International Journal of Multidisciplinary Research and Growth Evaluation.

A Cybersecurity Study on Zero-Day Ransomware Mitigation through Threat Intelligence Sharing Platforms

Roy Okonkwo [1*], Steve Folorunso [2], Ibrahim Olasege [3], Job Adegede [4], Kuceli Susan Englama [5]
[1] Department of Information Technology, North Carolina A&T State University, United States
[2] University of Liverpool United Kingdom, United Kingdom
[3] Department of Electrical & Computer Engineering, North Carolina Agricultural and Technical State University, United States
[4] Independent Researcher, USA
[5] Department of Computer Science, Cornell University, New York

* Corresponding Author: **Roy Okonkwo**

Article Info

ISSN (online): 2582-7138
Volume: 04
Issue: 02
March - April 2023
Received: 02-03-2023
Accepted: 03-04-2023
Published: 20-04-2023
Page No: 889-897

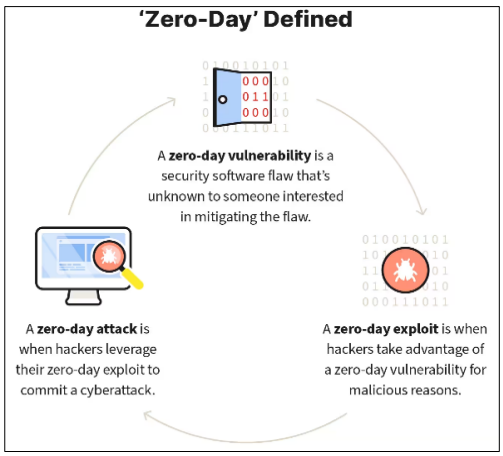
Abstract
The present study focuses on the volatile character of the zero-day ransomware risks, bringing into focus the preventive measures and importance of threat intelligence sharing platforms. Through studying related cases, especially the Maersk NotPetya attack, it is evident how the threat actors are adjusting their tactics. Recommendations are on the creation of collaboration, the standardization of the protocols, the preservation of privacy, and sector-specific tailoring. This in turn helps cyber security specialists implement a strategic plan to cope with zero-day ransomware threats, highlighting the necessity of an allied defence enabled by information-sharing platforms.

DOI: https://doi.org/10.54660/.IJMRGE.2023.4.2.889-897

Keywords: Zero-Day Ransomware, Threat Intelligence Sharing Platforms**,** Vulnerability

1. Introduction

Increasingly, nowadays organizations suffer from a wave of complex cybercrimes that lead to service interruptions, loss of sensitive data, or enable criminals to use victim machines and networks to execute their malicious activities. These malicious imposters are after business property to steal, wreck, or compromise it, particularly with financial, reputational, or intellectual values at stake. The complexity and pattern of cyberattacks in the ever-growing IT field endanger the security of digital systems (Preuveneers & Joosen, 2021).



Source: (Hunter, 2022)

Fig 1: Zero-day vulnerability

Zero-day vulnerabilities are particularly noteworthy among these threats because of the lack of detection and their susceptibility to causing huge harm Zero-day ransomware, a fast-changing type of cyber threat, is malicious software that exploits undisclosed vulnerabilities (zero-day vulnerabilities), before a fix or defence is available (Preuveneers & Joosen, 2021). Due to the tremendous development of interconnected systems, the consequences of zero-day ransomware have been a serious issue in cybersecurity. The evolution of ransomware attacks has seen a movement from simple encryption techniques to more advanced and tailored strategies which make traditional security measures less effective (Hunter, 2022).

This study was initiated due to the high increase in incidences of sophistication as well as the frequency of zero-day ransomware attacks. The dynamic nature of these attacks creates a serious issue for traditional cybersecurity frameworks. The rising financial and operational destruction caused by these attacks gives a clear indication that reactive measures are no longer enough. Traditional security strategies tend to be ineffective when it comes to zero-day threats because of the unpredictable nature of this type of threat, underlining the need for innovative and preventive solutions (Preuveneers & Joosen, 2021).

Several research objectives have been set for this research including the following:

- To assess the current landscape of zero-day ransomware threats.
- To evaluate the effectiveness of existing mitigation strategies.
- To investigate the role of threat intelligence sharing platforms in preventing zero-day attacks.
- To propose recommendations for organizations to enhance their resilience against zero-day ransomware.

The field of this study covers a complete study of zero-day ransomware threats and the remediation strategies through threat intelligence sharing platforms The study objective is to offer valuable insights; however, there are certain limitations that exist, for example, the dynamic nature of cyber threats and the ever-changing tactics of threat actors. The study acknowledges these limitations but highlights practical and actionable recommendations for cybersecurity practitioners and organizations (Hunter, 2022).

