Analysis of Vulnerability Factors and Severity Levels of Ransomware Strike on Organizational Data

ALENG EMMANUIE[L] ABEL1, OMEGA SARJIYUS[2], MICHAEL AUDU (MICHAEL)[3]
[1, 2]*Computer Science Department, Adamawa State University, Mubi, Nigeria*
[3]*Department of Office Technology, Federal Polytechnic, Mubi, Adamawa State, Nigeria*

Abstract- ***Common ransomwares including Crypto and Locker are a serious threat to the basic computer systems and infrastructures as their main target is to extract money from the victims by demanding ransom for the decryption key. The evolution of ransomware as a threat to both organizational and individual assets is captured in this paper. Additionally, the paper discusses the evolution, structures, and tactics of ransomware incidents and evaluates the effect of these events on both organizational and personal property throughout history. All the while, the paper looks at the underlying cause of ransomware's organizational impact and the aggressive scales it's in constant evolution of even on business personal. The explores proactive approaches which organizations could follow according to cybersecurity settings for the impetus and are prepared and aware of the ransomware assault. Additionally, the study also provides recommendations and precautions to mitigate the challenges of ransomware strikes within society.***

Indexed Terms- ***Cybersecurity Strike, Decryptions, Malicious, Ransomware, Threats.***

I. INTRODUCTION

The merciless development of malware is an important issue for cybersecurity. This makes ransomware appear as an ubiquitous and destructive threat (Mahendran, etal. 2024). Malicious software developed for electronic failures is constantly developing and hampering efforts to reduce (Mahendran etal. 2024). The lack of public disclosure related to malware attacks is due to concerns about potential damage to confidential information and reputation, which hinders joint prevention efforts and impedes comprehensive research (Mahendran, etal. 2024). In this landscape, ransomware stands out as a specific form of malware. This is used strategically by hackers to encrypt files and demand ransom (Alqahtani & Sheldon, 2022). Ransomware history dates to the late 90s, and has developed sophistication and effectiveness over the years (Mahendran et al., 2024). This study examines the diverse effects of ransomware on organizations dealing with patterns, prevention strategies, and recommendations for improving organizational resistance. Ransomware, often launched by phishing attacks that use human weaknesses, can be deeply damaged by organizations (Mahendran et al. 2024). In addition to financial fear tor, data injury organizations can be held responsible for criminal law, affect technical weaknesses, and paralyze important resources during attacks (Mahendran et al., 2024). Escalation frequency and refined attacks of ransomware attacks highlight the urgent need for organizations to enhance cybersecurity and promote resistance in view of these escalating cyber threats (Mahendran, etal. 2024). To improve destructive tactics and enhance attacks on critical assets, organizations need to actively adapt to protect their digital infrastructure, prioritize defence strategies, and mitigate possible obstacles (Alqahtani & Sheldon, 2022). The escalating prevalence of ransomware driven by low intrusion barriers and high reward temptations requires a comprehensive understanding of the cyber threat landscape and strategic mechanisms (CIFR team; Alqahtani & Sheldon, 2022).

II. PROBLEM STATEMENT

The fastest growing technologies, office ransomware, and personal systems become common. Ransomware is a type of malware that can be used to encrypt files on a device. This means that users cannot access or access it. As soon as a file is corrupted, the attacker will decrypt that location or request a ransom in exchange for property. The attacker also threatens to

reveal or sell information and documents if no ransom has been paid. This is usually necessary in cryptocurrency. The issues currently identified by some businesses and personal devices used in the office or home are:

1. Encrypting files without user or organization's user rights
2. Ransomware is corrupting impure documents on the device
3. Slowly retrieve documents affected by this ransomware
4. During the attack, governments and private organizations lose financial accounts.

Aim and Objectives

An investigation into the conceptions held by the general public about phishing, attempt and ransomware must be assessed. Comparison studies with state of the art field expert's commentary about threat likelihoods will be reviewed. Knowledge shall be obtained through literature review of previous Strike and to introduce the risks with a combination of interviews with expertise. The comparison will include metrics.

To carry out analysis of the potential risks and results of ransomware threats sensitives organizational data including loss of financial records, damage to organization fund recovery cost.

1. To investigate how ransomware has evolved in terms of its development, attack patterns, and methods employed by attackers.
2. To assess the potential impact of ransomware on important infrastructure, including industrial control systems and key sectors like healthcare and transportation.
3. To explore proactive cybersecurity measures that organizations can adopt to enhance preparedness and awareness regarding ransomware threats in this era and development.

