Open Access
Full Length Article

ORIGINAL ARTICLE

Mitigating Phishing and Social Engineering Ransomware Threats in Bioinformatics: Strategies for Education and Awareness

Shuaib Ahmed Wadho[1], Farhan Bashir[2], Sijjad Ali[3], Roshan Kumar[4], Shafique U Rehman Sahito[5]

[1, 2, 4] Faculty of Information and Communication Technology, University of Tunku Abdul Rahman, Kampar, Malaysia
[3] College of Electronics and information Engineering, Shenzhen University, Shenzhen
[5] Cloud Solutions for IT and Communication Co., city Riyadh, Saudi Arabia

ABSTRACT

Phishing and social engineering attacks, along with ransomware, have become an unforeseen obstacle in the quickly developing field of bioinformatics, putting confidential information at risk and interfering with research procedures. As the bioinformatics landscape continues to change, addressing cybersecurity vulnerabilities becomes a critical concern. Similarly, even the most knowledgeable experts in the given area may fall prey to such cyber dangers. Social engineering and phishing are the types of attacks that exploit people's weaknesses, thus a comprehensive approach by integrating technical fixes, awareness and education campaigns aimed at fighting cyber threats should be embraced. In this case, bioinformatics experts can traverse the digital sphere with resolve and get rid of bad data and maintain the integrity of the domain of science as they grow a responsible community. As a result of the systematic review we conducted, from the 551 studies we found, 20 that met the eligibility criteria were chosen for further analysis. This analysis of literature concentrated on the defence's biotechnology against ransoming crooks` constantly morphing strategy. The report went over a couple of things, like the increased complexness of encryption algorithms, and the RaaS (ransomware-as-a-service) model. This study offers a new toolkit focused on campaigns to sensitize the public and educate them to address the threats and dangers presented by ransomware. The physicists of bioinformatics are equipped to withstand the digital world with staunchness and see to securing the non-negotiables essential data safeguard and the limited but fundamental research activities by developing an elaborate culture of cybersecurity awareness.

Author`s Contribution
[1,2,4]*Faculty of Information and Communication Technology, University of Tunku Abdul Rahman, Kampar, Malaysia*
[4]*College of Electronics and information Engineering, Shenzhen University, Shenzhen, 518060*
Cloud Solutions for IT and Communication Co., city Riyadh, Saudi Arabia

Address of Correspondence
Shuaib Ahmed Wadho,
Email: shoaib.qau09@gmail.com

Article info.
Received: July 6, 2023
Accepted: November 13, 2024
Published: December 30, 2024

Cite this article: *Ahmad W.S,Bashir F,Ali S,Kumar R,Sahita Rehman U. SA. Mitigating Phishing and Social Engineering Ransomware Threats in Bioinformatics: Strategies for Education and Awarenes. appl.2024; 24-29*

Funding Source: *Nil*
Conflict of Interest: *Nil*

INTRODUCTION

In recent decades, the advancement of bioinformatics contributed significantly to research through the changing of strategies by which biologists deal with data to achieve significant results in the fields of genomics, personalized medicine, and agriculture. Also, the digital space opens the door to an assimilated scientific research and medical innovation that never has been discovered all the time, and even, at the same time, it exposes the effects of threats that never has been imagined all the time. The ransomware attackers and social engineering are among the two most efficacious cyber tools for disrupting key genetic information safety [1].

Phishing is the richest and most complex method used by the biologists to extract the sensitive data from the humans. On these sites, for those who read the messages, they can be sometimes misleading, and titles misappropriated as authentic messages. Stealing data and arriving at a conclusion that it will be possible to make the data unusable by applying a reliable encryption algorithm is one of the methods that the ransomware tries to take an advantage of the human weaknesses and persuade the victim to pay a ransom in order to make the data decrypted. The convergence of the devastating threats exhibits a multifaceted as well as a tough nut to crack a problem and therefore we need the concerted effort of the bioinformatics community to highlight the risk "as the first step." After that, educational programs must follow [2] Bioinformatics which is a rapidly growing area as an integral part of science, needs to be highly protected and maintained to secure digital platforms that support scientific research, medical diagnostics, and agricultural acceleration. This article investigates complex environments of cybersecurity risks where bioinformatics meets, identifies the most commons ways for data leaks, and offers practical strategies to minimize the risks of ransomware and phishing attacks. Through recognizing the various challenge positions arising the risks, the community of bioinformatics will develop an environment which is both resilient and vigilant, thus making sure that the projects are successful in the long run [3].

