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 propose (1) a data analysis framework for analyzing the cybercrime underground, (2) CaaS and crime ware 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 underground market where illegal services are provided to help underground buyers conduct cybercrimes, such as attacks, infections, and money laundering in an automated manner,". Thus, CaaS is referred to as a do-it-for-me service, unlike crimeware which is a do-it-yourself product. Because CaaS is designed for novices, its customers do not need to run a hacking server or have high-level hacking skills. Consequently, the CaaS business model can involve the following roles: writing a hacking program, performing an attack, commissioning an attack, providing an attack server (infrastructure), and laundering the proceeds. Sood and Enbody have suggested that crimeware marketplaces have three key elements, namely actors (e.g., coders, operators, or buyers), value chains, and modes of operation (e.g., CaaS, pay- per-install, crimeware toolkits, brokerage, or supplying data). Periodic monitoring and analysis of the content of cybercrime marketplaces could help predict future cyber threats.

Chapter 1

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

. 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.

The cybercrime underground has thus emerged as a new type of organization that both operates black markets and enables cybercrime conspiracies to flourish.In contrast, cybercrime networks are lateral, diffuse, fluid, and evolving.

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.

1.1 Motivation:

To achieve this goal, we propose (1) a data analysis framework for analyzing the cybercrime underground,(2) CaaS and crime ware 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.

1.2 Objectives:

This project 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 crimeware available in the cybercrime underground, but much in-depth analysis remains to be done on the configurations of cybercrime networks.

1.2.1 Advantages:

- Compelling and relevant content will grab the attention of potential customers and increase brand visibility.
- You can respond instantly to industry developments and be seen as 'thought leader' or expert in your field.
- This can improve how your business is seen by your audience.
- Positive feedback is public and can be persuasive to other potential customers.
- Negative feedback highlights areas where you can improve

The goal of the proposed framework is to "investigate the cybercrime underground economy." This Crimeware marketplaces have three key elements, namely

1.actors (e.g., coders, operators, or buyers),

2.value chains, and

3.modes of operation (e.g., CaaS, pay-per-install, crimeware toolkits, brokerage, or supplying data). Data mining is a technique used to mine out patterns of useful data from large data sets

1.2.2 Disadvantage:

- It is not secured process.
- Over under traction is invents
- Download files, time is invited

The cyber-crime differs from general crime in many ways; we need to conduct a variety of analyses using a large data set. A previous study proposed a data mining framework for crime, dividing crimes harmful to the general public into eight categories:

1.Traffic violations. 5.Gang/Drug Offenses.

2. Sex Crime. 6. Arson.

3. Theft. 7. Violent crime.

4. Fraud. 8.Cyber-crime.

Although this previous study explained how data mining techniques could be applied to crime analysis, it did not consider the specific features of cyber-crime.

1.3 FEASIBILITY STUDY:

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are,

- ECONOMICAL FEASIBILITY
- TECHNICAL FEASIBILITY
- SOCIAL FEASIBILITY

1.3.1 ECONOMICAL FEASIBILITY

This study is carried out to check the economic impact that the system will haveon the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customizedproductshad to be purchased.

1.3.2 TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands

being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required.

1.3.3 SOCIAL FEASIBILITY

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it.

Chapter 2

LITERATURE SERVEY:

Cybercrime has undergone a revolutionary change, going from being product-oriented to service-oriented because the fact it operates in the virtual world, with different spatial and temporal constraints, differentiates it from other crime taking place in the physical world As part of this change, the cybercrime underground has emerged as a secret cybercrime marketplace because emerging technological changes have provided organized cybercriminal groups with unprecedented opportunities for exploitation The cybercrime underground has a highly professional business model that supports its own underground economy . This business model, known as CaaS, is "a business model used in the underground market where illegal services are provided to help underground buyers conduct cybercrimes, such as attacks, infections, and money laundering in an automated manner," . Thus, CaaS is referred to as a do-it-for-me service, unlike
crimeware which is a do-it-yourself product. Because CaaS is designed for novices, its customers do not need to run a hacking server or have high-level hacking skills. Consequently, the CaaS business model can involve the following roles: writing a hacking program, performing an attack, commissioning an attack, providing an attack server (infrastructure), and laundering the proceeds. Sood and Enbody have suggested that crimeware marketplaces have three key elements, namely actors (e.g., coders, operators, or buyers), value chains, and modes of operation (e.g., CaaS, pay-per-install, crimeware toolkits, brokerage, or supplying data). Periodic monitoring and analysis of the content of cybercrime marketplaces could help predict future cyber threats . In criminology, routine activity theory (RAT) is used to explain the causes of crime, both general criminal activity and cybercrime .

