CyberPlural MSSP 2025 Annual Cybersecurity Report

Threat Intelligence, Incident Response Engagements, and Security Operations (SOC & Red Teaming) Insights from 2025.

Table of Content

Executive Summary

At CyberPlural MSSP, we facilitate practices and teams that are devoted to preventing, detecting, assessing, monitoring, and responding to cybersecurity threats and incidents. We are proud and excited to present to you the fourth edition of our annual cybersecurity report.

In 2025, the cybersecurity landscape in Nigeria became increasingly complex and challenging, marked by a surge in cyber threats and incidents.

As a Managed Security Service Provider (MSSP), we engaged and observed several critical trends and developments throughout the year. One notable trend is the active sale of stolen identities, or "stealer logs," obtained from malware and bot-infected devices. This underscores the ongoing risk posed by compromised personal information and highlights the need for enhanced identity protection measures.

Ransomware attacks emerged as one of the most significant cyber threats faced by organisations in 2025. These attacks have targeted various sectors, leading to substantial financial and operational impacts.

The exploitation of vulnerable servers and services further complicated the security landscape, as threat actors leverage these weaknesses to host malware and command-and-control (C2) operations within Nigeria. This exploitation necessitates robust defensive strategies to protect critical infrastructure.

In addition, threat actors attempted to sell and share exfiltrated data from successful cyber attacks on both open and dark web forums. This activity emphasises the importance of monitoring and mitigating data breaches, as stolen information can have far-reaching consequences for affected organisations.

Moreover, we observed the rise of locally based financially motivated threat groups targeting payment platforms and digital banking channels for vulnerabilities which are leverage to steal from imparted platforms.

2025 presents attackers' interest in diverse industries, including finance and fintech, public administration and government, information services, e-commerce, oil and gas, logistics, education, telecommunications, NGOs, and healthcare.

Our analysis identified over 44 cyber incidents throughout the year, encompassing ransomware attacks, web defacements, platform breaches, misconfigured services, and third-party data breaches.

This diverse range of incidents illustrates the multifaceted nature of the threats facing organisations today. Nigeria has emerged as one of the most intriguing environments for threat actors in Africa, driven by rapid digital adoption across sectors such as finance, government, logistics, and other services. This digital transformation presents both opportunities and challenges for security professionals.

As we move forward in 2026, organisations must adopt comprehensive cybersecurity strategies that address these evolving threats.

Continuous monitoring, employee training, and the implementation of robust security measures will be critical in safeguarding sensitive information and maintaining operational integrity in this dynamic environment.

Our commitment as an MSSP is to provide the necessary support and expertise to navigate these challenges effectively.

Insights from CyberPlural MSSP Engagements '25

Threat Intelligence as Observed, Tracked & Produced in 2025

Acreed, Rhamadanthys, Lumma, Others

8

Threat actors are selling stolen identities (stealer logs) from malware & bot infected devices.

NightSpire, Killsec, Funksec, Yurei, Others

14

Ransomware attacks are among the most critical cyber attacks organizations experienced in 2025.

FHC, FCTWB, and Others

15

Vulnerable servers and services are being leverage to host malware & C2 in Nigeria.

Privilege, Ghost, 888, Ghidra and others

12

Threat actors tried to sell and share exfil data from successful cyber attacks on open & dark web forum.

234 Cyber Task Force

Locally Based Financial Motivated Threat Groups

HK-FIN-01, **HK-FIN-05**, **HK-FIN-10**, HK-FIN-20, HK-FIN 25

A campaign by a threat group tracked as **HK-FIN-10**, hit two major channels in 2025. In both instance, series of malicious requests to the platforms impacted the victims financially and platform shutdown for days.

whitehat.ng

Industries Targeted

Finance & FinTech ,
Public Administration & Govt, Info Services, ,
E-Commerce,
Oil & Gas & Logistic,
Education ,
Telecom,
NGOs,
Health.

Total # of Identified Cases

44 +

Ransomware Attacks, Web Defacements, Platform Breach, Misconfigured Services, Third-Party Data Breach,

Please note that more incidents may have been recorded beyond what we've observed & engaged in our operational data review , reported and community chatters.

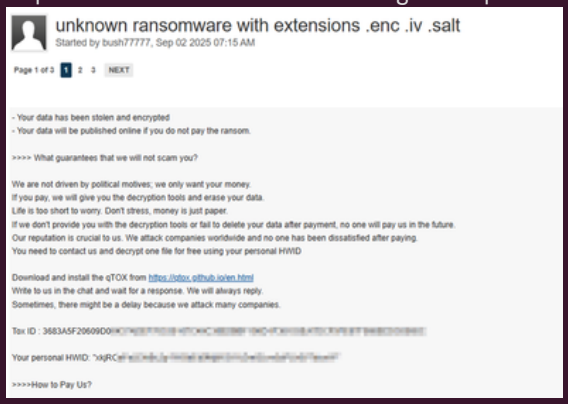
Overview of Africa Cyber Threat Landscape – Using number of identified Cases and comparing Notes with CyHawk Africa, Whitehat.NG

In 2025, Nigeria stands out as one of the most intriguing environments for threat actors in Africa. The rapid digital adoption in sectors such as finance, government, logistics, and other services is a significant factor driving this interest.

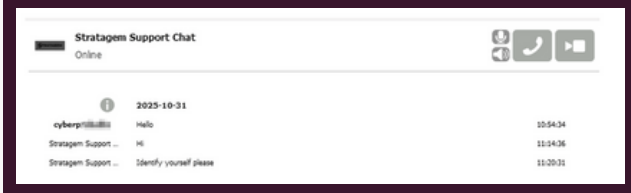
Rise of an Unnamed Ransomware Strain Targeting Nigerian Organisations

In the last quarter of 2025, it was observed that a new strain of ransomware was targeting organisations in Nigeria. Community discussions revealed that there was only one mention of the activities of this threat group, which remained unnamed, on both the open internet and the dark web. Notably, there were no victim-shaming websites associated with this group at that time. The only available documentation was through a support chat on qToX, referred to as the **Stratagem Support Chat.**

This update was deemed crucial for the community shared via the CERT, as multiple organisations had reportedly fallen victim to the same group. CyberPlural MSSP identified via threat intel that at least three incidents occurred within that period, and the national CERT was notified. Furthermore, the only known activity related to this group that was accessible on the open internet dated back to September 2nd at the time of filing our report to ngCERT.



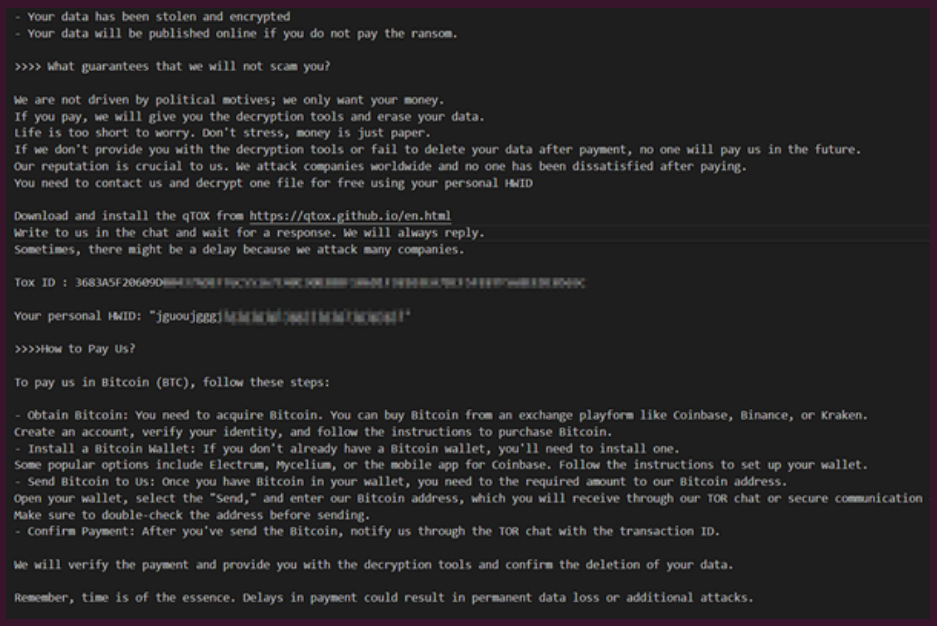
https://www.bleepingcomputer.com/forums/t/810457/unknown-ransomware-with-extensions-enc-iv-salt/



