



A DATA EXPLORATION APPROACH TO THE ELECTRONIC CRIME THROUGH INFORMAL ECONOMY

Chilukani Sravani Reddy¹, & Dr.S.Kishore Verma²,& T. Sai Santhoshi³

¹Research Scholar, Department of CSE, Sri Indu College of Engineering and Technology, Sheriguda (V), Ibrahimpatnam(M), RR District – 501510, Telangana,India

²Associate Professor , Department of CSE, Sri Indu College of Engineering and Technology, Sheriguda (V), Ibrahimpatnam(M), RR District – 501510, Telangana, India

³Assistant Professor , Department of CSE, Sri Indu College of Engineering and Technology, Sheriguda (V), Ibrahimpatnam(M), RR District – 501510, Telangana, India

ABSTRACT

The realm of cyber threats is rapidly evolving, yet there remains a significant gap in research regarding the fundamentals of this subject and methodologies that could aid Information Systems researchers and practitioners in tackling cyber security challenges. Particularly, there is a lack of understanding about Crime-as-a-Service (CaaS), a criminal business model that serves as the foundation of the cybercrime underground. This existing research gap, coupled with the pressing issues posed by practical cybercrime problems, has motivated us to delve into the cybercrime underground economy using a data analytics approach from a design science perspective. To address this, we develop an illustrative application to showcase the practical implementation of the proposed framework and classification model. By analyzing a substantial dataset sourced from the online hacking community, we gain insights into the cybercrime underground economy.

By adopting a design science research approach, this study not only contributes valuable design artifacts, foundations, and methodologies in the field, but also offers practical insights for practitioners. It suggests guidelines on how governments and organizations across various industries can prepare themselves against cyber attacks orchestrated by the cybercrime underground

1. INTRODUCTION

As the threat posed by massive cyber attacks (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 cyber security budgets. United States President Barack Obama proposed spending over \$19 billion on cyber security as part of his fiscal year 2017 budget, an increase of more than 35% since 2016 [2].

Global cyber attacks (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 hierarchies [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.

2. LITERATURE SURVEY

Title: A Data Analytics Approach to the Cybercrime Underground Economy

Authors: Jungkook An; Hee-Woong Kim

Abstract: 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: (1) propose a data analysis framework for analyzing the cybercrime underground; (2) propose CaaS and crimeware definitions; (3) propose an associated classification model, and (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 data set obtained from the online hacking community. By taking a design science research approach, this paper 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.

Title: A Data Analytics Approach to the Cybercrime Underground Economy



Authors: Hee-Woong Kim

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.

Title: An Effective Data Analytics Approach to Cybercrime Underground Economy Using ML Methodologies

Authors: A. Swarupa Rani, G. Manasa

Abstract :To achieve this goal, we propose (1) a data analysis framework for analyzing the cybercrime underground, (2) CaaS and crime ware definitions, and (1) an associated classification demonstrate. In addition, we (1) build up an example application to demonstrate how the proposed framework and classification model could be actualized in practice. We at that point utilize this application to investigate the cybercrime underground economy by analyzing a large dataset obtained from the internet hacking community. By taking a design science research approach, this examination adds to the design of artifacts, foundations, and methodologies in this area. Additionally, it gives helpful practical bits of knowledge to practitioners by proposing rules as to how governments and organizations in all businesses can prepare for attacks by the cybercrime underground.

3. PROBLEM STATEMENT

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 hierarchies [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, 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

3.1 LIMITATIONS

The existing work has 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.