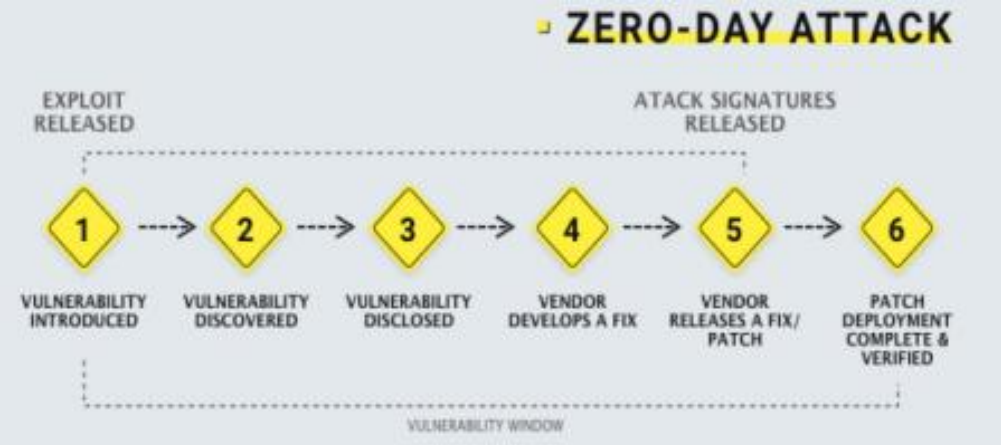
2. Overview of Ransomware

Ransomware has however shifted from simple and indiscriminate attacks to sophisticated and targeted campaigns posing serious threats to organizations across the globe. Significant occasions highlight the seriousness and consequences of ransomware (Rains, 2023). In the May 2017 attack, WannaCry compromised over 200,000 computers with Windows OS in more than 150 countries, successfully lodged into the vulnerability offered by Windows (Preuveneers & Joosen, 2021). The attack shut down critical infrastructures, such as healthcare facilities and enterprises, underlining the spread effects of ransomware (Guarascio *et al*., 2022).

Ransomware of different types possess specific features; for instance, CryptoLocker is a file-encrypting malware that encrypts files and demands a ransom for decryption keys while Winlocker is a locker ransomware that restricts access to the system (Rains, 2023). Apprehending these variations is paramount for the success of anti-countermeasures. The 2019 Ryuk ransomware attacks clearly showed a shift to the more targeted approaches (Guarascio *et al*., 2022). Ryuk precisely targeted tier 1 organizations, implementing sophisticated methods to gain access to their networks. It shows the dynamic nature of ransomware that makes changes to the existing cybersecurity technologies a necessity.

2.1 Zero-Day Vulnerabilities

The human element of zero-day vulnerabilities in ransomware attacks is that it grants threat actors the ability to profit from the exploitation of software or hardware bugs while allowing software developers to distribute patches after the fact. “Zero-day” denotes that things are arranged intentionally, so that organizations get zero days to prepare, thereby making these vulnerabilities effective weapons for cybercriminals (Rains, 2023). Detection and prevention of zero-day exploits is one complex issue because of their stealthy nature. Unlike known vulnerabilities with available patches, zero-day vulnerabilities lack well-established defences that make it possible for attackers to bypass traditional security measures. This game of cat and mouse implies a proactive stance, centering on threat anticipation instead of reaction (Guarascio *et al*., 2022).



Source: (Ekong *et al*., 2023)

Fig 2: Flow chart representation of Zero-day vulnerability Life cycle

For example, the Stuxnet worm, found in 2010, used multiple zero-day vulnerabilities to attack supervisory control and data acquisition (SCADA) systems. Iran's nuclear program suffered considerable damage from this presumed state-

backed cyberattack. The Stuxnet incident illustrates the power and effectiveness of zero-day vulnerabilities in mounting targeted and destructive attacks (Ekong *et al*., 2023).

2.2 TISP (Threat Intelligence Sharing Platforms)

The importance of threat intelligence sharing platforms to protect organizations against the persistence of ransomware attacks cannot be overemphasized in the dynamic cybersecurity arena. These platforms act as dynamic ecosystems that help in the timely exchange of actionable threat data between the diverse cybersecurity communities, thereby forming a collective defence against the ever-changing threats.

1. **Cyber Threat Alliance (CTA):** The diversity among threat intelligence sharing platforms can be observed in both public and private initiatives. Showing excellent initiative in the private sector is the Cyber Threat Alliance (CTA), a consortium of major cybersecurity vendors (Azzedin *et al*., 2022). CTA serves as a representation of cooperative initiatives involving industry leaders joining hands to collectively pool and exchange their Time Critical Actionable Information. In this way, member organizations are jointly proactive in monitoring and overcoming difficulties ahead. The CTA's model, however, goes beyond emphasizing cooperation but also highlights that in the event of a fast-changing threat landscape, a united force is more powerful than separate defences (Nkongolo *et al*., 2021).
2. **Information Sharing and Analysis Centers (ISACs):** Similarly, Information Sharing and Analysis Centers (ISACs) are also major players in the threat intelligence sharing scene. Acting as sector-specific platforms, ISACs like the Financial Services ISAC (FS-ISAC) hold a critical role in increasing threat awareness within their respective industries (Azzedin *et al*., 2022). These platforms are a platform for companies to exchange the threat intelligence that applies to their industry, allowing them to create a targeted defence approach. For example, the financial sector encounters specific threats not experienced in the healthcare sector, and ISACs provide solutions for the unique challenges in each sector (Nkongolo *et al*., 2021).
3. **Indicators of compromise (IOCs):** The effectiveness of threat intelligence exchanges in thwarting zero-day ransomware attacks is dependent on their capacity to provide relevant and timely threat intelligence to their member organizations. Indicators of compromise (IOCs), key elements marking potential threats, take a central position (Azzedin *et al*., 2022). The fast and widespread of the IOCs associated with a new ransomware strain enables organizations to proactively update their security controls, thus, strengthening their defences against emerging threats. The essential importance of these platforms in reducing the effect of ransomware is shown by the 2017 NotPetya incident (Nkongolo *et al*., 2021).