Indicator of Compromise (IoC)

- File Extensions: Encrypted data uses the extensions **.enc, .iv, and .salt.**
- Ransom Note Details:
  - ToxID: 3683A5F20609D00437ADEF76C55167C40C30B2BBF106D1F38103EA7DCF5FE87F568EEDC0565C
  - Personal HWID: "xkjRCaFeLEhiBc2XXXXXXXX3t1AZmt3Lnv5zPLk6V7dcwW"
- Threats - Victims are threatened with further attacks if they do not pay. There is currently no publicly available decryptor, and this strain does not appear to be associated with any well-known ransomware groups.
- Targets - The group has attacked both individuals and organisations, with **four incidents reported in Nigeria within three weeks in the last quarter of 2025**.
- Encryption Analysis - The encrypted samples reveal strong AES encryption with a PBKDF2-derived key, multi-layer obfuscation post-AES, and a fragmented, redundant payload structure.
- Support Chat - The support chat is known as **Stratagem Support Chat.**
- Targeted Technologies - This group targets **storage technologies** such as **VMware ESXi, Nutanix, and Hyper-V** once a foothold is established in a network.

Rise of an Unnamed Ransomware Strain Targeting Nigerian Organisations



```
- Your data has been stolen and encrypted
- Your data will be published online if you do not pay the ransom.

>>>> What guarantees that we will not scam you?

We are not driven by political motives; we only want your money.
If you pay, we will give you the decryption tools and erase your data.
Life is too short to worry. Don't stress, money is just paper.
If we don't provide you with the decryption tools or fail to delete your data after payment, no one will pay us in the future.
Our reputation is crucial to us. We attack companies worldwide and no one has been dissatisfied after paying.
You need to contact us and decrypt one file for free using your personal HWID

Download and install the qTOX from https://qtox.github.io/en.html
Write to us in the chat and wait for a response. We will always reply.
Sometimes, there might be a delay because we attack many companies.

Tox ID : 3683A5F20609D

Your personal HWID: "jguoujggg

>>>>How to Pay Us?

To pay us in Bitcoin (BTC), follow these steps:

- Obtain Bitcoin: You need to acquire Bitcoin. You can buy Bitcoin from an exchange playform like Coinbase, Binance, or Kraken.
Create an account, verify your identity, and follow the instructions to purchase Bitcoin.
- Install a Bitcoin Wallet: If you don't already have a Bitcoin wallet, you'll need to install one.
Some popular options include Electrum, Mycelium, or the mobile app for Coinbase. Follow the instructions to set up your wallet.
- Send Bitcoin to Us: Once you have Bitcoin in your wallet, you need to the required amount to our Bitcoin address.
Open your wallet, select the "Send," and enter our Bitcoin address, which you will receive through our TOR chat or secure communication
Make sure to double-check the address before sending.
- Confirm Payment: After you've send the Bitcoin, notify us through the TOR chat with the transaction ID.

We will verify the payment and provide you with the decryption tools and confirm the deletion of your data.

Remember, time is of the essence. Delays in payment could result in permanent data loss or additional attacks.
```

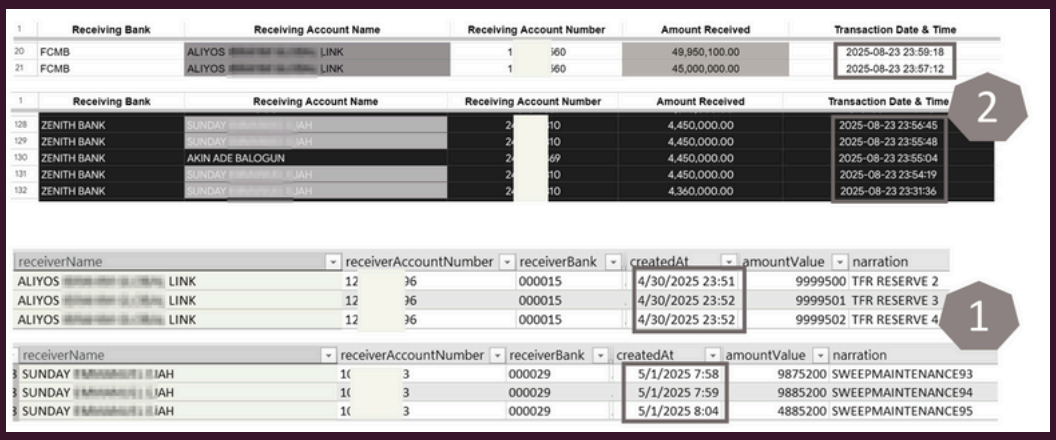
Analysis of Encrypted Sample at HAND

1. Strong AES Encryption with PBKDF2-derived Key - The initial payload is encrypted using AES-CBC. The encryption key is derived via PBKDF2-HMAC-SHA256 using a static password and a salt. Without knowledge of the exact password, the key space is computationally infeasible to brute-force
2. Multi-layer Obfuscation Post-AES - After AES decryption, the payload is still single-byte XOR-obfuscated. While XOR can theoretically be brute-forced, it multiplies complexity when combined with the AES layer because the XOR is applied to AES ciphertext outputs, not plaintext. Further stages include Base64 encoding, zlib/inflate compression, and possible repeated XOR layers, forming a deeply nested decode chain
3. Fragmented and Redundant Payload Structure - The ransomware splits its payload into small, fragmented blobs, many of which are duplicated across 256 XOR variants
4. Residual Artifacts are Incomplete Indicators - While some plaintext strings (service names, command fragments) are visible, they do not contain enough information to reconstruct the AES key or full logic
5. Cumulative Security Effect - AES encryption secures the primary payload. Multi-stage XOR + Base64 + Inflate obfuscation ensures that even if AES were partially reversed, the remaining stages would prevent execution understanding. Fragmentation and redundancy amplify reconstruction difficulty

Locally Based Financially Motivated Threat Groups In Nigeria. HK-FIN-10

Our team started tracking financially motivated threat groups in Nigeria since 2024. In a campaign by a threat group tracked as **HK-FIN-10**, it hit two major banking channels in 2025. In both instances, a series of malicious requests to the platforms impacted victims financially and led to platform shutdown for days. The first instance of these incidents [1] was observed in Q1 of 2025, and the second instance [2] was in Q3. In both instances, the group leveraged similar attack patterns on different victims, which were 4 months apart from each other.

This scenario presents a case where an unreported incident can aid attackers in further using the same method on multiple victims.



