



National Cyber Threat Forecast 2023

DECEMBER 2022

About CSEAN

Cyber Security Experts of Nigeria (CSEAN) was established as an advocacy group on all matters and challenges faced by information security in Nigeria to be an enabler focused on improving the standards and practices of Information Security in the country. CSEAN is a non-profit organisation centred on a collective purpose and vision to be a vehicle championing the cause and awareness of Information security best practices, acting as an agent of change to address Cyber Crime phenomena through engaging intellectual minds, business, and political leaders. As Cyber Security protagonists, we look to hold a healthy debate to expand the audiences' knowledge, awareness, and understanding of cyber-crime issues. Through workshops and seminars, we wish to share knowledge and grow the information security industry in the country while creating youth forums to breed future generations of information security professionals and to hold broader discussions with government officials on tackling Cyber Crime.

Authors

Oluwafemi Osho
John Odumesi
Hamzat Lateef
Hassanat Abdulraheem

Design

Moses Joshua

Contact

For further inquiries, please contact CSEAN's Director of Research and Development at rd@csean.org.ng

Legal Notice

This publication reflects the views and interpretations of CSEAN unless stated otherwise. It is not intended as a legal action on the part of CSEAN. CSEAN reserves the right to update this publication from time to time. External sources used in the report are referenced as appropriate, and CSEAN is not responsible for the content of such sources. This publication is provided for informational purposes only and must be accessed free of charge. CSEAN and any person acting on its behalf are not responsible for any use of the information contained in this publication.

Copyright Notice

© Cyber Security Experts of Nigeria (CSEAN), 2022. All rights reserved.

Reproduction of this work is authorized, provided that the source is acknowledged. For any use or reproduction of photos or other material not under the copyright of CSEAN, permission must be sought directly from the copyright holders.

Introduction

In 2022, we saw a significant increase in the complexity and impact of cyber threats worldwide, and Nigeria was no exception. As experts and active stakeholders in the cybersecurity sector, we collected and analyzed data from various sources, including cybersecurity professionals in the country, incident reports, and 2021 and 2022 threat trends, to present our forecast of cyber threats for 2023.

Several factors will contribute to the predicted threats, including the upcoming 2023 general elections, the economic situation in the country, a lack of transparency in reporting security breaches, and a lack of coordination among organisations within the same sector. Other contributing factors include inadequate and inconsistent responses to cyber threats by government and regulatory bodies, outdated government computing resources, a lack of incident response plans in many organisations, a shortage and an increase in the emigration of cybersecurity professionals, and frequent strikes in higher education institutions.

The cyber threats are categorized and discussed under two sections: (i) election-related threats and (ii) regular and emerging threats.

2023 Elections and the Deluge of Cyber Threats



Spread of Misinformation and Disinformation

It is expected that there will be a significant amount of misinformation and disinformation circulated through social media platforms in the run-up to, during, and after the 2023 general elections. We are very likely to experience the weaponization of manipulated information to influence people's perceptions and behaviours in relation to the elections. This can seriously affect the integrity of the electoral process and undermine public trust in democratic institutions. Disinformation, specifically related to the elections, is likely to increase, with political parties potentially hiring foreign actors to create and disseminate false or misleading information. Nigeria had a taste of weaponized, coordinated propagation of disinformation during the 2019 general elections¹. It is crucial for individuals to be vigilant and critically evaluate the information they come across, particularly during election periods. It is also vital for social media platforms and government agencies to take steps to address the spread of misinformation and disinformation, such as through fact-checking efforts and public education campaigns.



Hate Speech

In the past, Nigerian elections have been marred by instances of hate speech and threatening expressions by politicians². This trend is highly likely to continue as the 2023 general elections draw closer. This type of language can incite violence and create a toxic political environment. Political actors need to refrain from using hate speech and promote a respectful and peaceful campaign. It is also the responsibility of the government and relevant authorities to take action against hate speech and ensure that the elections are conducted in a fair and peaceful manner. The upcoming 2023 general elections will be an opportunity for Nigeria to demonstrate its commitment to democracy and peaceful transitions of power. Political actors must work to ensure that the elections are conducted in a way that respects the rights and dignity of all Nigerians.



