Review Article

BIOMEDICAL Journal of Scientific & Technical Research

ISSN: 2574 -1241

DOI: 10.26717/BJSTR.2021.35.005649

Ransomware Attacks on Remote Learning Systems in 21st Century: A Survey

Fadele Ayotunde Alaba*[1] and Abayomi Jegede[2]

[1]*Department of Computer Science, Federal College of Education, Nigeria*

[2]*Department of Computer Science, University of Jos, Nigeria*

***Corresponding author:** Fadele Ayotunde Alaba, Department of Computer Science, Federal College of Education, Zaria, Nigeria

ARTICLE INFO

Received: 📅 April 05, 2020

Published: 📅 April 15, 2021

Citation: Fadele Ayotunde Alaba, Abayomi Jegede. Ransomware Attacks on Remote Learning Systems in 21st Century: A Survey. Biomed J Sci & Tech Res 35(1)-2021. BJSTR. MS.ID.005649.

Keywords: Ransomware; Encryption; Detection; Malware; Attack

ABSTRACT

The expanded use of computers and IT draws the attention of cybercriminals who design different strategies to jeopardize data and information protection and privacy of legitimate users. To jeopardize privacy, honesty, and availability of the data and information saved, interpreted, and distributed by machines, this is done by unscrupulous security scheme approaches in hardware and software systems. To make unauthorized entry, reveal, or modify data, malicious persons exploit vulnerabilities in computers, programs, and applications. An effective assault on a computer system like Ransomware could lead to devastating losses for individuals and groups. Financial information, scores, and medical records will be revealed in access to confidential personal details. Besides, ransomware poses growing risks to the enterprise and individual files and computers. It blocks the use of corrupted files or stolen computers to innocent victims until they normally pay a ransom in bitcoin form. In certain instances, even though a survivor pays the ransom, hackers do not have the decryption key. At times, attempting to decrypt files using the attacker's key does more damage to systems-speiched files. Technological advances such as malware developing packages, bitcoins, and ransomware make it easier to maximize the number of ransomware attacks on personal computers, networks, and mobile devices. The study document aims to identify the attacks of ransomware and examine their effect on distant learning. There will be extensive discussion and analysis of different solutions and strategies. A detailed understanding of each of the technical difficulties and pitfalls for both organizations and developers is presented. Finally, the report would offer a general guideline for some preventive steps following the analysis on the effect and harm caused by ransomware that should be put in place to avoid such dangerous attacks on devices and infrastructure of remote learning.

Introduction

The future has changed most through digital conversion if not all content has been digital information. In addition, the automated data collection mechanism facilitating the bulk of the official transactions, such as financial transactions, have made all transactions electronically for the clients regardless of where they are. The data and information are readily visible and can be recovered. In addition, it simplifies and speeds up communication and collaboration across various sectors. While digital information has improved the life of people in different fields, there are still some shortcomings and deficiencies that could impact the easing of operations like cyber-attacks. Cyber-attacks that are called cyberspace offences committed by internet criminals or hackers are aimed at harming the device or network of a person or an organization to make profits or reprisals. Any of the cyber threats, for instance phishing, spyware, spam, trojan and ransomware, would be the last to be focused on by the post. Ransomware is malicious software which tries to lock or encrypt data and files for the purposes of money-making (demanding ransom). Ransomware was described as the Webster dictionary "malware which requires a victim to pay for a restitution to access encrypted files" (Merriam-Webster's dictionary, 2020).

From the ransomware description it can be understood that this attack is one of the risky threats that can allow the system to get out without losses. Once the victim has been locked, it prohibits them from accessing their files and results. Sensitive files, including financial records, corporate databases, or personal files, are also attacked by Ransomware. Attackers then call for money to decrypt the data and files. The main objective of such attacks is typically money. There are several ways to accomplish their objectives, including calls to the unauthorized publication of private content and confidential content among the victims [1]. There were therefore two alternatives open to the survivor in this situation, either to pay them no guarantee that the data will be decrypted and recovered or to format their machines. Software and networks blockage can have detrimental effects, and multiple data issues can result, in lack of productivities and expenditure of time to recover files and services, and loss of useful information on a permanent or temporary basis [2]. Moreover, the economic problems which occur because of paying ransoms and income losses due to the suspension of development, such as governmental, education and others [3].

However, cybercrimes have an impact that exceeds shutdown and data and money loss schemes, which can lead to life loss. The first cyber-attack death in Germany was declared according to the New York Times on 11 September 2020 [4]. The crash occurred after which a woman was diagnosed as a critical illness and emergency when she went to Düsseldorf University Hospital. Consequently, she wanted a medical emergency. Surprisingly, medical personnel detected the cyber hackers that used ransomware attacks in attempt to compel the hospital to pay a rescue to release their devices compromised all operating systems, in addition to patient hospital data registers. There are various and distinct ransomware attacks in previous years [5] that have imperiled several corporations, organizations and governments. The "WannaCry" that started on 12 May 2017 targeted many hospitals, colleges, and governmental institutions was one of the worst waves ever. It passed through at least 150 universities and in 48 hours it corrupted some 230,000 computers and killed more than 2,00,000 people. "This has triggered film effects, hospitals paralyzed, transit grids interrupted and industries immobilized" [6,7].