	Receiving Bank	Receiving Account Name	Receiving Account Number	Amount Received	Transaction Date & Time
20	FCMB	ALIYOS [redacted] LINK	1 [redacted]60	49,950,100.00	2025-08-23 23:59:18
21	FCMB	ALIYOS [redacted] LINK	1 [redacted]60	45,000,000.00	2025-08-23 23:57:12

	Receiving Bank	Receiving Account Name	Receiving Account Number	Amount Received	Transaction Date & Time
128	ZENITH BANK	SUNDAY [redacted] IAH	2[redacted]10	4,450,000.00	2025-08-23 23:56:45
129	ZENITH BANK	SUNDAY [redacted] IAH	2[redacted]10	4,450,000.00	2025-08-23 23:55:48
130	ZENITH BANK	AKIN ADE BALOGUN	2[redacted]69	4,450,000.00	2025-08-23 23:55:04
131	ZENITH BANK	SUNDAY [redacted] IAH	2[redacted]10	4,450,000.00	2025-08-23 23:54:19
132	ZENITH BANK	SUNDAY [redacted] IAH	2[redacted]10	4,360,000.00	2025-08-23 23:31:36

2

receiverName	receiverAccountNumber	receiverBank	createdAt	amountValue	narration
ALIYOS [redacted] LINK	12[redacted]96	000015	4/30/2025 23:51	9999500	TFR RESERVE 2
ALIYOS [redacted] LINK	12[redacted]96	000015	4/30/2025 23:52	9999501	TFR RESERVE 3
ALIYOS [redacted] LINK	12[redacted]96	000015	4/30/2025 23:52	9999502	TFR RESERVE 4

1

receiverName	receiverAccountNumber	receiverBank	createdAt	amountValue	narration
SUNDAY [redacted] IAH	1[redacted]3	000029	5/1/2025 7:58	9875200	SWEEPMAINTENANCE93
SUNDAY [redacted] IAH	1[redacted]3	000029	5/1/2025 7:59	9885200	SWEEPMAINTENANCE94
SUNDAY [redacted] IAH	1[redacted]3	000029	5/1/2025 8:04	4885200	SWEEPMAINTENANCE95

Indicator of Compromise (IoC)

- Tracked as **HK-FIN-10,** Pseudonym **HAYATU APE**
- Threats - The Internet Banking Channels of Banks were being targeted. Group dig APIs powering the channel and leveraging flaws in the APIs to identify accounts with funds and move funds to multiple accounts across banks.
- Targets - The group focused on financial institutions with internet banking channel integration accessible on the internet for customers, with **two incidents reported in Nigeria within Q1 and Q3 of 2025**.
- Transaction Narrations - TFR RESERVE [2,3,4], SWEEPMAINTENANCE[93.94,95]
- Targeted Technologies - Internet Banking Applications & Channel
- Other Group Being Tracked - HK-FIN-01, **HK-FIN-05**, **HK-FIN-20**, HK-FIN 25

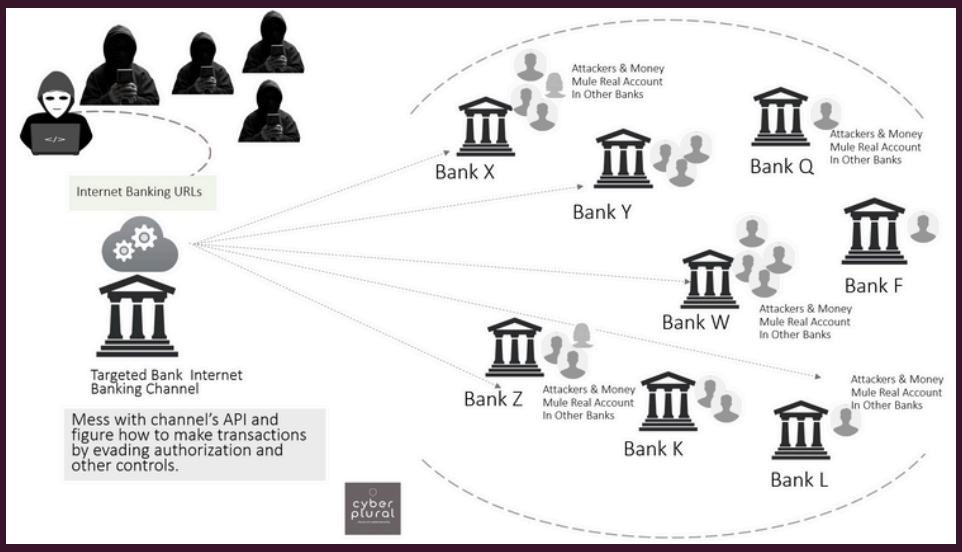
Locally Based Financially Motivated Threat Groups In Nigeria.

HK-FIN-10

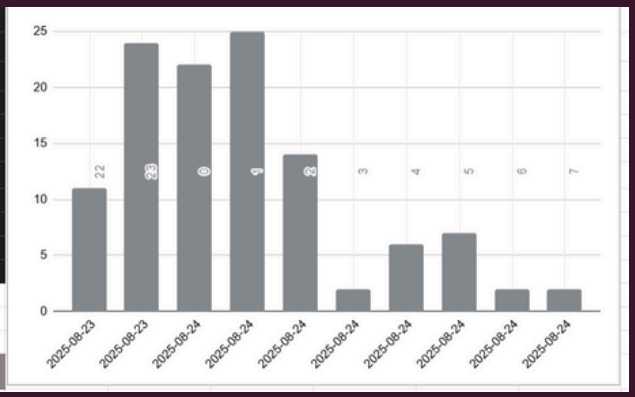
We observed that **HK-FIN-10** consistently executed all transactions between midnight and early morning on the following days. In both instances, over **150 transactions occurred**, draining the channels.

In addition, we noted that they maintained real accounts at other banks for receiving funds and often invited friends within their network to participate in these activities.

Law Enforcement Agencies (LEA) took action by freezing those accounts to prevent any further movement of funds, thereby aiding the investigation.



Date	Hour (24-hour format)	Number of Transactions
2025-08-23	22	11
2025-08-23	23	24
2025-08-24	0	22
2025-08-24	1	25
2025-08-24	2	14
2025-08-24	3	2
2025-08-24	4	6
2025-08-24	5	7
2025-08-24	6	2
2025-08-24	7	2
		115



Locally Based Financially Motivated Threat Groups In Nigeria.

HK-FIN-20

In 2025, we focused on a campaign by a group identified as **HK-FIN-20**, which targeted payment platforms. This group employed a strategy of initially registering as normal users to identify vulnerabilities within the payment application and to better understand its operational logic.

In a case investigated by our team, we observed that the application server was repeatedly targeted by automated probes and hacking attempts, as confirmed by our review of the application logs. We noted instances of users' PINs being brute-forced, as well as continuous attempts to transfer various amounts from the platform. In addition, user IDs were also subjected to brute-forcing, which was supported by our log reviews.

Ultimately, the attacker was able to guess a valid PIN, resulting in a significant sum of money being transferred to their account.

This scenario highlights how vulnerabilities inherent in the platform's design facilitated the attacker's success.

Furthermore, the lack of adequate monitoring exacerbated the situation, inviting additional attackers who were encouraged by the initial successful breach.

Indicator of Compromise (IoC)

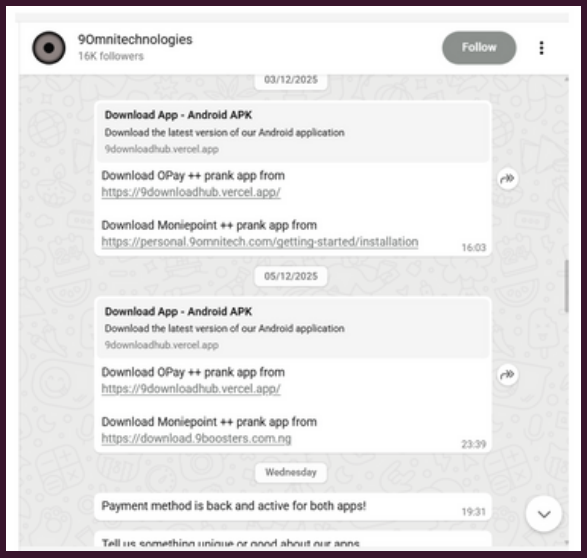
- Tracked as **HK-FIN-20**
- Threats - This group employed a strategy of initially registering as normal users to identify vulnerabilities
- Targets - Payment Platform - Naira & Crypto.
- Attackers Email - Hanacoxy85@gmail.com, coldeinkill@gmail.com, alexanderabbott30@gmail.com, wonderwonder006@gmail.com bigrate31@gmail.com" oludavid591@gmail.com olamiderate@gmail.com Jeffmatin14@gmail.com vojala3606@skatzy.com,angelinacolemilll@gmail.com, jetiwi5892@viperrow.com, vecoj94607@aperiol.com, angelinacolemiller@gmail.com, tonadeoludare213@gmail.com
- IP Addresses - 102.91.103.235, 102.91.93.241, 102.89.76.53, •52.169.249.88, 130.33.36.212, 13.74.151.138, 172.192.61.81, 185.177.72.10
- Targeted Platform - Naira & Crypto Payment Platforms