Malinformation/Cyber Smearing

The public has the right to accurate and reliable information to make informed decisions about their leaders. Regrettably, we have seen reports of private information being made public to malign individuals or groups³. There have also been instances where true information was shared out of context in an attempt to mislead the public⁴. Over the next year, we will witness more of such occurrences in the lead-up to the elections. These types of behaviour are unethical and can create a toxic political environment. Politicians have the responsibility not only to provide accurate and reliable information to the public but also to refrain from sharing private or true information out of context to mislead the public.

¹<https://apnews.com/article/8c5eec1f55bd4e209edbf5f9401e87c2>

²<https://humanglemedia.com/2023-these-politicians-are-fueling-violence-with-the-spread-of-hate-speech/>

³<https://www.vanguardngr.com/2022/09/adamus-letter-to-tinubu-is-apc-nwcs-position-officials-insist/>

⁴<https://factcheck.afp.com/doc.afp.com.32JH7WY>



Attacks Against INEC cyberinfrastructure

We forecast that INEC cyberinfrastructure will be targeted in the lead-up, during, and after the elections. Attacks will include cyber-based threats, such as the defacement of the INEC website and hacking of the Bimodal Voter Accreditation System (BVAS), as well as physical-based attacks, including arson and vandalism. If the frequency of attacks and arson on INEC facilities from 2021⁵ is anything to go by, we are in for more of such as we approach the general elections. INEC must be prepared for these types of attacks and to have measures in place to protect its cyberinfrastructure to ensure the integrity of the electoral process.

⁵<https://radionigeria.gov.ng/2022/12/01/repes-condemn-burning-of-inec-offices/>

Regular and Emerging Threats



Government Infrastructure as a Target (GlaaT)

In 2023, we envisage an increase in the exploitation of computing resources of government establishments for malicious use. Further, more government-related data will be exfiltrated. Based on the data gathered this year, we found threat actors exfiltrating critical information and maliciously leveraging government computing resources, including mining cryptocurrency and setting up Internet Relay Chat (IRC) platforms. Findings also revealed activities related to credential theft and backdoor setup. Threat actors leverage outdated and vulnerable internet-facing applications in most of these identified facilities. Government establishments need to be aware of these potential threats and take steps to secure their computing resources and protect them against data exfiltration. This may involve regularly updating and patching internet-facing applications and systems to ensure they are not vulnerable to exploitation.



Malware

Malware is a family of software designed for malicious purposes. In 2021, Nigeria experienced an onslaught of Trojans, Trojan-downloaders, and Trojan-droppers⁶. 2022 brought about an escalation in backdoor infections⁷. As one of the most common attacking tools preferred by cyber threat actors, malware will continue to be relied on by the actors in 2023. If they want to be secure from malware infection, individuals and organizations will do well to keep their operating systems and software up to date, adopt a strong password policy, ensure periodic backing up of data, and be cautious with clicking links.



Another Year of Ransomware

Ransomware, a type of malware, has gained popularity in recent years and therefore warrants being discussed as a standalone topic. In 2021, a significant percentage of organisations in Nigeria reported experiencing ransomware attacks, according to Sophos⁸. 2022 saw the first publicly reported Ransomware attack against a betting company in the country by BlackCat⁹. As the ransomware-as-a-service (RaaS) ecosystem continues to evolve, ransomware attacks will become more sophisticated and more common in Nigeria in 2023. Threat actors are likely to focus on devices with weak security and easily exploitable vulnerabilities. Small and medium-sized enterprises (SMEs) are particularly vulnerable to ransomware attacks, as they may not have the resources or expertise to implement advanced security solutions. To mitigate the risk of ransomware attacks, individuals and organisations in Nigeria should keep software and systems up to date, use antivirus software, regularly back up important data, enable two-factor authentication, educate employees on cybersecurity best practices, and consider implementing advanced security solutions.

⁶<https://guardian.ng/technology/nigeria-kenya-south-africa-responsible-for-30000-malware-attacks-in-six-months/>

⁷<https://www.telecomreviewafrica.com/en/articles/general-news/2958-backdoor-attacks-blew-up-in-africa-in-q2-2022>

⁸<https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf>

⁹<https://www.bankinfosecurity.com/blackcat-attack-on-betting-company-disrupts-service-a-18886>



Attacks on Financial Institutions

Over the years, attacks against banks and FinTech organisations in Nigeria have shifted from low-tech to high-tech, sophisticated breaches. We experienced an onslaught of financial phishing attacks¹⁰ and the danger of organized targets¹¹. As the country launches new Naira notes and transitions to a new democratic government in 2023, it is expected that the financial sector will continue to be a target for cybercriminals. These attackers may seek to collaborate with bank employees to gain unauthorized access to critical systems and obtain sensitive information that can be used to exploit the bank's systems. Threat actors may also use traditional tactics such as malware, social engineering, and phishing campaigns to lure employees and customers into revealing sensitive information. To protect against these types of attacks, financial institutions in Nigeria should implement strong security measures, educate employees on cybersecurity best practices, and regularly update their systems and software with the latest security patches.



