International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

RATTATA: Ransomware Analysis via Automated Impact Assessment of Philippine Organizations

Aaron Lensmer Abdon[1], Michael Gabriel Del Rosario[2], Jerome Gutierrez[3], Keinaz Domingo[4], Patricia Nicole Ople[5], Sophia Ysabelle Fallarme[6], Sofia Mariel Mitchell[7]

Submitted:14/03/2024 **Revised**: 29/04/2024 **Accepted**: 06/05/2024

Abstract: Contemporarily, Ransomware is a type of malicious software – Malware- that persists and evolves accordingly to organizational countermeasures. It aims to block user access to a system and its data, typically for monetary gain. Two major methods of doing so are the blatant blocking of a system's use and the encryption of these data. This poses a significant threat to organizations, causing major financial losses and disclosure of confidential or sensitive data to unauthorized individuals, as attackers often exfiltrate the data in the process. In the Philippines, the general overview of the cybersecurity landscape has been explored and evaluated. It is observed that the country is particularly lacking in its investment in the field, with a misconception of its insignificance, despite its looming and ever-growing threats. This has caused major data leakages and compromised services in recent years. Despite these existing evaluations, there remains an opportunity to delve deeper into this for a richer understanding. This journal intends to provide the initial groundworks for this, by assessing Ransomware experiences and impacts in Philippine organizations of different sectors and correlating such with existing knowledge. This is particularly conducted by thoroughly evaluating the qualitative data and extracting its key features for its automated categorization.

Keywords: *Attacks, Cybersecurity, Organizations, Philippines, Ransomware, Malware*

1. Introduction

An increasing amount of financially and politically motivated cybercrime is being observed in the Philippines. Significantly, as of 2024, 75% of businesses in the country have already experienced cyber-attacks, with the greatest concern being data loss. The country's government is also placed at 58th and 6th in the global and ASEAN ranking for readiness against cybersecurity threats [1]. Furthermore, the country has a lack of cybersecurity training and a need for improved cooperation of organizations. With the lack of IT security knowledge of Filipino end-users, the country will constantly be vulnerable to cybersecurity threats [2].

To this day, various malicious software - Malware – are still being distributed, one of these are Ransomwares which encrypts a victim's data with some leveraging on the COVID-19 pandemic's relevance [3]. The surface of the cybersecurity landscape of the Philippines has been explored, however, there remains an opportunity to delve deeper. This journal extends the coverage of the knowledge on this landscape regarding the incidents and impacts of Ransomware within different industries through the assessing data gathered from various organizations within the country regarding this, allowing for a better understanding of which.

1.1. Philippine Cybersecurity Landscape

With the ever-increasing digital activities of individuals and organizations in the Philippines, cybersecurity threats also follow. A global cybersecurity firm - Kapersky - estimates a 60% increase of web threats within the country in 2020, with the International Criminal Police Organization (INTERPOL) notably detecting a rise in Ransomware attacks [4]. In August 2023, the Philippine National Police investigated an alarming 16,297 cybercrime cases, noting its ever-evolving nature. Reliance on the internet for commercial activities is closely tied to the surge of cybercrime. The country's close ties with the United States places it as a significant target for politically motivated threats from China, North Korea, and Russia. Recent cases include the Philippine Health Insurance Corporation (PhilHealth) leakage of 1,000 email addresses which affected 13 million people, the Philippine Statistics Authority (PSA) data leak, and the hijacking of the Philippine House of Representatives website [1].

Despite the looming threats, cybersecurity within the country is not prioritized as the country is still in the initial stages of digitalization. Astoundingly, there is also a misconception that the Philippines is not a target for threat actors, this affects the country's lack of investment into cybersecurity. To enable the country to meaningfully participate and benefit from the growing digital economy, cybersecurity must become a key priority [4].

1.2. Ransomware

Ransomware is a popular attack vector that encrypts data within a machine to demand a ransom for its decryption. Two major types of this are Locker which blocks system access from display or keyboard, and Crypto which is much more destructive in ciphering the files of a system [5].

Recipients of ransoms are difficult to track as payments are done through cryptocurrency [3]. Infection vectors were ranked according to their popularity, this can be seen in Table 1. Historically, Windows systems are the most common targets of attacks due to their popularity [6].