Background to the Study

Ransomware, a serious danger to users' file access that requires payment to regain control, is acknowledged as a worldwide emergency that affects both corporate and personal data across a wide range of businesses.

Limited computer usage hampered the first ransomware, also known as PC Cyborg or AIDS Trojan, which initially appeared in 1989 and started the trend of harmful software (Mahendran et al., 2024). Payment issues with later developments, such as asymmetric ransomware, prompted the development of a dishonest antivirus program to safeguard developers' identity (Mahendran et al., 2024).

Mahendran et al. (2024) claim that ransomware assaults, which are motivated by financial gain, use email, spam, and phishing as vectors worldwide (Pascariu & Barbu, 2019), making tracking more difficult because they use virtual currency like Bitcoin for Ransomware, a serious danger to users' file access that requires payment to regain control, is acknowledged as a worldwide emergency that affects both government and personal files.

Afterward, Locker Ransomware went globally, presenting explicit images and demanding payments through various means of payments such as SMS or premium phone calls, extending ransomware Strike from one country to another (Richardson, Ronny, & MaxM, 2017). Later, the Trojan variant GPcode employed a 1024-bit RSA key and requested payment in e-gold or Liberty Reserve, highlighting early sophistication in ransomware operations and payment methods (Richardsonet al., 2017).

Impact on organizations

Despite the fact that perception of ransomware threats remains prepared, regardless of size, industry or inadequate enterprise, it means that it is a favorable destination for cybercriminals. With a focus on small businesses, this strike has become increasingly widespread, but has become more and more disruptive each year (Zakaria et al., 2017). MalwareBytes' research shows surprising facts. This shows that almost five-fifths of businesses and private owners have experienced ransomware strikes and reported a third economic loss. Large organizations and personal assets such as the US$300 million FedExs Revoport at NotPetya and Atlanta in 2017 have spent more than US$2.6 million on SAM ransomware attacks, but are spending maze ransomware assertion attacks and cognitive technology solutions after Hassan-Hassan-ransomwareware. The city, which was US$18 million after the maze ransomware attack, was netatachtage of over 18 million Doral and ransomware attacks, as well

as 18-year-old attacks and ransom goods attacks, and city IT network attacks that exceed US$18 million.

As a victim, can you consider your payment decision? A victim is someone who encrypts ransomware that attacks a decision-making document. An individual, organization, or state agency whose information technology devices are locked, has its infrastructure or systems being attacked, attacked and damaged by malignant software called ransomware and access.

i. "Don't rush to the ransom. No state has issued a final decision on ransomware payments, primarily due to the inherent complexity and unpredictability of each case, but some member states provide direct guidelines that are not paid.
ii. In the United States, for example, representatives of the General Ransomware Task Force, Cybersecurity and Infrastructure Security Agency, the National Security Agency, the Federal Investigation Agency, and multi-state information exchanges and analysis centers should not recommend ransoms that lead to such payments. Lead cup. Others emphasize or tolerate payments to cybercriminals.

To summarise everything, ransomware victims can consider paying for ransoms to recover data and property that they lost access after a thorough analysis of the case. There is no way to restore the data (i.e., fuses and infected backups only).

iii. There are no decryption tools for each ransomware extension period.
iv. Cost and impacts are the financial or other impact of reconstructing data from scratch to exceed the amount of ransom required or estimated further damage or damage. Most importantly, ransomware players have demonstrated their ability to decrypt data by providing a decryption key (or key) of reasonably important sample encrypted data. The actual steps that ransomware victims need to choose will depend on your behavior, various factors and potential risks. In this chapter you will receive the full details and then the greater details.

Important risks for ransom payments

Here is an intangible risk that the victim should always be considered essential for ransom payments and that must be evaluated in any case.

i. Crime accusations, illegal enrichment of cross-border organized crime and terrorist financing.
ii. Legality and compliance issues related to ransom payments.
iii. Probability of restoring data, and the possibility of continuous fear tor (double, triple, etc.)
iv. reputation and/or political damages.

In an unregulated context, the above risks are highly personal and subjective from the perspective of each victim. They can mostly be weighed by other factors determined by circumstances, such as the victim's key business line, sensitivity of invasion data, or potential impact on the rights of others. An example of such an effect is an organization responsible for maintaining the critical infrastructure of ransomware. In other words, infrastructure ends up putting people's lives in vain.