Today, following the declaration on 30 January 2020 [8], by the Global Health Organization of COVID-19 as a pandemic, several governments/county countries have adopted distance learning to supplement a conventional education solution to disease prevention and avoid the outbreak of the virus between students and workers [6]. Converting into remote teaching means that, apart from students and computers, school networks and university systems are exposed to bugs, ransomware and cybercrimes, especially because certain people or students have no experience defending their devices from hackers and malware [9]. In addition, the issue of the nature and impact of cyber-attacks to distant learning risks and challenges in the education sector is being asked and of how this can be prevented?

"Prevention is better than treatment" says the general saying that with the recent growth of attacks because of accelerated technological progress, weaknesses have arisen in the field of digital technologies and in the education sector. Therefore, it is important to define security measures and how to deal with ransomware attacks. The objectives of the research paper are to categorize the ransomware attacks and analyze the impact of these attacks in distant learning. Different solutions and techniques are thoroughly discussed and analyzed. Detailed knowledge for both organizations and entrepreneurs also includes of the technical difficulties and disadvantages. In conclusion, the study would include a general guideline, after a review of the effect and harm caused by ransomware, on some mitigation steps which should be taken to stop such risky attacks on remote learning devices and infrastructures. This paper is organized as follows. In section 2, we provide an extensive literature review on ransomware. Section 3 discussed the framework for analyzing ransomware using machine learning. Section 4 present the research discussion. The recommendation was provided in section 5. While section 6 concludes the paper.

Literature Review

In this section, some security strategies and techniques to detect and avoid ransomware attacks will be addressed. Common approaches such as anti-viruses to identify and prevent machines from being infected have been used for combating attacks and identifying malware. Users are often asked what services they try to reach, websites, e-mail attachments and connections. Backup methods are essential in order to protect from threats by their different versions, and could help to re-image viruses, machines and workstations and recover archives [10]. New sophisticated malware families though, thanks to their complicated algorithms, are difficult to detect using standard approaches. This includes techniques.

Honeypot

Honeypot is a tool developed specifically to identify and capture various approaches to attacks used by hackers (Seungjin). The honeypot strategy does not prevent or reduce attackers' target systems [11]. Thus, Honeypot's primary function is to gather and not deter information on the attack. Since it is a fake network administrator machine resource to serve as a decoy and to identify any unauthorized [12] entry. This method also functions as an interference file for the malware, i.e., it is a technique that can interrupt hackers into your system/server [13]. Honeypot's task is to be quiet and assume that the intruder is a real world. There are honeypots such that it is called a productive device and targeted by the attackers. It extracts data from the perpetrator and gives information about the assailant's movements [14]. In addition, the honeypot scheme must contain files to make the assailant believe it is a lawful server, not a decoy. In this situation, it is important that the user knows and has the characteristics of the ransomware types and the files that ransomware will invade. A proper safety system is then implemented on the network to prevent these attacks [15].

In summary, the Honeypot is widely classified in two categories: testing and manufacturing honeypots [11]. The Honeypots research is used to collect maximum information. This knowledge is used to understand the present threat and to create a stronger defense, while the manufacturing honeypot collects details about the attacker and mitigates the risks of the organization. The accelerated production and growth of high technology devices is currently increasing the number of ransomware attackers on different devices [16]. The Internet of Substances (IoT) is currently a trendy technical and research area. However, researchers have gained an interest in proposing various homeopathical approaches for tackling ransomware attacks based on their benefit and suitability for IoT applications for consumers to gather their trust in these devices. These include, [5,11], who uses social leopard algorithm to build an IDH that detects ransomware attacks on IoT networks. Intrusion detection honeypot(s).

Honey Checking and Complex Event Processing are the mechanism proposed (CEP). The proposed IDH uses the CEP approach to compare the host functionality, network functionality and various activities of other applications such as the audit watch and firewall, which increases the accuracy of the aggregated performance. In the development area, the proposed IDH can also be easily deployed. The findings indicate that the Honey used to track file system activity is incredibly real by showing its reaction to the ransomware of the host. The assessment further confirms that, without limited data loss, the IDH proposed is effective in restricting ransomware activity. The proposed functionality does not however include auto-tabling and transfers learning, the mechanism for optimizing loads in IoT devices. Likewise [14], honeypot techniques were developed using investigated ransomware detection methods. The methodology suggested can track all ransomware operations. The benefit of this technology is that the suggested strategy uses the “Event Sentry or Microsoft File Server Resource Manager File Screening Service” function for monitoring Windows safety logs after detection of illegal activity. Apps such as e-mail reminders when threats are observed are a problem.

In addition, the technique proposed is not meant to detect ransomware threats, which in turn is detrimental to device users. Moreover, the Dionaean honeypoth technique [15] was used for malware capture and analytics to capture various zero-day attacks and to ensure that the device has not been accessed/attacked. The strategy suggested can be divided into various classes depending on the actions and properties of caught Ransomware attacks. The classification would provide researchers with instructions on how to build a comprehensive malware protection system. However, on the higher operating system the system proposed cannot operate, except on the SQL 2000 XP version of windows. Additionally, the technique lacks high honeypot interaction capability.

