A Literature Review on the Pervasiveness of Ransomware Threats and Attacks in the Philippines

Eric B. Blancaflor *, Joselito Lizer C. Daluz, Roduel Adrian G. Garcia, Nathan Gadiel S. Monton, and Jhoana Marie S. Vergara

School of Information Technology, Mapúa University, Makati, Philippines; Email: jlcdaluz@mymail.mapua.edu.ph (J.L.C.), raggarcia@mymail.mapua.edu.ph (R.A.G.G.), ngsmonton@mymail.mapua.edu.ph (N.G.S.M.), jmsvergara@mymail.mapua.edu.ph (J.M.S.V.)
*Correspondence: ebblancaflor@mapua.edu.ph (E.B.B.)

***Abstract*—Ransomware is still widely prevalent and poses a serious danger to vital services and corporate infrastructure around the world. Through the usage of this malicious software, cybercriminals encrypt all of their victims' important data. Cybercriminals threaten their victims with blackmail to coerce them into paying a "ransom" to avoid losing, disclosing, or being locked out of their essential resources. According to experts, ransomware assaults target a firm every 11 seconds, causing $20 billion in harm globally. Given the financial power of ransomware, cybercriminals are encouraged to create new varieties that are more nefarious and charge bigger ransom costs to their victims. In several nations, including the Philippines, where ransomware attacks have impacted at least 7,000 Philippine enterprises, this expanding problem of ransomware attacks can be seen. The Philippines' use of technology is extremely susceptible to cyber events as it adapts to home-based situations in response to the COVID-19 epidemic. Ransomware attacks have affected PH businesses; this percentage will rise to 40% by 2020. In order to address the Philippines' vulnerability to ransomware attacks, this study investigates ransomware and its many forms of attacks there, identifies potential countermeasures to prevent, lessen, and end these kinds of attacks, and suggests various approaches to deal with the country's current ransomware attack problems. In the Philippines, ransomware assaults are typically thwarted using ransomware prevention techniques. Companies and organizations should invest in ransomware detection methods in order to assist stop more loss and harm, but they shouldn't limit their defensive strategies to prevention alone.**

***Keywords*—ransomware, ransom, cybercriminals, malicious software**

I. Introduction

Ransomware is a severe threat that has been known to interrupt critical services and commercial infrastructures. This extortion software, which gets its name from the word "ransom," encrypts all the data on the device and demands a ransom or a fee to the user to regain access to it [1]. By preying on their users' fears of losing essential data, revealing sensitive information, or being locked out of essential resources, this malware type blackmails the victim to pay the ransom [2]. Experts estimate that a corporation is targeted by a ransomware attack every 11 seconds, resulting in total damage costs of $20 billion in 2021 globally [1]. In most cases, victims' ransoms vary from $300–$700 (Php15,400–Php35,930) for individuals, $10,000–$17,000 (Php513,300–Php872,600) for businesses; and there have been instances that victim paid up to $400,000 (Php 2,000,000) in one month [2]. With ransomware's economic prowess, it contributes to the growing infection rate of softwares and organizations which motivates numerous cybercriminals to develop new variants [2]. Furthermore, cybercriminals are also setting their sights on least developed and developing countries, such as the Philippines, one of the countries with the most encounters of ransomware attacks.

The Philippines, with its utilization of technology, is said to be extremely vulnerable to cyberattacks and incidents [3]. According to the Manila Times, there has been an increased number of cyberattacks in the Philippines, specifically ransomware attacks which rose to 62% of incidents around the world during 2020 [4]. These ransomware attacks have affected at least 7000 Philippine companies. The encounters experienced during 2020 made the Philippines the 4th in SEA for most ransomware attempts from a report produced by the Kaspersky Security Network [4, 5]. A company in the Philippines that recently experienced this type of cyberattack is the S&R Membership Shopping company which compromised the personal data of about 22,000 individuals [6]. Other companies, such as PH firms surveyed in the Philippines, have also experienced numerous ransomware attacks, increasing from 30% to 42% in 2020 [7]. The following reports noted that Philippine organizations are below the global average of stopping attackers from encrypting data [7]. The report explains the severity of cybersecurity against ransomware in the Philippines compared to other

Manuscript received August 23 2022; revised October 23 2022, accepted December 15, 2022; published July 5, 2023.

countries. Hence, it can be concluded that a review of ransomware attacks in the Philippines is required to determine solutions to resolve and mitigate future attacks.

Therefore, to address the prevailing problems of ransomware attacks in the Philippines, this paper reviews the various types of ransomware attacks. By conducting a review of various ransomware attacks, people may be educated on the topic of ransomware. In addition, it could help diagnose the Philippines' susceptibility to ransomware attacks. With this review, the paper strives to determine possible solutions to prevent, mitigate, and resolve ransomware attacks in the Philippines. Additionally, this paper intends to analyze the current use of ransomware in the Philippines to determine the methodologies used in these attacks. Furthermore, the objective of this paper is to suggest different methods that can be used to resolve multiple ransomware attacks to avoid future damages from these types of attacks.