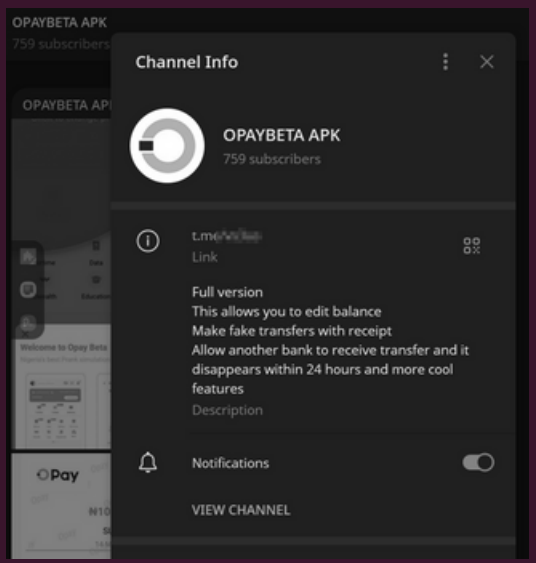
Threat Groups are Building Payment App Replicas for Fraud.

HK-FIN-25

We closely monitored the activities of a threat group tracked as **HK-FIN-25**, which has been actively leveraging software development skills to create fraudulent payment application replicas. These replicas mimic popular payment platforms such as Opay and Moniepoint, with specific instances identified as OpayBeta, OPay++, and Moniepoint++. These applications are being promoted by distinct players within the group, posing a significant risk to unsuspecting users.

The fraudulent applications enable users to manipulate their account balances, execute fake transfers complete with fabricated receipts, and facilitate transfers to other bank accounts that can disappear within 24 hours or more. This functionality not only deceives users but also undermines the integrity of legitimate financial systems. The threat group has utilised platforms like WhatsApp and Telegram to promote and advertise these replica applications for sale, creating channels where interested parties can engage with them directly.





Indicator of Compromise (IoC)

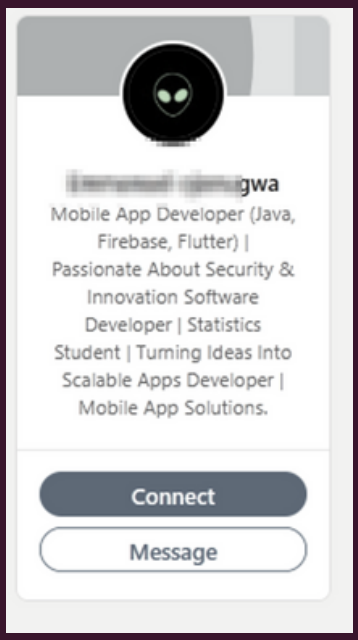
- Tracked as **HK-FIN-25**
- Threats - This group leverages software dev skills to create fraudulent payment application replicas
- Targets - Popular payment platforms such as Opay and Moniepoint
- Connected Details - download[.]9boosters[.]com.ng, personal[.]9omnitech[.]com/getting-started/installation, opaypro[.]9omnitech[.]com/, 9downloadhub[.]vercel.app, worldofhydras[@]gmail.com, facebook.com/61551922900339/, t[.]me/omniTech_hydra, omnicronhydra[.]com omiapps[.]9boosters[.]com.ng, nlhrlmk[@]gmail.com
- APK Hashes - SHA-256 [e79c905a2c90d40219e6ea2f102b3e774aac6e59e651bc1b49c63c93f74de83a]
- IP addresses - TCP 34.120.160.131:443 (opay-pro-default-rtdb.firebaseio.com), TCP 170.39.215.2:443 (api.schproject.com.ng), TCP 35.190.39.113:443 (opay-pro-default-rtdb.firebaseio.com)

Threat Groups are Building Payment App Replicas for Fraud. HK-FIN-25

Potential buyers are offered activation of these fraudulent applications at prices starting at 10,000 Naira. This pricing strategy indicates a calculated approach to monetize their illicit activities, making it accessible for various individuals looking to exploit the financial system.

In collaboration with our partners, and a focal interest on key players within this group, this facilitated the arrest of a member by Law Enforcement Agencies (LEA). This operation underscores the importance of coordinated efforts to combat cybercrime and dismantle such fraudulent networks. We continue to follow up on other members within **HK-FIN-25**, as the group's activities pose a persistent threat to the financial ecosystem.

Ongoing investigation aims to uncover additional details about the group's operations and to prevent further proliferation of these fraudulent applications. By sharing intelligence and collaborating with law enforcement, we hope to disrupt their activities and protect consumers from falling victim to these scams. The situation highlights the urgent need for enhanced security measures and awareness among users regarding the risks associated with unverified payment applications.



Infostealer Malware Campaign Rhamadanthys & Acreed Leading

In 2024, we conducted a special research study on an infostealer malware campaign in Nigeria, focusing on data collected from 2019 through the first quarter of 2024. Notably, certain malware variants, such as AgentTesla, Formbook, Asyncrat, and Lokibot, exhibited consistent persistence over time, while others appeared only briefly before vanishing.

By 2025, we observed new players like Rhamandanthys and Acreed emerging as leaders in their operations within Nigeria. These malware variants compromised several workstations across various organisations, leading to the availability of credentials on dark market forums. In some instances, these credentials were listed for sale for as little as $10, and researchers could even obtain them for free.

Leveraging these sources, initial access became a low-hanging fruit for attackers. During some of our red team engagements, we utilised credentials obtained from these sources to establish initial footholds or to gather more sensitive information about organisations from the dark web.

```
12219  apostlefavour@hig                    s.com.ng:favouruwaifo2020
12220  cinuade@      ade.ng:cimWisel$
12221  info@ad4      .com.ng:sullivantoby02
12222  enquirie      ghlc     l^      .com.ng:highlevel2020
12223  admin@illuminants.org.ng:(kuljnfy1cu0
12224  video1@gmconsulting.com.ng:mygm2020
12225  lawrence@d      tures.com.ng:okorodo@2021
12226  lawrence@d      tures.com.ng:david2004++
12227  admin@travelcentra.com.ng:@travel123
12228  maruf.ajimati@99creation.ng:amanwhoseeksyou35#
12229  advert@f      .com.ng:advert*123#god
12230  contact@      se.ng:gk^9uoq{m-bc
12231  support@      se.ng:u4p[r+k8i)2%
12232  info@pas      td.ng:pwk9kh{qyzw^
12233  emmanuel.o@in      b.ng:o*[umc#3y_xi
12234  admin@wheelsa      s.com.ng:kim20040428
12235  paulndioyemike@wh      up.ng:whitehorse1whitehorse2
12236  michael.epuechi@      rg.ng:empresswinnie37698
12237  admin@      s.ng:lahass2019#1234
12238  info@      ng:pathfinder@2019
12239  nosay
12240  devel
12241  dg@p
```

Building a repository of compromised credentials can aid in predicting which credentials may be used in an environment over the long term.

