CYBERSECURITY THREAT LANDSCAPE IN NIGERIA

Prevalent Threats and Key Actors

Ashekode Jamal ODIOMONAFE

30th November, 2024

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

This report highlights the critical cybersecurity challenges facing Nigeria's digital ecosystem, emphasizing the prevalent threats, key malicious actors, software risks, and notable cyberattacks over the past five years. It identifies ransomware, phishing, Business Email Compromise (BEC), and AI-driven threats as the most significant risks to organizations, coupled with insider threats. Key malicious actors include local fraud syndicates, international threat groups like APT33 and APT41, and ransomware gangs such as LockBit and Conti. Common software risks, particularly the use of pirated software and unpatched systems, exacerbate vulnerabilities. Recommendations provided include strengthening awareness training, collaborating with agencies, deploying advanced security tools, enforcing multi-factor authentication, and investing in secure software. These measures aim to fortify the nation’s defenses against an increasingly sophisticated threat landscape.

2 INTRODUCTION

The rapid digital transformation across Nigeria has brought remarkable economic growth but has also introduced a complex array of cybersecurity challenges. From the rise of fintech platforms to the growing reliance on cloud services, organizations face evolving threats that jeopardize critical assets and sensitive information. This report delves into the prevalent cybersecurity threats in Nigeria, key malicious actors behind these attacks, software risks stemming from outdated and pirated systems, and major incidents affecting critical sectors. Drawing on these findings, the report proposes actionable recommendations to enhance cybersecurity resilience, ensuring sustainable digital progress for the nation.

3 FINDINGS

3.1 PREVALENT THREATS

I. Ransomware Attacks

Ransomware attacks have become one of the most significant cyber threats in Nigeria and the world at large. These attacks target organizations by encrypting critical data and demanding payment, often in cryptocurrency, for the decryption keys. Recent incidents have shown an uptick in ransomware targeting sectors like telecommunications, education, and financial institutions. Tactics such as double-extortion—where attackers threaten to release stolen data in addition to encryption—are becoming more common, also Use of ransomware-as-a-service (RaaS) platforms, allowing less sophisticated threat actors to launch attacks. Attackers frequently exploit vulnerabilities in outdated systems or unprotected endpoints to gain access to sensitive networks.

II. Phishing Scams:

Phishing scams remain the most pervasive cyber threat in Nigeria, affecting both individuals and businesses. Attackers use fake emails, text messages, or social media communications to deceive victims into divulging sensitive information, such as credentials or financial data. Small and medium-sized enterprises (SMEs) are particularly vulnerable due to weaker defenses, while executives and high-ranking officials are often targeted through spear-phishing—a more personalized form of phishing. The increasing availability of phishing kits and AI-driven tools has become widely available on the dark web enabled attackers to scale and refine these campaigns.

III. Business Email Compromise (BEC):

Business Email Compromise (BEC) attacks are a sophisticated form of phishing where cybercriminals impersonate trusted individuals such as executives, vendors, or partners to manipulate employees into authorizing fraudulent transactions. These attacks are particularly prevalent in Nigeria's financial and oil sectors, where the stakes are high. Threat actors exploit weaknesses in email authentication protocols (e.g., DMARC not implemented) and leverage social engineering to make their emails appear legitimate. Notable cases have resulted in significant financial losses for targeted organizations, highlighting the need for better email security practices. This has propagated increased targeting of international clients of Nigerian businesses and the use of machine learning to craft convincing messages.

IV. **AI-Driven Threats**:

AI-driven threats are emerging as a new frontier in cybercrime. Threat actors are leveraging artificial intelligence and machine learning to increase the scale and sophistication of their attacks. Techniques include using deepfake technology to impersonate individuals in audio or video, automating phishing campaigns for greater personalization, and deploying AI-enhanced malware that can evade traditional security measures. These capabilities enable attackers to target victims with greater precision and effectiveness.