If payment is not possible. If the funds are not available to the victim or are unable to make them available, the discussion there will be halted without further discussion. For state victims, legal approval to move funds for such purposes can be an additional challenge for violence that requires payment. This is an exceptional case in which even attempts to negotiate the amount of ransom are not a practical option. In such cases, the victim must first decide to support the remediation of encrypted data using available public resources such as the National Computer Emergency Team (CERT) or computer CSIRT Band Response (Cortical Security), Incident Response and Security Team (First) Network 4 or No More Ransom Project 5 or No More Ransom Project 5 or No More Ransom Project 5 or No More Ransom Project 5 or No More Ransom Project 5 or No More Ransom Project 5 or No More Ransom Project 5 or No More Ransom Project 5. Make sure you restore the data and resume the data from scratch.

Explicit legal prohibition on ransom payments

Another serious consideration is the legality of paying ransom. There are some appropriate arguments for paying ransom under certain circumstances, but this is simply an impossible or a direct violation of national law by those responsible for enforcement and/or enforcement of such decisions with all legal consequences. Additionally, ransom payments could

lead to sanctions imposed by liability authorities for potential violations of data protection regulations.

A country with laws expressly prohibiting ransom forces may allow legal methods that allow exceptions to be made in certain cases. The only practical solution. Examples of such scenarios are when there is no way to recover or create important data, cause affordable costs, pose serious risks to human life, and when ransomware can demonstrate its ability to decipher samples of data. Although the current paper does not support ransom payments, it is extremely important that victims report ransomware accidents and work closely with national law enforcement agencies, their own legal counsel, relevant international organizations, and other partners to implement operations and implementation for the persecution and recovery of ransom payments.

How can victims recover their payments?
For attackers, the cost of carrying out an attack is relatively low, and profits can be important. Paying ransoms can be expensive, but many people want to spend money on a compromise. It can be believed that the impact of non-payment is more important than the cost of payment. However, paying victims can promote more ransomware strikes in the future by demonstrating that their efforts will benefit ransomware attackers. To minimize and prevent ransomware accidents, it is extremely important for organizations to develop a security-conscious culture to advocate for ransomware strikes and report ransomware cases to law enforcement or other appropriate authorities. This includes investments in cybersecurity infrastructure, which can report to law enforcement as soon as a ransomware incident occurs, identify relevant cryptocurrency addresses, and identify frozen accounts on VASP if necessary. Even if your organization is preparing for a ransomware attack, it is important to take these measures and measures as soon as possible to increase the likelihood of a successful ransom recovery.

Some jurisdictions may require that you notify law enforcement and other relevant authorities within a certain period of time. If the victim has cyber insurance, and if a ransomware incident covers it, the corresponding legal process must be followed. It is important that victims contact national-level law enforcement as soon as possible and notify the corresponding certificate/CSIRT (if configured). Law enforcement agencies can launch investigations and support international partners, financial institutions, VASPs and blockchain analytics companies. It is also important that the financial institution submits necessary reports when identifying suspicious transactions that may be related to ransom payments or related money laundering.

III. METHODOLOGY

The research methods and analysis of the results of the research were followed by a mixed method approach, following an exploratory sequential design. The phase is qualitative. Literature searches show that there are few tools available for this particular purpose. Crypto ransomware incidents have resulted in some unique consequences and punishments (e.g., encrypted data and disabled systems), and other cybercriminal research alternatives could not be used. The evaluation equipment had to be specific to crypto ransomware strikes.

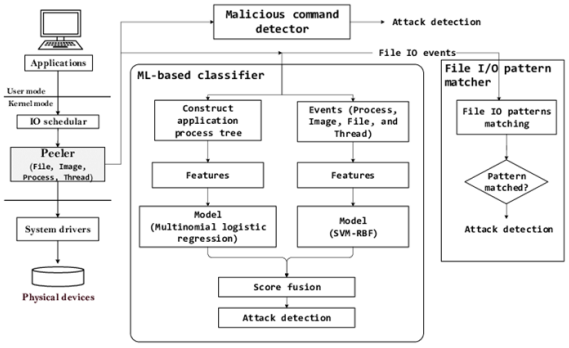
Data Collection Phases
Sample Strategy and Data Acquisition Target Sample Approach were used to collect data and methods for data collection using primary and secondary data collection were provided.

