www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86
https://doi.org/10.5281/zenodo.14066288

Exploring The Underground Economy Of Cybercrime Through Advanced Data Analytics

[1]S.VIJAYKUMAR,[2]BANDA PRAVALIKA
[1]Assistant Professor, [2]MCA Student
Department Of MCA Student
Sree Chaitanya College of Engineering, Karimnagar

ABSTRACT:

Research on the fundamentals of the field or approaches that might help inform information systems researchers and practitioners that work with cyber security has been lacking, despite the quick rise in cyberthreats. Furthermore, not much is known about the criminal business model known as Crime-as-a-Service (CaaS), which serves as the foundation for the underground cybercrime industry. We are inspired to explore the underground economy of cybercrime using a data analytics method from a design science viewpoint because of this research gap and the real-world cybercrime issues we encounter. We provide (1) a data analytic framework for examining the subterranean cybercrime scene, (2) definitions of CaaS and criminal ware, and (3) a related classification model in order to do this. Furthermore, we (4) provide a sample application to show how the suggested framework and classification model may be used in real-world scenarios. We then analyse a sizable dataset gathered from the internet hacking community using this program to look into the underground economics of cybercrime. This work adds to the design artefacts, foundations, and methodology in this field by using a design science research approach. Additionally, it offers practitioners helpful practical insights by proposing suggestions for how governments and organisations across all industries may get ready for subterranean cybercrime assaults.

1. INTRODUCTION

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

https://doi.org/10.5281/zenodo.14066288

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.

2. LITERATURE SURVEY

"FACT SHEET: Cybersecurity National Action Plan," ed: The White House, 2016.

From the beginning of his Administration, the President has made it clear that cybersecurity is one of the most important challenges we face as a Nation, and for more than seven years he has acted comprehensively to confront that challenge. Working together with Congress, we took another step forward in this effort in December with the passage of the Cybersecurity Act of 2015, which provides important tools necessary to strengthen the Nation's cybersecurity, particularly by making it easier for private companies to share cyber threat information with each other and the Government.

But the President believes that more must be done – so that citizens have the tools they need to protect themselves, companies can defend their operations and information, and the Government does its part to protect the American people and the information they entrust to us. That is why, today, the President is directing his Administration to implement a **Cybersecurity National Action Plan (CNAP)** that takes near-term actions and puts in place a long-term strategy to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security.

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

We analyze the threat of DDoS-for-hire services to low and medium power cloud-based servers or home users. We aim to investigate popularity and availability of such services, their payment models, subscription pricing, complexity of the generated attack traffic and performance.

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

https://doi.org/10.5281/zenodo.14066288

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.

DISADVANTAGES:

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

4. 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

https://doi.org/10.5281/zenodo.14066288

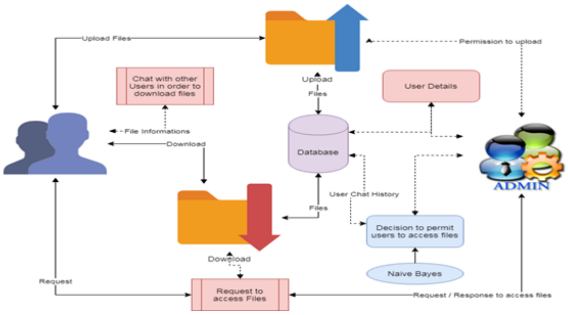
itself and obtained a malware database from a leading global cyber security research firm. Because cybercriminals often change their IP addresses and use anti-crawling scripts to conceal their communications, we used a self-developed crawler that can resolve captchas and anti-crawling scripts to gather 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. Since the product features, prices, and descriptions were explained within longer texts, we used a variety of text mining techniques to extract the important features: for example, we used named entity recognition to extract company names (see Section IV-C(2)). Since these texts included many typographic errors and jargon terms, we had to create a dictionary for use during a preprocessing step. In addition, we obtained a malware database from a cybersecurity firm containing over 53,815 entries covering cybercrimes between May 11, 2010 and January 13, 2014. This unique dataset strengthened our study by providing real-world evidence from a different viewpoint.

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.

5. SYSTEM DESIGN

ARCHITECTURE DIAGRAM



6. IMPLEMENTATION MODULES:

https://doi.org/10.5281/zenodo.14066288

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.

