Whitehat.NG 2024 Annual Report

whitehat.NG
S CYBERSPACE ISAC + PEOPLE CERT
ee Something,
Say Something But
Responsibly
Report and Fix:
Discover and report security vulnerabilities in Ni
digital applications and systems with our respo
disclosure program.
Track and Analyze:
Stay updated on the latest cyberse
Nigeria with our repository of ev
Collaborate and Innovate:
Partner with privat and public organ
cybersecurity in tives and project
cyberspace

cert@projectwhitehat.ng

Report Outline

whitehat.ng

Introduction

Whitehat.NG

whitehat.ng

Introduction

Whitehat.NG is a comprehensive community initiative focused on enhancing cybersecurity in Nigeria. With a multifaceted approach, the project addresses various aspects of cybersecurity and currently operates as the community CERT/ISAC, equipped with diverse capabilities.

It features a responsible disclosure program that allows for the ethical reporting of security vulnerabilities in Nigerian digital applications and systems, thereby contributing to the overall security of the country's digital infrastructure.

Whitehat.NG also maintains a repository of events and reports, keeping stakeholders informed about the latest cybersecurity incidents in Nigeria. .

This resource facilitates in-depth analysis and understanding of cybersecurity trends and patterns within the country.

The project actively promotes collaboration with both private and public organizations on cybersecurity initiatives, fostering innovation and effective strategies to secure Nigeria's cyberspace.

Additionally, Whitehat.NG offers workshops and sessions on various cybersecurity topics and skills, empowering individuals with the knowledge and expertise necessary to enhance cybersecurity efforts in Nigeria

Introduction

By reporting and disclosing security vulnerabilities, this project will enhance the safety of cyberspace in Nigeria by promoting a culture of responsible disclosure and proactive vulnerability management.

This strategy aligns with the project's **"Report and Fix"** initiative, encouraging the identification and reporting of security vulnerabilities in Nigerian digital applications and systems. This proactive approach enables organizations to address vulnerabilities swiftly, thereby improving their cybersecurity posture and minimizing the risk of exploitation.

The project's focus on **"Track and Analyze**" will benefit from these reports, as they will enrich the repository of cybersecurity incidents in Nigeria.

This repository will offer valuable insights into emerging threats and trends, allowing stakeholders to stay informed about the latest cybersecurity incidents and take proactive measures to safeguard digital assets.

In line with **"Collaborate and Innovate"** the responsible disclosure of these vulnerabilities will foster partnerships among private and public organizations on cybersecurity initiatives.
By collaborating to address these vulnerabilities, stakeholders can innovate together and develop best practices for securing Nigeria's cyberspace.

Finally, by sharing information about these vulnerabilities and their impacts, the project will support **"Learn and Grow"** by providing real-world case studies for educational resources.

Introduction

VULNERABILITY REPORTING
INITIATIVE FOR EDUCATION

To improve outcomes in each project focus area, we introduced initiatives that further emphasize critical areas identified from our 2023 operational data.

One of these new initiatives is the **Vulnerability Reporting Initiative for Education (VRIE),** which aims to enhance the cybersecurity resilience of educational institutions in Nigeria, ultimately protecting the digital infrastructure and safeguarding the data of students, faculty, and staff.

234 Cyber Task Force

Another initiative is the **234 Cyber Task Force (234-CTF)**, dedicated to combating malicious content and phishing on social media platforms, which is essential in today's digital landscape. By concentrating on detection, prevention, education, and collaboration, this task force will play a crucial role in protecting users and fostering a safer online community.

Immediate action is needed to tackle the growing threats posed by cybercriminals and to ensure the integrity of social media interactions.

Responsible Disclosure

Whitehat.NG

Rsponsible Disclosure

In our commitment to responsible disclosure in 2024, we identified and reported several vulnerabilities that significantly impacted the personally identifiable information (PII) of individuals and exposed organizations to non-compliance risks.

The following vulnerabilities were noted: Directory Traversal, Remote Code Execution (RCE), Insecure Direct Object Reference (IDOR), Poor Authentication and Session Management, Misconfigured Services in Web and API, Use of Default Credentials, SQL Injection Vulnerability, and Flawed Design Logic and Information Disclosure.

Our team's timely disclosure of these vulnerabilities played a crucial role in keeping organizations and individuals safe.

By reporting these issues promptly, we enabled organizations to take corrective actions before any potential exploitation could occur.

However, we faced challenges in reaching some organizations to communicate these vulnerabilities effectively. Fortunately, our partnership with the National CERT (ngCERT) and the Government CERT (CERRT.ng) proved invaluable in addressing these unreachable entities. Their support facilitated communication and ensured that critical information was relayed to the appropriate parties, ultimately enhancing the security posture of affected organizations.

Responsible Disclosure

These vulnerabilities highlight critical areas of concern that require immediate attention to safeguard sensitive information and ensure compliance with regulatory standards.

In 2024, over **50 responsible disclosures** were made across various sectors. The distribution of disclosures by category reveals significant trends in cybersecurity vulnerabilities.

The Education sector accounted for the largest portion, with 48% of the total disclosures, totaling 24 reports. This was followed by the Government sector, which represented 28% with 14 disclosures. The Health, Telecom, and Banking/Fintech sectors each contributed 6%, amounting to 3 disclosures per sector.

Additionally, the Information Technology sector had 4% of the disclosures, totalling 2 reports. Lastly, both the Construction and New Media sectors accounted for 2% each, with 1 disclosure in each category. This breakdown illustrates the diverse landscape of responsible disclosures and highlights the sectors most impacted in 2024.

By engaging with stakeholders in these sectors, proactive steps have been taken to address vulnerabilities, mitigate potential risks, and contribute to the overall security of digital systems and data.

The collaborative nature of these disclosures reflects a concerted effort to promote transparency, accountability, and continuous improvement in cybersecurity practices across multiple sectors.

By the Numbers

3	BANKING & FINANCE
14	GOVERNMENT
24	EDUCATION
3	TELECOMMUNICATION
2	INFORMATION TECH.
1	NEW MEDIA
1	CONSTRUCTION
3	HEALTH

The vast majority of disclosure activities are centered on identifying and addressing vulnerabilities that ultimately lead to unauthorized access to Personally Identifiable Information (PII)

Note **–** Addressing ongoing findings, some affected parties have been unresponsive.

Nigeria’s Cyberspace
ISAC + PEOPLE CERT

1

Detected the existence of a directory traversal vulnerability on the university's website. This vulnerability allowed an attacker to access and view files and directories outside of the web root directory, potentially exposing sensitive information.

This poses a critical risk to the company's operations, privacy, and security.

Industry - Education

2

Identified a directory traversal vulnerability in the medical professional portal. This misconfiguration exposes sensitive Personally Identifiable Information (PII) of members, potentially allowing unauthorized access to personal data.

This presents a severe risk to the security and privacy of the individuals affected and the organization's compliance with data protection regulations.

Industry - Government / Health

3

Reported a significant security concern on a portal at development (based on data found on the platform). The researcher discovered the platform was using default credentials, granting unauthorized access to sensitive information within the portal.

This poses a critical risk to the security and confidentiality of user data, and integrity of the portal

Industry - Information Technology

whitehat.ng

Nigeria's Cyberspace
ISAC + PEOPLE CERT

4

Leakage of student biodata information and other sensitive information personally relating to the Next of Kin (NoK) PII in the process as well - Unauthenticated access via poorly managed session, and directory transversal made this possible

This represents a critical risk to the security and confidentiality of sensitive data

Industry - Education

5

Identified an insecure direct object reference (IDOR) vulnerability on a digital repository platform. This allows unauthorized access to internal memos, communiques, and other sensitive information about the government.

This presents a severe risk to the privacy and security of the affected platform, as well as the confidentiality of the system and its data.

Industry - Government

6

Discovered a zip file containing the source code of a payment app on a server. This vulnerability, allows anyone with access to the server to download and inspect the source code.

This poses a severe risk to the security of the application, as well as the confidentiality of any data accessible through these source code.

Industry - Banking and Finance

7

Sensitive data exposure of personally identifiable information of student applying for admission such as email, DOB, addrsss, and other found on student application list available due to a misconfigure server.

This poses a critical risk to the security and confidentiality of sensitive data

Industry - Education

8

Over 10GB of files relating to students, and staff data discovered on a university portal via a directory transversal vulnerability.

This poses a critical risk to the security and confidentiality of sensitive data

Industry - Education

9

Wireless Access Points were found to be using default credentials and had their web management portal enabled, exposing them to potential exploitation by malicious actors.

This presents a severe risk to the security of customers and operations of the telecom service provider.

Industry - Telecom

10

SQL injection on a government website leads to full database access. This vulnerability was found to have been exploited to defaced some part of the website at the point of reporting

This poses a critical risk to the web platform potentially leading to unauthorized access and modification of content on server.

Industry - Government

11

Discovered and reported the existence of a defaced page on a State Ministry of Health's website. The defaced page contains unauthorized content and modifications, which indicates that the website has been compromised.

This poses a critical risk to the security and integrity of the web platform.

Industry - Government / Health

12

Two critical vulnerabilities were discovered in the back-office portal: the presence of default credentials and the leakage of taxpayer information which can be chained for access to another portal.

This presents a severe risk to the security and integrity of the backoffice portal.

Industry - Government

13

Certain administrative functions on the student portal can be accessed without authentication, exposing statistics on student registration, matric numbers, quotas, and more due to server misconfiguration.

This poses a critical risk to the privacy and security of students, as well as the potential for regulatory non-compliance on the institution.

