LUPINE PUBLISHERS

Current Trends in Computer Sciences & Applications

DOI: 10.32474/CTCSA.2023.02.000150

ISSN: 2643-6744

Research Article

Ransomware Attacks on Remote Learning Systems

Afnan Hussain Habibullah, Ghadeer Abdullateef Alfarshouti, Huda Dakheel Aljohani, Maha Nasser Alqahtani and Asia Othman Aljahdali*

Department of Computer Science and Engineering, Cybersecurity department, University of Jeddah, Saudi Arabia

***Corresponding author:** Asia Othman Aljahdali, College of Computer Science and Engineering, Cybersecurity department, University of Jeddah, Saudi Arabia

Received: July 12, 2023 **Published:** July 27, 2023

Abstract

The increasing use of computers and information technology attracts the interest of cybercriminals, who devise various means to compromise the security and privacy of legitimate users' data and information. This is achieved by using unscrupulous methods in the protection mechanisms in hardware and software systems in order to compromise the confidentiality, integrity, and availability of data and information stored, processed, and transmitted by computers. Malicious individuals leverage vulnerabilities in devices, systems, and applications to perform unauthorized access, revelation, or modification of data. Attackers also take advantage of the ignorance and/or negligence of administrators and users to exploit sensitive systems and information. For example, administrators may fail to provide a secure configuration of the system and application or leave sensitive information such as passwords or data in clear text. Users, on the other hand, may open doors to intruders by installing infected applications on their systems, clicking malicious links, and using improper password management. A successful attack such as Ransomware against a computer system can result in catastrophic losses for individuals and organizations. Access to sensitive personal data can reveal financial records, credit ratings, and medical histories. Moreover, ransomware poses increasing threats to files and devices used by businesses and individuals. It prevents innocent victims from accessing infected files or compromised devices until they pay a ransom, usually in the form of bitcoin. In many cases, hackers do not provide the decryption key even after a victim pays the ransom. At other times, an attempt to decrypt files using the key provided by the attacker causes further harm to files stored on the system. Technological innovations such as ransomware development kits, ransomware-as-a-service, and bitcoins facilitate the persistent increase in ransomware attacks against personal computers, networks, and mobile devices. The objectives of the research paper are to categorize the ransomware attacks and analyze the impact of these attacks on distant learning. Different solutions and techniques are thoroughly discussed and analyzed. Each of the technique's challenges and drawbacks is also provided for detailed understanding by both organizations and developers. Finally, after studying the impact and damage caused by ransomware, the research will provide a general recommendation on some preventive measures that should be put in place to avoid such dangerous attacks on devices and the infrastructure of remote learning.

Keywords: Ransomware; Encryption; Detection; Malware; Attack; Learning; Remote

Introduction

Digital conversion has changed the world so that most, if not all, information has been transformed into digital information. Information and data have become easily accessible and retrievable; moreover, the process of digital storage of information and data has facilitated most of the official transactions, such as banking transactions, which make the clients perform all the transactions online regardless of where they are. In addition, it makes communication and collaboration between the different sectors easier and faster. Despite the fact that digital information has improved people's lives in various fields, it still has some flaws and gaps that would affect the smoothing of operations, such as cyber-attacks. Cyber-attacks are considered cyberspace crimes that

are committed by cybercriminals or hackers. These crimes target an individual's or organization's computers or networks to cause harm with the purpose of making profit or retaliation. There are several examples of these cyber-attacks, such as phishing, spyware, spam, Trojans, and ransomware; the last one will be the author's focus in this paper. Ransomware is malicious software that attempts to lock or encrypt files and data for an individual or an organization for the purpose of making money [demanding ransom]. Webster's dictionary defines ransomware as "Malware" that requires the victim to pay a ransom to access encrypted files. [Merriam-Webster's dictionary, 2020]. From the definition of ransomware, one can understand that this is one of the most dangerous attacks that can infect systems because it is difficult to get out without causing losses. The attacker prevents the victims from accessing their data and files once they are encrypted. Ransomware often targets sensitive files, such as financial data, business databases, or personal files. Attackers subsequently demand ransom to decrypt those files and data. Money is usually the main goal of such attacks. There are different ways to achieve their goals; for example, the threats of illegally publishing private and secret contents belong to the victims [1]. s Therefore, the victim, in this case, has two options: either to pay ransom for them with no guarantee that the data is going to be decrypted and returned, or to format their computers.

Blocking software systems and networks can cause negative consequences and numerous problems with data, including the permanent or temporary loss of valuable information [2] and disruption of regular use of system functionality and resources, leading to loss of productivity and wasting time in order to restore the files and resources [2]. Furthermore, business sectors such as the governmental sector, educational sector, etc. may face economic issues as a result of paid ransoms and loss of revenue due to suspension of production [3]. Nevertheless, the effect of cybercrimes goes beyond the shutdown of systems and loss of data and money; it may reach the loss of people's lives. According to the New York Times, the first death case due to a cyberattack was announced on September 11, 2020, in Germany [1]. The accident took place when a woman went to Düsseldorf University Hospital. Her situation was diagnosed as serious and an emergency condition. Therefore, she needed urgent medical intervention. Surprisingly, the medical staff detected that all computer systems, including patients' data records, were encrypted by cyber criminals who used ransomware attacks to force the hospital to pay a ransom in order to release their systems. There are numerous and diverse waves of ransomware attacks that have happened in previous years [4], where many businesses, organizations, and governments have found their digital data imperiled. One of the worst waves to ever occur is WannaCry," which began on May 12, 2017. It attacked many hospitals, universities, and government organizations. It passed across at least 150 universities, infected an estimated 230,000 computers in 48 hours, and had more than 2,00,000 victims. "It caused kinetic effects, paralyzing hospitals, disrupting transport networks, and immobilizing businesses" [Sahi, Chen, and Bridges].

Today, after the World Health Organization announced COVID-19 as a pandemic on January 30, 2020 [5], many governments and countries introduced distance learning to replace the traditional schooling method, which serves as a way to fight against the disease and prevent the outbreak of the virus between students and staff [6]. As such, converting to distant learning means that the networks and systems of schools and universities, besides students and staff's computers, are exposed to viruses, malware, and cybercrimes, especially when there are employees or students who lack experience when it comes to protecting their devices from hackers and malicious software [7]. Moreover, research questions are proposed on the extent and effects of the risks and threats of cyber-attacks on distant learning in the educational sector and how they can be prevented. As the general saying goes "Prevention is better than cure", The current increase in attacks as a result of the rapid development of technology has given rise to the presence of vulnerabilities in the field of digital systems, most especially in the education sector. For this reason, it is important to identify methods of protection and how to tackle ransomware attacks. The objectives of the research paper are to categorize the ransomware attacks and analyze the impact of these attacks on distant learning. Different solutions and techniques are thoroughly discussed and analyzed. Each of the technique's challenges and drawbacks is also provided for detailed understanding by both organizations and developers. Finally, after studying the impact and damage caused by ransomware, the research will provide a general recommendation on some preventive measures that should be put in place to avoid such dangerous attacks on devices and the infrastructure of remote learning. The remaining part of the paper is structured as follows: The ransomware attack history is presented in Section 2. Ransomware types are discussed in Section 3. In Section 4, Studies and Numbers of Ransomware Attacks are mentioned. A comprehensive literature review on ransomware detection techniques is given in Section 5. The research discussion is presented in Section 6. Section 7 contains general recommendations. Finally, the paper's conclusion is written in Section 8.

