ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/339326833

Ransomware Prevention and Mitigation Techniques

Article *in* International Journal of Computer Applications · February 2020

DOI: 10.5120/ijca2020919899

CITATIONS
11

READS
7,531

3 authors:

Hesham Alshaikh
Faculty of Graduate Studies for Statistical Research (FGSSR)
2 PUBLICATIONS **11** CITATIONS
SEE PROFILE

Nagy Ramadan
Cairo University
96 PUBLICATIONS **318** CITATIONS
SEE PROFILE

Hesham A. Hefny
Faculty of Graduate Studies for Statistical Research (FGSSR)
279 PUBLICATIONS **2,144** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Enzyme Classification and Prediction View project

Exploring Key Performance Indicators View project

All content following this page was uploaded by Hesham Alshaikh on 22 February 2020.

The user has requested enhancement of the downloaded file.

Ransomware Prevention and Mitigation Techniques

Hesham Alshaikh
Sadat Academy for Management Sciences, Egypt

Nagy Ramadan
Department of Information Systems and Technology
Faculty of Graduate Studies for Statistical Research, Cairo University, Egypt

Hesham Ahmed Hefny
Department of Computer Science
Faculty of Graduate Studies for Statistical Research, Cairo University, Egypt

ABSTRACT
Ransomware is a malware family that using security techniques such as cryptography to hijacking user files and associated resources and requests cryptocurrency in exchange for the locked data. There is no limit to who can be targeted by ransomware since it can be transmitted over the internet. Like traditional malware, ransomware may enter the system utilizing "social engineering, malware advertising, spam emails, take advantage of vulnerabilities, drive-by downloads or through open ports or by utilizing back doors". But in contrast to traditional malware, even after removal, ransomware influence is irreparable and tough to alleviate its impact without its creator assistance. This kind of attack has a straightforward financial implication, which is fueled by encryption technology, cyber currency. Therefore, ransomware has turned into a profitable business that has obtained rising popularity between attackers. As stated by "Cybersecurity Ventures", ransomware is the quickest increasing type of cybercrime. Since, global ransomware wastage expense is predicted to hit $20 billion in 2021, up from just $325 million in 2015 which, is 57X extra in 2021. In this paper, a brief of the recent research in the prevention of ransomware attacks and the best practices to mitigate the attack impact is presented.

General Terms
Ransomware prevention technique, ransomware mitigation technique, signature-based, behavior-based.

Keywords
Ransomware, Cryptography, Cryptocurrency, Cybercrime, Malware, Cybersecurity, Vulnerability, Cyberattacks.

1. INTRODUCTION
Cybercriminal attackers understand that data, files, networks and all digital resources are the key factors for the growth of regular working and any business [1]. These digital assets are so precious to the business therefore, the quickest and preferable way to earn great money is to keep all these resources at ransom. Thus, rise ransomware which, a malware that commonly encrypts all files and requests for a payment in bitcoin to give the victim the decryption key [2].

As stated by the "Cisco/Cybersecurity Ventures 2019 Cybersecurity Almanac" cybercriminal activity considered one of the major challenges that mankind will confront in the following two decades. Cyberattacks are the quickest increasing crime globally, and they are growing, in size, sophistication, and expenses.

Also, they predict that cybercrime losses will cost the world $6 trillion annually by 2021 and more than 70% of all cryptocurrency bargains yearly will be for illegitimate activity.

Advances in technology are the main driver for economic growth but, have also led to a higher incidence of cyberattacks. The 10 major data breaches in the last two decades combined with the number of hacked accounts and year occurred. As claimed by Quartz, Yahoo, three billion (2013); Marriott, half billion (2014-2018); Adult FriendFinder, 412 million (2016); MySpace, 360 million (2016); Under Armor, 150 million (2018); Equifax, 145.5 million (2017); eBay, 145 million (2014); Target, 110 million (2013); Heartland Payment Systems, 100+ million (2018); LinkedIn, 100 million (2012).

Moreover, other research from "Cybersecurity Ventures" that approximate there are 111 billion code lines of new software being generated yearly, which brings in the possibility for an enormous number of vulnerabilities that can be exploited. Utilizing zero-day attack alone is forecasted to be once a day by 2021, up from once a week in 2015 [3]. This attack technique makes the prevention task very difficult, even for giant firms with a generous cybersecurity fund [4].

The 5 most cyber attacked industries over the previous 5 years are transportation, healthcare, financial services, manufacturing, government. "Cybersecurity Ventures" forecast that media and entertainment, retail, petrol and natural gas, teaching (kindergarten to 12 grade and higher education) and legal will be among the top 10 industries for 2019 to 2022.

Hacking tools and equipment for identity theft, cyberattacks, malware, ransomware, and other nefarious intent have been obtainable in the online market for many years at a low price as $1 which, makes it nearly free to enter the life of cybercrime.