Industry - Education

14

A critical vulnerability due to poor session management was found on a government portal and its subdomains, leading to the leakage of sensitive Personally Identifiable Information (PII) of applicants

This poses significant risks to both individuals and the government.

Industry -Government

15

Misconfigurations on a postgraduate portal have led to unauthorized access to student data, including payment invoices. This occurs due to public access to matric numbers, which serve as default usernames, and general passwords that students often do not change upon logging in.

This poses a critical risk to the security and confidentiality of sensitive data

Industry - Education

16

An incident was discovered involving a MikroTik router, where an attacker brute-forced the appliance through an API call and made modifications to establish a backdoor. We reported this vulnerable box to the NCC-CSIRT and the affected ISP.

This poses significant risks to both the customer and the ISP that own the router.

Industry - Telecommunication

17

A remote code execution (RCE) vulnerability was found on a commission web portal, potentially allowing an attacker to fully compromise the system and threaten its confidentiality, integrity, and availability

This presents a critical risk to the integrity and security of the web portal, as well as the operations of the commission.

Industry - Government

18

Insecure data access on a government site allows attackers to retrieve user passport photographs if they know the individual's NIN, leading to further leakage of Personally Identifiable Information (PII).

This poses a critical risk to the privacy and security of citizens, as well as the potential for severe legal and regulatory implications

Industry - Government

19

Directory listing of an API endpoint has disclosed the Personally Identifiable Information (PII) of over 3,000 users, including BVN, passports, and more.

This poses a severe risk to the privacy and security of users, as well as potential legal and regulatory implications.

Industry - Government / Health

20

A defaced page was detected on the NEICT Initiative's website, containing unauthorized content and modifications, indicating that the site has been compromised.

This poses a critical risk to the security and integrity of the web platform.

Industry - Technology / NGO

21

A GitHub repository belonging to the organization was found to contain hardcoded credentials, including usernames and passwords, for a critical email system. An unauthorized individual could easily access these credentials due to the repository's public availability

This poses a severe risk to the privacy and security of the email account

Industry - Telecommunication

Nigeria's Cyberspace
ISAC + PEOPLE CERT

22

Security findings related to a professional platform identified through its Facebook page reveal a membership system with sequentially arranged membership numbers and default credentials, posing significant security risks to the membership portal and members PII.

This presents a critical risk to the security and confidentiality of the affected systems, potentially leading to unauthorized access.

Industry – Technology / Management

Disclose a vulnerability today !

You can use the QR code below to disclose a vulnerability today. The second QR code also contains What You Should Know – Researchers and Organizations on Responsible Disclosure

Disclose Vulnerability (ies)

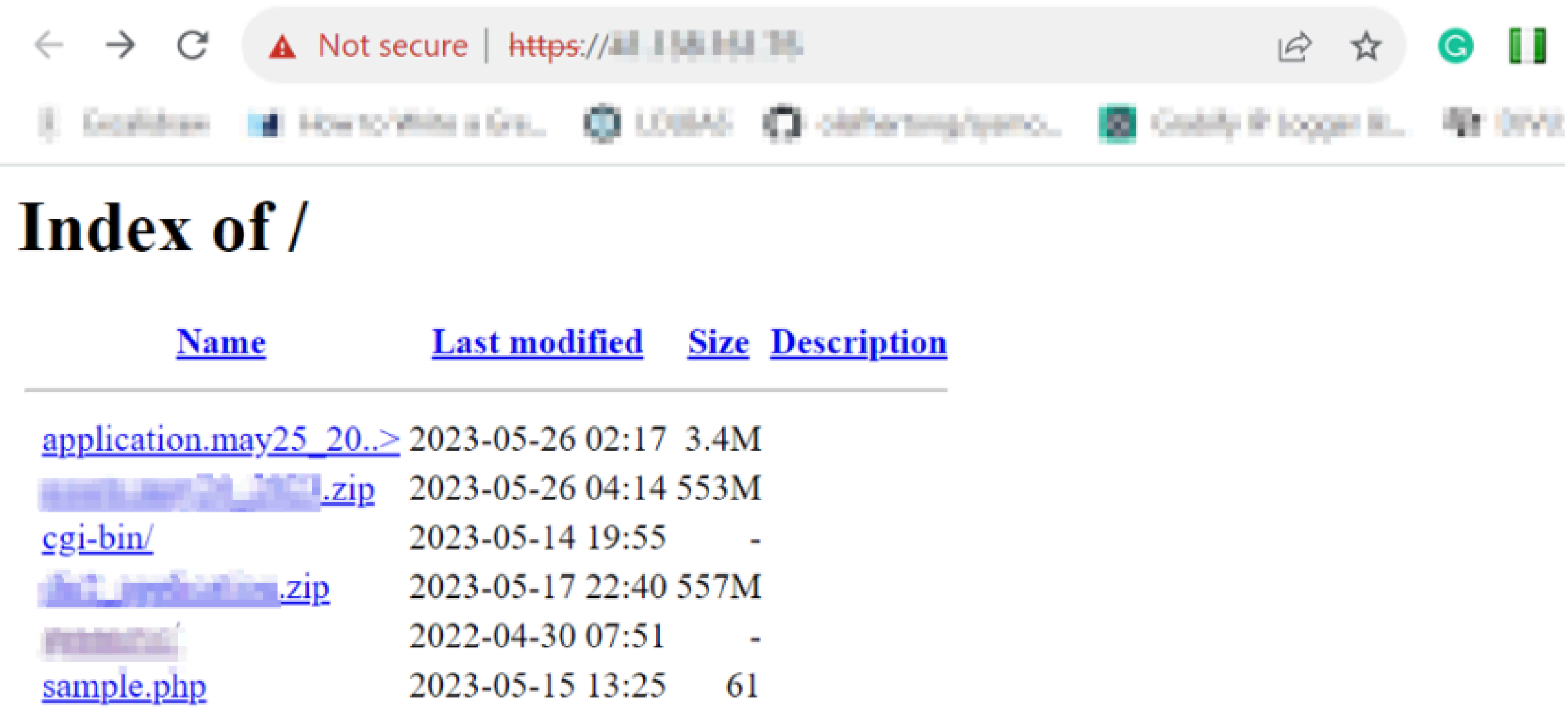
What you should know

Some of the findings are still being addressed, and there has been limited responsiveness from certain affected parties. We strongly encourage the organization to utilize our Vulnerability Disclosure Policy (VPD) template as a comprehensive guide for establishing a structured process that enables researchers to effectively communicate their findings. This will facilitate a smoother and more efficient engagement between the organization and external researchers, ensuring that vulnerabilities are addressed in a timely and coordinated manner.

The Risks of Misconfiguration on Internet-Facing Assets and Its Impact on Data Protection

The Scope of the Problem

Misconfigured servers, databases, and applications are alarmingly common. Often, organizations rush to deploy new services without fully securing them, leaving sensitive information vulnerable to unauthorized access. This negligence can result in significant data breaches, where PII such as names, addresses, National Identity Numbers (NIN), and financial information are exposed.

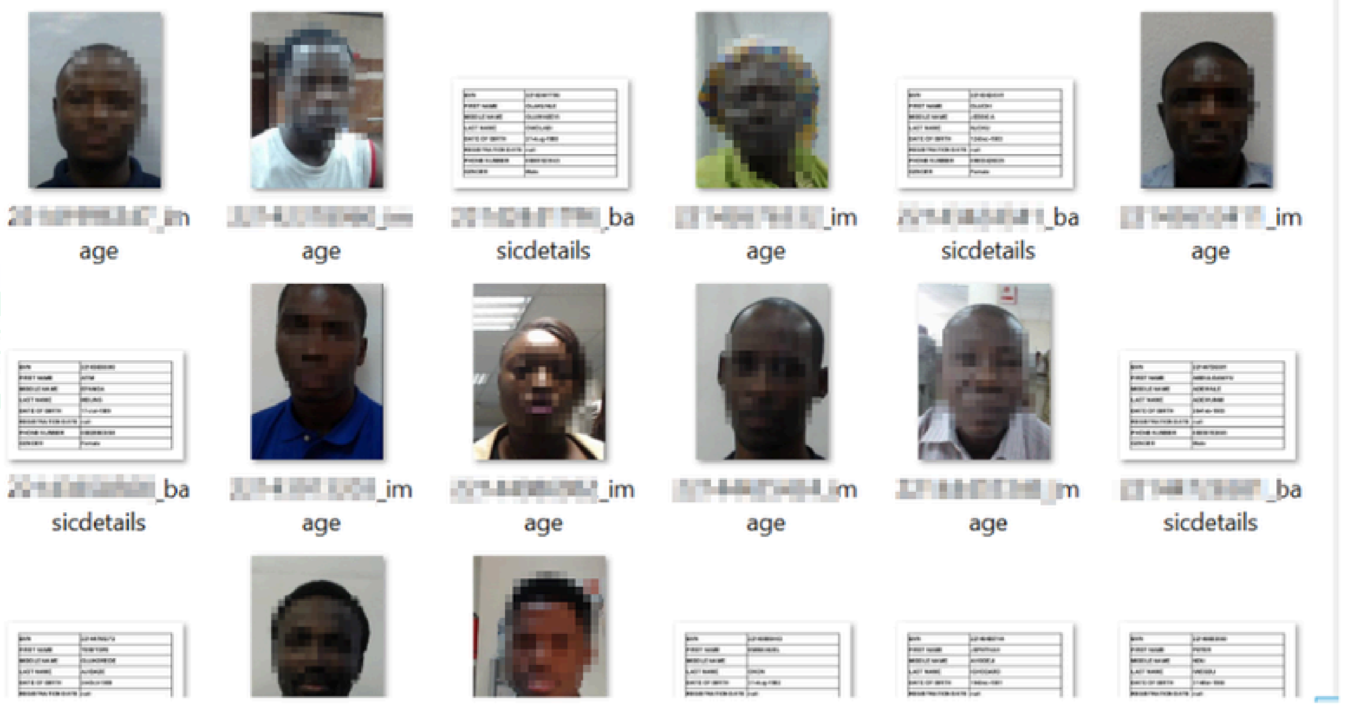


```
Index of /

Name                      Last modified     Size  Description

application.may25_20..>   2023-05-26 02:17  3.4M
[redacted].zip            2023-05-26 04:14  553M
cgi-bin/                  2023-05-14 19:55    -
[redacted].zip            2023-05-17 22:40  557M
[redacted]                2022-04-30 07:51    -
sample.php                2023-05-15 13:25   61
```

A misconfiguration introducing directory transversal vulnerability exposing personal data



The Illusion of Compliance

Many organizations believe that simply adhering to compliance frameworks—such as NDPR/A — means they are adequately protecting their data. However, this mindset often leads to a false sense of security. Compliance should not be viewed as a checkbox exercise; rather, it requires a proactive approach to security.