According to this theory, three elements are necessary for crimes to be committed:

(1) a likely offender,

(2) a suitable target, and

(3) the absence of capable guardians against crime.

In a cybercrime context, the "likely offenders" are motivated sellers and potential buyers in the underground market, and the "suitable targets" are the targeted vulnerable organizations. The "absence of capable guardians against crime" is due to organizations failing to take preventive measures against

cybercrime. 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. Examples include encryption and virtual private network (VPN) services, crypters, and proxies. From the perspective of RAT, the likely offenders are attackers motivated to attack organizations or products that constitute a suitable target. If such targets are attacked, however, both the targets and those who supply their cybersecurity products become aware of the vulnerabilities that made the attack possible, leading them to apply security updates to their software.

These updates can be seen as capable guardians against crime, and the preventive measures taken can be identified by looking through each program's version history. However, this is not the end of the matter, because the attackers will then develop and sell new versions of their hacking tools to combat the guardians, thus re-establishing the third RAT condition, the absence of capable guardians against crime. Such events can also be identified by the version numbers of the hacking tools sold on the black market: since it is an online marketplace, attackers must give detailed explanations to retain their customers' confidence.

2.1 Comparative analysis:

For a number of years, policy-makers at the highest levels have been expressing their concerns that insecure information systems threaten economic growth and national security. As a result of theseconcerns, a complex and overlapping web of national, regional, and multilateral initiatives has emerged. A recent publication offers a compilation and analysis of cybersecurity efforts in fourteen countries.76 The International CIIP Handbook provides an overview of issues of high importance inthe field of critical information infrastructure protection (CIIP), serves as a reference work for the interested community, and provides a basis for further research by compiling relevant material. In this chapter, the main findings of this volume are presented. We are focusing mainly on five focal points of high importance that emerged from a cross-comparison of country surveys:

1. **Critical Sectors**: This section compares critical infrastructure sectors as identified by therespective countries. To look at the concept of critical infrastructures is important, becausecybersecurity has

emerged in parallel to CIP in all countries.

2. Organizational Overview: The second part of this chapter provides an overview of important public actors in the national cybersecurity organizational framework. It only characterizes the specific responsibilities or public actors at the state (federal) level (such as ministries, national offices, agencies, coordination groups, etc.). Public actors at the lower state level and private actors (companies, industry, etc.) are not taken into account.

3. Early Warning Approaches: The third section describes national organizations responsible for cyber-early warning, namely cybersecurity-related information-sharing organizations such asCERTs (Computer Emergency Response Teams), ISACs (Information Sharing and Analysis Centers), etc.

4. Current Topics in Law and Legislation: The development of effective regulations, laws, and criminal justice mechanisms is essential in deterring virtual abuse and other offences against the information infrastructure. Moreover, a strict regulation may create trust in the new ICT and encourage the private sector and individuals to make better use of e-Commerce or e-Government services.

5. Research and Development: The last section gives an overview of recent efforts in Research and Development (R&D) concerning cybersecurity.

2.2 RESULTS AND INFERENCE DRAWN :

The data analysis step of the proposed framework involves four steps. Here, we report the data analysis results: CaaS and crimeware classification and market trends, cybercrime market dynamics, and potential hacking targets.

CaaS and Crimeware Classification and Market Trends

Here, we evaluate the accuracy of the proposed classifications. Specifically, we analyze the CaaS and crimeware trends between 2008 and October 2017 based on these classifications. the most common classes overall were botnets (17%) and exploits (17%). The most popular classes in 2017 were botnets (33%), VPN services (20%), exploits (13%), and brute force attack services (7%).

To validate our classification model, we used a confusion matrix, a common method of calculating classifier output accuracy. The training and testing datasets comprised 300 and 700 items, respectively. This gave an accuracy of 82.6% with a 95% confidence interval of (70.74%, 81.24%) for identifying the risks posed by CaaS- and crimewarerelated messages. There

Chapter 3

EXISTING SYSTEM

Cybercrime has undergone a revolutionary change, going from being product-oriented to service-oriented because the fact it operates in the virtual world, with different spatial and temporal constraints, differentiates it from other crime taking place in the physical world. As part of this change, the cybercrime underground has emerged as a secret cybercrime marketplace because emerging technological changes have provided organized cybercriminal groups with unprecedented opportunities for exploitation.

The cybercrime underground has a highly professional business model that supports its own underground economy. This business model, known as CaaS, is "a business model used in the underground market where illegal services are provided to help underground buyers conduct cybercrimes, such as attacks, infections, and money laundering in an automated manner,".

Thus, CaaS is referred to as a do-it-for-me service, unlike crimeware which is a do-it-yourself product. Because CaaS is designed for novices, its customers do not need to run a hacking server or have high-level hacking skills.