A random forest approach for the identification of ransomware using a computer teaching technique was recently used by [17]. The main difference of the proposed strategy is to distribute disassembly by continuously abstracting the raw byte attributes, using a repetitive, programmed mining process that abnormally increases the detection speed. In addition [17], a new blocking method was proposed, which uses honeypots to detect and effectively avoid the spread of botnet in software-defined networks with disappointment techniques and botnet detection honeypots. The proposed technique has the potential to reduce the contamination rate to 25 per cent and to maximize the time expended by the competitor. This approach, however, lacks dispersed decoy managers that increase system traffic and thus decrease overall system output and productivity. We provide a summary of the existing Honeypot techniques presented in Table 1.

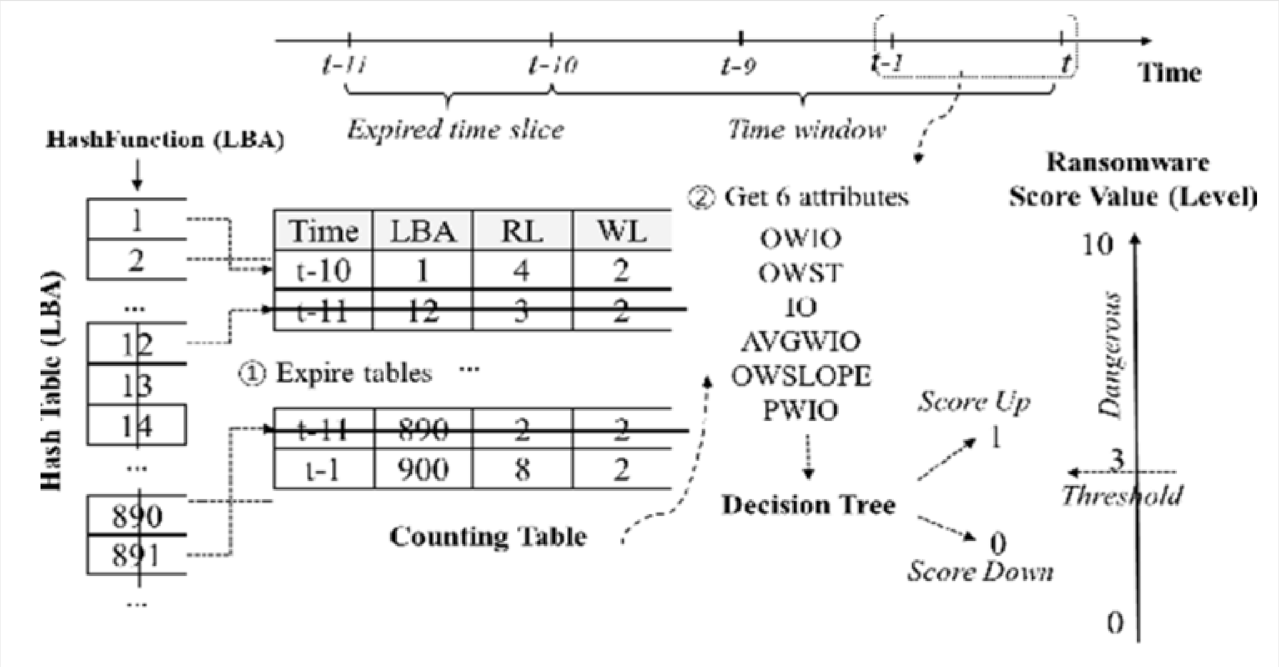
Table 1: The Existing Honeypot Techniques.

Author (s)	Title	Methodology	Purpose	Pros	Limitation
Moore [16]	Detecting honeypot technology ransomware	It used research explored approaches	To catch all ransomware behaviors	The Event Sentry and File Screening service is used to monitor Windows Safety logs.	Apps like email notifications when threats are observed are absent. Faults to detect new attacks through ransomware
Sibi Chakkaravarthy [23]	Design of Honeypot social leopard detecting attacks by using the social leopard Algorithm	Social Leopard Algorithm	To build a honeycomb for intrusion detection (IDH)	It can detect IoT network ransomware attacks	There is no self-tuning function and learning capacity is passed.
Sethia & Jeyasekar [22]	Malware detection by means of Random Forest Technique Dionaea honeypot Ransomware	Dionaea honeypot	For catching multiple assaults on zero days. To guarantee that the machine was not entered.	The captured ransomware attacks are divided into numerous categories. It helps and guides researchers in developing a robust malware protection mechanism	This will only run-on SQL 2000 XP Windows edition. It is not possible on a higher device. The strategy lacks a high degree of contact.

