International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 25 Issue 01, JAN, 2025

CYBER FRAUD DETECTION AND ANALYSIS OF CRYPTO RANSOMWARE

Dr.Yasaswini Vanapalli[1],Gutala Sushmitha[2],Jyothi Sharon David[3],Kanuma Harani[4]

[1] Associate Professor, School of CSE ,Malla Reddy Engineering College For Women(Autonomous Institution), Maisammaguda, Dhulapally,Secunderabad,Telangana-500100

[234]UG Student, Department of CSE,Malla Reddy Engineering College for Women, (Autonomous Institution), Maisammaguda,Dhulapally,Secunderabad,Telangana-500100

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 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.

Keywords:Crypto-ransomware, Forensic analysis, Virtual currency, Ransom demand, Cybersecurity threat

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. 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 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.

II.RELATED WORK

A survey on automated dynamic malware-analysis techniques and tools

Anti-virus vendors are confronted with a multitude of potential malicious samples today. Receiving thousands of new samples every single day is nothing uncommon. As the signatures that should detect the confirmed malicious threats are still mainly created manually, it is important to discriminate between samples that pose a new unknown threat, and those that are mere variants of known malware. This survey article provides an overview of techniques that are based on dynamic analysis and that are used to analyze potentially malicious samples. It also covers analysis programs that employ these techniques to assist a human analyst in assessing, in a timely and appropriate manner, whether a given sample deserves closer manual inspection due to its unknown malicious behavior.

"Attack detection application with attack tree for mobile system using log analysis.

Recently, the use of smart phones has greatly increased because of the development of cheap high-performance hardware. The biggest threat to a smart phone user is the loss of his/her personal information by an attacker. To protect a user's information from these threats, an attack detection application for the Android OS is proposed and developed, in which the detection system is comprised of two phases: the mobile detection system pre-phase and post-phase. The pre-phase includes the steps performed before an attack occurs for the comparison and analysis step of the post-phase, and the post-phase includes the steps performed to detect malware using an attack tree with level assignments from the post-phase. Three classes, interception, modification, and system damage are defined to classify attacks to determine the attacker's purpose. When an attack occurs, the application can recognize what kind of route the mobile attack goes through by comparing and analyzing the attack tree from the pre-phase and current attack data in the post-phase. Attack trees are used to easily extract attack scenarios and determine when an attack is occurring. We expect that using the proposed application will protect a user's personal information on a mobile system.

"Technological and human factors of malware attacks: A computer security clinical trial approach"

The success (or failure) of malware attacks depends upon both technological and human factors. The most security-conscious users are susceptible to unknown vulnerabilities, and even the best security mechanisms can be circumvented because of user actions. Although there has been significant research on the technical aspects of malware attacks and defense, there has been much less research on how users interact with both malware and current malware defenses.

This article describes a field study designed to examine the interactions between users, antivirus (AV) software, and malware as they occur on deployed systems. In a fashion like medical studies that evaluate the efficacy of a particular treatment, our experiment aimed to assess the performance of AV software and the human risk factors of malware attacks. The 4-month study involved 50 home users who agreed to use laptops that were instrumented to monitor for possible malware attacks and gather data on user behavior. This study provided some very interesting, non-intuitive insights into the efficacy of AV software and human risk factors. AV performance was found to be lower under real-life conditions compared to tests conducted in controlled conditions. Moreover, computer expertise, volume of network usage, and peer-to-peer activity were found to be significant correlates of malware attacks. We assert that this work shows the viability and the merits of evaluating security products, techniques, and strategies to protect systems through long-term field studies with greater ecological validity than can be achieved through other means.

"Static and dynamic analysis of third generation cerber ransomware.

Cyber criminals have been extensively using malicious Ransomware software for years. Ransomware is a subset of malware in which the data on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access returned to the victim. The motives for such attacks are not only limited to economical scumming. Illegal attacks on official databases may also target people with political or social power. Although billions of dollars have been spent for preventing or at least reducing the tremendous amount of losses, these malicious Ransomware attacks have been expanding and growing. Therefore, it is critical to perform technical analysis of such malicious codes and, if possible, determine the source of such attacks. It might be almost impossible to recover the affected files due to the strong encryption imposed on such files, however the determination of the source of Ransomware attacks have been becoming significantly important for criminal justice. Unfortunately, there are only a few technical analysis of real life attacks in the literature. In this work, a real life Ransomware attack on an official institute is investigated and fully analyzed. The analysis have been performed by both static and dynamic methods. The results show that the source of the Ransomware attack has been shown to be traceable from the server's whois information.

