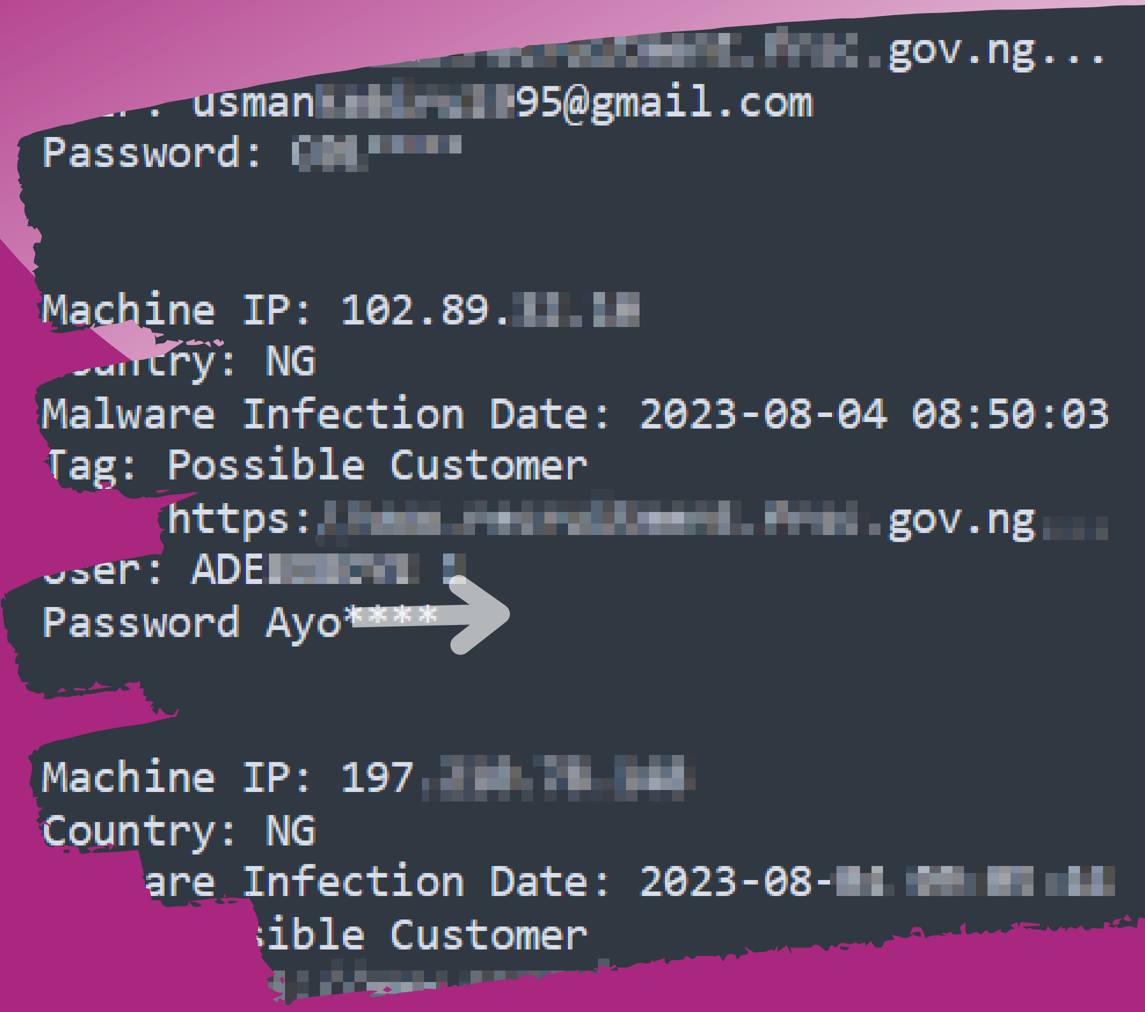
2023 | Q3 Report

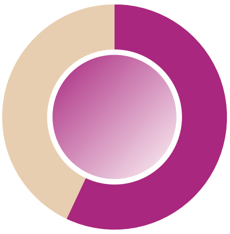
Cyber Incident Reports, Major CVEs & Threat Intel.



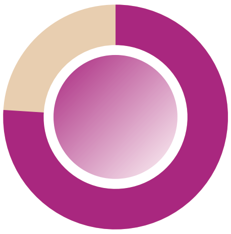
```
[redacted].gov.ng...
: usman[redacted]95@gmail.com
Password: [redacted]****

Machine IP: 102.89.[redacted]
ntry: NG
Malware Infection Date: 2023-08-04 08:50:03
Tag: Possible Customer
     https:[redacted].gov.ng[redacted]
ser: ADE[redacted]
Password Ayo****

Machine IP: 197[redacted]
Country: NG
    are Infection Date: 2023-08-[redacted]
        ible Customer
```

cyberplural.com
hello@cyberplural.com

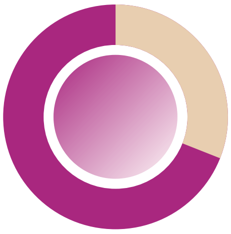
2023 | Q3 at a glance



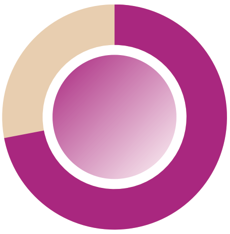
The issue of unreported cyber incidents continues into Q3 of 2023 in Nigeria. If organizations and businesses continue to conceal cyber incidents, it could undermine the digital trust that society relies on and provide more opportunities for threat actors to exploit vulnerabilities.



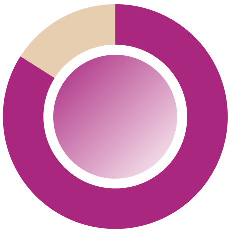
Info stealer malware is a specific type of malware that is created to extract sensitive information from compromised systems. Several SOC teams have reported activities relating to this class of malware targeting organizations in Nigeria. Additionally, there have been reports on online forums of credentials being sold on the dark web.



Anonymous Sudan, a threat group noted for causing havoc by launching DDoS attacks on vital systems and disrupting digital services has been found to continue their campaign. This was the case in Nigeria and Kenya, where the hacktivists targeted key infrastructure recently.



