typically, criminal groups buy and sell hacking tools and services on the cybercrime black market, wherein attackers share a range of hacking-related information. This online underground market is operated by groups of attackers, and it in turn supports the underground cybercrime economy [3]. The cybercrime underground has thus emerged as a new type of organization that both operates black markets and enables cybercrime conspiracies to flourish. Because organized cybercrime requires an online network to exist and to conduct its attacks, it is highly dependent on closed underground communities (e.g., Hackforums and Crackingzilla). The anonymity these closed groups offer means that cybercrime networks are structured differently than traditional Mafia-style heirarchies [4], which are vertical, concentrated, rigid, and fixed. In contrast, cybercrime networks are lateral, diffuse, fluid, and evolving. Since cyberspace is a network of networks [5], the threat posed by the rise of highly professional network-based cybercrime business models, such as Crimeware-as-a-Service (CaaS), remains mostly invisible to governments, organizations, and individuals. Even though Information Systems (IS) researchers and practitioners are taking an increasing interest in cybercrime, due to the critical issues arising from the rapid increase in cyber threats, few have attempted to put this new interest on a solid foundation or develop suitable methodologies. Previous studies have not analyzed the underground economy behind cybercrime in depth. Furthermore, little is known about CaaS, one of the primary business models behind the cybercrime underground. There is an overall lack of understanding, both in research and practice, of the nature of this underground and the mechanisms underlying it. This research gap, and the practical problems faced by cybercriminals, motivates our study. We take a data analytics approach and investigate the cybercrime economy from a design science perspective. To achieve this goal, we (1) propose a data analysis framework for analyzing the cybercrime underground to guide researchers and practitioners; (2) define CaaS and crimeware to better reflect their features from both academic research and business practice perspectives; (3) use this to build a classification model for CaaS and crimeware; and (4) build an application to demonstrate how the proposed framework and classification model could be implemented in practice. We then evaluate this application by applying it in a case study, namely investigating the cybercrime economy by analyzing a large dataset from the online hacking community. This study takes a design science research (DSR) approach. Design science “creates and evaluates information technology artifacts intended to solve identified problems” [6]. DSR involves developing a range of IT artifacts, such as decision support systems, models, frameworks, tools, methods, and applications [7]. Where behavioral science research seeks to develop and justify theories that explain or predict human or organizational phenomena, DSR seeks to extend the boundaries of human and organizational capabilities by creating new and innovative artifacts [6]–[8]. DSR’s contribution is to add value to the literature and practice in terms of “design artifacts, design construction knowledge (e.g., foundations), and/or design evaluation knowledge (e.g., methodologies),” [7]. This study follows these DSR guidelines and contributes design artifacts, foundations, and methodologies [7]. In particular, DSR must demonstrate that design artifacts are “implementable” in the business environment to solve an important problem [7], so we provide an implementable framework rather than a conceptual one. We also create a front-end application as a case example to demonstrate how the proposed framework and classification model could be implemented in practice. In addition, this study contributes to design theory [9], [10]. As for foundations, DSR should have a creative development of constructs, models, methods, or instantiations that extend the design science knowledge base [7]. This study therefore adds to the knowledge base by providing foundational elements such as constructs (definitions, frameworks, and applications), a model (classification model), a method (analysis), and instantiations (applications).

As for methodologies, the creative development and use of evaluation methods provide DSR contributions [7]. Accordingly, this study uses dynamic analysis to conduct an ex-ante evaluation of the classification model. It also conducts an ex-post evaluation of a front-end application using observational methods (case examples). From a practical perspective, this study also provides practitioners with useful insights by making suggestions to guide governments and organizations in all industries in solving the problems they face when preparing for attacks from the cybercrime underground.

II. PROPOSED SYSTEM

In the proposed system there are two types of product or service are available in the cybercrime underground. The first can be either CaaS or crimeware that are related to attack strategy, for example, phishing, brute force, or DDoS attacks, or can be used for spamming or creating botnets, exploits, ransomware, rootkits, or Trojans. Attack strategies often exploit system vulnerabilities such as application loopholes. In addition, social engineering attacks exploit human vulnerabilities.

The most well-known example of such an attack is the use of a ``secret question" for password recovery: attackers check into the user's background to guess the secret question and hence steal the account. However, because social engineering is one of the oldest account hacking techniques, most account holders are now aware of it. In addition, social engineering-related products and services are rarely traded underground, although a few sellers have been known to sell tutorials. As a result, we have not included ``social engineering services" as a CaaS type.