V. **Insider Threats**:

Insider threats, whether intentional or accidental, are a growing concern in Nigeria. (Aimuengheuwa, 2024). Poor access control measures and insufficient employee training often leave organizations vulnerable to malicious or careless insiders. With the rise in remote, the attack surface has expanded, further increasing the likelihood of unintentional breaches. Such incidents are challenging to detect because they originate within the organization and often exploit legitimate access to systems and data. This underscores the need for stronger internal controls and continuous monitoring.

These threats collectively emphasize the need for robust cybersecurity measures, enhanced awareness, and stricter enforcement of security policies to safeguard Nigeria’s digital landscape.

3.2 KEY MALICIOUS ACTORS

I. Local Fraud Syndicates

Local cybercriminal groups in Nigeria have gained infamous for their involvement in phishing and financial scams. Often referred to as "Yahoo" boys, these individuals or sometimes found in groups (HKs) use social engineering to exploit unsuspecting victims (Olayinka, 2019). Their methods include creating fake investment schemes, impersonating legitimate businesses, and executing romance scams. These syndicates leverage readily available phishing kits and exploit the lack of cybersecurity awareness among individuals and smaller businesses. The proceeds from these activities are often laundered or used to fund further criminal operations.

II. International Threat Groups

Global Advanced Persistent Threat (APT) groups are actively targeting Nigeria, particularly its oil and gas sectors and critical infrastructure.

i. **APT33**: A threat group associated with Iranian interests, APT33 focuses on the oil and gas sector, using tools like Shamoon malware for data destruction and espionage. Their campaigns aim to disrupt operations and steal valuable intellectual property related to energy resources.

ii. **APT41**: A China-linked cyber-espionage group known for targeting governments and enterprises worldwide. In Nigeria, APT41 has shown interest in government and telecommunications sectors, aiming to gather intelligence and exploit vulnerabilities.

These groups employ sophisticated tools and techniques, such as spear-phishing, zero-day exploits, and backdoors, making them formidable adversaries.

3. Ransomware Gangs

Ransomware groups have increasingly targeted Nigeria due to the country’s growing reliance on digital platforms. Prominent groups include:

i. **LockBit**: Known for its highly automated ransomware-as-a-service (RaaS) model, LockBit has targeted various Nigerian enterprises, encrypting systems and demanding hefty ransoms. They also engage in double-extortion tactics, threatening to leak stolen data if their demands are unmet.

ii. **Conti**: This notorious ransomware gang has targeted financial institutions and businesses in Nigeria. Their attacks typically involve exploiting Remote Desktop Protocol (RDP) vulnerabilities and phishing schemes to gain access to systems. Conti is also known for its extensive use of encryption and data exfiltration techniques.

These ransomware gangs are part of a global trend that leverages sophisticated tools and operational efficiency, often operating from regions with limited extradition agreements, which makes them difficult to prosecute.

These malicious actors represent a diverse spectrum of threats, from local scams to international espionage and ransomware campaigns. Combating them requires a combination of improved cybersecurity infrastructure, international collaboration, and robust legal frameworks.

3.3 SOFTWARE RISKS

Commonly Used Software

i. **Microsoft Windows**: Microsoft Windows remains the dominant operating system across Nigeria. However, the widespread use of pirated versions poses a significant security risk. These unauthorized versions often lack essential security updates, leaving systems vulnerable to exploitation by malware and ransomware attacks.

ii. **Fintech Tools**: With the rapid growth of the fintech sector, platforms like **Flutterwave** and **Paystack** are widely adopted for payment processing and online transactions. While they are well-secured, the broader ecosystem of smaller payment providers and merchants using outdated or unpatched integrations can become weak points.

iii. **Local Cloud Providers**: Local cloud service providers, though cost-effective, often struggle with maintaining updated security protocols. Many businesses also rely on shared hosting services, which increases the likelihood of cross-tenant vulnerabilities if one account is compromised.

iv. **Website Technologies**: A significant portion of Nigerian websites are built using open-source platforms such as **WordPress**. When these platforms are not regularly updated or are paired with pirated plugins, they become easy targets for hackers. These vulnerabilities are exploited for defacements, phishing schemes, or malware injection.