Consequently, the CaaS business model can involve the following roles: writing a hacking program, performing an attack, commissioning an attack, providing an attack server (infrastructure), and laundering the proceeds.

Sood and Enbody have suggested that crimeware marketplaces have three key elements, namely actors (e.g., coders, operators, or buyers), value chains, and modes of operation (e.g., CaaS, pay-per-install, crimeware toolkits, brokerage, or supplying data). Periodic monitoring and analysis of the content of cybercrime marketplaces could help predict future cyber threats.

3.1 PROPOSED SYSTEM:

The goal of our data analysis framework is to conduct a big-picture investigation of the cybercrime underground by covering all phases of data analysis from the beginning to the end. This framework comprises four steps: (1) defining goals; (2) identifying sources; (3) selecting analytical methods; and (4) implementing an application. Because this study emphasizes the importance of RAT for analyzing the cybercrime underground, the proposed RAT-based definitions are critical to this

framework: **Steps 1–4** all contain the RAT elements

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.**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 captcha's and anti-crawling scripts to gather the necessary data. We collected a total of 2,672,091 posts selling CaaS or crimeware, made between August 2008 and October 2017, from a large hacking community site (www.hackforums.net) with over 578,000 members and more than 40 million posts. We also collected 16,172 user profiles of sellers and potential buyers, based on their communication histories, as well as prices and questions and answers about the transactions. The black market uses traditional forum threads (e.g., bulletin boards) instead of typical e-commerce platforms (e.g., eBay, and Amazon). For example, sellers create threads in marketplace forums to sell items, and potential buyers comment on these threads. One of the most significant challenges was therefore converting this unstructured data into structured data.

Chapter 4

SYSTEM REQUIREMENTS SPECIFICATION

A **Software Requirements Specification (SRS)** is a document that describes the nature of a project, software or application. In simple words, SRS document is a manual of a project provided it is prepared before you kick-start a project/application. This document is also known by the names SRS report, software document. A software document is primarily prepared for a project, software or any kind of application.

There are a set of guidelines to be followed while preparing the software requirement specification document. This includes the purpose, scope, functional and nonfunctional requirements, software and hardware requirements of the project. In addition to this, it also contains the information about environmental conditions required, safety and security requirements, software quality attributes of the project etc.

The system requirement and specification of our project is as follows:

4.1 Function Requirements:

4.1.1 Purpose of the requirements document

A requirements document is a document containing all the requirements to a certain product. It is written to allow people to understand *what* a product should do. Purpose and ((scope, from both a technical and business perspective.Product overview and use cases Requirements, including functional requirements (e.g. what a product should do) usability requirements technical requirements (e.g. security, network, platform, integration, client) environmental requirements support requirements interaction requirements (e.g. how the product should work with other systems) Assumptions Constraints Dependencies

4.2 Non-functional requirements:

4.2.1 Practicality

Project practicality is where you use only what is viewed as least needed to meet your goals.A communication system like tis needs hundreds of thousands of users to survive and thrive. Therefore, it should be designed to support large numbers of users, e.g., a substantial percent of a town or a campus.

4.2.2 Efficiency

Efficiency measures how well and productively a manger uses his resources to achieve goals. Project management places heavy focus on how to acquire the right project team to perform project tasks and to close project successfully within the agreed constraints.

4.2.3 Cost

Cost management is concerned with the process of planning and controlling the budget of a project or business. It includes activities such as planning, estimating, budgeting, financing, funding, managing, and controlling costs so that the project can be completed within the approved budget. Cost management covers the full life cycle of a project from the initial planning phase towards measuring the actual cost performance and project completion.

4.2.4 Flexibility

The need for flexibility is to deal with changed circumstances. Flexibility is used to scale back activities needing less effort while diverting resources to areas with unexpected problems.

4.2.5 Modularity

Modularity refers to the concept of making multiple modules first and then linking and combining them to form a complete system. Modularity enables re-usability and minimizes duplication. In addition to re-usability, modularity also makes it easierto fix problems as bugs can be traced to specific system modules, thus limiting the scope of detailed error searching

4.2.6 Extensibility

Extensibility is a software engineering and systems design principle where the implementation takes future growth into consideration. The term extensibility can also be seen as a systemic measure of the ability to extend a systemand the level of effort required to implement the extension. Extensions can be through the addition of new functionality or through modification of existing functionality.

4.2.7 Reliability

Reliability refers to the probability and or the likelihood that a given product will perform in the way and or manner it was intended to perform in the efforts that have been deemed required of that given product within or under a specific period of time required.

4.2.8 Maintainability

It is the probability that a system or system element can be repaired in a defined environment within a specified period of time. Increased maintainability implies shorter repair times.