The second type of product or service available neutralizes organizations' preventive measures, such as anti-virus programs. These are based on programs designed to evade anti-virus software to either cause mischief or be left behind for later activation. Examples include encryption and virtual private network (VPN) services, crypters, and proxies.

III. PROPOSED SYSTEM ARCHITECTURE

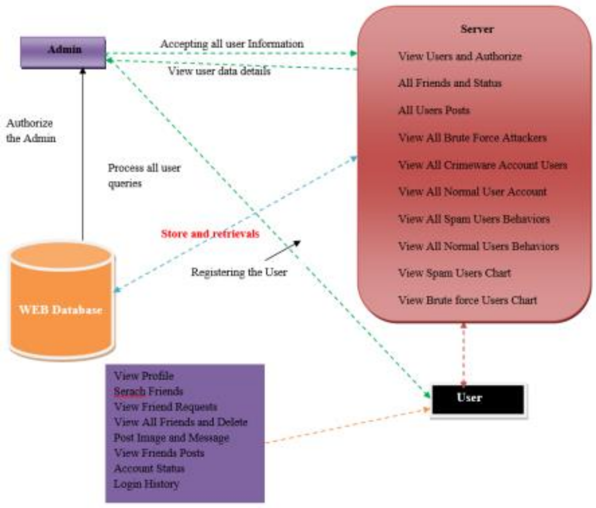


Fig. Proposed System Architecture

We take a data analytics approach and investigate the cybercrime economy from a design science perspective. To achieve this goal, we propose

- a data analysis framework for analyzing the cybercrime underground,
- CaaS and crimeware definitions, and

- an associated classification models. In addition, we
- develop an example application to demonstrate how the proposed framework and classification model could be implemented in practice.

criminal gatherings purchase and sell hacking devices and administrations on the cybercrime underground market, wherein aggressors share a scope of hacking-related data. This online black market is worked by gatherings of aggressors, and it thusly bolsters the underground cybercrime economy. The cybercrime underground has hence risen as another kind of association that both works bootleg trades and empowers cybercrime schemes to prosper. Since composed cybercrime requires an online system to exist and to direct its assaults, it is exceedingly subject to shut underground networks (e.g., Hackforums and Crackingzilla). The namelessness these shut gatherings offer implies that cybercrime systems are organized uniquely in contrast to conventional Mafia-style hierarchies, which are vertical, concentrated, inflexible, and fixed. Conversely, cybercrime systems are parallel, diffuse, liquid, and developing. Since the internet is a system of systems, the danger presented by the ascent of exceedingly proficient system-based cybercrime plans of action, for example, Crimeware-as-a-Service (CaaS), remains for the most part undetectable to governments, associations, and people. Despite the fact that Information Systems (IS) analysts and experts are taking an expanding enthusiasm for cybercrime, because of the basic issues emerging from the fast increment in digital dangers, few have endeavored to put this new enthusiasm on a strong establishment or create reasonable approaches. Past examinations have not investigated 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 research and practice, of the idea of this underground and the systems basic it.

Increasing crime day by day is the main issue facing human society. The crime occurs when the personal space or the workspace of the criminal and the target intersects at one point. The target may be one person or group of people or it can be a territory. The crime may be accidental or planned. The accidental crime is regrettable and unexpected. An unintended crime occurs in many places. The group of people fights with others because of a small issue that may harm people who have nothing to do with it. Planned crime is a crime committed intentionally. The person who intends to commit the offense, primarily research the target or target area and accordingly study them for implementation. Segregated places have greater chances of crime, with police patrols less than.

Earlier, data on crime are mostly police complaints, news reports and articles available in handwritten or printed form, but with technological development, crime data is available in hard copy as well as electronic version format. The previous scenarios differ with the low crime rate, and the data generated on criminal activities were also low. That the amount of less traditional data analysis techniques are effective data to analyze and predict crime. Previous data on criminal activities play a vital role in mapping crime and predicting where crime can occur. Analyzing those previously available data was a very tedious and time-consuming task by traditional data extraction techniques although data were much lower. Data generation nowadays is vast due to the increase in the crime rate, which cannot be addressed by conventional data analysis techniques. These large generated data are large data that can be easily processed with Big Data Analytics [2].

