Cyber Fraud: Crypto Ransom ware Analysis and Detection

Dr. G Ahmed Zeeshan[1], Dr. Sara Ali[2], Dr. E Mohan[3]
Associate Professor, Professor[2,3]
Department of CSE
Global Institute of Engineering and Technology

ABSTRACT

The current meteoric rise in the usage of virtual money (such as Bitcoin, Ethereum, Ripple, and Litecoin) has attracted malicious actors who have developed and distributed ransomware to extort users for their digital assets. This malware sneaks into the victim's system via cunningly crafted means and encrypts all of the data located there. Following the encryption procedure, the assailant sends a message threatening inaccessibility of the encrypted data unless a ransom in virtual currency is paid. At the moment, this kind of ransomware poses the greatest risk to IT security since it is rapidly growing in popularity. Detection and analysis of cyberbullying has been the subject of several research in the literature. This research looked specifically at crypto-ransomware and examined a forensic investigation of a real-world attack case. By studying the attack technique and behavior of the crypto-ransomware, we were able to determine that the attacker's personal information was available in this case. We believe our work will make a substantial contribution to the fight against this menace with this dimension.

1. INTRODUCTION

New dangers have surfaced alongside the conveniences brought about by the information and technology sector's fast expansion. The target, kind, and techniques of assault have all changed due to the attackers' quick adaptation to new technology. A new generation of security measures is required to cope with these dangers by governmental organizations and institutions, commercial firms, and even ordinary internet users. Cyberattacks have persisted despite all efforts to prevent them. Ransomware is becoming the cyberattack type most often seen. Malicious software or virus known as ransomware encrypts the user's data and then demands payment to decrypt it. The two main types of ransomware that are often studied are crypto-ransomware and crypto locker ransomware. Most people agree that crypto-ransomware was the first kind of contemporary ransomware.

Until the ransom is paid, this virus will block the victim's operating system or system entry. The standard method of demanding ransom is by the use of a code for a prepaid card, electronic card system, or telephone message. By encrypting a specific subset of data, crypto-ransomware blocks access until the user inputs a code key.

These days, crypto-ransomware has surpassed all other malware in terms of popularity. As the usage of virtual currencies grows globally, so does the attention of potential attackers. The virus is built on the idea of virtual currency, which are convenient and impossible to track. Following encryption, crypto-ransomware has the ability to erase data from the affected user's computer. A notice saying that the files are encrypted and payment is necessary is flashed on the screen whenever the user tries to access the files they seek. Once the victim's PC is inaccessible, the attacker takes possession of the encrypted data and promises to unlock them once the ransom is paid. According to the samples we looked at, decrypting the data becomes very difficult even after paying the ransom.

2. LITERATURE SURVEY

With the expansion and improvement of the internet, cyber fraud has emerged as a major issue in the contemporary day. There has been a lot of focus on crypto ransomware as a kind of cyber fraud recently. Threat actors use crypto ransomware to encrypt victims' data and then demand money in return for decryption key. Finding and analyzing crypto ransomware is the main topic of this literature review.

In order to identify and analyze crypto ransomware, this study suggests a method that relies on machine learning. To get characteristics out of the ransomware samples, the writers employ both static and dynamic

analysis methods. With these characteristics in hand, they train machine learning models to identify ransomware. Detection rates are high and false positive rates are minimal, according to the authors.

"Crypto Ransomware Detection and Analysis Techniques: A Survey" written by S. Singh, S. Saini, and others

Finding and analyzing crypto ransomware has been the subject of several suggested methods, and this comprehensive study summarizes them all. The authors classify these methods primarily into three groups: hybrid approaches, behavior-based techniques, and signature-based strategies. They also point out areas that still need more investigation and evaluate the merits of each technique.

The purpose of this survey study is to examine machine learning methods for detecting ransomware, particularly crypto ransomware. The writers survey several ML algorithms—such as decision trees, neural networks, and support vector machines—that have served this function. Additionally, they go into the pros and cons of using machine learning to identify ransomware.

A behavior-based method for crypto ransomware detection is presented in this research. In order to detect ransomware, the authors utilize a mix of machine learning and system call monitoring. Their detection rates are high while their false positive rates are low.

Various crypto ransomware families are covered in this survey article, along with the recommended detection approaches. Crypto ransomware may elude typical detection procedures, which is one of the issues discussed by the writers. Additionally, they pinpoint areas that might benefit from further investigation into ransomware detection.

Developing efficient approaches for identifying and analyzing crypto ransomware is emphasized throughout these publications. Although there are still several obstacles to overcome, machine learning methods show promise for this task. The ever-changing nature of crypto ransomware necessitates constant research into new detection methods so that we can remain one step ahead of cybercriminals.