History and Evolution of Ransomware Attacks

Ransomware is considered one of the most complicated cyberattacks experienced by both individuals and organizations, with a record of global losses ranging up to billions of dollars. Cybercriminals use this form of attack to monitor and force their target victims [8]. The intention of ransomware is not to corrupt the computer system files but to leave them in a working condition to show the ransom information ['payment instruction'] on the targeted user's screen and to provide a means of ransom payment to the victim. This will make data on the victim's device inaccessible until payment of the ransom is made by the victim to get rid of the restriction [8]. Furthermore, there is a record of success in ransomware currently due to the increase in ransomware families some years ago [9]. It uses various means, such as email attachments, websites, and infected software, to multiply quickly. Due to the increase in reliance on digital technology, individuals

now depend more on computing gadgets to perform their tasks and support their endeavors. However, important private data is saved on that gadget, which may contain corporate data that consists of some confidential information, such as business operations or trade secrets, and budgets presented in digital form only. Thus, the change in information technology implies that a successful ransomware attack on an unsafe device can result in grave consequences [10]. Computing gadgets that have been attacked by ransomware will always notify the users with a threatening message to make a payment as a ransom within a specified period to avoid permanent corruption of data. The eavesdropping that acts as ransomware obtains ransom money by employing anonymous means of payment [such as cryptocurrency [Bitcoin], cards, or prepaid cash] to restrict their money trace. Ransomware usually requests an average of $300 to $2,000 from the targeted victims. The initial version of ransomware usually employs a basic approach to block access to personal files, system resources, system tools, or even the desktop. New families of ransomware employ encryption to strictly block the victims' data, making it unrecoverable in the absence of a decryption key counterpart. Also, it is important to note that ransomware has different behaviors when compared with conventional malware. For example, the most common form of malware tends to obtain users' information, such as bank credentials, using a subtle method. However, ransomware exhibits different behavior since there is a notification given to the victims of the attack that the device is infected. This is because several ransomware programs use various means to penetrate the system and utilize malicious advertisement, social engineering, drive-by downloads, and spamming, whereas other malware programs use a backdoor or open ports to penetrate the system in an attempt to discover vulnerabilities for exploitation [44]. In subsequent paragraphs, the evolution of ransomware attacks right from their inception will be discussed. The ransomware attack has been in existence as far back as when the traditional computer virus was introduced. Various studies have revealed that the AIDS Trojan, also referred to as the PC Cyborg virus, was the first record of ransomware, which occurred in the year 1989 [11]. The culprit, Joseph Popp, who is a biologist, sent over 20,000 floppy disks that had been infected by the ransomware to the World Health Organization's AIDS conference attendees. The disks contain the label "Aids Information Introductory Diskettes", together with an interactive questionnaire employed to activate the malware at the point that the victim's computer is re-booted about 90 times. The AIDS Trojan behaves by hiding all the folders and locking the filenames of the victim's computer, saved on the "C: drive", which makes the Windows operating system useless. This will require the victim to make a payment of $189 to a Panamanian P.O. [post office] box to regain access to the machine. The ransomware [AIDS Trojan] is not complex as it uses a simple cryptographic algorithm for encryption of victims' computer files, which can be easily defeated. Thus, this has caused global damage in various research centers [12].

The year 1996 marked the most significant step forward in ransomware's evolution. This happened when two scholars presented a research paper during the "IEEE Security & Privacy Conference '96". The manuscript recommended a proof-of-concept program that utilizes public-key encryption to form a malicious code for extorting money from the machine of the victim infected with this form of malware. The study recommended that this form of cyberattack be designated using the terms cryptovirology and cryptoviral extortion [13]. According to the author, cryptovirology is defined as the science that combines malware with the cryptographic protocol to form malicious software. Until 2005, ransomware was not globally known for cybercrime, and there have not been any recorded cases of the utilization of this form of malware. However, there was a drastic change in 2005 when the encryption key became useful in malicious code by ransomware programmers. This gave birth to various forms of ransomware, including Archiveus, Krotten, and GPCoder. According to the obtained result, GPCoder that uses 1,024 bits of RSA is the most observed strong encryption, which makes it hard to use the brute-force method to recover victim files. During that time, various antivirus companies acted on this attack by coding information, also referred to as a signature, for every identified form of ransomware into the list of antivirus signatures, which resulted in halting the activities of most ransomware attacks during that time [Tanana]. In addition, a variant of ransomware referred to as Vundo occurred in 2009. It uses scareware tactics to steal money from the targeted victims [that is, by subtlely telling the victim that their machine has been infected by the virus and persuading them to purchase security software like XP AntiVirus 2009 to get rid of the virus]. This changes the function of ransomware to encryption of files and requesting a ransom of $40 for decryption of files. Vundo is a polymorphic malware, as it often changes its execution. Thus, the vendors of antivirus have been adding all the noticed forms of Vundo to the database of virus signatures to prevent it [40]. Similarly, in 2012, ransomware increased its activity against service providers and employed intimidating strategies to extort money from the target individuals. For instance, ransomware culprits target counterfeit software and pornographic sites and pose a threat message to their viewers, stating that they break the copyright agreement by downloading pirated software and breach the law by watching the contents of children's pornography. As a result, their file system was blocked by the law enforcement agency in their locality, requesting that a payment of a fine be made to the police before the computing device can be unlocked for them to have access again. It has been found that Reveton and Kovter are the most prominent ransomware that employs such tricks in mimicking law enforcement agencies [Al-rimy et al.]. With this notable popularity, different types of ransomware that use strong encryption standards such as Cryptolocker, Torrentlocker, Cryptowall, and Teslacrypt began to emerge from 2013 to 2015 [Pandey et al.]. Ransomware kept on advancing in 2016 by incorporating additional innovative features into its activities, like a countdown timer [with an increase in ransom over time when the targeted victim fails to pay], alongside modern

ransomware variants with the ability to automatically multiply over the computer network. Moreover, ransomware inventors incorporated an alternative, simplified method of ransom payment in such a way that users without computer literacy could easily make the payment. The most famous types of ransomware that emerged that year include Locky, Sam Sam, and Petya. In addition, the same year serves as the most remarkable year for ransomware families because new ransomware families are introduced [14].

While 2017 was designated by various security scholars as the unique year of ransomware, the most famous ransomware threat recorded was WannaCry. This ransomware expanded globally, and about 27 languages are supported by its ransom note, which has the capability of propagating across connected networks to attack computing devices and network servers. Although this high expansion in ransomware harm in 2017 was primarily triggered after the hacker group published the hacking tools [NSA-leaked repository] that consist of secret exploits that facilitate the exploitation of vulnerabilities by the culprits in computer servers and PC Windows OS, together with VPNs and firewall systems, Mostly, the NSA-leaked gadgets were employed by offenders' gangs to globally distribute the ransomware using 'Windows operating systems' unpatched vulnerabilities. In contrast to the rapid growth of this attack, in 2018 we observed a decrease in ransomware infection, i.e., 8 ransomware attacks reduced to 30% globally [Tanana]. Though these numbers are inspiring, the statistics indicate that the decrease in ransomware volume in 2018 made it more refined, and numerous new variations emerged with self-multiplication ability. Even though it is hard to predict the exact future of cybersecurity, cybersecurity enterprises predict that the damage will extend to reach $6 trillion by 2021; similar research envisages that ransomware attacks will smash businesses in 2021 at a cycle of 11 seconds, and the expected harm produced by ransomware will require an estimate of $20 billion globally in 2021. It should also be noted that the discussion on ransomware damage points to the total damage produced by ransomware attacks. The damage consists of the budgets related to the performing of forensic experiments on the infected networks and computer systems, the damage to productivity, the costs of employing emergency consultants and enterprise crisis managers, and the cost of recovering backup data to continue its normal operations. Moreover, ransomware is part of digital extortion cybercrime, which also consists of other forms of cybercrime to illegally obtain or reject access to individual information in exchange for financial gain. However, lockers and crypto ransomware are two primary types of ransomware [Humayun et al.]. The locker ransomware does not apply an encryption algorithm to lock files but prevents the targeted users from accessing their data by refusing access to system resources [for example, it can lock the desktop or refuse the victim login access] and requesting a ransom payment before the access can be regained [15]. Typical locker ransomware, on the other hand, when compared with crypto ransomware, refuses access to individual files by employing basic methods that can be avoided by any technician, and as a result, locker ransomware can be eliminated from the damaged system with no influence on the personal files as well as the underlying OS [16]. Moreover, the crypto ransomware uses an encryption key on the user's machine to prevent them from accessing important files. In this case, all the personal files on the victim's computer are encrypted to block access for the user until a ransom is paid by the victim to gain the decryption key from the invader [13]. Certain variations of crypto ransomware will gradually wipe the victim's files or expose them publicly in a situation where the victim refuses to comply with the ransom payment at the specified time. Contemporary ransomware categories usually rely on this form. It can have destructive effects, particularly on governmental and corporate agencies, if a backup operation that can restore the system to a normal state before the attack is not found. In such a case, the victim is left with only a ransom payment option to retrieve the lost files [17]. Most crypto ransomware attacks do not cause any damage to the victim's system files but will enable the victim to carry out some simple operations with restricted access to the encrypted hostage files. Some common or famous ransomware examples and their targets are: Locky [it is the first form of the ransomware initially published in 2016 by the prepared collection of the attacker]. This form of ransomware targets various forms of files employed by engineers, designers, developers, and testers [18]. The attack of this ransomware extended to over 150 nations in the year 2017. It is constructed to manipulate attacks on windows. It was purportedly formed by the "United States National Security Agency and leaked by the Shadow Brokers Group." For instance, WannaCry affected 230,000 computers worldwide [18], and Bad Rabbit [this form of ransomware attack was initially published in 2017 and uses an approach referred to as a drive-by' attack by targeting unprotected websites to perform an attack]. It usually utilizes a fake demand to provide and install Adobe Flash as a malware dropper to expand the attack. Ryuk [this form of ransomware was multiplied in August 2018 and disabled the Restore option of the Windows System, making it difficult to restore encrypted files in the absence of a backup]. It also employs the cryptographic key to encrypt network drives [16]. Recently, researchers across the globe have started to develop an interest in these attacks, and thus, they have started developing countermeasures for them, which will be discussed in the following sections.