Cybersecurity worldwide market value was $3.5 billion in 2004 while, its value was more than $120 billion in 2017. The cybersecurity marketplace rises by about 35X during that period. The 2019 U.S. president's financial plan includes $15 billion for cybersecurity, the Department of Defense (DoD) was the greatest subscriber with $8.5 billion in cybersecurity financing in 2019 [3].

Ransomware is a malware family that using security techniques such as cryptography to hijacking user files and associated resources, then requests cryptocurrency in exchange for the locked data [5]. Some ransomware gets into the system utilizing social engineering, malicious advertisements, spamming, drive-by downloads, while others try to discover vulnerabilities to exploit it, using open ports or exploiting a backdoor to get inside [1]. Consequently, vulnerability testing and security loopholes must be identified, and people must be aware of these kinds of exploiting

mechanisms [6].

Ransomware as a service (RaaS) is a service that grants easy attainment of ransomware codes without any special programming skills at a monetary value. The price could be an explicit buy, or a profit margin scheme could be employed. This shows that collaboration exists between criminals [7]. One side oversees originating a custom binary ransomware code, while the other side simply downloads the customized binary ransomware and organize the dissemination of the contagion or the attack campaign usually through botnet email, and both parties enjoy the profit from a successful attack [8].

Therefore, ransomware has become a profitable profession that has gained boosting popularity between attackers [5]. The publicity of ransomware has originated an extraordinary ecosystem of cybercriminals. The ransomware attack has a direct financial implication, which is fueled by encryption technology, cyber currency. Encryption is effective and almost unbreakable. Anonymous cyber currency can obviate traceability. Easily attainable ransomware code permits easy entry to the cybercrime world. A combination of these provides an attractive avenue for cybercriminals, producing specialist cybercriminals [7,9].

The U.S. Department of Justice (DOJ) has depicted ransomware as a new profession model for cybercrime, and a universal phenomenon. Global ransomware devastation price is forecasted to hit $20 billion in 2021, up from just $325 million in 2015, as stated by "Cybersecurity Ventures". So, it is 57X extra in 2021. That turns out ransomware into the fastest increasing type of cybercrime. "Cybersecurity Ventures" anticipates that businesses shall fall prey for ransomware onslaught every 11 seconds by 2021, up from every 40 seconds in 2016. Hence, global spending on security awareness training for employees one of the quickest increasing categories in the cybersecurity industry is predicted to reach $10 billion by 2027, up from about $1 billion in 2014 since, training operator on how to reveal and behave with ransomware is a critical obstacle [3].

Ransomware is the biggest threat to businesses, and it is the main reason for enormous damages such as *first:* business deadlock and massive casualties to the economy [1]. In May 2019, the town of Baltimore uncovers that it was a martyr of a ransomware attack, in which crucial files are encrypted remotely till a ransom is settled. The town instantly puts systems offline to hinder the ransomware from propagating, but unfortunately, it was after taking down the parking mulcts database, email, voice mail and the water invoices system, property taxes and vehicle citations [10].

Second: breakdown production of Renault and Nissan motor manufacturing UK, after the ransomware infected some of their systems. Spain's Telefónica, FedEx and Deutsche Bahn were hit with WannaCry ransomware infection as well in 2017.

Third: life-threatening damages. National Health Service hospitals in England and Scotland, and up to 70,000 devices, including computers, MRI digital scanners, Operation room gears, and blood storage fridges have been infected with WannaCry [11].

In this survey, a comprehensive review of ransomware recovery, mitigation, and prevention techniques are performed to facilitate future research, study, and analysis. Furthermore, understanding of ransomware and assist researchers and developers in their efforts to find adequate solutions. The obtained results hopefully may be used to form a base for designing and developing more effective defense solutions against ransomware attacks.

This survey is organized into five sections, *the first one* being the present introduction in which, the relevant background information on cybercrime in general and particularly on ransomware is presented to provide an insight into how the ransomware attack is achieved. Then, *section 2* shows an updated review of research in the area of ransomware and the employed techniques for detection, mitigation, and prevention of ransomware attack. *Section 3* discusses the present research directions in ransomware and summarizes its pros and cons. The concluding remarks are presented in *section 4*. Finally, *section 5* discusses potentially future directions. *Table (1), (2)* shows a summary of related work.

2. RELATED WORK

There are a lot of research efforts have been done to prevent the ransomware attacks employing different approaches to identify the presence of ransomware such as:

2.1 Signature-based Approach:

The signature approach focuses on, detecting ransomware unique patterns such as a distinctive sequence of bytes in the ransomware source code, the order of call functions and the content of the ransom demand message. Such sequences are saved in a database and during the scanning, the anti-malware software tries to detect such patterns in executable files.

Signature-based malware detection techniques have conventionally been hugely preferable because they have a low false positive ratio. So that an alarm is triggered if a certain well-known pattern is observed. However, Goyal et al. [12] Emphasize that the signature-based approach is unable to cope with the obfuscated code in ransomware and cannot detect new strains until they have been analyzed by analyst [13].