The research field of bioinformatics cybersecurity is of great interest as more scholars and experts focus on different facets of emerging security issues and potential

RELATED WORK

preventive interventions. It also include the publications below which do a summarized review of the topic by studying ransomware, phishing, social engineering, and cybersecurity education programme in bioinformatics [7].

The paper provides a brief overview of malware, however, it specifies the ransomware, and enlists the many types it possesses and their impacts. It allows for understanding the ransomware development and evasion techniques, that is perfect basis for development of DNAact-Ran. To find ransomware, the research hereby proposes a Digital DNA Sequencing Engine which harnesses the use of innovative design design limits and k-mer frequency vectors. Through the examination of a dataset, the DNAact-Run has shown its capabilities of being accurate and effective in predict and detecting the ransomware. This can efficiently aid in the cybersecurity measures [8].

The paper considers various cyber security hurdles in bioinformatics. It provides a comprehensive case study of various types of threats like the phishing and ransomware, with the intention to enrich the knowledge of the bioinformatics experts on threats and how they respond when it comes to protecting sensitive biological data [9].

The survey below is dedicated to email-based threats in bioinformatics in general sense, particularly, phishing attacks against bioinformatics experts. It shows the methods used by attackers to get to the subject, it tries bring to light community flaws by making recommendations on more secure email systems [10].

This paper will discuss the case of ransomware in the context of bioinformatics. It finds motives and results of such assaults presenting possible outlook for bioinformatics society. The research seeks to enrich the knowledge on ransomware threats and the appropriate response measures [11].

The present study concentrates on the human aspect found in the social engineering attacks in the field of bioinformatics. It investigates the psychological and behavioural factors that contribute to the case of social engineering approaches and provides shopping lists on how bioinformatics professionals can be resilient [12].

The realm of cybersecurity education is discussed in this survey as it showcases the lags in awareness among bioinformatics professionals. This paper purposefully focuses on the identification of knowledge areas that need to be powerfully reinforced within the bioinformatics community in order to spark relevant educational initiatives [13].

Implementing user-oriented methodology, this essay performs the behavioural study of the people who are pursued by phishing attacks in bio informative. Using the study findings, a comprehensive user perspective on anti-phishing measure on bioinformatics will be developed [14]..

This study emphasizes training in cybersecurity, and it presents a template for educating bioinformatics professionals. Which is based on the practices that are running right now and it proposes future directions for the development of the comprehensive and effective cybersecurity educational programs that address the needs of the bioinformatics community. [15]..

RESEARCH METHODOLOGY

In conducting our study, we adopted a comprehensive review methodology, gathering data from diverse sources such as IEEE Xplore, Scopus, and Google Scholar. Our search query, skilfully crafted as "Bioinformatics," "Ransomware," and "Social Engineering," served as an effective guide in pinpointing relevant literature. Within this structured framework, we formulated specific research questions that facilitated the extraction of key objectives from the pertinent literature. The figure 1 shows the methodology which opt in this paper.

4. The Threat Landscape:

In bioinformatics, phishing attacks often aim to attack researchers, physicians, and institutions that deal with health-related genetic or genomics data, which is also very sensitive. Unlike the technical ransomware which relies on exploiting computer vulnerabilities to gain unauthorized access and endanger the data integrity, the social engineering ransomware explores any human susceptibility. Analyzing and studying the complexities of such risks is one substantial part for creating successful mitigation strategies.

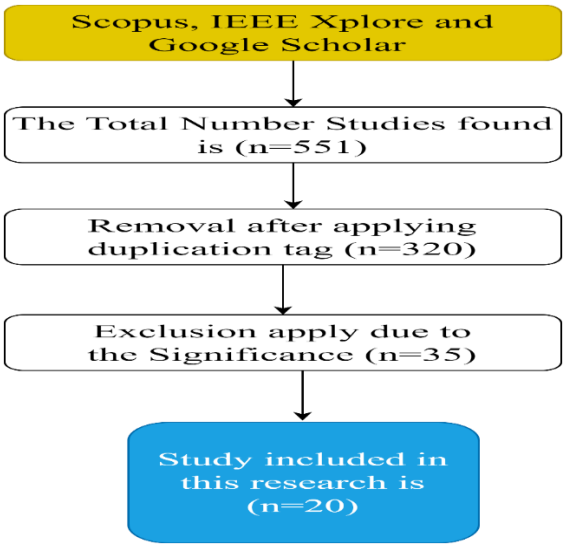

Figure 1. Methodology

4.1 Phishing Attacks in Bioinformatics:

Targets: By including the terms such as academics, clinical area, and organisations processing genetic, genomic, and healthcare data, it becomes clear which group is at risk. The prunting campaigns are developed to use the credibility and access permissions of bioinformatics professionals who deal with highly important and sensitive data [16].