The Risks of Misconfiguration on Internet-Facing Assets and Its Impact on Data Protection

Misconfigurations often arise from a lack of understanding of the compliance requirements themselves, leading to superficial implementations that do not genuinely protect user data. This “check-the-box” mentality can invalidate the very efforts organizations make toward data protection, leaving them exposed to both legal repercussions and reputational damage.

Recommendations for Improvement

To combat the risks associated with misconfiguration, organizations must adopt a more comprehensive approach to data security:

Regular Audits and Assessments: Conduct frequent security audits and vulnerability assessments to identify and rectify misconfigurations before they lead to breaches.

Implement Best Practices: Follow industry best practices for securing internet-facing assets, including proper access controls, encryption, and regular updates.

Employee Training: Educate employees about the importance of security configurations and the implications of misconfiguration. A well-informed team is crucial in maintaining security standards.

Automated Tools: Utilize automated tools to monitor configurations and detect vulnerabilities in real time. These tools can help organizations maintain compliance and secure their assets effectively.

Incident Response Plans: Develop and maintain a robust incident response plan to quickly address any data breaches or security incidents that may occur.

Cybersecurity Incidents Tracking

Whitehat.NG

whitehat.ng

Cyber Incidents Tracking

In 2024, Phishing Campaigns emerged as the most prevalent threat, accounting for 40% of incidents. Following closely, Defacement incidents represented 35%. Both Ransomware (attributed to various ransomware groups, including Phobos, Lockbit, Black Suit, Funksec, and Conti variant) and Info Stealer/Malware Campaigns each comprised 25% of the total incidents. Other threats, including Breach and Stolen Funds, Cyber Squatting, and Insider Threats, each made up 5% of the occurrences. This distribution highlights the ongoing challenges organizations face in securing their digital assets against a diverse range of cyber threats.

The trend of ransomware incidents notably declined, particularly in Nigeria, as evidenced by reported cases and discussions within closed information security groups compared to the previous year, 2023.

At the individual level, we observed several reports of sophisticated phishing schemes that defrauded unsuspecting individuals of their hard-earned money.

We acknowledge that there may be more incidents in these categories that have not been reported for various reasons. Information sharing has become invaluable in the fight against cybercriminals, serving as a crucial tool for enhancing collective security.

We urge stakeholders to maintain the practice of reporting incidents to enable access to more quality data. This collaboration can assist in making informed decisions to tackle national cybersecurity challenges effectively, ultimately strengthening our defenses against evolving threats.

By the Numbers

5 RANSOMWARE	7 DEFACEMENT
2 PONZI / CRYPTO SCHEME CRASHES OFF	3 BREACH & STOLEN FUND
8 PHISHING / DATA COLLECTION	1 DDOS
1 INSIDER THREAT	5 INFO STEALER / MALWARE CAMPAIGN

In 2024, the trend of ransomware incidents notably declined, particularly in Nigeria, as evidenced by reported cases and discussions within closed information security groups compared to the previous year, 2023.

March 2024

Phishing / Data Collection

A report indicated that some malicious actors had capitalized on the situation by setting up fake or replica versions of corporate banking websites to deceive individuals into divulging their personally identifiable information.

It was noted that by mimicking the legitimate interfaces of banks, these fraudulent websites trick users into entering sensitive data, such as login credentials, token codes, and NINs, under the guise of security compliance

https://blog.cyberplural.com/stay-secure-stay-informed-a-look-into-deceptive-practices-targeting-bank-customers/

May 2024

Ransomware

A major merchant bank reported that it had fallen victim to a devastating ransomware attack by the **LockBit** 3.0 gang. They expressed concern over the alarming fact that the bank's backup systems had also been affected, which further complicated the recovery process.

Whitehat.NG Telegram Group

May 2024

Breach & Stolen Fund

A leading fintech player experienced a security breach that allowed unknown individuals to illegally transfer billions of naira to various bank accounts. According to sources, the perpetrators diverted at least ₦11 billion ($7 million), with claims that the actual amount could be as high as ₦20 billion ($13.5 million).

This incident is the latest in a series of security breaches at the fintech, raising concerns about the company's ability to protect its clients' funds and data. No official statement yet on the matter, and the investigation is ongoing.

https://techcabal.com/2024/05/16/exclusive-flutterwave-loses-%E2%82%A611-billion-in-security-breach/

May 2024

Ransomware

A report stated that a prominent Nigerian engineering and construction firm serving the oil and gas industry had been targeted by the **Black Suit Ransomware**.

It was noted that the attack had disrupted the company's operations, raising concerns about the potential impact on its clientele and the broader industry

Whitehat.NG Telegram Group

June 2024

Breach & System Hijack

A threat actor or group known as ParanoidHax compromised the push messaging feature of a payment app used by a telecom service provider in Nigeria. They sent a notification to nearly 13,000 users, demanding that the ISP contact them at **mr.claratzz@proton.me** to pay 10 million Rupiah (approximately 985,000 Naira) to prevent the database from being put up for sale.

Whitehat.NG Telegram Group

June 2024

Defacement

Website defacement remained a significant issue in 2024. A closer examination of threat groups targeting digital infrastructure in Nigeria under the Whitehat.NG project revealed multiple **defacement incidents involving the websites of tertiary institutions and government agencies**. Notably, the groups **xNight** and **M@raz Ali** were responsible for several of these defacements. Indicators of Compromise (IoCs) such as *sirmaraz@gmail.com* and *A_MaRaz@yahoo.com* were associated with these activities, and xNight was identified as a member of the **Blackpaper** group. These groups sometimes exploit vulnerable sites by installing shells and backdoors.

June 2024

Breach & Stolen Fund

According to the bank, the 1.7 billion naira hack that occurred in 2023 as a result of a technical glitch in its USSD channel. The bank was able to recover some of the stolen funds.

However, the remaining 1.1 billion of the stolen money was tracked back to previously engaged ICT staff of the bank. The bank approached the court to obtain an order to freeze the accounts containing the 1.1billion in stolen funds

https://nairametrics.com/2024/06/25/court-freezes-n1-1billion-linked-to-globus-bank-ex-staff-accused-of-hacking-stealing-customers-n3-5-billion/

https://theverdict.ng/2023/06/12/globus-bank-in-trouble-as-hacker-get-away-with-1-7billion/

June 2024

Ransomware

A federal agency reported a **Conti ransomware** incident that targeted the agency's internet-facing server. A server managed by a consultant was impacted by the attack. However, the incident was well responded to and contained

Whitehat.NG Telegram Group

July 2024

Ransomware

An indigenous cloud service provider experienced a security breach in the management section of its cloud service infrastructure, resulting in operational downtime. According to reports from the CERT, the **Phobos ransomware** group was identified as the culprit behind the incident.

https://nairametrics.com/2024/07/10/ransomware-threat-phobos-group-targets-nigerias-critical-cloud-providers/

https://blog.cyberplural.com/advisory-exploitation-of-cve-2023-27532-on-veeam-by-ransomware-groups/

https://www.gtbank.com/media-centre/gtbank-in-the-news/clarification-on-news-reports-regarding-the-banks-web-domain-and-customer-data-2

August 2024

Cyber Squatting

A leading bank in Nigeria experienced an isolated incident affecting the availability of its website domain, which was down for a few hours before being restored. There are speculations that this disruption was an attempt at cybersquatting due to delayed registration. Importantly, this incident did not involve any compromise of customer personal data.

September 2024

Info & Credential Stealer Malware Campaign

Credential and information-stealer malware have gained prominence with the rise of Initial Access Brokers (IABs) as a significant industry on the dark web. Recent observations from Managed Security Service Providers (MSSPs) and Security Operations Centers (SOCs) in the country indicate that these malware types are frequently associated with phishing emails, found in compromised systems, bundled with cracked software, and increasingly packaged alongside ransomware. This combination adds another layer of extortion for ransomware victims who refuse to pay the ransom.

