Ransomware in IoT: A Digitized Nightmare

Shaik Asif Hussain[1], Zahraa Alrikabi[1] and Khoula Al Harthy[1#]

[1]Middle East College, Muscat, Oman
[#]Advisor

ABSTRACT

One of the most exponentially growing issues in the world of computing is malware, specifically ransomware. Ransomware is the leading cause of data loss and corruption, which is caused by the encryption of files by an attacker who demands a ransom fee that must be paid to regain access to the encrypted files. There are two main types of ransomwares: locker ransomware and crypto ransomware. The focus here will be crypto ransomware. The Internet of Things – IoT – is usually an overlooked security concern by many organizations and companies. If a vulnerable IoT device is found by an attacker, they can easily exploit it and launch a ransomware attack through it. This will, in turn, compromise and potentially lock the entire system, blocking all users from accessing any data. This paper discusses the impact of ransomware in IoT and how the attack takes place in an IoT device. Further, it talks about the initial stages of an algorithm that can be used to detect anomalies in IoT devices that are relevant to ransomware attack. This can help prevent such an attack from being launched by taking the appropriate preventative measures.

Introduction

Viruses are no strangers to the everyday user. In fact, they have become increasingly common to the point where downloading an anti-malware application is common practice. Although these applications can prevent and quarantining most simple viruses, they usually fail at catching ransomware, which leads to data loss and corruption. Because of ransomware, many companies have suffered monetary losses worth millions of dollars. However, the network is not the only affected system anymore. The Internet of Things, more commonly known as IoT, can be affected by ransomware attacks, even crypto ransomware attacks. Things like smart cameras, smart TVs, fingerprint detection systems, anything connected to the internet, is susceptible to this malicious virus. Thus, developing an algorithm that can detect such attacks is crucial in terms of security and safety. As previously mentioned, the growth of viruses is not going to stop any time soon. In fact, it has only increased ever since the start of the pandemic. Since most companies and organizations have switched to depending on the cloud, data centers, IoT devices, and anything connected to the internet. While this provides the companies with many advantages in terms of availability and continuity, there will always be some disadvantages here and there. One of the biggest disadvantages would be their vulnerability to malicious attacks greatly increasing – ransomware being one of them. Thus, designing a ransomware detection algorithm will greatly benefit organizations across Oman with preventing disastrous data loss and data corruption.

Literature Review

Hu's paper provides an in-depth explanation about the different types of encryptions used in ransomware and the different types of decryptions as well. It starts off with a brief history on what ransomware is and how it came to be and defines the different types of ransomwares that currently exist. Further, it shows several examples of ransomware attacks that have taken place throughout the years and explains how they have affected the targeted systems. To conclude, this paper focuses on how the encryption methods are becoming stronger by the day. Therefore, instead of focusing on cracking them and decrypting them, it would be a better idea to shift the focus to defending against