In addition, with the help of AI, this data can be utilized to train models for offensive capability.

NG	2025-09-29	2025.09.18	acreed	10.00	0.23Mb	Nu####ez [Diamond]	MTN NIGERIA Communication limited	Rivers State
NG	2025-09-24	2025.09.22	rhamadanthys	10.00	2.76Mb	d0####ey [platinum]	Airtel Networks Limited	Abia State
NG	2025-09-18	2025.09.10	acreed	10.00	0.20Mb	Nu####ez [Diamond]	MTN NIGERIA Communication limited	Lagos
NG	2025-07-08	2025.06.30	acreed	10.00	0.04Mb	Nu####ez [Diamond]	Airtel Networks Limited	FCT
NG	2025-06-30	2025.06.20	acreed	10.00	0.18Mb	Nu####ez [Diamond]	MTN NIGERIA Communication limited	Lagos

Infostealer Malware Campaign

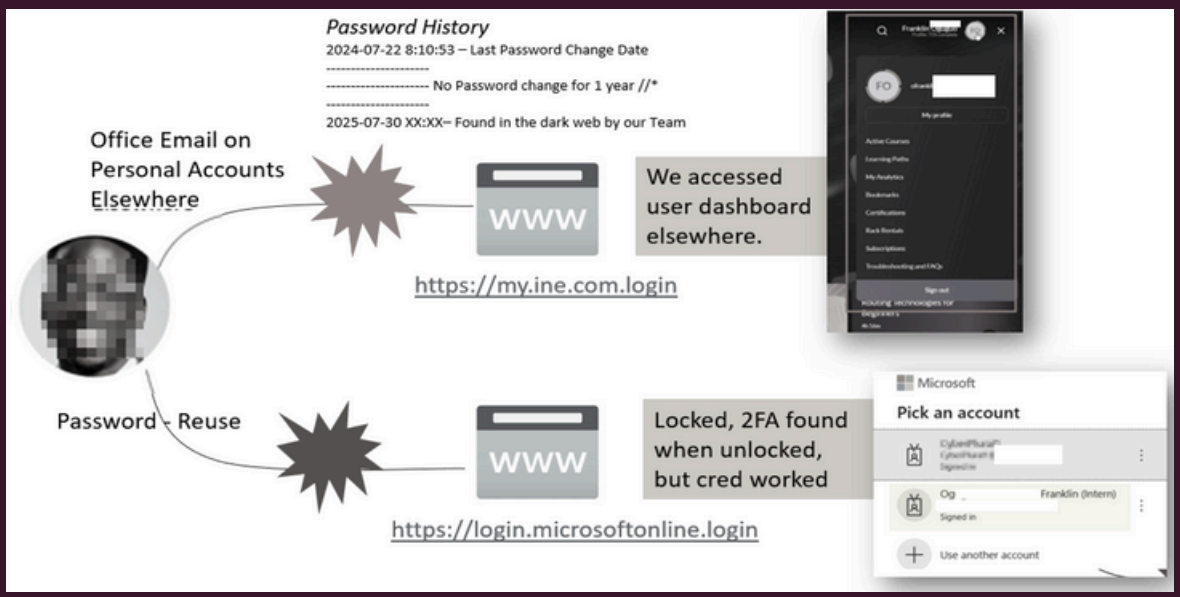
Case Study 1 - Credential for Initial Access

During a recent red team engagement, our threat intelligence team discovered several employee credentials listed on the dark web. Notably, one of these credentials belonged to an intern who used the same login information for a personal learning platform as they did for their office email on Outlook. This practice of reusing credentials posed a significant security risk.

We leveraged the compromised credentials to further enumerate information about the company's cloud infrastructure. Although the user's account had been disabled for Office 365 at the time of our discovery, we later validated that the credentials were still functional. This allowed us to gain direct access to the learning platform, as there was no multifactor authentication (MFA) implemented.

The lack of MFA on the learning platform provided us with an opportunity to explore the intern's access rights and gather sensitive information that could potentially expose the organisation to further risks. This incident underscores the critical importance of enforcing strong password policies and implementing multifactor authentication across all platforms to enhance security posture and reduce vulnerabilities.

Moving forward, organisations must prioritise employee training on the dangers of credential reuse and the importance of utilising MFA to safeguard their accounts. Additionally, regular audits of user accounts and access rights should be conducted to identify and mitigate potential security threats before they can be exploited by malicious actors.



Vulnerable servers and services in Nigeria are being used to host malware & C2

In 2025, we observed a trend involving the exploitation of vulnerable servers and services in Nigeria, which were leveraged to host malware and command-and-control (C2) operations. This alarming situation highlights significant security weaknesses within digital infrastructure and raises concerns about the potential consequences for both organisations and the public.

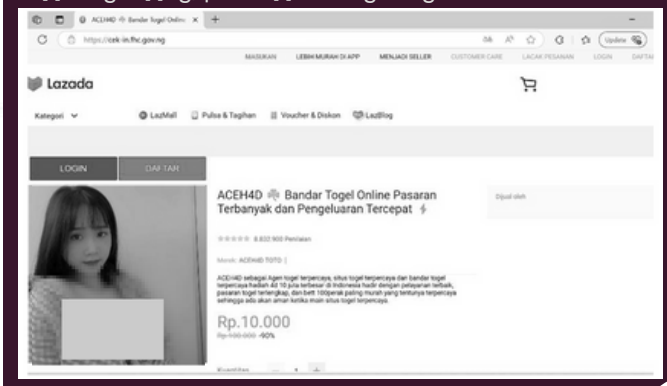
In two notable instances, malicious and pornographic content was served from government portals, specifically those of the Federal High Court (FHC) and the Federal Capital Territory (FCT) Waterboard. The presence of such inappropriate content on official government websites not only undermines the integrity of these institutions but also poses a serious risk to their reputation and public trust. This breach illustrates how attackers can exploit vulnerabilities in government systems to disseminate harmful material, potentially leading to legal and regulatory repercussions.

In addition, we identified another case where compromised vulnerable servers were utilised to host malware specifically designed for launching Distributed Denial of Service (DDoS) attacks. This malware actively scanned the internet for other vulnerable services, aiming to recruit them into a botnet. By doing so, the attackers significantly increased their capacity to execute large-scale DDoS attacks, which can cripple targeted websites and disrupt essential services on the internal network.

The ability to create such a botnet underscores the urgent need for organisations to fortify their defenses against exploitation.

The exploitation of vulnerable servers for malicious purposes highlights a critical gap in cybersecurity practices across various sectors in Nigeria. Organisations must prioritise the identification and remediation of vulnerabilities within their systems to prevent such breaches. This includes implementing regular security assessments, applying timely software updates, and employing advanced threat detection mechanisms.

IOC - reload[.]fhc.gov.ng, nextfhc[.]fhc.gov.ng, cek-in[.]fhc.gov[.]ng, portal[.]fctwb.gov.ng



Major Cyber Incidents as Engaged & Observed

Major Cyber Incidents as Engaged & Observed In 2025 – From Exposed PII & PHI, Impacted Sectors, Top Incidents & Causes

Government, Education & Technology Services.

24.8K

Bank Verification Number (BVN), NIN Slip, Civil Servant Bio Data Form, Students Bio Data Form, Certificate

FinTech Platform, Finance Companies, Logistic, e-Commerce, Health

337.1K

Personally Identifiable Info (PII), Names, Phone Number, BVN, Addresses, Password Hashes, Protected Health Information (PHI)

Telecommunications, Oil & Gas, NGO and Others.

50K

Organisation Data, KYC Data, Passport, NIN Slips, Stolen Email Credential by Info Stealer Malware.

Please note that more PII and PHI may have been exposed beyond what we've observed in our operational data review and community chatters.