Types of Ransomware

One type of ransomware locks users' computers and shows a message saying the rewards are coming from a law enforcement agency. This message, which uses official-looking pictures, states that the client has engaged in illegal activity and must promptly pay a fine online by entering the credit card number. The computer is "held prisoner" and locked until the ransom is paid. An example of this type of message is illustrated in Figure 1.

Figure 1 shows a ransomware message from the Symantec Security Reaction Center website. Another new variation of ransomware triggers a recorded message through computer speakers using a regional and semi-personal voice message. There

is another type that shows fake warning messages, such as malware infection or an impending hard drive failure problem in the computer. Regardless of the status of the computer, ransomware always reports a problem. This kind of ransomware informs users that they should purchase additional software online to fix a problem that actually does not exist. These warnings appear to be authentic and valid since they imitate the appearance of the original programs and improperly use trademarks or symbols. An example of such ransomware messages is illustrated in Figure 2. The ransomware illustrated in Figure 2 uses shading plans and symbols like those found in genuine Windows programs. The clients discover those who provide their credit card information to establish the purchase. This will let the attackers easily capture that information and then utilize it for their own purposes.

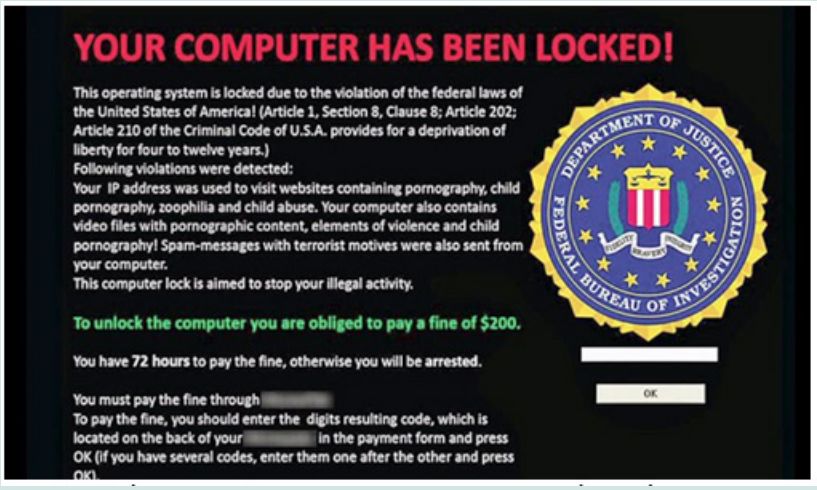

Figure 1: Ransomware Message from the Symantec Security Reaction Center.

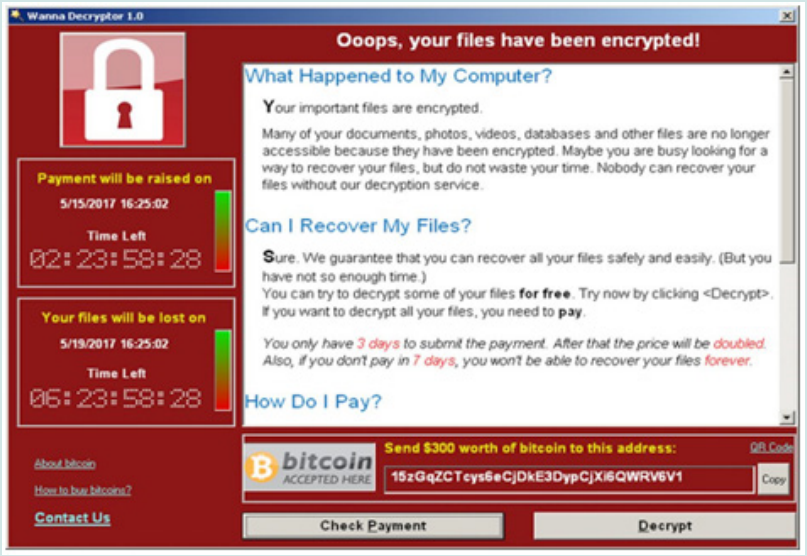

Figure 2: Ransomware that uses Shading Plans and Symbols.

Studies and Numbers of Ransomware Attacks

Many schools are affected by ransomware threats. For instance, ransomware attacks shut down California's online learning. In Central California, the Selma Bound Together school district unexpectedly stopped online classes during the middle of the day on account of a ransomware attack that was spreading over the locale's organization. ABC station KFSN reported on the school district cyber-attack, and before afternoon, all educators were contacted and told they needed to end this instruction instantly [19]. The programs needed for online instruction were targeted rather than the personal data of students and workers. Moreover, one of the projects hacked and attacked was a student information system, which holds student demographics along with attendance. Furthermore, the ransomware attack also hit schools in North Carolina. In North Carolina, the Haywood County region is restarting web classes after a few weeks break due to ransomware attacks. A significant cyberattack forced the school system to take down

most technology services in order to stop the corruption of school system servers and computers. Since many technological services are transmitted through system servers. The students, staff, and community need the schools to be open as much as possible after the negative impact of COVID-19 and the recent ransomware attack. To be free from the attack, the IT department needs to play a major role by providing 247 backups of the entire school's data [20]. In addition, the Texas school district is also not left out of this attack. For example, most schools in this district pay ransom to hackers so they can start classes. The attack encrypted all of the data on school district servers, including various information reinforcements and two or three hundred locale PCs, which made all access to data like teacher communications, student schedules, grades, and assignments blocked, as indicated by an assertion from Athens ISD [21]. These attacks are fueled mainly by greed and the ability to make money, regardless of the consequences for students and teachers. Also, programmers as of late made $50,000 from the Athens, Texas, School District after it consented to pay a payoff. The attack delayed the commencement of school by a week. Although governmental technology has covered the extent of the ransomware attack on that district.

Literature Review

In this section, this paper will discuss some security solutions and techniques aimed at the detection and prevention of ransomware attacks. In defending against attacks and malware detection, traditional methods have been utilized, such as antiviruses, to detect and prevent computers from being compromised. Also, the users are required to be aware of what resources, websites, email attachments, and links they are trying to access. Having backup strategies is a necessity regarding defense against attacks by their various versions, which would help in case of infections. Computers and workstations can be re-imaged, and files can be restored [22]. However, new advanced malware families are hard to detect using traditional methods due to their complex algorithms. Among these techniques are Honeypot, SSD-Insider++, and Machine Learning.