Risks Associated with Software Use

i. **Unpatched Vulnerabilities**: Many pirated software versions do not receive official patches, leaving systems exposed to known exploits. This is particularly risky for business-critical systems such as enterprise resource planning (ERP) platforms or financial transaction systems.

ii. **Outdated Software**: Businesses and government agencies often rely on outdated software due to budget constraints or limited technical expertise. Legacy systems without active vendor support create significant cybersecurity gaps.

iii. **Insecure Third-Party Applications**: The dependence on third-party apps, especially in sectors like retail, education, and health, exposes organizations to risks if those applications are not vetted or regularly updated.

iv. **Pirated Software Risks**: Beyond the lack of updates, pirated software frequently contains embedded malware, providing a backdoor for attackers. This is a prominent issue in Nigeria’s SMB sector, where cost-saving measures often take precedence over security.

v. **Cloud Security Challenges**: While local cloud providers are growing in popularity, they sometimes fall short in implementing best practices such as robust encryption, incident response plans, and multi-layered defenses. Additionally, data residency laws and poor contract management may hinder adequate risk management.

Major Attacks that have rocked the Nigeria over the past five years

S/N	Name of Organization	Sector	Attack Type / Technique	Threat Actor	Period of Discovery	Discovered By
1.	Globacom	Telecommunications	Ransomware (Phobos Group). (Olowogboyega, 2024)	Phobos Ransomware Group	2023-2024	ngCERT
2.	MTN		DDoS Attack (Pandagle, 2023)	Anonymous Sudan. Pro-Niger Hackers	2023	
			Theft Airtime and Data valued N1.9bn	Two Polytechnic students	2024	NPF-NCCC
3.	Government Ministries	Government	Advanced Persistent Threat (APT)	Gamaredon, Lyceum	2024	Cybervergent Analysis
4.	Financial Institutions	Financial	Credential Theft, Ransomware	Gelsemium, Circus Spider	2024	Reports from Nigerian Banks
5.	Multiple Oil Companies	Oil and Gas	Phishing, Malware Infiltration	Unknown	2021-2023	IT Security Firms

3.4 KEY OBSERVATIONS:

1. **Ransomware Surge**: Groups like Phobos have targeted critical cloud and telecom providers, exploiting vulnerabilities in Remote Desktop Protocol (RDP) and phishing emails.

2. **Financial Institutions**: These have faced ransomware attacks, credential theft, and insider threats, often linked to sophisticated groups like Gelsemium and Circus Spider.
3. **Government Agencies**: APT groups such as Gamaredon have focused on espionage, targeting critical national infrastructure and public administration.
4. **Oil Sector**: The oil and gas industry has been a frequent target of phishing and malware, particularly due to its high-value intellectual property.

4 RECOMMENDATIONS

I. **Conduct Security Awareness Training**: Employees are often the first line of defense against cyber threats. Regular security awareness training should be implemented to educate staff on recognizing phishing attempts, fraudulent emails, and other common cyberattack techniques. These training sessions should also include simulations of real-world attacks to enhance preparedness.

II. **Collaborate with Cybersecurity Agencies**: Organizations should actively collaborate with Nigerian cybersecurity agencies like the **Nigerian Communications Commission (NCC)**, the **Nigeria Computer Emergency and Response Team (ngCERT)** and the **National Information Technology Development Agency (NITDA)**. These agencies provide critical threat intelligence, guidelines, and resources that can help organizations strengthen their cybersecurity posture. Participation in public-private partnerships and information-sharing initiatives can also improve overall resilience.

III. **Deploy Endpoint Security Tools**: Employing services of Managed Cybersecurity Service Providers proficiently aid in deploying and managing all endpoint security tools across all devices within the organization. These tools offer advanced threat detection, malware prevention, and incident response capabilities, ensuring endpoints are safeguarded against evolving cyber threats.