A report by CyberPlural MSSP focusing on information-stealer malware in Nigeria highlights the evolving landscape of these threats, emphasizing the persistence of certain variants such as Vidar, Asyncrat, and Agent Tesla, alongside the more transient variants like Redline, Lokibot, and Stealerium

December 2024

Ransomware

The Government of Ekiti State in Nigeria reportedly fell victim to FUNKSEC ransomware. According to the group, they have acquired 300 MB of the organization's data and have shared sample screenshots on their dark web portal.

https://blog.cyberplural.com/nigeria-a-battleground-against-info-stealing-malware/

https://www.vanguardngr.com/2024/04/info-stealer-malware-7-ways-to-protect-yourself-organization-nitda/

https://bsky.app/profile/falconfeedsio.bsky.social/post/3ldee3skmf22o

December 2024

Defacement

The NBS (National Bureau of Statistics) website has reportedly been defaced, prompting the organization to issue a statement. They announced, "This is to inform the public that the NBS website has been hacked, and we are working to recover it. Please disregard any messages or reports posted until the website is fully restored." Restoration is reportedly taking several days, as the site has yet to come back online.

https://x.com/NBS_Nigeria/status/1869465890905083969?t=dE6kPwyRDHN57F1ciMflOw&s=19

Cybersecurity Incidents Tracking - Whitehat.NG

You can continue to follow the cybersecurity incidents tracking for previous and upcoming years and on our GitHub page by using this link https://github.com/ngwhitehat/Nigeria-Cyber-Incidents or scan the QR code below

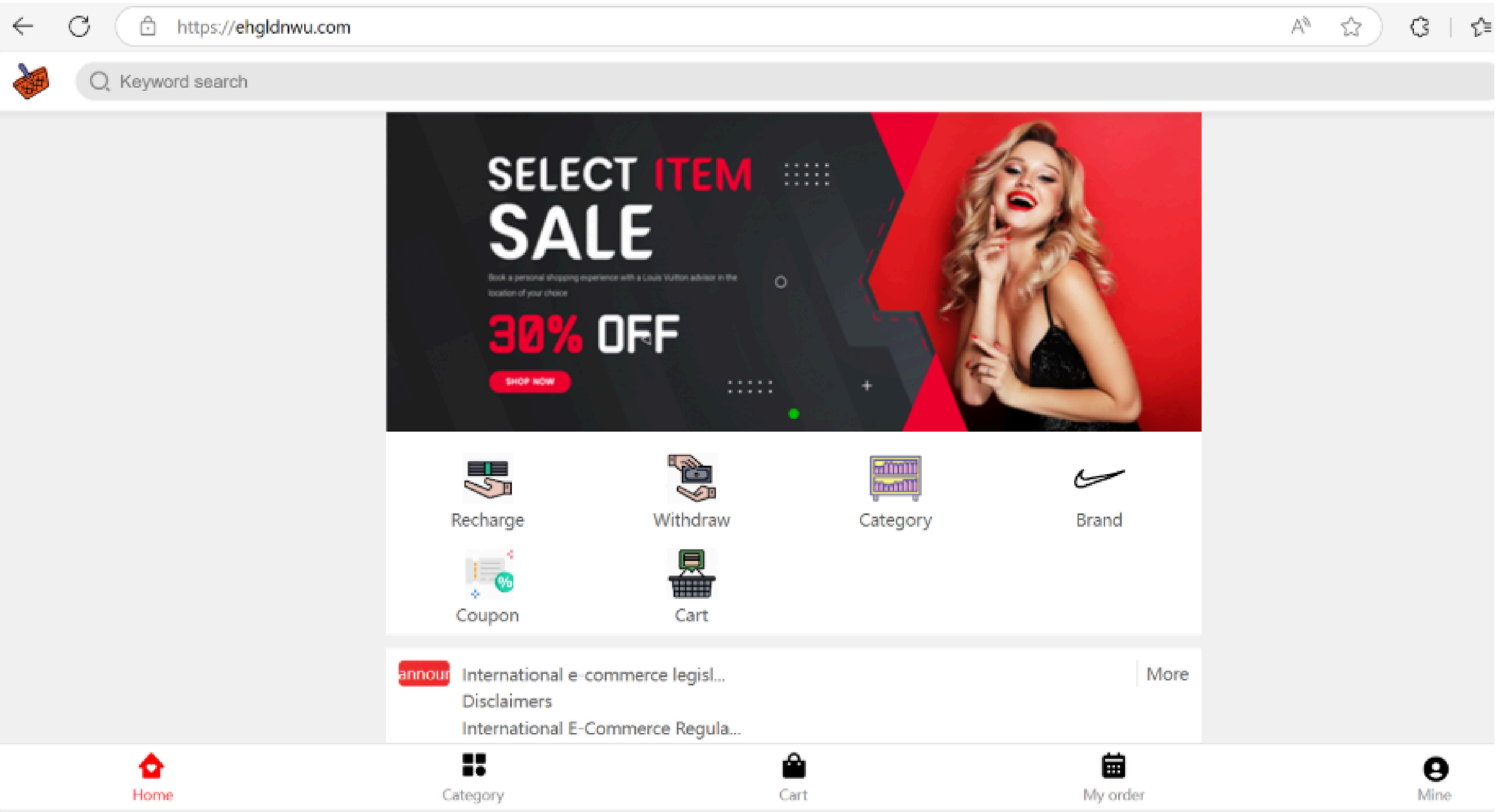
Track Incident(s)

Report Incident(s)

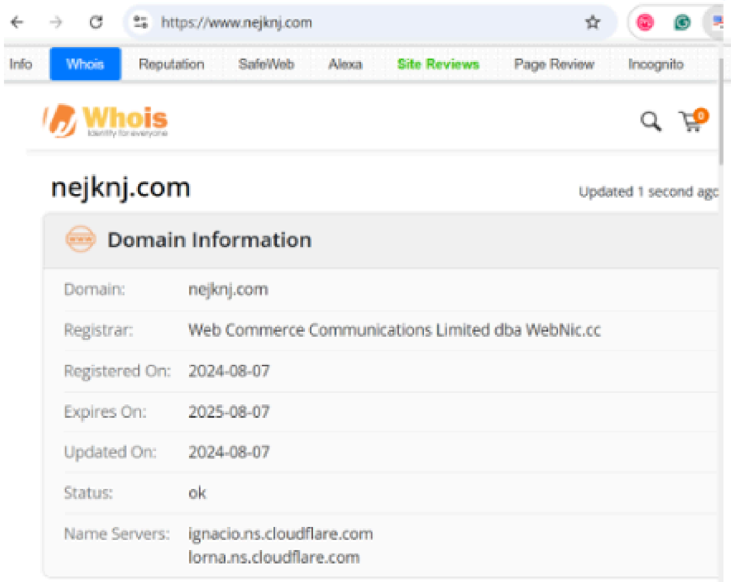
whitehat.ng

ZamaniMart – New Phishing Campaign Targeting Victims in Nigeria

Our team investigated a new phishing campaign targeting Nigerians. This threat group employs a deceptive shopping module to lure victims via WhatsApp, aiming to collect sensitive financial information, including credit card details and login credentials. Once obtained, this information is used to transfer funds from the victims' accounts.



phishing landing page –

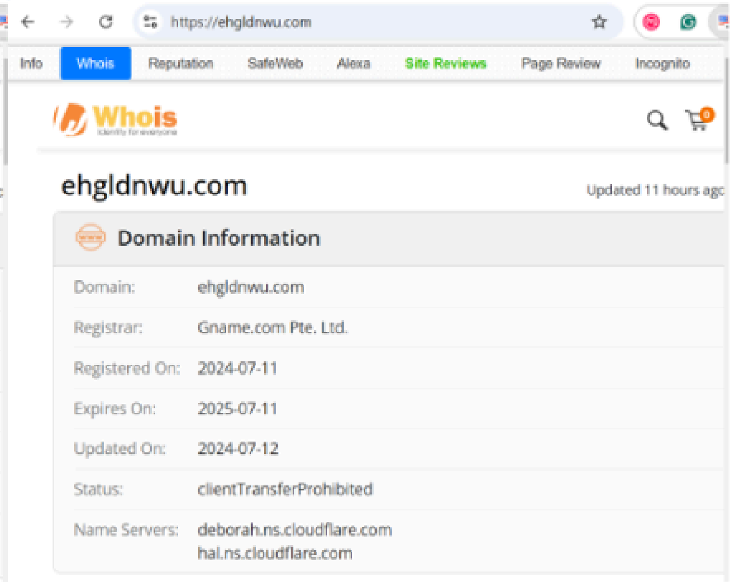


nejknj.com

Updated 1 second ago

Domain Information

Domain:	nejknj.com
Registrar:	Web Commerce Communications Limited dba WebNic.cc
Registered On:	2024-08-07
Expires On:	2025-08-07
Updated On:	2024-08-07
Status:	ok
Name Servers:	ignacio.ns.cloudflare.com lorna.ns.cloudflare.com

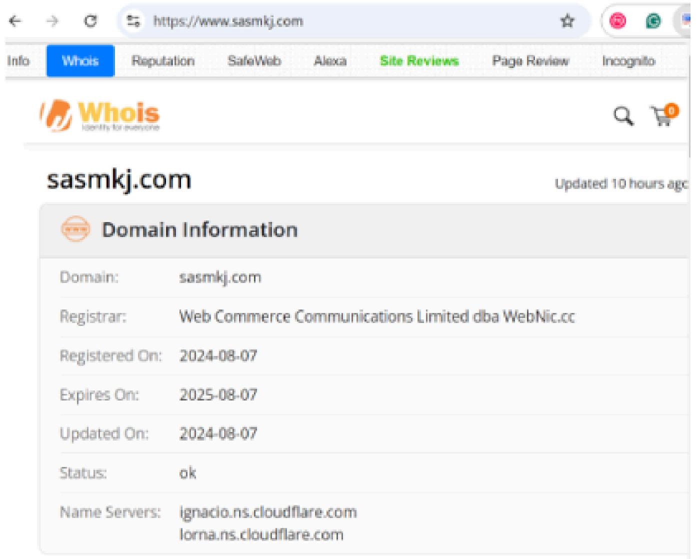


ehgldnwu.com

Updated 11 hours ago

Domain Information

Domain:	ehgldnwu.com
Registrar:	Gname.com Pte. Ltd.
Registered On:	2024-07-11
Expires On:	2025-07-11
Updated On:	2024-07-12
Status:	clientTransferProhibited
Name Servers:	deborah.ns.cloudflare.com hal.ns.cloudflare.com