3. EXISTING SYSTEM

The detection and analysis of ransomware has so far made use of a wide variety of methods. Most of the attention is going into algorithms that use detection logic based on signatures [11]. The approach's efficacy is questionable because of its flaws. Traditional signature-based methods cannot detect new-generation (fileless) ransomware. To address these shortcomings, new methods are constantly being created. Some of these methods include dynamic analysis, which looks at how ransomware operates.

An approach to ransomware detection using signatures and graphic mining was introduced by Fatemah et al. They were able to identify 96.6% of the time, according to the research [12].

In order to combat ransomware, Daniele et al. [13] created a method for dynamic analysis that makes use of machine learning reasoning. To detect and avoid crypto-ransomware, Donghyun et al. [14] suggested a digital model in 2015.

3.2 Suggested Framework

Our suggested architectural scheme is detailed in this section. Cryptoransomware detection and analysis were the primary goals of the study's recommended methodology model. We have a three-part strategy. Here they are:

• First Unit.

A snapshot, or forensic copy, of the infected machine is captured. Images are one-to-one representations of the data storage units of the examined materials. Photographs of physical and cognitive processes may be captured using two distinct techniques. We do all analysis on this picture in a secure setting, namely on a workstation. The objective is to safeguard the live system from any potential danger.

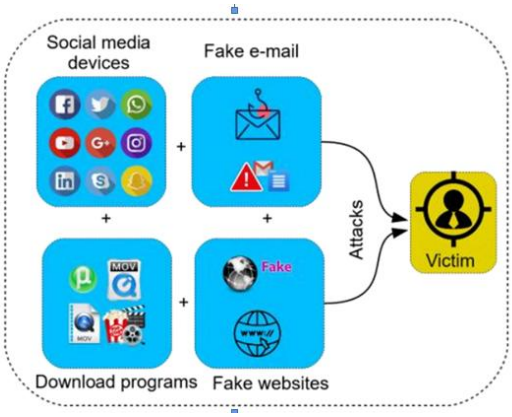
Module 2.

The picture examination process starts when the analysis environment is set up. Completed analyses, ranging from the most basic to the most complex, are compiled here. Finding any ransomware has to be done first. This is the last step if the PC was found to be safe. The first step in identifying ransomware is to gather information about it without actually running it. Analysis of the ransomware's signature behavior, including file-array transfers and code architecture, is carried out after execution. Finally, in an effort to get in touch with the ransomware perpetrator, it is possible to look into doing so.

• Unit 3

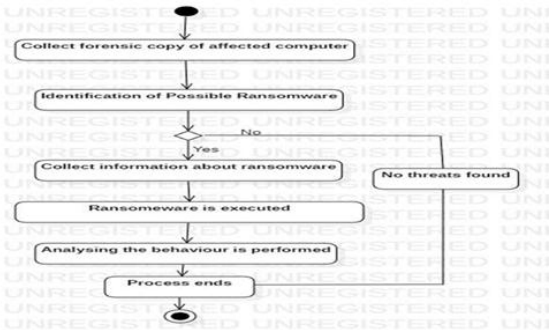
The results of the studies are then submitted to the investigating units or made public for use in the event of future assaults of a similar kind.

4.SYSTEM ARCHITECTURE .



Activity Diagram

A graphical representation of the work process of stepwise exercises and activities with support for decision, emphasis and simultaneousness, used to depict the business and operational well-ordered stream of parts in a framework furthermore demonstrates the general stream of control.



5. SYSTEM IMPLEMENTATION

MODULES

1.TAKE IMAGE (FORENSIC COPY) OF THE COMPUTER

2.INVESTIGATION AND ANALYSIS OF THE IMAGE

3.EXECUTION OF RANSOMWARE

5.1.1 Take Image (forensic copy) Of The Computer

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.