Khammas [14]	Detecting honeypot technology ransomware	Machine learning technique	To detect botnet dissemination in SDN and avoid it effectively.	The host infection rate can be decreased up to 25 percent. It may also maximize the wasted time of the opponent.	There are no dispersed decoy managers which increase the load on the system. It limits the completeness and efficiency of the method

SSD-Insider++

It is a ransomware scheme that protects user files from ransomware harm. It is a backup tool which saves copies of files in backup storage, it is found in the SSD console as a firmware. It has two functions, namely ransomware and very low-cost retrieval. When ransomware is discovered, it is executed to recover the original files using the delays of the disk [18]. This technique measures both inputs and outputs of malware. Each input or output request has four parts: time (i.e.); time, LBA (i.e., addressee with evidence as information starts to be played or written), RL and WL Input and Output Requests (this represents the length of successive reading or writing blocks of LBAs). A time window is defined as a monitoring schedule for the routine detection of malicious ransomware behavior. Figure 1 illustrates how this technique works. In Figure 1 Reading LBA 1 is the first submission. SSD-Insider++ produces a new entry, starting at LBA 1, with time stamp 0 seconds since there is no matched entry in the table. The table is also recorded. Initially, RL becomes 1 as one LBA is read. The second and third queries are read respectively by LBAs 2 and 3. Based on LBA 1, RL is changed to 3. As LBA 1 has been read. It is simply ignored because there are duplicate reads. While recovery storage data using this technique is provided in Figure 2.



Time	LBA	RL	WL
t-10	1	4	2
~~t-11~~	~~12~~	~~3~~	~~2~~

~~t-11~~	~~890~~	~~2~~	~~2~~
t-1	900	8	2

Figure 1: An Illustration of SSD-Insider++ [9].

Figure 2 shows knowledge recovery, data from the previous entries (i.e., LBA 0! PPA 0, LBA 1! PPA 1, and LBA 2! The LBA 3 data are reduced and thus its mapping entry is not important. SSD-Insider++ has a separate information structure, a recovery line that monitors the upsets of the LBAs and old PPAs, to track old versions of data. SSD-Insider++ sets in queue a pair of the LBA and the accompanying old PPA any time a change is issued to a new LBA. Using old LBAs/PPAs in the rows, SSD-Insider++ will figure out where old knowledge renditions are stored and use them later for recovery. Similarly, the reduced LBAs are handled. For instance, SSD-Insider++ places a pair of LBA 3/PPA 3 in the line when LBA 3 is discarded. Thus, the SSD-Insider++ can revive the deleted files even when it has not been used for ransomware after writing the encrypted ones elsewhere with different LBAs, since the information required is kept in the queue, which shown in Figure 2.

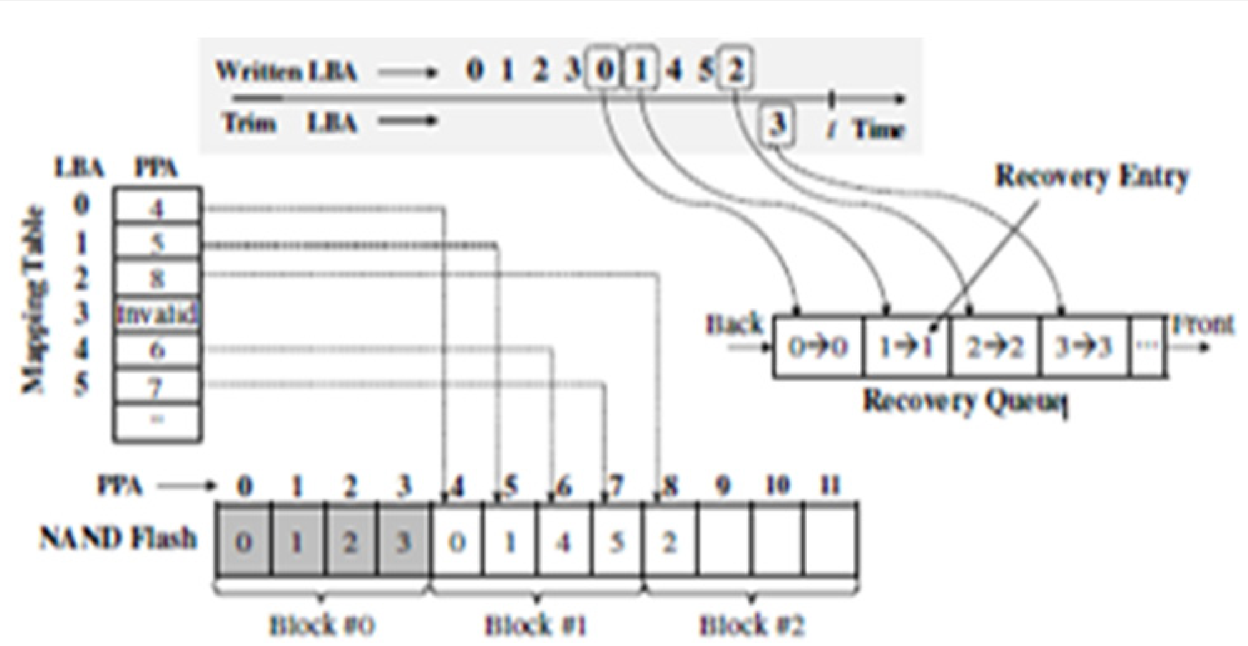


Figure 2: Recovery Storage Data using SSD-Insider++ [9].

