A Review of the South African Public Sector's Capability in Combating Ransomware

Nokuthaba Siphambili
Information & Security Centre
Council of Scientific and Industrial Research
Pretoria, South Africa
0009-0006-6091-9838

Oyena Mahlasela
Information & Security Centre
Council of Scientific and Industrial Research
Pretoria, South Africa
0009-0006-4188-6145

Errol Baloyi
Information & Security Centre
Council of Scientific and Industrial Research
Pretoria, South Africa
0009-0009-6959-3485

Elekanyani Mukondeleli
Information & Security Centre
Council of Scientific and Industrial Research
Pretoria, South Africa
0009-0001-1165-7521

***Abstract*—Ransomware attacks have emerged as a significant cybersecurity threat, impacting organisations globally, including the South African public sector. This study conducted a narrative review aimed at investigating the South African public sector's capability to address ransomware attacks. The review examined news articles, reports, and literature from databases such as Scopus, Google Scholar, and ScienceDirect. Furthermore, this review explored the evolving landscape of ransomware, including its modus operandi and impacts. The findings revealed that since 2019, ten different South African public sector entities have been targeted by ransomware, with one entity being hit twice. Based of those findings, this study provided recommendations to strengthen the South African public sector's national defences and improve its preparedness for future ransomware attacks.**

Keywords— Ransomware, Readiness, Common threats, Mitigation, Defence mechanisms

I. INTRODUCTION

Organisations throughout the world face a serious issue as a result of the constantly changing cyber threat scenario. Ransomware attacks are becoming a common and disruptive danger that affects both public and private organisations. The increasing digitisation of operations and reliance of public sector organisations on interconnected networks for the delivery of key services without the necessary security controls make them increasingly vulnerable and susceptible to cyber-attacks, such as ransomware. Ransomware is a type of malware that encrypts a victim's file systems or data by preventing them from accessing their files. The threat actor would then demand a ransom payment, usually in bitcoin in exchange for the decryption key which will be used to decrypt the compromised file system or data [4].

As the digital world continuously grows, so does the impact of ransomware attacks continue to grow. This is mainly due to the accessibility of ransomware attack tools. Evidently, this has made it easier for threat actors to launch these types of cyber-attacks and demand cryptocurrencies such as Bitcoin [5]. Emerging ransomware is not making it any easier. Threat actors are constantly innovating and improving the current breed of ransomware from using traditional encryption techniques to using ransomware as a service (RaaS) and Artificial Intelligence (AI) [2].

There are two different types of ransomware, i.e. locker ransomware and crypto ransomware. Locker ransomware locks users out of their devices to prevent them from accessing their data and then demand a ransom to release them back to the victim [1], [17], [41]. Crypto ransomware on the other hand encrypts data and requires victims to pay ransomware before gaining access to their data [1], [17]. Crypto ransomware aims at encrypting data where a victim is unable to access their personal files whereas the Locker ransomware locks a user out of their system and does less data encryption [41]. Crypto ransomware leaves the victim's files unreadable whereas the locker ransomware makes the victim's files inaccessible but not encrypted. There are different types of Crypto ransomware attacks namely: DirtyDecrypt, TelsaCrypt, Crypt Locker, PadCrypt and Cryptowall and the Locker ransomware types are: DMA Locker, Locky Ransomware, CTB-Locker, Winlock, and TorrentLocker [42].