Honeypot

Honeypot is a mechanism designed solely for detecting and capturing different attack approaches that are utilized by hackers [23]. The honeypot technique does not stop or mitigate attackers from attacking their target system [24]. Thus, the main purpose of Honeypot is to gather information about the attack and the attackers rather than prevent it. Because it is a bogus computer resource installed by network administrators to act as decoy computers and detect any illegal access [25]. In addition, this technique also serves as a distraction file for the ransomware to attack, i.e., it is a technique that is capable of disrupting attackers from hacking into the system or server [26]. The job of Honeypot is to remain silent, pretend to be a real environment, and trap the attacker. Honeypots are deployed in such a way that the attackers consider them productive systems and attack them. It collects information about the attacker by observing their movements and giving the details required by the attacker [27]. Furthermore, the honeypot system needs to contain files that make the attacker think it is a legitimate server and not a decoy file. In this case, it is imperative for the administrator to know the characteristics of the ransomware types as well as the files the ransomware is potentially targeting to attack. Hence, a suitable security mechanism to avoid such attacks is deployed on the network [28]. In summary, the Honeypot is broadly categorized into two types [24] namely, research honeypots and production Honeypots. The research Honeypots are used to gather as much information as possible. This information is exploited to understand the vulnerabilities in the existing environment and build a better defense system, while the production Honeypot is used to collect information about the attacker and mitigate the organization's risks. The rapid growth in technologies and development of hi-tech devices has currently increased the number of ransomware attackers on various devices [29]. Most especially Internet of Things [IoT] devices, which are presently the trending technological as well as research domain. However, for users to gain trust in these devices from ransomware, researchers have developed an interest in proposing different honeypot techniques to tackle ransomware attacks based on their advantages and suitability for IoT devices. Among these are Sibi Chakkaravarthy et al., who used the Social Leopard Algorithm to design an Intrusion Detection Honeypot [IDH] that is capable of detecting ransomware attacks in IoT networks. The proposed mechanism consists of Honeyfolder Audit Watch and Complex Event Processing [CEP]. The proposed IDH utilizes the CEP technique to correlate the host features, network features, and various events from other systems such as Audit Watch and Firewall, thus producing the aggregated results with better accuracy.

Further, the proposed IDH can be deployed in the production environment with ease. The results show that the Honeyfolder deployed for monitoring file system [host] activities is extremely real by portraying its responsiveness to the host's ransomware. The experimental evaluation also confirms that the proposed IDH is efficient in restricting ransomware activities without causing minimal data loss. However, the proposed solution lacks an auto-tuning feature and transfer learning ability, which are tools for load optimization in IoT devices. Similarly, Moore developed Honeypot techniques using research-investigated methods to detect ransomware. The proposed technique is capable of detecting all activities carried out by ransomware. The advantage of this technique is that, after detecting the illicit behavior, it uses either the "EventSentry or the File Screening service of the Microsoft File Server Resource Manager" feature to control the Windows Safety logs. Lack of feedback, such as email alerts when attacks are detected, is a challenge with this technique. Also, the proposed technique is not designed to detect novel ransomware attacks, which in turn is dangerous for system users. Furthermore, Sethia and Jeyasekar used the Dionaea Honeypot approach to design malware capture and analysis mechanisms to capture different zero-day attacks and make sure they did not enter the system. The proposed technique has the ability to classify the captured ransomware attacks into different groups based on their behavioral activities and properties.

The classification will enable and guide researchers on how to develop a robust security mechanism against malware. However, the proposed system cannot run on higher operating systems, except on SQL 2000 and XP versions of Windows. Additionally, the technique lacks high Honeypot interaction capability. Recently, a random forest technique was used by Khammas [41] for ransomware detection through machine learning. The major distinction of the suggested technique is the distribution of the disassemble procedure through uninterrupted abstraction of features from the raw byte through the utilization of repeated configured mining, which abnormally increases the detection speed. Also, Khammas proposed a novel blocking approach that uses Honeypots to detect and efficiently prevent botnet propagation in software-defined networks [SDN] using deception techniques and Honeypots to detect botnets. The proposed technique has the capability of reducing the host infection rate by up to 25% and increasing the adversary's wasted time. However, this approach lacks distributed decoy managers, which increases the system traffic load and thus reduces the entire system's performance and efficiency.

SSD-Insider++

SSD-Insider++ is a ransomware protection system that protects users' files from being damaged by ransomware. It is a backup-based tool that stores copies of files in backup storage. It is found as firmware in the SSD console. It has two features, namely, ransomware detection and data recovery at very low costs [30]. In the event that ransomware is detected, the algorithm is run to restore the original files by using the drive's delayed deletion feature [45]. This technique monitors all inputs and outputs to detect ransomware. Each input and output request contains four elements: time [i.e., the time the request was created within the system], LBA [i.e., the address that contains the evidence where data begins to be read or written], RL and WL [this represents the length of LBA blocks that have been consecutively read or written], and the request [the request is indicated by the input and output requests, the length Furthermore, SSD-Insider++ addresses the restrictions of the current programming and equipment-based ones by putting the ransomware identification and information recuperation calculations into a SSD. SSD-Insider++ is simply ready to get to 1 the header of a square I/O parcel and [2] its payload [31]. A payload could have helpful data, such as information entropy, which can be utilized as a significant pointer reflecting tainted information Inferable from restricted processing power, in any case, analyzing the substance of a payload slowly at runtime is infeasible. This functional constraint drives us to build up the location calculation, which settles on a choice by alluding to the header of a square I/O parcel. The square I/O header contains fundamental data with respect to an I/O demand, for example, the sort of solicitation [i.e., read, compose, or trim], the area of information to be perused or composed [i.e., an intelligent square location or logical block address [LBA]], and its length. By checking a surge of parcels showing up from the host, SSD-Insider++ can 1 identify extraordinary I/O designs that are seen when a ransomware runs and know which information is being altered by a ransomware [42]. Additionally, this is what happens when a set-up update of ransomware contaminates documents. The substance of a casualty record is perused, scrambled, and overwritten. Ransomware endeavors to contaminate whatever number of documents could be allowed in a snappy way, making an effort not to be seen by a client. In this way, if comparative 'update-after-read' I/O designs are intensely noticed, then it may be viewed as an indication of ransomware assaults. Notwithstanding, some ransomware acts in an unexpected way by not overwriting casualty records. Despite the fact that regular 'update-after-read' designs are not seen here, the Class B/C ransomware needs to unequivocally erase a unique record to keep it from being found and recovered by a client later. Luckily, at whatever point a document is taken out, a record framework sends a trim order to a SSD right away. Unfortunately, while ransomware itself has remarkable instances that are not seen in typical applications, the I/O designs really observed by SSD-Insider++ are the combination of I/O demands from ransomware and ordinary applications. In this manner, recognizing the remarkable examples of ransomware in approaching I/O traffic is a central point of contention. In addition, the backup and recovery policy strategy of SSD-Insider++ gives us another open door for more vigorous ransomware recognition. Since old and new forms of information exist together in the blaze for a generally lengthy timespan [except if GC eliminates old ones]. The expansion of entropy and its unique information could be a decent marker of ransomware disease. The high overheads for figuring entropy esteems can be covered up over inert occasions or can be moderated by inspecting input information.