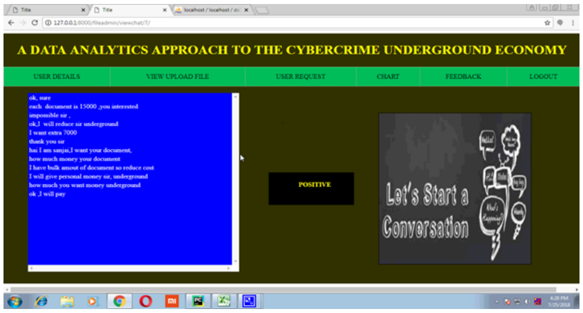
3. **Download Files**

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.

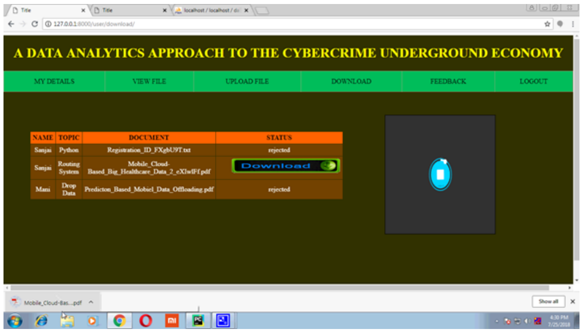
4. **Graphical Representations**

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.

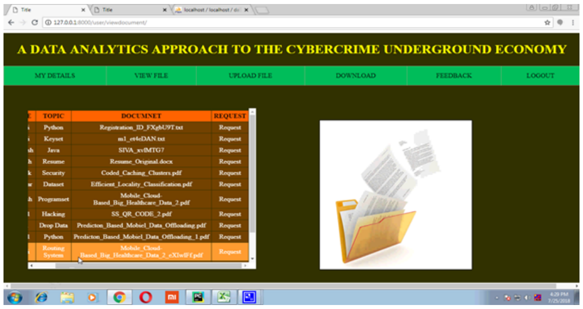
7. RESULTS


127.0.0.1:8000/fileadmin/viewchat/7/
A DATA ANALYTICS APPROACH TO THE CYBERCRIME UNDERGROUND ECONOMY
USER DETAILS
VIEW UPLOAD FILE
USER REQUEST
CHART
FEEDBACK
LOGOUT
POSITIVE
Let's Start a Conversation

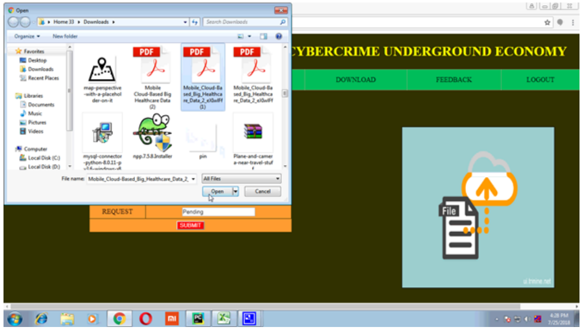
ok, sure
each document is 15000 ,you interested
impossible sir ,
ok,I will reduce sir underground
I want extra 7000
thank you sir
hai I am sanjai,I want your document,
how much money your document
I have bulk amout of document so reduce cost
I will give personal money sir, underground
how much you want money underground
ok ,I will pay


127.0.0.1:8000/user/download/
A DATA ANALYTICS APPROACH TO THE CYBERCRIME UNDERGROUND ECONOMY
MY DETAILS
VIEW FILE
UPLOAD FILE
DOWNLOAD
FEEDBACK
LOGOUT
Mobile_Cloud-Bas....pdf
Show all

NAME	TOPIC	DOCUMENT	STATUS
Sanjai	Python	Registration_ID_FXgbU9T.txt	rejected
Sanjai	Routing System	Mobile_Cloud-Based_Big_Healthcare_Data_2_eXIwlFf.pdf	Download
Mani	Drop Data	Predicton_Based_Mobiel_Data_Offloading.pdf	rejected


127.0.0.1:8000/user/viewdocument/
A DATA ANALYTICS APPROACH TO THE CYBERCRIME UNDERGROUND ECONOMY
MY DETAILS
VIEW FILE
UPLOAD FILE
DOWNLOAD
FEEDBACK
LOGOUT