2.2 Behavior-based Approach:

In this approach, the researchers create an artificial, realistic execution environment and monitors how ransomware interacts with it. Behavior-based detection is the notion of observing the characteristics of how the malware operates. Hence, it relies on study typical ransomware behavior like file access, file system activity, and network activity.

2.2.1 File Access and File System Activity:

Grant and Parkinson [13] investigated the behavioral characteristics of ransomware focusing on interplay with the underlying file system. They implemented a file monitoring application to monitor all interactions with files in a delimited directory due to the utilization of windows core functionality. This study identifies that each ransomware instance has a unique behavioral pattern regarding file system activity which is, remarkably dissimilar to those of normal user interactions. Furthermore, it shows that ransomware may be identified using individual or shared patterns.

Furthermore, Kok et al. [14] proposed a pre-encryption algorithm that composed of two phases the first, is a machine learning algorithm used to detect the ransomware before encrypting user files, which based on API pattern recognition. Hence, it uses Cuckoo sandbox to captures the (API) generated by the suspicious program and analyzes them, but it may have a high false positive rate. The second phase is a signature repository used to store the generated signatures of suspicious programs that, used to detect the crypto ransomware in the pre-execution stage using signature

matching however it, can only detect known crypto ransomware. Therefore, each of the two phases complements each other and provides an efficient method to protect users from crypto ransomware.

Whereas Scaife et al. [15] presented an early warning awareness system called CryptoDrop, which generate a notification at the time of suspicious file activity and allow users to make the final decision on whether the activity is desired or not. Using a set of behavior denotations CryptoDrop can eliminate any process that seems to be manipulating an enormous amount of user data. The authors allege this system prevent ransomware from executing with a median loss of only 10 files and does not inspect files outside of the user documents directory. Though, Wolf [16] underdetermined the CryptoDrop efficiency, claiming that 40 files on average could be properly encrypted before it can detect suspicious activity.

While, Continella et al. [17] proposed a technique called ShieldFS that copying files when it altered, saving the copy in a preserved area permitting any alterations to be made to the original file while it keeps track of changes made to it. The detection system established on the integrated analysis of entropy of write operations, frequency of reading, write, and folder itemization operations, fraction of files renamed, and file type usage statistics. Subsequent if ShieldFS determines that the process is normal, the saved file can be discarded from the kept area since the original file has not been encrypted by ransomware. However, if ShieldFS decided that a process is harmful, the aggressive process will be suspended, and the saved copies can be brought back, substituting the altered (encrypted) versions.

Likewise, Kharraz and Kirda [18] proposed a similar approach to ShieldFS called Redemption where file operations are being redirected to a dummy copy. This technique initiates a copy from each file subject to be modified by the ransomware, and then redirects the file system processes (demanded by the ransomware to encrypt the target files) to the copies, hence leaving the original files undamaged. Redemption uses the Windows kernel development framework to reflect the write requests from the target files to the preserved files in a transparent data buffer. However, rewrite and create operations can experience slowdowns ranging from 7% to 9% when dealing with many small files. Creating the reflected files and redirecting the write demands to the restricted area are the main reasons for this performance hit under high workloads.

Different perspectives adopted by, Winter et al. [19] they emphasize that technology is not improving as fast as the complexity of threats. They have started a cyber-autoimmune disease where an antivirus system is responsible for destroying the computer's operating system after they infected system files with malicious code. To draw interest to flaws in protection systems which, allow attackers to reach their targets more easily causing serious damage.

However, Lika et al. [20] concluded that no actual solution could be used to decrypt the hard disks that have been encrypted by NotPetya, ransomware. While crucial answers are lacking, the vaccine has been found where, the existence of a local file, prevents the NotPetya execution. Hence, the authors intended to educate users to increase their awareness reactively through gamification.

2.2.2 Network behavior:

Some of the research works were interested in finding the network behavior of ransomware. Zimba et al. [21] studied the emerging cyber threat to crucial infrastructure and magnify the network segmentation approach, prioritize the security of production network devices and limiting ransomware propagation. By applying reverse engineering on WannaCry ransomware and perform source code analysis they uncover the employed techniques to discover vulnerable nodes.

Thus, Zimba and Mulenga [22] employed reverse engineering on the underlying malware program logic. Using the dynamic analysis to captivate the corresponding network actions associated with such logic to unmask WannaCry ransomware network interactions. The source code analysis shows that the ransomware fetches the network adapter properties to determine whether it's residing in a private or public subnet to effectuate substantial network propagation and subsequent damage. Nonetheless, the employed network techniques are specified to WannaCry ransomware only.