II. Discussion

A. Overview of Ransomware

Malware, short for "malicious software", have evolved and improved their efficiency towards data systems as information technologies develop and proliferate worldwide. The term "malware" refers to a series of intrusive software variants (i.e., Trojan horses, ransomware, backdoors, and viruses) created by cybercriminals (commonly referred to as "hackers") to encrypt files partially or entirely, gradually slowing down computer systems, eventually making computers and computer systems unstable [8]. As the world shifted to cater to home-based scenarios due to the COVID-19 pandemic, business and consumption models are required to focus on the use of technology even more. One variant of malware that has significantly increased in popularity during these times are the Ransomware attacks [9]. Ransomware is a malware variant that prohibits access to a user's data until a "ransom" is paid [9]. Even before the pandemic, Kara and Aydos showed that ransomware attacks have risen exponentially in the last five years due to their increased financial benefits [8].

B. Ransomware Timeline

The idea of ransomware attacks was conceptualized in 1989 when a floppy disk containing an AIDS Trojan. (Also known as Aids Info Disk or PC Cyborg Trojan) was distributed at the World Health Organization's International Aids conference [10]. This malware infected the target computers by encrypting the system's file extensions, filenames, and printed a ransom demand of $189 [11]. Following the discovery of AIDS, a new age of malicious code development and cyber-attacks by lone hackers and cybercriminals began. However, unlike the AIDS Trojan, the attacks and ransoms processes were not fully automated until 2004.

In 2004, GPCode, the first contemporary ransomware was released in 2004. It used a weak and easily deciphered proprietary symmetric encryption algorithm and was transmitted using a spam email attachment that looked like a job application [10]. With the breakthrough of GPCode, it inspired other modern ransomware strains which further enhance and modify their software through the years.

The success of GPCode brought forth numerous modern ransomware strains and variants. These variants' softwares were improved and tweaked over the course of time. For instance, Archievus was recorded to be the earliest ransomware to use RSA encryption [10]. Nowadays, modern ransomwares (i.e., WannaCry, Petya, Locky) use a hybrid encryption scheme combining both AES and RSA encryption to secure their malware [12]. Fig. 1 shows a sample message received by a customer from an AIDS DOS Trojan attack.

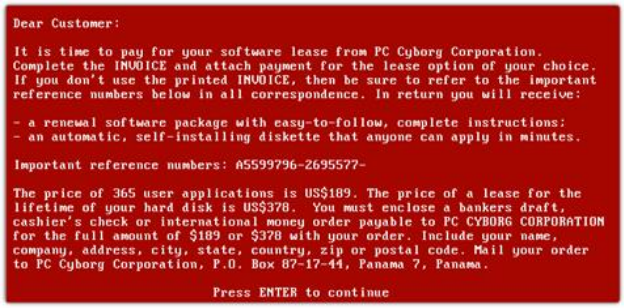

Figure 1. Part of AIDS DOS trojan horse payload message.

In 2011, a large-scale ransomware outbreak emerged which led to the discovery of various well-known ransomware strains like Reveton, Cryptolocker, CryptoWall CTB-Locker, etc. These ransomwares infect the victim's computer through a wide range of attacks that vary from email spams, phishing, file attachments, macros, etc. [8, 15]. In 2015, the number of ransomware attacks have grown exponentially thanks to the emergence of easily attainable ransomware software services or Ransomware-as-a-Service (RaaS) which offers services for cybercriminals who lack the technical knowledge to set up or create their own ransomware [13]. Through RaaS, it became a huge contributor to the rising distribution rate of popular ransomware threats due to its availability and convenience [14].

Other types of ransomwares focused on attacking both public and private organizations like Reveton, Samsam, Dharma, etc. [8, 15]. Ransomware can even function as a worm; for instance, the WannaCry, a crypto ransomware known for its global epidemic attack during May 2017 [16]. In only a few days, it had infected over 200,000 Windows PCs in 150 countries [9]. Even though most of its attacks occurred in Asia, the virus continued to infect 10,000 individuals every hour [16]. The attack wreaked havoc on hospitals, businesses, universities, transportation firms, government institutions, and Britain's National Health Service [16].

Ransomware assaults are on the rise as more people access the internet. From past exploits and knowledge of pre-existing ransomware strains, cybercriminals continue to modify and establish a new generation of ransomware strains. An example of this is the ONION, a malicious program that belongs to the Dharma ransomware family. It encrypts data and requests payment for decryption tools/software through bitcoin. All affected files are

renamed through a pattern and added a ".ONION" suffix [8]. It has become a possible successor to Cryptolocker, a very dangerous menace, as one of the most sophisticated malwares today [8]. Table I offers a summary and timeline of popular ransomware strains over the years.