Table 1. Ransomware Infection Vectors

Infection Vector	Description
1. Phishing	Uses malicious emails, links, and attachments posing as legitimate.
2. Remote Desktop Protocol (RDP)	Allows for remote control of a system. New vulnerabilities leveraging this keep on arising.
3. Software	Outdated or unpatched software renders a system vulnerable.
4. Web Pages	Ransomware may be automatically downloaded from compromised or illegitimate websites.
5. Pop-Ups	May trick users into downloading Ransomware or redirecting them to malicious links.

Another infection vector of Ransomware includes Social Engineering, which aims to exploit the built trust of legitimate personnel. Table 2 shows the several ways of its execution [7].

Table 2. Social Engineering Attacks

Attack	Description
1. Technical	Disguise as a known and reliable entity.
2. Ego	Displays intelligence for trustworthiness.
3. Sympathy	Displays empathy for trustworthiness
4. Bullying	Utilizes fear for coercion.

Incidents related to Ransomware double every year and adapt to organizational security measures [8]. A relevant example of Ransomware is CovidLock, it leveraged on COVID-19 by disguising itself as a pandemic statistics monitoring application [3]. Another is WannaCry which spread to 150 countries in 2017, there is still no countermeasure for this as of 2020 [8]. Various organizations and sectors can be affected by Ransomware. In 2022, Nvidia became a victim of a Ransomware attack by the Laspus group, employee and proprietary data were leaked online. In the same year, the Costa Rican Government suffered a major ransomware attack by the Conti group which became a nationwide emergency, the Department of Finance and business activities were affected [9]. Numerous studies and works have already explored Ransomware detection and prevention through conducting static and dynamic analyses on various parts of a system. However, these are useless if an infection has already occurred [6].

With this, this journal intends to provide the initial groundworks and context of Ransomware in Philippine organizations of varied sectors for future studies to delve further into.

2. Methodology

Interviews were conducted with multiple cybersecurity experts in the field, utilizing a qualitative approach in terms of data collection through a structured questionnaire to explore the impacts of ransomware attacks in the Philippine context. Purposive sampling was employed to determine respondent eligibility, ensuring that the selected participants have had firsthand experience in handling cybersecurity incidents.

2.1. Qualitative Research

A predetermined set of questions was formulated to ensure the consistency and comparability of the respondent input. Table 3 shows the relevant questions in deriving the key data.

Table 3. Key Interview Questions

1. What characterizes a ransomware attack?
2. What attack vectors are usually taken advantage of by threat actors on cybersecurity incidents determined to be primarily caused by ransomware?
3. What strategies are generally employed to ensure a swift recovery from a breech, especially from a company standpoint?
4. What preventative measures are typically implemented to minimize risks involving cybersecurity incidents?

After a series of interviews with trained professionals, five respondents were determined to be most appropriate for the given study. The selection was made following the basis of respondent-knowledge correlation to employ both relevance and accuracy, further ensuring that the insights gathered reflect the actual incident response practices in the field.

2.2. Data Preprocessing

To ensure the accuracy of processed data, manual data cleaning was employed to consolidate similar responses and eliminate redundancy. The dataset was then standardized to maintain uniformity for subsequent analyses.

Python was then used to facilitate dataset organization and provide informative visual representation of the relevant metrics for comparison. Multiple libraries such as pandas and matplot.lib were utilized to manage and manipulate data to illustrate emerging trends for evaluation.

3. Grounded Theory

A Grounded Theory is a flexible qualitative method for developing theoretical patterns from an empirical data set. It involves the aggregation of data into meaningful parts – coding – which is common in qualitative studies. It generally starts with a pre-literature review and determination of the research area. After which, the data will be collected with theoretical sampling for sources that show potential. The extracted data will be coded and finally, the findings will be correlated to the reviewed literature to form the theory [10]. This journal follows this method by foremost identifying the research gap on Ransomware in the Philippines, after reviewing contemporary literatures regarding it and evaluation of the country's cybersecurity landscape on a surface-level. Theoretical sampling was conducted by selecting respondents which may be experienced and knowledgeable enough in the matter. Coding was executed through the identification of key data from the interviews. Finally, the findings were connected to the reviewed literature. The theory of this journal is discussed by its hypothesis.

4. Results and Discussion

4.1. Data and Observation

An overview of the key observations and identified trends are to be discussed in detail in the following sections.