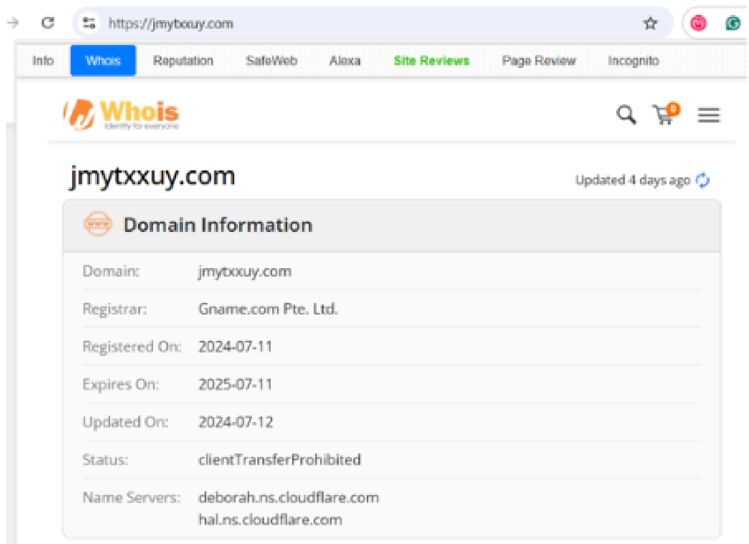


sasmkj.com

Updated 10 hours ago

Domain Information

Domain:	sasmkj.com
Registrar:	Web Commerce Communications Limited dba WebNic.cc
Registered On:	2024-08-07
Expires On:	2025-08-07
Updated On:	2024-08-07
Status:	ok
Name Servers:	ignacio.ns.cloudflare.com lorna.ns.cloudflare.com



jmytxxuy.com

Updated 4 days ago

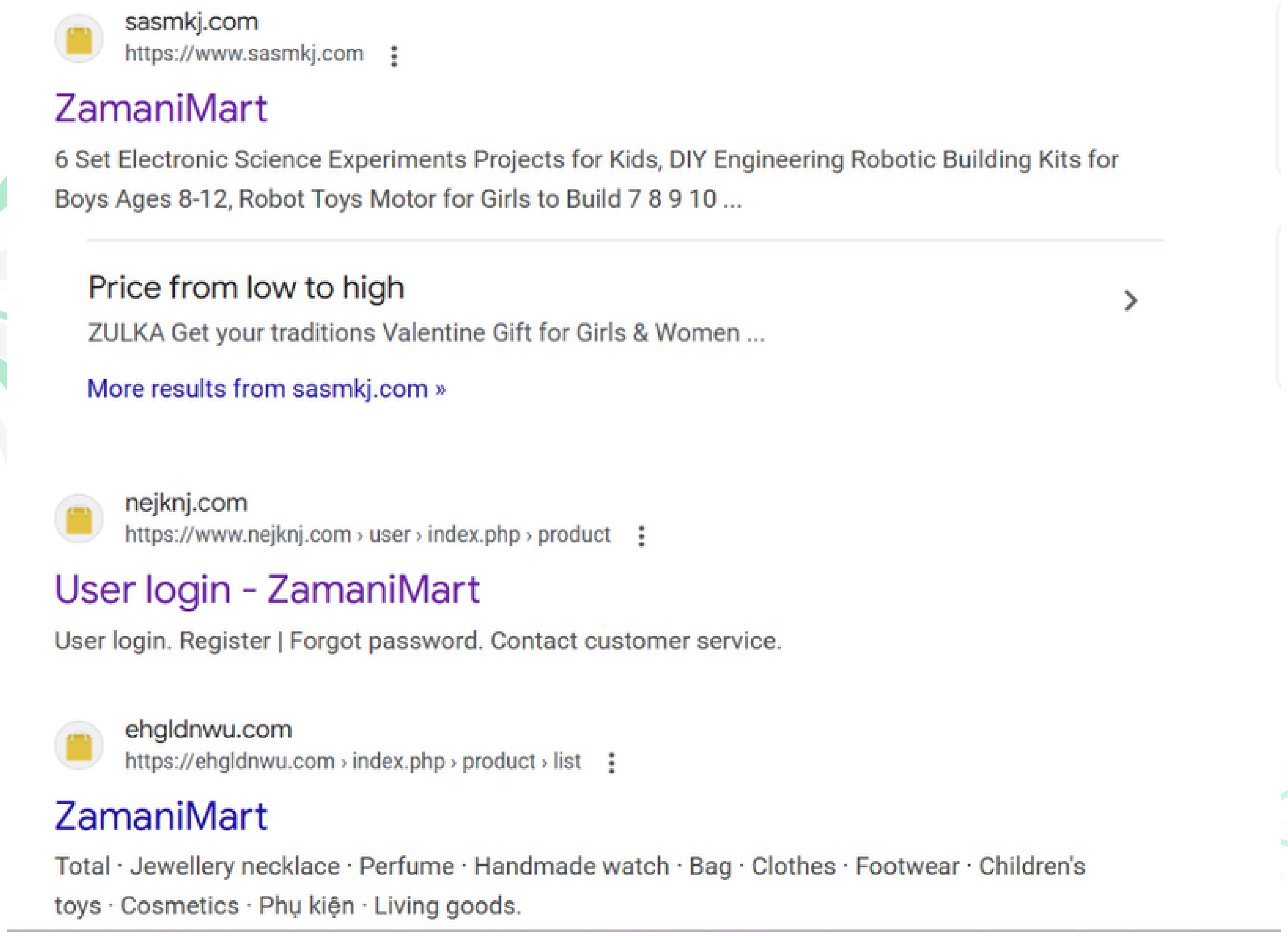
Domain Information

Domain:	jmytxxuy.com
Registrar:	Gname.com Pte. Ltd.
Registered On:	2024-07-11
Expires On:	2025-07-11
Updated On:	2024-07-12
Status:	clientTransferProhibited
Name Servers:	deborah.ns.cloudflare.com hal.ns.cloudflare.com

In our investigation, we uncovered that the threat group's infrastructure hosts a deceptive script, and we have identified four domains that are all serving the same malicious content.

ZamaniMart – New Phishing Campaign Targeting Victims in Nigeria

The code primarily handles image loading optimization, menu interactions, user login checks, and loading external scripts. The page is associated with phishing or malicious activities, due to how the login checks and redirects are implemented, potentially misleading users into providing sensitive information.



sasmkj.com
https://www.sasmkj.com

ZamaniMart

6 Set Electronic Science Experiments Projects for Kids, DIY Engineering Robotic Building Kits for Boys Ages 8-12, Robot Toys Motor for Girls to Build 7 8 9 10 ...

Price from low to high
ZULKA Get your traditions Valentine Gift for Girls & Women ...

More results from sasmkj.com »

nejknj.com
https://www.nejknj.com › user › index.php › product

User login - ZamaniMart

User login. Register | Forgot password. Contact customer service.

ehgldnwu.com
https://ehgldnwu.com › index.php › product › list

ZamaniMart

Total · Jewellery necklace · Perfume · Handmade watch · Bag · Clothes · Footwear · Children's toys · Cosmetics · Phụ kiện · Living goods.

To help raise awareness and protect potential victims, we have included additional Indicators of Compromise (IOCs) related to this campaign below. It's crucial for users to remain vigilant and cautious when sharing personal information online

Indicators of Compromise

- https[:]//www.sasmkj[.]com/
- https[:]//www.nejknj[.]com/
- https[:]//www.ehgldnwu[.]com/
- https[:]//jmytxxuy[.]com/

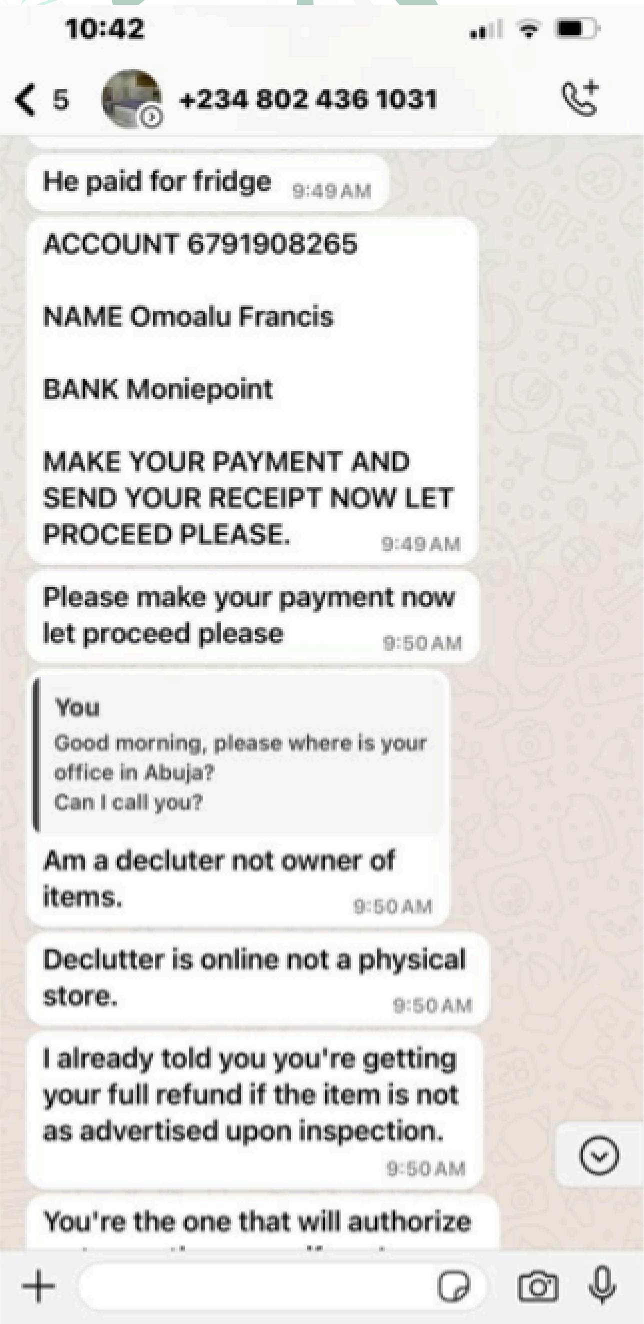
Note: In one case, a victim fell for this scheme, resulting in the theft of over 6 million naira from the account, which was subsequently transferred to multiple Moniepoint accounts.
6733748180 – BOSE AJOKE OGUNDIMU
7070140519 – SAKIRAT BOLANLE RAHEEM
9133961397 – ILEBAYE GRACE OMACHI