5.1.2 Investigation and Analysis of the Image

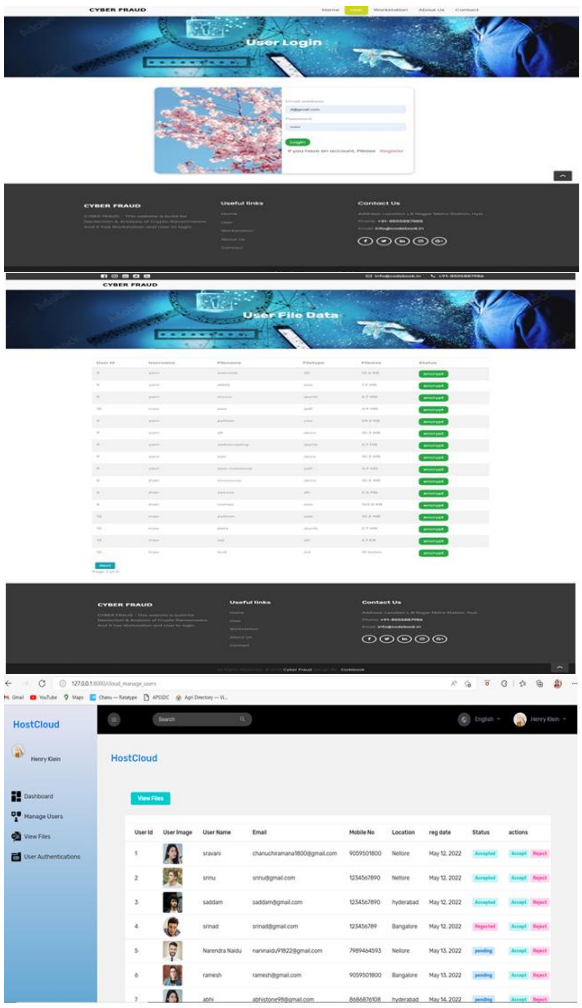
After creating the analysis environment, investigations of the image begin. In this step, analyses are completed from simple towards complicated methods. The first step is identification of possible ransomware. If there is no threat identified on the computer, the process ends at this step. If ransomware is identified, the first stage is to collect information about the ransomware without executing it. Later the ransomware is executed and characteristic behaviour (file-array movements, code

architecture) analysis is performed. In the final step, the possibility contacting the ransomware attacker is investigated in an attempt to obtain contact information.

5.1.3 Execution of Ransomware

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

fig.7. 1 Home page



6.1 TYPES OF TESTING

■Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

■Integration testing

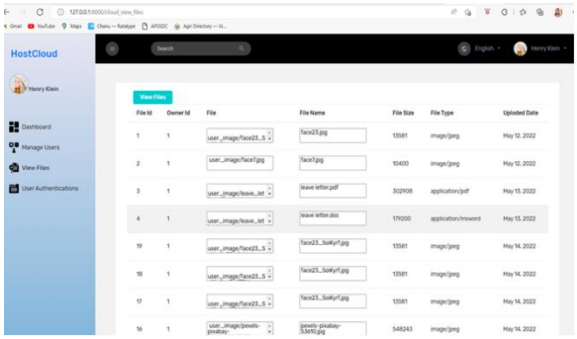
Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

■Functional test

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

7.RESULTS



8. CONCLUSION & FUTURE WORK

The prevalence of crypto-ransomware assaults has skyrocketed, paralleling the meteoric rise in value of digital currencies. The difficulty in lawfully tracking virtual money is the root cause of this predicament. The perpetrators use crypto-ransomware to encrypt the victim's data and then demand payment for a decryption key. The ransomware encryption method is widely acknowledged as being theoretically hard to decrypt via external means. After encrypting data on the victim's computer, the hacker removes them and claims to have them stored in a secure location. Recently, cybercriminals have been sending messages claiming they can decrypt a file up to 100 MB in size that the victim specifies, all in an effort to trick them into believing the lie. Gaining access to the file is as simple as getting the victim to agree. Once the victim pays the requested ransom, however, the attacker has accomplished their goal and contact stops.

Ransomware analysis includes finding the malware, learning how it operates, and tracking down the perpetrator. In order to deduce the crypto-ransomware's structure and how it interacts with the system, researchers use reverse engineering approaches.

REFERENCES

Reference: [1] Egele, Kirda, Scholte, and Kruegel (2008).The methods and tools for automated dynamic malware analysis are reviewed here.CSUR, volume 44, issue 2, pages 1–4.

Citation: [2] Kim, D., Shin, D., and Kim, Y. H., 2019. An program that uses log analysis to identify attacks on mobile systems, complete with an attack tree. Chapters 184–192 of the journal Mobile Networks and Applications, volume 24, issue 1.

In 2018, F. L. Lévesque, S. Chiasson, A. Somayaji, and J. M. Fernandez published a work together. A clinical trial approach to computer security: the human and technological aspects of virus assaults. Journal of the Association for Computing Machinery (ACTM): Transactions on Privacy and Security (TOPS), 21(4), 1-30.

"4" (2019) by İ. Kara and M. Aydos. Technical investigation of remote access trojan: a specter in the system. Volume 11, Issue 1 of the International Journal on Information Technologies and Security.

5. Kara, I., and Aydos, M., December 2018. Cerber ransomware of the third generation: static and dynamic analysis. Presented at the 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT) (pp. 12-17). IEEE.

Citation: [6] Al-rimy, B. A., Maarof, M. A., and Shaid, S. Z. M. (2018). The causes, taxonomy, and countermeasures of ransomware threats: a survey and suggestions for future study. Computers & Security, volume 74, pages 144–166.

S. Baek, Y. Jung, A. Mohaisen, S. Lee, and D. Nyang published a paper in July of 2018.SSDinsider: A flawless data recovery solution that protects solid-state drives against ransomware from inside. Pages 875–884 in 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS).IEEE.