4. PROPOSED SYSTEM

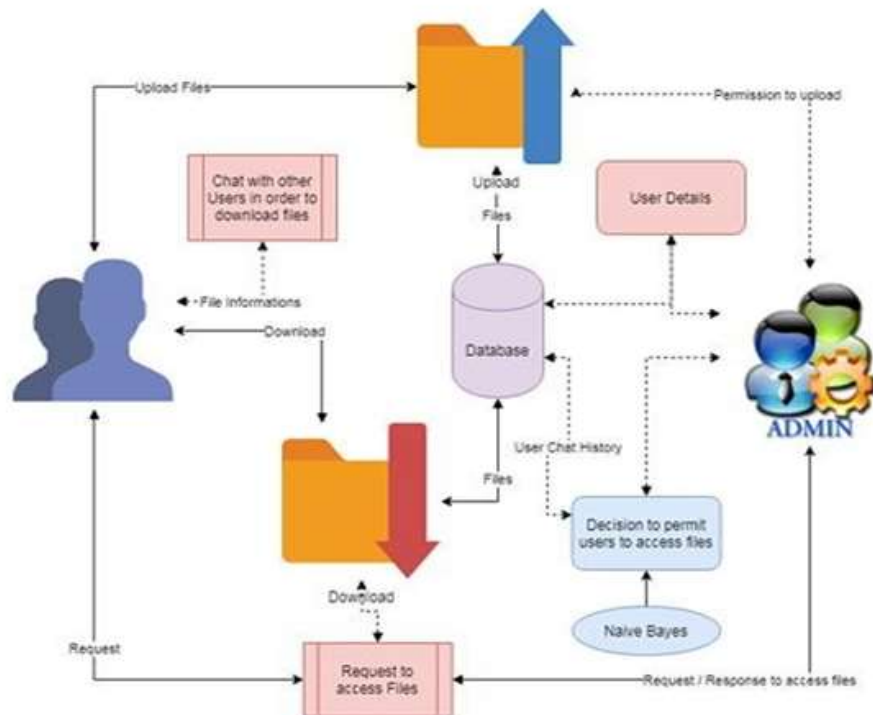
We take a data analytics approach and investigate the cybercrime economy from a design science perspective. To achieve this goal, we (1) propose a data analysis framework for analyzing the cybercrime underground to guide researchers and practitioners; (2) define CaaS and crimeware to better reflect their 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.

4.1 ADVANTAGES OF PROPOSED SYSTEM

In the business practice field, an exploit is defined as “a program created specifically to exploit a vulnerability, in other words—simply trying to take advantage of an error in the design or programming of a system or application,” and is used to obtain Administrator privileges on a system. We thus define an exploit as a program or script that exploits vulnerabilities in applications, servers, or clients. Ransomware: Ransomware is a type of malicious software that disables the functionality of a computer in some way . We thus define ransomware as malicious software that encrypts a victim’s data to extort money from them.

Rootkit: The business practice literature defines a rootkit as “a program that allows someone to obtain root-level access to the computer.”. We thus define a rootkit as a piece of malicious software that enables administrator-level access to an operating system or computer network.

5. ARCHITECTURE OF PROPOSED SYSTEM



6. IMPLEMENTATION

6.1 Admin

Here the admin is the main module, the admin can directly login with the application and the admin after his successful login can perform some actions like view users, add cyber crime words, view crime words.

6.2 User

The user is the module should register with the application and the user should be authorized by the admin then only the user can be able to login with the application and the user after his successful login can perform the following actions such as public content, view published content, view shared content by the other users.

6.3 Cyber Crime Detection

The cyber crime detection is the module to analyze the data which consist of the cyber crime related information. If the information found then that file will detect by the detector and also the detector can detect the file which is published by the attacker for providing the unavailable resource to the users.

6.4 DDoS Attacker

The DDoS attacker can directly access the publish page from the server then the DDoS attacker can publish the content which is not helpful to the users. And the DDoS attacker can also check view his all published content.

7. RESULTS

DATA EXPLORATION APPROACH
Home Admin User CyberCrime Detection

Project 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

Home Page

SUBMODULES IN ADMIN

Home
View Users Add CyberCrime Words View Crime Words Logout

VIEWING USERS

View All Users And Authorize

FIRST NAME	LAST NAME	EMAIL	MOBILE	ADDRESS	STATUS
sravani	reddy	sravani@gmail.com	1234567890	hyd	Activated



ADDING THREATENING CYBER WORDS

Add Cyber Crime Words

CyberCrime Word:

Adding Cyber Words

VIEWING CYBER WORDS

View All Cyber Crime Words

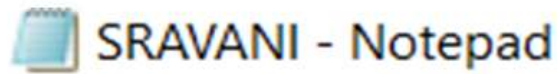
ID	WORDS
33	DANGEROUS

SUB MODULES IN USER





PUBLISHED TEXT DOCUMENT



File Edit Format View Help

DANGEROUS

published Text Document

View All Published Content

Published ID	Title	File Name
33	sravani	SRAVANI.txt

Viewing Published Content

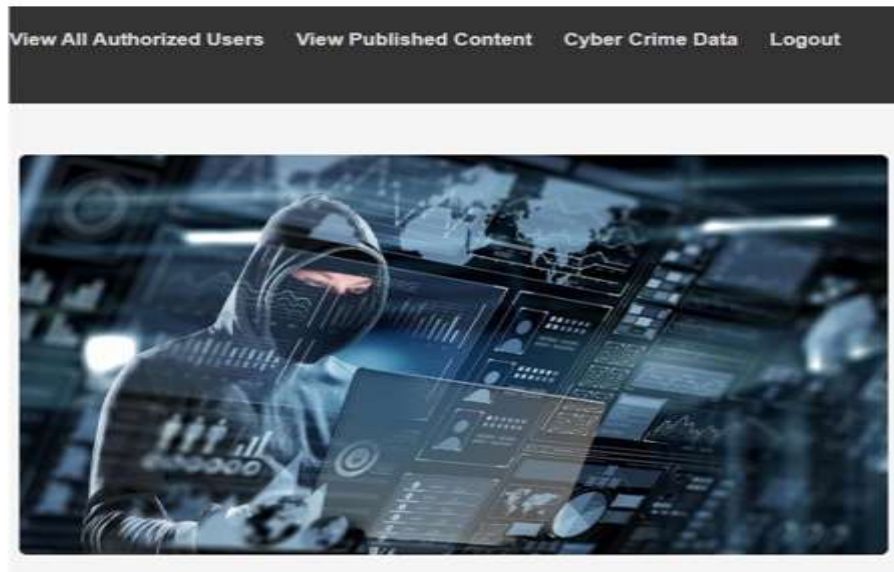
CYBER CRIME LOGIN PAGE

DATA EXPLORATION APPROACH Home Admin User Cyber Crime Detection

can prepare for attacks by the cybercrime underground.



SUBMODULES IN CYBER DETECTION



View ALL Published Content

OWNER	FILE NAME	SHARE	ANALYZE DATA
sravani@gmail.com	SRAVANI.txt	public	Analyze

Viewing Published Content

ANALYSING THE WORD

localhost:8084 says

Data Analysed CyberCrime Detected





CYBERDATA

DATA EXPLORATION APPROACH [Home](#) [View All Authorized Users](#) [View Published Content](#) [Cyber Crime DATA](#) [Logout](#)

OWNER	FILE NAME	CRIME DATA	CRIME WORDS
		DANGEROUS	
sravani@gmail.com	SRAVANI.txt		DANGEROUS

8. CONCLUSION

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. More importantly, these tools could be based on vulnerabilities in their organizations, products, and services. Governments and organizations therefore need to increase their technical capabilities when it comes to analyzing large-scale datasets of different types. Although the proposed framework and classification model are of particular use to companies mentioned specifically by the cybercrime underground, the framework can also be used to analyze more general types of issues commonly encountered in practice. In this regard, legal and technical training is needed to reduce the impact of cyberattacks.

9. REFERENCES

1. J. C. Wong and O. Solon, Massive Ransomware Cyber-Attack Hits Nearly 100 Countries Around the world, Available: <https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs>.
2. FACT SHEET: Cybersecurity National Action Plan, Washington, DC, USA, 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. Infrastruct. Protect.*, vol. 6, pp. 28-38, 2013.



4. S. W. Brenner, "Organized cybercrime-how cyberspace may affect the structure of criminal relationships", North Carolina J. Law Technol., vol. 4, no. 1, pp. 1-50, 2002.
5. K. Hughes, "Entering the World-Wide Web", ACM SIGWEB Newslett., 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.