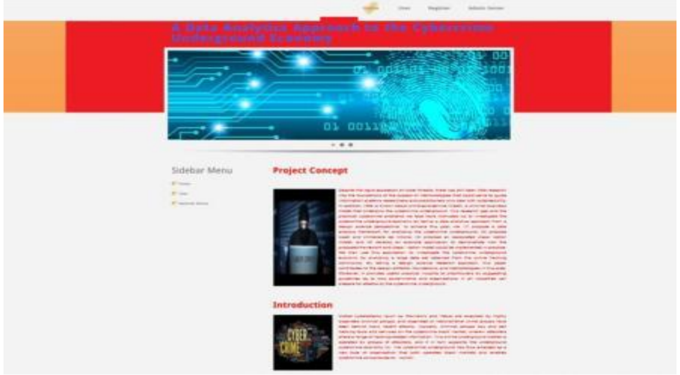
Digital data may be organized, semi-structured or unorganized. The digital data analyzed so far has been a systematic type of data to predict crime. Structured data can be considered as ordered data in tabular format with the help of appropriate rows and columns. Previous data is useful for predicting volatile places or saying hot spots. After applying some data extraction techniques such as aggregation, classification and other techniques, locations where there were more opportunities for crime were identified, and police capacity could be allocated there.

Many people can access this social networking site through iPhone, Android Phone, Tab, Laptop or other electronic gadgets. They can expertise their profile through posting any comment, uploading a photo, text or scrap posting, uploading of music and video in their profile to make the profile more attractive in front of their Facebook friends. By this site, users may choose to communicate through various digital objects are connected with friends who are staying far away from them. Facebook users are used to access this social networking site regularly or time to create personal profile is very easy on the home page on the Facebook and there must no longer be allotted any registration charge whilst some of the new users need to create their profile or join with others in the Facebook community.

By taking a design science research approach, this project 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.

IV. EXPERIMENTAL RESULTS

1. LOGIN PAGE


A Data Analytics Approach to the Cybercrime Underground Economy

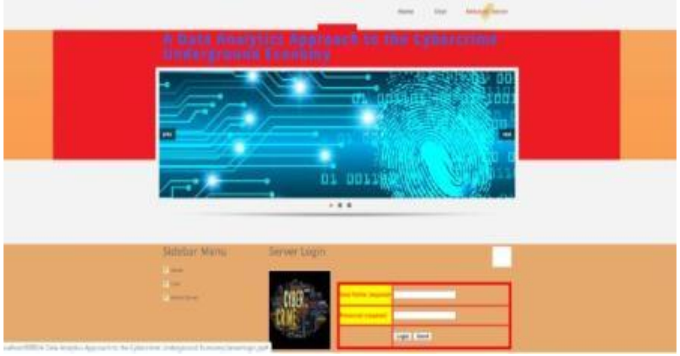
Project Concept

Introduction

Fig. 1 Login Page

The above screenshots depict about the login page of data analytics cybercrime this is how the front sheet looks like. It gives short description of project concept and introduction to cybercrime.

2. SERVER LOGIN


A Data Analytics Approach to the Cybercrime Underground Economy

Server Login

Fig. 2 Server Login

The above snapshots depict the server login. As authentication is necessary so we have server login we authorized server name and access identification is required. Then all the necessary credentials is given then login or reset button is given. once login is clicked the login happens.

3. SERVER MENU

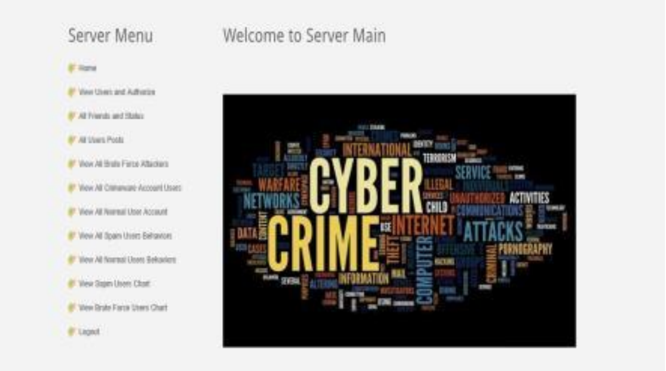
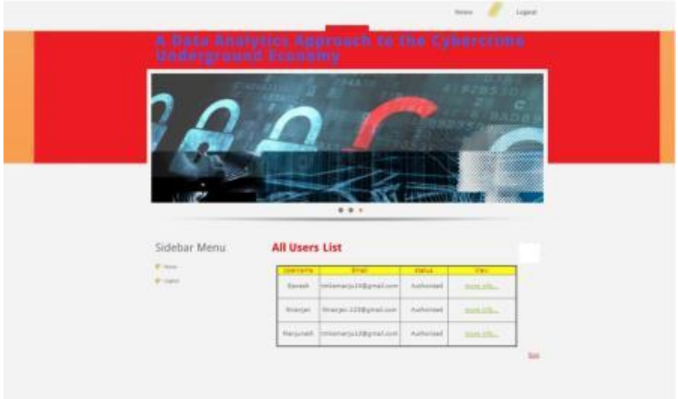