   For NotPetya, the hackers used the zero-day vulnerability in Ukrainian accounting software which caused a wave of turbulence spreading overseas and disrupting organizations across the globe. If there had been a more efficient, all-inclusive threat intelligence sharing framework in place, the associated indicators of zero-day vulnerability would have been distributed promptly (M Buksov, 2020). It allows global organizations to strengthen their defence system and probably avert the attack before it gets unleashed. This emphasizes the crucial need for progressive and constant improvement of threat intelligence platforms in the current fight against advanced cyber threats (Ryan, 2020).

   Nevertheless, the road to ultimate effectiveness is filled with challenges that call for careful analysis. The main challenges include the privacy and confidentiality of data that is shared. Organizations usually struggle with the ratio of sharing meaningful threat intelligence and safeguarding proprietary or confidential data. This balance should be struck by providing clear guidelines, trust-building mechanisms, and, probably, the use of anonymization techniques to ensure open collaboration without harming confidentiality (M Buksov, 2020). The other critical challenge is the need for standardization of data formats across many threat intelligence sources. The lack of commonality could be a hindrance to the smooth flow and integration of threat intelligence. Standardizing protocols leads to effective sharing, processing, and integration of threat data into existing security infrastructures across different platforms. Moreover, the incorporation of threat intelligence into the pre-existing security platforms is a technical issue. Compatibility with different cybersecurity tools and systems is an important requirement for organizations to derive more benefits from shared threat intelligence data. Such initiatives require the continuation of efforts in developing interoperability standards and building joint cooperation ties between threat intelligence-sharing platforms and cybersecurity product manufacturers (Ryan, 2020).

3. Methodology

3.1 Data Collection

The approach used in this research is largely derived from secondary sources, which include a thorough examination of case studies, incident reports, and threat intelligence feeds. Such sources also contain numerous real-life cases for empirical data and thus a cognizant analysis of the forces affecting the threat intelligence sharing forums (Elsayed, 2020). Cases of famous cyber incidents such as the WannaCry and NotPetya attacks provide an invaluable perspective on the effect of ransomware and the role played by sharing threat intelligence in mitigating such threats. Cybersecurity reports, put out by the industry and government agencies, add another level of understanding about the tactics, techniques, and procedures (TTPs) used by attackers. Additionally, by using threat intelligence feeds from sources, a current and changing view on cyber threats is enabled. These feeds are designed to aggregate and disseminate information on indicators of compromise (IOCs), for a real-time assessment of the threat landscape. Adding various sources guarantees a comprehensive and multidimensional approach to data gathering, adding to the study's strength (H. R. & Aithal, 2022).

3.2 Data Analysis

The analysis methodology employed for assessing the performance of threat intelligence sharing systems is based on a qualitative study of the findings obtained from the

gathered data. This analysis does not use particular software tools but adopts a systematic and logical approach to get useful conclusions (Elsayed, 2020). The performance of threat intelligence sharing platforms is assessed using key performance indicators (KPIs) which are extracted from the literature and expert opinions. Metrics including the speed of information propagation, the consistency of the threat intelligence shared with the reality, and the effect of such sharing on the incident response times are systematically evaluated. Through the qualitative scrutiny of these metrics crosswise numerous case studies and incidents, a sophisticated comprehension of the performance of the platforms comes to light (H. R. & Aithal, 2022).