Risk to Data Integrity: Attacks like phishing have remained notorious for misleading users into providing their login passwords or important information like financial details to them. The bioinformatics context could also include phishing attacks which breaks into databases that contain genetic data and are very sensitive [17]

4.2 Social Engineering Ransomware:

Exploiting Human Vulnerabilities: This part of the conversation will be focused on the human factor of cyber protection. Psychological attack exploiting the weak points of people in the area of biotechnology is a common feature of social engineering ransomware. During these raids, the criminals use ingenious administrative techniques like impersonation or trust-based figures to validate their illegal trespasses [18].

Unauthorized Access and Data Compromise: Contrary to the ordinary ransomware that may either employ exploitation or social engineering, this one relies on an individual to cause a breach of security. Now the attacker has been in the system, and he/she initiate to encrypt the valuables data point that will make the legal user unable to decrypt it. Such attack opens to the loses of the important bioinformatics data by hacking or data permanent damage [19].

4.3 Cruciality of Understanding Threat Intricacies:

Tailored Mitigation Strategies: It focuses on the significance of being in the know of the main natures of these risks. Generally, the most inventive phishing and social engineering ransomware are the most elaborate, and they normally grow more sophisticated and complex. Standards or common cybersecurity strategies cannot be effective in handling such sophisticated cyber-attacks [5].

Risk Mitigation: Through the in-depth knowledge of the use of bioinformatics tools in hacker attacks, specialized mitigation tools are developed. To have these defenses against phishing reinforced, the initiatives might involve educational programs, better spam filters, and user-awareness campaigns. For social engineering ransomware technical constraints and letting the users to recognize the deceitful actions is the key [6].

4. Common Attack Vectors in Bioinformatics:

a. Email-Based Phishing: Spam messages that are sent from accounts that appear to belong to reputable organizations, are often employed by phishers to lure recipients to visit harmful sites or disclose personal information.

b. Spear Phishing: Specifying certain members of the bioinformatics community who personally can be employed for the specific purpose of maximising the possibilities of success.

c. Malicious Attachments: Generally, ransomware attacks are performed via indirect vectors that trigger after the victim opens or clicks the infected files or attachments.

d. Impersonation: Social engineering is a tricky approach that always attempts to impersonate as a trustworthy authority in order to induce individuals voluntarily disclose personal data.

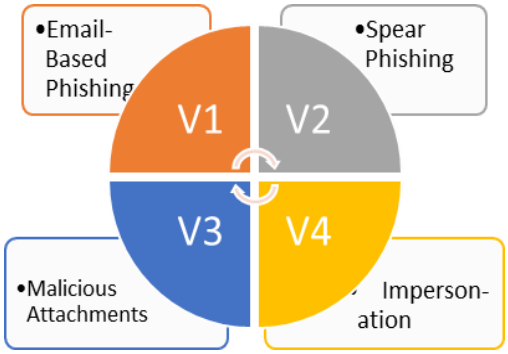

Figure 2. Infection Vetor Scale

5. Mitigation Strategies and Result

We pinpointed the useful methods to protect ourselves from almost all perils once we analyzed many of the researches. As shown on Figure 3, these findings of the survey are divided into 20 researched papers that will be used for the analysis later. It is quite evident that performing these steps with the urgency required in the industry are the necessary factors for the execution of the mitigation plan.