Welcome to Server Main
Server Menu
Home
View Users and Authorize
All Friends and Status
All Users Posts
View All Brute Force Attackers
View All Cotmaware Account Users
View All Normal User Account
View All Spam Users Behaviors
View All Normal Users Behaviors
View Spam Users Chart
View Brute Force Users Chart
Logout
CYBER
CRIME

Fig. 3 Server Menu

The above fig depicts the server menu once the server login occurs then the server menu will be logged into that has menu tab and other server menu bars are present then the server can login to it and works accordingly. Cyber crime can be avoided if security is maintained.

4. USERS LIST


A Data Analytics Approach to the Cybercrime Underground Economy

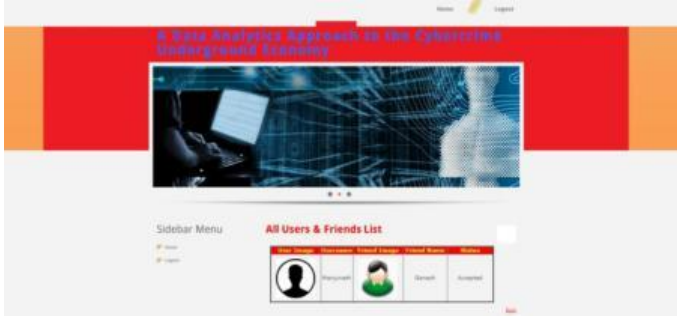
All Users List

Username	Email	Status	View
Ganesh	[illegible]@gmail.com	Authorized	more info...
[illegible]	[illegible]@gmail.com	Authorized	more info...
Manjunath	[illegible]@gmail.com	Authorized	more info...

Fig. 4 Users List

The above screenshot depicts the users list that is number of user list login along with their necessary details and other requirements will be taken and accessed.

5. USERS AND FRIENDS LIST


A Data Analytics Approach to the Cybercrime Underground Economy

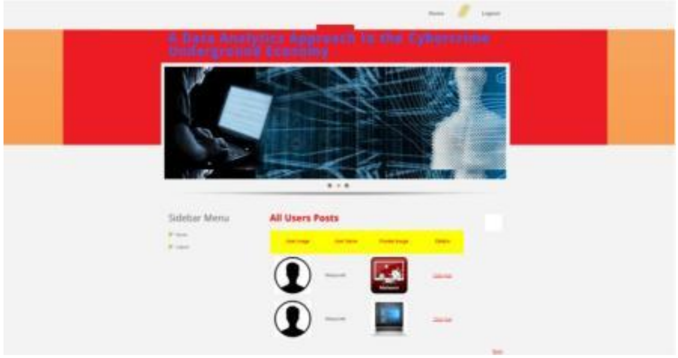
All Users & Friends List

User Image	Username	Friend Image	Friend Name	Status
	Manjunath		Ganesh	Accepted

Fig. 5 Users and Friends List

The above fig depicts the users and friends list which ever account we want to access if we have the necessary bank credentials, we can easily login. They have all users and friends list.