The Declutter Deception: A Digital Fraud Story

Online shopping has become increasingly popular in the digital age, opening the door to various fraudulent schemes.

One such scheme involves a fraudster who steals images of items from legitimate declutter businesses and masquerades as a genuine seller. By creating enticing advertisements on platforms like Instagram and Facebook, they attract potential buyers looking for great deals.

Once a victim expresses interest in an item, the fraudster requests payment upfront, often using persuasive tactics to instil urgency or fear of missing out. After the initial contact, they smoothly transition the conversation to WhatsApp, where they can manipulate the situation further and avoid detection.



10:42

5 +234 802 436 1031

He paid for fridge 9:49 AM

ACCOUNT 6791908265

NAME Omoalu Francis

BANK Moniepoint

MAKE YOUR PAYMENT AND SEND YOUR RECEIPT NOW LET PROCEED PLEASE. 9:49 AM

Please make your payment now let proceed please 9:50 AM

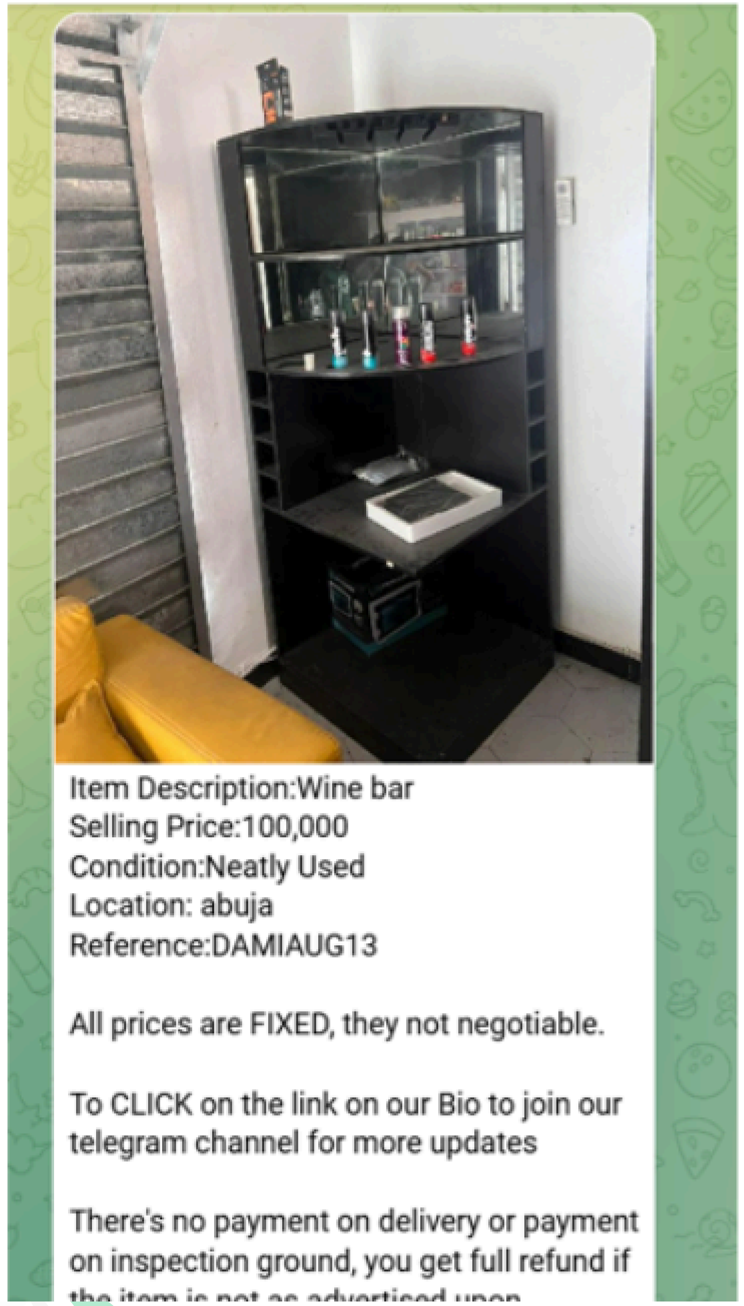
> You
> Good morning, please where is your office in Abuja?
> Can I call you?

Am a decluter not owner of items. 9:50 AM

Declutter is online not a physical store. 9:50 AM

I already told you you're getting your full refund if the item is not as advertised upon inspection. 9:50 AM

You're the one that will authorize



Item Description:Wine bar
Selling Price:100,000
Condition:Neatly Used
Location: abuja
Reference:DAMIAUG13

All prices are FIXED, they not negotiable.

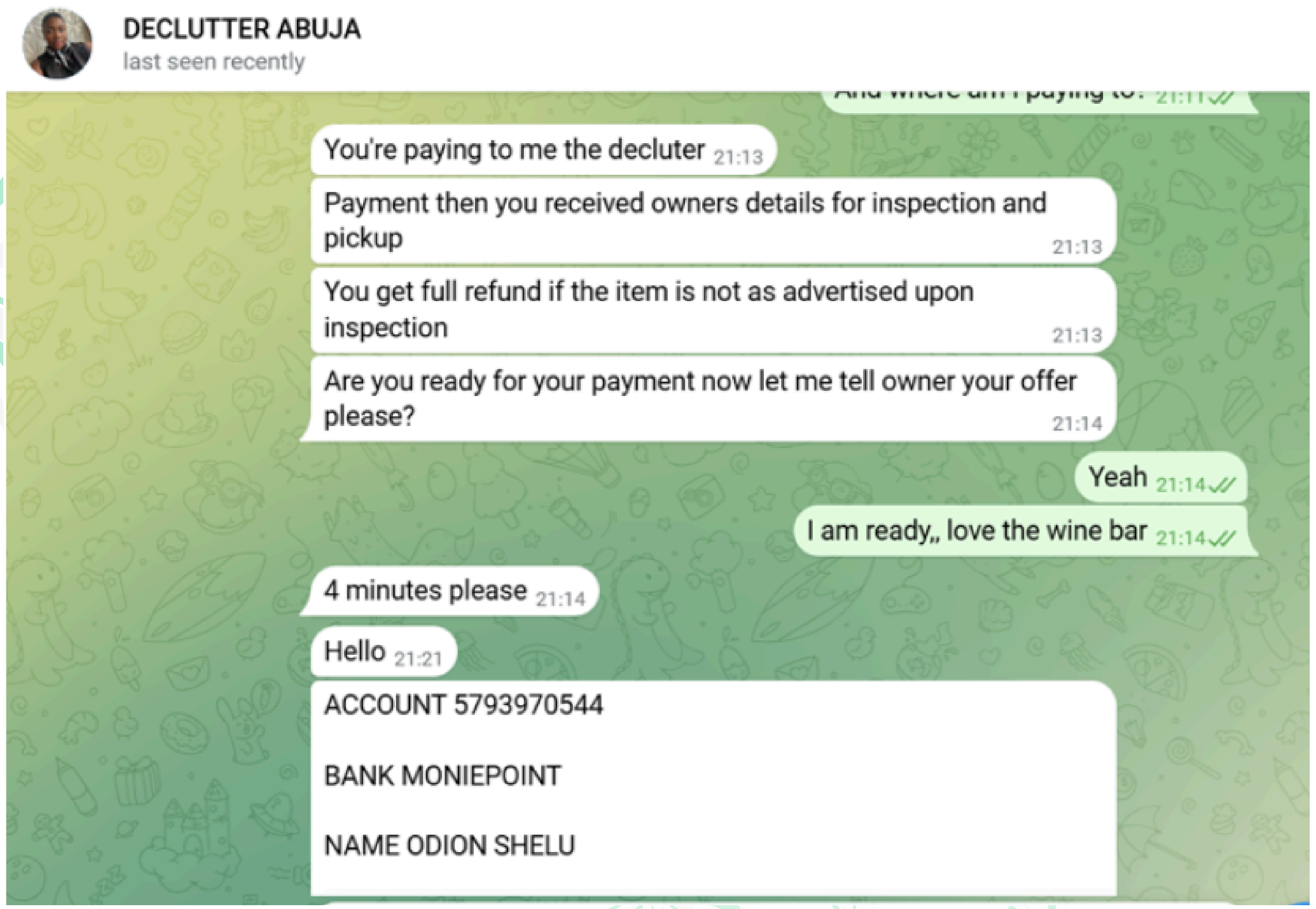
To CLICK on the link on our Bio to join our telegram channel for more updates

There's no payment on delivery or payment on inspection ground, you get full refund if the item is not as advertised upon

The 234-CTF team diligently tracked this fraudulent campaign for a long time in 2024.