Assume that the infection with the ransomware is found in t. New information is encrypted for LBAs 0, 1 and 2 and the malware removes the data for LBA 3. The original data is recovered only by modifying its mapping table to replace current mapping pairs (i.e., LBA 0! PPA 4, LBA 1! PPA 5, LBA 3!”-’ and LBA 8) with the old ones (i.e., LBA 0! LBA 1! PPA 1, LBA 2! PPA 2, and the LBA 3! PPA 3). FTL is only retrieved with modified mapper table data. The recovery queue expands as the upgrade and trim commands are issued by the SSD. As DRAM in an SSD is a valuable resource shared amongst other modules, all LBA/PPA pairs in DRAM can be maintained. Therefore, as the tail reaches height, SSD-Insider++ must reduce its full size and flush its contents into the flash. The input retrieval queue is 8-KB to conform to a physical page size of 8-KB. Each queue entry is composed of an LBA (4-byte), one PPA (4-byte) and one time stamp (4-byte), which keeps the sum of 682 entries in the memory queue of 8 KB. This ensures that, anywhere 682 commands are updated and trimmed, only a one-page flush procedure is needed.

Machine Learning

Machine learning is an artificial intelligence division that deals with the design and creation of algorithms and technologies that enable computers to have “learning” property. Two levels of learning are commonly available: inductive and deductive. General laws and decisions from Big Data inductively assumed. The key role of machine learn is to derive useful knowledge from data, so data mining, statistics and theoretical computer science are very similar to each other. In several areas from mechanics to medicine Machine Learning is included [17]. Machine learning renders a computational software for role analysis, and it allows the machine to measure observable results and enhance it, as this enhanced method increasingly expands computer programming knowledge without computer programming. Machine learning provides machine guidance to learn from data without providing the programmer with fresh step-by-step training, through decision making and data-based forecasting. The easy way to learn machines is to offer a learning algorithm training detail. In a wide range of fields including medical diagnosis, patterns recognition, natural language processing, robotics, computer games, traffic prediction, product recommendation, data mining, etc. mechanical learning is used.

The authors (Ray, 2019) explored the most used machine learning algorithms, such as Gradient Decrease, linear regression algorithm, multiple linear regression, Logistic regression, Decision Tree, Vector Machine Support (SVM), Bayesian Learning, Naïve Bayes (NB), K Nexest Neighbor (KNN). Stochastic Gradient Descent (SGD) will be tested as an example of machine learning with three kinds of problems, such as grouping, regression and clustering. The required machine learning algorithm could be used to pick “supervised learning,” “unsupervised learning” and “semi-supervised learning” based on available styles and categories of training data. The utilization of computer education seemed to the advantages of evaluating processes that rely on various algorithms for combating cyber criminality and ransomware programs.

Ransomware Detection Using Machine Learning: The rapid growth in internet use and technology lead to the emergence of many information and data-safety challenges for Internet users, called internet crimes, which are estimated to cost the worldwide economy $10.5 trillion a year in 2025 (Globe Newswire, 2020) and ransomware is one of the world's most prominent crimes. The origin of the ransomware was established by Young and Yung at Columbia University (Young and Yung, 2017), where the concept of the encrypted ransomware program appeared and applied for the first time in 1996 and was first presented at the Security and Privacy Conference made by the Foundation of Engineers Electrical and Electronics. The program was called cryptocurrency viral extortion. In the last year, a group of malware programs, which has been used in cyber-attacks, is ransomware for people, organizations and governments. The writers in [19] said that modern family ransomware, such as Locky, Cryptowall, Cerber, etc. are difficult to detect and have separate variants such as CryptXXX2.0, CryptXX3.0. Two major ransomware forms are locker-ransomware and crypto-ransomware (encrypts data to block the patient to get access to a device). The authors stated in [20,21] that malware analyses focused on text, signature, and trends are less effective than the high malware growth rate. Invaders are creating new versions of current malware using polymorphic, metamorphic, obfuscation, and other masking techniques (Dynamic Method). Automatic behavioral malware monitoring using machine learning methods as a smart warning solution when any deviation happens. The action of each malware is automatically screened and reports on a simulated (sandbox) environment.

These findings are pre-processed into machine learning models (classification). To classify the malware samples based on their behavior, algorithms are required, which can create models and learn during the classification process. The ability of the computer to learn from data during the classification process makes it more valuable and accurate in the classification of malware. Ge [22] construct the detection model automatically by means of machine learning algorithms to improve the detection model, to identify new ransomware samples. The procedure is based on a CF-NCF algorithm update of the TF-IDF algorithm. CF-NCF focuses on the appearance of features in each class, while TF-IDF focuses on the appearance of words in each paper. Experimental findings demonstrate that CF-NCF does better than TF-IDF for the identification of ransomware.2019).

For crypto-ransomware detection, SH Kok and others are using the Pre-encryption detection algorithm (PEDA). The PEDA is determined by the division into two stages of the detection mechanism. The first is the old Signature Repositories (SR) cache, which seeks to identify some matches (for ransomware) with known Signature repositories. The other level depends on a learning algorithm (LA) that can find known and unknown ransomware in the system. learning algorithm uses machine learning by the predictive model using data from the application program interface (Kok. Et al. 2020.). Since, the PEDA algorithm enables ransomware detection before the process of encryption, it is likely to be fooled if new models are used and prediction is a vital choice in the process.