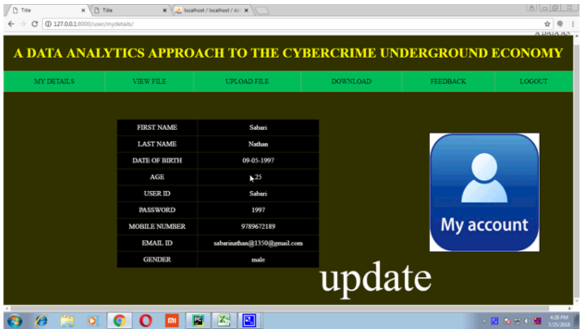
E	TOPIC	DOCUMNET	REQUEST
i	Python	Registration_ID_FXgbU9T.txt	Request
i	Keyset	m1_et4eDAN.txt	Request
sh	Java	SIVA_xvIMTG7	Request
h	Resume	Resume_Original.docx	Request
k	Security	Coded_Caching_Clusters.pdf	Request
ar	Dataset	Efficient_Locality_Classification.pdf	Request
h	Programset	Mobile_Cloud-Based_Big_Healthcare_Data_2.pdf	Request
l	Hacking	SS_QR_CODE_2.pdf	Request
	Drop Data	Predicton_Based_Mobiel_Data_Offloading.pdf	Request
l	Python	Predicton_Based_Mobiel_Data_Offloading_1.pdf	Request
i	Routing System	Mobile_Cloud-Based_Big_Healthcare_Data_2_eXIwlFf.pdf	Request


Open
Home 33 ▸ Downloads ▸
Search Downloads
Organize ▾
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Local Disk (D:)
map-perspective-with-a-placeholder-on-it
Mobile Cloud-Based Big Healthcare Data (2)
Mobile_Cloud-Based_Big_Healthcare_Data_2_eX0wlFf (1)
Mobile_Cloud-Based_Big_Healthcare_Data_2_eX0wlFf
mysql-connector-python-8.0.11-py3.6-windows-x8
npp.7.5.8.Installer
pin
Plane-and-camera-near-travel-stuff
All Files
Open
Cancel
CYBERCRIME UNDERGROUND ECONOMY
DOWNLOAD
FEEDBACK
LOGOUT
File

File name: Mobile_Cloud-Based_Big_Healthcare_Data_2_

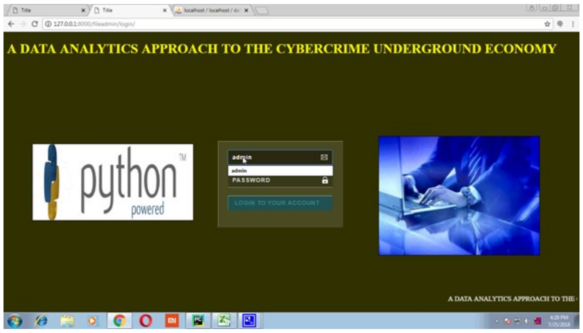
REQUEST	Pending

SUBMIT



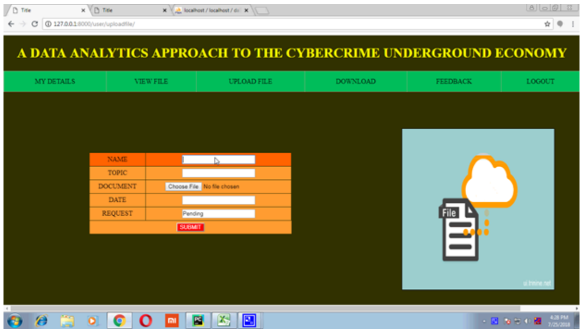
A DATA ANALYTICS APPROACH TO THE CYBERCRIME UNDERGROUND ECONOMY

FIRST NAME	Sabari
LAST NAME	Nathan
DATE OF BIRTH	09-05-1997
AGE	25
USER ID	Sabari
PASSWORD	1997
MOBILE NUMBER	9789672189
EMAIL ID	sabarinathan@1350@gmail.com
GENDER	male


127.0.0.1:8000/fileadmin/login/
python powered
LOGIN TO YOUR ACCOUNT
A DATA ANALYTICS APPROACH TO THE