TABLE I. RANSOMWARE TIMELINE

Name	Description/Propagation Method	Year	Source
AIDS Trojan	First recorded ransomware virus. Distributed via Floppy disks that were mailed to its victims	1989	[10]
GPCode	First modern ransomware. Spread via spam email attachments posing as a job application.	2004	[10]
Archiveus	The earliest ransomware to use RSA encryption. These were transmitted via spam emails, file-sharing sites and other deceitful means.	2006	[10]
Reveton	Along with the large-scale ransomware break in mid-2011, Reveton ransomware, also known as "police ransomware," impersonates and pretends to be law enforcement agencies. These were propagated via "drive-by" techniques.	2012	[8]
Cryptolocker	Most prominent ransomware to date and considered to be the first ransomware malware. These were disseminated through emails posing as computer service issues from FedEx, UPS, DHS, and others. These emails contained a zip attachment that infects the computer. If the ransom fails to be paid within three days, the demanded ransom increases.	2013	[15]
CryptoWall CTB-Locker	An improved version of Cryptolocker. It uses java vulnerability and is delivered through malicious advertising. An estimate of $27 million was paid by the end of 2015, surpassing Cryptolocker.	2014	[8]
Ransomware as a Service (RaaS)	An online software package sold to cybercriminals who lack the technical skill to create their ransomware. This is paid through a subscription type method, with the user sharing a portion of the ransom with the software's creator.	2015	[16]
SamSam	A type of ransomware that targeted healthcare organizations, hospitals, and city municipalities. Brute-force tactics and a series of vast range exploits were used to infect its victims.	2015	[15]
Dharma	Ransomware which targets various companies and organizations worldwide and is still releasing new variants in 2019. These are transmitted through malicious email spams and brute-force unprotected RDP connections.	2016	[15]
Locky	Distributed via phishing emails and Locky is a ransomware email worm that contains malicious "macros". Encrypts files via AES encryption and will be renamed to different formats.	2016	[9, 10]
Petya	Spread via phishing emails and lock the whole hard drive until the ransom is paid, which is accomplished through overwriting the infected computer's master boot record (MBR), making the operating system unable to recreate the unencrypted files without the MBR.	2017	[10, 15]
WannaCry	A ransomware worm that rapidly spreads over a vast number of computer networks. The targets were government systems, transit networks, commercial organizations, universities, and hospitals. It employs RSA-2048 encryption with random hexadecimal strings, and if the ransom is not paid within seven days, the virus begins to erase the encrypted files.	2017	[9, 10, 15]
ONION Ransomware	Due to its AES encryption and intimidation techniques used to obtain the ransom from its victim, this new generation of ransomware is thought to be a potential successor to Cryptolocker.	2019	[8]

C. Ransomware in the Current Times

In recent times, ransomware remains the number one threat to large and medium-sized businesses and the government, healthcare, and other essential industries [14]. In the mid-year 2021 report [14] conducted by Acronis, a leading company dedicated to cyber protection, the Philippines ranked top 7 among the Asian and Middle Eastern countries with the most detected ransomware (See Fig. 2).

Country	Regional ransomware detections percentage in Q1 2021	Regional ransomware detections percentage in Q2 2021
Japan	32.4%	38.1%
China	6.2%	8.6%
South Korea	6.3%	5.5%
Turkey	5.6%	5.5%
Taiwan	5.2%	5.4%
Iran	4.1%	4.5%
Philippines	11%	4.2%
Lebanon	0.3%	3.8%
India	4.9%	3.7%
Israel	3.6%	2.5%

Asia and the Middle East

Figure 2. Report of regional detection of ransomwares based on Asia and Middle East Regions.

With the current rise of ransomware attack cases experienced in the Philippines [4, 5], a review of present malware detection and mitigation techniques is required to understand how these attacks may be prevented. However, to understand the following malware detection and mitigation techniques, a review of the types of ransomware attacks should be discussed.

According to Kara and Aydos [8], Beaman and Barkworth *et al*. [9], there are two types of ransomwares, namely crypto ransomware, and locker ransomware. Crypto ransomware involves encrypting all data files in a system without interfering with any essential computer functions. This type of encryption is irreversible without the decryption key, which may only be given if the ransom has been paid. Locker ransomware may also encrypt files in the system; however, it can also encrypt files to lock a system, making it unusable. This type of ransomware may allow limited access, and it may be resolved by rebooting the system or running anti-malware software [9].

From the following types of ransomwares, it is apparent that it is more challenging to manage crypto ransomware than locker ransomware. This may be caused by the encryption techniques used by crypto ransomware which enables the encryption of these attacks. Crypto ransomware may use encryption schemes such as symmetric, asymmetric, and hybrid. The symmetric approach embeds an encryption key in the ransomware, making it vulnerable to reverse engineering. In contrast, the asymmetric approach struggles to encrypt large files due to its slower performance than the symmetric approach [9]. The hybrid approach is the most effective and complex to encrypt due to its composition, which uses symmetric and asymmetric encryption [9]. This encryption scheme creates and uses a symmetric key to encrypt files. In contrast, a public-private key pair is generated, which encrypts the symmetric key using the public key and decrypts the symmetric key when the ransom is paid [9]. With the following encryption techniques stated, it appears that ransomware attacks should be approached according to its type of encryption due to the damage it may cause.

