The Rise of Ransomware: A Review of Attacks, Detection Techniques, and Future Challenges

[1]Samar Kamil
Department of Computer Science and Information Systems,
Al-Mansour University College
Baghdad, Iraq
Samarkamil2021@yahoo.com

[2]Siti Norul, Huda Sheikh Abdullah
Center for Cyber Security, Faculty of Information Science & Technology,
Universiti Kebangsaan Malaysia
Bangi, Malaysia
snhsabdullah@ukm.edu.my

[3]Ahmad Firdaus
Faculty of Computing, College of Computing and Applied Sciences,
University Malaysia Pahang, Pekan, Pahang Darul
makmurfirdausza@ump.edu.my

[4]Opeyemi Lateef Usman
Department of Computer Science, Tai Solarin University of Education,
Ogun State, Nigeria
usmanol@tasued.edu.ng

2022 International Conference on Business Analytics for Technology and Security (ICBATS) | 978-1-6654-0920-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICBATS54253.2022.9759000

***Abstract*— Cybersecurity is important in the field of information technology. One most recent pressing issue is information security. When we think of cybersecurity, the first thing that comes to mind is cyber-attacks, which are on the rise, such as *Ransomware*. Various governments and businesses take a variety of measures to combat cybercrime. People are still concerned about ransomware, despite numerous cybersecurity precautions. In ransomware, the attacker encrypts the victim's files/data and demands payment to unlock the data. Cybersecurity is a collection of tools, regulations, security guards, security ideas, guidelines, risk management, activities, training, insurance, best practices, and technology used to secure the cyber environment, organization, and user assets. This paper analyses ransomware attacks, techniques for dealing with these attacks, and future challenges.**

Keywords—cybersecurity, cyber-attacks, security, Ransomware

I. INTRODUCTION

The Internet is currently the fastest-growing infrastructure. In today's technological world, many modern technologies are changing the face of human activities. However, we cannot adequately protect our personal information due to these emerging innovations, and cybercrime is becoming more prevalent by the day. Today, more than 60% of all business transactions are conducted online. Hence, ensuring transparency and the highest level of security is a major problem.Consequently, cybersecurity has become a major concern. The scope of cyber security includes protecting information in the IT sector and many other areas such as cyberspace [1][2].

This work was supported by Ministry of Higher Education, Malaysia under research LRGS-1-2019-UKM-UKM-2-7.

According to Brewer [3] the term "***ransomware***" is derived from the words "*ransom*" and "*malware*". It is a significant factor contributing to the rise in cyber-attacks that include the ability to profit from victims. Meanwhile, Noubir believes that cybercriminals had a difficult time profiting from attacks in the past, but that has changed. Ransomware attacks, or attackers who gain access to a victim's data, encrypt it, and demand a ransom, are becoming increasingly popular among cybercriminals [4]. Ransomware refers to a type of virus that demands payment for a hacked service. The most common ransomware heavily employs file encryption as a method of extortion. They essentially encrypt data on victims' hard drives before demanding a ransom to unlock them [3]. According to Richardson and North [19], Ransomware is a growing threat to personal and corporate data files. It encrypts data on an infected machine and keeps the secret key to decrypt the contents until the victim pays compensation. Every year, this virus causes damage worth hundreds of millions of Dollars. Consequent upon the large sums of money that must be paid, new versions emerge on a regular basis. This enables the avoidance of security software and other intrusion prevention techniques [5].

Ransomware has been one of the most significant cyber frauds that have affected businesses in recent years. Indeed, the FBI predicts that ransomware will cause $1 billion in damages in 2016. Ransomware is a type of malicious software that allows a hacker to restrict access to vital information of a person or business and then demand payment to remove the restriction. Encrypting critical data on a computer or network is the most common type of restriction nowadays. It primarily allows the attacker to keep user data or a system backup [6].

Therefore, the objective of this study is to conduct a review of phases of critical ransomware attacks, discuss some techniques for dealing with them, and highlight future challenges.

II. PHASES AND TECHNIQUES OF RANSOMWARE

A ransomware attack occurs in stages, depending on whether it is a mass deployment or a targeted attack. Recognizing and comprehending what happens at each stage, as well as the compromise indicators (IOC) to be identified, increases the likelihood of successfully defending against or at least mitigating an attack. [7]. The phases and techniques of ransomware attacks are summarized below:

1. *Exploitation and infection:* For this phase to be successful, the dangerous ransomware must be executed on a machine. This is frequently accomplished through an infected email or vulnerabilities, a toolkit for the exploitation of security vulnerabilities for malware spread in software programs. These kits are designed for

978-1-6654-0920-9/22/$31.00 ©2022 IEEE

people who use unsafe or outdated software on their computers [7].