Attacks in the Cloud

Following the COVID-19 pandemic, more organisations have wholly or partly adopted enterprise-wide cloud for IT operations. As expected, cybercriminals have ramped up attacks. Research has shown that cloud adoption is expected to increase significantly over the next two years¹². This will translate to an expansion in the threat surface. Thus, we forecast increased attacks on cloud infrastructure in 2023. Organisations should integrate security into the planning and operation of cloud services. It is also critical for them to invest in cloud-threat detection capabilities and identity perimeter to protect their cloud assets.



Menace of Insider Threats

Insider collaborators will continue to pose a significant threat to organisations in Nigeria in 2023. Insider threats are threats to an organisation that comes from individuals within the organisation, such as employees, contractors, or business associates, who have insider knowledge of the organisation's security practices, data, and digital networks. These individuals may intentionally or unintentionally expose the organisation to risks, such as data breaches, unauthorized access to systems, or theft of sensitive information. We saw cases of employees being lured with money to divulge sensitive organization information in 2022¹³. More of such is likely to occur in 2023. There are several countermeasures organisations in Nigeria can take to mitigate the risk of insider threats in 2023. These include conducting thorough background checks on new hires to ensure that they do not have a history of malicious activity or security breaches, implementing access controls to limit the amount of information and resources that employees have access to, monitoring employee activity on networks and systems to detect suspicious behaviour, providing security awareness training to educate employees on the importance of protecting sensitive information and how to identify and report potential insider threats, and implementing technical controls such as data loss prevention systems

¹⁰<https://furtherafrica.com/2022/09/30/financial-cyberattacks-increased-in-kenya-and-nigeria-in-q2-of-2022/>

¹¹<https://www.bankinfosecurity.com/nigerian-police-bust-gang-planning-cyberattacks-on-10-banks-a-19320>

¹²<https://news.microsoft.com/en-xm/2022/10/03/as-cloud-adoption-increases-data-breaches-top-the-list-of-security-concerns-for-nigerian-cios/>

¹³<https://aag-it.com/the-latest-2022-cyber-crime-statistics/>

to help prevent the unauthorized transfer of sensitive information. By implementing these countermeasures, organisations can better protect themselves against the risks posed by insider threats.



Cryptocurrency-Based Threats

The cryptocurrency industry has undergone significant changes and developments in recent years, and it has become an increasingly popular and widely adopted form of digital currency. 2022 has been a rollercoaster year for the industry. At the same time, the industry experienced an increase in the number of threats. This includes various types of cyberattacks and scams that aim to steal or fraudulently obtain cryptocurrencies from individuals and organisations. We forecast this trend to continue in 2023. Threat actors may use a variety of methods to carry out attacks, such as malware that is spread through cracked software or games from torrent sites or phishing scams that use fake websites or emails to trick people into giving away their login credentials or personal information. To protect themselves and their assets, cryptocurrency users should be aware of these risks and take steps to protect themselves and their assets. This might include using strong passwords, enabling two-factor authentication, and being cautious when clicking on links or downloading software.



Ponzi Schemes, Rug Pull, Pump and Dump

Ponzi schemes¹⁴ and crypto and forex trading rug pull are two of the many financial frauds Nigerians have been contending with in recent years. While these threats are inherently not cyber threats, perpetrators leverage cyberspace to pull off frauds. These scams thrive on people's vulnerability to the promise of quick returns. With a growing interest in crypto in Nigeria, which has made the country to be labelled the most crypto-obsessed nation¹⁵, Nigerians will remain susceptible to these kinds of threats. Individuals must be vigilant and cautious when considering investment opportunities to protect themselves against these risks.