4.2.9 Portability

It is a measure of how easily an application can be transferred from one computer environment to another. A computer software application is considered portable to a new environment if the effort required to adapt it to the new environment is within reasonable limits. The phrase "to port" means to modify software and make it adaptable to work on a different computer system.

4.3 SOFTWARE REQUIREMENTS:

Operating system : Windows 10 ,Linux

Coding Language : Python.

Front-End Designing : Python, Html , css , javascript.

Data Base : MySQL.

Domain : Machine Learning and Data Analytics.

4.2 HARDWARE REQUIREMENTS:

System: Intel i3 2.4 GHz.

Hard Disk: Min 100 GB.

Monitor: 14’ Colour.

Mouse: Optical Mouse.

Ram : Min 2 GB.

Summary:

A software requirements specification is a description of a software system to be developed. The software requirements specification lays out functional and non-functional requirements, It should also provide a realistic basis for estimating product costs, risks, and schedules. Used appropriately, software requirements specification scan help prevent software project failure.

Chapter 5

ARCHITECTURE:

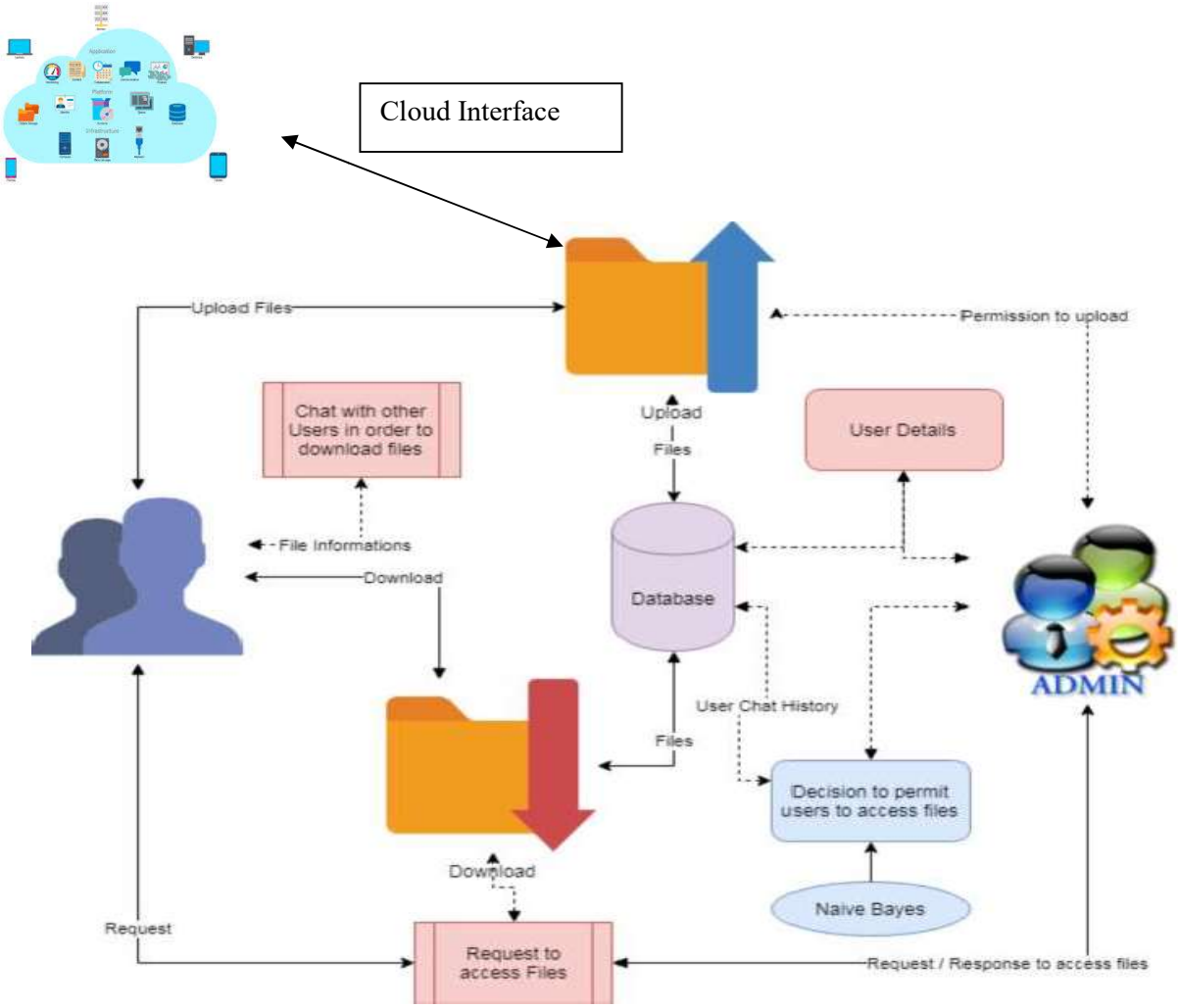


Figure 6.0:Architecture of proposed model.