III. IMPLEMENTATION

The implementation of the proposed system for detecting and analyzing crypto ransomware involves several key components corresponding to the system architecture. The Ransomware Detection Layer continuously monitors system activities using real-time file monitoring tools, intrusion detection systems (IDS), and file integrity checkers. These tools detect changes in files, such as encryption activities, and trigger alerts when suspicious modifications occur, enabling early detection of ransomware behavior. The Analysis Layer focuses on analyzing ransomware behavior, such as file encryption patterns and network communication with external servers. It employs forensic tools to capture attack traces, analyze memory dumps, and inspect network traffic for malicious activities. In the Investigation Layer, digital evidence is collected and preserved through system logs, encryption traces, and communication logs. Forensic tools are used to correlate this evidence, and an attribution engine helps trace the ransomware's origin, identify the attacker’s infrastructure, and track ransom payments to virtual wallets. The Reporting and Mitigation Layer generates detailed incident reports, which include attack timelines, encryption methods, and ransom demands. It also tracks virtual currency transactions related to the ransom payment using blockchain explorers. Finally, the User Interface Layer provides a user-friendly dashboard to visualize ransomware activities, alerts, and system health status in real-time. This interface allows cybersecurity professionals to review data and generate detailed forensic reports for further analysis and mitigation. The integration of these components ensures a comprehensive system for detecting, analyzing, and investigating crypto-ransomware attacks, focusing on tracking virtual currency ransom payments and identifying attacker information.

IV.ALGORITHMS

The implementation of the proposed system for detecting and analyzing crypto ransomware is based on several algorithms that work together to provide effective detection, analysis, and forensic investigation. These algorithms can be explained as follows:

File Integrity Check Algorithm: This algorithm is designed to monitor and detect any changes in system files that might indicate ransomware encryption activity. It works by continuously computing and comparing the hash values of files. If a file’s hash value changes unexpectedly, it triggers an alert, indicating potential encryption or modification by ransomware. This helps in detecting ransomware early in the attack process.

Suspicious Process Detection Algorithm: This algorithm monitors the system for processes that exhibit typical ransomware behavior, such as the encryption of files or the establishment of connections to malicious external servers. It looks

for suspicious patterns, such as processes that access a large number of files or initiate communication with unknown or suspicious IP addresses. If such patterns are detected, the system flags them for further investigation.

Network Traffic Analysis Algorithm: Ransomware often communicates with a remote server to receive commands or send information about the compromised system. This algorithm analyzes outgoing and incoming network traffic for signs of unusual behavior. It identifies traffic to known malicious IP addresses or abnormal communication patterns, which may indicate a ransomware infection. This helps to detect ransomware that tries to communicate with command-and-control servers or send ransom-related data.

Blockchain Transaction Tracking Algorithm: This algorithm is used to track ransom payments made in virtual currencies such as Bitcoin, Ethereum, or other cryptocurrencies. By monitoring blockchain transactions, the algorithm identifies and traces payments made to the ransomware wallet addresses. It analyzes transaction histories, helping to uncover the flow of ransom payments and potentially link the activity to a specific ransomware campaign or attacker.

Digital Evidence Collection Algorithm: To conduct a thorough forensic investigation, it is essential to collect and preserve digital evidence of the attack. This algorithm gathers system logs, file access records, network activity, and other relevant data during and after the attack. It organizes and indexes this data for later analysis, ensuring that crucial evidence is preserved and available for detailed examination.

Ransomware Behavioral Signature Algorithm: This algorithm works by identifying specific patterns or signatures of ransomware behavior. These signatures can include typical encryption methods, file extension changes, or abnormal file access patterns. The algorithm compares system activity with known ransomware signatures, flagging suspicious behaviors that match these signatures. It helps to quickly identify and respond to new ransomware threats based on their behavioral characteristics.

These algorithms are integrated into the system to provide a multi-layered defense against crypto-ransomware attacks. By combining file monitoring, process analysis, network traffic inspection, blockchain tracking, and forensic evidence collection, the system is able to detect, analyze, and trace the activities of ransomware attacks effectively, especially those demanding virtual currency payments.