According to Kara and Aydos [8], Beaman and Barkworth *et al*. [9], there are two ways to approach ransomware attacks, these approaches are known as ransomware detection and prevention. However, to discuss ransomware detection and prevention, the topic of malware analysis requires a review since ransomware is a type of malware. Malware analysis is a useful approach used in detecting and preventing malware by using automatic and manual analysis techniques. There are two types of malware analysis, mainly manual and automatic malware analysis. Manual malware analysis may be used to develop intuitive detection techniques that can overcome disadvantages of automatic malware analysis at a slower and more expensive cost [8]. Alternatively, automatic malware analysis may analyze binary file contents to detect unique patterns like known malware or predict malware through irregular behavior and actions of processes is conducted [8, 9]. The former definition is one of the categories of malware analysis called static analysis, while the latter definition is for the other category called dynamic analysis [9]. From the two categories of malware analysis, the static analysis approach is recognized as a better option in detecting malware due to its fast and low-positive detection rate as seen in signature-based malware detection [9]. However, the static analysis has its disadvantages such as the concealment of malware through code obfuscation techniques, causing the malware to avoid detection [9]. For these types of malwares, the dynamic analysis approach overcomes this error since it analyzes the unique patterns found within the lines of code as seen in behavior-based detection [8, 9]. However, these types of malware analysis may be exploited due to time constraints and the inability to make intelligent decisions. Another type of automatic malware analysis combines both types of malware analysis called hybrid analysis which overcomes both issues present within both static and dynamic analysis by jointly using these techniques together [8]. From the following types of malware analysis stated, the advantages and disadvantages of these detection and prevention techniques may be used to create an effective ransomware detection and prevention with its design in malware detection.

In recent ransomware analysis software, similar types of malware analysis have been used as tools in ransomware detection and analysis. The most used types of malware analysis come from the automatic malware analysis category which features static, dynamic, and hybrid analysis [8].

Although these tools may provide a layer of protection to systems from different types of ransomwares, it may still be possible for other cases of ransomware to enter systems undetected since automated analysis approaches may fail to detect newly created ransomware [8]. A different approach to overcome ransomware attacks may be through ransomware prevention approaches. The preventive approach in ransomware is a solution that intends to prevent, mitigate, and/or reverse damages received from a ransomware attack [9].

There are different types of ransomware prevention approaches; techniques for prevention may be through the enforcement of access control, storing data backups, key management, and raising user awareness to avoid and prevent these types of attacks [9]. To summarize these prevention approaches, the techniques were categorized into four categories: access control, data backup, key management, and user awareness. Access control is a

prevention approach that restricts access to files in the system by using a mechanism similar to access control lists which enables file access to programs based on privileges and permissions set for files [9]. Data backup is an approach that minimizes the damage of ransomware attacks by regularly storing backups on different computers or networks [9]. Key management is an approach to retrieve the encryption key used in the file encryption of the ransomware attack to decrypt encrypted files without paying the ransom set by the attacker [9]. User awareness is an approach that allows regular employees with little to no experience in technical skills in programming the opportunity to prevent ransomware attacks [9]. Users, such as employees, are instructed to take precautionary measures against ransomware attacks with guidelines that prevent users from accidentally creating vulnerabilities within the system [9].

Based on the following ransomware prevention approaches stated, ransomware may be resolved through prevention rather than detection, however, there are different cases when detection is better than prevention and vice versa. To determine the appropriate use of ransomware detection and prevention approaches for ransomware attacks, an analysis of different cases from the Philippines must be reviewed to examine the vulnerabilities that may cause these attacks and to prepare different ransomware detection and prevention approaches to resolve these types of attacks.

D. Philippines' Cases of Ransomware Attacks

According to research published in the Philippines [17], there is a concerning gap in cybersecurity expertise among Philippine's enterprises and organizations. Nearly 45% of these businesses lack the requisite cybersecurity capabilities to safeguard themselves, and 48% of the respondents said it was challenging to find qualified cybersecurity personnel [17]. According to Microsoft Philippines, the Philippines has above-average exposure to drive-by download sites (websites that contain one or more exploits that target vulnerabilities in web browsers and browser add-ons) with 0.05 to 0.1 per 1000 URLs. It also states that the country has ransomware encounter rates of 0.08%–0.12% [18]. If the Philippines wants to reap the benefits brought by the digital world, they should examine and improve their cybersecurity programs fast. The frequency of ransomware attacks grows, and there are no signs of stopping. In a report provided by Statista, a source of market and consumer data, ransomware attacks increased by 62% to 304 million instances in 2020 globally, the highest level in four years [19].

On the other hand, the global security firm, Kaspersky Security Network (KSN), reported that among the Southeast Asian countries, less than one million ransomware attempts (804,513) were tracked, which is less than half of the 1.9 million detections recorded in 2019 [20]. The same report [20] stated that the Philippines was placed 50th in the world in terms of ransomware attacks, with over 22,000 attempts prevented, down from 45th in 2019 with 26,000 ransomware attempts blocked (see Table II).