- Step 1:User upload

  Users upload their data through any media to the database or cloud server.

- Step 2:Admin process.:Admin response for the request and process data.
- Step 3:Decisions to provide access

  Using algorithm for decision making and provide access to requested customers.

- Step 4:Download access files.

  Tracking of files and download the requested files.

5.1 MODULES:

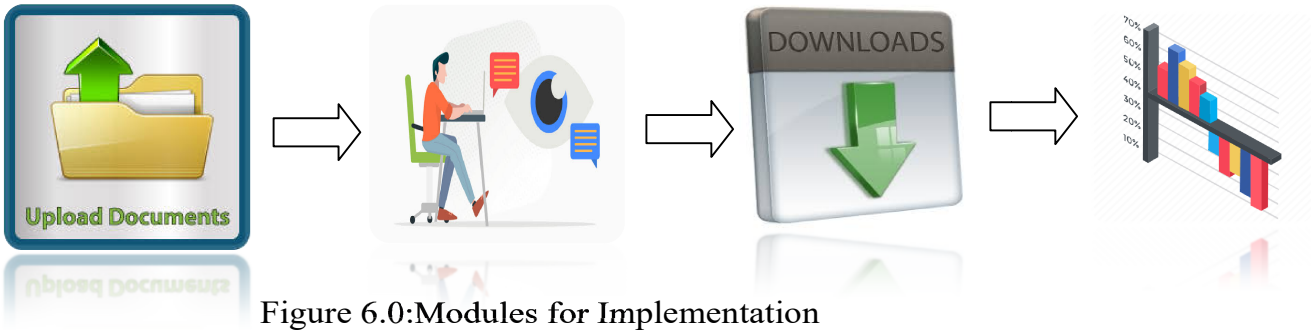


Figure 6.0:Modules for Implementation

Modules that are Implementing this system include the following,

1.Upload Files

Users are allowed to upload the files with the tags given. Once the file is uploaded, then it is sent to approval from admin to publish or make view to other users. These uploaded files can be in any form document, audio or video but not allowed to upload the executable (.exe) files.

2.Conversation Monitoring

Users are allowed to communicate among the other users. This could be monitor by the admin. The malicious conversion likes to threaten the data. In order to protect the cybercrime and prevents from forming cybercrime community. This can be achieved by the help of classification algorithm named naïve Bayes classification.

3.Download Files

The files can be downloading by requesting for the file and once admin approved the files then can be downloadable. The decision to approve files can be taken from the conversation between users. Admin takes the action on download files and approvable status of users. The users are allowed further actions based on the users.

4.Graphical Representations

The analyses of proposed systems are calculated based on the approvals and disapprovals. This can be measured with the help of graphical notations such as pie chart, bar chart and line chart. The data can be given in a dynamical data.

Chapter 6

ALGORITHM

6.1Naive Bayes Classifier:

Naive Bayes is a classification algorithm for binary (two-class) and multi-class classification problems. The technique is easiest to understand when described using binary or categorical input values. It is called naive Bayes or idiot Bayes because the calculation of the probabilities for each hypothesis is simplified to make their calculation tractable. Rather than attempting to calculate the values of each attribute value P(d1, d2, d3|h), they are assumed to be conditionally independent given the target value and calculated as P(d1|h) * P(d2|H) and so on.This is a very strong assumption that is most unlikely in real data, i.e. that the attributes do not interact. Nevertheless, the approach performs surprisingly well on data where this assumption does not hold.

Make Predictions with a Naive Bayes Model:

Given a naive Bayes model, you can make predictions for new data using Bayes theorem.

MAP (h) = max(P(d | h) * P(h))

Using our example above, if we had a new instance with the weather of sunny, we can calculate:

go-out = P(weather=sunny | class=go-out) * P(class=go-out) stay-home = P(weather=sunny| class=stay- home) * P(class=stay-home)

We can choose the class that has the largest calculated value. We can turn these values into probabilities by normalizing them as follows:

P(go-out | weather=sunny) = go-out / (go-out + stay-home) P(stay-home | weather=sunny) = stay-home / (go-out + stay-home)

If we had more input variables we could extend the above example. For example, pretend we have a "car" attribute with the values "working" and "broken". We can multiply this probability into the equation.