Top Incidents

[1] Info Stealer Malware Campaign

[2] Ransomware Attack

[3] Platform Breach

[4] Third Party Data Breach

Both defenders and cyber threat groups are increasingly leveraging AI to gain an advantage over one another.

Top Causes

[1] Insecure Design, Vulnerable & Misconfigured Services

[2] Lack of Proactive Monitoring on Digital Assets.

[3] Prioritise Paper Compliance Culture.

[4] Poor Incident Reporting Culture, Coordination with industry peers, and CERTs

Insight from Red Team Engagements in 2025

Top Vulns in Web, Mobile & APIs

- Logic Vulnerability,
- Lack of Rate Limiting
- IDOR/BOLA,
- Auth Failure /Auth bypass
- Biometric Bypass, Inconsistent Policy (Password Policy)

Top Vulns in Cloud –AWS & Azure

- Misconfigurations & Over Permission
- Exposed Buckets,
- PrivEsc Through PutUser Policy,
- Improper Inventory Management – Active Past Employees – 2 to 3 years

Top Vulns in Network

- Default Password – Low hanging fruits
- High-privilege accounts on IOT devices
- Active Directory Misconfigurations
- Outdated Services & Devices

Organisations are encouraged to build a secure platform and network environment by engaging professionals to test and retest their applications, services, and networks before going live in 2026.

Platform Breach

5 Nigerian Digital Platforms Hit

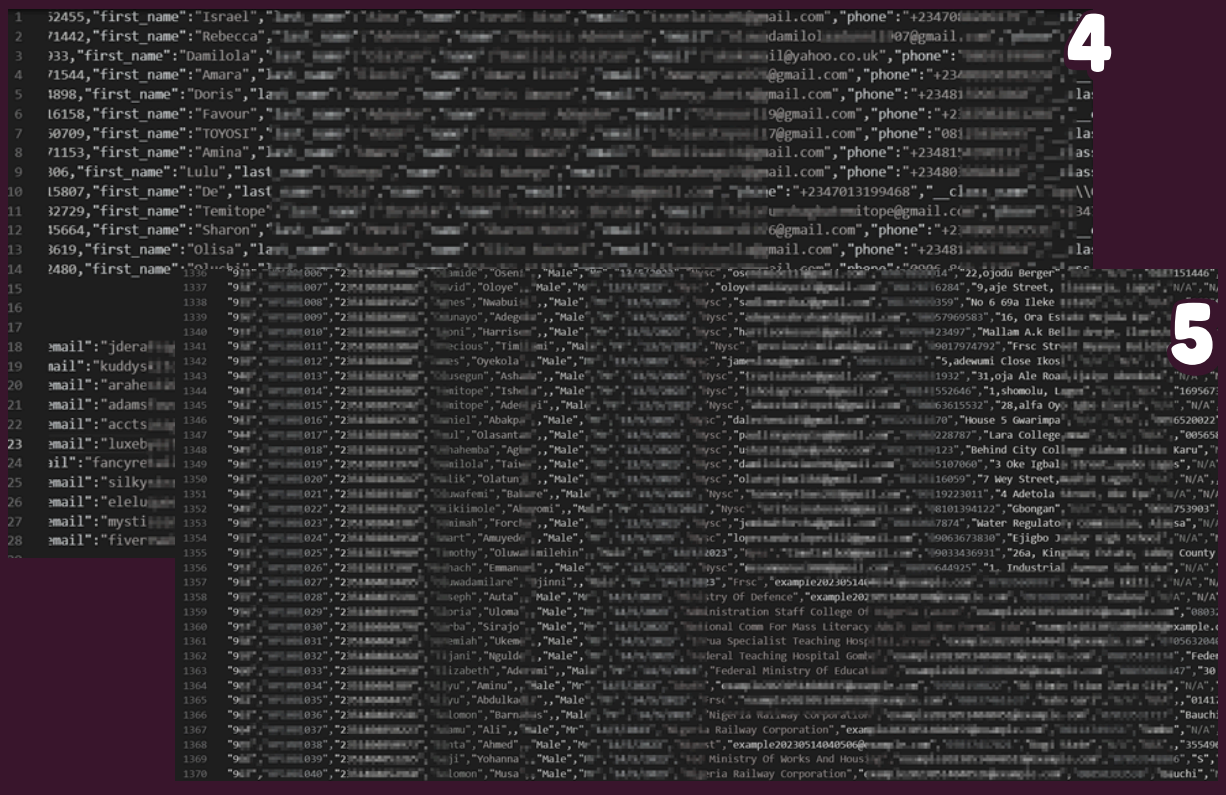
In September 2025 alone, over five Nigerian digital platforms, including fintech companies, finance firms, online store providers, and food delivery services, had their databases leaked to the dark web. It is estimated that the personal identifiable information (PII) of more than 340,000 customers and employees may have been exposed during this period. In connection with one of the leaks, which is currently available for sale, the threat actor is offering it for $500.

Platform Breach

5 Nigerian Digital Platforms Hit

Most of the platform breaches observed in 2025 have primarily involved the leakage of personally identifiable information (PII) belonging to customers and users. This sensitive data includes critical details such as names, addresses, phone numbers, dates of birth, and email addresses. The exposure of such information not only compromises individual privacy but also poses significant risks to organizations and their customers.

The ramifications of these breaches can be severe. For individuals, the leakage of PII can lead to identity theft, financial fraud, and a host of other malicious activities that exploit their personal information. Attackers can use stolen data to open fraudulent accounts, make unauthorised transactions, or launch targeted phishing attacks, further exacerbating the threat landscape.



For organizations, the consequences of failing to protect customer data can be equally damaging. Beyond the immediate financial costs associated with remediation efforts, companies may suffer reputational damage that can erode customer trust and loyalty. Regulatory penalties may also be imposed in cases of non-compliance with data protection laws, adding to the financial burden.