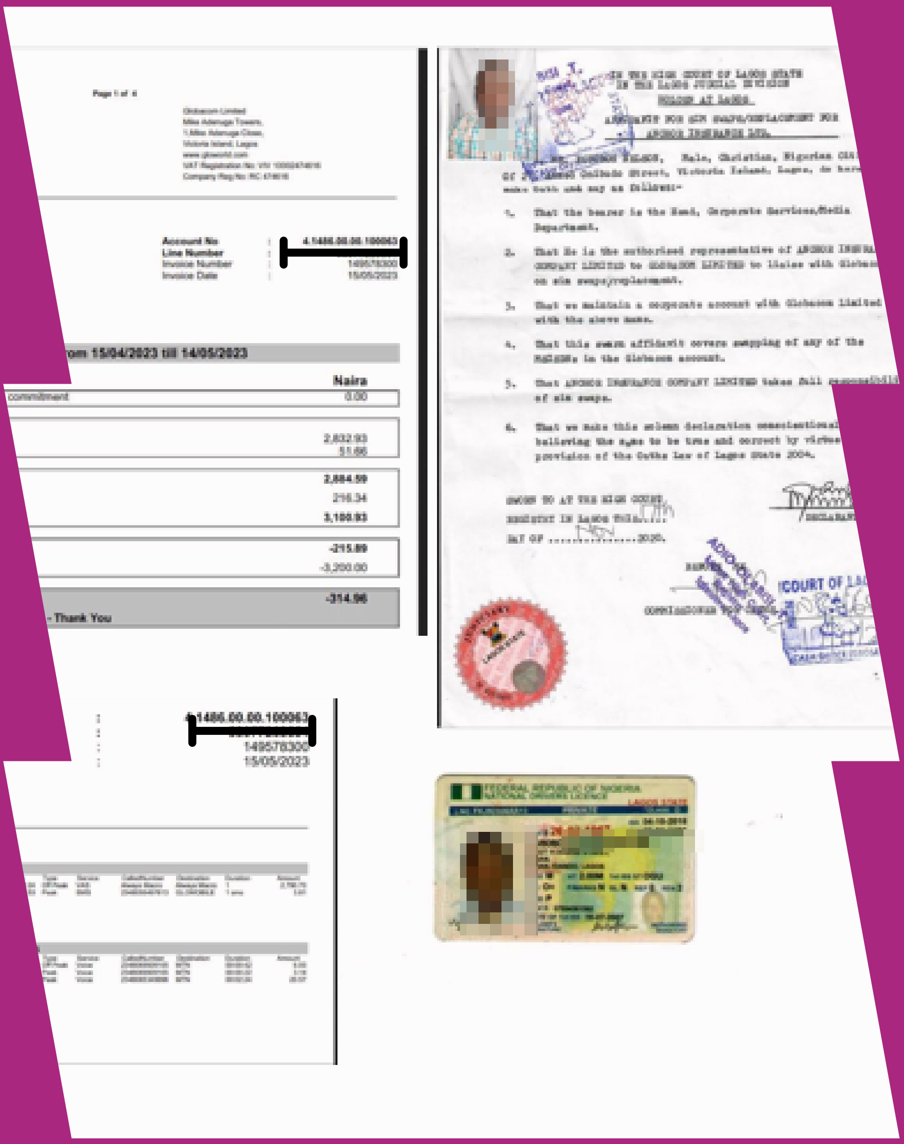
Threat Intelligence Ops has identified and reported misconfigurations that have caused sensitive data leaks on critical systems and facilities in Nigeria. Our reports have played a crucial role in preventing these leaks and addressing the vulnerabilities, thereby contributing to a safer cyberspace.



The ALPHV ransomware group continues to pose a significant threat to organizations in Nigeria. It is important for businesses to take proactive steps to protect themselves.

cyber
plural
...focus on cybersecurity

ALPHV Ransomware Group Strikes Again: Major Nigerian Telecom Company Hit in Latest Attack



Page 1 of 4

Globacom Limited
Mike Adenuga Towers,
1,Mike Adenuga Close,
Victoria Island, Lagos
www.gloworld.com
VAT Registration No: [illegible]
Company Reg No: RC [illegible]

Account No	:	[redacted]
Line Number	:	
Invoice Number	:	1495783300
Invoice Date	:	15/05/2023

rom 15/04/2023 till 14/05/2023

	Naira
commitment	0.00
	2,832.93
	51.66
	2,884.59
	216.34
	3,100.93
	-215.89
	-3,200.00
	-314.96
- Thank You	

[redacted]
1495783300
15/05/2023

IN THE HIGH COURT OF LAGOS STATE
IN THE LAGOS JUDICIAL DIVISION
HOLDEN AT LAGOS.

AFFIDAVIT FOR SIM SWAPS/REPLACEMENT FOR
ANCHOR INSURANCE LTD.

I, [illegible], Male, Christian, Nigerian Citi[illegible] of [illegible] Street, Victoria Island, Lagos, do here[illegible] make oath and say as follows:-

1. That the bearer is the Head, Corporate Services/Media Department.
2. That He is the authorized representative of ANCHOR INSURA[illegible] COMPANY LIMITED to GLOBACOM LIMITED to liaise with Globaco[illegible] on sim swaps/replacement.
3. That we maintain a corporate account with Globacom Limited with the above name.
4. That this sworn affidavit covers swapping of any of the MSISDNs in the Globacom account.
5. That ANCHOR INSURANCE COMPANY LIMITED takes full responsibili[illegible] of sim swaps.
6. That we make this solemn declaration conscientiousl[illegible] believing the same to be true and correct by virtue [illegible] provision of the Oaths Law of Lagos State 2004.

SWORN TO AT THE HIGH COURT
REGISTRY IN LAGOS THIS...[illegible]
DAY OF ......[illegible]......2020.

DEPONENT

BEFORE ME

COMMISSIONER FOR OATHS

COURT OF LA[illegible]

FEDERAL REPUBLIC OF NIGERIA
NATIONAL DRIVERS LICENCE
LAGOS STATE

ALPHV Ransomware Group Strikes Again: Major Nigerian Telecom Company Hit in Latest Attack

In the latest ransomware attack to hit Nigeria, a major player in the telecom industry has fallen victim to the ALPHV ransomware group. This is the third major Nigerian company to be hit by the group in just 18 months, following attacks on a gaming company and an insurance company.

According to reports from Whitehat.NG and the dark web, the ALPHV group had access to the victim's network for 12 days before exfiltrating critical organizational data, including personally identifiable information of customers and stakeholders. The group then encrypted this data and demanded a large ransom from the victim.

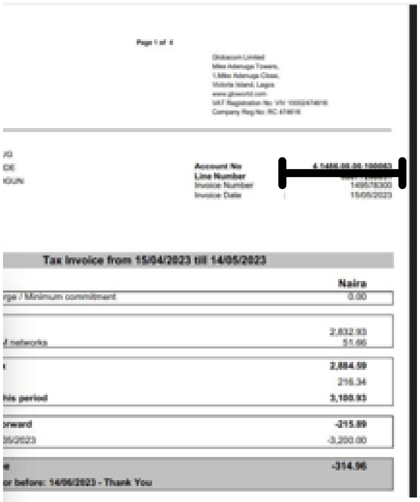
The organization was given an ultimatum to respond to the ransom demand through negotiation, or the threat actors would start releasing exfiltrated information to the dark web. Unfortunately, there has been no official statement from the impacted organization, and it is unclear if notifications have been sent to affected customers to guard against secondary attacks that may arise from this incident.