TABLE II. RANSOMWARE ATTEMPTS AGAINST SMBS IN SOUTHEAST ASIA PREVENTED BY KASPERSKY [20]

Countries	2020		2019	
	Detections	Global Ranking	Detections	Global Ranking
Indonesia	439,473	5	1,158,837	4
Malaysia	12,191	56	67,285	34
Philippines	22,011	50	25, 946	45
Singapore	3,191	78	2,275	99
Thailand	122,934	21	191,281	22
Vietnam	204,713	11	536,586	7

Although there has been a significant drop in detections, the decrease should not make cybersecurity organizations and businesses complacent. Ransomware groups are more focused on the quality of strains and not the quantity. Attackers mostly prioritized attacking their targeted victims more aggressively than waiting for them to fall under an attack [20]. In fact, one-third of the ransomware attacks Kaspersky prevented in 2019 was reported to be aimed at corporate users, indicating that cybercriminals are increasingly targeting organizations and enterprises rather than individual consumers [21]. Although 22,000 ransomware attempts were prevented in the Philippines, the country remains vulnerable to such assaults. Small and midsize businesses (SMBs) in the Philippines have been the victim of different ransomware attacks in recent years. An example of these attacks is the WannaCry ransomware- see Fig. 3.

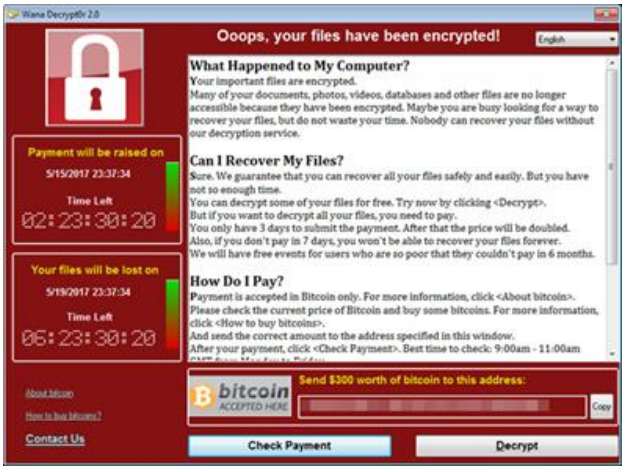

Figure 3. WannaCry ransomware message.

The WannaCry ransomware is still the most prominent ransomware not only in the Philippines but all over the world; even though it has not been supported by its developers in over three years and persists as a "zombie", the WannaCry family accounts for a considerable portion of all identified ransomware [20]. This ransomware strain rose to prominence back in 2017 when it started a threat of attacks worldwide, hitting approximately 150 countries,

including the Philippines [22]. During its 2017 outbreak, it affected more than two dozen companies in the Philippines [23]. Even after years, the ransomware still exists and continues to spread due to its variants that can bypass and evade the so-called "kill switch", a specific URL that could stop the infection process [22]. According to the published report of Chua [22], a security firm, about 249,400 WannaCry infection attempts were made in the Philippines, accounting for 5.8% of the global WannaCry infection attempts. Chua points out that the reason why WannaCry still prevails is because of devices that are not being patched properly to fight against the main exploits of the various ransomware strains [22]. As the WannaCry ransomware continues to significantly affect numerous companies and organizations based in the Philippines, it is apparent that the problem continues to occur due to the variants of the ransomware evading detection. In this case, the best way to counter the following ransomware attack may be using ransomware prevention approaches. To mitigate these attacks, the firm recommends updating all devices' patches and backing up essential files and data to an offline storage device to avoid paying a ransom in the event of a ransomware attack [22]. By mitigating these attacks, damages may occur but its effect on the company or organization affected may be lessened through the prevention approach.

One company recently targeted with the use of ransomware was Accenture. During the 30th of July, 2021, the company Accenture was targeted by a group named LockBit, demanding ransom to prevent the distribution of stolen data [24, 25]. LockBit is a group known for their ransomware-as-a-service operation called LockBit 2.0, a service that has been targeting numerous companies with its attack of Accenture being a more recent victim [26]. From statements of representatives at Accenture, it appeared that a ransomware attack had stolen documents which identified clients and materials created by clients [25]. The ransomware attack was contained and isolated from other servers of the company with backups provided to restore the affected systems as soon as security controls and protocols detected irregular activity within their system environment [25, 26]. From the following statements, it appeared that Accenture had used numerous countermeasures to resolve the ransomware attack. Based on the following statements made by Accenture representatives, Accenture managed to detect the attack through irregular activity which could be through dynamic malware analysis. Additionally, Accenture managed to regain their affected files and systems through their data backup. In this example, both ransomware detection and prevention approaches were used to resolve the issue. Results show that the company managed to reduce damages and recover encrypted files, however, the problem of blackmail is present since the attackers managed to download these files. Although the ransomware attack failed to earn income through their original attack, the files obtained by the attackers were used for ransom which could have affected their business if this were crucial to their competition. As shown in Fig. 4 is a lockbit message received by Accenture.