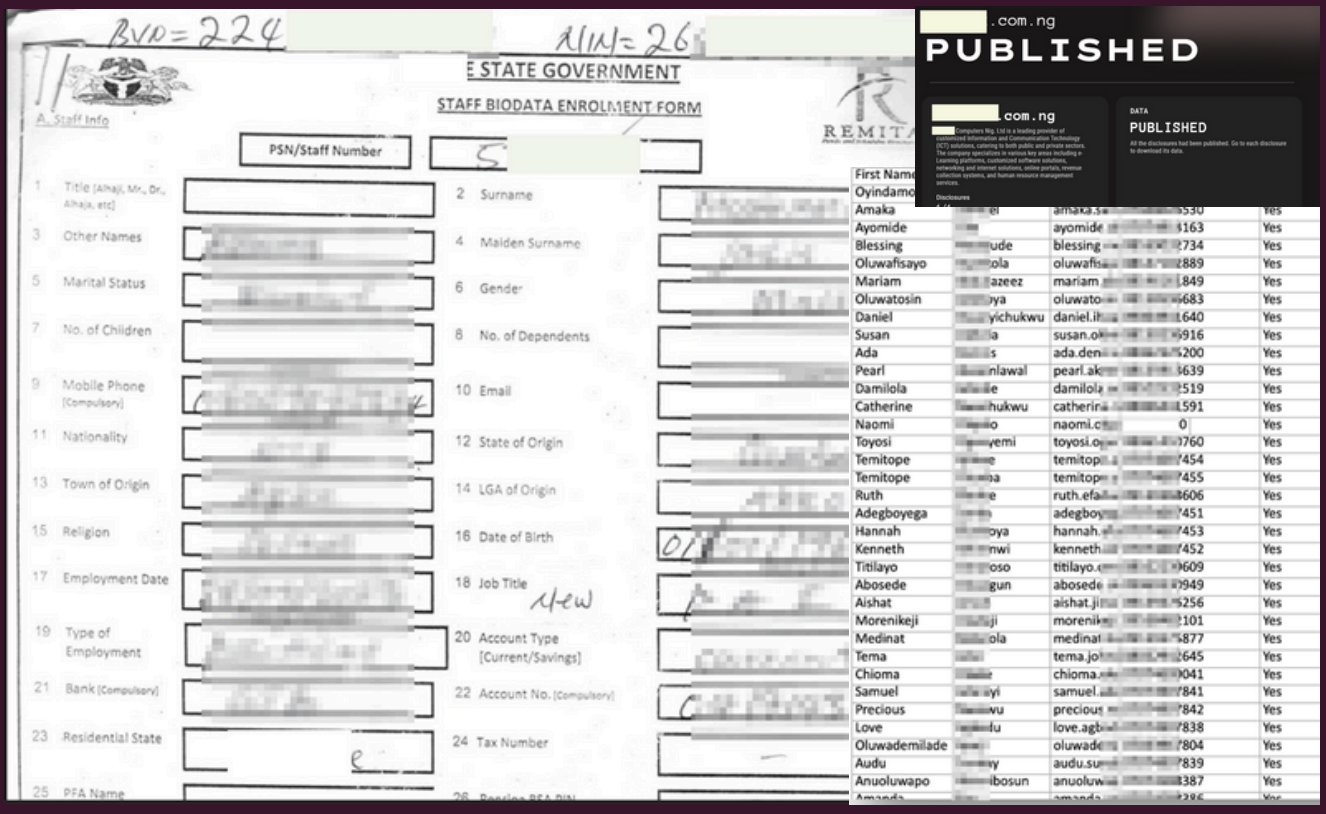
Platform Breach

KillSec Ransomware Group In Nigeria

The KillSec Ransomware Group, which has been active in Nigeria since late 2024, successfully breached the systems of over five Nigerian organisations (players in finance, technology service, government and food). Our investigation revealed a significant leak of sensitive data from a state government, which was included among the information published on their victim-shaming website.

This breach not only highlights the group's increasing focus on high-profile targets within Nigeria but also raises serious concerns about the security of governmental data. The leaked information may contain critical details that could jeopardise the privacy and safety of citizens, as well as undermine public trust in governmental institutions.

The KillSec Ransomware Group's tactics demonstrate a disturbing trend in cybercrime, where attackers exploit vulnerabilities in organisational defences to access and disseminate sensitive data. This incident serves as a stark reminder of the urgent need for enhanced cybersecurity measures across all sectors, particularly in protecting vital government infrastructure and sensitive information



The Shadow Perimeter | A Red Team Retrospective on 2025

1 Traditional Infrastructure - The Persistence of Legacy Flaws

In the realm of traditional networking, "low-hanging fruit" continued to yield high-impact results in 2025. We frequently secured initial access through the most basic of oversights - default credentials. It is a sobering reality that in 2025, common services like FTP and administrative interfaces for routers and IoT hardware - including smart office equipment - still ship with and retain factory-default usernames and passwords.

One of the most significant "war stories" involved a standard office printer. By exploiting the lack of network segmentation and the use of default credentials, we successfully performed an LDAP poisoning attack.

Because the printer was configured to authenticate against the domain with the domain Admin AD credential, we intercepted Domain Admin credentials, effectively compromising the entire corporate forest from the printer - a device that is often overlooked in a standard patch cycle. Furthermore, we noted that high-profile exploits like EternalBlue are becoming rarer in modern environments.

2 The Pattern Trap - Password Psychology vs. Complexity

Despite organisations enforcing "complex" policies - requiring symbols, numbers, and capital letters - the human element defaulted to a standard formula: [OrganizationName] + [Year] + [SpecialCharacter] (e.g., CyberPural2025!).

Systemic Propagation: This pattern was not limited to low-level users; we discovered it across all tiers of the infrastructure. We found this exact logic being used for:

Wifi and Administrative Router Interfaces: Where wifi passwords and router "default" were changed to a predictable pattern that was easily guessed during initial reconnaissance.

Service Accounts: Which often go unrotated for years, making them susceptible to "Yearly" pattern guessing (e.g., trying 2024 or 2023 for older accounts).

Cloud and SaaS Portals: Where employees used the same organisational pattern for various Saas and Cloud logins.

The Registration vs. Reset Paradox: Another prevalent finding throughout the year was the inconsistency in how these policies are enforced. Many web applications had strong password policies on the initial registration page, forcing users to create unique credentials. However, those same restrictions were often absent on the "Update Password" or "Forgot Password" endpoints. This allowed users (and our pentesters) to change a once-strong password to a weak, predictable pattern later in the account lifecycle, effectively nullifying the initial security controls.

The Shadow Perimeter | A Red Team Retrospective on 2025

3 Web Applications - Logic Failures and Compliance Risks

Our web application assessments in 2025 showed a shift from simple injection flaws to complex logic vulnerabilities and broken authentication. We identified numerous instances where the business logic of an application could be manipulated to gain unauthorized access to administrative panels. Improper use of HTTP methods; specifically, the use of the GET method for login forms and sensitive data transmission.

The danger here is twofold. Technically, it causes sensitive credentials to be stored in server logs and browser histories, turning these logs into a goldmine for attackers. From a compliance perspective, this exposes the organization to massive liability under frameworks like the Nigeria Data Protection Act (NDP Act 2023) and GDPR.

If an attacker gains access to these logs, the resulting data breach could lead to crippling fines and loss of consumer trust. We also identified critical logic errors in payment endpoints where the flow of a transaction could be interrupted or modified to bypass payment verification, leading to direct and immediate financial loss.

4 The API Frontier - Where Firewalls Fail

If 2025 had a primary theater of operations, it was the API. We observed a significant "security gap" where organisations would deploy a robust Web Application Firewall (WAF) to protect their user-facing web portal but leave the underlying API completely exposed. This is a critical blind spot; an API is often the direct line to the database, and without equivalent protection, it becomes an easy target.

The most common vulnerability we exploited was the total absence of rate-limiting. On "forgotten password" or "OTP" endpoints, the lack of rate-limiting allowed our pentesters to brute-force 4 or 6-digit reset pins with ease, leading to widespread account takeovers. We also saw a high frequency of Broken Object Level Authorization (BOLA), often aided by predictable UIDs or weak Base64 encoding. By simply changing an ID in a URL, we could dump thousands of customer PII records - including National Identity Numbers (NIN) and Bank Verification Numbers (BVN) - across various sectors.

5 Mobile Security and Cross-Platform Inconsistency

While mobile applications are often perceived as more secure due to their sandboxed nature, our 2025 engagements proved that "hardened" does not mean "impenetrable." We encountered a variety of client-side protections, such as SSL Pinning, Root Detection, and Biometric Authentication, that were designed to thwart attackers, yet we successfully bypassed them in nearly every instance.

The Shadow Perimeter | A Red Team Retrospective on 2025

SSL Pinning and Emulator Evasion - Many organisations rely on SSL pinning to prevent Man-in-the-Middle (MITM) attacks. However, through the use of dynamic instrumentation tools like Frida and Objection, our pentesters were able to hook into the application's runtime and disable these checks.

This allowed us to intercept and manipulate traffic between the mobile app and the backend server. Furthermore, we bypassed sophisticated emulator detection scripts that were meant to prevent the app from running in a controlled testing environment, giving us a platform to perform deep analysis without the constraints of physical hardware

Biometric and Root Detection Bypass: We also saw a rise in the use of biometric authentication (Fingerprint/FaceID) as a primary security layer. Our team demonstrated that if a device is rooted or jailbroken, these biometric checks can often be bypassed by manipulating the boolean values the application receives from the OS.

As organisations rush to support Android, iOS, and Web platforms simultaneously, we identified a trend of "Security Inconsistency."