Machine Learning

Machine learning is a branch of artificial intelligence that is concerned with designing and developing algorithms and technologies that allow computers to possess the property of "learning". In general, there are two levels of learning: inductive and deductive. Inductive inferred general rules and judgments from big data [32]. The primary task of machine learning is extracting valuable information from data, so it is very close to data mining, statistics and theoretical informatics. Machine learning is used in many fields from engineering to medicine [16]. Arthur Samuel is considered to be the first to use machine learning in 1959 to solve the game of checkers [33]. In the 1960s, machine learning was mostly used to categorize patterns. Machine learning is making computer software analyze tasks, and it makes machines evaluate the measurable performance to improve it, as this improved process increases more and more experience in implementing without needing programming the computer every time. Machine learning gives the computer instructions which allow it to learn from data without giving new step-by-step instructions by the programmer, via making decisions and does predictions and forecasting based on data. The simple method of machine learning is to give training data to a learning algorithm. Machine learning is utilized in a broad variety of fields such as medical diagnosis, pattern recognition, natural language processing, robotics, computer games, traffic prediction, product recommendation, data mining and etc. The

author in [Ray] discussed the most widely used machine learning algorithms for example Gradient Descent, linear regression algorithm, multiple linear regression, Logistic regression, Decision Tree, Support Vector Machines [SVM], Bayesian Learning, Naïve Bayes [NB], K Nearest Neighbor [KNN], K Means Clustering Algorithm and Back Propagation Algorithm. An example application of machine learning is SGD ["Stochastic Gradient Descent"] will be evaluated with three types of challenges such as classification, regression, and clustering. depending on the availability of types and categories of training data one may need to select from the available techniques of "supervised learning", "unsupervised learning", "semi-supervised learning" and "reinforcement learning" to apply the appropriate machine learning algorithm. The use of machine learning appeared in the fight against cybercrime and ransomware programs due to the advantages it enjoys in analyzing processes that depend on different algorithms. Ransomware Detection Using Machine Learning,the rapid development of the use of the Internet and technology has led to the emergence of many challenges related to the security of information and data for users of the Internet, and these challenges are called Internet crimes, which will cost the global economy estimated losses of 10.5 Trillion dollars annually in 2025 [GLOBE NEWSWIRE, 2020], and ransomware is one of the most prominent crimes in the world of the Internet and it is expected that ransomware has a greater share of all cybercrime by 2021.

The origin of the ransomware was established by Young and Yung at Columbia University [34], 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. One of the categories of malicious programs used in cyber-attacks is ransomware for individuals, organizations, and governments, which has increased in popularity in the recent period due to the high revenue. The authors in [35] mentioned that there is a difficulty to detect new ransomware families, such as Locky, Cryptowall, Cerber etc., and have different versions i.e., CryptXXX2.0, CryptXXX3.0. Two main types of ransomware are locker-ransomware locks the device to prevent the sufferer from accessing] and crypto-ransomware[encrypts the data to block sufferer's access]. In [32] the authors mentioned that content-based, signature-based and pattern matching techniques [Static Method] of malware analysis is less efficient compared with the high grow rate of malware the invaders create new variants of existing malware using polymorphic, metamorphic, obfuscation and other masking techniques [Dynamic Method] witch hard to detect by using static detection systems. Automated behavior-based malware detection using machine learning techniques as a clever solution to alarm when any deviation occurs. The behavior of each malware on an simulate [sandbox] environment will be automatically analyzed and will generate behavior reports. These reports will be pre-processed into models for further machine learning [classification]. The classification of malware samples based on their behavior requires implementation of algorithms that are capable of producing models and learning through the classification process. The ability of machine learning to learn with data during the process of classification makes them more attractive and effective for malware classification. Seong and other methods automatically create the detection model using machine learning algorithms to evolve the detection model, so that new ransomware samples can be detected. The method is based on modification of TF-IDF algorithm to CF-NCF algorithm. CF-NCF focuses on feature appearance in each class, whereas TF-IDF focuses on term appearance in each document. Experimental results showed that CF-NCF has better performance than TF-IDF for ransomware detection [36].

[Kok et al.]use a pre-encryption detection algorithm [PEDA] for detecting crypto ransomware before working. The PEDA depends upon division of the detection process to two levels. The first is based on the previous archive of signature repositories [SR] which try to find any matches of the signature [for ransomware] with that of known ransomware. 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.]. Although the pre-encryption detection algorithm [PEDA] achieves ransomware detection prior to the encryption process, it is vulnerable to being misled if it uses new models, and the prediction process remains the critical option in the process. Machine learning is a branch of artificial intelligence that is concerned with designing and developing algorithms and technologies that allow computers to possess the property of "learning". In general, there are two levels of learning: inductive and deductive. Inductively inferred general rules and judgments from big data [34]. The primary task of machine learning is extracting valuable information from data, so it is very close to data mining, statistics, and theoretical informatics. Machine learning is used in many fields, from engineering to medicine [37].

Arthur Samuel is considered to be the first to use machine learning in 1959 to solve the game of checkers [36]. In the 1960s, machine learning was mostly used to categorize patterns. Machine learning is making computer software analyze tasks, and it makes machines evaluate the measurable performance to improve it, as this improved process gains more and more experience in implementing without needing to program the computer every time. Machine learning gives the computer instructions that allow it to learn from data without being given new step-by-step instructions by the programmer, via making decisions and making predictions and forecasts based on the data. The simple method of machine learning is to give training data to a learning algorithm. Machine learning is utilized in a broad variety of fields, such as medical diagnosis, pattern recognition, natural language processing, robotics, computer games, traffic prediction, product recommendation, data mining, etc. The author [Ray] discussed the most widely used machine learning algorithms, for example, Gradient Descent, linear regression algorithms, multiple linear regression, Logistic regression, Decision trees,

Support Vector Machines [SVM], Bayesian Learning, Nave Bayes [NB], K Nearest Neighbor [KNN], K mean Clustering algorithms, and Back Propagation algorithms. An example application of machine learning is SGD [Stochastic Gradient Descent], which will be evaluated with three types of challenges such as classification, regression, and clustering. Depending on the availability of types and categories of training data, one may need to select from the available techniques of "supervised learning", "unsupervised learning", "semi-supervised learning," and "reinforcement learning" to apply the appropriate machine learning algorithm. The use of machine learning appeared in the fight against cybercrime and ransomware programs due to the advantages it enjoys in analyzing processes that depend on different algorithms. Ransomware Detection Using Machine Learning, the rapid development of the use of the Internet and technology has led to the emergence of many challenges related to the security of information and data for users of the Internet, and these challenges are called Internet crimes, which will cost the global economy estimated losses of 10.5 Trillion dollars annually in 2025 [GLOBE NEWSWIRE, 2020]. Ransomware is one of the most prominent crimes in the world of the Internet, and it is expected that ransomware will have a greater share of all cybercrime by 2021.

The origin of the ransomware was established by Young and Yung at Columbia University [Al-Zwainy et al.], where the concept of the encrypted ransomware program appeared and was applied for the first time in 1996 and was first presented at the Security and Privacy Conference organized by the Foundation of Engineers in Electrical and Electronics. The program was called cryptocurrency viral extortion. One of the categories of malicious programs used in cyberattacks is ransomware for individuals, organizations, and governments, which has increased in popularity in recent years due to the high revenue. The authors in Noorbehbahani et al. mentioned that it is difficult to detect new ransomware families, such as Locky, Cryptowall, Cerber, etc., and that they have different versions, i.e., CryptXXX2.0 and CryptXXX3.0. Two main types of ransomware are locker-ransomware [which locks the device to prevent the sufferer from accessing it] and crypto-ransomware [which encrypts the data to block the sufferer's access]. In Firdausi et al., the authors mentioned that content-based, signature-based, and pattern-matching techniques [the static method] of malware analysis are less efficient compared with the high growth rate of malware. The invaders create new variants of existing malware using polymorphic, metamorphic, obfuscation, and other masking techniques [the dynamic method], which are hard to detect by using static detection systems. Automated behavior-based malware detection using machine learning techniques is a clever solution to alarm when any deviation occurs. The behavior of each malware in a simulated [sandbox] environment will be automatically analyzed and will generate behavior reports. These reports will be pre-processed into models for further machine learning [classification]. The classification of malware samples based on their behavior requires the implementation of algorithms that are capable of producing models and learning through the classification process. The ability of machine learning to learn from data during the process of classification makes it more attractive and effective for malware classification.