For example below is the calculaion for the "go-out" class label with the addition of the car input variable set to "working":

go-out = P(weather=sunny | class=go-out) * P(car=working | class=go-out) * P(class=go-out)

Chapter 7

SYSTEM DESIGN AND IMPLEMENTATION

7.0 DESIGN:

- In contrast, the goal of our data analysis framework is to conduct a big-picture investigation of the cybercrime underground by covering all phases of data analysis from the beginning to the end (see Fig. 1). This framework comprises four steps: (1) defining goals; (2) identifying sources; (3) selecting analytical methods; and (4) implementing an application.
- The data analysis step of the proposed framework involves four steps. Here, we report the data analysis results: CaaS and crimeware classification and market trends, cybercrime market dynamics, and potential hacking targets.

A. CaaS and Crimeware Classification and Market Trends .

B. Cybercrime Market Dynamics

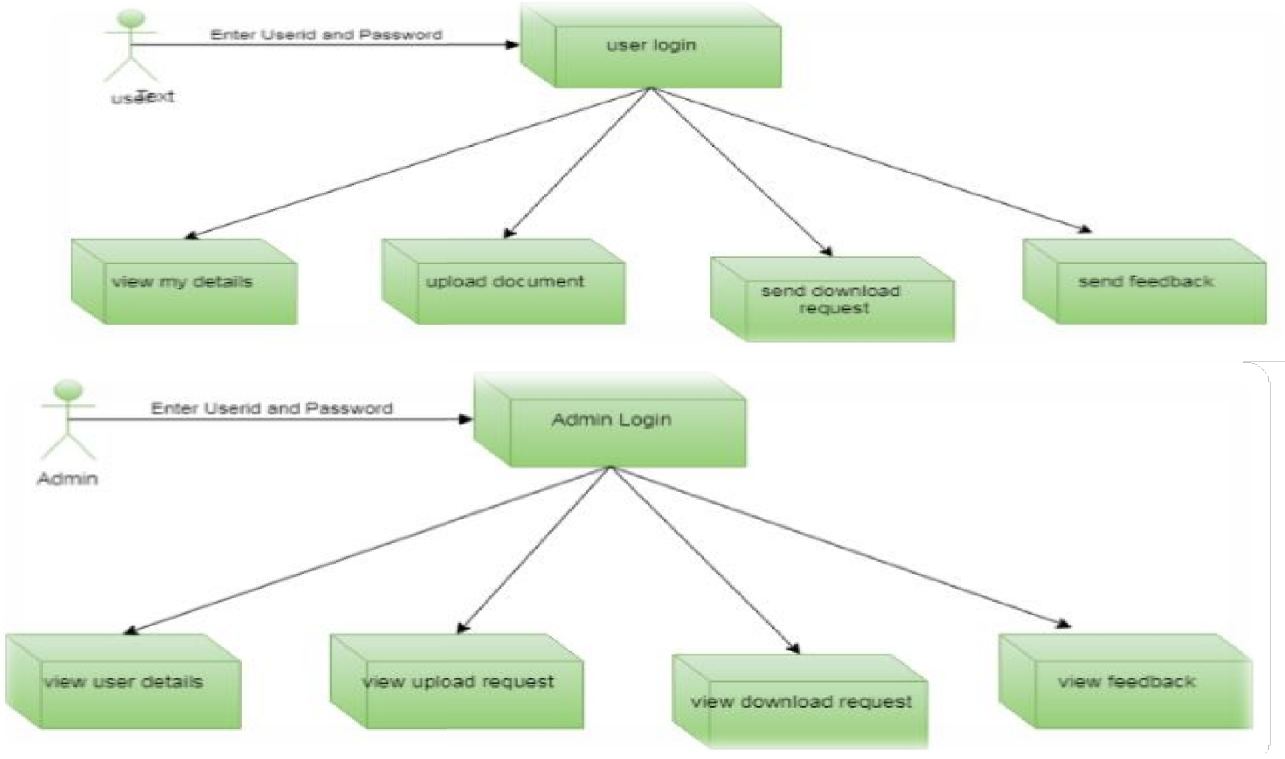
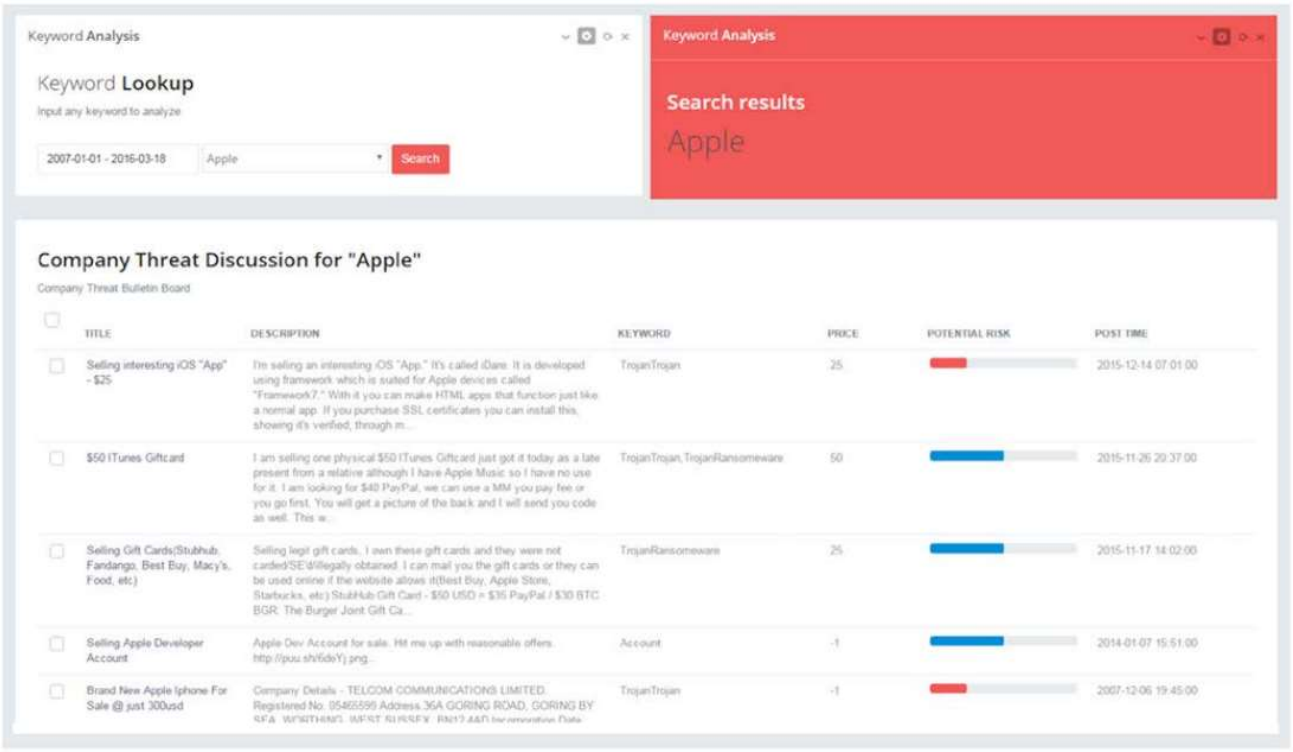