6. USERS POST



A Data Analytics Approach to the Cybercrime Underground Economy

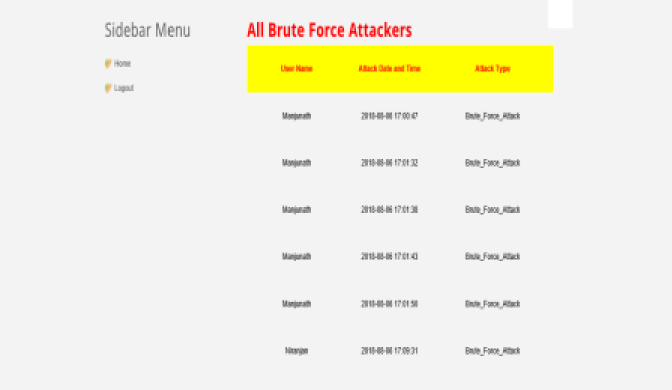
Sidebar Menu

All Users Posts

Fig. 6 Users Post

The figure depicts the users post the server will have a backup of all the data that is available and the previous users who have used it. The details will be stored.

7. BRUTE FORCE ATTACKERS



Sidebar Menu

Home

Logout

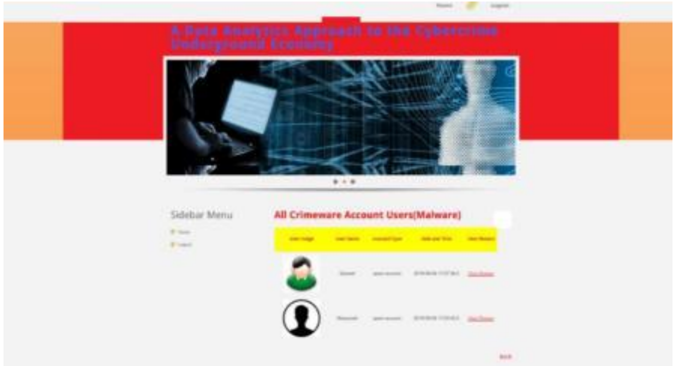
All Brute Force Attackers

User Name	Attack Date and Time	Attack Type
Manjunath	2018-08-06 17:00:47	Brute_Force_Attack
Manjunath	2018-08-06 17:01:32	Brute_Force_Attack
Manjunath	2018-08-06 17:01:38	Brute_Force_Attack
Manjunath	2018-08-06 17:01:43	Brute_Force_Attack
Manjunath	2018-08-06 17:01:58	Brute_Force_Attack
Niranjan	2018-08-06 17:09:31	Brute_Force_Attack

Fig. 7 Brute Force Attackers

The figure Brute Force attackers and all the necessary details of the cyber-crime we can easily find out and the details will be available. We can have a look at details this can easily find out the cyber crime.

8. CRIMEWARE ACCOUNT USERS



A Data Analytics Approach to the Cybercrime Underground Economy

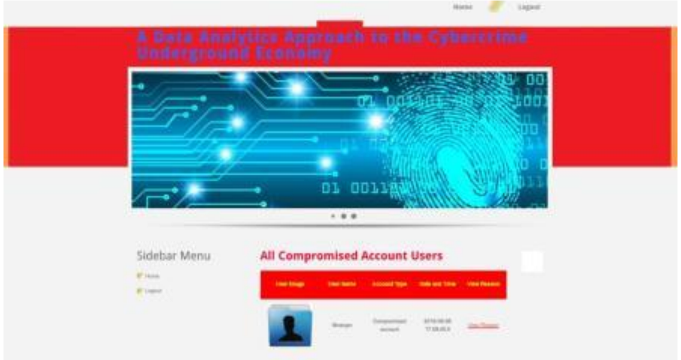
Sidebar Menu

All Crimeware Account Users(Malware)

Fig. 8 Crimeware Account Users

In case if there are other crime ware account users we can easily identify them through this page. It is easy to know who had logged in and other issues.

9. COMPROSMISED ACCOUNT USERS



A Data Analytics Approach to the Cybercrime Underground Economy

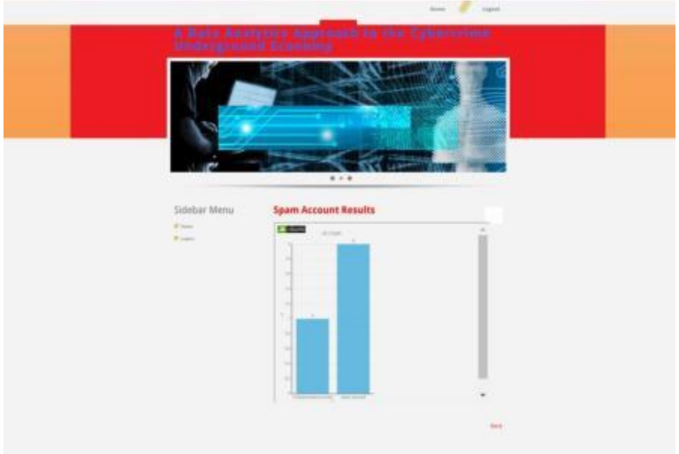
Sidebar Menu

All Compromised Account Users

Fig. 9 Comprosmised Account Users

The above figure depicts the compromised account users who had to use the web page but due to malware and unwanted account users. These users are compromised.