A. Evolution of Ransomware

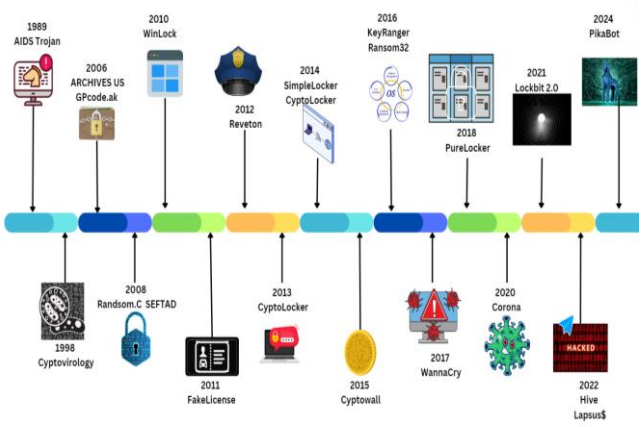

Fig. 1. Evolution of Ransomware attacks *(adapted from [2])*

AIDS trojan (aka, PC Cyborg) was the first ransomware attack in 1989 where floppy disks were sent to an AIDS conference and the victims paid $189 through the post office [1] - [3]. The age of the internet (2000s) came with ransomware that aimed at using digital currencies with the first locker ransomware: GP code and Achieves in 2006, Crypto Locker in 2007 [2], [38]. The birth of the cryptocurrencies era (2010s) gave birth to the inception of Ransomware as a service (RaaS) with Winlock (2011), Reveton(2012), Cyptowall (2015), WannaCry (2017) and PureLocker (2018) where cryptocurrencies where used as a form of payment [2], [38]. Big game hunting era which is the 2020s where the Covid-19 pandemic helped strengthen ransomware by focusing on double extortion with the establishment of Corona ransomware (2020), Dark Side and Lockbit 2.0 (2021), Hive (2022) and the PikaBot (2024) [2], [38].

Ransomware attacks occur in different stages: the criminal exploits the victim by sending out an infected email, the ransomware then targets the victim's files which are then encrypted, and the victims receive a notification of the demand specifications to gain access to their files until the payment has been sent [5].

Due to the sensitive nature of the data, they store and generally less robust cybersecurity postures, public sector organisations might be particularly exposed. The South African public sector is not immune to these attacks such as how the Public Service Coordinating Bargaining Council and the General Public Service Sector Bargaining Council suffered a ransomware attack in February 2023 where their critical services were disrupted, and sensitive data was exposed [7]. The malicious nature of ransomware, coupled with its ability to encrypt critical data and demand ransom for its release, has made it a formidable challenge for governments and public agencies worldwide. These ransomware attacks have consequences on public sector organisations such as loss of public trust, reputational damage, and financial losses [6].

There is less research done on assessing the readiness of South African public sector organisations. Thus, this study focuses on assessing the readiness of the South African public sector in terms of ransomware attacks and recommending defence mechanisms that will help tackle these ransomware attacks. To lessen the effects of ransomware attacks and protect sensitive data and critical services, it is of utmost importance to comprehend how prepared the public sector is to mitigate against ransomware attacks.

II. METHODOLOGY

NARRATIVE ANALYSIS

Narrative analysis is a qualitative method focused on interpreting human experience through narratives or stories [40]. This narrative research method explored the real experience of ransomware attacks in South Africa. This was useful for learning from previous attacks and determining the readiness of South African organisations to safeguard against future attacks.

A. Data collection

Document analysis, such as news articles, reports, and academic publications, like research articles and journal publications, were analysed for a case study of ransomware in South Africa. Patterns in attacks, targeted sectors, and the impact of reported cases were determined.

Therefore, different publications narrated the stories of ransomware attacks in South Africa from (2021 to 2024). Looking at the threat landscape, data breaches, ransomware attacks and some of the targeted industries as illustrated in Table 1 below:

Author	**Contribution**
[26]	The cyber threat landscape in South Africa: A 10-Year review
[30]	Cybersecurity Readiness in South African Public Sector Organizations
[35]	The State of Ransomware in South Africa
[32]	ENISA threat landscape 2023
[34]	Hackers who breached South Africa's companies database say it's much worse than anyone knows
[27]	Justice Department battles to contain ransomware attack
[24]	Lockbit takes credit for February shutdown of South African Pension Fund
[25]	DBSA becomes target of ransomware attack
[28]	Ransomware hits Johannesburg Electricity Supply

Thereafter, a thorough literature review was conducted to examine the common threats, the effects of ransomware and some ransomware attacks in the South African public sector.

III. LITERATURE REVIEW

A. Common threats of ransomware

Public sector organisations often provide critical services and store sensitive information, which makes them prime targets of ransomware attacks. Attackers are strategic when attacking public sector organisations since they know that the repercussions of disrupting public services extend beyond data loss, but it can create disarray and public safety risks [22]. Therefore, unlike private entities, disruptions of critical services in the public sector can create immense pressure on the organisation to pay for the ransom to restore vital services [21]. Therefore, in most cases, public sector organisations tend to face double extortions where attackers do not only encrypt data but steal data before they perform encryption [22]. Thereafter, threaten to leak the sensitive information if the ransom is not paid.