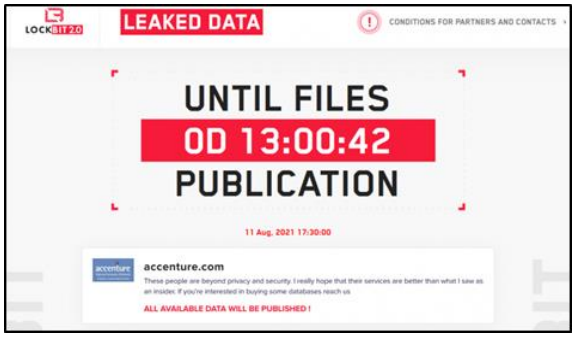

Figure 4. Lockbit 2.0 message on Accenture.

On the other hand, the S&R Membership Shopping also experienced a case of ransomware attack. On Nov. 14, 2021, S&R Membership Shopping experienced a ransomware attack on their membership system, which affected 22,000 individuals' personal data, including date of birth, contact number, and gender. The incident was reported to the National Privacy Commission (NPC) a day after the incident was discovered. According to S&R's Data Protection Officer (DPO), important information such as credit card details and other financial information were not included in the compromised data from the incident. S&R informed NPC that they had organized security measures to their system, recovered the compromised data, and prevention measures to prevent similar incidents [27]. S&R Membership Shopping posted a public statement about the incident on Nov. 21, 2021, to inform their customers that membership data has been compromised while also indicating that no financial information was stolen [28]. In this case, it appeared that several user data were compromised during the incident. However, the company managed to use several prevention approaches to address the ransomware attack such as using data backups to recover lost data.

Another case of ransomware in the Philippines is the AXA group Avaddon Attack in May of 2021. AXA is an insurance company based in France [29]. Three terabytes of data were affected, including customers' identity, health status, IDs, passports, and bank documents. The headquarters of the group, located in the Philippines, Malaysia, and Thailand, were hit by Avaddon Ransomware Attackers, and will be listed and shamed on their website avaddongun7rngel[.]onion if they do not pay their ransom of $40,000.00 worth of Bitcoin. Suppose they pay the said amount without attempting to recover the files in another way and modify the encrypted files themselves. In that case, they will release the decryption key, or the AXA group will lose all their files. After the Avaddon ransomware released the decryption key, the AXA group found a flaw in their encryption and later released free decryption to the public. Avaddon then responded by modifying the encryptor entirely after a day of the release of the decryption key- making it obsolete [30]. Recommendations for this type of attack are listed as follows: a consistent patch of security updates to prevent exploitation of known problems, limitation of user permissions in the system, disabling of administrative tools to avoid misuse, establishing a recovery plan when a disaster comes, and backup policies, 24/7 monitoring of

network security, and utilizing network segregation to restrict nodes communication [31]. From the recommended prevention measures of the following ransomware attack, it appeared that the appropriate prevention approaches to resolve the attack is through access control, data backups, and user awareness.

E. Ransomware Prevention and Mitigation

In the previous section, different cases in the Philippines involving ransomware were discussed. Based on the cases discussed, it appeared that most cases were handled by using ransomware prevention approaches such as access control, data backups, and user awareness. Most Philippine companies and organizations commonly use ransomware prevention approaches to resolve incidents involving ransomware. According to Castillo, instead of stopping attackers from using ransomware to target their systems, organizations and companies in the Philippines would rather deal with ransomware attacks through recovery plans such as data backups [32]. Other companies such as Globe and Smart have started similar ransomware prevention approaches by implementing user awareness campaigns to reduce these types of incidents [33]. Another company known as Palo Alto prevents ransomware attacks through user awareness and data backups [34]. Although the implementation of different ransomware prevention approaches may prevent further damages to the company, the limitations of these approaches may fail to protect their data from being sold to others due to the attacker's ability to obtain these data while conducting the ransomware attack.

Ransomware prevention approaches may offer a layer of protection against ransomware attacks, however, additional approaches to overcome ransomware attacks such as ransomware detection approaches may improve the overall cybersecurity of Philippine companies. Ransomware detection and prevention approaches are both important in cybersecurity since multiple approaches to ransomware attacks may increase the chances to defend companies from different forms of attacks. By using the following ransomware detection and prevention approaches discussed in the previous sections, it is believed that ransomware attacks in the Philippines may be reduced since the following approaches stated have been proven effective against ransomware attacks [8, 9, 35, 36]. For this reason, it is recommended to numerous Philippine companies and organizations to utilize both ransomware detection and prevention approaches to avoid future incidents and reduce further damages that ransomware attacks may cause to their respective organization or company.

III. Conclusions

Ransomware remains a prevalent threat worldwide; by preying on their victim's fears of locking them out of their data or disclosing the said data to the public, cybercriminals benefit from blackmailing their victims to pay the "ransom" fee. As the world shifts to adjust to the "new normal", it triggers necessary changes to business and consumption models. Companies and industries shift to cater to home-based scenarios, which makes the people rely on technology even more, prompting a need to reevaluate the country's defenses and susceptibility against cyber-attacks. Companies from the Philippines have been susceptible to ransomware attacks due to the current state of their cybersecurity defenses, with the country lacking on cybersecurity knowledge and trained personnel. With, cybercriminals continued to target large companies such as S&R Membership shopping, Accenture, and Philippines' insurance company AXA Group, based in France. From the review, it can be concluded that cybercriminals are setting their sights on quality rather than the quantity of ransomware they produce. This growing movement of quality over quantity can be seen through the development of ransomware over time and the ransomware instances in the Philippines. To secure their defenses against cyberattacks, it was apparent that most companies in the Philippines rely on ransomware prevention approaches such as data backups since it is the most effective solution to resolve these incidents. Although data backups may provide a layer of defense for ransomware attacks, these may lead to further ransoms made by attackers due to their ability to retrieve the information through the initial attack. Ransomware attacks require a more in-depth defense in cybersecurity to address the issue of accessing information before the attack. By investing in various ransomware detection and prevention approaches, companies from the Philippines may overcome issues caused by these ransomware attacks.