ransomware (Hu, 2017). In the next paper written by Egunjobi et al., it starts off with a brief history of ransomware and how it has affected millions of systems all across the world wide web. Further, it explains how previous solutions to older ransomware can no longer be as efficient as malicious users are able to exploit their vulnerabilities and render them useless. Thus, this research shows how a classification technique that combines static and dynamic information to improve the detection and classification of ransomware can be used. Supervised machine learning algorithms are trained on a test set and utilize a confusion matrix to measure accuracy, allowing us to compare each algorithm in detail. In this study, supervised algorithms such as the Nave Bayes algorithm achieved a test set accuracy of 96%, SVM 99.5%, random forest 99.5%, and 96%. Youdens index is also used to measure sensitivity and specificity(Egunjobi et al., n.d.). Therefore, this paper also aims to reduce the number of false positives produced in relevance to ransomware attacks. For this reason, samples of older ransomware were collected to help improve the accuracy of this research. Additionally, this paper, written by Bello et al., talks about how ransomware attacks have been targeting infrastructures related to information security more and more as of late. For this reason, this paper aims to delve into algorithms used in machine and deep learning that can detect and potentially ward off ransomware. Unlike prior evaluations on ransomware attacks, this study intends to undertake a thorough assessment on ransomware attack detection utilizing clever machine learning techniques. The study examined the literature from several viewpoints, with a focus on intelligent algorithms for ransomware detection. Deep learning algorithms are gaining popularity due to their capacity to handle enormous datasets, importance in the scientific community, and ability to solve problems better than traditional intelligent algorithms(Bello et al., 2021). Future research opportunities, big data analytics, and deep learning to handle survey-identified difficulties are highlighted, providing the scientific community with a fresh direction in dealing with ransomware assaults. Further, in “Kharraz et al’s paper, it was stated in their paper that Ransomware is an attack that locks the user out of their system and requests money in return. That is the gist of what ransomware is. Even though users are always recommended to have a reliable backup strategy, the growing number of victims falling for these attacks in recent years suggests it is required for new defense mechanisms that minimize the destructive effects of ransomware attacks (Kharraz et al., 2018). Howbeit, there are undeniable similarities between ransomware and other types of malware attacks. This article summarizes some of the challenges in developing anti-ransomware solutions by considering the differences and similarities amongst different malware attacks and ransomware attacks. Lastly, this paper, by Kolodenker et al., proposes a prototype with the name of “PayBreak”, which is used to defend systems against ransomware attacks – cryptographic ransomware attacks. This sample is based on the realization that secure file encryption relies on hybrid encryption, in which symmetric session keys are utilized on the target machine. PayBreak then monitors the usage of these keys, maintains them in safe-keeping, and thus decrypts files that would otherwise be recoverable solely by paying the ransom. This prototype uses low overhead hooking techniques that are dynamic and asymmetric encryption to implement a key escrow mechanism that enables victims to retrieve ransomware-encrypted files. To conclude, PayBreak was tested against twenty distinct ransomware and demonstrated that the proposed solution can restore all files encrypted by samples from twelve of these attacks. This is including the infamous CryptoLocker and more contemporary threats like SamSam and Locky (Kolodenker et al., n.d.). Lastly, PayBreak accomplishes its protective role with low performance overhead for the common office workloads, making it suitable for use as a practical online security system.

Methodology

The methodology that has been decided to be chosen is the Kanban Methodology. This methodology is the most suitable type for this research article, especially since it falls under the agile category, which is known to be used with projects related to the world of computing.

The Kanban Methodology

The word “Kanban” is of Japanese origin, and it means billboard. This methodology was developed by a Japanese engineer in the 1940’s with the name of Taiichi Ohno and it falls under the agile methodology model (Kissflow, 2022). The main focus of the Kanban methodology is the fact that it is more on the visual side when compared to other methodologies. Further, this methodology utilizes something known as the Kanban board as well as Kanban tools in general. A Kanban board is a type of a Kanban tool that envisions the entire track of the project (Kissflow, 2022). Some software sites that use Kanban tools are Trello and Kissflow. The way a Kanban board works is quite simple: it is made up of different lists such as to-do tasks, in-progress tasks, and completed tasks. Furthermore, the Kanban system in general is known to be a pull system that uses the Work in Progress (WIP) principle. To go into further detail, a pull system kind of functions similarly to a vending machine: a Kanban system replaces whatever is completed, or restocks what has been completely run out in the case of a vending machine (Kissflow, 2022). Next, the WIP principle provides the methodology with consistency and order. Of course, the Kanban methodology has its pros and cons:

Advantages

- Readily accessible to anyone since there are many websites and applications for Kanban boards.
- Flexible and customizable (Cohen, 2022).
- A significantly responsive system with no delays.
- Due to its visual nature, tasks are displayed clearly.

Disadvantages

- Requires constant maintenance and updates.
- Lack of timeframes (Kanbanchi, 2021).

There is not one way to truly represent a Kanban Methodology, but the general framework can be shown below:

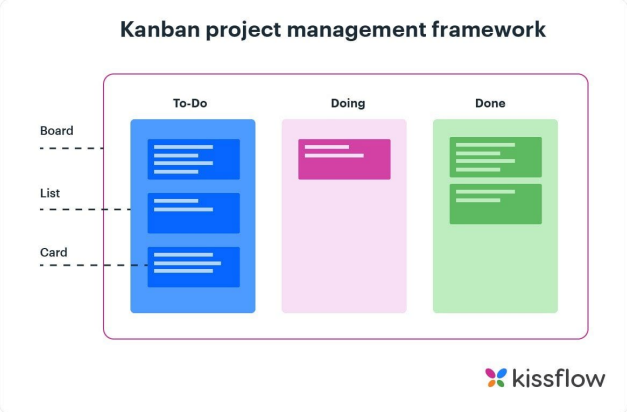

Figure 1. Kanban Methodology (Kissflow, 2022)