This latest attack highlights the growing threat posed by the ALPHV ransomware group, which has become a prolific threat actor in Nigeria. Organizations must take proactive measures to protect their systems and data from these types of attacks. This includes implementing robust cybersecurity measures, focusing on detection, active defense, and regular data backups.

It is also important for organizations to have an incident response plan in place, which outlines the steps to be taken in the event of a cyber-attack. This should include a clear communication plan, both internally and externally, to ensure that all stakeholders are kept informed throughout the incident.

In conclusion, the ALPHV ransomware group continues to pose a significant threat to organizations in Nigeria. It is important for businesses to take proactive steps to protect themselves from these types of attacks and have an incident response plan in place to minimize the impact of any potential breach.

ALPHV Ransomware Group Strikes Again: Major Nigerian Telecom Company Hit in Latest Attack



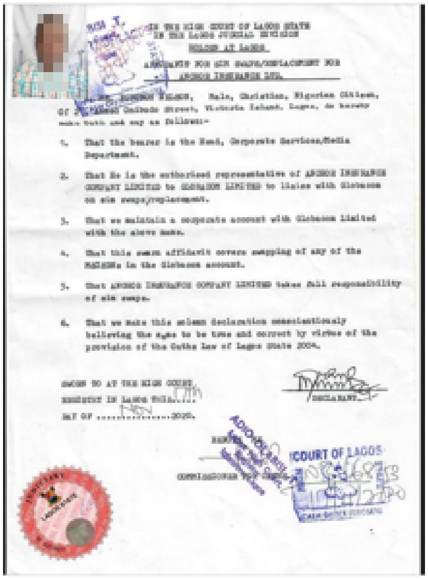
Page 1 of 4

Globacom Limited
Mike Adenuga Towers,
1,Mike Adenuga Close,
Victoria Island, Lagos
www.gloworld.com
VAT Registration No: [illegible]
Company Reg No: RC [illegible]

Account No [redacted]
Line Number
Invoice Number 149578300
Invoice Date 15/05/2023

Tax Invoice from 15/04/2023 till 14/05/2023

	Naira
rge / Minimum commitment	0.00
	2,832.93
f networks	51.66
	2,884.59
	216.34
his period	3,100.93
orward	-215.89
05/2023	-3,200.00
e	-314.96
or before: 14/06/2023 - Thank You	



IN THE HIGH COURT OF LAGOS STATE
IN THE LAGOS JUDICIAL DIVISION
HOLDEN AT LAGOS

AFFIDAVIT FOR SIM SWAPS/REPLACEMENT FOR
ANCHOR INSURANCE LTD.

I, [illegible], Male, Christian, Nigerian Citizen, of [illegible] Ahmed Onibudo Street, Victoria Island, Lagos, do hereby make Oath and say as follows:-

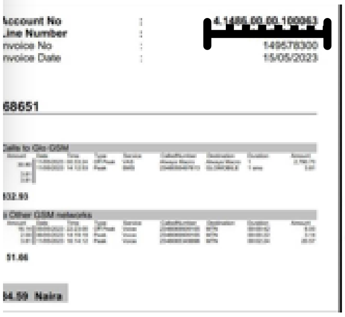
1. That the bearer is the Head, Corporate Services/Media Department.
2. That He is the authorized representative of ANCHOR INSURANCE COMPANY LIMITED to GLOBACOM LIMITED to liaise with Globacom on sim swaps/replacement.
3. That we maintain a corporate account with Globacom Limited with the above name.
4. That this sworn affidavit covers swapping of any of the NUMBERs in the Globacom account.
5. That ANCHOR INSURANCE COMPANY LIMITED takes full responsibility of sim swaps.
6. That we make this solemn declaration conscientiously believing the same to be true and correct by virtue of the provision of the Oaths Law of Lagos State 2004.

SWORN TO AT THE HIGH COURT
REGISTRY IN LAGOS THIS.....
DAY OF ......NOV..........2020.

DECLARANT

COMMISSIONER FOR OATHS

COURT OF LAGOS



Account No : 4.1486.00.00.100063
Line Number : [redacted]
Invoice No : 149578300
Invoice Date : 15/05/2023

68651

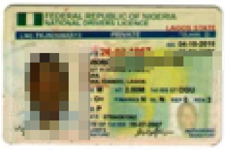
Calls to Glo GSM

832.93

Other GSM networks

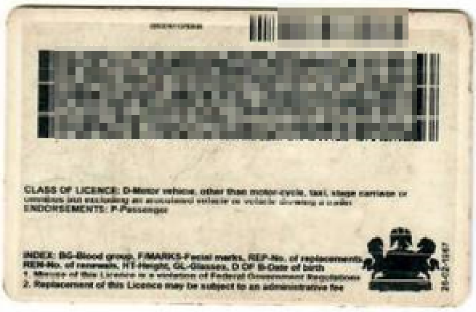
51.66

84.59 Naira



FEDERAL REPUBLIC OF NIGERIA
NATIONAL DRIVERS LICENCE
LAGOS STATE

[redacted]

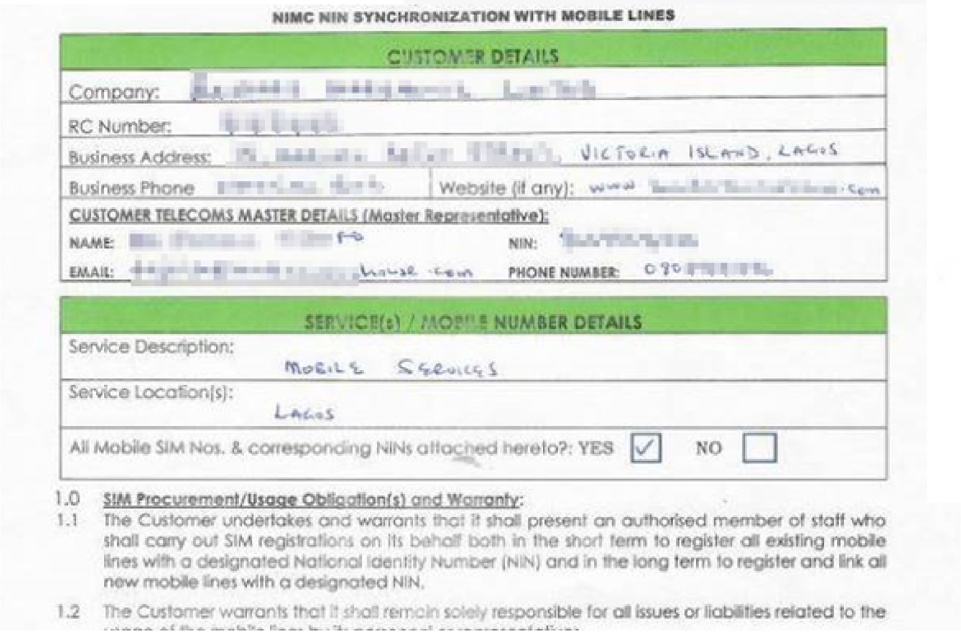


[redacted]