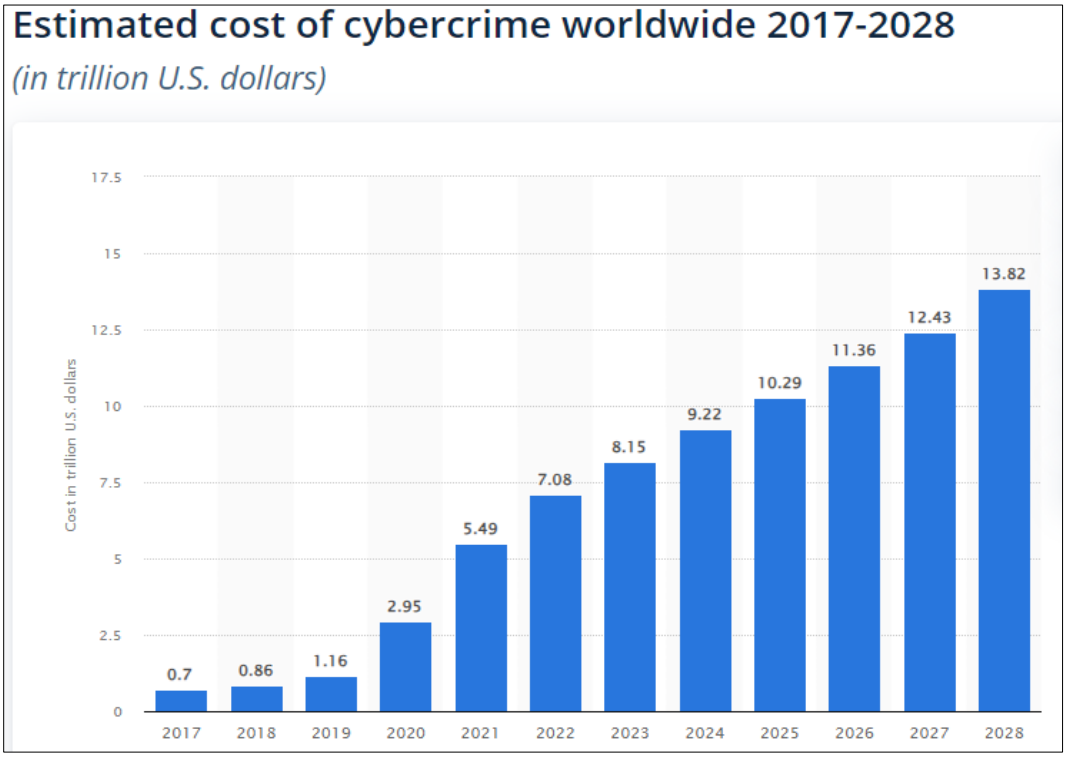
Taking, for example, the analysis is about how fast the threat intelligence shared via platforms such as the Cyber Threat Alliance (CTA) or ISACs reaches affected organizations in particular ransomware incidents (Elsayed, 2020). The interrelation between the timely distribution of threat intelligence and the following attack mitigation will highlight the platforms' real utilization. Moreover, the study also looks at the collaborative element of threat intelligence sharing, assessing how what is shared within cybersecurity communities is converted into actionable defence mechanisms. This also deals with the evaluation of how organizations incorporate shared threat intelligence into their existing security postures and the consequent capabilities to stop or react to zero-day ransomware threats (H. R. & Aithal, 2022).

This qualitative analytical approach aims to provide an in-depth understanding of the tangible advantages and challenges of threat intelligence-sharing platforms, without referring to any specific software tools. This method provides a systematic and logical assessment that is based on real-world case studies and empirical data which in turn improve the research findings' validity and credibility.

4. Result and Discussion

Results

The cyber threat landscape is constantly evolving, and the recent trends of zero-day ransomware attacks demonstrate a sobering advancement. Threat actors are increasingly leveraging newly developed tactics to exploit vulnerabilities before they are discovered and patched (Zahoora *et al*., 2022). A very popular trend is the adoption of polymorphic malware that keeps changing its code to escape traditional signature-based antivirus detection. This flexibility allows attackers to constantly be one step ahead of the security measures. Furthermore, the increase in double-extortion incidents is remarkable. Threat actors not only encrypt but also threaten to publish data unless the ransom is paid. The used tactics in these attacks show a strategical shift towards money maximization, and victim exploitation through psychological pressure.