Furthermore, Almashhadani et al. [23] established a thorough behavioral analysis of crypto ransomware network interactions, taking Locky, one of the extremely dangerous ransomware families. A devoted testbed was constructed, and a set of worthy and informational network characteristics were educed and categorized into multiple types. A network-based invasion discernment system was implemented, utilizing two separate classifiers working side by side on packet and flow levels. The authors assume that most ransomware families try to get in touch with command and control servers before harmful payloads are achieved which, is not the case in all ransomware families. Also, monitoring outbound connections can be simply eschewed by connection encryption.

Moreover, Akbanov et al. [24] accomplished extensive dynamic analysis on WannaCry ransomware and they found out that its mechanism based on two different components. The first enables WannaCry to disseminate through network devices like a worm by generating a list of local and global IP addresses and scanning both internal and external networks for Microsoft's MS17-010 vulnerability by sending packets via port 445 to infect unpatched systems. The second is the encryption process since it has embedded RSA keys used for decrypting the required malicious DLL representing the encryption component. Also, they have revealed that WannaCry communicates with command and control server through embedded. onion addresses via a secure channel on port 443 and the common Tor ports 900, 9050 to download the "Tor-browser" installation software. The outcome of this research may help to accomplish an efficient mitigation mechanism against WannaCry and any ransomware family that has the same behavior.

2.3 Contemporary Prevention Methods

2.3.1 Categorizing Ransomware Characteristics:

To facilitate the ransomware detection operations. Rajput [6] studied the different types of ransomware families as he focused on their evolution and characteristics. The result of this analysis shows that many ransomware families exhibit similar characteristics.

Therefore, the main contribution of Hull et al. [25] is a predictive model for categorizing ransomware behavioral characteristics, which can then be used to ameliorate uncovering and dealing with ransomware incidents. The categorization was done with respect to the deployment stages

of ransomware, by establishing a predictive model called "Randep". The stages are fingerprinting, propagate, communicate, map, encrypt, lock, delete and intimidation. This model concluded from a study of 18 ransomware families. By observing windows Application Programming Interface (API) function calls throughout each ransomware execution, to comprehend what actions a ransomware strain might do. Nevertheless, not all ransomware families go through all these deployment stages.

Moreover, Chen and Bridges [26] established an automated method to extract distinguishing features of malware from host logs, which contain many non-malicious events. They have utilized behavior logs from analysis reports created by Cuckoo sandbox under several situations of ordinary and malware interactions.

likewise, Verma et al. [27] focused on the indicators of compromises (IOCs) for ransomware using Cuckoo sandbox. Which will be used to set the base for analyzing and classifying new ransomware based on their behavior. Using supervised machine learning classifiers to classify the ransomware samples to their respective 7 families that they have worked on.

While Popli and Girdhar [1] ran the ransomware in a simulated environment using Cuckoo to analyze their attack process, then predict future ransomware, its expected impact and how it will be difficult to be detected if polymorphic, metamorphic and other obfuscation techniques used by ransomware. Even though these methods reveal how ransomware interacts with the environment, but it can't be used to reveal ransomware infection immediately.

2.3.2 Access Control:

Another prevention technique is to adopt an authentication-based access control mechanism under the name of "AntiBotics" presented by Ami et al. [28]. "AntiBotics" has three components. *The first component* is the Policy Enforcement Driver which acts as an initial gate that records and halts any file modification attempts such as, renames or deletions. To modify a file, a challenge is created such as CAPTCHA or biometric authentication to authenticate the user actions. *The next component* is the Policy Specification Interface, which is a GUI program that allows administrators to configure the system policies. *The last component* is the Challenge-Response Generator wich, controls the generated challenges, i.e. the time-out rate, and mechanisms to prevent large generations of challenges. Since humans, are always the fragile bond in any defense system. Users may grant access to a process which, is infected with malignant code.

Also, Christopher and Kumar [29] Presented a preventative technique based on ransomware behavior, targeting three Indicators of Compromise (IOC), file changes within a time interval, file entropy and manipulation of canary files. The File system watcher filter used to monitor two artificial network drives and disabling methods used to alter Access Control Levels (ACL) of files and folders to revoke the writing privileges when compromise confirmed. Nevertheless, the system will suffer from a lot of strain when the monitoring is done on physical drives instead of artificial drives.

2.3.3 Recovery After Infection:

This is a different technique aims to recovering from the ransomware attack without ransom paying to accomplish this, Zimba and Chishimba [9] suggested to follow mitigation strategies and recommend best practices based on clarifying core components of successful ransomware attack campaigns. Such as securing email since emails are a major source of ransomware and apply security patches regularly to fix vulnerabilities and avoid ransomware. Results show that lack of offline backup and poorly implemented offline backup strategies end up costing businesses more than the ransom demand itself. Nonetheless, systems may still vulnerable to zero-day attacks.