CLASS OF LICENCE: D-Motor vehicle, other than motor-cycle, taxi, stage carriage or omnibus but excluding an articulated vehicle or vehicle drawing a trailer
ENDORSEMENTS: P-Passenger

INDEX: BG-Blood group, F/MARKS-Facial marks, REP-No. of replacements, REN-No. of renewals, HT-Height, GL-Glasses, D OF B-Date of birth
1. Misuse of this Licence is a violation of Federal Government Regulations
2. Replacement of this Licence may be subject to an administrative fee

Sample data from the darkweb



NIMC NIN SYNCHRONIZATION WITH MOBILE LINES

CUSTOMER DETAILS

Company: [redacted]

RC Number: [redacted]

Business Address: [redacted] VICTORIA ISLAND, LAGOS

Business Phone [redacted] | Website (if any): www. [redacted] .com

CUSTOMER TELECOMS MASTER DETAILS (Master Representative):

NAME: [redacted] | NIN: [redacted]

EMAIL: [redacted] house .com | PHONE NUMBER: 080 [redacted]

SERVICE(s) / MOBILE NUMBER DETAILS

Service Description: MOBILE SERVICES

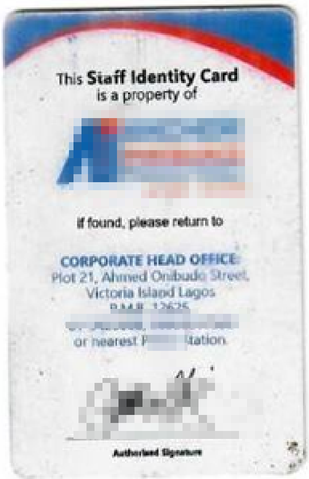
Service Location(s): LAGOS

All Mobile SIM Nos. & corresponding NINs attached hereto?: YES ☑ NO □

1.0 SIM Procurement/Usage Obligation(s) and Warranty:

1.1 The Customer undertakes and warrants that it shall present an authorised member of staff who shall carry out SIM registrations on its behalf both in the short term to register all existing mobile lines with a designated National Identity Number (NIN) and in the long term to register and link all new mobile lines with a designated NIN.

1.2 The Customer warrants that it shall remain solely responsible for all issues or liabilities related to the



This Staff Identity Card
is a property of

[redacted]

If found, please return to

CORPORATE HEAD OFFICE
Plot 21, Ahmed Onibudo Street,
Victoria Island Lagos
P.M.B. 12625
[redacted]
or nearest P[redacted]station

[redacted]

Authorised Signature

July 2023

Organizations Breached / Experienced Ransomware Attack

- U.S. Ambassador to China Hacked through Microsoft Exchange email
- Hawaii Community College
- Estonian crypto platform CoinsPaid
- Japan’s Port of Nagoya
- NATO investigates alleged data theft
- Nickelodeon Data Leak
- Razar confirms a data breach
- Estée Lauder's network Breach by ALPHV
- Major Nigerian Telecom Company

Critical CVEs Reported

- Cisco and VMware Products
- Citrix addressing CVE-2023-3519
- Adobe - Adobe ColdFusion

Interesting Highlight

- Estonian cryptocurrency payment service provider CoinsPaid reported a cyber attack in July, resulting in the theft of $37.2 million worth of cryptocurrency.
- VirusTotal issued an apology for a data exposure incident that resulted in sharing information about over 5,000 of the site's customers online. The company attributed the leak to human error on the part of one of its employees.
- GitHub revealed a social engineering campaign that specifically targeted employees of technology firms on their platform. The Lazarus group, an APT group from North Korea, attempted to gain the trust of users by proposing collaboration on a shared repository.
- Anonymous Sudan hit Kenya’s government with a massive DDOS attack affecting over 5,000 services. The government confirmed that this affected the eCitizen portal, used by the public to access over 5,000 government services.

cyber plural
...focus on cybersecurity

Anonymous Sudan Launches Cyberattacks on Nigeria's Vital Information Systems

Anonymous Sudan Launches Cyberattacks on Nigeria’s Vital Information Systems

On August 1, 2023, Anonymous Sudan announced on their Telegram channel that they would be launching cyberattacks on Nigeria’s vital information systems. This announcement was made in response to Nigeria’s participation in ECOWAS’s recent instructions to the Nigerien military to hand over power to the democratically elected government of the Niger Republic.

The planned DDoS attack began on August 2nd, with over 100GB of traffic hitting an ISP. As a result, customers and users of various services experienced a partial service outage. The attack caused partial downtime for some ISPs, as many businesses and individuals rely heavily on online services.

Following and prior to the cyberattack launched by Anonymous Sudan on Nigeria’s vital information systems, the Computer Emergency Response Teams (CERTs) in Nigeria have taken proactive measures to help organizations protect their systems.

The Nigeria Computer Emergency Response Team (ngCERT), which is located at the Office of the National Security Adviser (ONSA), and the National Information Technology Development Agency (NITDA) Computer Emergency Readiness and Response Team (CERRT) have both released advisories to help organizations during this period.

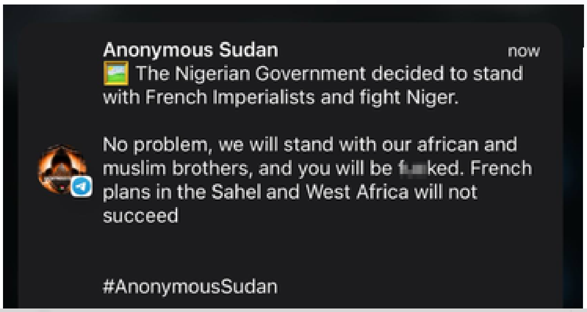
The advisories provide guidelines on how organizations can protect their systems from cyber threats and what to do in case of a cyberattack. They also provide information on how to report cyber incidents and seek assistance from the relevant authorities.

The ngCERT advisory includes deploying DDoS protection services where possible. The NITDA CERRT advisory also emphasizes the need for organizations to educate their employees on cybersecurity best practices and to implement robust incident response plans

Anonymous Sudan Launches Cyberattacks on Nigeria’s Vital Information Systems

The release of these advisories by the CERTs is a step in the right direction towards enhancing Nigeria’s cybersecurity posture. It is important for organizations to take these advisories seriously and implement the recommended measures to protect their systems from cyber threats.