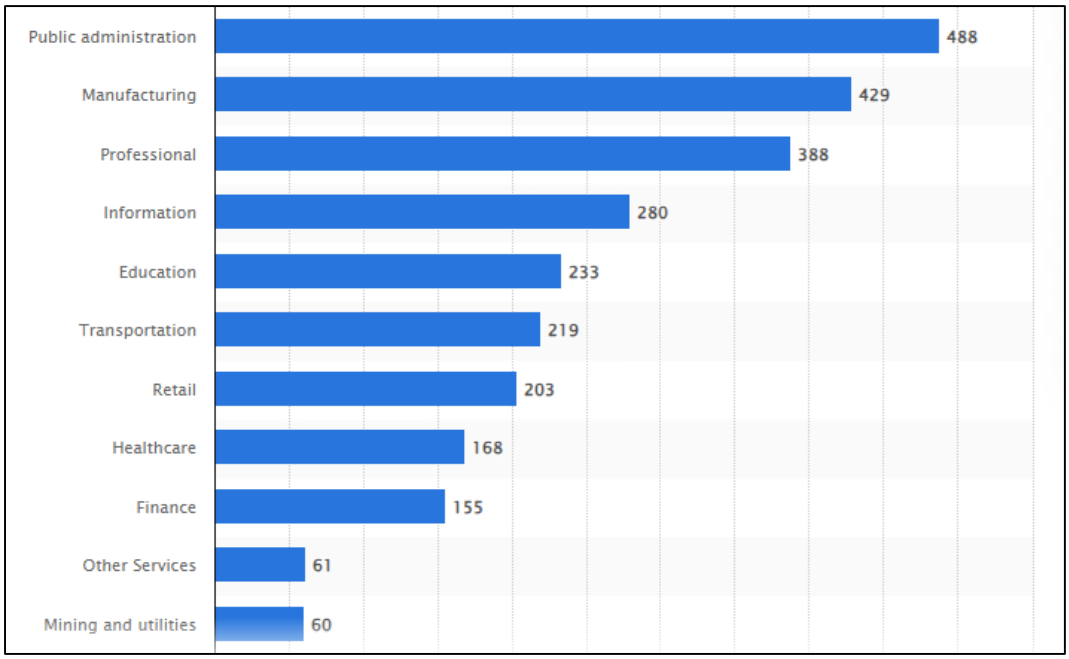


Source: (Kapoor *et al*., 2021)

Fig 3: Estimated cost of cybercrime worldwide 2017-2028 (in trillion US $)

The Colonial Pipeline ransomware attack in 2021 in an unfortunate situation (Zahoora *et al*., 2022). The group behind the attack, DarkSide, exploited a zero-day vulnerability in the pipeline's VPN, thus shutting down its critical infrastructure and creating fuel shortages across the U.S. This incident has shown us how precisely exploited zero-day vulnerabilities can cause major disruption. Another substantial case is the Triton/Trisis attack on a Saudi Arabian petrochemical plant in 2017 (Saprykin, 2021). The advanced attack was directed at the industrial control systems (ICS) and, by utilizing a zero-day vulnerability, was aimed at influencing the safety systems. The incident could have been far worse, which highlights the perils of zero-day ransomware, and not just some data but also human lives are at risk (Saprykin, 2021).

Potential Targets



Source: (Özdemir, 2021)

Fig 4: Worldwide industry sectors most targeted by malware attacks from November 2021 to October 2022

Some industries and sectors are specifically susceptible to zero-day ransomware attacks because of their strategic value and interdependent structure. Take, for instance, in healthcare, the number of attacks has increased. The criminals use exploits to deny services, steal data, and extort huge ransoms (Saprykin, 2021). The interoperability between medical devices and systems makes this industry a good point of attack. Likewise, the critical sector covering energy and water supply systems also provides an attractive target to the bad actors wishing to abuse zero-day vulnerabilities. The interdependency of these systems amplifies the probability of cascading failures with severe results (Kapoor *et al*., 2021).

Discussion

1. Threat Intelligence Sharing Platforms: Orchestrating Collective Defence

Threat intelligence-sharing platforms play an essential role in defending organizations from the fast-changing threat landscape. The Cyber Threat Alliance (CTA), to give a perfect example, is an initiative of cybersecurity companies to provide each other with timely threat intelligence (Saprykin, 2021). This private initiative enables the pooling of resources between member organizations so that they can reactively guard against new risks. Unlike ISACs which are tailored for industry-specific threat landscapes, such as the FS-ISAC, they increase the awareness of the threat to many more people from the same sector (cycles & Text, 2023).

Features and Capabilities: The strength of threat intelligence sharing platforms in the fight against zero-day ransomware lies in their unique features and capabilities. Rapid information diffusion is a crucial element, enabling IOCs associated with new ransomware strains to reach organizations in time (Saprykin, 2021). The dynamics of these platforms make real-time collaboration possible, allowing organizations to rapidly update their defences. Additionally, these platforms usually supply context-rich threat intelligence, giving details about the tactics, techniques, and procedures (TTPs) used by threat actors. This contextual information increases the adaptability of organizations in adjusting their security postures and predicting the changing threats. For example, learning the TTPs implemented by the zero-day ransomware attack last month enables the organizations to reinforce their specific vulnerabilities/weaknesses targeted by the threat actors (cycles & Text, 2023).

Challenges

Despite their significant contributions, cloud-based threat-sharing systems face challenges in attaining the optimum effect. The balancing act on the privacy aspects of shared information is a tricky one. Organizations need to walk on the very thin line between providing valuable threat intelligence and protecting sensitive data (Özdemir, 2021). The creation of trust based on clearly defined guidelines and anonymization techniques is indispensable for the facilitation of collaboration without sacrificing confidentiality. Normalizing data structures is another problem, preventing smooth exchange and integration of threat intelligence. With no uniformity, the scope for advantages of common threat data is restricted. Efforts to introduce common procedures will achieve interoperability and promote the fusion of threat data into different security infrastructures (Kumar & Subbiah, 2022).