Ransomware attacks can cause a serious threat that can be devastating for both individuals and organisations. Recently, there has been a rise in ransomware attackers adopting ransomware as a service (RaaS) model, taking advantage of RaaS pre-built tools to attack businesses and individuals maliciously. Adopting the RaaS model enables attackers to expand their pool of targets without possessing the technical expertise [9]. Nevertheless, any system or device connected to the internet may be vulnerable to online attacks. However, there seemed to be a pattern in the literature that places organisations and individuals to be considered easy targets by ransomware attackers.

The lack of cybersecurity best practices may cause organisations and individuals to become easy targets for

ransomware attacks. For example, not updating applications and operating systems may leave software vulnerable to known security holes that attackers can exploit [10]. The lack of cybersecurity awareness also includes setting weak passwords that can be easily guessed, becoming susceptible to phishing, and lack of backups where it becomes impossible to recover lost or encrypted data, placing individuals or organisations in a position to be more likely to pay for the ransom [11].

Organisations with limited resources also find themselves becoming easy targets for ransomware attacks. Government departments usually have limited budgets to safeguard their organisations [19]. The lack of budgets may lead to organisations having outdated systems that can easily be exploited by attackers and inadequate security software, for example, a lack of anti-malware, antiviruses, and firewall solutions [19]. Furthermore, organisations with limited resources face the challenge of having undertrained IT specialists and employees who lack cybersecurity best practices, making them more susceptible to social engineering, such as the spread of ransomware [20].

Some of the organisations that become easy targets for ransomware attacks are organisations with valuable data. Organisations such as healthcare providers, education institutions and government agencies are more prone to ransomware attacks since they often hold sensitive data like financial information, making them a target for extortion [21]. For example, education institutions store sensitive student data, which can be valuable to be sold on the dark web or used by attackers for identity theft.

B. Effects of ransomware

The majority of ransomware-affected firms experience financial losses as a result of the impact of recovery costs, which reduces production [12]. An organisation that is attacked must pay to access its data and information; if it doesn't pay, its data may be lost or leaked [17]. Organisations are forced to pay as a result, or else they run the danger of losing their data and suffering damages. Due to their inability to pay the ransomware, which causes data loss and financial losses, organisations wind up declaring bankruptcy [13]. Organisations will then lose both their data and money because access to the compromised data will require payment.

When a criminal obtains access to organisational data, ransomware attacks lead to operational interruption and prevent victims from accessing their data [14]-[15]. Organisations suffer financial losses when they are unable to continue operating since they are typically required to make payments in Bitcoin. Resuming commercial activities after a ransomware attack takes an organisation roughly 21 days [17]. IT specialists need time to evaluate the extent of the ransom attack's harm, which results in business interruption. For example, the Development Bank of Southern Africa faced a ransomware attack in May 2023, resulting in business downtime as they had to investigate to find out the extent of information that was unlawfully accessed. [18] Additionally, this causes workers to concentrate more on business-related matters than their regular responsibilities.

Organisations faced with ransomware attacks are subject to reputational damage due to customers losing trust that their data and information are kept safe which is held by that specific organisation [13]. This leads to an organisation's image being tarnished due to the customers losing trust and financial losses. Employees may be hesitant to continue working in the organisation as these attacks may show that an organisation does not have the means to have the right cyber security measures to protect the organisational data [16]. The organisation may not be able to attract new talent due to the reputational damage where they may not see potential career growth should they work for the specific organisation.

As most public sector organisations render their services to the public and handle personally identifiable information (PII) such as financial information and health information this leads to customers information being exposed. Therefore, when an organisation faces ransomware attacks, it loses public trust as they do not have the right security practices. For example, the 2017 WannaCry attack on the NHS led to disruption in operations and the public lost their confidence in the services being rendered [17]. Organisations that face ransom attacks face damaging effects where investors, stakeholders, and organisations linked to that company may lose their trust in the organisation [16].

C. Ransomware in South African Public Sector

Sophos, a United Kingdom based cybersecurity company, commissioned a survey of 3,000 cybersecurity leaders in mid-sized organisations across 14 countries, including 200 in South Africa. Conducted between January and March 2023, respondents were asked about their experiences in the previous 12 months. Results showed a significant increase in ransomware attacks in South Africa, with 78% of organisations affected, up from 51% in the 2022 survey [35].

The rise in ransomware attacks can be attributed to various factors. However, the declaration of a National State of Disaster highlighted South Africa's cybersecurity posture and readiness to handle such threats. According to [30], the South African public sector witnessed a significant increase in cyber-attacks, predominantly ransomware attacks, making ransomware the most prevalent attack vector in the public sector over the past two years. Consequently, this section will delve into ransomware attacks that emerged post the COVID-19 pandemic.