In conclusion, the cyberattack launched by Anonymous Sudan on Nigeria’s vital information systems highlights the need for organizations to prioritize cybersecurity. The release of advisories by ngCERT and NITDA CERRT is a welcome development and demonstrates the government’s commitment to enhancing Nigeria’s cybersecurity posture. It is crucial for organizations to take proactive measures to protect their systems and seek assistance from the relevant authorities in case of a cyber incident.

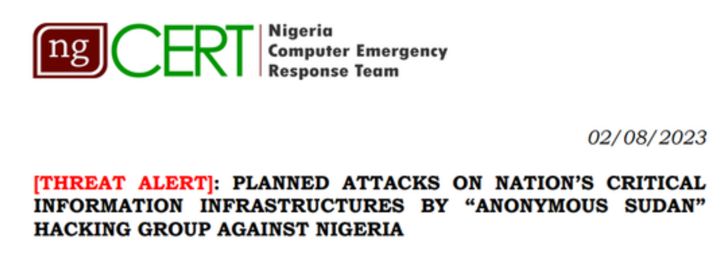


Anonymous Sudan now

🖼️ The Nigerian Government decided to stand with French Imperialists and fight Niger.

No problem, we will stand with our african and muslim brothers, and you will be f[redacted]ked. French plans in the Sahel and West Africa will not succeed

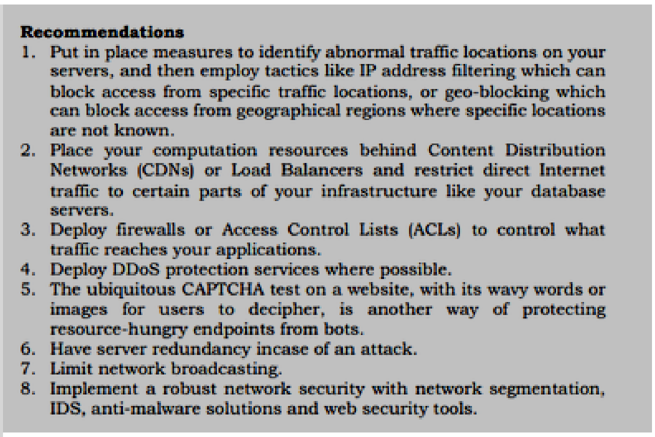
#AnonymousSudan



ngCERT Nigeria Computer Emergency Response Team

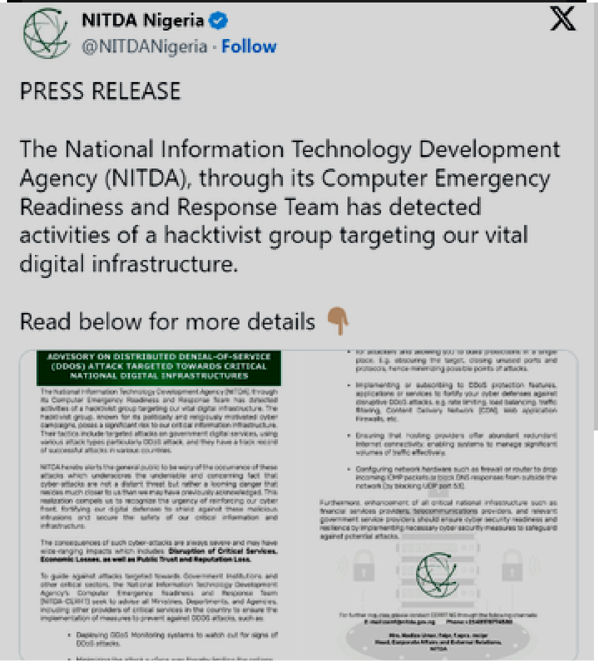
02/08/2023

[THREAT ALERT]: PLANNED ATTACKS ON NATION’S CRITICAL INFORMATION INFRASTRUCTURES BY “ANONYMOUS SUDAN” HACKING GROUP AGAINST NIGERIA



Recommendations

1. Put in place measures to identify abnormal traffic locations on your servers, and then employ tactics like IP address filtering which can block access from specific traffic locations, or geo-blocking which can block access from geographical regions where specific locations are not known.
2. Place your computation resources behind Content Distribution Networks (CDNs) or Load Balancers and restrict direct Internet traffic to certain parts of your infrastructure like your database servers.
3. Deploy firewalls or Access Control Lists (ACLs) to control what traffic reaches your applications.
4. Deploy DDoS protection services where possible.
5. The ubiquitous CAPTCHA test on a website, with its wavy words or images for users to decipher, is another way of protecting resource-hungry endpoints from bots.
6. Have server redundancy incase of an attack.
7. Limit network broadcasting.
8. Implement a robust network security with network segmentation, IDS, anti-malware solutions and web security tools.



NITDA Nigeria
@NITDANigeria · Follow

PRESS RELEASE

The National Information Technology Development Agency (NITDA), through its Computer Emergency Readiness and Response Team has detected activities of a hacktivist group targeting our vital digital infrastructure.

Read below for more details 👇

ADVISORY ON DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACK TARGETED TOWARDS CRITICAL NATIONAL DIGITAL INFRASTRUCTURES

The National Information Technology Development Agency (NITDA) through its Computer Emergency Readiness and Response Team has detected activities of a hacktivist group targeting our vital digital infrastructure. The hacktivist group, known for its politically and religiously motivated cyber campaigns, poses a significant risk to our critical information infrastructure. Their tactics include targeted attacks on government digital services, using various attack types particularly DDoS attack, and they have a track record of successful attacks in various countries.

NITDA hereby alerts the general public to be wary of the occurrence of these attacks which underscores the undeniable and concerning fact that cyber-attacks are not a distant threat but rather a looming danger that resides much closer to us than we may have previously acknowledged. This realization compels us to recognize the urgency of reinforcing our cyber front, fortifying our digital defenses to shield against these malicious intrusions and secure the safety of our critical information and infrastructure.

The consequences of such cyber-attacks are always severe and may have wide-ranging impacts which includes: **Disruption of Critical Services, Economic Losses, as well as Public Trust and Reputation Loss.**

To guide against attacks targeted towards Government Institutions and other critical sectors, the National Information Technology Development Agency's Computer Emergency Readiness and Response Team (NITDA-CERRT) seek to advise all Ministries, Departments, and Agencies, including other providers of critical services in the country to ensure the implementation of measures to prevent against DDOS attacks, such as:

- Deploying DDoS Monitoring systems to watch out for signs of DDoS attacks.
- Minimizing the attack surface area thereby limiting the options for attackers and allowing you to build protections in a single place. E.g. obscuring the target, closing unused ports and protocols, hence minimizing possible points of attacks.
- Implementing or subscribing to DDoS protection features, applications or services to fortify your cyber defenses against disruptive DDoS attacks, e.g. rate limiting, load balancing, traffic filtering, Content Delivery Network (CDN), web application firewalls, etc.
- Ensuring that hosting providers offer abundant redundant internet connectivity enabling systems to manage significant volumes of traffic effectively.
- Configuring network hardware such as firewall or router to drop incoming ICMP packets or block DNS responses from outside the network (by blocking UDP port 53).