2. *Delivery and execution:* Following the exploit procedure, the actual ransomware program is sent to the victim's PC in this phase. After execution, persistence mechanisms are implemented. In general, this procedure takes a few seconds depending on network latencies. Regrettably, executables are frequently sent over an encrypted channel - a customized encryption layer over a standard HTTP access is provided in place of SSL. Because malware employs strong encryption, obtaining the executable from the wire is impossible. We usually find executable files under the user profile in the %APPDATA% or %TEMP% folders. This should be known to detect because the organization can monitor the development of a defense line for these occurrences. Most virus encryption methods include persistence methods, so if the affected computer is restarted during the encryption process, the ransomware may resume where it left off and continue to encrypt the system until it is finished [7]. Fig.1 illustrates the transaction that is associated with the ransomware attack.

Fig. 1. Ransomware Attack [8]

3. *Backup spoliation:* Ransomware targets and deletes backup files and folders from the system shortly after the virus is run to hinder backup restoration. Other types of malware, including APTs, do not bother deleting backup files. The majority of ransomware versions will try to eliminate any way for the victim to recover without paying the ransom.

4. *Encryption of File:* When the backups are properly deleted, the malware communicates with the command and monitor servers to perform a secure key exchange and establish the encryption keys used by the local machine. The virus typically tags the system with a unique identification number, which the user will find in the application's instructions. In this manner, the C2 server distinguishes between the encryption keys used by various victims. Regrettably, most versions now use strong encryption, such as AES256, so the victim cannot independently crack the encryption [7].

5. *Notification to user and clean-up:* After the backup files are deleted and the encryption operation is completed, the demand specifications for recovery and payment are sent. Normally, the victim is given a few days to pay, after which the ransom increases [7].

III. MAJOR RANSOMWARE ATTACKS AND SOFTWARES

The first ransomware attack was claimed to have used an AIDS Trojan program in 1989 [8]. In Russia in 2005, only a few cases were reported. Following 2005, ransomware evolved and spread by utilizing various social engineering methods to cover user data with sophisticated encryption techniques. In 2013, a significant increase in ansomware attack was observed, particularly after introducing CryptoLocker ransomware. CryptoLocker is rapidly spreading and infecting both personal and public devices and networks. A few months later (when Cryptolocker was introduced), it caused $27 million in ransom money damages [10]. According to the information on CryptoWall website, hackers made more than $18 million from April 2014 to June 2015 by releasing new ransomware software known as CryptoWall [11]. The statistics provided by US government agencies further stated that Cryptolocker affected 4,593 computers in the United Kingdom, 336,856 computers in the United States, 25,841 computers in Canada, 1,832 computers in India, 15,427 computers in Australia, and 100,448 computers in other countries of the world as at 2014. In summary, CryptoLocker infects approximately 50,000 PCs per month [12].

Dridex, a Financial Trojan, was one of the most severe and dangerous cyber threats consumers and businesses faced in 2015. Dridex steals credentials and data from over 300 banks and other organizations in over 40 countries during online banking transactions. Dridex appears to be one of the most significant financial risks in 2016 [13]. Dridex is typically distributed via phishing emails and infected files, and it can inject itself into the three most popular internet browsers on Windows OS. Windows-based web browsers are affected when accessing online back computers (during a live bank session) [13]. The number of ransomware victims increased by 3,500% in the first-quarter of 2016 compared to the fourth-quarter of 2015 [8]. According to CNN News, $209 million was paid during the first few months of 2016.

The WannaCry ransomware attack in 2017 was the world's most severe cyberattack. WannaCry Ransomware is malicious software that restricts access to users' files or systems, encrypts data or entire systems, and holds the victim hostage until the victim pays the ransom for a decryption key that allows the user to access programs encrypted files or systems. It may be challenging to think. The first Ransomware in history was created in 1989 (33 years ago). It was dubbed the "Trojan Horse of AIDS", but it now appears primitive. This is distributed on diskettes, and $189 was sent to a post office box in Panama to pay a ransom. There are several types of Ransomware, such as Reveton, CryptoLocker.F, CryptoLocker, and TorrentLocker. With over 2,000 victims, the ransomware Wannacry targeted hospitals, businesses, colleges, and government

organizations in 150 institutions. All machines were locked, and ransom was demanded [9].

IV. RANSOMWARE ATTACKS DETECTION METHODS

Despite the fact that the WannaCry outbreak marks the beginning of a new era of ransomware. Critical information systems are breaking down, wreaking havoc on civilization. Cybercriminals who control traffic control or medical care systems are terrified of bombs and missiles. The dynamic analysis process, file system, registry, and network activities are all investigated in this study. This interactive behavioral analysis promotes cybersecurity integration by gathering massive volumes of malware signals and increasing the system's malware information exchange. Multidimensional collaboration in connecting threat information is necessary to prevent complex malware attacks. The usage of malware database synchronization protects against new ransomware generation [14]. Despite the fact that the WannaCry attack ushers in a new era of ransomware. Critical information systems are failing, causing massive damage to civilization. Cyber thieves who take over the traffic control or medical care systems are scared of nothing less than bombs and missiles. This study examines the dynamic analyzing process, file system, registry, and network activity. This interactive behavioral analysis aids cybersecurity integration by collecting large amounts of malware signals and improving the system's malware information exchange. To prevent sophisticated malware attacks, multidimensional collaboration in connecting information about threats is required. The use of malware database synchronisation protects against ongoing ransomware development [14], [31].