At the time of this investigation, the most recent ransomware incident targeted the Companies and Intellectual Property Commission (CIPC), an entity within the Department of Trade, Industry, and Competition responsible for registering companies, cooperatives, and intellectual property. The ransomware attackers demanded a $100,000 [R1.9 million] ransom and claimed to have infiltrated the agency's systems since 2021 [34]. Furthermore, Transnet, South Africa's largest rail, port, and pipeline company, predominantly owned by the Department of Public Enterprises, encountered a ransomware attack that rendered its port operations inactive for nearly a week. Transnet reported an IT systems disruption, widely suspected to be a ransomware attack, leading to a complete cessation of the company's activities [26]-[27].

The Department of Justice and Constitutional Development experienced a security breach that compromised its information technology system, attributed to a ransomware attack. This incident resulted in the encryption of all departmental systems, rendering them inaccessible to both internal staff and the public. Consequently, electronic services

provided by the department, such as issuing letters of authority, bail services, email, and the departmental website, were affected [26]-[27]. Similarly, the South African Government Pensions Administration Agency (GPAA), responsible for managing the Government Employees Pension Fund (GEPF) — the largest pension fund in Africa — fell victim to a ransomware attack. The GPAA oversees the pensions of approximately 1.7 million government employees and pensioners, as well as their spouses and dependents [24].

The Development Bank of Southern Africa (DBSA) also experienced a ransomware attack. As a development finance institution that funds infrastructure projects and educational initiatives, the bank has an annual net income of approximately $122 million and employs over 600 individuals [25]. Additionally, the City of Johannesburg (CoJ), a metropolitan municipality overseeing local governance, faced a network breach that was identified following receipt of a ransom note, this incident resulted in downtime for several customer-facing systems [26]. City Power Johannesburg, a state-owned power utility wholly owned by the CoJ, also disclosed that their IT systems were forcibly shut down.

In a tweet, the company stated, "It has encrypted all our databases, applications and network," referring to the virus. As a result, City Power's website remained offline, and residents had to report electricity supply issues on social media. The ransomware attack initially impacted customers' ability to purchase prepaid electricity and hindered the firm's response to localized blackouts [25] [28]. Meanwhile, the Nama Khoi Municipality in the Northern Cape Province faced challenges in restoring IT systems following a ransomware attack. The municipality's chief information officer revealed that the municipality's ICT systems were compromised by a ransomware virus known as Pysa, developed during the COVID-19 pandemic to target local government and healthcare systems [26] [29].

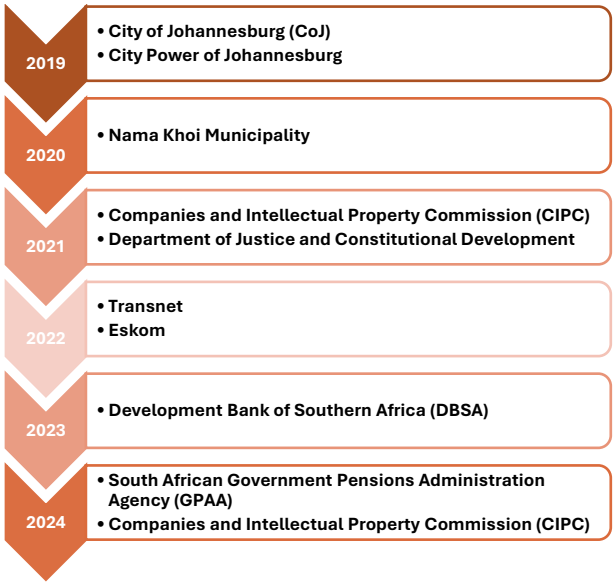

Fig. 2. Timeline of ransom attacks on public sector organisations

D. *Ransomware threat actors*

Ransomware poses a significant threat to organisations of all sizes and industries. Recent analysis [32] has highlighted the five most active ransomware groups globally, with a primary focus on the European Union (EU). Among these, Lockbit ransomware has emerged as a prominent Ransomware-as-a-Service (RaaS) group in the EU, responsible for more than half of the documented ransomware incidents. The increased activity of Lockbit may be linked to the leakage of its builder code, enabling new actors to utilize Lockbit for attacks. Furthermore, two other ransomware groups, PLAY and BlackCat, have had a substantial impact on the cybersecurity landscape, contributing to the complexity and diversity of ransomware attacks in Europe.