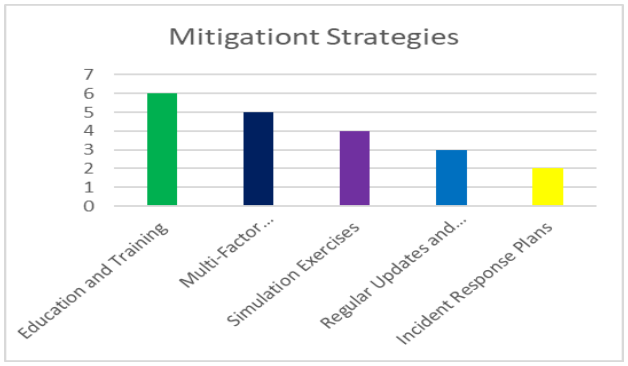

Figure 3. Mitigation Measures

RESULT METHODOLOGY

Table 1. Comparative Study

L.Ref	Scope of Work	Technique	Gap	Limitation
[8]	Cybersecurity threats in bioinformatics	Survey analysis	Cybersecurity awareness and proposing educational	Limited focus on specific malware types and detection

			initiatives	methods
[9]	Email-based phishing attacks on bioinformatics professionals	Survey and pattern analysis	Lack of emphasis on preventive measures and training for individuals targeted by phishing	Limited exploration of advanced phishing techniques and their count
[10]	Trends and patterns in ransomware attacks in bioinformatics	Analysis of ransomware incidents	Insufficient exploration of the human factor in ransomware attacks	Limited discussion on strategies for ransomware incident response
[11]	Comparative analysis of defensive strategies against phishing	Comparative analysis of defensive measures	Lack of focus on specific vulnerabilities within healthcare-oriented bioinformatics	Limited discussion on the integration of defensive strategies with healthcare systems
[12]	Behavioral analysis of social engineering tactics in bioinformatics	Behavioral analysis	Limited insights into emerging social engineering g tactics and their impact on bioinformatic ics	Scope restricted to behavioral analysis, overlooking technical aspects of social engineering attacks
[13]	Identification n of educational gaps in cybersecurity ty awareness	Survey and analysis of educational programs	Limited exploration of the effectiveness of existing educational initiatives	Reliance on self-reported data for educational program evaluation
[14]	Comparative e analysis of defensive strategies against phishing	Comparative e analysis of defensive measures	Lack of focus on specific vulnerabilities within healthcare-oriented bioinformatics	Limited discussion on the integration of defensive strategies with healthcare system
[15]	Preparedness of genomic data centers against ransomware attacks	Case study and incident analysis	Limited coverage of preventive measures, with a focus on incident response	Narrow focus on genomic data centers, may not generalize to broader bioinformatics infrastructure
[16]	Behavioral analysis of individuals targeted by phishing attacks	Behavioral analysis and user-centric approach	Limited exploration of evolving phishing tactics and their impact on user behaviour	Relies on self-reported data for understanding user behaviour and may lack real-world validation
[17]	Framework for bioinformatics cybersecurity training	Proposal of a comprehensive training framework	Lack of empirical validation of the proposed framework	Theoretical approach without practical implementation and validation

CONCLUSION

We have carefully outlined a range of mitigation techniques in this paper with the goal of protecting data from future attacks. Because bioinformatics is a dynamic field, our safeguards for sensitive data must constantly change. To effectively counteract the threats posed by ransomware and phishing emails, the bioinformatics community must unite behind a common initiative that includes raising awareness and providing thorough education. Through proactive measure implementation, the development of a cybersecurity-focused culture, and ongoing threat monitoring, the bioinformatics community is well-positioned to fortify its defences and guarantee the

unwavering integrity and confidentiality of vital biological data. In conclusion, the proactive implementation of these tactics creates a strong Defence in the rapidly developing field of bioinformatics against changing cyber threats.

REFERENCE

[1] Kathryn, K, Millett., Eduardo, dos, Santos., Piers, Dominic, Millett. (2019). Cyber-Biosecurity Risk Perceptions in the Biotech Sector. Frontiers in Bioengineering and Biotechnology, 7:136-. doi: 10.3389/FBIOE.2019.00136

[2] Adrie, Bekker. (2022). Strategical Analysis of Cyberbiosecurity in 2022: How to Defend Biotech and Healthcare Sector from Cyber Treats. doi: 10.36227/techrxiv.20485929

[3] Dr., Alex, Roney, Mathew., Hannah, Alex. (2022). Cyberbiosecurity as the Foremost Biological Weapon to the Digital World. International research journal of innovations in engineering and technology, 06(02):75-79. doi: 10.47001/irjiet/2022.602013

[4] Tao, Tao., Yuan, Chen., Bijing, Liu., Xueqi, Jin., Mingyuan, Yan., Shouling, Ji. (2018). Security Analysis of Bioinformatics WEB Application. 383-397. doi: 10.1007/978-3-030-16946-6_30

