DETECTING AND ANALYZING CRYPTO-RANSOMWARE IN CYBER FRAUD

Dr. S. Venkata Achutha Rao[1],P.Sriya[2],S.Meghana[3],J.Sai Teja[4],E.Vishnu[5]
Professor, Department of Computer Science and Engineering[1]
Student, Department of Computer Science and Engineering[2,3,4,5]
Sree Dattha Institute of Engineering and Science, Sheriguda, Telangana.

ABSTRACT

Currently, as the widespread use of virtual monetary units (like Bitcoin, Ethereum, Ripple, Litecoin) has begun, people with bad intentions have been attracted to this area and have produced and marketed ransomware to obtain virtual currency easily. This ransomware infiltrates the victim's system with smartly-designed methods and encrypts the files found in the system. After the encryption process, the attacker leaves a message demanding a ransom in virtual currency to open access to the encrypted files and warns that otherwise the files will not be accessible. This type of ransomware is becoming more popular over time, so currently, it is the largest information technology security threat. In the literature, there are many studies about the detection and analysis of this cyber-bullying. In this study, we focused on crypto-ransomware and investigated a forensic analysis of a current attack example in detail. In this example, the attack method and behavior of the crypto-ransomware were analyzed and it was identified that information belonging to the attacker was accessible. With this dimension, we think our study will significantly contribute to the struggle against this threat.

Index terms: Crypto-ransomware, forensic analysis, virtual currency, information technology security, cyber-bullying.

DOI Number: 10.48047/nq.2024.22.4.nq24012 **NeuroQuantology 2024; 22(4):106-112**

I.INTRODUCTION

In addition to convenience created by rapid developments in the field of technology and information, new threats have emerged. Attackers rapidly adapting to new technologies have changed the target, type and methods of attack. In order for public organizations and institutions, private companies and simple internet users to deal with these threats, they need to use a new generation of security precautions. In spite of all precautions, cyber-attacks have continued to increase. Currently the most commonly observed cyber-attacks are ransomware. Ransomware is harmful software or malware which encrypts the victim's personal files and folders and demands a ransom. Ransomware is generally investigated in two categories of crypto-ransomware and crypto locker ransomware. Crypto-ransomware is accepted as the first example of modern ransomware .

This malware obstructs the operating system or system entry of the victim until the ransom is paid. Ransom is generally demanded, with money transfer demanded by telephone message, electronic card system or prepaid card system code. Crypto-ransomware prevents access by encrypting a certain section of files

and entering an appropriate code key opens the files for access again.

Crypto-ransomware is the most popular malware observed in recent times. With the spread of virtual currency use around the world, it has become a focus of interest for attackers. The convenience of virtual currencies and inability to trace them forms the basis of the designed malware. Crypto-ransomware can delete files from the victim's system after encryption. When the user attempts to access the desired files, a message is shown on the screen stating that the files are encrypted and payment is required. After the encrypted files are deleted from the victim's system, they are stored in an area belonging to the attacker and a promise is made that they will be reopened for sharing when the ransom is paid. Investigated examples show that even if the ransom is paid it is nearly impossible to access the encrypted files.

II.LITERATURE SURVEY

- Manuel Egele, Theodoor Scholte, and Engin Kirda proposed that antivirus vendors face a multitude of potential malicious samples daily, receiving thousands of new samples. Given that signatures to detect confirmed threats are mainly created manually, distinguishing between new unknown threats and mere variants of known malware is crucial. Their survey article provides an overview of dynamic analysis techniques used to analyze potentially malicious samples. It covers analysis programs employing these techniques to assist human analysts in timely and appropriate manual inspection of samples with unknown malicious behavior.
- Dongil Shin, Dongkyoo Shin, and Yong-Hyun Kim recently proposed an attack detection application for Android OS smartphones, addressing the increasing threat to personal information. The application includes two phases: a pre-phase for comparison and analysis before attacks occur, and a post-phase using an attack tree to detect and classify malware attacks into interception, modification, and system damage categories. This approach aims to protect user information by identifying attack routes through real-time analysis and comparison with pre-defined attack scenarios.
- Fanny Lalonde Lévesque, Sonia Chiasson, and Anil Buntwal Somayaji explored how both technological and human factors contribute to the success or failure of malware attacks. They conducted a field study involving 50 home users over four months to evaluate antivirus software efficacy and human risk factors. The study revealed insights into antivirus performance under real-life conditions versus controlled tests, highlighting computer expertise, network usage volume, and peer-to-peer activity as significant correlates of malware attacks. This work emphasizes the importance of evaluating security products through long-term field studies for better ecological validity.
- Ilker Kara and Murat Aydos addressed the pervasive use of ransomware by cybercriminals, highlighting its economic and socio-political motives. They emphasized the critical need for technical analysis to trace the source of ransomware attacks, despite the challenges in recovering affected files due to strong encryption. Their study analyzed a real-life ransomware attack on an official institute using both static and dynamic methods, demonstrating traceability through server WHOIS information.
- Reza Iuxel Curtmola, Juan A. Garay, and Seny Kamara focused on searchable symmetric encryption (SSE), allowing secure data outsourcing with selective search capabilities. They proposed new, stronger security definitions and efficient constructions that enable multi-user search scenarios, surpassing previous constructions in efficiency and security guarantees.