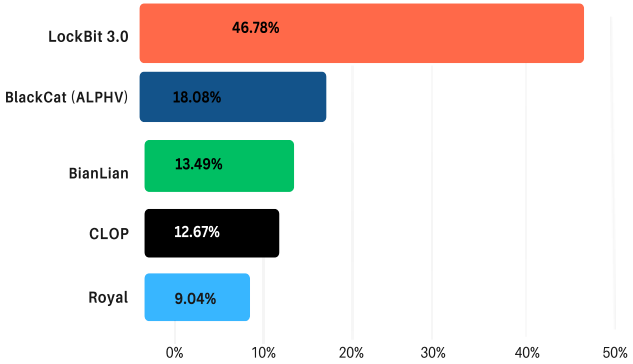

Fig. 3. Ransomware Groups [32]

In the South African context, the LockBit ransomware group has claimed responsibility for the attack on South Africa's government workers' pension fund, leading to operational disruptions and pension payment delays [24]. The DBSA bank suspects the involvement of Akira, a Russian ransomware group, based on initial investigations [25]. The Transnet ransomware incident has been linked to a ransomware group associated with "Death Kitty", "Hello Kitty", and "Five Hands", with the group leaving a note asserting access to Transnet company files [31]. The Shadow Kill Hackers group has taken credit for the network breach experienced by the CoJ, resulting in business downtime due to inaccessible systems [25]-[26].

The Nama Khoi Municipality fell victim to the Mespinoza/Pysa ransomware family, which deployed a Pysa virus to encrypt files, targeting local governments and appending the ". pysa" file extension. This attack led to inaccessible electricity services for five days [28]. Additionally, in some cases, even individuals with limited skills, known as script kiddies, can perpetrate attacks. According to [34], the group responsible for the CIPC ransomware attack consisted of script kiddies. Below is a typical screenshot displayed to victims of ransomware attacks.

Fig. 4. Ransomware Note [36]

IV. Discussion and Recommendations

A. Discussion

Research conducted by Sophos in 2023 state that that 78% of organisations in South Africa were faced with ransomware attacks [39], [35]. Based on the findings, it can be stated that the increase in ransomware attacks focusing on the public sector is influenced by how organisations are easy targets of ransomware attacks.

The availability of information being publicly available of the organisations that faced ransomware attacks continuously helps threat actors know how vulnerable public sector organisations are [26]. Due to the availability of published information criminals are able to find which organisations to attack that will result in an increase in ransomware attacks. This results in government being easy targets due to the data and sensitive information they process and store. As public sector organisations render their services to customers, this results in being prime targets for ransomware attacks.

The unpreparedness of public sector organisations in terms of protecting their systems continuously contributes to the increase in ransomware attacks where criminals will capitalize on vulnerable unprepared organisations [33]. Public sector organisations are vulnerable due to the low defence mechanisms that are out of place. This is evident due to the outdated systems and technologies that exist in public sector organisations that lead to threat actors gaining access to systems and exposing public information. With cases such as the CoJ and the GPAA falling victim to ransomware resulting in beneficiaries of the largest pension fund system being unable to access their payments.

Emerging technologies are continuously improving which results in threat actors using these technologies to improve their ransomware attacks. This results in the evolution from floppy disks being used to issue out ransomware attacks to the use of phishing emails and the use of RaaS. Lack of awareness helps threat actors find vulnerabilities in people as people are the main causes of data breaches. There is a lack of investments that will focus on the adoption of new technologies that will ensure organisations implement resilient defence mechanisms [26].

B. Recommendations

This section provides recommendations on how the South African public sector or any other organisation must do to enhance their cybersecurity defences and avoid being a victim of ransomware attacks. These recommendations are based on best practices, and it is crucial that any of the organisation align these recommendations based on their unique challenges, this will ensure the protection of critical services and sensitive data. The first recommendation is the adoption of cybersecurity awareness, according to [23] this entails regular training, education, and awareness campaigns that promote a cybersecurity culture among employees, which will ensure adherence to best practices such as strong passwords, avoiding suspicious links, and reporting security incidents promptly.