Furthermore, enhancement of all critical national infrastructure such as financial services providers, telecommunications providers, and relevant government service providers should ensure cyber security readiness and resilience by implementing necessary cyber security measures to safeguard against potential attacks.

For further inquiries please contact CERRT.NG through the following channels:
E-mail: [illegible]@nitda.gov.ng Phone: [illegible]

Mrs. Hadiza Umar, Fdipr, Fspra, mnipr
Head, Corporate Affairs and External Relations,
NITDA

August 2023

Organizations Breached / Experienced Ransomware Attack

- Prospect Medical Holdings, a major healthcare services provider
- West Oaks School suffers ransomware
- Poland's Train Network
- Forever 21 disclose data breach
- The German Federal Bar (BRAK) Association
- Japanese Watch Manufacturer SEIKO
- Discord.io breached

Critical CVEs Reported

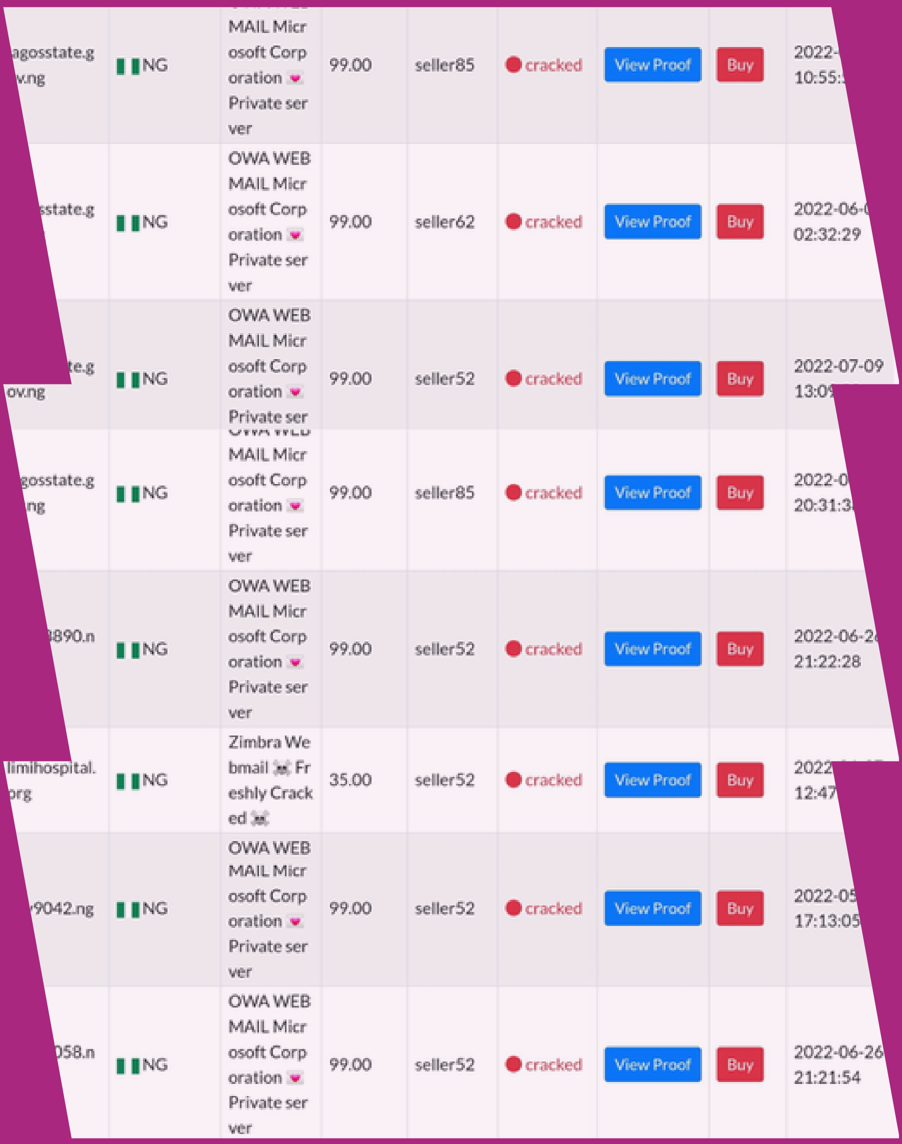
- Papercut - CVE-2023-39143
- Mozilla Firefox
- WordPress Elementor Plugin
- Juniper Firewall -CVE-2023-36844, CVE-2023-36847

Interesting Highlight

- Anonymous Sudan hit Nigeria's Cyberspace with a massive DDOS attack The attack caused partial downtime in some ISPs, as many businesses and individuals rely heavily on online services.
- APT29 (aka Midnight Blizzard, NOBELIUM, Cozy Bear) carried out a social engineering campaign leveraging Microsoft Teams.
- 16shop, a phishing-as-a-service (PaaS) platform was brought down by Interpol.
- CloudNordic, a Danish cloud service provider, experienced a ransomware attack. According to CloudNordic, the attack resulted in the destruction of customer data stored on their servers, including both primary and secondary backups.
- Kroll announces that personal information related to the bankruptcy cases of crypto firms BlockFi, FTX, and Genesis was exfiltrated by a threat actor
- AI-driven malicious tools emerging on the dark web – FraudGPT, WormGPT

cyber plural
...focus on cybersecurity

Info Stealer Malware Infests Organizations in Nigeria



agosstate.gov.ng	🇳🇬NG	MAIL Microsoft Corporation 💌 Private server	99.00	seller85	● cracked	View Proof	Buy	2022- 10:55:
sstate.g	🇳🇬NG	OWA WEB MAIL Microsoft Corporation 💌 Private server	99.00	seller62	● cracked	View Proof	Buy	2022-06- 02:32:29
te.gov.ng	🇳🇬NG	OWA WEB MAIL Microsoft Corporation 💌 Private ser	99.00	seller52	● cracked	View Proof	Buy	2022-07-09 13:0
gosstate.g ng	🇳🇬NG	MAIL Microsoft Corporation 💌 Private server	99.00	seller85	● cracked	View Proof	Buy	2022-0 20:31:3
890.n	🇳🇬NG	OWA WEB MAIL Microsoft Corporation 💌 Private server	99.00	seller52	● cracked	View Proof	Buy	2022-06-2 21:22:28
limihospital.org	🇳🇬NG	Zimbra Webmail ☠️ Freshly Cracked ☠️	35.00	seller52	● cracked	View Proof	Buy	2022 12:47
9042.ng	🇳🇬NG	OWA WEB MAIL Microsoft Corporation 💌 Private server	99.00	seller52	● cracked	View Proof	Buy	2022-05 17:13:05
058.n	🇳🇬NG	OWA WEB MAIL Microsoft Corporation 💌 Private server	99.00	seller52	● cracked	View Proof	Buy	2022-06-26 21:21:54