Based on research into the ransomware ecosystem, Mercaldo et al. [15] discovered that the phenomenon of cybercriminals increasingly using bitcoin for payments provides an opportunity to obtain valuable information about these organizations' financial operations. They developed a set of measuring methods that they used in a two-year end-to-end study of the ransomware environment in the United Kingdom. They were able to trace ransom payments from the point where victims purchased bitcoins to the point where ransomware attackers cashed out cryptocurrencies using bitcoins techniques. They were able to estimate the total ecosystem income over the last two years, which they believe to be in excess of $16 million USD, extorted from somewhere in the neighbourhood of 20,000 victims. Their subsequent investigation into ransomware operators' cash-out methods revealed that BTCe was a critical piece of infrastructure required to convert millions of dollars in stolen bitcoins into fiat money. As a result of their investigation, they discovered numerous unresolved technical and ethical issues related to monitoring and acting in the ransomware environment. These include transaction filtering, timing analysis, and cluster coverage [15].

Ransomware has become the focus of many cyber-criminals who are rapidly evolving, owing to the monetary benefits obtained. Therefore, it is critical to address novel variations of existing and new families. Mohurle and Patil [16] demonstrated that Machine Learning is a feasible and successful method for detecting new ransomware variants and families for subsequent analysis and signature extraction, as well as for an AV supplement. Mutual data has proven to be a useful method for selecting features automatically, whereas Regularized Logistical Regression has proven to be an accurate, easy-to-train, and fast algorithm. In terms of outcomes, it compete favourably with more advanced algorithms and produced significantly better results than more naive methods [16].

Significant advancements in advanced technology have paved the way for a new computing paradigm in the Internet of Things. O'Brien [17] conducted research on IoT ransomware attacks and security issues. First, they addressed the rise in ransomware attacks and investigated the challenges associated with them. Second, cutting-edge research efforts on IoT security have been examined, documented, and highlighted. Third, the classification and categorization of the literature results in the development of a taxonomy. Fourth, a number of realistic cases are presented in order to warn consumers about the vulnerability of IoT devices to attacks. Fifth, they have outlined the requirements for IoT security. The sixth step is to identify and discuss some critical research problems. Seventh, there are numerous important research avenues. Finally, they conclude that, while IoT may make many aspects of people's lives easier [32], the majority of IoT devices are vulnerable to ransomware attacks. Therefore, it is critical to improve IoT security and mitigate ransomware attacks in order to increase user confidence in the IoT system [17]. Given the massive increase in IoT devices and the massive data they collect [12], Ransomware attacks have become a possibility. Although they are not used to store user data and documents, locker-ransomware attacks can cause significant damage by preventing access to monitoring systems, causing power outages, or causing severe industrial disruptions. Android.Lockdroid.E [18] is an example of IoT-based Ransomware that locks smart TVs.

Richardson and North [19] proposed a two-fold approach. To begin, they propose the development of a ransomware attack model based on data from both static and dynamic analytic analyses in order to ensure a thorough understanding of ransomware infection and attack patterns. To the best of their knowledge, none of the previous researchers used this technique. They also suggested that a hybrid algorithm be used instead of just one method. The reason for this is that the component algorithms may complement one another in such a way that the hybrid algorithm outperforms the theory of the separate method.

Richardson and North [19] further developed a method for automatically removing malware characteristics from host logs. The tests made use of the relatively new and potent WannaCry Ransomware. They used behavior logs from Cuckoo Sandbox analytical reports under various normal and malware activity scenarios as experimental evidence. The experimental results confirmed that the approach can extract malware characteristics from logs containing most non-malicious events and that it is polymorphism resistant. Most importantly, given the large volume of ambient logs containing ransomware activity, numerous ransomware characteristics are automatically extracted with high accuracy. They have also discovered and demonstrated experimentally, how misleading malware indicators can be derived from the technique in order to extract non-malware characteristics in the malicious document, which is very unusual. This situation can be easily avoided by using dynamic analysis to create patterns. The next step will be to

investigate the testing of malware analysis and the creation of a pattern on environmental logs gathered by operations [19].

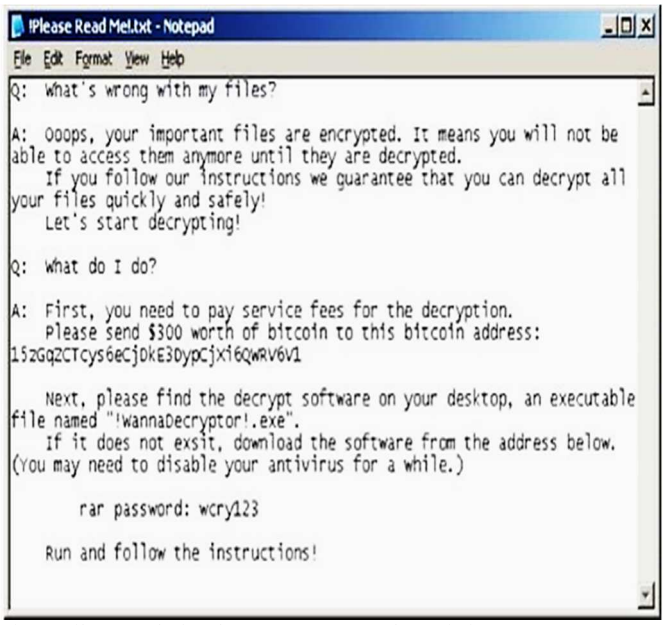

Fig. 2. File created after the ransomware attack on victim's PC [20]