Ransomware can be distributed in various forms. However, email remains a top method for ransomware distribution, often through spam campaigns orchestrated using botnets [37]. These emails frequently contain malicious attachments or links that, when interacted with, initiate the download and installation of ransomware. Therefore, organisations should enhance email security measures as a second recommendation. This includes strengthening email security protocols to prevent phishing attacks and malicious attachments, implementing email filtering solutions, and providing employees with training on recognizing and reporting phishing attempts [23].

Implementation of robust Endpoint Protection solutions, such as antivirus software and intrusion detection systems, to detect and block ransomware threats at the endpoint level help organisations stay prepared of ransomware attacks by regularly update these solutions. These solutions help ensure that organisations protect their systems from malicious activities. Organisations should ensure that they adopt a Défense-in-Depth Approach through the implementation of a comprehensive security strategy that includes network segmentation, access controls, and encryption to create multiple barriers against ransomware threats, ensuring data protection and reducing attack surface [23].

It is of utmost importance for organisations to perform encrypted data backups of critical systems and data regularly and automatically in secure off-site locations, maintaining multiple copies for rapid recovery in case of ransomware attacks. This helps ensure that organisations have backup files in case of data breaches where they will not succumb to meeting the hackers' demands by paying money. Organisations should develop a comprehensive incident response plan, including communication protocols, containment measures, and recovery procedures, and regularly conduct exercises and simulations to ensure effective stakeholder response [23].

The South African government should enhance its threat intelligence capabilities by collaborating with entities such as the South African Police Service (SAPS) or the National Prosecuting Authority (NPA), which can provide resources or statistics on local cyber incidents [26]. Collaboration with the Cybersecurity Hub, South Africa's national Computer Security Incident Response Team (CSIRT), is also crucial, as it offers a service for stakeholders to report cyber incidents. This collaboration enables organisations to stay informed about ransomware threats, trends, and best practices by working with cybersecurity experts, government agencies, and industry partners. Such collaboration helps assess vulnerabilities, develop defence mechanisms, and enhance overall cybersecurity posture.

Furthermore, a study identified several challenges hindering the enhancement of cybersecurity in South African local government, which include insufficient funding, lack of support from top officials, talent shortage, inability to pay competitive salaries, lack of capacity, absence of cybersecurity awareness campaigns, lack of end-user accountability, deficiency in cybersecurity policies and practices, absence of a cyberculture, and a silo approach to addressing cybersecurity-related challenges [33]. Addressing these challenges and adopting the study's recommendations could enable the South African public sector to strengthen its cybersecurity defences and mitigate ransomware risks.

V. Conclusion

This study aimed to assess the readiness of the South African public sector in terms of ransomware attacks and recommend ways of fortifying their national defences. The COVID-19 pandemic helped with the strengthening of

ransomware attacks as threat actors targeted public sector organisations as they provided fence-assessing ways for public sector organisations to strengthen their defences. A narrative review was used due to its flexibility when assessing ways for public sector organisations to strengthen their defences against ransomware attacks. The Covid-19 pandemic helped with the strengthening of ransomware attacks as threat actors targeted public sector organisations as they provided critical services to the public. The recommendations included cyber security awareness, implementing end-point solutions, regular back-ups, improvement in email security, and collaboration with private enterprises and other stakeholders.

With the rise of Artificial Intelligence (AI) ransomware attacks are foreseen to become more sophisticated and public sector organisations need to implement viable defence mechanisms that will assist in fortifying the states' security. There is a need for organisations to focus on collaboration between people, technology and legislations that will help ensure that organisations are prepared for ransomware attacks. The recommendations stated in this study will help ensure South African public sector organisations can be prepared for these ransomware attacks.

ACKNOWLEDGMENT

We will like to thank the Council for Scientific and Industrial Research (CSIR) for the financial support.

REFERENCES

[1] Ekta and U. Bansal, "A review on Ransomware attack," 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), May 2021. doi:10.1109/icsccc51823.2021.9478148

[2] H. Oz, A. Aris, A. Levi, and A. S. Uluagac, "A survey on Ransomware: Evolution, taxonomy, and Defense Solutions," *ACM Computing Surveys*, vol. 54, no. 11s, pp. 1–37, Jan. 2022. doi:10.1145/3514229

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

[4] F. Almeida, M. Imran, J. Raik, and S. Pagliarini, "Ransomware attack as Hardware trojan: A feasibility and demonstration study," *IEEE Access*, vol. 10, pp. 44827–44839, 2022. doi:10.1109/access.2022.3168991