Likewise, Lee et al. [30] provided a new technique to recover from a ransomware attack using the key backup. They assumed that the ransomware uses windows operating system CNG cryptography library to encrypt user files. Therefore, they seek to pick up the keys when ransomware generating it inside the host or receiving it from the server. Hence, using it for file recovery after ransomware infects the system and encrypt the files. Despite this, some ransomware uses libraries other than CNG such as Cryptolocker which uses the CAPI cryptography library and others implement their own cryptography library. Furthermore, a few ransomwares don't obtain a key from the server, such as Ordinypt and Petya instead, they encrypt files with randomly generated keys which lead to data loss. Moreover, monitoring the outbound communication can be simply bypassed by encrypting these connections.

Whereas, Zimba et al. [31] used a ransomware categorization framework to classify the ransomware attack maliciousness based on data deletion and file encryption attack structures. The categories classify the technical skill and the overall effectiveness of potential ways of retaining the data without paying the ransom demand. This framework helps to understand potential inadequacies and glitches to be utilized for data retrieval via system volume shadow copies or third-party software.

Furthermore, Zimba et al. [32] employed reverse engineering and dynamic analysis to assess the underlying attack structures and data deletion techniques that ransomware use. And have concluded that no matter how destructive a crypto ransomware attack might seem, the key to data recapture options lies in the underlying attack design and the implemented data deletion methodology. Though other ransomware has an irreversible impact, for example, no actual solution could be used to decrypt the hard disks that have been encrypted by NotPetya.

2.3.4 Trapping Attacker:

lately, some authors have developed further prevention methods. Gómez-Hernández et al. [33] proposed a general methodology called R-Locker to thwart crypto ransomware actions. It is based on the deployment of a honey file design of the Linux system to block the ransomware when it accesses a canary file, thus allowing it to maintain the rest of the data. In addition to that, this approach can automatically launch steps to solve the infection. Nevertheless, this solution has some limitations such as, that just a part of the complete file system (that corresponding to the user that installs R-Locker) is protected, also the poor distribution of the traps can reduce the efficiency of the actual protection of the data. At the same time, this defense can be passed over by the removal of the central trap file. Moreover, it can be partially bypassed by accessing given folder files by ransomware in a random way where all files in the folder may be encrypted before the sample can be blocked.

Whereas, Wang et al. [34] utilized an advanced defense schemes to protect important hosts under targeted ransomware attacks. By employing the cyber deception technology to blocking attackers via a network deception environment to

help protect crucial systems through attack guidance, by drawing attackers off from these preserved systems. As a result, they deliberately set the administrator privileges of the deception environment as weak passwords and leave common vulnerabilities in the environment, such as EternalBlue, to attract attackers. Furthermore, they have developed an automatic analysis system by taking preference crypto ransomware natural language processing and machine learning techniques to trace-back (RDP) Remote Desktop Protocol-based ransomware attacks and identify the original attack sources. Accordingly, this approach is just for hindering RDP-based ransomware attacks only.

Furthermore, Shaukat and Ribeiro [35] works is based on analyzing an extensive dataset of ransomware families presents RansomWall, a layered safeguard system for protection versus cryptographic ransomware. It follows a hybrid approach of combined static and dynamic analysis to generate a compact set of features that characterizes the ransomware behavior. It uses trap layer to help in early detection and supervised machine learning algorithms for unearthing zero-day intrusions. When preliminary layers of RansomWall tag a process for suspicious ransomware behavior, files altered by this process are copied into a protected place for preserving user data until it is classified as "ransomware or benign" by the machine learning layer. Nevertheless, user critical files may be attacked earlier than honey files.

3. DISCUSSION

It is significant to note that the research community has put attention in detection, prevention, and even recovery techniques to prevent ransomware infections and mitigates its impact to avoid data and large economic loss. The main contribution of this paper is to summarize the presented literature which, employs different mechanisms to protect the business from ransomware attacks, and revealing its strengths, weaknesses. Moreover, realizing the related challenges that confront with this kind of attack. Therefore, this work may be used as a starting point for future research. The pros and cons of the related work are summarized in table (1), (2).

Table (1) (Related Work Summary)