2. Mitigation Strategies: Crafting Resilient Defences Against Zero-Day Ransomware Threats

1. **1 Proactive Measures:** Preventing zero-day ransomware attacks means having a proactive approach to security that is not limited to traditional protection methods. Primarily, regular and comprehensive vulnerability assessments should be a priority for organizations. Pinpointing and remedying probable vulnerabilities in software and systems reduces attack surface substantially (Ilca *et al*., 2023). Furthermore,

firm network segmentation should be carried out. This approach cripples the lateral movement of threat actors within a network narrowing the possible impact of a successful compromise. Air-gapped backups, stored safely and tested for restoration are the last line of defence in case of a ransomware incident, guaranteeing data recovery without surrendering to extortion (Kumar & Subbiah, 2022).

The principle of least privilege should determine access controls, allowing users and systems access only to the permissions required for their roles. Equally essential regular security awareness training to foster a security-aware culture and lower the chance of phishing is social engineering, a common vector of zero-day ransomware attacks (Ilca *et al*., 2023).

2. **Role of Threat Intelligence Sharing:** Threat intelligence sharing platforms significantly contribute to protecting organizations from zero-day ransomware. Organizations can exploit shared threat intelligence to have an integrated benefit on the rise of a prepared response. The real-time traffic of indicators of compromise (IOCs) correlated with zero-day vulnerabilities enables organizations to update their responses immediately (Kumar & Subbiah, 2022). A key contribution is the capability to pre-emptively adjust the security postures based on the TTPs identified in previously observed attacks. Such as, if a threat intel-sharing platform warns about a new zero-day ransomware variant targeting a specific vulnerability, organizations should tailor their security parameters to answer the identified TTPs. Furthermore, collective intelligence presents about the changing nature of the threat landscape. Knowledge of threat actors' motives and tactics enhances organizations' ability to predict and defend against zero-day ransomware attacks. Through this common pool of knowledge, organizations solidify their defence against the unforeseeable nature of these threats (Ilca *et al*., 2023).

3. Best Practices

To enhance resilience against zero-day ransomware, organizations should adopt a multifaceted approach that comprises the following:

1. **1 Continuous Monitoring and Anomaly Detection:** Implement continuous monitoring to detect unusual patterns or activities that may indicate a zero-day ransomware attack. Anomaly detection systems can help identify deviations from normal behavior, triggering timely responses (Deochakke & Tyagi, 2022).
2. **Incident Response Planning and Endpoint Security:** Develop and regularly update incident response plans specifically tailored for zero-day ransomware incidents. This ensures a swift and coordinated response, minimizing the potential impact of an attack. Strengthen endpoint security by deploying advanced endpoint protection solutions capable of detecting and blocking zero-day threats. Behavioral analysis and heuristics can identify malicious patterns indicative of zero-day attacks (Vasani *et al*., 2023b).
3. **Regular Security Audits and Collaboration:** Conduct regular security audits to assess the effectiveness of existing security measures. This includes reviewing access controls, patch management processes, and overall network security posture. Actively participate in threat intelligence sharing communities and platforms. Collaborating with industry peers enhances collective situational awareness, enabling organizations to stay ahead of emerging threats (Deochakke & Tyagi, 2022).
4. **Case Studies on Successful Mitigation: " Maersk NotPetya Incident"**

The 2017 NotPetya attack on Maersk stands as an emblem of effective mitigation through the proper use of threat intelligence sharing (Vasani *et al*., 2023b). At first, disguised as a typical ransomware attack, the way of offensive mutated into a destructive wiper malware that would profoundly damage one of the world's leading shipping companies. The case highlighted the crucial function of CTA and other threat intelligence-sharing platforms in the early detection and immediate circulation of key IOCs (Vasani *et al*., 2023b). Through preemptive sharing, other organizations, including Maersk, could quickly recognize and react to the changing risk. Maersk's incident response demonstrated effective isolation of affected systems, open communication, and a dedication to constant improvement (Deochakke & Tyagi, 2022).

Lessons Learned

1. **Early Identification through Threat Intelligence Sharing:** The Cyber Threat Alliance (CTA) was instrumental in the early identification of NotPetya. Researchers from various member organizations worked together to look into the attributes of the attack and then shared IOCs with the community at large. Such speedy sharing of threat information made it possible for organizations like Maersk to react to the threat almost immediately.
2. **Effective Incident Response:** The incident response played a major role in the intensity mitigation. The organization identified malfunctioning systems, switched off infected networks, and informed openly about the attack. Their proactive reaction prevented the ransomware from infecting the entire company.
3. **Global Collaboration and Transparency:** The attack illustrated once again the role of interconnectedness and Candor in the time of a widespread threat. Maersk, however, was a victim and disclosed details of the attack openly. This increased transparency benefited the wider cybersecurity community by providing valuable knowledge about the attack's tactics and giving others the opportunity to improve their defences.