Figure7.0: System Design Modules.



(a)

Car Hacking - Reaper590 - **07-05-2011 06:20 PM**

I just read that it is possible to hack cars. This totally makes sense. So, I wonder if anyone has ever done it. One guy says he hack his 2006 Impala with an Android phone and some code he made. Others plug machines into the cable underneath the dashboard. It's even possible to attach virus code to a mp3 and once in the CD player it will do its job.

Why would you do this you may ask. Well you could start cars, turn off security systems, turn off brakes, and many other things.

So I'm wondering if anyone has done this or knows how to do it. Especially with an Android.

***** - DDoS ViRuS - **07-06-2011 06:14 PM**

This depends very much on the car itself. Old cars with very little electronics don't allow you do do much of anything. Newer cars you can do more with because electronics control more of the system. The Nissan Leaf allows you to connect to RSS feeds in your car but every time it sends a request it gives the website real-time about your car such as its location, driving history, power consumption, and battery reserves. That is just it sending out info. On most cars however information isn't broadcasted like this but you can still hack its electronic computer units. On most cars you need physical access to do this using the diagnostic port or whatever it is (usually under the dash on the drivers side) I actually have a device that reads real-time information from this and sends it to my phone. On newer cars this is sometimes becoming wireless instead of needing to have physical access to it. While this makes it easier to get the diagnostic information it makes it very easy for hackers to compromise. Here is an article on it http://www.infosecurity-us.com/view/12270/car-hacking-goes-wireless-as-modern-vehicles-open-to-hacke

(b)

Nissan Leaf electric cars hack vulnerability disclosed

By Leo Kelion
Technology desk editor

24 February 2016 | Technology

BBC

Some of Nissan's Leaf cars can be easily hacked, allowing their heating and air-conditioning systems to be hijacked, according to a prominent security researcher.

Troy Hunt reported that a flaw with the electric vehicle's companion app also meant data about drivers' recent journeys could be spied on.

Mr Hunt said he gave the firm a month to fix the issue before he decided to make it public.

Nissan said there was no safety threat.

The problem remains unresolved but Mr Hunt said car owners could protect themselves by disabling **their Nissan CarWings account**. Those who have never signed up are not at risk.