No.	Researcher/s	Contribution	Pros.	Cons.
1	Popli and Girdhar [1], 2018	Ran recent ransomware in a simulated environment and analyze their attack process	Make a prediction of future ransomware, its expected impact and how difficult it would be to detect if polymorphic, metamorphic techniques used.	They didn't suggest a specific solution to prevent or detect ransomware infection.
2	Rajput [6], 2017	Studied the characteristic of ransomware families and its evolution	He shows that many Ransomware families exhibit similar characteristics.	They didn't suggest a specific solution to prevent the ransomware infection.
3	Zimba and Chishimba [9], 2019	Suggested mitigation strategies utilizing the recommend best practices based on successful ransomware attacks campaigns	Availability of offline backup will mitigate the impact of ransomware infection	The system still vulnerable to a zero-day attack which, can break the system.
4	Goyal et al. [12], 2020	Detected crypto ransomware using a classification model	This paper demonstrates the limitation of signature-based detection methods, and emphasize the behavior-based detection mechanism capability to detect crypto ransomware.	Misclassification may happen due to decision boundary errors.
5	Grant and Parkinson [13], 2018	Proposed a file monitoring application	Identify the ransomware behavioral pattern	It just monitors interaction with files only in a "specific directory", not all user data.
6	Kok et al. [14]	Proposed a pre-encryption algorithm	The proposed LA algorithm has accomplished the prediction utilizing only API data to detect crypto ransomware.	The LA can only be implemented using a new dataset with API from the pre-encryption stage.
7	Scaife et al. [15], 2016	Proposed "CryptoDrop" an early warning detection system	It can halt a suspicious process.	- Does not inspect files outside of the user documents directory. - Needs user interaction. - 40 files could be encrypted before it can detect suspicious activity.
8	Continella et al. [17], 2016	Proposed "ShieldFS" detection system	No file encrypted by ransomware	Creating the reflected files and redirecting the write requests to the protected area are the main reasons for performance hit under high workloads.
9	Kharraz and Kirda [18], 2017	Proposed "Redemption " detection system		

10	Winter et al. [19], 2018	Started a cyber-autoimmune disease	Emphasize that technology is not evolving as fast as the complexity of threats.	There is no specific solution proposed other than requesting anti-virus companies to update their inefficient methods and techniques.
11	Lika et al. [20], 2018	Proposed cyberattack prevention through awareness via gamification	Educate users to increase their awareness in an interactive manner	- They didn't suggest a specific solution to prevent or detect ransomware infection. - They just confirmed the efficiency of using the "perfc" file to avoid "NotPetya" ransomware.
12	Zimba et al. [21], 2018	Studied the emerging cyber threat to the critical infrastructure	Uncovered the WannaCry employed techniques to discover vulnerable nodes.	The discovered network interactions adopted only by WannaCry ransomware.
13	Zimba and Mulenga [22], 2018	Employed reverse engineering on the underlying malware program logic	Unmasked WannaCry ransomware network interactions	

Table (2) (Related Work Summary)

No.	Researcher/s	Contribution	Pros.	Cons.
1	Almashhadani et al. [23], 2019	Proposed a multi-classifier network-based ransomware detection.	Implemented a network-based intrusion detection system.	- The extracted network traffic is specified to "Locky" ransomware. - Not all ransomware families connect to command and control servers such as "win-locker" for example.
2	Akbanov et al. [24]	Accomplished extensive dynamic analysis on WannaCry ransomware	The results of this research can help to accomplish an efficient mitigation mechanism against WannaCry	The uncovered network attitude is utilized by WannaCry ransomware only.
3	Hull et al. [25], 2019	Proposed Randep a predictive model for categorizing ransomware according to its behavioral characteristics.	It can be used for improving detection and handling of ransomware incidents.	Not all ransomware families go through all these deployment stages.
4	Chen and Bridges [26], 2018	Presented a method to automatically extract distinguishing features of malware from host logs.	- It can be used to improve ransomware detection and make it more robust to polymorphism.	They didn't suggest a specific solution to prevent or detect ransomware infection.
5	Verma et al. [27], 2018	Implemented an automated system using supervised machine learning classifiers to classify the ransomware samples.	Classifying the ransomware variants in the real-time environment.	- Misclassification due to decision boundary errors. - Some ransomware has limited file system activity. Though, a few user files may be encrypted.
6	Ami et al. [28], 2019	Adopted authentication-based access control mechanism.	It can halt file modification attempts such as renames or deletions.	Users may grant access to a process which, is infected with a malicious code.
7	Christopher and Kumar [29], 2019	Presented a preventative technique based on ransomware behavior.	Alter access control levels of files and folders to revoke ACL writing privileges when compromise confirmed.	The system will suffer from a lot of strain when the monitoring is done on physical drives instead of artificial drives.
8	Lee et al. [30], 2017	Provided a new technique to recover from a ransomware attack using key backup.	The recovered key used for file recovery after ransomware infects the system and encrypt user files.	- Not all ransomware uses the CNG library such as "Cryptolocker"