[5] Xavier-Lewis, Palmer., Lucas, Potter., Saltuk, Bugra, Karahan. (2022). Exploration on APTs in Biocybersecurity and Cyber biosecurity. Proceedings of the ... international conference on information warfare and security, 17(1):532-535. doi: 10.34190/iccws.17.1.67

[6] Randall, S., Murch., William, K., So., Wallace, G., Buchholz., Sanjay, Raman., Jean, Peccoud. (2018). Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy.. Frontiers in Bioengineering and Biotechnology, 6:39-39. doi: 10.3389/FBIOE.2018.00039

[7] Ingrida, Domarkienė., Laima, Ambrozaitytė., Linas, Bukauskas., Tautvydas, Rančelis., Stefan, Sütterlin., Benjamin, James, Knox., Kaie, Maennel., Olaf, Maennel., Karen, Parish., Ricardo, G., Lugo., Agnė, Brilingaitė. (2021). CyberGenomics: Application of Behavioral Genetics in Cybersecurity.. Systems Research and Behavioral Science, 11(11):152-. doi: 10.3390/BS11110152

[8] Khan, F., Ncube, C., Ramasamy, L. K., Kadry, S., & Nam, Y. (2020). A digital DNA sequencing engine for ransomware detection using machine learning. IEEE Access, 8, 119710-119719.

[9] Reddy, B. V., Krishna, G. J., Ravi, V., & Dasgupta, D. (2021). Machine learning and feature selection based ransomware detection using hexacodes. In Evolution in Computational Intelligence: Frontiers in Intelligent Computing: Theory and Applications (FICTA 2020), Volume 1 (pp. 583-597). Springer Singapore.

[10] Bat-Erdene, M., Park, H., Li, H., Lee, H., & Choi, M. S. (2017). Entropy analysis to classify unknown packing algorithms for malware detection. International Journal of Information Security, 16, 227-248.

[11] Manas, Kumar, Yogi., D, Aiswarya. (2023). A Comprehensive Review -Application of Bio-inspired Algorithms for Cyber Threat Intelligence Framework. 2(1):101-111. doi: 10.36548/rrrj.2023.1.08

[12] Wadho, S. A., Yichiet, A., Lee, G. M., Kang, L. C., Akbar, R., & Kumar, R. (2023, October). Impact of Cyber Insurances on Ransomware. In 2023 IEEE 8th International Conference on Engineering Technologies and Applied Sciences (ICETAS) (pp. 1-6). IEEE.

[13] Simon, A., Levin. (2023). Challenges in cybersecurity: Lessons from biological defense systems. Mathematical biosciences, 362:109024-109024. doi: 10.1016/j.mbs.2023.109024

[14] Bayan, Hassan, Banimfreg. (2023). A comprehensive review and conceptual framework for cloud computing adoption in bioinformatics. Healthcare analytics, 3:100190-100190. doi: 10.1016/j.health.2023.100190

[15] (2023). Challenges in Cybersecurity: Lessons from Biological Defense Systems. Social Science Research Network, doi: 10.2139/ssrn.4342051

[16] Adrie, Bekker. (2022). Strategical Analysis of Cyber biosecurity in 2022: How to Defend Biotech and Healthcare Sector from Cyber Treats. doi: 10.36227/techrxiv.20485929

[17] Adrie, Bekker. (2022). Strategical Analysis of Cyber biosecurity in 2022: How to Defend Biotech and Healthcare Sector from Cyber Treats. doi: 10.36227/techrxiv.20485929.v1

[18] Xavier-Lewis, Palmer., Lucas, Potter., Saltuk, Bugra, Karahan. (2022). Exploration on APTs in Bio cybersecurity and Cyber biosecurity. Proceedings of the ... international conference on information warfare and security, 17(1):532-535. doi: 10.34190/iccws.17.1.67

[19] Lucy, L., Thomson. (2022). Privacy and security challenges in bioinformatics. doi: 10.4337/9781839105951.00021

[20] Haris, Smajlovic., Ariya, Shajii., Bonnie, Berger., Hyunghoon, Cho., Ibrahim, Numanagić. (2022). Sequre: a high-performance framework for rapid development of secure bioinformatics pipelines. 164-165. doi: 10.1109/IPDPSW55747.2022.00040.