IV. **Implement Robust Patch Management**: Outdated software is a significant vulnerability exploited by attackers. Organizations should establish a structured patch management program to ensure all software, including operating systems and third-party applications, is regularly updated with the latest security patches. Automated patch management tools can streamline this process.

V. **Enforce Multi-Factor Authentication (MFA)**: Multi-factor authentication adds an extra layer of security to sensitive accounts by requiring multiple forms of verification, such as an authentication app. This reduces the risk of unauthorized access, even if login credentials are compromised.

VI. **Invest in Secure Software and Infrastructure**: Replace pirated or outdated software with licensed and secure versions to eliminate risks associated with unpatched vulnerabilities and embedded malware. Local businesses should also vet their cloud providers to ensure compliance with security best practices, including data encryption, backup systems, and incident response protocols.

VII. **Adopt Advanced Cybersecurity Frameworks**: Implement internationally recognized frameworks such as the **NIST Cybersecurity Framework** or **ISO 27001** to establish and maintain comprehensive cybersecurity policies and procedures. These frameworks help identify, protect, detect, respond to, and recover from cybersecurity incidents.

VIII. **Perform Regular Security Audits and Penetration Testing**: Periodic audits and penetration tests can help organizations identify vulnerabilities in their systems before attackers exploit them. Engaging professional cybersecurity firms to perform these assessments ensures an unbiased evaluation of the organization's defenses.

IX. **Develop an Incident Response Plan**: Organizations must have a documented and tested in-house incident response plan that outlines steps to take in the event of a cybersecurity breach. This plan should include roles and responsibilities, communication protocols, and recovery procedures to minimize damage and downtime.

X. **Promote a Culture of Cybersecurity**: Leadership should prioritize cybersecurity at all levels of the organization. By integrating security into the corporate culture and holding everyone accountable, organizations can reduce the risk of human error and foster proactive risk management practices.

By adopting these measures, organizations can significantly enhance their cybersecurity defenses and mitigate the risks posed by evolving cyber threats in Nigeria.

5 CONCLUSION

Nigeria’s cybersecurity landscape faces formidable challenges as threat actors exploit vulnerabilities in software, systems, and human behavior. The surge in ransomware, phishing, and insider threats underscores the urgency for robust defenses, particularly against sophisticated attackers like APT33 and ransomware gangs such as LockBit. The use of pirated and unpatched software, coupled with limited cybersecurity awareness, amplifies the risks. By implementing the recommended measures—including regular training, adopting advanced frameworks, and enhancing collaboration with cybersecurity agencies—Nigeria can mitigate these risks and create a secure digital environment. The call to action is clear: a collective effort from businesses, government agencies, and individuals is essential to safeguard Nigeria’s digital infrastructure against an ever-evolving threat landscape.

REFERENCES

Abuchi, J., & Abuchi, J. (2023, February 9). NCC alerts Nigerians against latest cyber threats THE AUTHORITY NEWS. https://authorityngr.com/2023/02/09/ncc-alerts-nigerians-against-latest-cyber-threats/

Aimuengheuwa, J. (2024, September 16). Cybervergent reveals 37% surge in Africa's cyber threats, over 586,000 detected in H1 2024. Tech | Business | Economy. https://techeconomy.ng/cybervergent-reveals-37-surge-in-africas-cyber-threats-over-586000-detected-in-h1-2024/

Famous DDoS attacks | Biggest DDoS attacks | Cloudflare. (2024). https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/

Olayinka, W. (2019, July 26). Yahoo Yahoo: Inside the life of a Nigerian cyber criminal. TechCabal. https://techcabal.com/2019/07/26/yahoo-yahoo-inside-the-life-of-a-nigerian-cyber-criminal/

Olowogboyega, O. (2024, October 21). The Globacom breach: How hackers held Nigeria's telco giant hostage. TechCabal. https://techcabal.com/2024/10/21/how-hackers-held-globacom-hostage/

Pandagle, V. (2023, August 3). Anonymous Sudan hacker group claims the MTN cyber attack. *The Cyber Express*. https://thecyberexpress.com/mtn-cyber-attack-anonymous-sudan-group/