10. SPAM ACCOUNT RESULTS



A Data Analytics Approach to the Cybercrime Underground Economy

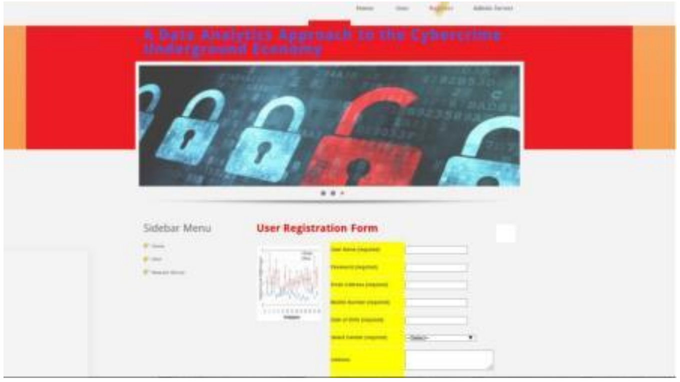
Sidebar Menu

Spam Account Results

Fig. 10 Spam Account Results

The above snapshots depicts the spam account results how many unwanted or malicious users have used the account and how it's been detected and identified and cleared it.

11. USER REGISRATION FORM



A Data Analytics Approach to the Cybercrime Underground Economy

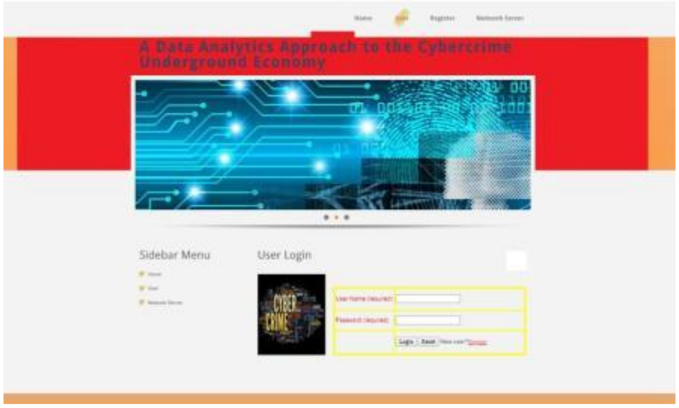
Sidebar Menu

User Registration Form

Fig. 11 User Registration Form

The above snapshots depicts the user registration form which has all the necessary details about the new customers and new registers who has to enroll there details will be stored in the database so that if unauthorized people access it they can be caught.

12. USER LOGIN



A Data Analytics Approach to the Cybercrime Underground Economy

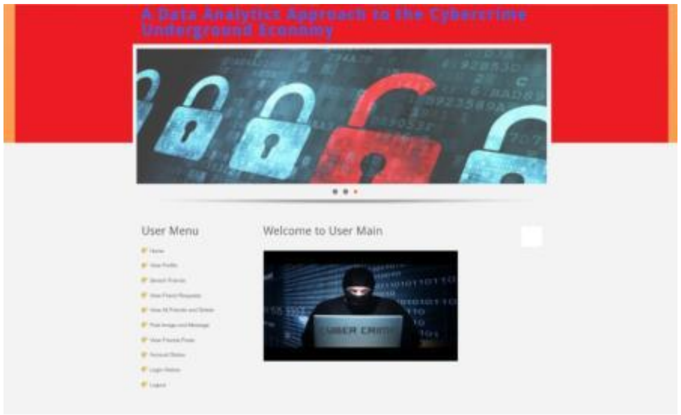
Sidebar Menu

User Login

Fig. 12 User Login

The above snapshots tells the user login and password and we can easily login.