In determining the types of ransomware detection and prevention approaches to use, it is appropriate for companies to start investing in training personnel to recognize various types of ransomware and possible solutions to prevent and mitigate these attacks. It is appropriate to learn about ransomware attacks before deriving a solution for these attacks since assigning numerous types of ransomwares without proper planning may lead to a more costly investment for the company. For ransomware detection approaches, it is recommended to use hybrid ransomware analysis tools due to its effectiveness in detecting ransomware attacks surpassing both problems in static and dynamic ransomware analysis. For ransomware prevention approaches, companies in the Philippines have been consistently using data backups to retrieve locked systems, however, companies must not limit themselves to solely data backups. Other ransomware prevention approaches are equivalently important to protecting systems since these may help prevent ransomware attacks from entering the system. Access control and user awareness are two ransomware prevention approaches necessary for preventing these attacks since both approaches can control how ransomware may enter the system. Key management may also provide a solution to retrieve lost data without paying ransom, however, there may be risks involved when performing key management which could further damage the system. Overall, it is important to have multiple layers of defense against ransomware attacks since more layers may help lessen and/or prevent future incidents regarding ransomware.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

E. B., J. L. D, R. A. G., and N. G. M.: Conceptualization; J. M. V., R. A. G., J. L. D.: methodology; E. B., J. M. V.: writing, review and editing. All authors have read and agreed to the published version of the manuscript.

ACKNOWLEDGMENT

We thank our research adviser, Dr. Eric B. Blancaflor who provided his guidance and expertise that significantly assisted the research. We would also like to show our appreciation to the reviewers that thoroughly analyzed our paper and given their insights.

REFERENCES

[1] United Nations Office on Drugs and Crime. (2021). Ransomware attacks, a growing threat that needs to be countered. [Online]. Available: https://www.unodc.org/southeastasiaandpacific/en/2021/10/cybercrime-ransomware-attacks/story.html

[2] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions," *Comput. Secur*., vol. 74, pp. 144–166, 2018, doi: 10.1016/j.cose.2018.01.001.

[3] International Trade Administration. (2020). Philippine Cybersecurity. [Online]. Available: https://www.trade.gov/market-intelligence/philippine-cybersecurity

[4] The Manila Times. (2021). Cyberattacks threaten PH, other economies. [Online]. Available: https://www.manilatimes.net/2021/06/07/opinion/editorial/cyberattacks-threaten-ph-other-economies/1802184

[5] NewPost. (2021). Ransomware attacks continue; Philippines ranks 4th in SEA for most attempts. [Online]. Available: https://newpost.com.ph/ransomware-attacks-continue-philippines-ranks-4th-in-sea-for-most-attempts/

[6] CNN Philippines. (2021). 22,000 data subjects affected in S&R cyber-attack. [Online]. Available: https://cnnphilippines.com/business/2021/11/24/NPC-SnR-breach-report-submission.html

[7] Rappler. (2021). Ransomware attacks cost PH firms P40 million on the average in 2020. [Online]. Available: https://www.rappler.com/technology/ransomware-attacks-average-cost-philippines-firms-2020/

[8] I. Kara and M. Aydos, "The rise of ransomware: Forensic analysis for windows based ransomware attacks," *Expert Systems with Applications*, vol. 190, 116198, 2022, doi: 10.1016/j.eswa.2021.116198.

[9] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, "Ransomware: Recent advances, analysis, challenges and future research directions," *Comput. Secur*., vol. 111, 102490, 2021, doi: 10.1016/j.cose.2021.102490.

[10] R. Richardson and M. North, "Ransomware: Evolution, mitigation and prevention," *Int. Manag. Rev*., vol. 13, no. 1, pp. 10–21, 2017.

[11] Malwiki. (2021). AIDS Trojan. [Online]. Available: https://malwiki.org/index.php?title=AIDS

[12] T. Marinho. (2018). Ransomware encryption techniques. [Online]. Available: https://medium.com/@tarcisioma/ransomware-encryption-techniques-696531d07bb9

[13] K. June. (2020). The new generation of ransomware—An in depth study of Ransomware-as-a-Service. [Online]. Available: http://essay.utwente.nl/81595/1/Keijzer_MA_EEMCS.pdf

[14] A. Ivanyuk and C. Wuest. (2021). Acronis Cyberthreats report: Mid-year 2021. [Online]. Available: https://dl.acronis.com/u/rc/White-Paper-Acronis-Cyber-Protect-Cloud-Cyberthreats-Report-Mid-year-2021-EN-US.pdf

[15] I. A. Chesti, M. Humayun, N. U. Sama, and N Z Jhanjhi, "Evolution, mitigation, and prevention of ransomware," in *Proc. 2020 2nd International Conference on Computer and Information Sciences (ICCIS)*, 2020, pp. 1–6, doi: 10.1109/ICCIS49240.2020.9257708.