RESULTS

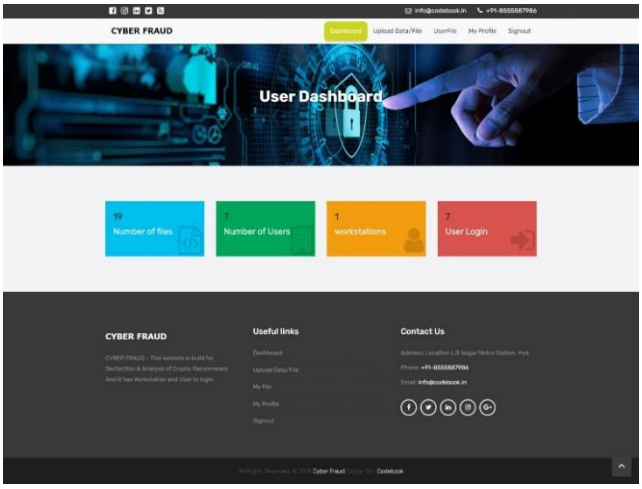

Fig 1 :User Dashboard

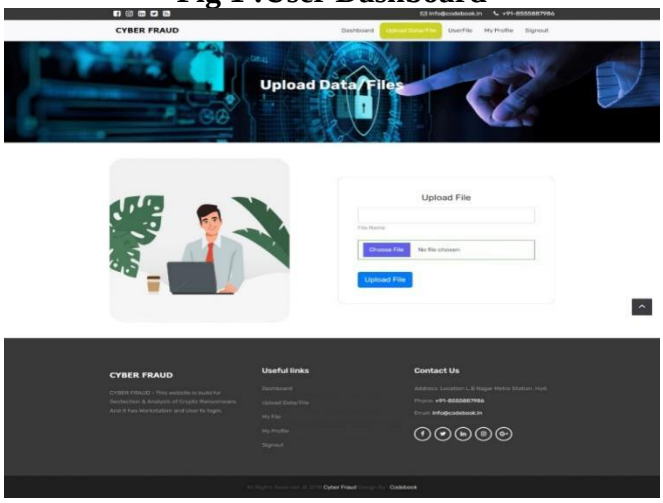

Fig 2 :Upload Data Files

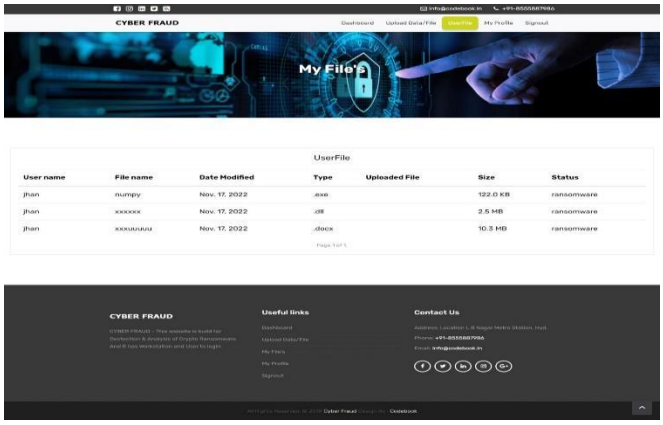

Fig 3:My Files

Fig4 :Encrypted Files

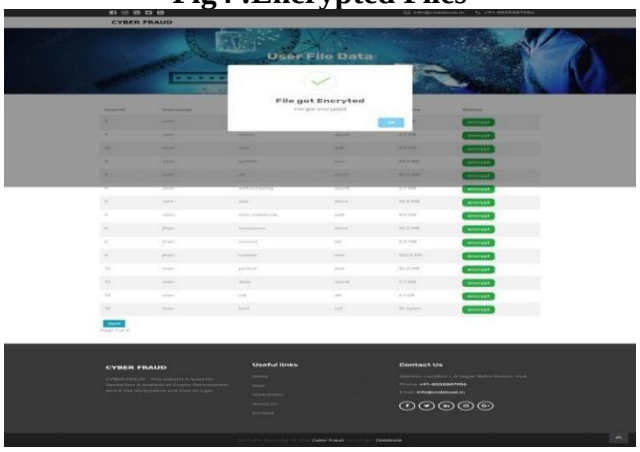

Fig5 :Secured Files

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.

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.