Fig.2 shows a typical example of files created on victim's PC during and after ransomware attacks. In some ways, ransomware is similar to other types of viruses, but in others, it is distinct. For example, ransomware typically performs a large number of file-related actions in order to lock or encrypt files on a victim's computer in a short period. Malware detections based on signatures, which have difficulty detecting zero-day Ransomware, are insufficient for protecting user data from dangerous unknown attacks. A new security method specializing in ransomware and focused on ransomware-specific activities is thus required to distinguish Ransomware from other types of malware and innocuous files. The research by Bae et al. [2] provides a ransomware technique for detecting ransomware and benign files, as well as viruses and ransomware. According to experimental data conducted by Scaife et al. [21], the proposed approach can detect ransomware in both malware and benign files.

V. Ransomware Prevention Tools

A. CryptoDrop

CryptoDrop is an anti-ransomware tool that detects and removes ransomware while also assisting in recovering affected files [23-24]. It includes many synchronous calls, debugging, verbose logging, and other performance-degrading features. Compiler optimizations had been deactivated throughout the tests to ensure proper operation and support debugging. They tracked the code during protected file changes and discovered that this CryptoDrop version had overhead latencies for open and read files of less than 1ms. Closing procedures now have an average delay of 1.58ms. Writing and renaming operations are the most expensive, with additional delays of 9ms and 16ms. Because CryptoDrop does not examine files outside the user's documents directory, other files (including your own) are not impacted by the operating system and application access [24].

According to Yorkdale [25], ransomware continues to infect suspicious victims due to its strong encryption. Victims often have no choice but to pay the ransom, which encourages attackers to build a dynamic economy that allows them to quickly deploy new versions. In this paper, researchers limit attackers to CryptoDrop, an early warning system for ransomware attacks, and reduce victims' motivation to pay. The approach is designed to combat ransomware by tracking the victim's data and identifying the behaviors. Researchers first identify the necessary transactions, then categorize ransomware attacks into three major groups. Finally, indicators are created to check, collect, and notify ransomware products while preventing harmless uses. They discovered that ransomware frequently employs all three main indicators, whereas genuine programs do not provide a shortcut for detecting ransomware with less data loss [26-32]. The CryptoDrop studies look at 492 real-world ransomware strains and discover a 100% detection rate with no victim data destroyed before detection. The burden of paying ransomware victims is reduced or eliminated with fewer deleted files, protecting users while destroying the attacker's economy [22].

B. PayBreak

PayBreak is a new security method that addresses the issue of crypto-based ransomware. It is currently in beta testing stage. Previous ransomware variants failed due to the malware's designers' incorrect use of cryptographic capabilities. Families who were successful in making the transition to using the proper cryptographic technique are hybrid encryption. Researchers discover that to perform file encryption on the victim's host, the symmetric session keys must be used on the host. To that end, PayBreak offers a key escrow system that stores session keys in a key vault on the PayBreak server. Because the keys in the vault are encrypted with the user's public key, only the user's private key can be used to unlock the vault and decrypt the keys. PayBreak, rather than relying on government-mandated key escrow systems, ensures that only authorized users have access to keys held in escrow on their behalf. PayBreak was tested using 107 ransomware samples, and the results show that PayBreak can effectively recover from the damage inflicted by twelve different ransomware families. Furthermore, PayBreak's operational cost is much lower than the human perception threshold, allowing it to be used on production systems without sacrificing performance. Finally, PayBreak will be available to the general public as a free and open-source project.

VI. Visual Analytics of Bitcoin Heist Dataset

This section provides insights into the Bitcoin dataset encompassing six features (income, neighbors, weight, length, count, and loop) [30]. The detail of each feature is as follows:

1. Income: the total amount of coins output
2. Neighbors: the number of transactions
3. Weight: sum of the fraction of coins that originate from a starter transaction.
4. Length: is the number of a non-starter transactions on its longest chain
5. Count: number of server transactions that are connected through a chain.
6. Loop: number of starter transactions that are connected with more than one directed path

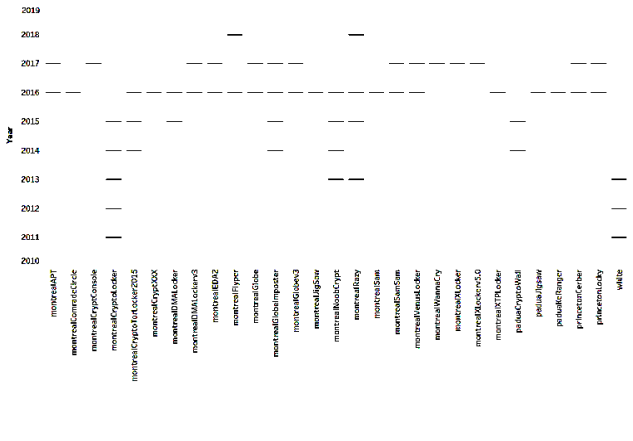

Fig. 3. Occurrences of each ransomware according to year

Fig. 3 shows that Wannacry ransomware only appeared in 2017, instead of the rest of the years. Similarly, Flyper and Razy were appeared in one year only, which was in 2018. However, in 2016, most ransomware families participated in the event. This demonstrates that 2016 is the beginning of the ransomware attack and the existence of a new family of ransomware in the following year.