Seong and others method automatically creates the detection model using machine learning algorithms to evolve the detection model so that new ransomware samples can be detected. The method is based on the modification of the TF-IDF algorithm to the CF-NCF algorithm. CF-NCF focuses on feature appearance in each class, whereas TF-IDF focuses on term appearance in each document. Experimental results showed that CF-NCF has better performance than TF-IDF for ransomware detection [Ge et al.]. Kok et al. use a pre-encryption detection algorithm [PEDA] for detecting crypto-ransomware before working. The PEDA depends on the division of the detection process into two levels. The first is based on the previous archive of signature repositories [SR], which try to find any matches of the signature [for ransomware] with that of known ransomware. The other level depends on a learning algorithm [LA] that can find known and unknown ransomware in the system. The learning algorithm uses machine learning to create a predictive model using data from the application program interface [Kok et al.]. Although the pre-encryption detection algorithm [PEDA] achieves ransomware detection prior to the encryption process, it is vulnerable to being misled if it uses new models, and the prediction process remains the critical option in the process. A Framework for Analyzing Ransomware using Machine Learning: Experts have been trying to detect ransomware by analyzing the mechanism by which the computer will recognize the malicious programs via the effect that it inflicts on the computer and the programs. Some methods were adopted by the following: analyze I/O requests and follow-up changes that occur to the system to protect the master file in the NTFS file system so as to detect and prevent the significant number of zero-day ransomware attacks. Another method focuses on a machine learning approach for dynamically analyzing and classifying ransomware using logistic regression [32]. Most of the methods for discovering ransomware focus on noticing its effect on the system through the changes it makes to it during the encryption process and taking advantage of that to track ransomware from end to end by tracking ransomware's behavior from infection to payment [37]. Track financial transactions from the time the victim sends the money to the time the ransomware operators spend it. Data mining techniques are used to find unique correlation rules to identify and discover families of ransomware using a static and dynamic approach [Subedi et al.] [38]. In another direction, by designing an automated static analysis framework and making use of compilation instructions and dll files to improve the detection accuracy of ransomware, By reverse engineering the tested ransomware [8 samples] and regular binaries, you can get the code for different levels. After analyzing the data via static analysis, the model was built using machine learning, with an average of 92.11% ransomware detection accuracy [22]. With these good results, the process needs more experiments with more ransomware programs and a detailed study of its effect on machine learning algorithms [39-45].

Discussion

This section will discuss a comparison between the three prevention techniques previously mentioned. The research shows that ransomware attacks are on the rise and have doubled in the first quarter of 2020 due to the increase in remote working culture imposed by the COVID-19 pandemic. Many individuals who work remotely do not practice the same cybersecurity measures commonly imposed by the office environment. Also, most remote workers use personal devices that are not adequately equipped with security mechanisms such as antimalware packages, firewalls, intrusion detection and prevention systems, password management tools, and encryption software. Ransomware leverages new vulnerabilities found in systems and networks. Attacks focus on small, medium, and large companies that implement a remote working culture. Apart from encrypting files and locking devices, ransomware can also use sophisticated techniques to carry out data exfiltration, resulting in the exposure of sensitive information that may lead to severe security concerns and privacy violations in addition to financial losses and reputational damage suffered by victims. A detailed description of existing techniques such as honeypot, SSD-insider, and machine learning proposed by different scholars will be analyzed in the subsequent paragraph. The Honeypot is a non-artificial intelligence-based method. The goal is to create and monitor Honeypot folders for changes that could be used to detect the presence of ransomware. Although a Honeypot is a useful tool for tracking network activity, the method offers a limited view of ransomware and their activities on the network, as the absence of attack alerts does not mean that a Honeypot is not a target of ransomware attacks. A simple technique for easy recovery from ransomware attacks irrespective of the availability of the attacker's tools on the victim system to prevent recovery from such attacks has also been proposed. "A novel method for recovery from Crypto Ransomware infections". The approach analyzed common crypto ransomware and discovered that the ransomware attack involves the installation of tools on a victim's device to make recovery from a ransomware attack a herculean task. This technique provides easy recovery from ransomware infections by renaming the system tool that handles shadow copies of files. A similar study focused on preventing ransomware and protecting computer systems by identifying and blocking an attack. The strategy involves luring an attacker to ignorantly encrypt a large dummy file over a long period of time. This provides valuable time to render the remaining contents of the file system inaccessible to the ransomware. Performance evaluation of the proposed technique in a real-time environment showed that the approach is effective against ransomware attacks. A related work proposed an algorithm that probes a network for passive monitoring of traffic in order to detect the presence of ransomware and prevent attacks. Experimental analysis using 19 different ransomware families shows that it takes the presented algorithm less than 20 seconds to detect the presence of ransomware. Also, it was observed that not more than 10 files were lost within the 20-second duration. The method allows the recovery of lost files as their contents are stored in network traffic. It also has low false positives based on experiments conducted on traffic data from real-life corporate networks. In addition, detecting ransomware with Honeypot techniques that detect all activities carried out by ransomware was also proposed. The technique controls the Windows Safety logs using EventSentry and the File Screening service. Though it lacks feedback such as email alerts when attacks are detected and features to detect novel ransomware attacks, Moreover, a Social Leopard Algorithm to Detect IoT Ransomware Attacks was proposed for Intrusion Detection Honeypot. The approach is capable of detecting ransomware attacks on IoT networks. However, it lacks auto-tuning features and transferable learning abilities. The Dionaea Honeypot was proposed to capture different zero-day attacks and make sure they did not enter the system. This technique classifies the captured ransomware attacks into different groups. However, it cannot run on higher operating systems, except on SQL 2000 and XP versions of Windows.

The greatest disadvantage of Honeypots is that they have a narrow field of view. They just observe what movement is directed against them. If an attacker breaches into your network and attacks a number of systems, your Honeypot will be blissfully unaware of this activity unless it is attacked directly. If the Honeypot environment has been identified by the attacker for what it is, the attacker can now avoid that system and penetrate the organization, with the Honeypot never knowing that the attacker got in. As noted earlier, Honeypots have a microscope effect on the value of the data the users collect, enabling them to focus closely on data of known value. Machine learning is a branch of artificial intelligence that provides systems with the ability to learn from and detect patterns in existing data while making decisions with little or no human intervention. It is a method commonly used in data analysis to automate the building of analytical models [SAS Analytics Software & Solutions]. ML techniques enable computers to make predictions based on patterns found in large datasets. The algorithms are able to adapt to changes and make improvements as the size of the dataset increases. The ability of ML to make predictions based on known and unknown datasets makes it a verifiable tool for detecting ransomware attacks due to the unending release of new ransomware variants coupled with the large number of vulnerabilities that exist in information systems. File behavior detection is the fulcrum of the use of machine learning for detecting ransomware. The ability to make predictions based on file behavior makes ML a powerful tool for ransomware detection. The technique uses file behavior detection to distinguish between legitimate codes and malicious programs. This is because the execution of legitimate code presents a pattern of behavior that is distinguishable from that of malicious code execution. ML algorithms use specialized analysis [such as interactive debugging or post-mortem code execution analysis] to extract large amounts of salient and discriminant information in order to learn the behavior of a legitimate or normal application. ML-based ransomware detection tools perform detailed analysis of legitimate code execution and are able to identify malicious applications. Such tools make intelligent decisions and prompt

specific actions by leveraging their ability to distinguish between normal and abnormal program execution. Furthermore, ransomware detection using the Random Forest Technique, which is a Machine learning technique, was also proposed.