				- Not all ransomware obtains the key from the server like "Ordinypt" and "Petya". - Monitoring the outbound communication can be easily avoided by encrypting these connections.
9	Zimba et al. [31], 2019	Categorized ransomware based on data deletion and file encryption attack structures.	This framework helps to uncover ransomware design flaws in order to exploiting them in data recovery, via system volume shadow copies or third-party software without paying the ransom.	Some ransomware has an irreversible impact, for example, no actual solution could be used to decrypt the encrypted hard disks by NotPetya.
10	Zimba et al. [32], 2018	Evaluated the underlying ransomware attack structures and data deletion techniques.	Its concluded that the key to data recovery options lies in, uncovering the underlying of attack structure and the implemented data deletion methodology.	
11	Gómez-Hernández et al. [33], 2018	Proposed a general methodology called R-Locker to thwart crypto ransomware actions.	The proposed methodology eliminates the ransomware when it accesses a trap file, thus allowing to preserve the rest of the data.	- just a part of the complete file system is protected. - the poor distribution of the traps can reduce the efficiency of data protection. - this defense can be passed over by the removal of the central trap file. - it can be partially bypassed by accessing given folder files by ransomware in a random way where all files in the folder may be encrypted before the sample can be blocked.
12	Wang et al. [34], 2018	Utilized cyber deception technology by trapping attackers.	- This approach helps to Protect important hosts under targeted ransomware attacks. - Utilized NLP and machine learning to trace-back RDP-based ransomware attacks and identify the original attack sources.	This approach is just for hindering RDP-based ransomware attacks only.
13	Shaukat and Ribeiro [35], 2018	Presented "RansomWall", a layered defense system for protection against cryptographic ransomware.	When the trap layer suspects a process as malicious, the modified files are backed up until it is classified as ransomware or benign by the "machine learning layer".	- User critical files may be attacked earlier than honey files. - Some ransomware has limited file system activity. Though, a few user files may be encrypted. - Another misclassification is due to decision boundary errors.

4. CONCLUSION

With the existence of ransomware as a service (RaaS) which, facilitates obtaining ransomware codes easily. In addition to the availability of free development kits, such as "Torlocker, TOX and Hidden-Tear" which, are available for unskilled individuals. This greatly reduces the entry barrier of ransomware remunerative business, and its activities are only expected to be on the rise and users should brace themselves against such attacks.

The more critical the data, the more likely the victim is to pay the ransom. Reversing ransomware encryption is quite difficult and consumes time and resources. Even though, employing techniques such as reverse engineering and cryptanalysis will contribute considerably to ransomware attacks declining. These techniques will make it possible for victims to regain access to their files without paying the ransom.

Moreover, approaches to prevent ransomware and protect devices are necessary. But ransomware developers will soon adapt to the current detection tools and new families with different behavior will spread.

5. FUTURE WORK

In the future, this work will be extended by establishing an efficient hybrid approach that combines two or more techniques to prevent ransomware and make user data more resistant to ransomware. Also, the work can be extended to be the foundation to propose a ransomware prevention model.

6. REFERENCES

[1]. Popli N, Girdhar A. Behavioural Analysis of Recent Ransomware and Prediction of Future Attacks by Polymorphic and Metamorphic Ransomware. In Verma, Nishchal K, Ghosh, A. K. (eds) Computational Intelligence: Theories, Applications, and Future Directions - Volume II ICCI-2017. Springer, Singapore. 2018;799(4):65–80.

[2]. Caporusso N, Chea S, Abukhaled R. A game-theoretical model of ransomware. In: Proceedings - International Conference on Applied Human Factors and Ergonomics 2018 Jul 21 (pp. 69-78). Springer, Cham.

[3]. Morgan, Steve. "Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics." Cybercrime Magazine Cisco and Cybersecurity Ventures. 2019, https://www.cybersecurityventures.com/cybersecurity- a lmanac- 2019.

[4]. Maccari M, Polzonetti A, Sagratella M. Detection: Definition of New Model to Reveal Advanced Persistent Threat. InProceedings of the Future Technologies Conference 2018 Nov 15 (pp. 305-323). Springer, Cham.

[5]. Al-rimy B, Maarof M, Shaid S. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers and Security. 2018; 74:144-166.

[6]. Rajput T. Evolving Threat Agents: Ransomware and their Variants. International Journal of Computer Applications. 2017 April;164(7):28-34.

[7]. Kok S, Abdullah A, Jhanjhi N, Supramaniam M. Ransomware, Threat and Detection Techniques: A Review. IJCSNS International Journal of Computer Science and Network Security. 2019;19(2):136-146.

[8]. Tandon A, Nayyar A. A Comprehensive Survey on Ransomware Attack: A Growing Havoc Cyberthreat. InData Management, Analytics and Innovation 2019 (pp. 403-420). Springer, Singapore.

[9]. Zimba A, Chishimba M. On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems. European Journal for Security Research. 2019 January;4(1):3-31.

[10]. BBC-News 2019, *Baltimore ransomware attack: NSA faces questions*, BBC-News, viewed 28 December 2019, https://www.bbc.com/news/technology-48423954/

[11]. Wikipedia 2019, *WannaCry ransomware attack*, Wikipedia, viewed 28 December 2019, https://en.wikipedia.org/wiki/WannaCry_ransomware_attack/

[12]. Goyal, P.; Kakkar, A.; Vinod, G. & Joseph, G. Crypto-Ransomware Detection Using Behavioral Analysis *Reliability, Safety and Hazard Assessment for Risk-Based Technologies, Springer*, 2020, 239-251.

[13]. Grant L., Parkinson S. Identifying File Interaction Patterns in Ransomware Behavior. In: Parkinson S, Crampton A, Hill R. (eds) Guide to Vulnerability Analysis for Computer Networks and Systems. Springer, Cham. 2018;14:317-335.