A DATA ANALYTICS APPROACH TO THE CYBERCRIME UNDERGROUND ECONOMY

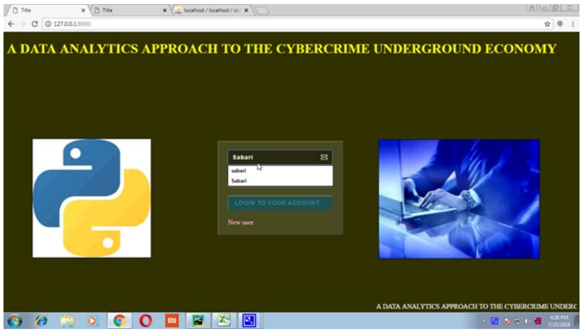
admin
admin
PASSWORD



A DATA ANALYTICS APPROACH TO THE CYBERCRIME UNDERGROUND ECONOMY

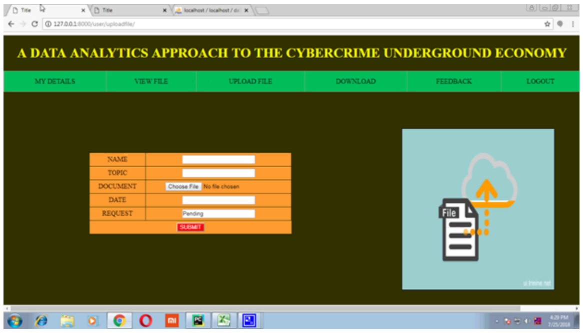
NAME	
TOPIC	
DOCUMENT	Choose File No file chosen
DATE	
REQUEST	Pending

SUBMIT



A DATA ANALYTICS APPROACH TO THE CYBERCRIME UNDERGROUND ECONOMY

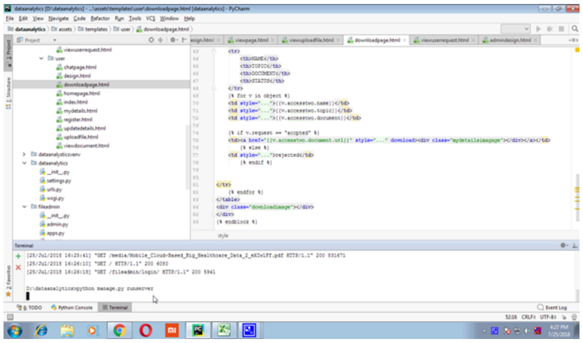
Sabari
sabari
Sabari



A DATA ANALYTICS APPROACH TO THE CYBERCRIME UNDERGROUND ECONOMY

NAME	
TOPIC	
DOCUMENT	Choose File No file chosen
DATE	
REQUEST	Pending

SUBMIT



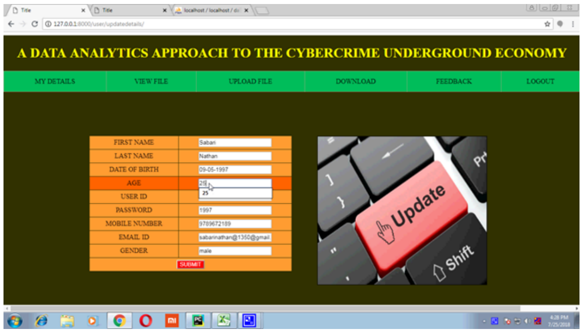
```
<tr>
    <th>NAME</th>
    <th>TOPIC</th>
    <th>DOCUMENT</th>
    <th>STATUS</th>
</tr>
{% for v in object %}
<td style="...">{{v.accesstwo.name}}</td>
<td style="...">{{v.accesstwo.topic}}</td>
<td style="...">{{v.accesstwo.document}}</td>

{% if v.request == "accpted" %}
<td><a href="{{v.accesstwo.document.url}}" style="..." download><div class="mydetailsimagage"></div></a></td>
    {% else %}
<td style="...">rejected</td>
    {% endif %}


</tr>
    {% endfor %}
</table>
<div class="downloadimage"></div>
</div>
{% endblock %}
```

```
[25/Jul/2018 16:25:41] "GET /media/Mobile_Cloud-Based_Big_Healthcare_Data_2_eXIwlFf.pdf HTTP/1.1" 200 831671
[25/Jul/2018 16:26:10] "GET / HTTP/1.1" 200 4080
[25/Jul/2018 16:26:15] "GET /fileadmin/login/ HTTP/1.1" 200 5941

D:\dataanalytics>python manage.py runserver
```