[5] S. Kamil, H. S. Siti Norul, A. Firdaus, and O. L. Usman, "The rise of ransomware: A review of attacks, detection techniques, and future challenges," *2022 International Conference on Business Analytics for Technology and Security (ICBATS)*, Feb. 2022. doi:10.1109/icbats54253.2022.9759000

[6] S. Corbet and J. W. Goodell, "The reputational contagion effects of ransomware attacks," *SSRN Electronic Journal*, 2024. doi:10.2139/ssrn.4674924

[7] C. Smith, "Hackers target public service bargaining councils, dispute resolution suspended for Month," Business, https://www.news24.com/fin24/economy/force-majeure-leaves-dispute-resolution-on-ice-as-hackers-strike-public-service-bargaining-councils-20230303 (accessed Mar. 12, 2024).

[8] A. Hussain, S.F.Ahmad, M Tanveer & A.S. Iqbal, "Computer Malware Classification, Factors, and Detection Techniques: A Systematic Literature Review (SLR)". *International Journal of Innovations in Science & Technology, 4*(3), 899-918. 2022

[9] B. Greenstein, "*The Impact of Ransomware-as-a-Service on Critical Infrastructure"* (Doctoral dissertation, Utica University). 2022.

[10] Ö. Aslan, S.S. Aktuğ, M. Ozkan-Okay, A.A. Yilmaz & E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions". *Electronics, 12*(6), 1333. 2023.

[11] M. Alsharif, S. Mishra, S., & M. AlShehri, "Impact of Human Vulnerabilities on Cybersecurity". *Computer Systems Science & Engineering, 40*(3). 2022.

[12] N. Thamer and R. Alubady, "A survey of ransomware attacks for healthcare systems: Risks, Challenges, Solutions and opportunity of research," 2021 1st Babylon International Conference on Information Technology and Science (BICITS), Apr. 2021. doi:10.1109/bicits51482.2021.9509877

[13] A. Yuryna Connolly and H. Borrion, "Reducing ransomware crime: Analysis of Victims' payment decisions," Computers & Security, vol. 119, p. 102760, Aug. 2022. doi:10.1016/j.cose.2022.102760

[14] P. H. Chen, R. Bodak, and N. S. Gandhi, "Ransomware recovery and imaging operations: Lessons learned and planning considerations," Journal of Digital Imaging, vol. 34, no. 3, pp. 731–740, Jun. 2021. doi:10.1007/s10278-021-00466-x

[15] B. Greenstein, "The Impact of Ransomware-as-a-Service on Critical Infrastructure", 2022.

[16] S. Corbet and J. W. Goodell, "The reputational contagion effects of ransomware attacks," vol. 47, p. 102715, 2022, doi: 10.1016/j.frl.2022.102715.

[17] G. R. Permana, T. E. Trowbridge and B. Sherborne, "Ransomware mitigation: An analytical investigation into the effects and trends of ransomware attacks on global business," 2022.

[18] J. Greig, "State-owned bank in South Africa confirms 'Akira' ransomware attack," The Record from Recorded Future News, https://therecord.media/development-bank-of-southern-africa-akira-ransomware-attack (accessed Mar. 10, 2024).

[19] L. Yuryna Connolly, D.S .Wall, M Lang, M., & B. Oddson "An empirical study of ransomware attacks on organisations: an assess,ment of severity and salient factors affecting vulnerability". *Journal of Cybersecurity*, *6*(1), tyaa023. 2020

[20] J. Roberts & D.A. McEntire, "Professionals in the Department of Homeland Security: The Swiss Army Knife of America's Defense and Protection". In *The Distributed Functions of Emergency Management and Homeland Security* (pp. 158-174). CRC Press.

[21] C.S. Anand & R. Shanker, "Advancing Crypto Ransomware with Multi Level Extortion: A Peril to Critical Infrastructure". In *2023 2nd International Conference for Innovation in Technology (INOCON)* (pp. 1-5). IEEE. March 2023.

[22] T. Rains, "*Cybersecurity Threats, Malware Trends, and Strategies: Discover risk mitigation strategies for modern threats to your organisation"*. Packt Publishing Ltd. 2023.

[23] C. Van der Walt, A. Collard, R. A. Grimes and D. K. Pillay, "Defending Against Ransomware," *Cybersecurity Hub*, 2021.