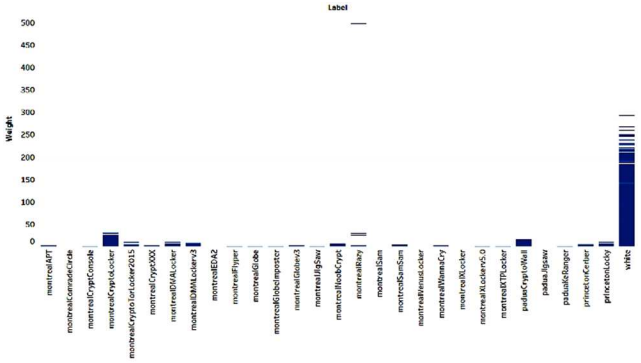

Fig. 4. Weight of each Ransomware

Fig. 4 above exhibits the weight of the ransomware, including the white label (none ransomware). This figure shows the trend white's weight shows a significant gap between all the ransomware families, and this demonstrates that this weight feature is the suitable feature to differentiate between ransomware and none ransomware.

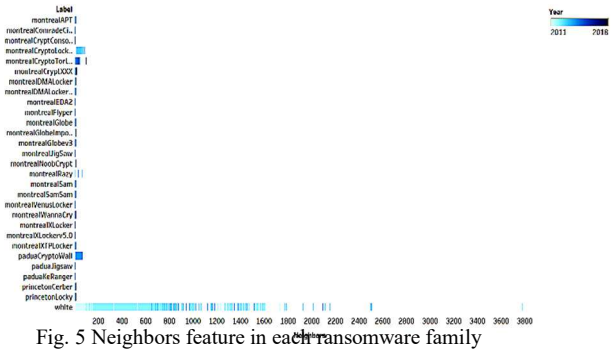

Fig. 5 Neighbors feature in each ransomware family

Another significant feature is neighbors, which shows a significant gap between white and ransomware families as indicated in Fig. 5. However, compared to Fig. 6 below, both count and looped features show similar trends between white and ransomware families, which is unsuitable features to apply for classification investigation.

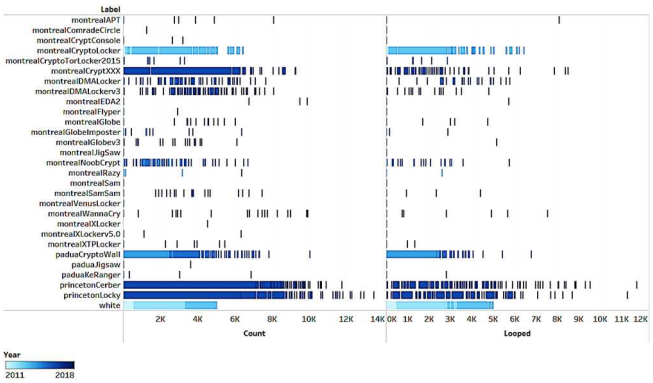

Fig. 6 Count and looped features according to ransomware families

In a nutshell, we can conclude from the visual analytics of the Bitcoin Heist dataset that 2016 is the year for Ransomware to begin and will increase in the near future. Furthermore, weight and neighbours are suitable features for distinguishing between white (none ransomware) and ransomware [30-35].

Using BitCoinHeistData from [30], just 3,000 out of 1.04 million data points from 2011 to 2018 were utilized.We performed some preliminary experiments on ransomware features comprising of address, year, day, length, weight, count, looped, neighbors, and income to detect twelve ransomware classes using several classifiers in WEKA Tools, namely J48, Random Forest, Decision Table, and Deep Learning based on 10-fold cross-validation. The class labels of ransomware are princetonCerber, princetonLocky, montrealCryptoLocker,montrealCryptXXX,paduaCryptoWall,montrealWannaCry,montrealDMALockerv3,montrealCryptoTorLocker2015,montrealSamSam,montrealFlyper,montrealNoobCrypt and montrealDMALocker. Based on Table 1, we observed that all nine features are more important for classifying the ransomware-type than selected features defined by CfsSubsetEval.

TABLE 1. Preliminary Accuracy Results of BitCoinHeistData in Montreal using J48, Random Forest, Decision Table and Deep Learning4j Classifiers before and after feature selection.