The technique detects and efficiently prevents botnet propagation in SDN. It has the capability of reducing the host infection rate by up to 25%. But the proposed technique lacks distributed decoy managers, which increases the system traffic load. It also reduces the entire system's performance and efficiency. Moreover, a model was built using machine learning after analyzing the data through static analysis. The model is capable of detecting ransomware with an average of 92.11% detection accuracy. However, the model needs further improvements in terms of its detection rate. However, the main issue that Machine Learning faces is the absence of good data. While improving algorithms often consumes most of the time for AI developers, data quality is essential for the algorithms to function as intended. The quintessential enemies of ideal machine learning are noisy data, dirty data, and incomplete data. The solution to this problem is to take the time to evaluate and scope data with meticulous data governance, data integration, and data exploration until you get clear data. Lastly, SSD-Insider++ can peruse and read page by page and erase block by block. Besides, ransomware can likewise read and encrypt the user's information and then overwrite it. Subsequently, pages that are infected with ransomware show a typical IO execution example of Read After Write. The answer to adapting to ransomware is to back up data in advance and recover it when compromised. However, the current methods, which backup and recovery data via a file system, require additional space costs for backup and IO performance overhead to calculate the ransomware infection, which implies the risk of damage to the backup data copy due to intelligent ransomware attacks. With this regard, the SSD-Insider++ technique monitors all inputs and outputs to detect ransomware. Due to the unique file system structure of an SSD, data extraction can be an extremely difficult and lengthy process. Because the data recovery process is so difficult and takes so long, it can be quite expensive. The summary of the existing techniques presented in Table 1

Table 1: Summary of The Existing Techniques.

Author (s)	Title	Methodology	Purpose	Pros	Limitation
Honeypot Techniques					
(Moore)	Detecting ransomware with honeypot techniques.	It used research investigated methods.	To detect all activities carried out by ransomware.	To control the Windows Safety logs using Event-Sentry and File Screening service.	Lack of feedback such as email alerts when attacks are detected. Lack features to detect novel ransomwares attacks.
(Sibi Chakkaravarthy et al.)	Design of Intrusion Detection Honeypot Using Social Leopard Algorithm to Detect IoT Ransomware Attacks.	Social Leopard Algorithm.	To design an Intrusion Detection Honeypot (IDH).	It is capable of detecting ransomware attacks in IoT networks.	It lacks auto-tuning features and transfer learning ability.
(Sethia and Jeyasekar)	Malware capturing and analysis using Dionaea honeypot.	Dionaea honeypot.	To capture different zero-day attacks.	It classifies the captured ransomwares attacks into different groups.	It cannot run on higher operating system, except on SQL 2000 XP version of windows.
			To make sure they did not enter the system.	It enables and guide researchers on how to develop a robust security mechanism against the malwares.	The technique lacks high honeypot interaction capability.
Machine Learning Techniques					
(Khammas)	Ransomware Detection using Random Forest Technique.	Machine learning technique.	To detect and efficiently prevent botnet propagation in SDN.	It has the capability of reducing the host infection rate up to 25%.	It lacks distributed decoy managers which increases the system traffic load.
				Also, it can increase an adversary's wasted time.	It reduces the entire system performance and efficiency.
(Daku et al.)	Behavioral-Based Classification and Identification of Ransomware Variants.	Machine Learning	To identify finest behavioral attributes.	It achieves best classification precision.	It only works for small datasets.
(Firdausi et al.)	Analysis of machine learning techniques used in behavior-based malware detection.	Machine Learning Techniques.	To provide another malware detection technique	The proof-of-concept result obtained was good	The methods need to accommodate large datasets
(Shemitha and Dhas)	Research perceptions on ransomware attack.	Machine Learning Techniques	A complete analysis on conventional authentication protocols in network	To provide a network security models alongside with the authentication protocol	The proposed model is not empirically proven.

SSD-Insider++					
(Sungha Baek, Youngdon Jung et al.)	SSD-assisted Ransomware Detection and Data Recovery Techniques	SSD-Insider++ Technique.	To detects I/O configurations of a host system.	It attains high accuracy of detecting ransomware. Also, it provides an instant data recovery	The techniques need to be optimized in terms of speed.
(Baek et al.)	Internal defense of solid-state drive against ransomware with perfect data recovery.	SSD-Insider	To protect SSD against ransomware with perfect data recovery.	To analyze correlation between ransomware activities.	Achieving feasible results are challenging due to the fact that different ransomware possesses different features.

Recommendation

There are general recommendations for those who are interested in this field of research, including remote workers, students, and ordinary internet users, in order to avoid ransomware and other malware attacks. The ability to safely communicate in an E-Learning system is an important element in providing a safe learning environment that serves students, staff, faculty, and visitors. A necessary Cybersecurity consideration to protect higher education institutions might be taken into account. First, using genuine anti-virus programs with continuous updating of the software [provide patches for vulnerabilities] and always monitoring the results by creating access control lists Second, avoid using crack programs; make sure to use the original software version. Next, be careful to make backup copies of devices and data in case any problem occurs, or loss of information occurs, such as using an external hard disk or flash, etc., which will be easily recoverable in the case of a breach. In addition, embezzlement in the name of distance education It is possible to send false messages to request material matters, so care must be taken with the sources of information. Change the password and use strong passwords; try to use a minimum of 12 characters long and mix uppercase, lowercase, and special characters. Moreover, avoid opening any suspicious links and ensure the safety of the sites. It is important to carefully monitor the networks so that users can have confidence knowing that the business infrastructure is protected by a strong security protocol. Also, empowering and supporting cybersecurity education and training for employees and students using some Learning Management Systems [LMSs], like Cybersecurity Learning Management Systems [CyLMS], Finally, the E-Learning environment must establish and implement strong written internal and external cybersecurity policies for safe deployment, maintenance, and responsible or acceptable use to minimize potential weaknesses, such as implementing access points on the network, and prevent unauthorized access.

Conclusion

Despite the fact that digital information has improved people's lives in various fields, it still has some flaws and gaps that would affect the smoothing of operations, such as cyber-attacks. Cyber-attacks are considered cyberspace crimes that are committed by cybercriminals or hackers. These crimes target an individual's or organization's computers or networks to cause harm with the purpose of making profit or retaliation. This study provides a comprehensive evolution of ransomware attacks from the inception of computer development. It is important to note that ransomware has different behaviors when compared with conventional malware. Some examples of schools that were affected by this deadly attack are presented in this paper. Furthermore, several enhanced techniques, such as honeypot, SSD-Insider, and machine learning, have been proposed for effective and reliable detection of ransomware. The advantages and disadvantages of these algorithms have been discussed, along with examples of practical applications using the mentioned techniques. Finally, some insightful advice and recommendations for remote workers and school communities are mentioned. This study will serve as a guideline for potential researchers, and it is expected that it will give insight to the readers in making a decision about identifying the available options and choosing the appropriate algorithm in the specific problem-solving context.

References

1. Pont Jamie, Osama Abu Oun, Calvin Brierley, Budi Arief (2017) A Roadmap for Improving the Impact of Anti-Ransomware Research. Renewable and Sustainable Energy Reviews 12(3): 23-30
2. Zhang Kennedy, Leah, et al. (2018) The Aftermath of a Crypto-Ransomware Attack at a Large Academic Institution. Proceedings of the 27th USENIX Security Symposiumpp. 1061-1078.
3. Zhang Kennedy Popoola Segun I, Aderemi A Atayero, Ujioghosa B Iyekekpolo, Samuel O Ojewande, Faith O Sweetwilliams et al. (2018) Ransomware: Current Trend, Challenges, and Research Directions. Communication and Media Ethics 1(1): 469-484.
4. Tanana Dmitry (2019) Complex Ransomware Counteraction Technique. SIBIRCON 2019 - International Multi-Conference on Engineering, Computer and Information Sciences, Proceedings 5(1): 636-638.
5. Pambhar Hiral (2018) An Advanced Web-Based Bilingual Domain Independent Interface to Database Using Machine Learning Approach pp. 197-204.
6. Chen Qian, Robert A Bridges (2017) Automated Behavioral Analysis of Malware: A Case Study of Wannacry Ransomware. Proceedings - 16th IEEE International Conference on Machine Learning and Applications, ICMLA 2017 pp. 454-60.
7. Bhardwaj Akashdeep, Vinay Avasthi, Hanumat G Sastry (2016) Ransomware Digital Extortion: A Rising New Age Threat. Indian Journal of Science and Technology 9(14): 1-5.
8. Al Rahmi, Waleed Mugahed, Ahmed Alzahrani, Noraffandy Yahaya, Nasser Alalwan, et al. (2020) Digital Communication: Information and Communication Technology (ICT) Usage for Education Sustainability 12(12): 1-18.
9. Humayun Mamoona, NZ Jhanjhi, Ahmed Alsayat, Vasaki Ponnusamy (2020) Internet of Things and Ransomware: Evolution, Mitigation and Prevention. Egyptian Informatics Journal 22(1): 105-117.