[24] J. Greig, "Lockbit takes credit for February shutdown of South African Pension Fund," The Record from Recorded Future News, https://therecord.media/lockbit-ransomware-takes-credit-for-south-african-pension-fund-attack (accessed Mar. 28, 2024).

[25] S. Mzekandaba, "DBSA becomes target of ransomware attack," ITWeb, https://www.itweb.co.za/article/dbsa-becomes-target-of-ransomware-attack/WnpNgM21r9Q7VrGd (accessed Mar. 28, 2024).

[26] H. Pieterse, "The cyber threat landscape in South Africa: A 10-Year review," The African Journal of Information and Communication, vol. 28, 2021. doi:10.23962/10539/32213.

[27] A. Moyo, "Justice Department battles to contain ransomware attack," ITWeb, https://www.itweb.co.za/article/justice-department-battles-to-contain-ransomware-attack/DZQ58vVPOB1MzXy2 (accessed Mar. 28, 2024).

[28] "Ransomware hits Johannesburg Electricity Supply," BBC News, https://www.bbc.com/news/technology-49125853 (accessed Mar. 28, 2024).

[29] A. Moyo, "Ncape municipality battles devastating ransomware attack," ITWeb, https://www.itweb.co.za/article/ncape-municipality-battles-devastating-ransomware-attack/8OKdWqDY581vbznQ (accessed Mar. 28, 2024).

[30] G. T. Letseka, "Cybersecurity Readiness in South African Public Sector Organisations" MCom thesis, College of Bus. and Eco., University of Joh., JHB., Gau., 2022.

[31] R. G. & P. Burkhardt, "'death kitty' ransomware linked to attack on South African ports," Business, https://www.news24.com/fin24/companies/death-kitty-ransomware-linked-to-attack-on-south-african-ports-20210729 (accessed Mar. 28, 2024).

[32] I. Lella, C. Ciobanu, E. Tsekmezoglou, M. Theocharidou, E. Magonara, A. Malatras, & R. Svetozarov Naydenov, 2023. ENISA threat landscape 2023: July 2022 to June 2023.

[33] M. Masombuka, M. Grobler, and P. Duvenage, “Cybersecurity and local Government: Imperative, Challenges and Priorities,” 20th European Conference on Cyber Warfare and Security, pp. 285–293, 2021. doi: 10.34190/EWS.21.501.

[34] J. Vermeulen, Hackers who breached South Africa’s companies database say it’s much worse than anyone knows, https://mybroadband.co.za/news/security/527499-hackers-who-breached-south-africas-companies-database-say-its-much-worse-than-anyone-knows.html (accessed Mar. 29, 2024).

[35] Sophos The State of Ransomware in South Africa 2023, May 2023.

[36] Y. Perwej, S. Qamar Abbas, J. Pratap Dixit, N. Akhtar, and A. Kumar Jaiswal, “A systematic literature review on the cyber security,” *International Journal of Scientific Research and Management*, vol. 9, no. 12, pp. 669–710, Dec. 2021. doi:10.18535/ijsrm/v9i12.ec04.

[37] H. Oz, A. Aris, A. Levi, and A. S. Uluagac, “A survey on Ransomware: Evolution, taxonomy, and Defense Solutions,” ACM Computing Surveys, vol. 54, no. 11s, pp. 1–37, Jan. 2022. doi:10.1145/3514229

[38] S. Razaulla et al., "The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions," in IEEE Access, vol. 11, pp. 40698-40723, 2023, doi: 10.1109/ACCESS.2023.3268535.

[39] C. Tredger, “No let-up in ransomware attacks on South Africa,” ITWeb, https://www.itweb.co.za/content/GxwQDq1Dro1MlPVo (accessed Mar. 29, 2024).

[40] M. Bamberg, “Narrative analysis: An integrative approach”. *Qualitative analysis: Eight approaches for the social sciences*, pp.243-264 (2020)

[41] P. Dand and D. Chudasama, “A Comparative Study about the Ransomware,” *Journal of Advanced Database Management & Systems*, vol. *8*,no. 3, pp.8-15(2021)

[42] M. Humayun, N. Jhanjhi, A. Alsayat, and V. Ponnusamy, “Internet of things and Ransomware: Evolution, mitigation and prevention,” *Egyptian Informatics Journal*, vol. 22, no. 1, pp. 105–117, Mar. 2021. doi:10.1016/j.eij.2020.05.003