Framework for Analyzing Ransomware Using Machine Learning

Experts also attempted to identify ransomware by studying the process by which the device identifies malicious programs through the effects it has on the computer and the programs. Certain approaches have been adopted: To track and stop the large amount of zero-day ransomware attacks in the NTFS file system evaluate I/O queries and follow-up improvements to the system to secure the master file [23]. Another tool. the emphasis of a master learning approach to evaluate and categorize complex analyzes of ransomware using logistic regression [24].

Much of the approaches for finding ransomware are concerned with noting its impact on the device by changing it during encryption and using the ransomware trail by using the actions of ransomware from infection to payment (Liu et al., 2018). Follow up banking transactions where the claimant sends cash and where it is invested by the ranchers. Data extraction methods are used to classify and discover families by means of a static and dynamic process to identify and compare [25]. Another way to increase the identification accuracy of ransomware is to develop an automatic static analysis system and use reconstruction instructions and the dll archives. The tested ransomware (8 samples) and standard binaries are reverse engineered to obtain the code at various speeds. The model was developed with machine learning after the analytical of the data by static analysis with an average accuracy of Ransomware 92.11 per cent [26]. With these positive outcomes, further experimentation with ransomware programs and a thorough analysis of its impact on machine learning algorithms are essential.

Discussion

This section will discuss the comparison between 3 prevention techniques. Analysis reveals that ransomware threats have risen and have doubled as the distant work community introduced by the pandemic COVID-19 increased in the first quarter of 2020. Most people who operate remotely do not obey the same cybersecurity policies that the workplace atmosphere usually applies. Moreover, most remote employees use personal computers that do not have effective protection features such as antimalware kits, firewall, intrusion prevention, password management and encryption applications. Ransomware leverages new vulnerabilities discovered in used applications and networks centered on small, medium and larger enterprises carrying out remote operations.

In addition to files encryption and locking computers, ransomware can use advanced methods to exfiltrate data. Sensitive information can result in serious security and privacy problems and breaches. This includes loss of money and disruption to the image of the victims. Relevant information can also be exposed to serious breaches of confidentiality and privacy. This includes loss of money and disruption to the image of the victims. A further review is conducted in the following paragraphs of an emerging methodology as honeypot, SSD-insider and master learning suggested by various scholars. The honeypot is an information system focused on artificial materials. The aim is to build and track the honeypot folder to detect the existence of ransomware in the event of changes. Even though an honeypot is a valuable tool to monitor network operation, the approach provides a narrow view of the ransomware industry and its network behavior since a honeypot is not the object of ransomware attacks because of the lack of attack warnings. A quick strategy for fast recovery from ransomware attacks was also suggested regardless of the availability of software by an attacker on the target machine to avoid recovery from such attacks. "A new approach for recovery from infections of Crypto Ransomware".

The methodology analysed by popular ransomware cryptography found that the ransomware attack requires the installation of tools on a victim's computer to render ransomware recovery a heroic job. This approach makes recovering from ransomware infections possible by renaming the device utility that manages file shadow copies. A related study focusing on the prevention and protection of ransomware by detecting and stopping an attack. The technique involves instructing an attacker to ignore a long time to encrypt a big dummy file. This gives a precious time to render malware unavailable for the remaining contents of the file system. Output assessment of the proposed strategy shows that the method to ransomware attacks is successful in a real-time context. An algorithm was suggested in this connection which examines a network for passive traffic monitoring to detect the existence of ransomware and prevent attacks. Experimental analyzes using 19 various ransomware families reveal that the proposed algorithm is less than 20 years old when ransomware is found. In comparison, not more than 10 files have been destroyed in 20s. The moth enables the retrieval of missing files when their contents have been saved in network transmission.

There are also low false positive findings based on studies in real-life business network traffic data. In addition, a ransomware detector with honeypot techniques was also proposed, which detects all actions done by ransomware. The method manages the Windows security logs with Event Sentry and File Screening. However, is inability to offer updates, such as email updates when threats are found and no new Ransomware attacks are observed. In addition, the Intrusion Detection Honeypot social leopard algorithm for the Detection of IoT Ransomware attacks was suggested. The method will detect IoT network ransomware attacks. However, the features of auto-tuning and switch are lacking. A separate zero-day assault was introduced for the Dionaea honeypot. And they have not reached the scheme. This technology classifies the attacks in various categories. It cannot be worked on a higher OS, except for the SQL 2000 XP Windows version.