5. Recommendations: Optimizing Threat Intelligence Sharing Against Zero-Day Ransomware

1. Enhance Inter-Platform Collaboration

1. The foster of the collaboration between the different forms of threat intelligence-sharing platforms was to form an interconnected and comprehensive defence network. This partnership should involve more than one sector to get the most cumulative wisdom. A joined-force action enables quicker identification and wider distribution of threat intelligence, bolstering more resilient security in the face of zero-day ransomware (Zhao *et al*., 2020). As an example, after a significant cyber incident, for example, the SolarWinds supply chain attack, cross-platform collaboration will allow for a more unified response. The ability to share intelligence and threat indicators across heterogeneous platforms

enables an improved defence against advanced threats (Nkongolo *et al*., 2022).

2. **Establish Regulations of Details and Standards of Information**
   Standardize data formats and information exchange procedures across the industry in the threat intelligence sharing platforms. Standardization enables the streamlining of threat intelligence integration across different cybersecurity tools and systems, thereby facilitating smooth and effective data exchange (Zhao *et al*., 2020). This would tackle the issue of data format heterogeneity that is currently inhibiting effective knowledge exchange. Existing standards STIX and TAXII concerning interoperability of threat intelligence should be mentioned. More widespread usage of such standards guarantees one language for exchanging threat information (Nkongolo *et al*., 2022).
3. **Prioritize Privacy-Preserving Measures**
   Apply privacy-preserving mechanisms in threat intelligence sharing platforms to answer the issue of sensitive information. Promote anonymization techniques and set clear policies on the number of shared details. The balance between the requirement of transparency with the considerations of data privacy is vital to preserve the trust among contributors. The utilization of pseudonymization or tokenization methods by shared threat intelligence helps to preserve the identity of the involved organizations while giving much-needed information on emerging threats (Zhao *et al*., 2020).
4. **Facilitate Sector-Specific Tailoring**
   Foster threat intelligence sharing platforms in tailoring threat data towards sector-specific contexts. This allows organizations in a specific industrial sector to receive threat intelligence specific to their particular challenges and vulnerabilities (Nkongolo *et al*., 2022). Sector-specific targeting increases the relevance and usability of threat intelligence which helps organizations defend themselves against threats, tailoring their defence that way. Financial Services Information Sharing and Analysis Center (FS-ISAC) concentrates on sharpening threat information related specifically to the financial sector, recognizing the unique threats faced by organizations within this industry (Ali *et al*., 2022).
5. **Push Continuous Training and Education**
   Stress the necessity of continuous training and education for cybersecurity experts involved in threat intelligence sharing. This also covers the monitoring of newly developed methods used by the threat actors in the ransomware zero-day attacks. The regular training programs guarantee that security practitioners are trained to analyze and benefit from the threat intelligence received from the common platform (Nkongolo *et al*., 2022). The SANS Institute provides continuous training and certification programs that cover different aspects of cybersecurity such as threat intelligence. Such programs shall have people interested hence a highly skilled and experienced workforce in threat intelligence (Ali *et al*., 2022).

6. Conclusion

This in-depth exploration addresses the complex realm of zero-day ransomware threats, uncovering the shifting approaches of threat actors and evaluating the part played by threat intelligence networks in tackling these ever-changing dangers. The recent cases of zero-day ransomware attacks, e.g. NotPetya and Colonial Pipeline, point to the need for reactive cybersecurity measures. The cyber threat intelligence sharing platforms, epitomized by initiatives like the Cyber Threat Alliance (CTA) and Information Sharing and Analysis Centers (ISACs), assume critical roles in bolstering the organizations against these advanced threats. The study emphasizes the importance of early identification, swift information sharing, and collective defence.

The significance of our findings echoes in the cybersecurity sphere, providing useful information for professionals to practitioners. Pre-emptive steps such as continuous vulnerability scans, network segmentation, and developing sound incident response strategies can be considered feasible in subverting zero-day ransomware attacks. Collective defence via threat intelligence sharing platforms adoption is essential, as key recommendations include improving collaboration, data normalized formats alignment, and privacy as a top priority, tailored by sector. Cybersecurity pros must emphasize continuous training to remain on the offensive against ever-changing threats. Furthermore, the research reinforces the need for collaboration between government and private sectors, acknowledging government agencies as the facilitators to enhance the abilities of threat intelligence sharing platforms. With the cyber threat landscape constantly in motion, the study offers a plan for organizations to shield themselves and work through zero-day ransomware threats.