4.1.1. Data

Classifications on whether a particular response is either major or minor would depend on their frequency of occurrence. To classify a response as a major input, it must be cited by at least three of the selected respondents.

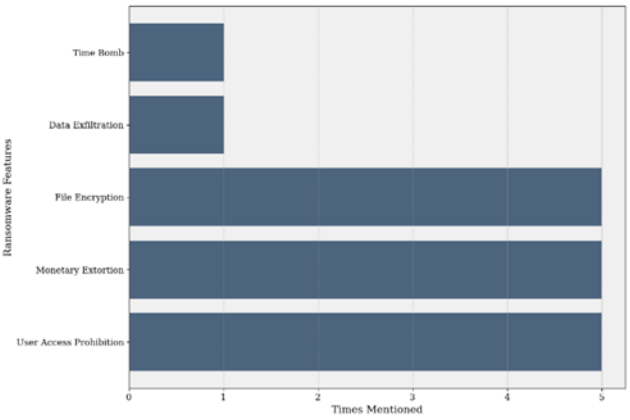

Fig 1, Frequency of cited recurrent ransomware features

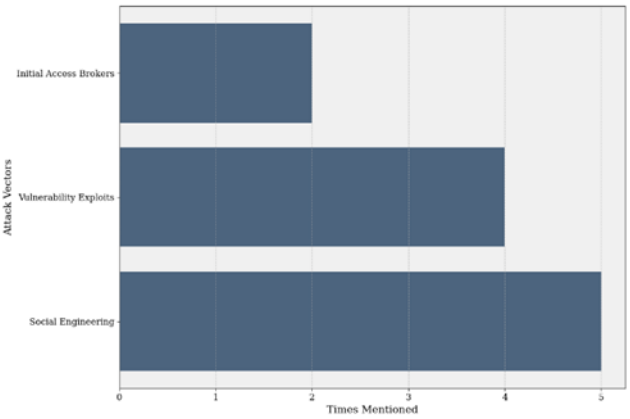

Fig 2, Frequency of cited methods used by threat actors to initiate cybersecurity attacks involving ransomware

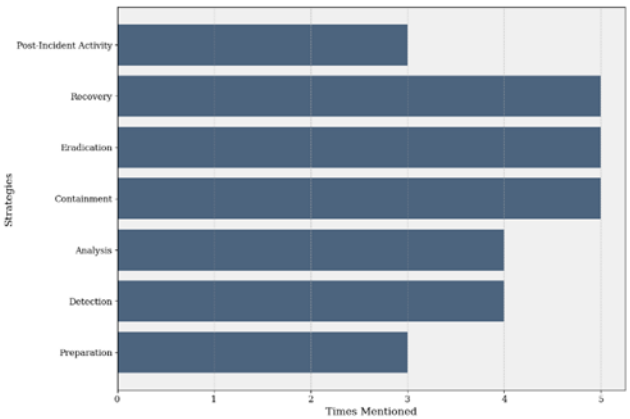

Fig 3, Frequency of cited employed strategies to deal with and resolve cybersecurity incidents involving ransomware

4.1.2. Observation

This section highlights key observations, focusing on identified patterns and trends that form the basis for further analysis.

Table 4. Recurrent Ransomware Feature Classification

Major	Minor
1. Data Exfiltration	1. Time Bomb
2. Monetary Extortion	2. Data Exfiltration
3. User Access Prohibition	

Table 4 outlines the classification of recurrent ransomware features; categorizing entries into major and minor classifications. Those consistently mentioned by all respondents include File Encryption, Monetary Extortion, and User Access Prohibition.

Table 5. Attack Vector Classification

Major	Minor
1. Social Engineering	1. Initial Access Brokers
2. Vulnerability Exploits	

In terms of attack vectors, Social Engineering predominantly appears across all respondent claims – solidifying its prevalence as the method of choice used by threat actors in their attempts to gain access to a computer system. Table 5 also includes parallel entries for Vulnerability Exploits and Initial Access Brokers.

Table 6. Recovery Strategy Frequency

Strategy [1/2]	CT	Strategy [2/2]	CT
1. Recovery	5	5. Identification	4
2. Eradication	5	6. Post-Incident Activity	3
3. Containment	5	7. Preparation	3
4. Analysis	4		

Incidentally, all seven recovery strategies appear to have been mentioned a significant number of times, relative to the number of available respondents, for all entries to fall under the major classification.