What kind of cooperation is needed to facilitate recovery?
A successful recovery of ransom payments requires strong cooperation from all participants, including governments, private companies and citizens. Companies specializing in cybersecurity and blockchain analytics can provide expert knowledge to examine the movement of virtual assets and identify off-ramps that criminals use to convert profits into cash. While law enforcement and prosecutors investigate ransomware strikes and pursue perpetrators, financial institutions can play an important role in identifying and reporting suspicious activities that may be related to ransomware and other cyber strikes through recognition, reporting and blocking ransom payments. They can also help victims with the support of law enforcement authorities to help them regain their own measures.

Expected Consequences Awareness and Education

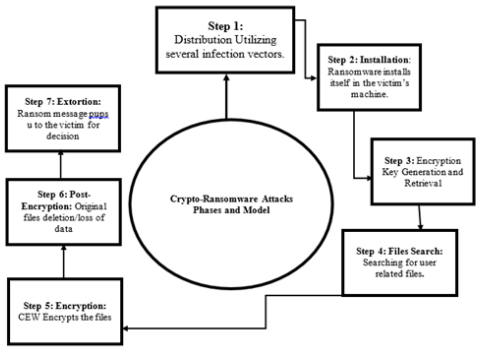
In order to effectively combat ransomware crime, it is important to increase public awareness and education in several important aspects, including targets and victims of organizations such as ransomware criminals and organizations and individuals. These efforts are not only beneficial for law enforcement authorities, but also for society as a whole. Through education campaigns and initiatives for public awareness, individuals can gain a deeper understanding of crime and how to respond effectively to it. Additionally, schools and community organizations can be encouraged to have useful discussions on this topic. With a proper understanding, anyone who detects ransomware threats and ransomware can be more aware. This could lead to better reporting and more effective answers about crime, ultimately contributing to reducing the prevalence of crime.

Algorithm of the System



Overview of Peeler. Algorithm enlists all the keys towards the steps required in ransomware attack (Muhammad, et al, 2012)

Ransomware attack model

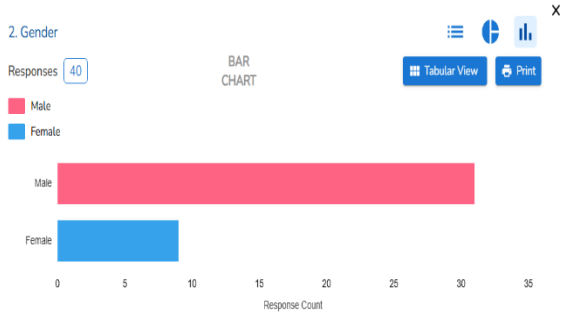


Ransomware attack model (Bander, 2020)

IV. RESULTS AND DISCUSSIONS

The result and discussion will be presenting the outcome of interviewers and their decision, also analysis and interpretation of data collected during the research.

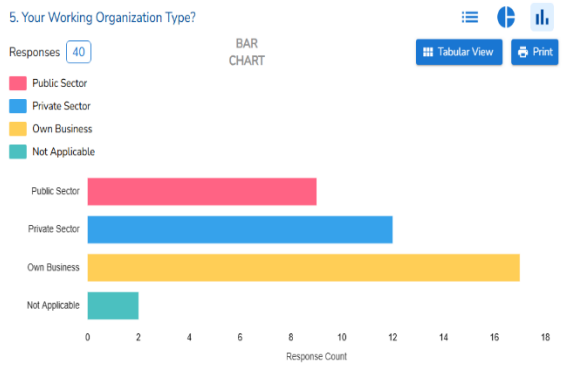
Result showing the responds of Genders



From the chart above shows that Male gender are more affected by ransomware assails. While Female are less affected by ransomware assails.

According to the aforementioned results, the majority of ransomware assails affected are male base on the bar chart presented above and the result gotten from the finding.

You're Working Organization Type?

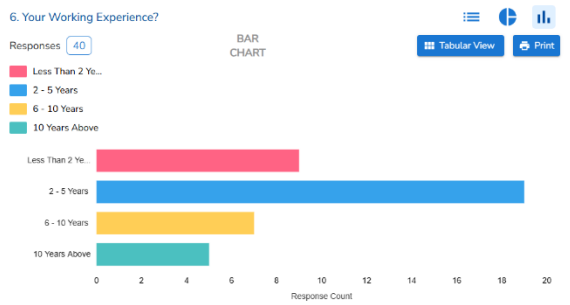


The chart above indicates that Own Business are more affected by ransomware assails, followed by private sector, while public sector is less affected by ransomware assails.