Machine learning is an artificial intelligence industry that allows programs the ability to learn from or identify patterns in existing knowledge when making decisions with little to no human involvement. December 24, 2019, Spina One https://spinbackup.com/blog/ransomware-service-machine-learning/). It is a tool used mostly for data processing to automate the construction of an analytical model (SAS Analytics Software & Solutions) [27]. ML techniques enable computers to predict trends in vast datasets. The algorithms will respond to modifications and boost the size of the dataset. The capacity of ML to predict on known and unknown datasets allows it a real weapon for detecting ransomware assaults, leading to the endless release and comprehensive vulnerabilities of new ransomware variants in information systems. The detection of file actions is the foundation of computer education for ransomware detection. ML is a valuable tool for ransomware identification because of its capacity to allow prediction on file behavior. The strategy uses file conduct tracking to differentiate between lawful codes and malware. The reason is that the execution of a legal code provides a behavior pattern that differs from the execution of the malicious code. To learn the actions of a legal or ordinary program, ML algorithms use specialist analyzes (for example, interactive debugging or post-mortem code execution analysis) for vast amounts of salient and discriminatory knowledge. ML-based ransomware identification systems provide the legal code execution with thorough review and can distinguish malicious programs. Such tools make smart choices and lead activities to differentiate between usual program execution and irregular execution.

In addition, a ransomware detector using the Random Forest Technique was also suggested. The technology effectively identifies and prevents SDN botnet spread. The host infection rate can be decreased up to 25 percent. But there are no distributed decoy operators for the proposed technologies that improves system flow. The whole machine capacity and efficiency are reduced as well. Moreover, after evaluating the data through static processing, a model was developed using machine learning. The model will detect ransomware accuracy at an average of 92.11 percent. The detection rate of the model, however, needs a further development. Ultimately, SSD-Insider++ can read and write page by page. Also, ransomware will interpret, encrypt and overwrite the user data. Pages infected by ransomware thus display a standard IO output trend for reading after writing. Ransomware is the workaround in which to safeguard and recover original information in advance when compromised. However, existing methods, which backup and restore data via a file system, entail additional space costs for overhead backup and IO performance to assess ransomware intrusion and include the possibility of harm due to intelligent ransomware attacks to the backup data.

Recommendation

In this section, we include some suggestions to developers and scientists interested in this field of study. To provide a healthy learning atmosphere for students, teachers, professors, and guests, the ability to interact securely in an eLearning system is an important aspect. A required cybersecurity consideration should be taken into consideration to secure higher education institutions.

a. SSD-Insider should act as part of the SSD firmware, meaning that only with minimal CPU power and memory should it detect rankings.

b. SSD-Insider should be able to remove behavioral features of Ransomware by only viewing IO request headers rather than by viewing the entire request files.

c. The narrow vision of the ransom Ware operation makes it harder to detect the layer program detectors with far more context and information like file names, file size, access time, process ids, process names, memory quantity, etc. Detection latency is inevitable by any means, so some portion of disk blocks will have been already encrypted. A method to provide perfect data recovery even under detection latency should be provided.

d. Use of antivirus original package for constant software updates and testing by creating access control lists, to include patches for vulnerabilities.

e. Do not use the crack systems, maintain that the original version is used.

f. Diligent copying of computers and files should be done to make them easy to restore where there has been a problem or information lost, such as using external disk or flash, etc.

g. In the interest of remote education, embezzlement. False messages may be received to submit materials, so the sources of information need to be considered.

h. Change the password to use solid passwords, consider using a minimum of 12 long, uppercase, and lowercase mixture characters.

i. Do not open questionable connections and guarantee site protection (if students share them between them).

j. Careful management of networks is critical. Such that users will trust that a robust security protocol protects their company infrastructure.

k. Improve and promote cyber-security education and preparation for staff and students through LMSs, such as cybersecurity learning management systems (CyLMS).

l. Lastly, the e-learning environment needs strong and written cyber protection protocols for secure use, maintenance and/or responsible/acceptable use to mitigate possible weaknesses such as implementing network access points and preventing unwanted access.

Conclusion

While digital information in a wide variety of areas has changed lives, there are still some shortcomings and deficiencies which will affect the smoothing of cyberattacks. Cyber-attacks are called cyber-space offenses perpetrated by cybercriminals and hackers, which are targets of profitability or retribution by individuals or organizational computers or networks. This research offers a detailed development from the beginning of the computer development of the ransomware attacks. It is important to remember that ransomware shifts actions differently than traditional malware. Moreover, several improved techniques have been suggested for efficient and accurate sensing of the ransomware such as honeypot, SSD-Insider, and deep learning. This paper has included several schools affected by this deadly attack.

This post aims to review the most popular machine learning algorithms used for the detection of ransomware. The efficiency, learning rate, etc are discussed with the advantages, drawbacks of these algorithms along with the comparison of the various algorithms. These algorithms were also used to investigate instances of practical implementations. Different authors debated types of machine learning techniques. It is anticipated that it will offer readers a clear pathway in defining the choices for machine learning algorithms, and then in the light of the relevant problems solving selection of the right machine learning algorithm. Additionally, other approaches were presented in this study, such as honeypot and SSD-insider. The advantages and drawbacks have been detailed. We also advise and advise academics and ransomware designers in a very informative way.