13. USER MENU



A Data Analytics Approach to the Cybercrime Underground Economy

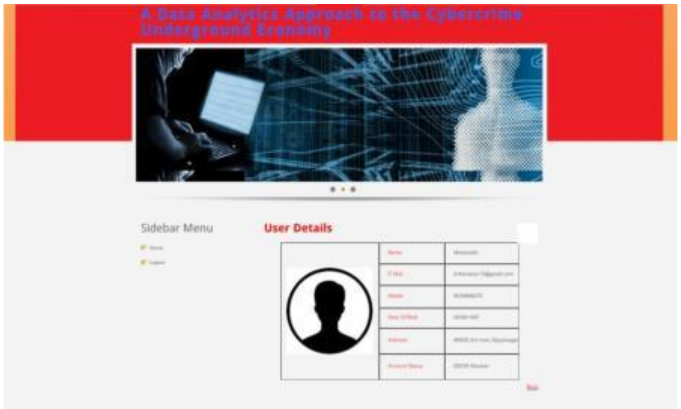
User Menu

Welcome to User Main

Fig. 13 User Main

The above snapshots tell the user main so that cyber-crime is easily found out.

14. USER DETAILS



A Data Analytics Approach to the Cybercrime Underground Economy

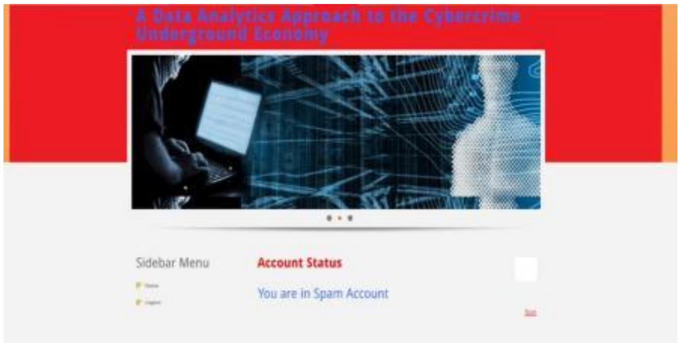
Sidebar Menu

User Details

Fig. 14 User Details

The above figure depicts the user details how many user details will be provided.

15. ACCOUNT STATUS



A Data Analytics Approach to the Cybercrime Underground Economy

Sidebar Menu

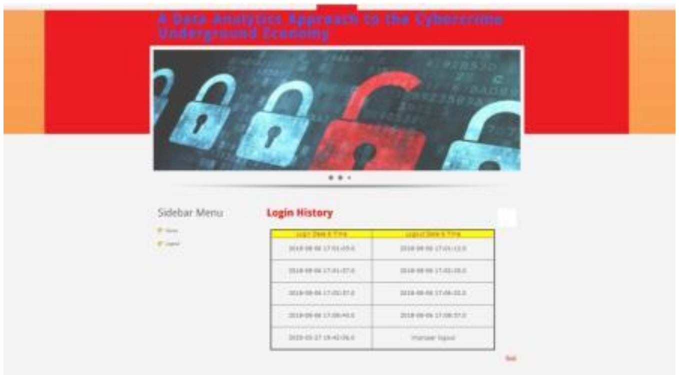
Account Status

You are in Spam Account

Fig. 15 Account Status

The above fig depicts account status of the malicious users.

16. LOGIN HISTORY



A Data Analytics Approach to the Cybercrime Underground Economy

Sidebar Menu

Login History

Login Date & Time	Logout Date & Time
2018-08-06 17:01:05.0	2018-08-06 17:01:13.0
2018-08-06 17:01:27.0	2018-08-06 17:02:20.0
2018-08-06 17:02:37.0	2018-08-06 17:06:22.0
2018-08-06 17:08:40.0	2018-08-06 17:08:37.0
2019-03-17 19:42:26.0	improper logout

Fig. 16 Login History

The above snapshots depict the login history of the users.

VI. CONCLUSION

Any intelligent device that can pass data to one or more other devices (either through a network or not) is encompassed within the scope of Cyber Security that includes pretty much the entire foundation of modern society. All need to be aware of cyber security as well as cybercrimes and its causes. There is little seriousness about security regarding online, social and other activities through which probability of risk will be higher. The cybercrime underground economy is to be investigated by taking a data analytics approach from a design science perspective. The cyber-attack and its association on national Security is analyzed with the data mining approaches. The economic impact mainly affects the national security. We have therefore proposed two artifacts: a data analysis framework and a classification model that is to be implemented in next phase.

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. 75105, 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.