2023 | Q3 Report

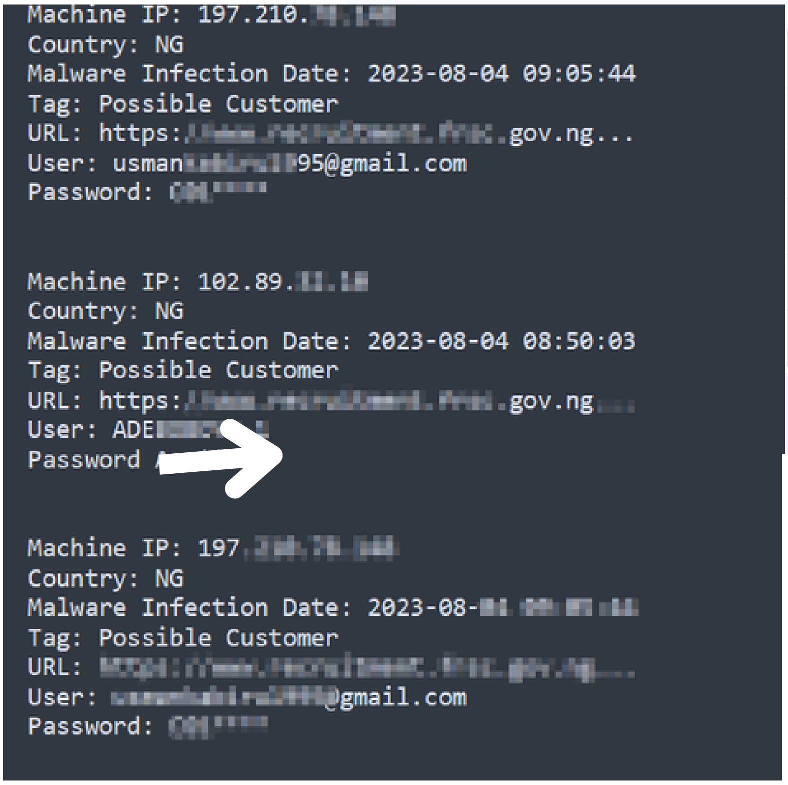
cyberplural.com

Info Stealer Malware Infests Organizations in Nigeria

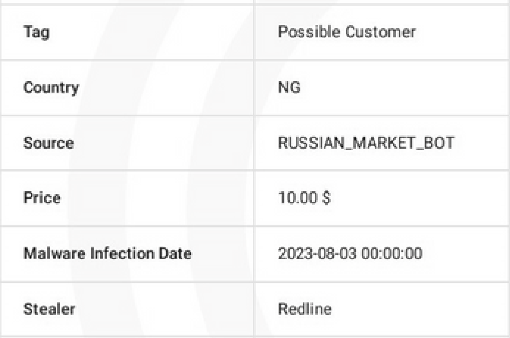
In recent years, Nigeria has seen a significant increase in cyber-attacks, with organizations of all sizes and industries falling victim to various forms of malware. One type of malware that has become increasingly prevalent in Nigeria is the Info stealer malware.

The Info stealer malware is a type of malware that is designed to steal sensitive information from infected systems. It can steal a wide range of data, including login credentials, financial information, and personally identifiable information (PII). Once the malware has successfully stolen the data, it sends it back to the attacker's command and control (C&C) server.

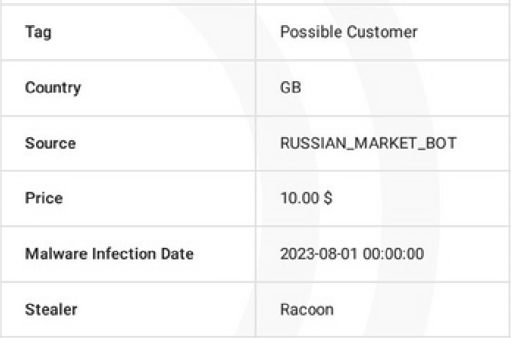
Our CTI team has found on the dark web stolen credentials from Nigeria and other activities related to Info stealer malware listed on different underground forums for sale. This highlights the growing threat posed by this malware in Nigeria.



```
Machine IP: 197.210.[redacted]
Country: NG
Malware Infection Date: 2023-08-04 09:05:44
Tag: Possible Customer
URL: https:[redacted].gov.ng...
User: usman[redacted]95@gmail.com
Password: [redacted]


Machine IP: 102.89.[redacted]
Country: NG
Malware Infection Date: 2023-08-04 08:50:03
Tag: Possible Customer
URL: https:[redacted].gov.ng[redacted]
User: ADE[redacted]
Password [redacted]


Machine IP: 197[redacted]
Country: NG
Malware Infection Date: 2023-08-[redacted]
Tag: Possible Customer
URL: [redacted]
User: [redacted]@gmail.com
Password: [redacted]
```