The Declutter Deception: A Digital Fraud Story

We identified several individuals participating in this widespread scam, gathering evidence from multiple accounts linked to their activities. Many of these fraudsters maintain active Instagram pages, run Telegram channels, and utilize moderator accounts on Telegram to manage communication and further deceive potential victims.



DECLUTTER ABUJA
last seen recently

And where am I paying to? 21:11

You're paying to me the decluter 21:13

Payment then you received owners details for inspection and pickup 21:13

You get full refund if the item is not as advertised upon inspection 21:13

Are you ready for your payment now let me tell owner your offer please? 21:14

Yeah 21:14

I am ready,, love the wine bar 21:14

4 minutes please 21:14

Hello 21:21

ACCOUNT 5793970544

BANK MONIEPOINT

NAME ODION SHELU

Our findings suggest that this operation involves a network of five to ten young people, primarily based in Edo State. The evidence collected includes screenshots of conversations, records of transactions, and links to the fraudulent accounts, painting a clear picture of a well-organized scheme designed to exploit unsuspecting consumers.

Indicators of Compromise

- 08024361031 - The initial number that contacted the victim from the Instagram Ad
- 07045475014 - The phone number sent for pick-up
- 6791908265 – Omoalu Francis – Moniepoint
- 5793970544 - ODION SHELU - Moniepoint

To safeguard yourself from falling victim to similar scams, consider the following recommendations: Verify Sellers, Avoid Upfront Payments, Look for Signs of Fraud

Collaborative Initiatives

Whitehat.NG

whitehat.ng

The Whitehat.NG team seized the opportunity to emphasize the importance of collaboration and how the community project has been improving organizational security across various industry sectors.

The third edition of the ECOWAS Hackathon, hosted by Nigeria, officially opened on Tuesday, October 15, 2024, in Abuja. The event gathered 44 young tech-savvy individuals, aged 18 to 35, from 11 ECOWAS Member States and Mauritania. Participants competed in a 30-hour Capture the Flag (CTF) Hackathon. After 30 hours of intense competition, TeamERROR from Nigeria emerged third. The M3V7R team from Benin Republic came second, while the First Prize went to Shell X Roots from Cote d' Ivoire

whitehat.ng

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh
'Wallet Address'
OSINT and Other Investigation and Analysis
eva

2 days Cybersecurity Table Top Exercise (TTX) organized by the ngCERT in collaboration with UK FCDO under the African Cyber Program – managed by both foreign and local partners. The TTX focus was strengthening incident preparedness and response.

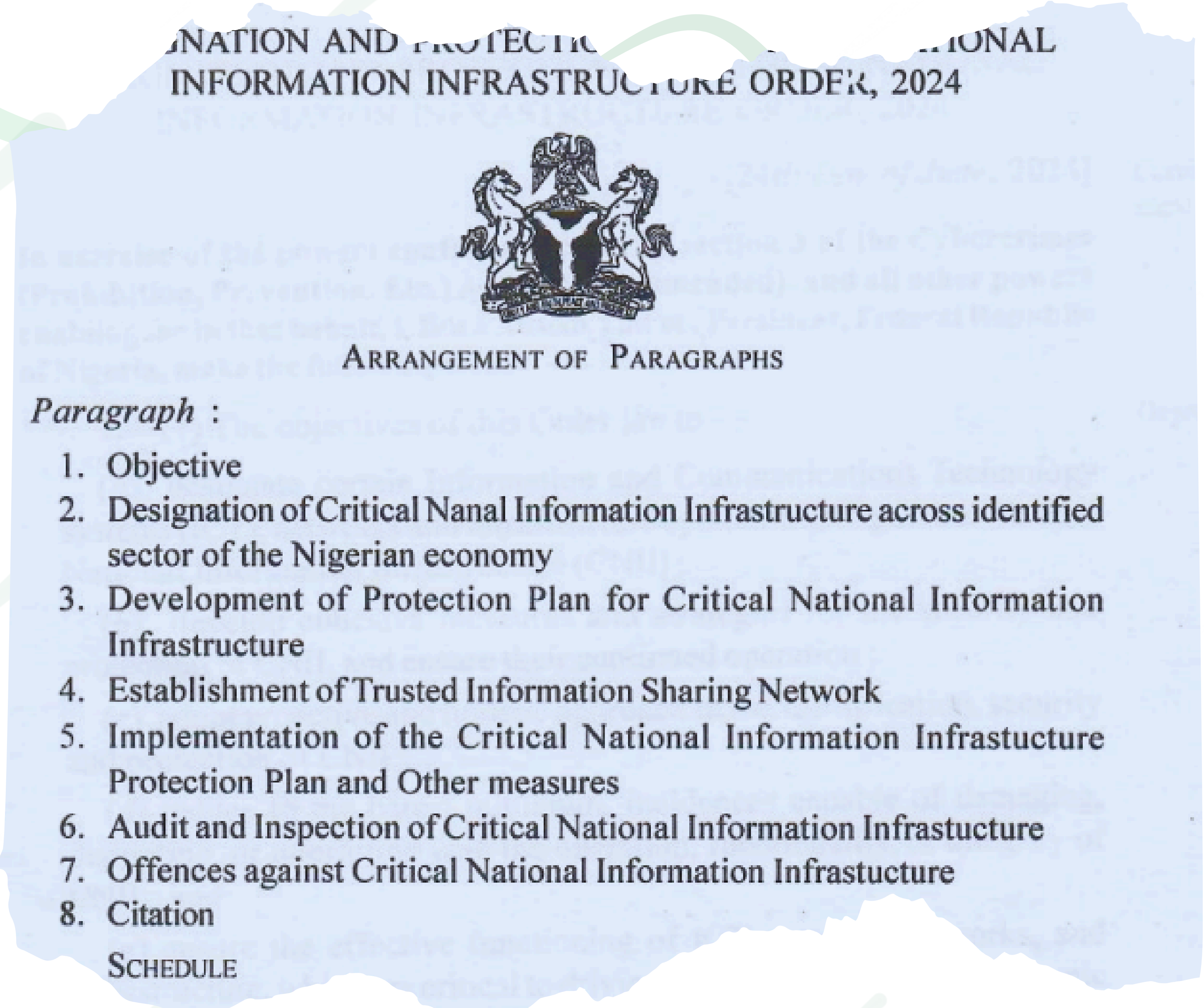
The National Security Adviser (NSA), Mallam Nuhu Ribadu, inaugurated a significant workshop series aimed at enhancing the protection and resilience of Nigeria's Critical National Information Infrastructure (CNII-P). This initiative follows the recent approval of the Order for the Designation and Protection of Critical National Information Infrastructure

Photo courtesy of NCCC via X

NPF-NCCC
(CyberHawks)
Presents
CYBERSECURITY AWARENESS WEEK
Themed: SECURE OUR WORLD
The NPF-NCCC Cordially invites the Media to join us as we sensitize the Nation on how to be safe digitally
Date: 9th, 10th
venue: ECOWAS SECRETARIATE ASOKORO, ABUJA
CYBERSECURITY IS EVERYONES BUSINESS.
this message is brought to you by the NPF-NCCC Public Relations liaison department
NIGERIA POLICE FORCE NATIONAL CYBERCRIME CENTER
CYBER AWAERNESS MONTH
SECURE OUR WORLD
Password Management
Software Updates
Internet Safety
Device Security
Privacy Settings
Data Backup
NCCCNPF.GOV.NG

The Nigeria Police Force National Cyber Crime Center (NPF-NCCC) reaffirmed its commitment to eradicating all forms of cybercrime in the country during its Cybersecurity Awareness Walk in Abuja. This event was part of ongoing efforts to educate the public about the importance of digital security and the measures individuals can take to protect themselves in an increasingly connected world.

Photo courtesy of NPF-NCCC via X



NATION AND PROTECTIC IONAL
INFORMATION INFRASTRUCTURE ORDER, 2024

ARRANGEMENT OF PARAGRAPHS

Paragraph :

1. Objective
2. Designation of Critical Nanal Information Infrastructure across identified sector of the Nigerian economy
3. Development of Protection Plan for Critical National Information Infrastructure
4. Establishment of Trusted Information Sharing Network
5. Implementation of the Critical National Information Infrastucture Protection Plan and Other measures
6. Audit and Inspection of Critical National Information Infrastucture
7. Offences against Critical National Information Infrastucture
8. Citation

SCHEDULE

On June 24, 2024, The Federal Government issued a new order to enhance the security of Nigeria's Critical National Information Infrastructure. Titled the Designation and Protection of Critical National Information Infrastructure Order 2024, the order was published in an official gazette signed by President Bola Tinubu

The Chief Information Security Officers (CISOs) of financial institutions convened at the annual Committee of Chief Information Security Officers of the Nigeria Financial Industry (CCISONFI) conference held in Uyo.

Photo courtesy of CYSED Uchenna Stella Emeka-Obivia LinkedIn

The inaugural Nigeria and UK Cyber Dialogue, led by the NSA and NCCC Coordinator at ONSA, featured productive discussions on shared objectives related to Cyber Resilience, Cybercrime, Incident Management, and Emerging Technologies.