CV-10	J48	Random Forest	Decision Table	Deep Learning4j
Before FS\	96.43%	93.8%	91.2%	80.16%
After FS - CfsSubsetEval	86.16%	62.15%	86.4%	80.03%

VII. INDIVIDUAL REFLECTION AND FUTURE CHALLENGES

As long as infected consumers are willing to pay for their ransomed data, the ransomware industry will grow even stronger, seeking new and creative ways to circumvent traditional preventative mechanisms. Consider the following anticipated developments in order to highlight the continued advancements of the ransomware industry:

1 One issue is that simply resetting IoT devices may not be effective in many cases because hacked

devices may leave the user with no choice but to pay the ransom. In order to combat this problem, researchers must develop methods for the early detection of ransomware. Furthermore, IoT device developers should provide a list of data file extensions that are safe to use within the IoT networking environment.

2 Because IoT networks are so diverse, implementing a unified security strategy is difficult. To completely protect IoT devices from a ransomware attack, ransomware mitigation capabilities must be integrated throughout the entire lifetime of application execution[36-44].

3 Some attackers target backup systems with network-connected. A backup is a viable option when it comes to recovering data rather than paying a ransom, but the backup must be recent. Because some attackers target the linked backup system as well, it is preferable to use the services of a reputable cloud service provider for backup to deal with this issue effectively. Another solution to the data backup problem is to keep multiple backups of data and keep them safe from prying eyes [14].

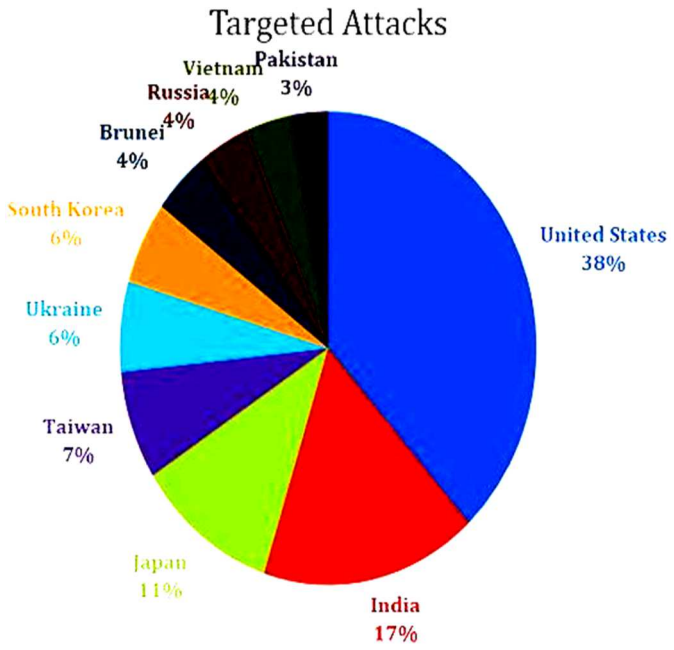

Fig.7. Targeted ransomware attacks [26].

4 Criminals send out fraudulent emails and links for advertising purposes, and new users are sometimes drawn in by these adverts and click on the link [26]. To address this issue, businesses should educate their employees on identifying and using reputable websites. Furthermore, security should be integrated into IoT to alert the user when necessary. The spread of ransomware across the network is one of the most difficult aspects of dealing with it. Organizations should limit user privileges to protect data security; additionally, malicious nodes should be discovered as soon as possible to prevent the network from being harmed. Once detected, the infected computer should be turned off as soon as possible [26-30].

VIII. Conclusion

The world's current expansion and progress are in sync with technological innovation and advancement. Aside from people and businesses, this advancement has introduced the possibility of threat and open hazards for technology. Ransomware is one of the most powerful sources in this category, as it has the ability to cause significant disruption in companies, people, and technological development. According to recent studies [33], there has been a significant increase in the number of ransomware victims worldwide, with the majority of victims hailing from advanced nations, specifically the United States. Each year, the number of ransomware variants increases exponentially, and it is necessary to distinguish ransomware from other types of malware to protect users' computers from ransomware-based attacks. Cybersecurity seeks to ensure that the company's security characteristics and user assets are achieved and maintained in the cyber environment against appropriate security threats. This report examines the domain of ransomware attacks as well as tools that can be used to prevent them. Several techniques have been developed, but attackers continue to find new ways to use cutting-edge technology to attack the victim. Therefore, there are never-ending challenges in dealing with ransomware to avoid such attacks in the future.

Acknowledgment

Ministry of Higher Education supported this work, Malaysia under research LRGS-1-2019-UKM-UKM-2-7.

References

[1] Al-rimy, B.A.S., Maarof, M.A. and Shaid, S.Z.M.,"Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions, " *Computers & Security*, *74*, 2018,pp.144-166.

[2] Bae, S.I., Lee, G.B. and Im, E.G., "Ransomware detection using machine learning algorithms. *Concurrency and Computation: Practice and Experience*, "*32*(18),2020, p.e5422.

[3] Brewer, R., 2016. Ransomware attacks: detection, prevention, and cure. *Network Security*, 2016(9), pp.5-9.