Phishing and Social Engineering

Social engineering has remained one of the most powerful techniques used by threat actors for malicious purposes. Phishing, a social engineering attack, has evolved over the years. Despite widespread awareness of these types of attacks, many people are still susceptible to them, and our data shows that phishing attacks continue to be successful. In some cases, threat actors have even been able to use the InterPlanetary File System (IPFS) to host their phishing platforms, further increasing the likelihood of success. To protect against these types of attacks, it is important for individuals to be aware of the risks and to take steps to protect themselves, including being suspicious of unsolicited emails or messages, not clicking on links or downloading attachments from unfamiliar sources, and enabling two-factor authentication whenever possible.

¹⁴<https://guardian.ng/business-services/nigerians-lose-over-n911b-to-ponzi-schemes-related-fraud-in-23-years/>

¹⁵<https://cointelegraph.com/news/nigeria-becomes-the-most-crypto-obsessed-nation-after-april-crash-report>



SMEs Will Feel the Brunt of Cyber Threats More

According to reports, small and medium-sized enterprises suffered increased password stealing, Internet, and Remote Desktop Protocol (RDP) attacks in 2022, compared to 2021¹⁶. This trend is very likely to continue in 2023. SMEs may be easier targets for cyber threat actors, and there are several reasons for this. Generally, small businesses have limited resources to invest in cybersecurity, may have fewer IT staff or less expertise in cybersecurity, and often lack the level of security awareness that big organisations have. SMEs must be aware of the cyber risks associated with their business and take necessary steps to protect their systems.



Privacy Breaches by Online Money Lenders

Digital money lending services, which offer short-term loans to individuals, were introduced in Nigeria to provide easy access to credit for ordinary people. However, many of these operators have been ignoring the Nigerian Data Protection Regulation (NDPR) and violating the data privacy rights of their customers. Reports suggest that they have been accessing the phone details of the family members of defaulted loanees without authorization and then contacting the family members via text messages containing threatening and derogatory content¹⁷. This behaviour is a clear breach of data privacy rights and will likely continue if relevant regulatory institutions do not address it. To protect against data privacy violations in Nigeria's digital money lending industry, regulatory bodies should enforce the Nigerian Data Protection Regulation (NDPR) and implement stricter penalties for violators. Consumers should also be educated on their data privacy rights and how to protect them. They should be cautious when taking out short-term loans, reviewing the terms and conditions to ensure their data will be protected.



Increased Cyber Attacks through Networks of Higher Institutions

Unfortunately, it is common for higher education students to become involved in online scamming, often using the networks and resources of their schools to launch their attacks. The long-term strikes and disruptions in the education sector in Nigeria may have contributed to an increase in the number of individuals participating in online scams, as some students may be seeking alternative sources of income. As a result of this trend, more online scams will likely be launched from behind the networks of higher education institutions in the country. Higher education institutions can mitigate the trend of online scammers exploiting their networks by educating students about the risks of online scams, implementing strong cybersecurity measures, monitoring and enforcing appropriate use of institutional networks, encouraging students to report suspicious activity, and working with law enforcement.

¹⁶<https://kaspersky.africa-newsroom.com/press/small-businesses-in-nigeria-are-still-in-danger-facing-an-89-increase-in-remote-desktop-protocol-attacks-in-2022?lang=en>

¹⁷<https://www.premiumtimesng.com/news/headlines/499999-investigation-how-digital-loan-providers-breach-data-privacy-violate-rights-of-nigerians.html>

Conclusion

In 2023, Nigeria will face a range of cyber threats that will be perpetrated by threat actors using a variety of tactics, techniques, and procedures. The threats will include large-scale propagation, and potential weaponization, of mis/disinformation, ransomware attacks, and phishing attacks, among others. One of the main factors that are expected to influence the cyber threat landscape of 2023 is the general elections. To mitigate these threats, individuals, organizations, and relevant government bodies must adopt appropriate cybersecurity measures and strategies. Furthermore, all stakeholders must work together to ensure a concerted effort to protect the cyber sovereignty of the country. Cybersecurity is a collective responsibility



CSEAN

CYBER SECURITY EXPERTS
ASSOCIATION OF NIGERIA

Learn more at www.csean.org.ng

CSEAN
Suite C4, HCR Plaza
521 Sylvester U. Ugoh Crescent,
Jabi, Abuja, Nigeria
info@csean.org.ng

© Cyber Security Experts of Nigeria (CSEAN), 2022. All rights reserved.