Commentary

AFRICA'S RESPONSE TO RANSOMWARE THREATS

Digitalization has significantly transformed Africa, especially post-pandemic, with rapid adoption of technologies like 4G and growing interest in 5G. This shift is prominent in sectors such as fintech and e-commerce, driven by a youthful demographic. However, with digital progress comes challenges, particularly cybersecurity threats like ransomware. Reports show South Africa faces the highest ransomware attack rate in the region. International efforts, such as the Counter Ransomware Initiative (CRI), have begun addressing these threats. Regional initiatives, although nascent, aim to strengthen cybersecurity. Moving forward, comprehensive national cybersecurity policies and proactive measures against ransomware are crucial for Africa's digital future.

Rohit Kumar Sharma*

Digitalization has significantly impacted the African continent, much like other parts of the world. Following the pandemic, numerous African nations have witnessed a swift rebound, marked by a substantial rise in the adoption and utilization of digital technologies. In Sub- Saharan Africa, mobile connectivity remains a key catalyst for digital transformation and socio- economic progress.[1] The uptake of 4G technology has recently accelerated, with projections suggesting it could more than double in the coming years. Further, the region is also experiencing a growing momentum in adopting 5G technology.

African nations have witnessed a swift rebound, marked by a substantial rise in the adoption and utilization of digital technologies.

The region's swift advancement of digital technologies is especially noticeable in the financial technology and e-commerce sectors. The potential for technological growth is immense, driven by the young demographic, with about 60 per cent of Africa's population being under 25 in 2020[2]. Critical economic sectors such as finance, education, agriculture, government, security, and manufacturing are proactively embracing digital technologies and shifting their operations to online platforms.

However, as with any technological advancement, digitalisation comes with challenges, with cybersecurity threats, such as ransomware attacks emerging as a pressing concern. The

* Research Analyst, North America & Strategic Technologies Centre, Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA), New Delhi

speed of digitalisation in the region has surpassed the development of laws and regulations concerning cybersecurity. This lag is somewhat expected, as nations and institutions often needs time to adapt to rapid changes in the technological landscape. However, this problem continues to be especially acute in Africa, where essential industries are becoming more dependent on new forms of digital technology.

Ransomware threat in Africa

Prior to delving into the intricacies of ransomware, it is imperative to define the concept and comprehend its ramifications. According to Check Point Software, an IT security firm, ransomware is defined as malware that denies a user or organisation access to the files on their computer.[3] The attackers demand a ransom in exchange for the decryption key, compelling organisations to weigh the difficult choice between paying the ransom to retrieve their data or risking the loss of data by refusing to comply with the attackers' demand. In a digitalised world where businesses are built on and around the availability or possession of data, losing access to it is a nightmare scenario for any organisation. Data is also fundamental to the seamless operation of organisations across various sectors, making it a prime target for threat actors. These reasons underscore why attacks concerning data loss or theft cause global concern.

Ransomware has evolved into a pervasive global issue, impacting countries and continents on a wider scale. Particularly, Africa has experienced a notable escalation in ransomware attacks in recent years, driven by diverse factors. In order to understand the seriousness of this problem in the region, it is necessary to consider the information presented in the "State of Ransomware2023" report, written by Sophos, a well-known IT security company.

South Africa faced the most considerable increase in ransomware attack rate, with 78 per cent of organisations acknowledging being hit in Sophos' survey.

While the report's scope is limited to South Africa and may not fully reflect the broader regional landscape, it nonetheless offers invaluable insights into the prevailing circumstances. Furthermore, it is crucial to highlight that South Africa ranks highest on the Digital Quality of Life (DQL) index within Africa, making it a significant case study for understanding the correlation between digitalization and the escalating cyber threats in the region[4]. South Africa faced the most considerable increase in ransomware attack rate, with 78 per cent of organisations acknowledging being hit in Sophos' survey.[5]

Interpol's Africa cyber threat assessment report categorises the ransomware threat as one of the most serious threats faced by organisations of all sizes around the world.[6] The report also noted that South Africa is the country most affected by ransomware attacks, accounting for 42 per cent of all detected attacks occurring in the region. Morocco follows, with 8 per cent, while Botswana and Egypt come in at 6 per cent. Meanwhile, Nigeria and Tanzania each account for 4 per cent of the ransomware attacks detected. The report also highlights that individuals in Africa are facing targeted attacks from various ransomware families, including Lockbit 2.0, Pysa, Lockbit 3.0, and Conti. Among these, Lockbit 2.0 stands out as

the most widespread, being responsible for the highest number of infections across the African region.