[4] Burnham, K., "*Emerging Trends in Cybersecurity*. [online] Northeastern University Graduate Programs, "2021 Available at: <https://www.northeastern.edu/graduate/blog/trends-in-cybersecurity/> [Accessed 12 July 2021].

[5] Chen, Q., and Bridges, R.A., "Automated behavioral analysis of malware: A case study of wannacry ransomware, " In *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)* , 2017, (pp. 454-460). IEEE.

[6] Choi, K.S., Scott, T.M. and LeClair, D.P., "Ransomware against police: diagnosis of risk factors via application of cyber-routine activities theory, " *International Journal of Forensic Science & Pathology*, 2016.

[7] Gazet, A., "Comparative analysis of various ransomware virii. *Journal in Computer Virology*, "6(1), 2008,pp.77-90.

[8] Hampton, N. and Baig, Z.A., 2015 Ransomware: Emergence of the cyber-extortion menace.

[9] Huang, D.Y., Aliapoulios, M.M., Li, V.G., Invernizzi, L., Bursztein, E., McRoberts, K., Levin, J., Levchenko, K., Snoeren, A.C. and McCoy, D., 2018, May. "Tracking Ransomware end-to-end. In *2018 IEEE Symposium on Security and Privacy (SP)* (pp. 618-631). IEEE.

[10] Humayun, M., Jhanjhi, N.Z., Alsayat, A. and Ponnusamy, V., 2021. "Internet of things and Ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*, *22*(1), pp.105-117.

[11] Kao, D.Y. and Hsiao, S.C., 2018, February. "The dynamic analysis of WannaCry ransomware. In *2018 20th International conference on advanced communication technology (ICACT)* (pp. 159-166). IEEE.

[12] Karkouch, A., Mousannif, H., Al Moatassime, H. and Noel, T., 2016. "Data quality in internet of things: A state-of-the-art survey. *Journal of Network and Computer Applications*, *73*, pp.57-81.

[13] Kok, S., Abdullah, A., Jhanjhi, N. and Supramaniam, M., 2019. "Ransomware, threat and detection techniques: A review. *International Journal of Computer Science and Network Security*, *19*(2), p.136.

[14] Kolodenker, E., Koch, W., Stringhini, G. and Egele, M., 2017, April. "Paybreak: Defense against cryptographic Ransomware. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security* (pp. 599-611).

[15] Mercaldo, F., Nardone, V., Santone, A. and Visaggio, C.A., 2016, June. "Ransomware steals your phone. formal methods rescue it. In *International Conference on Formal Techniques for Distributed Objects, Components, and Systems* (pp. 212-221). Springer, Cham.

[16] Mohurle, S. and Patil, M., 2017. "A brief study of Wannacry Threat: Ransomware Attack 2017. *International Journal of Advanced Research in Computer Science*, 8(5), pp.1938-1940.

[17] O'Brien, D., 2016. "Dridex: Tidal waves of spam pushing dangerous financial trojan. *Symantec Corporation*.

[18] Reddy, G. And Reddy, G., 2014. "A Study Of Cyber Security Challenges And Its Emergning Trends On Latest Technologies. *Arxiv Preprint Arxiv:1402.1842.*,.

[19] Richardson, R. and North, M., 2017. Ransomware: Evolution, Mitigation and Prevention. *International Management Review*, 13(1), pp.10-21.

[20] Rubenking, N., 2018. "*CryptoDrop Anti-Ransomware*. [online] PCMag India. Available at: <https://in.pcmag.com/software/120247/cryptodrop-anti-ransomware> [Accessed 12 July 2021].

[21] Scaife, N., Carter, H., Traynor, P. and Butler, K., 2016. "*CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data*". [online] Ieeexplore.ieee.org. Available at: <https://ieeexplore.ieee.org/document/7536529> [Accessed 12 July 2021].

[22] Sgandurra, D., Muñoz-González, L., Mohsen, R. and Lupu, E.C., "Automated dynamic analysis of ransomware: Benefits, limitations and use for detection , " 2016, *arXiv preprint arXiv:1609.03020*.

[23] von Solms, R. and van Niekerk, J.,From information security to cyber security, "*Computers & Security*, 38, 2013, pp.97-102.

[24] Yaqoob, I., Ahmed, E., ur Rehman, M.H., Ahmed, A.I.A., Al-garadi, M.A., Imran, M. and Guizani, M., "The rise of ransomware and emerging security challenges in the Internet of Things, " *Computer Networks*, *129*, 2017, pp.444-458.

[25] Yorkdale, G., 2015. "Criminals Continue to Defraud and Extort Fund s from Victims Using CryptoWall Ransomware Schemes. *Federal Bureau o f Investigation*.

[26] Zakaria, W.Z.A., Abdollah, M.F., Mohd, O. and Ariffin, A.F.M., The rise of Ransomware, " In *Proceedings of the 2017 International Conference on Software and e-Business* (pp. 66-70)

[27] .Amanlou, Sanaz, Mohammad Kamrul Hasan, and Khairul Azmi Abu Bakar. "Lightweight and secure authentication scheme for IoT network based on publish–subscribe fog computing model." *Computer Networks* 199 (2021): 108465.