10. Shemitha P A, Julia Punitha Malar Dhas (2020) Research Perceptions on Ransomware Attack: A Complete Analysis on Conventional Authentication Protocols in Network. Evolutionary Intelligence 15(7): 1-16.

11. Hassan, Nihad A (2019) Ransomware Revealed: A Beginner's Guide to Protecting and Recovering from Ransomware Attacks. Access, IEEE.

12. Genç, Ziya Alper, Gabriele Lenzini (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. Cole Bruce (2020) PREVENTING RANSOMWARE WITHIN LOCAL GOVERNMENT AGENCIES: A PUBLIC POLICY ANALYSIS PERSPECTIVE. Computer and Information Science 6(3): 12–67.

14. Yaqoob Ibrar, Ejaz Ahmed, Muhammad Habib ur Rehman, Abdelmuttlib Ibrahim Abdalla Ahmed, Mohammed Ali Al-garadi et al. (2017) The Rise of Ransomware and Emerging Security Challenges in the Internet of Things. Computer Networks 129(1): 444-458.

15. Gómez Hernández J A, L Álvarez González, P García Teodoro (2018) R Locker: Thwarting Ransomware Action through a Honeyfile-Based Approach. Computers and Security 73(1) 389-398.

16. Kansagra Deneesha (2016) Ransomware: A Threat to Cyber Security. Computre Science & Electronics Journals 7(1): 224-227.

17. Su, Dan, Jiqiang Liu, Xiaoyang Wang, Wei Wang (2019) Detecting Android Locker-Ransomware on Chinese Social Networks. IEEE Access 7(1): 20381-20393.

18. Al-rimy Bander Ali Saleh, Mohd Aizaini Maarof, Syed Zainudeen Mohd Shaid (2018) Ransomware Threat Success Factors, Taxonomy, and Countermeasures: A Survey and Research Directions 72(1): 144-166.

19. Ray Susmita (2019) A Quick Review of Machine Learning Algorithms. Proceedings of the International Conference on Machine Learning, Big Data, Cloud and Parallel Computing: Trends, Prespectives and Prospects, COMITCon pp. 35-39.

20. Poudyal Subash, Kul Subedi, Dipankar Dasgupta (2018) A Framework for Analyzing Ransomware Using Machine Learning. Proceedings of the 2018 IEEE Symposium Series on Computational Intelligence pp. 1692-1699.

21. Daku Hajredin (2018) Behavioral-Based Classification and Identification of Ransomware Variants Using Machine Learning. Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering pp. 1560-1564.

22. Pascariu Cristian (2019) Ransomware Honeypot.

23. Seungjin Lee, Azween Abdullah, Noor Zaman Jhanjhi (2020) A Review on Honeypot-Based Botnet Detection Models for Smart Factory. International Journal of Advanced Computer Science and Applications 11(6): 418-435.

24. Sibi Chakkaravarthy S, Dimple Sangeetha, Meenalosini Vimal Cruz, V Vaidehi, Balasubramanian Raman (2020) Design of Intrusion Detection Honeypot Using Social Leopard Algorithm to Detect IoT Ransomware Attacks. IEEE Access 8(1): 169944-169956.

25. GENÇ Ziya Alper (2019) ANALYSIS, DETECTION, AND PREVENTION OF CRYPTOGRAPHIC RANSOMWARE. IEE Irish Signals and Systems Conference 2(5): 12.

26. Kok S H, Ransomware, Azween Abdullah, NZ Jhanjhi, Mahadevan Supramaniam (2019) Threat and Detection Techniques: A Review. IJCSNS International Journal of Computer Science and Network Security 19(2): 136-146.

27. Moore Chris Detecting Ransomware with Honeypot Techniques. Proceedings - 2016 Cybersecurity and Cyberforensics Conference pp. 77-81.

28. Sethia Vasu, A Jeyasekar (2019) Malware Capturing and Analysis Using Dionaea Honeypot. Proceedings - International Carnahan Conference on Security Technology pp. 0–3.

29. Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, Faiz Alotaibi (2017) Internet of Things Security: A Survey. Journal of Network and Computer Applications 88(1): 10-28.

30. Sgandurra Daniele, Luis Muñoz-González, Rabih Mohsen, Emil Constantin Lupu (2016) Automated Dynamic Analysis of Ransomware: Benefits, Limitations and Use for Detection pp. 1-13.

31. Sungha Baek, Youngdon Jung, David Mohaisen, Sungjin Lee, DaeHun Nyang (2020) SSD-Assisted Ransomware Detection and Data Recovery Techniques. IEEE Transactions on Computers 70(10): 1762-1776.

32. Firdausi Ivan, Charles lim, Alva Erwin, Anto Satriyo Nugroho (2010) Analysis of Machine Learning Techniques Used in Behavior-Based Malware Detection. Proceedings - 2010 2nd International Conference on Advances in Computing, Control and Telecommunication Technologies pp. 201-203.

33. Fosso Wamba Samuel, Shahriar Akter, Andrew Edwards, Geoffrey Chopin, Denis Gnanzou (2017) How 'Big Data' Can Make Big Impact: Findings from a Systematic Review and a Longitudinal Case Study. International Journal of Production Economics 165(1): 234-246.

34. Al Zwainy Faiq, Ibraheem A Mohammed, Kamil A K Al-Shaikhli (2017) Diagnostic and Assessment Benefits and Barriers of BIM in Construction Project Management. Civil Engineering Journal 3(1): 63-77.

35. Noorbehbahani, Fakhroddin, Farzaneh Rasouli, Mohammad Saberi (2019) Analysis of Machine Learning Techniques for Ransomware Detection. Proceedings of 16th International ISC Conference on Information Security and Cryptology pp. 128-133.

36. Ge Mengmeng, Jin B Hong, Walter Guttmann, Dong Seong Kim (2017) A Framework for Automating Security Analysis of the Internet of Things. Journal of Network and Computer Applications 83(1): 12-27.

37. Huang, Kaixing, Qi Zhang, Chunjie Zhou, Naixue Xiong, et al. (2017) An Efficient Intrusion Detection Approach for Visual Sensor Networks Based on Traffic Pattern Learning 47(10): 2704-2713.

38. Subedi, Kul Prasad, Daya Ram Budhathoki, Dipankar Dasgupta (2018) Forensic Analysis of Ransomware Families Using Static and Dynamic Analysis. Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops pp. 180–185.

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

40. Pandey Abhishek Kumar, Ashutosh Kumar Tripathi, Gayatri Kapil, Virendra Singh, Waris Khan et al. (2020) Trends in Malware Attacks: Identification and Mitigation Strategies. Journal of Computer Assisted Learning 3(6): 47-60.

41. Khammas Ban Mohammed (2020) Ransomware Detection Using Random Forest Technique. ICT Express 6(4): 325-331.

42. Fan Zunlin, Duyan Bi, Linyuan He, Ma Shiping, Shan Gao et al. (2017) Low-Level Structure Feature Extraction for Image Processing via Stacked Sparse Denoising Autoencoder. Neurocomputing 243(1): 12-20.

43. Al zahrani Abdulrahman, Ali Alshehri, Hani Alshahrani, Huirong Fu (2020) Ransomware in Windows and Android Platforms. IEEE Communications Surveys & Tutorials 2(12): 23-32.

44. Hesham Alshaikh, Nagy Ramadan, Hesham A Hefny (2020) Ransomware Prevention and Mitigation Techniques. International Journal of Computer Applications 177(40): 31-39.

45. Baek Sungha, Youngdon Jung, Aziz Mohaisen, Sungjin Lee, DaeHun Nyang (2018) SSD-Insider: Internal Defense of Solid-State Drive against Ransomware with Perfect Data Recovery. Proceedings - International Conference on Distributed Computing Systems pp. 875-84.

DOI: 10.32474/CTCSA.2023.02.000150