III.EXISTING SYSTEM

To date, many approaches have been used for identification and analysis of ransomware. The approaches with most focus are algorithms based on signature-based detection logic [11].

Success of this approach is debatable due to weaknesses. It is impossible to identify new-generation (fileless) ransomware with classic signature-based approaches. New types of approaches continue to be developed to resolve these deficiencies. These approaches encompass techniques investigating the operating behavior of ransomware (dynamic analysis).

Fatemah et al. presented a signature-based ransomware identification method based on graphic mining. The study concluded they had 96.6% rate of successful detection [12].

Daniele et al. developed a dynamic analysis approach working with machine-learning logic for ransomware [13]. In 2015, Donghyun et al. recommended a digitalized model to prevent and identify crypto-ransomware [14].

IV.PROPOSED SYSTEM

A. SYSTEM OVERVIEW

In this section, we explain our proposed architectural system. In the study, the proposed approach model was designed in order to implement identification and analysis of cryptoransomware specifically. Our approach comprises three modules. These are;

- **Module 1.**

An image (forensic copy) is taken of the computer attacked by the crypto-ransomware. An image is the name given to a one-to-one copy of the data storage unit of the material to be investigated. There are two different methods used to take images of physical and logical methods. All analyses are performed on this image in a safe environment (on a workstation). Thus, the aim is to prevent possible harm to the live system.

- **Module 2.**

After creating the analysis environment, investigations of the image begin. In this step, analyses are completed from simple towards complicated methods. The first step is identification of possible ransomware. If there is no threat identified on the computer, the process ends at this step. If ransomware is identified, the first stage is to collect information about the ransomware without executing it. Later the ransomware is executed and characteristic behavior (file-array movements, code architecture) analysis is performed. In the final step, the possibility of contacting the ransomware attacker is investigated in an attempt to obtain contact information.

- **Module 3**

After completing analyses, the procedures are reported for use against possible similar attacks or communicated to investigation units.

V.SYSTEM ARCHITECTURE

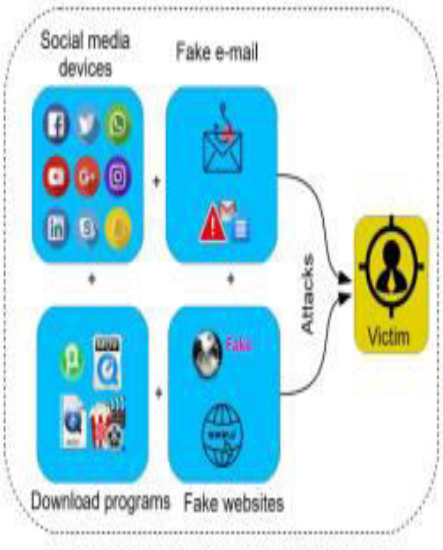

Figure.1 System Architecture

VI.IMPLEMENTATION:

User Module:

The User module allows regular users to register and securely log in to access their account. Users can upload files, manage their uploads, and view them conveniently. They can also update their profile information and log out securely when done.

Admin Module:

The Admin module is for system administrators. Admins can register new admin accounts, securely log in, and access administrative tools. Key tasks include static and dynamic analysis of uploaded files for threats like ransomware.

They manage safe and ransomware file data, and generate detailed analysis reports. Admins can securely log out after completing their tasks.

These modules ensure efficient and secure interaction tailored to user and administrator roles.