[16] N. Latto. (2020). What is WannaCry? [Online]. Available: https://www.avast.com/c-wannacry#gref

[17] Business Mirror. (2021). IT security budget stagnant despite rise in cyber-attacks. [Online]. Available: https://businessmirror.com.ph/2021/04/01/it-security-budget-stagnant-despite-rise-in-cyber-attacks/

[18] Microsoft Philippines Communication Team. (2017). Philippines is 8th most vulnerable to malware in Asia Pacific. [Online]. Available: https://news.microsoft.com/en-ph/2017/10/12/philippines-8th-most-vulnerable-to-malware-in-asia-pacific/

[19] The Manila Times. (2021). Cyberattacks threaten PH, other economies. [Online]. Available: https://www.manilatimes.net/2021/06/07/opinion/editorial/cyberattacks-threaten-ph-other-economies/1802184

[20] E. V. Abadilla. (2021). Ransomware attacks on SMBs drop but became more vicious—Kaspersky. [Online]. Available: https://mb.com.ph/2021/04/20/ransomware-attacks-on-smbs-drop-but-became-more-vicious-kaspersky/

[21] NewPost Tech Desk. (2020). Ransomware attacks continue; Philippines ranks 4th in SEA for most attempts. [Online]. Available: https://newpost.com.ph/ransomware-attacks-continue-philippines-ranks-4th-in-sea-for-most-attempts/

[22] K. Chua. (2019). Close to 250,000 WannaCry infection attempts in PH stopped in August alone—Report. [Online]. Available: https://www.rappler.com/technology/241701-sophos-continuing-wannacry-infections-august-2019/

[23] R. Dancel. (2017). Dozens of Philippine companies hit by ransomware. [Online]. Available: https://www.straitstimes.com/asia/se-asia/dozens-of-philippine-companies-hit-by-ransomware

[24] Rappler. (2021). Accenture hit with ransomware attack. [Online]. Available: https://www.rappler.com/technology/accenture-lockbit-ransomware-attack/

[25] NewsFounded. (2021). Accenture Knows About Ransomware Attack in Last July: Report. [Online]. Available: https://newsfounded.com/philippines/accenture-knows-about-ransomware-attack-in-last-july-report/

[26] D. Olenick. (2021). Accenture Hit by Apparent Ransomware Attack. [Online]. Available: https://www.bankinfosecurity.com/accenture-hit-by-apparent-ransomware-attack-a-17265

[27] National Privacy Commision. (2021). Statement of NPC on S&R data breach. [Online]. Available: https://www.privacy.gov.ph/2021/11/statement-of-npc-on-sr-data-breach/

[28] CNN Philippines Staff. (2021). 22,000 data subjects affected in S&R cyber-attack—National privacy commission. [Online]. Available: https://www.cnnphilippines.com/business/2021/11/24/NPC-SnR-breach-report-submission.html

[29] Cyberint. (2021). Avaddon Ransomware Attack Hits AXA Philippines, Malaysia, Thailand and Hong Kong. [Online]. Available: https://cyberint.com/blog/research/avaddon-ransomware-attack-hits-axa-philippines-malaysia-thailand-and-hong-kong/

[30] AXA. (2020). About us—AXA. [Online]. Available: https://www.axa.com/en/about-us

[31] P. Mackenzie. (2021). What to expect when you've been hit with Avaddon ransomware. [Online]. Available: https://news.sophos.com/en-us/2021/05/24/what-to-expect-when-youve-been-hit-with-avaddon-ransomware/

[32] J. Castillo. (2021). Sophos survey shows ransomware recovery cost more than P40 million in the country. [Online]. Available: https://mb.com.ph/2021/05/07/sophos-survey-shows-ransomware-recovery-cost-more-than-p40-million-in-the-country/

[33] A. Balinbin. (2021). Telcos ramping up investments in cybersecurity. [Online]. Available: https://www.bworldonline.com/telcos-ramping-up-investments-in-cybersecurity/

[34] B. Lacsamana. (2021). Prepare for more digital fraud and unauthorized data exploits in 2022—Palo Alto. [Online]. Available: https://www.bworldonline.com/prepare-for-more-digital-fraud-and-unauthorized-data-exploits-in-2022-palo-alto/

[35] N. Lord. (2020). Ransomware protection & removal: How businesses can best defend against ransomware attacks. [Online].

Available: https://digitalguardian.com/blog/ransomware-protection-attacks

[36] H. Alshaikh, N. Ramadan, and H. Hefny, "Ransomware prevention and mitigation techniques," *International Journal of Computer Applications*, vol. 117, pp. 31–39, 2020, doi: 10.5120/ijca2020919899.