4.1.3. Discussion

Prior to data cleaning, respondents were able to provide a considerable amount of commonly used cybersecurity terminologies. Social Engineering, for example, as referenced in Fig. 2, serves as an umbrella term for respondent mentions of Phishing, Vishing, Smishing, and many other methods that employ deceptive means on individuals to providing sensitive information. Likewise, there have also been mentions of Zero-Day Exploits on unpatched systems as well as certain variants of ransomware that have trojan and worm-like properties for Vulnerability Exploits.

Generally, from what can be surmised using the given dataset – Monetary Extortion, as referenced in Fig. 1, would refer to the typical feature of a ransomware to demand payment from affected entities. While Bitcoin serves as the primary mode of payment requested by threat actors, another aspect of ransomware is its inclusive nature – allowing for the acceptance of cheques, credit, and the like. Despite being classified as a minor feature, Initial Access Brokers remain to be an emergent cause in the popularity of ransomware attacks [11]. These external entities are responsible for providing leased access to ransomware-capable code/software, usually benefiting a certain percentage of the total earnings from the fraudulent activity.

Figure 3 further covers the recovery strategies employed by the respondents during a ransomware attack. Following the NIST SP 800-61 publication [12], responses were standardized and split into seven distinct categories. Respondent entries concerning Telemetry, Endpoint Isolation, and Persistence Eradication were standardized into Preparation, Containment, and Eradication respectively. Consequently, the Recovery aspect factors in mentions of the use of backups and/or system snapshots as well as the clean restoration of both the affected files and the file system functionality. It should also be noted that various analysis methods such as the Root-Cause Analysis were frequently mentioned throughout the course of the interview across multiple respondents.

4.1.4. Patterns and Relationships

Given the centricity of respondent answers to File Encryption, Monetary Extortion, and User Access Prohibition for recurrent ransomware features as seen in Fig. 1, it can be hypothesized that cybersecurity attacks tend to primarily exhibit tactics that leverage coercion to meet threat actor demands. This is further supported by the results on common attack vectors as shown on Fig. 2, where the weakest link is exemplified to be the human factor via Social Engineering.

In terms of recovery strategies, while all entries appear to have been consistently mentioned by all respondents, focus is greatly placed on the containment of the attack to minimize the damage caused by the threat actor, eradication of persistence methods to prevent further exploits, and the over-all recovery of affected files and restoration of system functions.

4.2. Comparison with Contemporary Literature

The data's major features of Ransomware align with the types of which. File Encryption aligns with Crypto Ransomwares while User Access Prohibition aligns with Locker. Monetary Extortion aligns with the typical demand for ransom [5]. Notably, modes of payment include bitcoin which aligns with the typical use of cryptocurrency [3], alongside cheques.

As for the major Attack Vectors, Social Engineering aligns with its use in Ransomware infection [7]. Vulnerability Exploits aligns with those in infection vectors like software [3].

All strategies align exactly with the main stages of an Incident Response strategy [11], Table 6 shows these aligned strategies and their descriptions.

Table 6. Stages in an Incident Response Strategy

Strategy	Description
1. Preparation	Evaluation of the adequacy and potential gaps in the implemented security controls.
2. Identification	Discovery of signs of malicious activity.
3. Analysis	Determination of Ransomware type and tactics used. Reverse-engineering may be involved.
4. Containment	Prevention of further infection.
5. Eradication	Erasure of any trace of Ransomware. Also identifies the indicators and tactics used for compromise.
6. Recovery	Restoration of impacted resources.
7. Post-Incident Activity	Learning from gaps, security logs, practices, and response strategy.

4.3. Contextualization

Since the recent COVID-19 pandemic, the global trend of attackers taking advantage of new opportunities has accelerated. Ransomware has become a service in which operators rent out such to attackers for a fee or percentage of the ransom. It is a modern transnational organized crime that has become a growing multi-billion-dollar industry. Various operators and brokers serve a role in the execution of a Ransomware attack, Table 7 shows this [13]. The Philippines is not an exception to being a part of this context, Ransomware attacks within the nation could very well be a part of this new industry. Future studies may delve deeper into the Philippine context of the matter, with this journal's established groundwork for such.