Recently, the Development Bank of South Africa, a state-owned bank, acknowledged a ransomware attack on its systems.[7] In this incident, servers, log files, and documents were encrypted by the Akira gang, posing a significant threat to the bank's digital infrastructure. The Akira group that emerged in March 2023 is reportedly operating from Russia.[8]

Cyberattacks, especially ransomware attacks, pose significant challenges to organisations, particularly businesses. The costs extend beyond financial losses and also encompass damage to the organisation's reputation. According to Cybereasons' *Ransomware: The True Cost to Business* report that studies the ransomware business impact, the cost of ransomware is all-encompassing, impacting the brand and reputation of an organisation along with other disturbing repercussions.[9] The cascading effect of a successful attack also includes resignations at the Chief Information Security Officers' (CISO) level and significant layoffs of staff and employees. In worse cases, businesses may be compelled to cease their operations. Moreover, such attacks can lead to legal actions from affected clients and regulatory penalties imposed by the government.

International Efforts and African Response

Despite the challenges posed by ransomware in the region, it is crucial to gauge the level of international cooperation and actions taken to counter this growing threat. It is equally important to appraise Africa's position within such collaborative efforts. It is also essential to evaluate regional initiatives aimed at countering the ransomware threat, if any. While broader cybersecurity issues have become an intrinsic part of intergovernmental organisations and other multi-stakeholder platforms, it is essential to inquire whether similar arrangements explicitly address the issue of ransomware.

In a first of its kind on ransomware, the White House brought together world leaders for deliberations on a plan of action to address the ransomware threat. The initiative came in the form of the first Counter Ransomware Initiative (CRI) meeting held in October 2021.[10]The meeting was held virtually, and the joint statement of ministers and representatives outlined the broader contours of the problem and proposed measures to tackle the issue. The statement highlighted the "global nature" of the ransomware threat that warrants a shared response. Notably, only three participants were from Africa: Kenya, Nigeria, and South Africa.

...four key pillars to address the issue: resilience, countering illicit finance, disruption and other law enforcement efforts, and diplomacy.

The joint statement focused on the four key pillars to address the issue: resilience, countering illicit finance, disruption and other law enforcement efforts, and diplomacy.[11]The statement emphasized resilience is more than technical capabilities but includes "policy frameworks, well-rehearsed incident response procedures, a trained and ready workforce," and other important segments.[12] It also highlighted the need to cooperate with the virtual asset industry to enhance ransomware-related information sharing. Interestingly, the statement

also shared its commitment to consider "all national tools" available to take action against the perpetrators to disrupt their infrastructure and ecosystem, echoing sturdy resolve.

Following the first CRI, five working groups were established: resilience, disruption, counter-illicit finance, public-private partnership, and diplomacy.[13]The Second International Counter Ransomware Initiative summit declared its intention to establish specific institutions to address the ransomware issue. The International Counter Ransomware Task Force (ICRTF) is mandated to coordinate "resilience, disruption and counter illicit finance activities" in alignment with the initiative's thematic pillars.[14] Another important institution is the Regional Cyber Defense Centre (RCDC), which is specially tasked to operationalize ransomware-related threat information-sharing commitments. The joint effort also endeavors to prevent and dissuade ransomware actors from being able to use the cryptocurrency ecosystem.

The third and latest summit welcomed thirteen new members, including three from Africa: Egypt, Rwanda, and Sierra Leone.[15] The summit focused on developing capabilities to disrupt attackers and the infrastructure they use to conduct their attacks, enhancing cybersecurity through information sharing, and actively combating ransomware actors. The joint declaration also discouraged the member states against ransomware payments.[16] Nigeria became the first African nation in CRI as a lead of the Diplomacy and Capacity Building pillar along with Germany. Observing how this issue-specific initiative led by the White House trickles down to the broader African context will be intriguing.

Nigeria became the first African nation in CRI as a lead of the Diplomacy and Capacity Building pillar along with Germany.

Nonetheless, formulating policy frameworks and creating institutions to address the ransomware threat are commendable and essential first steps. Moreover, the participation of African nations in the CRI, at the very least, encourages these countries to adopt adequate measures. These measures can then be shared with regional groupings, fostering a collaborative approach to enhance overall cybersecurity in the African region.