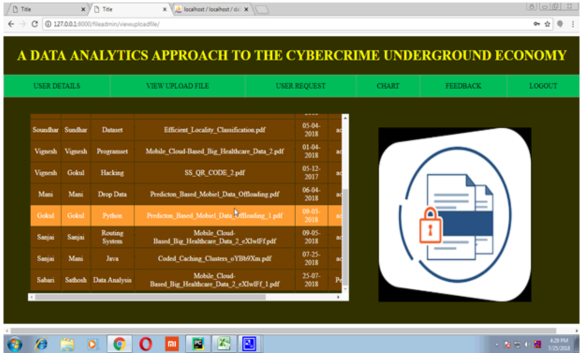


A DATA ANALYTICS APPROACH TO THE CYBERCRIME UNDERGROUND ECONOMY

FIRST NAME	Sabari
LAST NAME	Nathan
DATE OF BIRTH	09-05-1997
AGE	25
USER ID	
PASSWORD	1997
MOBILE NUMBER	9789672189
EMAIL ID	sabarinathan@1350@gmail
GENDER	male

SUBMIT

https://doi.org/10.5281/zenodo.14066288



A DATA ANALYTICS APPROACH TO THE CYBERCRIME UNDERGROUND ECONOMY

Soundhar	Sundhar	Dataset	Efficient_Locality_Classification.pdf	05-04-2018	ac
Vignesh	Vignesh	Programset	Mobile_Cloud-Based_Big_Healthcare_Data_2.pdf	01-04-2018	ac
Vignesh	Gokul	Hacking	SS_QR_CODE_2.pdf	05-12-2017	ac
Mani	Mani	Drop Data	Predicton_Based_Mobiel_Data_Offloading.pdf	06-04-2018	ac
Gokul	Gokul	Python	Predicton_Based_Mobiel_Data_Offloading_1.pdf	09-03-2018	ac
Sanjai	Sanjai	Routing System	Mobile_Cloud-Based_Big_Healthcare_Data_2_eXIwIFf.pdf	09-05-2018	ac
Sanjai	Mani	Java	Coded_Caching_Clusters_oYBb9Xm.pdf	07-25-2018	ac
Sabari	Sathosh	Data Analysis	Mobile_Cloud-Based_Big_Healthcare_Data_2_eXIwIFf_1.pdf	25-07-2018	Pe

8. CONCLUSION

Since this study uses a DSR method, we have mostly concentrated on creating and assessing artefacts rather than creating and defending theory because behavioural science is typically thought to be primarily concerned with actions. As a result, we have suggested two artefacts: a categorisation model and a framework for data analysis. Additionally, using sample applications, we have evaluated the accuracy of our classification model ex ante and its implementation ex post. According to DSR's initiating perspective, these four sample applications show the variety of real-world uses that academics and practitioners in the future may encounter. Our work has mainly concentrated on CaaS and crimeware from a RAT viewpoint, in contrast to other research that has provided broader explanations of a wide variety of cybercrime. Based on definitions from the academic and business practice literature, we have also proposed sets of definitions for various forms of crimeware (drive-by download, botnets, exploits, ransomware, rootkits, Trojans, crypters, and proxies) and CaaS (phishing, brute force attack, DDoS attack, spamming, crypting, and VPN services). We have developed a RAT-based categorisation model based on them. These RAT-based criteria are crucial components of our framework as this study highlights the value of RAT for looking into the underground cybercrime scene. Furthermore, we have examined extensive datasets gathered from the underground community, in contrast to other studies that talked about the underground economics of cybercrime without making an effort to analyse the data. Considering the trends in CaaS and crimeware, our findings indicate that in 2017, botnets (crimeware connected to attacks) and VPNs (caaS-related preventative measures) became more common. This suggests that attackers take into account an organization's weaknesses as well as its preventative measures. Technology firms are the most prevalent possible target organisations (28%), followed by content companies (22%), financial companies (20%), e-commerce companies (12%), and telecommunications companies (10%). This suggests that a wide range of businesses across many industries are becoming exposed to attacks as a result of their increased 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/20

https://doi.org/10.5281/zenodo.14066288

17/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.