VII.RESULTS

Figure.2

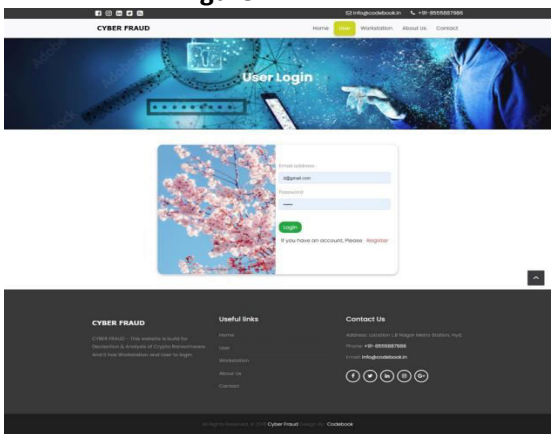

Figure.3

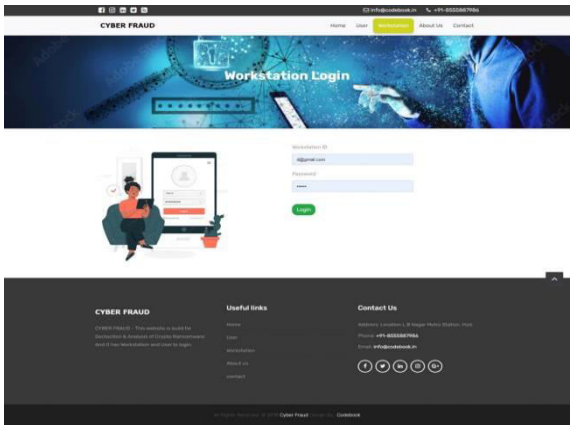

Figure.4

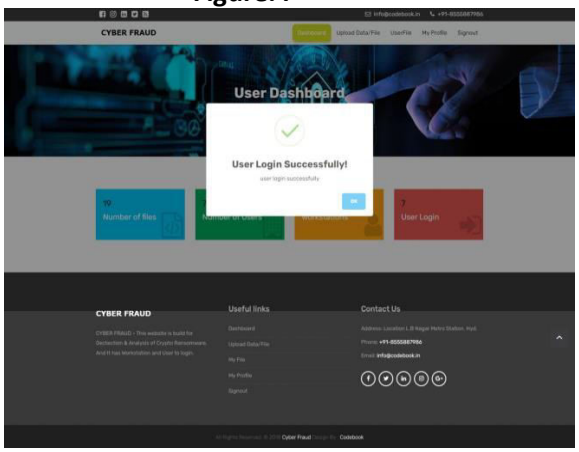

Figure.5

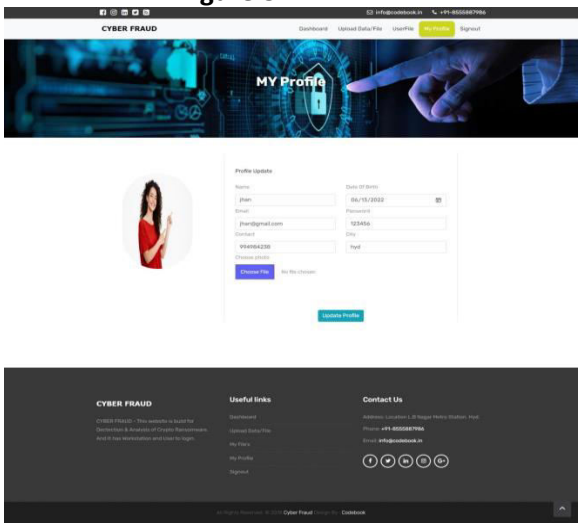

Figure.6

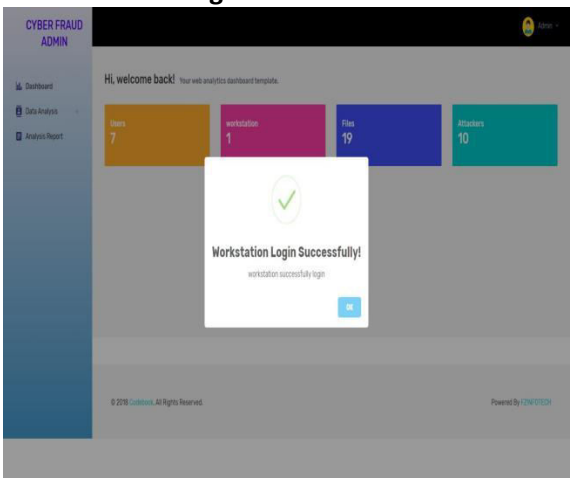

Figure.7

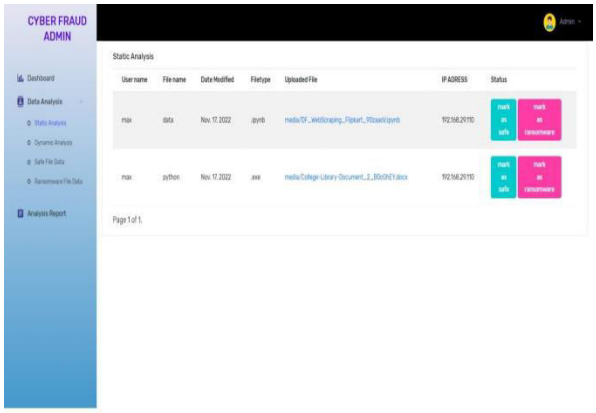

Figure.8

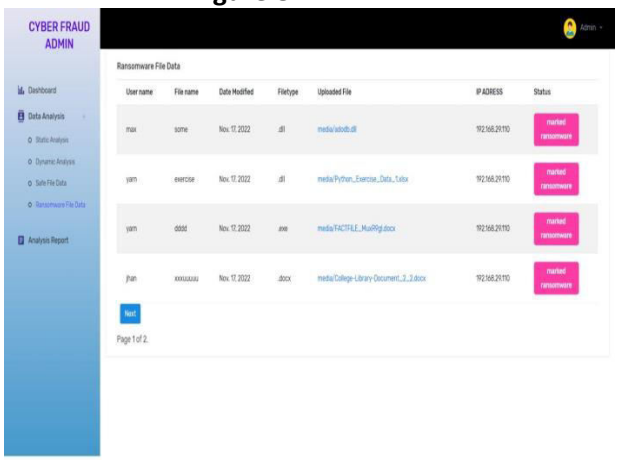

Figure.9

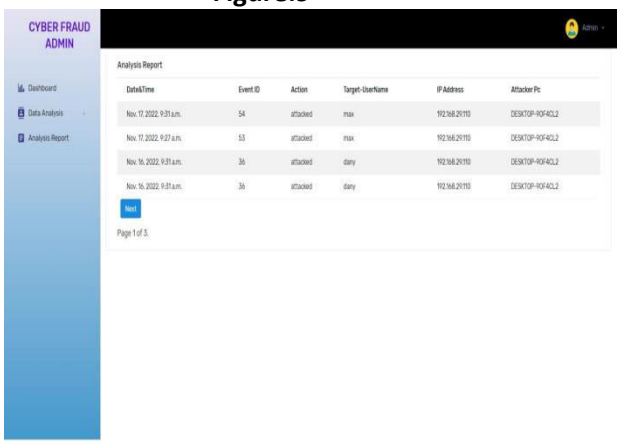

Figure.10

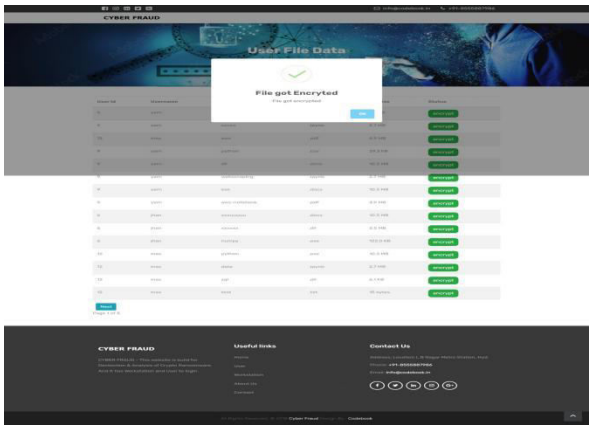

Figure.11

VIII.CONCLUSION

A large increase in the number crypto-ransomware attacks has been experienced, especially with the popularity of virtual currency. This situation is due to the difficulty in legally tracing virtual currency. Attackers encrypt the victim's files with crypto-ransomware and inform them that they need to buy an encryption key to ensure access to their files again. Due to the encryption type used in ransomware it is nearly impossible to break the encryption through outside intervention and this is accepted as technically impossible. The attacker deletes the encrypted files from the victim's computer and asserts that they are held in a storage area they own. In recent times, attackers have sent a message stating that they will unencrypt a file of the victim's choosing not above 100 MB in order to make sure the victim believes the situation. When the victim agrees, they are successfully given access to the file. However, when the victim pays the desired ransom the attacker has achieved their aim and communication ceases.