[14]. Kok SH, Abdullah A, JhanJhi NZ, Supramaniam M. Prevention of Crypto-Ransomware Using a Pre-Encryption Detection Algorithm. Computers. 2019 Dec;8(4):79.

[15]. Scaife N, Carter H, Traynor P, Butler K. CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. In: Proceedings - International Conference on Distributed Computing Systems. 2016 August;2016:303-312.

[16]. Wolf J. "Ransomware Detection." Friedrich-Alexander-University Erlangen-Nuremberg. 2018.

[17]. Continella A, Guagnelli A, Zingaro G, Pasquale G, Barenghi A, Zanero S, Maggi F. ShieldFS: A Self-healing, Ransomware-aware Filesystem. In: Proceedings - Annual Computer Security Applications Conference (ACSAC). 2016 December:336-347.

[18]. Kharraz A, Kirda E. Redemption: Real-Time Protection Against Ransomware at End-Hosts. In: Dacier M, Bailey M, Polychronakis M, Antonakakis M. (eds) Research in Attacks, Intrusions, and Defenses. Springer. 2017;10453:98-119.

[19]. Winter R, Ruiz R, Army B, Archer R. Cyber Autoimmune Disease When the Virtual Life Imitates the Real Life. International Journal of Cyber-Security and Digital Forensics (IJCSDF).2018;7(1):21-30.

[20]. Lika R, Murugiah D, Brohi S, Ramasamy D. NotPetya: Cyber Attack Prevention through Awareness via Gamification. In: International Conference on Smart Computing and Electronic Enterprise (ICSCEE).2018:1-6.

[21]. Zimba A, Wang Z, Chen H. Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. ICT Express. 2018;4(1):14-18

[22]. Zimba A, Mulenga M. A Dive Into the Deep: Demystifying Wannacry Crypto-Ransomware Network

Attacks Via Digital Forensics. International Journal on Information Technologies & Security. 2018;10:57-69.

[23]. Almashhadani A, Kaiiali M, Sezer S, O'Kane P. A Multi-Classifier Network-Based Crypto-Ransomware Detection System: A Case Study of Locky Ransomware. IEEE Access. 2019;7:47053-47067.

[24]. Akbanov M, Vassilakis VG, Logothetis MD. WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention, and Propagation Mechanisms. Journal of Telecommunications & Information Technology. 2019 Mar 1(1).

[25]. Hull G, John H, Arief B. Ransomware deployment methods and analysis: views from a predictive model and human responses. Crime Science. 2019 February;8(1)1:22.

[26]. Chen Q, Bridges R. Automated behavioral analysis of malware: A Case Study of Wannacry Ransomware. In: Proceedings - 16th IEEE International Conference on Machine Learning and Applications, (ICMLA) 2017. 2018 January:454-460.

[27]. Verma M, Kumarguru D, Deb S, Gupta A. Analyzing indicator of compromises for ransomware: Leveraging IOCs with machine learning techniques. IEEE International Conference on Intelligence and Security Informatics, (ISI). 2018:154-159

[28]. Ami O, Elovici Y, Hendler D. Ransomware prevention using application authentication-based file access control. In: The 33rd ACM/SIGAPP Symposium on Applied Computing. Pau, France. 2018 April:1610-1619.

[29]. Chew C, Kumar V. Behavior Based Ransomware Detection. In: Proceedings - 34th International Conference on Computers and Their Applications. 2019;58:127-116.

[30]. Lee K, Oh I, Yim K. Ransomware-prevention technique using key backup. Lecture Notes of the Institute for Computer Sciences, Social-Informatics, and Telecommunications Engineering (LNICST). 2017 August;194:105-114.

[31]. Zimba A, Wang Z, Chishimba M. Addressing Crypto-Ransomware Attacks: Before You Decide whether To-Pay or Not-To. Journal of Computer Information Systems. 2019 January;4417:1-11.

[32]. Zimba A, Wang Z, Simukonda L. Towards Data Resilience: The Analytical Case of Crypto-Ransomware Data Recovery Techniques. International Journal of Information Technology and Computer Science. 2018 January;10(1):40-51.

[33]. Gómez-Hernández J, Álvarez-González L, García-Teodoro P. R-Locker: Thwarting ransomware action through a honey-file-based approach. Computers & Security. 2018;73:389-398.

[34]. Wang Z, Cui X, Su S, Qiu J, Liu C, Tian Z. Automatically Traceback RDP-Based Targeted Ransomware Attacks. Wireless Communications and Mobile Computing. 2018;2018:1-13.

[35]. Shaukat S, Ribeiro V. RansomWall: A Layered Defense System against Cryptographic Ransomware Attacks using Machine Learning. In: Proceedings - 10th International Conference on Communication Systems & Networks (COMSNETS). 2018:356-363.

View publication stats