Due to the developing nature of the ransomware threat, there is currently a lack of issue-specific regional policy frameworks to address this emerging challenge. However, some efforts and arrangements indirectly touch upon the issue of ransomware within the broader category of cybersecurity and cybercrime activities. One such initiative is the African Joint Operation Against Cybercrime (AFJOC), which aims to strengthen the capabilities of national law enforcement agencies to prevent, detect, and investigate cybercrime.[17] It also focuses on promoting cooperation and best practices among African member countries. The role of AFRIPOL[1] becomes equally important when it comes to cooperation between the police agencies of African Union member states. Recently, in a joint operation conducted by INTERPOL and AFRIPOL, individuals and groups running online scams in the region were targeted.[18] Such operations have solidified cybercrime departments in member countries and other regional stakeholders. The Economic Community of West African States (ECOWAS) is also contemplating a joint effort to address broader cybersecurity issues, including cybercrimes.[19]

Way Forward

While it might be too early to expect a ransomware-specific framework and initiative similar to the CRI in the region, there is an opportunity to incorporate prevention and mitigation measures into regional and national rules and regulations. Developing and implementing national cybersecurity policies and strategies involving a broad spectrum of stakeholders is necessary. Governments in the region should also focus on developing legislation for personal data protection, incorporating substantial penalties for organisations that fail to comply, especially those dealing with individuals' data. It is also essential to identify critical infrastructure, the disruption of which could have non-tolerable consequences at the industrial and national levels. Allocating resources accordingly to secure and safeguard these critical assets is imperative.

Developing and implementing national cybersecurity policies and strategies involving a broad spectrum of stakeholders is necessary.

Moreover, every country in the region should establish Cyber Incident Response Teams (CIRTs) to monitor threats actively and assist organisations in recovering from cyber attacks. Discouraging ransomware payments is crucial and should not be supported or anchored in any cyber insurance policy. This aligns with the broader strategy of minimizing the financial incentives for ransomware attackers.

---

1 AFRIPOL is a technical institution of the African Union with a mandate to strengthen cooperation between the police agencies of AU member states in the prevention and fight against organized transnational crime, terrorism, and cybercrime.

2 GSMA, "The Mobile Economy Sub-Saharan Africa 2023", https://www.gsma.com/mobileeconomy/wp-content/uploads/2023/10/20231017-GSMA-Mobile-Economy-Sub-Saharan-Africa-report.pdf (Accessed 13 September 2023)

3 Positive Technologies, "Cybersecurity threat scape of African countries 2022-2023", 28 July 2023, https://www.ptsecurity.com/ww-en/analytics/africa-cybersecurity-threatscape-2022-2023/ (Accessed 25 August 2023)

4 Check Point, "What is Ransomware", https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/ (Accessed 2 September 2023)

5 Chinedu Okafor , "10 African countries with the best digital quality of life index", Business Insider Africa, 30 September 2022, https://africa.businessinsider.com/local/lifestyle/10-african-countries-with-the-best-digital- quality-of-life-index/71msdlz (Accessed 2 November 2023)

6 Sophos, "The State of Ransomware2023" https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf (Accessed 25 September 2023)

7 Interpol, "African Cyberthreat Assessment Report Cyberthreat Trends: Outlook by the African Cybercrime Operations Desk", March 2023, (Accessed 13 September 2023)

8 Jonathan Greig, "State-owned bank in South Africa confirms 'Akira' ransomware attack", The Record, 14 June 2023, https://therecord.media/development-bank-of-southern-africa-akira-ransomware-attack (Accessed 13 September 2023)

9 Ibid.

[10] Cybereason,"Ransomware: The True Cost To Business", 2022, https://www.cybereason.com/hubfs/Ransomeware_True_Cost_e-book_NewBrand.pdf (Accessed 22 October 2023)

[11] The White House, "Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021", 14 October 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/ (Accessed 7 November 2023)

[12] Ibid.

[13] Ibid.

[14] The White House, "FACT SHEET: The Second International Counter Ransomware Initiative Summit", 1 November 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/fact-sheet-the- second- international-counter-ransomware-initiative-summit/ (Accessed 27 November 2023)

[15] Ibid.

[16] The White House, "International Counter Ransomware Initiative 2023 Joint Statement", 1 November 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware- initiative-2023-joint-statement/ (Accessed 27 November 2023)

[17] Ibid.

[18] Interpol, "AFJOC - African Joint Operation against Cybercrime", https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/AFJOC-African-Joint-Operation- against-Cybercrime (Accessed 22 September 2023)

[19] Africa Defense Forum, "Africa Cyber Surge II Tackles Cybercrime Through International Cooperation", 19 September 2023, https://adf-magazine.com/2023/09/africa-cyber-surge-ii-tackles-cybercrime-through-international-cooperation/ (Accessed 15 October 2023)

[20] Africa Defence Forum, "ECOWAS Takes Joint Approach to Cybersecurity", 22 September 2023, https://adf-magazine.com/2023/09/ecowas-takes-joint-approach-to-cybersecurity/ (Accessed 15 October 2023)