According to the aforementioned results, the majority of ransomware assails affected are Own

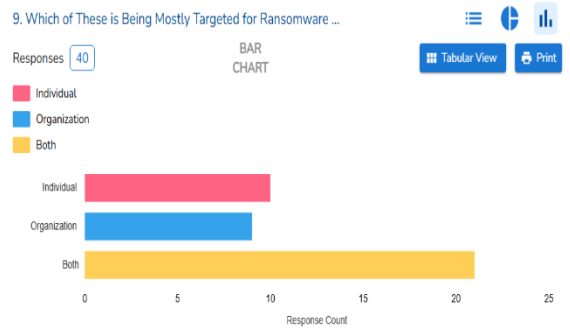
Business base on the bar chart presented above and the result gotten from the finding.

Result showing the Working Experience of respondents



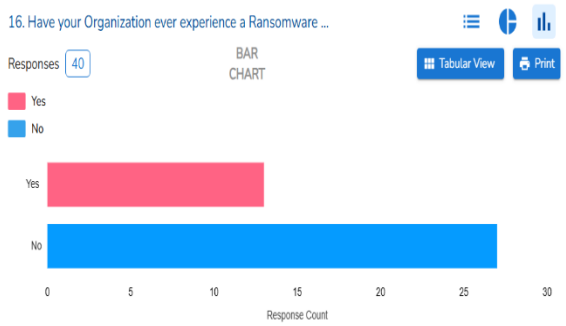
The chart above indicates that the working experience with 2 – 5 years are more affected by ransomware assails, followed by those less than 2 years, 6-10 years while 10 years above are less affected by ransomware assails. The bar chart clearly indicates that the more experience you have in technology, the more secure you become. According to the aforementioned results, the majority of ransomware assails affected are Own Business base on the bar chart presented above and the result gotten from the finding.

Which of These is Being Mostly Targeted for Ransomware Attacked?



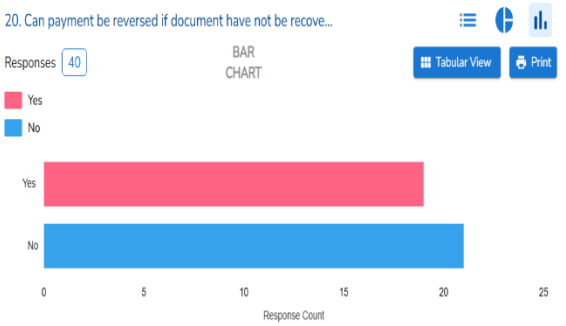
The chart above indicates that both individual and organization are targeted by ransomware assails.

Result showing the Organization experience on Ransomware Attacked?



The chart above shows that people who have now more organization have no experience of ransomware assails.

Can payment be reversed if document have not been recovered?



The chart above indicates that once you are affected by ransomware assails and ransom have been paid, the percentage of getting back your payment is less because the traitor, may not pay back after receiving the money or even released the document.

According to the aforementioned results, the majority of ransomware assails affected may not get back their payment if document not recovered, based on the bar chart presented above and the result gotten from the finding.

CONCLUSION

Lastly, it should come as no surprise that ransomware will change over the next few years to come. If ransomware is not taken seriously, it will be more than simply a software capable of disrupting entire organization infrastructure; it will have the power to

disable an entire city or perhaps a country until the desired ransom is paid (Muslim et al., 2019). Cyber criminals are likely to employ tactics such as hacking industrial control systems (ICS) and other key infrastructure in order to disable ecosystems rather than just networks. Payment systems such as E-bay are among the few possible targets for cyber attackers. In 2016, there was a transit attack in which ransomware targeted a service provider's kiosk. Ransomware has already targeted hospitals and transportation providers. In the future, attackers will be able to target larger targets such as industrial robots that are frequently utilized in manufacturing or infrastructure sectors that connect smart cities (Muslim et al., 2019). Ransomware can be expensive and catastrophic for businesses that are not actively protecting themselves or preparing for the outcome of an attack. As this form of attack becomes more common and develops, it is important for organizations to recognize that they can do to avoid the latest effective attack patterns and sensitivity. By implementing best practice recommendations, businesses can reduce the likelihood of successful ransomware attacks in relation to reaction efforts, downtime, costs, organizational effectiveness, and reputational damage.

REFERENCES

[1] Abdullah Alqahtani and Frederick T. Sheldon (2022), Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving Outlook 2022, *22*(5), 1837; https://doi.org/10.3390/s22051837.