In one notable engagement, we discovered a stored XSS (Cross-Site Scripting) vector on a mobile application endpoint. While the mobile app itself didn't render the script, the payload was triggered on the web app ,and things changed rapidly when an administrator viewed the stored payload on the web-based management portal. We successfully chained this "invisible" mobile vulnerability to steal administrative session cookies, leading to a full system takeover.

6 Cloud Misconfigurations and the Human Element

The transition to the cloud has not eliminated old risks; it has simply rebranded them as "The Great Misconfiguration." Overly permissive Identity and Access Management (IAM) policies remained our primary vector in cloud environments. We frequently utilised the PutUserPolicy permission to escalate a low-privileged developer account into a full Cloud Administrator.

Perhaps the most alarming finding was the failure of asset inventory and offboarding processes. We discovered active accounts for employees who had left their respective organisations more than two years prior. These "ghost accounts" provide a silent, persistent entry point for attackers. This human element was further highlighted by our OSINT (Open Source Intelligence) research. Our threat intel operations provided some of the most "human" insights of the year. We focused heavily on credential leaks and "Black Market" data portals, where we recovered valid credentials for high-profile staff.

One of the most compelling "war stories" involved a valid credential belonging to a member of the in-house cybersecurity team. This discovery highlighted a dangerous trend: an overestimation of security amongst professionals. There is often a subconscious belief that "no one would dare attack the experts," or that being a "Guru" makes one immune to common mistakes like credential reuse or phishing.

Attackers, however, are indifferent to your job title; they look for the path of least resistance. Our team proved that unimaginable oversights, like a security engineer using a common password pattern or failing to enable MFA on a personal account linked to corporate assets, are often what grant an attacker their first foothold.

AI In Cybersecurity & Cybersecurity of AI in 2025

AI In Cybersecurity In 2025 - Offensive

In 2025, threat actors didn't necessarily replace the existing tactics, techniques and procedures but they used the Gen AI to enhance their operations.

Nation-state actors use GenAI for the following

- Reconnaissance operations, intelligence gathering
- Vulnerability research and exploit identification
- Phishing Campaign content development
- Payload development and refinement

While other malicious actors used it for the following

- Task automation and workflow optimisation
- Script generation and code development
- Malware development and evaluation

RedVDS Infrastructure Used for AI-Enabled Fraud, AI-generated videos and voice deepfakes for Impersonation, and AI-Assisted Phishing Campaign.

AI In Cybersecurity In 2025 - Defensive

In 2025, there was an increase in the number of deployed AI systems within Security Operations Centres (SOCs) and defensive architectures to match evolving threats.

AI has become essential to defensive security for reducing alert fatigue, shortening response windows, and enabling proactive security strategies.

Top AI-focused cybersecurity tools and platforms for defense in 2025.

SentinelOne Singularity XDR & Purple AI, Torq HyperSOC, Microsoft Security Copilot, Dropzone AI SOC Analyst, Google BigSleep & SEC-Gemini, Fortinet FortiAI,

Cybersecurity of AI Systems In 2025

In early 2025, Chinese AI startup DeepSeek experienced a sustained and highly coordinated Distributed Denial-of-Service (DDoS) attack that significantly disrupted its services.

In April 2025, CrowdStrike observed multiple threat actors exploit CVE-2025-3248, an unauthenticated code injection vulnerability in Langflow AI.

In mid-September 2025, AI safety company Anthropic detected the **first documented large-scale cyber espionage campaign** primarily executed by an AI system, marking a pivotal moment in the evolution of AI misuse.

Agentic AI systems development and usage are expected to blow up in 2026, and Continuous research by adversarial groups and state-sponsored groups will continue on AI systems, targeting those in public and private use.

We can expect cyber threat actors to increasingly use AI to automate and improve the accuracy of cyber attacks. This will result in a rapid evolution of the threat landscape, similar to the advancements seen in generative AI tools for deep fake creation and phishing attacks. Cyber defenders will also continue to leverage AI in defense, as the race for integration into security technology keep advancing.

https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf
https://www.crowdstrike.com/en-us/resources/reports/threat-hunting-report/ https://adversa.ai/top-ai-security-incidents-report-2025-edition/
https://cloudsecurityalliance.org/artifacts/data-security-within-ai-environments
https://redmondmag.com/articles/2026/01/15/microsoft-knocks-offline-redvds-cybercrime-marketplace.aspx
https://www.microsoft.com/en-us/security/blog/2026/01/14/inside-redvds-how-a-single-virtual-desktop-provider-fueled-worldwide-cybercriminal-operations
https://genai.owasp.org/2025/07/14/owasp-gen-ai-incident-exploit-round-up-q225
https://torq.io/blog/ai-soc-benefits/

Proactive Strategies for Cyber Resilience in 2026

In 2026, businesses must prioritise cybersecurity. **Budgeting for cybersecurity** is essential; allocate resources for technology, training, and incident response to protect against emerging threats.

Implement **security measures that ensure compliance** with industry regulations to avoid penalties and maintain stakeholder trust. A strong security foundation safeguards sensitive data and fosters a culture of compliance.

Focus on **technical capacity building** by investing in training and certifications for your team. Enhancing their skills will empower them to effectively combat cyber threats.

Learn from past incidents; **preparation is key**. Conduct post-incident reviews to identify weaknesses and improve your incident response plans, reducing the likelihood of future issues.

Coordinate with industry peers, CyberPlural MSSP, the National & Sectoral CERTs to share knowledge and threat intelligence. Collaboration strengthens collective security efforts

Finally, commit to **continuous improvement** in your cybersecurity practices. Regularly update policies, conduct training, and adopt new technologies to stay ahead of evolving threats.

2026 Cyber Outlook

Based on the data and trends observed in 2025, we anticipate that the cybersecurity landscape in Nigeria will continue to evolve, presenting both challenges and opportunities for organisations.

Increased Ransomware & Infostealer Activity

We expect ransomware attacks to remain a significant threat in 2026, with more sophisticated tactics employed by threat actors.

Growth in Data Breaches

With the ongoing exploitation of vulnerabilities in servers and services, we project a rise in data breaches, particularly involving sensitive personal and organisational information.

Regulatory Developments & LEAs Crackdown

As cyber threats increase, we anticipate that regulatory bodies will implement stricter enforcement for data protection and cybersecurity and continuous crackdown from LEAs.

Expansion of Financially Motivated Threat Groups

The rise of locally based financially motivated threat groups is expected to continue, with these actors increasingly targeting sectors such as finance, healthcare, and government.

Adoption of Advanced Security Measures

In response to the growing threat landscape, organisations are expected to invest more in cybersecurity measures, including fundamentals like MFA, advanced threat detection systems, and employee training programs.

Collaboration and Information Sharing

The importance of collaboration among organisations, government agencies, and cybersecurity firms will become more pronounced.

In summary, 2026 is likely to see a continuation of the trends established in 2025, with heightened threats and increased focus on cybersecurity investments. Organisations must remain vigilant and proactive in their security strategies to effectively navigate this dynamic environment.

CyberPlural MSSP

We help startups and enterprises create and manage resilient cybersecurity plans and implementation across the board while they focus on profit-making and business growth.

CyberPlural's MSSP methodology is unique in its approach, providing the opportunity to creatively design a cybersecurity strategy and plans that provide businesses/organizations with the resiliency to scale in the ever-growing world of the Internet at a very affordable cost targeted at driving value for clients.

Our strategies and approaches are tightly structured and aim to provide the overall security required for business continuity, as our services are packed into Security Operations, CyberDemia, Threat Intelligence, Governance, Risk and Compliance (GRC), System Assessment & Audit, with Research & Development.

Do you need help with any of our cyber offerings? Feel free to consult and use our services.

email

hello@cyberplural.com

web

cyberplural.com

cyberdemia

cyberdemia.com

blog

blog.cyberplural.com

social

cyberplural