[28] Hasan, Mohammad Kamrul, et al. "Lightweight Cryptographic Algorithms for Guessing Attack Protection in Complex Internet of Things Applications." *Complexity* 2021 (2021).

[29] Hasan, Mohammad Kamrul, et al. "Lightweight encryption technique to enhance medical image security on internet of medical things applications." *IEEE Access* 9 (2021): 47731-47742.

[30] Akcora, Cuneyt Gurcan, et al. "BitcoinHeist: Topological data analysis for ransomware detection on the bitcoin blockchain." *arXiv preprint arXiv:1906.07852*,2019.

[31] A. Zafar and T. Rahim Soomro, "An Efficient Mining Based Approach Using PSO Selection Technique For Analysis and Detection of Obfuscated Malware," *J. Inf. Assur. Cybersecurity*, vol. 2018, pp. 1–13, 2018, doi: 10.5171/2018.836339.

[32] T. M. Ghazal et al., "IoT for smart cities: Machine learning approaches in smart healthcare—A review," *Futur. Internet*, vol. 13, no. 218, pp. 1–19, 2021, doi: 10.3390/fi13080218.

[33] T. R. Soomro and M. Hussain, "Social Media-Related Cybercrimes and Techniques for Their Prevention," *Appl. Comput. Syst.*, vol. 24, no. 1, pp. 9–17, 2019, doi: 10.2478/acss-2019-0002.

[34] Hasan, Mohammad Kamrul, Musse Mohamud Ahmed, Sherfriz Sherry Musa, Shayla Islam, Siti Norul Huda Sheikh Abdullah, Eklas Hossain, Nazmus Shaker Nafi, and Nguyen Vo. "An improved dynamic thermal current rating model for PMU-based wide area measurement framework for reliability analysis utilizing sensor cloud system." IEEE Access 9 (2021): 14446-14458.

[35] Hasan, Mohammad Kamrul, Shayla Islam, Rossilawati Sulaiman, Sheroz Khan, Aisha-Hassan Abdalla Hashim, Shabana Habib, Mohammad Islam et al. "Lightweight encryption technique to enhance medical image security on internet of medical things applications." IEEE Access 9 (2021): 47731-47742.

[36] Hasan, Mohammad Kamrul, Siti Hajar Yousoff, Musse Mohamud Ahmed, Aisha Hassan Abdalla Hashim, Ahmad Fadzil Ismail, and Shayla Islam. "Phase offset analysis of asymmetric communications infrastructure in smart grid." Elektronika ir Elektrotechnika 25, no. 2 (2019): 67-71.

[37] Akhtaruzzaman, Md, Mohammad Kamrul Hasan, S. Rayhan Kabir, Siti Norul Huda Sheikh Abdullah, Muhammad Jafar Sadeq, and Eklas Hossain. "HSIC bottleneck based distributed deep learning model for load forecasting in smart grid with a comprehensive survey." IEEE Access 8 (2020): 222977-223008.

[38] Hasan, M. K., Ismail, A. F., Islam, S., Hashim, W., Ahmed, M. M., & Memon, I. (2019). A novel HGBBDSA-CTI approach for subcarrier allocation in heterogeneous network. *Telecommunication Systems*, *70*(2), 245-262.

[39] Saeed, M. M., Hasan, M. K., Obaid, A. J., Saeed, R. A., Mokhtar, R. A., Ali, E. S., ... & Hossain, A. Z. (2022). A comprehensive review on the users' identity privacy for 5G networks. *IET Communications*.

[40] Hasan, M. K., Alkhalifah, A., Islam, S., Babiker, N., Habib, A. K. M., Aman, A. H. M., & Hossain, M. (2022). Blockchain Technology on Smart Grid, Energy Trading, and Big Data: Security Issues, Challenges, and Recommendations. *Wireless Communications and Mobile Computing*, *2022*.

[41] Hasan, M. K., Kamil, S., Shafiq, M., Yuvaraj, S., Kumar, E. S., Vincent, R., & Nafi, N. S. (2021). An improved watermarking algorithm for robustness and imperceptibility of data protection in the perception layer of internet of things. *Pattern Recognition Letters*, *152*, 283-294.

[42] Ghazal, T. M., Hasan, M. K., Hassan, R., Islam, S., Abdullah, S. N. H. S., Afifi, M. A., & Kalra, D. (2020). Security vulnerabilities, attacks, threats and the proposed countermeasures for the Internet of Things applications. *Solid State Technol*, *63*(1s), 2513-2521.

[43] Memon, Imran, et al. "Protect mobile travelers information in sensitive region based on fuzzy logic in IoT technology." *Security and Communication Networks* 2020 (2020).

[44] Ghazal, Taher M., Mohammad Kamrul Hasan, Muhammad Turki Alshurideh, Haitham M. Alzoubi, Munir Ahmad, Syed Shehryar Akbar, Barween Al Kurdi, and Iman A. Akour. "IoT for smart cities: Machine learning approaches in smart healthcare—A review." Future Internet 13, no. 8 (2021): 218.