Design and Discussion

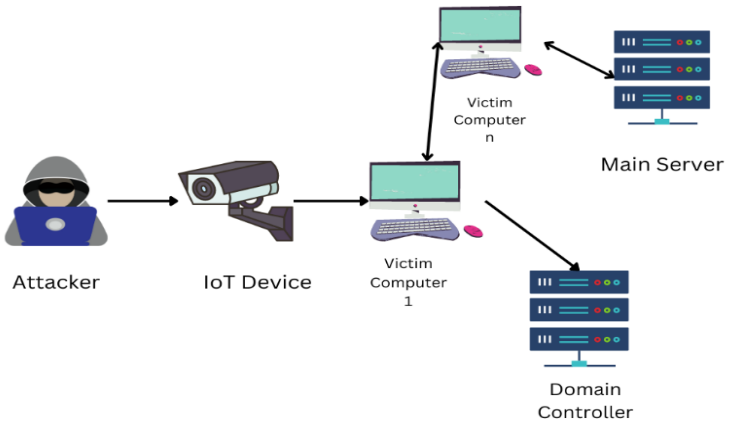

Figure 2. Ransomware attack

The figure above starts by demonstrating the attacker accessing an IoT device in an establishment. This connection was established due to either a vulnerability or an exploitation of the IoT device. Such vulnerabilities happen since IoT security is usually overlooked, since no one would think about a smart TV, or a smart CCTV camera being hacked by a malicious user. Once the hacker has successfully penetrated the device, they can find further vulnerabilities such as weak passwords to further enter the system. In this case, the figures display several victim computers being exploited by the attacker. This can then lead to the entire system being compromised by having the domain controller exploited, as well as the main server. Once the malicious user has taken over the entire system, they can now start encrypting files and locking out users, whilst asking for a ransom payment to actually return access. However, it must be kept in mind that even when the payment is made, it is not guaranteed that the decryption key will be given.

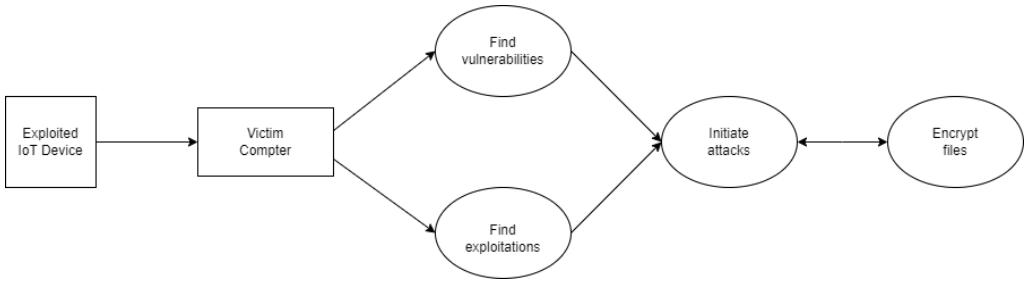

Figure 3. In depth ransomware attack

The figure above shows the procedure of the ransomware attack that takes place in a victim computer, through an exploited IoT device. Once the hacker has gained access to the victim's computer, they will try to find vulnerabilities and exploits by searching for bugs, weak backdoors, weak passwords, weak logins, and even bad or redundant code. After gaining access to such vulnerabilities, the malicious user may now initiate the attack: this consists of all files being inaccessible by being encrypted. Once the whole system is encrypted, it is deemed unusable by anyone. All data has potentially been lost and can only be regained by paying the proposed ransom by the attacker. However, it is not guaranteed that the attacker will oblige and provide the key, given their malicious nature.

Algorithm

This algorithm will consist of several steps. The first step would be to gather the relevant data. In this case, that would be finding the vulnerabilities in the IoT device. The following equation can be presented:

$$X = \sum_{M}^{T} = V$$

Such that, X is the attacker, T is the traffic being monitored by the attacker, M is the message that represents the targeted files, and V is the established vulnerability in the IoT device. Further, analyzing the traffic is a crucial step that helps with finding any anomalies or backdoors in the IoT device. Once that is done, there will be a prediction that is divided into four classifications. This prediction helps with building the algorithm. These classifications are true positive (TP), true negative (TN), false positive (FP), and false negative (FN). From that, there will be three equations for accuracy, recall, and precision.

$$Accuracy = \frac{TPr + TNr}{TPr + TNr + FPr + FNr} \qquad Precision = \frac{TPr}{TPr+FPr}$$

$$Recall = \frac{TPr}{TPr + FNr}$$

Such that, the r stands for rate. Therefore, FPr = 1 -TNr and FNr = 1 – TPr (Egunjobi et al., n.d.).