Analysis of ransomware encompasses detection of this software, understanding how it works and reaching the attacker. During crypto-ransomware analysis, reverse engineering techniques are used and the structure of the malware and interaction with the system are determined.

IX.FUTURE ENHANCEMENT

The future of ransomware analysis will likely focus on developing more robust detection and prevention methods. This includes advancements in machine learning and AI to enhance early detection capabilities. Moreover, international cooperation and legal frameworks will be essential to address the challenges posed by virtual currencies in tracing and prosecuting cybercriminals involved in ransomware attacks.

X.REFERENCES

[1] M. Egele, T.Scholte, E. Kirda, & C. Kruegel, 2008. A survey on automated dynamic malware-analysis techniques and tools. ACM computing surveys (CSUR), 44(2), 1-42.

[2] D. Kim, D. Shin, D. Shin, & Y. H. Kim, 2019. Attack detection application with attack tree for mobile system using log analysis. Mobile Networks and Applications, 24(1), 184-192.

[3] F. L. Lévesque, S. Chiasson, A. Somayaji, & J. M. Fernandez, 2018. Technological and human factors of malware attacks: A computer security clinical trial approach. ACM Transactions on Privacy and Security (TOPS), 21(4), 1-30.

[4] İ. Kara, M. Aydos, 2019. The ghost in the system: technical analysis of remote access trojan. International Journal on Information Technologies & Security, 11(1).

[5] I. Kara, M. Aydos, 2018, December. Static and dynamic analysis of third generation cerber ransomware. In 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT) (pp. 12-17). IEEE.

[6] B. A. S. Al-rimy, M. A. Maarof, S. Z. M. Shaid, 2018. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security, 74, 144-166.

[7] S. Baek, Y. Jung, A. Mohaisen, S. Lee, D. Nyang, 2018, July. SSDinsider: Internal defense of solid-state drive against ransomware with perfect data recovery. In 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS) (pp. 875-884). IEEE.

[8] M. A. S. Monge, J. M. Vidal, L. J. G. Villalba, 2018, August. A novel Self-Organizing Network solution towards Crypto-ransomware Mitigation. In Proceedings of the 13th International Conference on Availability, Reliability and Security (pp. 1-10).

[9] K. İlker, M. Aydos. (2019, October). Detection and Analysis of Attacks Against Web Services by the SQL Injection Method. In 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 1-4). IEEE.on Electronic Crime Research (eCrime) (pp. 1-13). IEEE.

[10] S. Mohurle, M. Patil, 2017. A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science, 8(5).

[11] F. Karbalaie, A. Sami, and M. Ahmadi. 2012.Semantic malware detection by deploying graph mining. International Journal of Computer Science Issues,9(1):373-379.

[12] D. Sgandurra, L. Munoz-Gonz_alez, R. Mohsen, and E. C. Lupu. 2016. Automated dynamic analysis of ransomware: Bene_ts, limitations and use for detection. arXiv preprint arXiv:1609.03020.

[13] D. Kim and S. Kim. 2015. Design of quanti-cation model for ransom ware prevent. World Journal of Engineering and Technology, 3(03):203.

[14] A. Kharraz, S. Arshad, C. Mulliner, W. K. Robertson, and E. Kirda. 2016.Unveil: A large-scal, automated approach to detecting ransomware. In USENIX Security Symposium, pages 757-772.

[15]https://websitem.karatekin.edu.tr/ilkerkara /paylasimlar/dosya/0f7a100dc f5c42d2

[16] M. Boldt, andB. Carlsson.2006 Analysing privacy-invasive software using computer forensic methods. ICSEA, Papeetee.

[17] S. Z. M. Shaid, and M. A. Maarof. 2014. Malware behavior image for malware variant identification", 2014 International Symposium on Biometrics and Security Technologies (ISBAST). IEEE, 2014.

[18] I. Kara. 2019. A basic malware analysis method. Computer Fraud & Security, 2019(6), 11-19.

[19] M. Kbanov, V. G. Vassilakis, M. D. Logothetis. 2019. WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. Journal of Telecommunications and Information Technology.

[20] J. Hwang, J. Kim, S. Lee, K. Kim, K. 2020. Two-Stage Ransomware Detection Using Dynamic Analysis and Machine Learning Techniques. Wireless Personal Communications, 112(4), 2597-2609.