(c)

Figure7.1 Hacking vulnerability disclosed and the earlier signal from the underground: (a) monitoring system. (b)relevant result (July 6, 2011). (c)BBC news (Feb. 24, 2016).

Chapter 8

FUTURE WORK

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 crimeware 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.

Implications for Research :

This study contributes to the DSR literature in a broader IS context in several ways. Because it takes a DSR approach, it contributes to the design artifacts, foundations, and methodologies in this area [6]–[8]. First, by creating example front-end applications, we have demonstrated how our design artifacts (the proposed framework and classification model) can be implemented in practice. Despite the rapidly growing threat from cybercrime, there has been little research into practical frameworks for future cybersecurity researchers: the previous studies have not attempted to analyze the data or take a systematic modeling approach [3], [58]–[62]. In DSR, we must demonstrate that the artifacts can be implemented in a business environment for them to qualify as solving an important unsolved problem [7]. We have therefore provided an implementable framework, not just a conceptual one.

Implications for Practice :

From a RAT perspective, the practical implications of this study mainly affect the capable guardians against crime, because our results indicate how underground attackers perceive preventive measures. A previous review of the current status of legal, organizational, and technological efforts to combat

cybercrime in different countries relied on a case study of the work being done in Taiwan [64]. It made four recommendations for governments, lawmakers, international organizations, intelligence and law enforcement agencies, and researchers:

(1) regularly update existing laws;
(2) enhance specialized task forces;
(3) use civil resources; and
(4) promote cybercrime research.

The practical implications of our study are based on those of the previous study [64]. We have already discussed the fourth recommendation ("promote cybercrime research") in the previous section, so we will now focus on the other three areas.

First, our study has implications for governments and lawmakers in that it recommends existing laws be regularly updated. The proposed CaaS and crimeware definitions and classification model may improve national defense and security by suggesting potential government roles and the adoption of particular regulatory policies.

Second, the proposed data analysis framework can be used to enhance specialized task forces. This study suggests that organizations in all industries should attempt to gain a deeper understanding of the nature of the cybercrime underground.

For example, they should be aware that there are cybercrime underground markets where hacking tools are sold.

Third, this study calls for researchers, companies, antivirus vendors, and governments to collaborate in the fight against cybercrime using civil resources. Rather than acting alone, these groups should unite to maximize their efficiency and effectiveness.

Finally, this study also has important implications for society. Over the last few years, the world has been facing cyber terrorism and cyberwar threats from nation-sponsored attackers [70]. Pollitt [71] defined cyber terrorism as "the premeditated, politically motivated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by subnational groups or clandestine agents." Unlike most cybercrime, which is primarily motivated by monetary gain [72], cyber terrorists are politically motivated. As a result, governments should, for example, strengthen their ability to protect their citizens in online virtual environments by enhancing their immediate responses to threats such as cyber espionage and cyber terrorism.

CONCLUSION

Because this study takes a DSR approach, 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, crypting, and VPN services) and crime ware (drive-by download, botnets, exploits, ransomware, rootkits, Trojans, crypters, 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 crimeware trends, our results show that the prevalence of botnets (attack-related crimeware) 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. (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]V. G. Tasiopoulos and S. K. Katsikas, "Bypassing Antivirus Detection with Encryption," in Proc., 18th Panhellenic Conf. on Informatics - PCI '14, New York, New York, USA, 2014, pp. 1–2: ACM Press.

[8]R. Venkateswaran, "Virtual private networks," IEEE Potentials, vol. 20, no. 1, pp. 11–15, 2001.

[9]A. K. Sood, S. Zeadally, and R. Bansal. "Cybercrime at a Scale: A Practical Study of Deployments of HTTP-Based Botnet Command and Control Panels," IEEE Commun. Mag., vol. 55, no. 7, pp. 22–28.

2017.

[10]Z. Shi, G. M. Lee, and A. B. Whinston, "Toward a Better Measure of Business Proximity: Topic Modeling for Industry Intelligence," *MIS Quart.,* vol. 40, no. 4, pp. 1035–1056, 2016.

[11]A. Majchrzak and S. L. Jarvenpaa, "Safe Contexts for Interorganizational Collaborations Among Homeland Security Professionals," *J. Manag. Inf. Syst.,* vol. 27, no. 2, pp. 55–86, 2010.

[12]G. Giacomello, "Close to the Edge: Cyberterrorism Today," in *Understanding Terrorism*, Emerald Group Publishing Limited, 2014, pp. 217–236.

[13]M. M. Pollitt, "Cyberterrorism — Fact or Fancy?," *Comput. Fraud Security,* vol. 1998, no. 2, pp. 8–10, 1998.