7. References

1. Ali S, Rehman SU, Imran A, Adeem G, Iqbal Z, Kim KI. Comparative Evaluation of AI-Based Techniques for Zero-Day Attacks Detection. Electronics. 2022;11(23):3934. Available from: https://doi.org/10.3390/electronics11233934
2. Azzedin F, Suwad H, Rahman MM. An Asset-Based Approach to Mitigate Zero-Day Ransomware Attacks. Computers, Materials & Continua. 2022;73(2):3003–20. Available from: https://doi.org/10.32604/cmc.2022.028646
3. Statista. Topic: Ransomware. 2023. Available from: https://www.statista.com/topics/4136/ransomware/#statisticChapter
4. Deochakke A, Tyagi AK. Analysis of Ransomware Security on Cloud Storage Systems. In: Advancements in Interdisciplinary Research. 2022. p. 47–59. Available from: https://doi.org/10.1007/978-3-031-23724-9_5
5. Bitragunta SLV. Midterm Dynamic Simulation for the Governance of Reserves in Systems with Elevated Renewable Energy Integration. 2023;1(1):1956–62.
6. Ekong AP, Etuk A, Inyang S, Ekere-obong M. Securing Against Zero-Day Attacks: A Machine Learning Approach for Classification and Organizations' Perception of its Impact. Journal of Information Systems and Informatics. 2023;5(3):1123–40. Available from: https://doi.org/10.51519/journalisi.v5i3.546
7. Elsayed D. Research Design, Methodology, and Data Collection. In: Corruption in the MENA Region. 2020. p. 49–59. Available from: https://doi.org/10.1007/978-3-030-55314-2_4
8. Guarascio M, Cassavia N, Pisani FS, Manco G. Boosting Cyber-Threat Intelligence via Collaborative Intrusion

Detection. Future Generation Computer Systems. 2022;135:30–43. Available from: https://doi.org/10.1016/j.future.2022.04.028
9. H. R. G, Aithal PS. How to Choose an Appropriate Research Data Collection Method and Method Choice among Various Research Data Collection Methods and Method Choices during Ph.D. Program in India? 2022. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4275696
10. Hunter B. 'til the Next Zero-Day Comes: Ransomware, Countermeasures, and the Risks They Pose to Safety. Safety-Critical Systems EJournal. 2022;1(1). Available from: https://scsc.uk/journal/index.php/scsj/article/view/5
11. Ilca LF, Lucian OP, Balan TC. Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response. Sensors. 2023;23(15):6757. Available from: https://doi.org/10.3390/s23156757
12. Kapoor A, Gupta A, Gupta R, Tanwar S, Sharma G, Davidson IE. Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions. Sustainability. 2021;14(1):8. Available from: https://doi.org/10.3390/su14010008
13. Kumar R, Subbiah G. Zero-Day Malware Detection and Effective Malware Analysis Using Shapley Ensemble Boosting and Bagging Approach. Sensors. 2022;22(7):2798. Available from: https://doi.org/10.3390/s22072798
14. Buksov M. Characteristics of a Successful Ransomware Attack. 2020. Available from: https://search.proquest.com/openview/959ee3bcc91dd4d5e1fbb9162f5cc53f/1?pq-origsite=gscholar&cbl=18750&diss=y
15. Nkongolo M, van Deventer JP, Kasongo SM. UGRansome1819: A Novel Dataset for Anomaly Detection and Zero-Day Threats. Information. 2021;12(10):405. Available from: https://doi.org/10.3390/info12100405
16. Nkongolo M, Van Deventer JP, Kasongo SM, Zahra SR, Kipongo J. A Cloud Based Optimization Method for Zero-Day Threats Detection Using Genetic Algorithm and Ensemble Learning. Electronics. 2022;11(11):1749. Available from: https://doi.org/10.3390/electronics11111749
17. Özdemir A. Cyber threat intelligence sharing technologies and threat sharing model using blockchain. 2021. Available from: https://open.metu.edu.tr/handle/11511/90897
18. Preuveneers D, Joosen W. Sharing Machine Learning Models as Indicators of Compromise for Cyber Threat Intelligence. Journal of Cybersecurity and Privacy. 2021;1(1):140–63. Available from: https://doi.org/10.3390/jcp1010008
19. Rains T. Cybersecurity Threats, Malware Trends, and Strategies: Discover risk mitigation strategies for modern threats to your organization. Packt Publishing Ltd; 2023. Available from: https://books.google.com/books?hl=en&lr=&id=TN-oEAAAQBAJ
20. Ryan M. The ransomware revolution: how emerging encryption technologies created a prodigious cyber threat. 2020. Available from: https://unsworks.unsw.edu.au/entities/publication/d82015d4-8065-4b72-9d44-c2a6dd7af603
21. Saprykin OS. Models and Methods for Diagnosing Zero-Day Threats in Cyberspace. Herald of Advanced Information Technology. 2021;4(2):155–67. Available from: https://doi.org/10.15276/hait.02.2021.5
22. Vasani V, Bairwa AK, Joshi S, Pljonkin A, Kaur M, Amoon M. Comprehensive Analysis of Advanced Techniques and Vital Tools for Detecting Malware Intrusion. Electronics. 2023;12(20):4299. Available from: https://doi.org/10.3390/electronics12204299
23. Zahoora U, Rajarajan M, Pan Z, Khan A. Zero-day Ransomware Attack Detection using Deep Contractive Autoencoder and Voting based Ensemble Classifier. Applied Intelligence. 2022. Available from: https://doi.org/10.1007/s10489-022-03244-6
24. Zhao J, Yan Q, Li J, Shao M, He Z, Li B. TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. Computers & Security. 2020;95:101867. Available from: https://doi.org/10.1016/j.cose.2020.101867