[2] Cristian Pascariu and Daniel Barbu (2019),

[3] Ransomware Honeypot: Honeypot solution designed to detect a ransomware infection identify the ransomware family June 2019 DOI:10.1109/ECAI46879.2019.9042158.

[4] Egyptian Science Magazine. 8 (2): 24-28.

[5] Egyptian Science Magazine. 8 (2): 24-28.

[6] Egyptian Science Magazine. 8 (2): 24-28.

[7] Egyptian Science Magazine. 8 (2): 24-28.

[8] Egyptian Science Magazine. 8 (2): 24-28.

[9] Hassan, M. Younis, Shfika, A. El-Kassabany and Hesham, Z. Ibrahim (2013).

[10] Hassan, M. Younis, Shfika, A. El-Kassabany and Hesham, Z. Ibrahim (2013).

[11] Hassan, M. Younis, Shfika, A. El-Kassabany and Hesham, Z. Ibrahim (2013).

[12] Hassan, M. Younis, Shfika, A. El-Kassabany and Hesham, Z. Ibrahim (2013).

[13] Hassan, M. Younis, Shfika, A. El-Kassabany and Hesham, Z. Ibrahim (2013).

[14] Hassan, N. A. (2019). Enterprise defense strategies against ransomware Strike. Ransomware

[15] Revealed,115–154. https://doi.org/10.1007/978-1-4842-4255-1_5

[16] Inhibition of chloroplast ATPase activity by cyanazine and simazine herbicides. The

[17] Inhibition of chloroplast ATPase activity by cyanazine and simazine herbicides. The

[18] Inhibition of chloroplast ATPase activity by cyanazine and simazine herbicides. The

[19] Inhibition of chloroplast ATPase activity by cyanazine and simazine herbicides. The

[20] Inhibition of chloroplast ATPase activity by cyanazine and simazine herbicides. The

[21] Jennifer C Richardson, Secil Caskurlu and Jing Lv. Social Presence in Relation to Students'

[22] Satisfaction and Learning in the Online Environment: A Meta-analysis, June 2017, Computers in Human Behavior 71:402–417, DOI:10.1016/j.chb.2017.02.001

[23] Mahendran Muniandy, Noor Azma Ismail, Abdulaziz Yahya Yahya Al-Nahari and Danny Ngo Lung Yao (2024), Evolution and Impact of Ransomware: Patterns, Prevention, and Recommendations for Organizational Resilience 14(1), January 2024, DOI:10.6007/IJARBSS/v14-i1/19803

[24] Mahendran, S. A., Wathes, D. C., Booth, R. E. et al. (2024.) Effects of the individual and pair housing of calves on long-term heifer production on a UK commercial dairy farm. Animals 14(1), 125. https://doi.org/10.3390/ani14010125.

[25] Muhammad Ejaz Ahmed, Hyoungshick Kim, Seyit Camtepe, and Surya Nepal (2012) Peeler: Profiling Kernel-Level Events to Detect Ransomware, arXiv:2101.12434[cs.CR], v1 https://doi.org/10.48550/arXiv.2101.12434, [v1] Fri, 29 Jan 2021

[26] Maurya, A. K., Kumar, N., Agrawal, A., & Khan, R. A. (2018). Ransomware evolution, target and safety measures. International Journal of Computer Sciences and Engineering, 6(1), 80–85. https://doi.org/10.26438/ijcse/v6i1.8085

[27] Muslim, A. K., Mohd Dzulkifli, D. Z., Nadhim, M. H., & Haizal Abdellah, R. (2019). A Study of Ransomware Strike: Evolution and Prevention. Journal of social Transformation and regional development, 1(1), 18–25.

[28] Norfaeza Zakaria, Harwati Hashim and Melor Md. Yunus (2019) A Review of Affective Strategy and Social Strategy in Developing Students' Speaking Skills, January 2019, Creative Education 10(12):3082-3090, DOI:10.4236/ce.2019.1012232

[29] Ronny Richardson, and Max M. North, (2017)Ransomware: Evolution, Mitigation and Prevention, 1-1-2017 Journal Title International Management Review, Volume13,Issue 1

[30] Travis Reese, Lior Frenkel and Kent Mcgaughy (2007), Revolutionizing Physical Assets Protection.

[31] Zakaria, W. Z., Abdollah, M. F., Mohd, O., & Ariffin, A. F. (2017). The rise of Ransomware.

[32] Proceedings of the 2017 International Conference on Software and e-Business -ICSEB 2017. https://doi.org/10.1145/3178212.3178224