Further,

$$TPr = \frac{TP}{TP+FN} \text{ (sensitivity)} \qquad FPr = \frac{FP}{FP+TN} \text{ (false alarm)}$$

$$TNr = \frac{TN}{TN+FP} \text{ (specificity)} \qquad FNr = \frac{FN}{FN+TP} \text{ (miss rate)}$$

The aforementioned rates help with measuring the tests' accuracy and also help with forming the three equations that were mentioned (Split, n.d.). Thus, these three equations work together to help build the algorithm and aid with the detection of ransomware in IoT.

Conclusion

To conclude, this research paper aims to raise more awareness about the dangers of ransomware and how destructive in nature it can get. Further, an algorithm is proposed to help detect ransomware related anomalies in IoT devices which can, in turn, allow the authorized personnel to take preventative measures and deny the attacker from executing such an attack.

References

Kanbanchi. (2021, September 9). Kanban Style Work Boards: Pros and Cons. https://www.kanbanchi.com/kanban-style-work-boards

Kissflow. (2022, March 2). What is Kanban Methodology | Introduction to Kanban Framework. https://kissflow.com/project/agile/kanban-methodology/

Cohen, E. (2022, November 2). Pros & Cons Of The Kanban Method In Project Management.

https://www.workamajig.com/blog/kanban-methodology-guide/pros-cons-kanban-method
Hu, Y. (2017, January 13). A brief summary of encryption method used in widespread ransomware. https://resources.infosecinstitute.com/topic/a-brief-summary-of-encryption-method-used-in-widespread-ransomware/
Bello, I., Chiroma, H., Abdullahi, U. A., Gital, A. Y., Jauro, F., Khan, A., Okesola, J. O., & Abdulhamid, S. M. (2021). Detecting ransomware attacks using intelligent algorithms: recent development and next direction from deep learning and big data perspectives. Journal of Ambient Intelligence and Humanized Computing, 12(9), 8699–8717. https://doi.org/10.1007/S12652-020-02630-7/METRICS
Egunjobi, S., Parkinson, S., & Crampton, A. (n.d.). Classifying Ransomware Using Machine Learning Algorithms. https://www.researchgate.net/publication/337077991_Classifying_Ransomware_Using_Machine_Learning_AlgorithmsBello, I., Chiroma, H., Abdullahi, U. A., Gital, A. Y., Jauro, F., Khan, A., Okesola, J. O., & Abdulhamid, S. M. (2021). Detecting ransomware attacks using intelligent algorithms: recent development and next direction from deep learning and big data perspectives. Journal of Ambient Intelligence and Humanized Computing, 12(9), 8699–8717. https://doi.org/10.1007/S12652-020-02630-7/METRICS
Cohen, E. (2022, November 2). Pros & Cons Of The Kanban Method In Project Management. https://www.workamajig.com/blog/kanban-methodology-guide/pros-cons-kanban-method
Egunjobi, S., Parkinson, S., & Crampton, A. (n.d.). Classifying Ransomware Using Machine Learning Algorithms.
Hu, Y. (2017, January 13). A brief summary of encryption method used in widespread ransomware. https://resources.infosecinstitute.com/topic/a-brief-summary-of-encryption-method-used-in-widespread-ransomware/
Kanbanchi. (2021, September 9). Kanban Style Work Boards: Pros and Cons. https://www.kanbanchi.com/kanban-style-work-boards
Kharraz, A., Robertson, W., & Kirda, E. (2018, June). Protecting against Ransomware: A New Line of Research or Restating Classic Ideas? https://kharraz.org/publications/2018magazine.pdf
Kissflow. (2022, March 2). What is Kanban Methodology | Introduction to Kanban Framework. https://kissflow.com/project/agile/kanban-methodology/
Kolodenker, E., Koch, W., Stringhini, G., & Egele, M. (n.d.). PayBreak : Defense Against Cryptographic Ransomware. https://doi.org/10.1145/3052973.3053035
Split. (n.d.). False Positive Rate. Retrieved May 3, 2023, from https://www.split.io/glossary/false-positive-rate/