Photo courtesy of Andy Penpraze via LinkedIn

The 10th INTERPOL Africa Working Group Meeting on Cybercrime for Heads of Units took place in Abuja from April 29th to May 3rd, 2024. Organized by the INTERPOL Cybercrime Directorate in Singapore, in collaboration with the National Central Bureau Abuja, the meeting aimed to unite African law enforcement officials (LEOs) and relevant stakeholders. The discussion focused on the growing threat of cybercrime and explored effective operational strategies and international cooperation to combat cybercrime in the African region.

Photo courtesy of Nne Ikoiwak via LinkedIn

Lagos State announced the inauguration of the Lagos State Cybersecurity Council, which includes esteemed ICT experts such as Dr. Obadare Peter Adewale, Dr. Fene Osakwe, Chinenye Chizea, and Dr. Bharat Sani from both the public and private sectors. This significant event, officiated by Deputy Governor Dr. Kadri Obafemi Hamzat, highlights Lagos' commitment to implementing cybersecurity projects and programs aimed at creating a smarter and more secure Lagos.

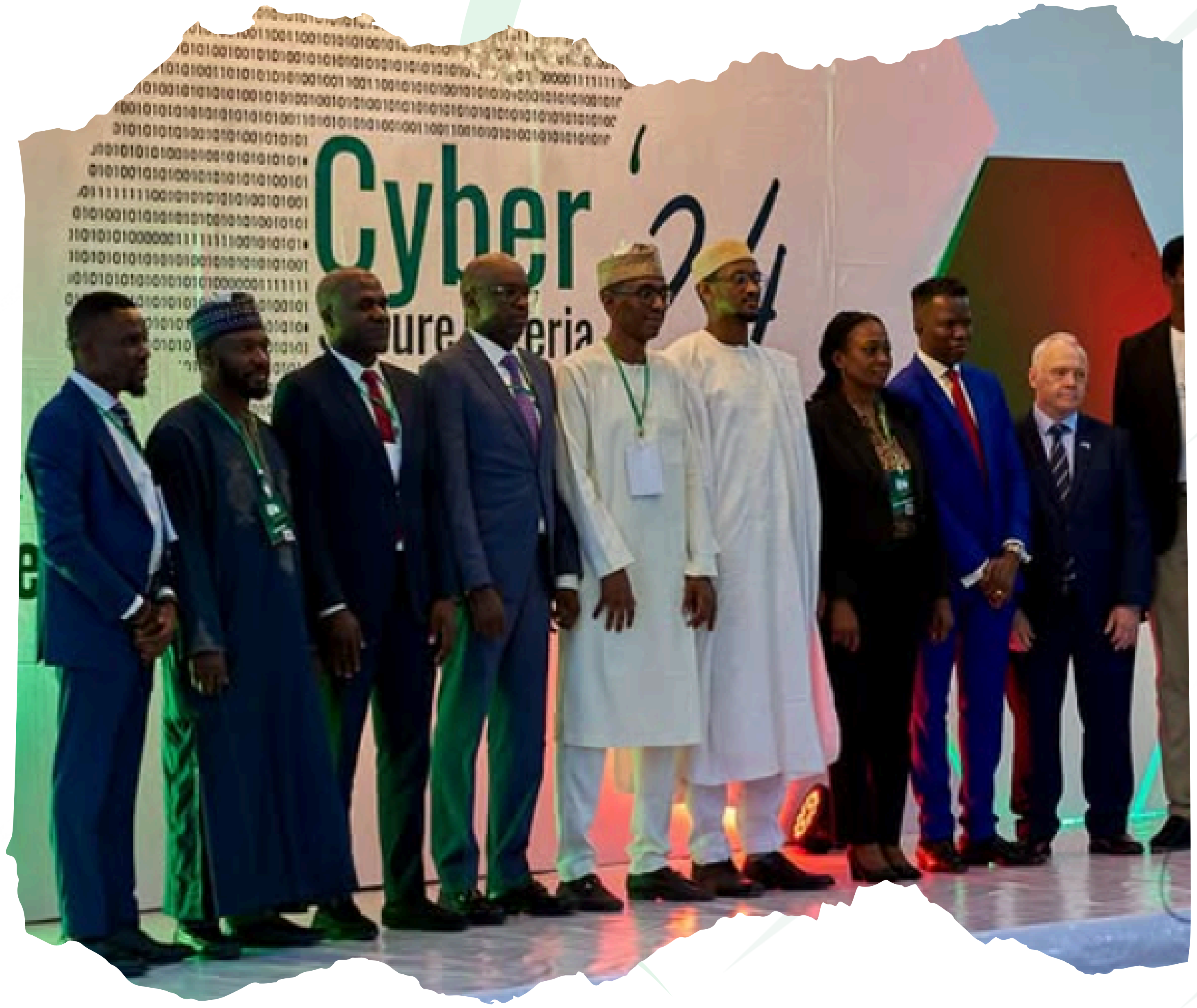
Photo courtesy of LASG Min of Science, Innovation and Tech via LinkedIn

NATIONAL CYBERCRIME SUMMIT
THE ECONOMIC AND FINANCIAL CRIMES COMMISSION WITH SUPPORT FROM THE RULE OF LAW AND ANTI-CORRUPTION PROGRAMME

The national summit on cybercrimes, organized by the Economic and Financial Crimes Commission, took place at the Banquet Hall of the Presidential Villa in Abuja. Themed "Alternative to Cyber Crime: Optimizing Cyber Skills for National Development," the summit aimed to explore and recommend ways to utilize cyber skills for nation-building instead of engaging in criminal activities.

Team Error, which represented Nigeria at the ECOWAS Cybersecurity Hackathon and secured third place, paid a special visit to the NITDA Headquarters.

Photo courtesy of NITDA via Instagram



The leadership of CSEAN, alongside dignitaries, participated in the Cyber Secure Nigeria Conference 2024, themed "Leveraging AI for Cyber Resilience: Building a Secure Future Bridge."

Photo courtesy of CSEAN via Instagram

Women in Cybersecurity (WiCyS) Nigeria held its inaugural leadership forum, themed "Advancing Cybersecurity Through Inclusive Leadership.

Photo courtesy of WiCyS Nigeria

The Security and Defence Partnership between Nigeria and the UK has been strengthened with the signing of a Memorandum of Understanding (MoU) by ONSA, Mal Nuhu Ribadu. This agreement facilitates deeper cooperation in capacity building and addressing cyber threats.

Photo courtesy of Andy Penpraze via LinkedIn

Nigerian Data Protection Commission (NDPC) Trains NIPOST Staff On Data Privacy And Protection

Photo courtesy of NPDC Gallery

The inaugural edition of the Africa Cyber Fest was held in Lagos, Nigeria. This youth-focused cybersecurity conference brings together young talents from across Africa to foster knowledge sharing and capacity building, to strengthen the resilience of the continent's cybersecurity ecosystem.

Photo courtesy of Africa CyberFest via LinkedIn

ISACA Abuja leadership and participants gathered at the ISACA Abuja Annual Conference (ANNCON2024), themed "Harnessing Digital Trust for Inclusive Financial and Technological Access.

Photo courtesy of ISACA Abuja via LinkedIn

Educational Offerings

Whitehat.NG

Educational Offerings

Throughout 2024, several non-profit organizations and NGOs dedicated themselves to providing cybersecurity training across various learning paths, including Devsecops, GRC, Security Operations, and VAPT. Notable leaders in this field include the Cybersafe Foundation, Tech4Dev, Cyblack, and the Cybersecurity Education Initiative (CYSED). Their efforts have resulted in capacity building for participants from diverse cohorts, contributing significantly to capacity building within Nigerian cyberspace.

During the cybersecurity awareness month, we witnessed awareness sessions taking place at various levels, conducted by both public and private sector entities, as well as at the organizational, marketplace, and religious centre levels. This widespread effort reflects a growing commitment to raising awareness about cybersecurity across different sectors of society.

Professional bodies and associations like the Cyber Security Expert Association of Nigeria (CSEAN), Nigeria Computer Society (NCS), ISACA, CCISONFI and others organized conferences and workshops that brought stakeholders, professionals, members, and the public together to discuss and address key cybersecurity issues relevant to Nigeria.

Conclusion

Whitehat.NG

whitehat.ng

Conclusion

We extend our gratitude to our team, researchers, and partners (MSSP, SOCs, and CERTs) whose contributions have been instrumental in the success of the Whitehat.NG project.

As we look ahead to 2025, we remain open to collaborating with additional researchers and receiving support from MSSPs, CERTs and in-house SOCs nationwide.

We'd like you to express your willingness to contribute by using our email, and we eagerly anticipate the opportunity to work with you.

The 2024 Annual Report highlights project Whitehat.NG's steadfast commitment to strengthening Nigeria's cybersecurity landscape. Our responsible disclosure of security vulnerabilities, monitoring of cyber incidents, and tracking of collaborative initiatives demonstrate our dedication to protecting Nigeria's digital infrastructure.

As we progress, we remain committed to fostering partnerships, driving innovation, and promoting education in cybersecurity. This report serves as a testament to our collective efforts in enhancing cybersecurity resilience.

Together, we are building a safer and more secure digital environment for Nigeria.

whitehat.ng

Nigeria’s Cyberspace ISAC + PEOPLE CERT

YOU SEE SOMETHING,
SAY SOMETHING
BUT RESPONSIBLY.

whitehat.ng

Follow and Contact Us

- https://whitehat.ng
- ngwhitehat
- https://linkedin.com/company/whitehat-ng
- cert@projectwhitehat.ng
- ngwhitehat

Partnering

ngCERT Nigeria Computer Emergency Response Team

NITDA CERRT.NG

NCC CSIRT