References

1. Curiel M, Pont A (2018) Workload Generators for Web-Based Systems: Characteristics, Current Status, and Challenges. IEEE Communications Surveys and Tutorials (99): 1-1.
2. Zhang-Kennedy L, Assal H, Rocheleau J, Mohamed R, Baig K, et al. (2018) The aftermath of a crypto-ransomware attack at a large academic institution. Proceedings of the 27th USENIX Security Symposium 1061-1078.
3. Popoola SI, Ujioghosa B Iyekekpolo, Samuel O Ojewande, Faith O Sweetwilliams, Samuel N John (2018) Ransomware: Current Trend, Challenges, and Research Directions. Communication and Media Ethics 1(3): 469-484.
4. Pont J, Oun OA, Brierley C, Arief B, Hernandez-castro J (2017) A Roadmap for Improving the Impact of Anti-Ransomware Research. Renewable and Sustainable Energy Reviews 12(3): 23-30.
5. Tanana D (2019) Complex ransomware counteraction technique. SIBIRCON 2019 - International Multi-Conference on Engineering, Computer and Information Sciences, Proceedings 5(1): 636-638.
6. Chen Q, Bridges RA (2017) Automated behavioral analysis of malware: A case study of wannacry ransomware. Proceedings - 16th IEEE International Conference on Machine Learning and Applications, ICMLA pp. 454-460.

7. Sahi SK (2017) A Study of Wannacry Ransomware Attack. International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) 4(9): 5-7.

8. Zorawar V, Mohit D (2017) An Advanced Web-Based Bilingual Domain Independent Interface to Database Using Machine Learning Approach. Proceedings of International Conference on Communication and Networks pp. 581-589.

9. Bhardwaj A, Avasthi V, Sastry H, Subrahmanyam GVB (2016) Ransomware Digital Extortion: A Rising New Age Threat. Indian Journal of Science and Technology 9(14).

10. Pascariu C (2019) Ransomware Honeypot.

11. Sibi Chakkaravarthy S, Sangeetha D, Cruz MV, Vaidehi V, Raman B (2020) Design of Intrusion Detection Honeypot Using Social Leopard Algorithm to Detect IoT Ransomware Attacks. IEEE Access 8: 169944-169956.

12. Genç ZA, Lenzini G (2020) Dual-use research in ransomware attacks: A discussion on ransomware defence intelligence. ICISSP 2020-Proceedings of the 6th International Conference on Information Systems Security and Privacy pp. 585-592.

13. Kok SH, Abdullah A, Jhanjhi NZ, Supramaniam M (2019) Ransomware, Threat and Detection Techniques: A Review. IJCSNS International Journal of Computer Science and Network Security 19(2): 136-146.

14. Moore C (2016) Detecting ransomware with honeypot techniques. Proceedings-2016 Cybersecurity and Cyberforensics Conference, CCC pp. 77-81.

15. Sethia V, Jeyasekar A (2019) Malware capturing and analysis using dionaea honeypot. Proceedings - International Carnahan Conference on Security Technology p. 3.

16. Fadele AA, Othman M, Hashem IAT, Alotaibi F (2017) Internet of things Security: A Survey. Journal of Network and Computer Applications 88: 10-28.

17. Khammas BM (2020) Ransomware Detection using Random Forest Technique. ICT Express 6(4): 325-331.

18. Baek S, Jung Y, Mohaisen A, Lee S, Nyang D (2018) SSD-Insider: Internal defense of solid-state drive against ransomware with perfect data recovery. Proceedings - International Conference on Distributed Computing Systems pp. 875-884.

19. Awwad S, Ng C, Noordin N (2011) Cluster based routing protocol for mobile nodes in wireless sensor network. Wireless Personal.

20. Elzein NM, Majid MA, Abaker I, Hashem T, Yaqoob I, et al. (2018) Managing big RDF data in clouds: Challenges, opportunities, and solutions 39: 375-386.

21. Hanapi MS, Mohd W, Firdaus K, Khairuldin W (2017) Applying the Thematic Hadith Method in Research Related to Islam 7(12): 576-586.

22. Ge, M., Hong JB, Guttmann W, Kim DS (2017) A framework for automating security analysis of the internet of things. Journal of Network and Computer Applications 83: 12-27.

23. Arshad S, Abbaspour M, Kharrazi M, Sanatkar H (2011) An anomaly-based botnet detection approach for identifying stealthy botnets. ICCAIE 2011 - 2011 IEEE Conference on Computer Applications and Industrial Electronics, Iccaie pp. 564-569.

24. Farooq MJ, Zhu Q (2019) Modeling, Analysis, and Mitigation of Dynamic Botnet Formation in Wireless IoT Networks. IEEE Transactions on Information Forensics and Security 14(9): 2412-2426.

25. Zhou F, Zhao B, Tao M, Bai X, Chen B, et al. (2013) A large scene deceptive jamming method for space-borne SAR. IEEE Transactions on Geoscience and Remote Sensing 51(8): 4486-4495.

26. Silverio-Fernandez MA, Renukappa S, Suresh S (2019) Evaluating critical success factors for implementing smart devices in the construction industry: An empirical study in the Dominican Republic. Engineering, Construction and Architectural Management 26(8): 1625-1640.

27. Fan Z, Bi D, He L, Shiping M, Gao S, Li C (2017) Low-level structure feature extraction for image processing via stacked sparse denoising autoencoder. Neurocomputing 243: 12-20.

ISSN: 2574-1241

DOI: 10.26717/BJSTR.2021.35.005649

Fadele Ayotunde Alaba. Biomed J Sci & Tech Res