Table 7. Cybercrime Operators and Brokers

Role	Description
1. Databrokers	Trades stolen data, including personal profiles.
2. Crimeware-as-a-service	Rents out malware for attackers, including Ransomware.
3. Darkmarketeers	Trades malicious services.
4. Bullet Proof Hosters	Hosts networks and sites allowing unrestricted content (i.e. data leaks).
5. Monetisers	Converts laundered cryptocurrency to flat currency for a fee.
6. Bug Brokers	Sells malicious codes and vulnerabilities.
7. Negotiators	Negotiates ransom with the victim from the attacker's side.

5. Conclusion

Responses elicited from cybersecurity professionals throughout the course of the study reveal that threat actors predominantly exploit human vulnerabilities through social engineering. The latter further leverages upon the susceptibility of humans and their potential lack of awareness and security training to obtain sensitive information and breech security systems. Should their efforts fail, they then rely on zero-day exploits and other various vulnerabilities that unpatched systems pose to their users

The recurring themes: file encryption, monetary extortion, and user access prohibition highlight the coercive nature of ransomware attacks. As part of experts' incident response plans, mitigation and damage control strategies primarily focus on containment, eradication, and recovery among all others. These findings exemplify the need to educate the vast majority of people and strive for continued vigilance

against evolving threats in the field of cybersecurity.

6. Recommendations

A larger sample size is recommended to generate a more comprehensive understanding of the impact of cybersecurity threats, particularly that of ransomware attacks. Additionally, further investigative efforts may be conducted in the form of comparative analyses between incident response strategies of two or more Philippine-based cybersecurity firms to better assess the knowledge and incident response capacities of professionals within the local context.

Acknowledgements

Deepest gratitudes are extended to Bernardo, Juan Pablo C., and Folkard, Sean Michael from De La Salle University Manila for their invaluable assistance with the interviews during the data gathering process. While they may not concur with all surmised interpretations, their contributions were crucial in terms of providing the information needed for this research.

References

[1] D. J. Dacanay, J. Fajutagana, M. S. Quinto and F. Parayno, "A Comparative Study of the Philippines in a Global Cybersecurity Context and its Implications on Local Cybersecurity Practices," May 2024. [Online]. Available: ResearchGate.

[2] C. D. Qmorog and R. P. Medina, "Internet Security Awareness of Filipinos: A Survey Paper," November 2020. [Online]. Available: ResearchGate.

[3] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak and M. K. Khan, "Ransomware: Recent Advances, Analysis, Challenges, and Future Research Directions," December 2021. [Online]. Available: PubMed.

[4] Secure Connections, "Cybersecurity in the Philippines: Global Context and Local Challenges," March 2022. [Online]. Available: The Asia Foundation.

[5] J. G. Hernandez, L. A. Gonzalez and P. D. Teodoro, "R-Locker: Thwarting Ransomware Action through a Honeyfile-based Approach," March 2020. [Online]. Available: ResearchGate.

[6] S. Razaulla, C. Fachka, C. Markarian, A. Gawanmeh, W. Mansoor, B. Fung and C. Assi, "The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions," April 2023. [Online]. Available: IEEE Xplore.

[7] P. G. Segovia, J. F. Torres, V. L. Rosillo, P. V. Tapia, I. Y. Albarado and J. J. Saltos, "Social Engineering as an Attack Vector for Ransomware," October 2017. [Online]. Available: IEEE Xplore.

[8] H. M. Puat and N. A. Rahman, "Ransomware as a Service and Public Awareness," November 2020. [Online]. Available: PalArch.

[9] M. Cen, F. Jiang, X. Qin, Q. Jiang and R. Doss, "Ransomware Early Detection: A Survey," December 2023. [Online]. Available: ScienceDirect.

[10] M. Yu and S. M. Smith, "Grounded Theory: A Guide for a New Generation of Researchers," July 2021. [Online]. Available: ResearchGate.

[11] P. Bajpai and R. Enbody, "Know Thy Ransomware Response: A Detailed Framework for Devising Effective Ransomware Response Strategies," October 2023. [Online]. Available: ACM Digital Library.

[12] P. Cichonski, T. Miller, T. Grance and K. Scarfone, "Computer Security Incident Handling Guide," vol. 800, no. 61, August 2012.

[13] D. S. Wall, "The Transnational Cybercrime Extortion Landscape and the Pandemic: Changes in Ransomware Offender Tactics, Attack Scalability, and the Organisation of Offending," August 2021. [Online]. Available: Elsevier.