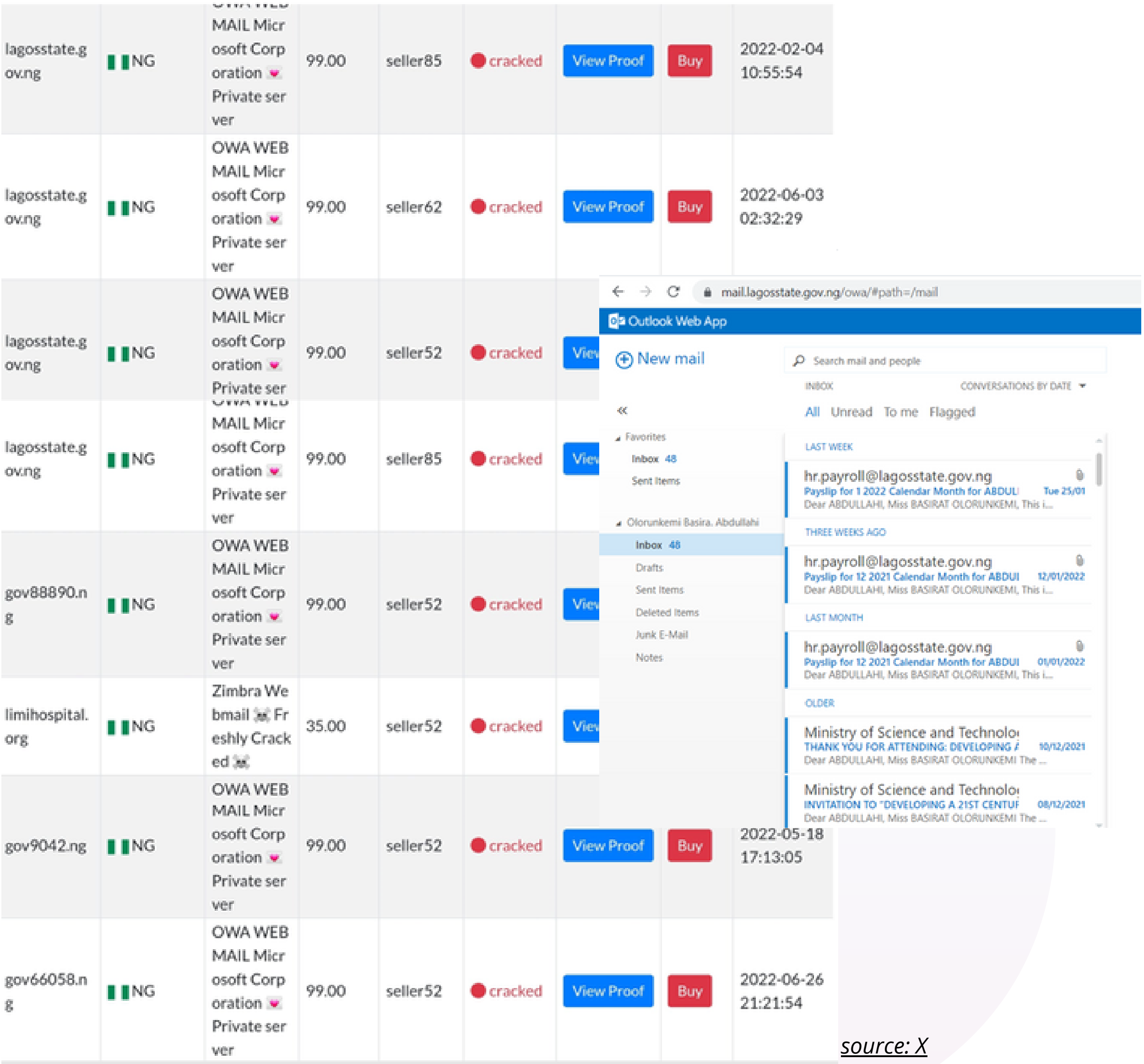


Tag	Possible Customer
Country	NG
Source	RUSSIAN_MARKET_BOT
Price	10.00 $
Malware Infection Date	2023-08-03 00:00:00
Stealer	Redline



Tag	Possible Customer
Country	GB
Source	RUSSIAN_MARKET_BOT
Price	10.00 $
Malware Infection Date	2023-08-01 00:00:00
Stealer	Racoon

Info Stealer Malware Infests Organizations in Nigeria



lagosstate.gov.ng	NG	OWA WEB MAIL Microsoft Corporation 💌 Private server	99.00	seller85	● cracked	View Proof	Buy	2022-02-04 10:55:54
lagosstate.gov.ng	NG	OWA WEB MAIL Microsoft Corporation 💌 Private server	99.00	seller62	● cracked	View Proof	Buy	2022-06-03 02:32:29
lagosstate.gov.ng	NG	OWA WEB MAIL Microsoft Corporation 💌 Private ser	99.00	seller52	● cracked	View		
lagosstate.gov.ng	NG	OWA WEB MAIL Microsoft Corporation 💌 Private server	99.00	seller85	● cracked	View		
gov88890.ng	NG	OWA WEB MAIL Microsoft Corporation 💌 Private server	99.00	seller52	● cracked	View		
limihospital.org	NG	Zimbra Webmail ☠ Freshly Cracked ☠	35.00	seller52	● cracked	View		
gov9042.ng	NG	OWA WEB MAIL Microsoft Corporation 💌 Private server	99.00	seller52	● cracked	View Proof	Buy	2022-05-18 17:13:05
gov66058.ng	NG	OWA WEB MAIL Microsoft Corporation 💌 Private server	99.00	seller52	● cracked	View Proof	Buy	2022-06-26 21:21:54

mail.lagosstate.gov.ng/owa/#path=/mail

Outlook Web App

LAST WEEK

hr.payroll@lagosstate.gov.ng
Payslip for 1 2022 Calendar Month for ABDUL Tue 25/01
Dear ABDULLAHI, Miss BASIRAT OLORUNKEMI, This i...

THREE WEEKS AGO

hr.payroll@lagosstate.gov.ng
Payslip for 12 2021 Calendar Month for ABDUI 12/01/2022
Dear ABDULLAHI, Miss BASIRAT OLORUNKEMI, This i...

LAST MONTH

hr.payroll@lagosstate.gov.ng
Payslip for 12 2021 Calendar Month for ABDUI 01/01/2022
Dear ABDULLAHI, Miss BASIRAT OLORUNKEMI, This i...

OLDER

Ministry of Science and Technolo
THANK YOU FOR ATTENDING: DEVELOPING A 10/12/2021
Dear ABDULLAHI, Miss BASIRAT OLORUNKEMI The ...

Ministry of Science and Technolo
INVITATION TO "DEVELOPING A 21ST CENTUF 08/12/2021
Dear ABDULLAHI, Miss BASIRAT OLORUNKEMI The ...

source: X

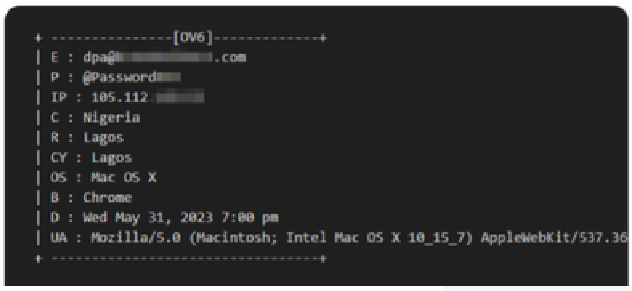
One factor contributing to the prevalence of Info stealer malware in Nigeria is the lack of or ineffectiveness of cybersecurity awareness among employees. Many employees are not aware of the risks associated with opening suspicious emails or clicking on links from unknown sources. This makes them more susceptible to phishing attacks, which are often used to distribute malware.

Another factor is the lack of robust and effective cybersecurity measures in many Nigerian organizations. Many businesses do not have adequate and effective controls in place, making them more vulnerable to targeted and non-targeted cyber-attacks.

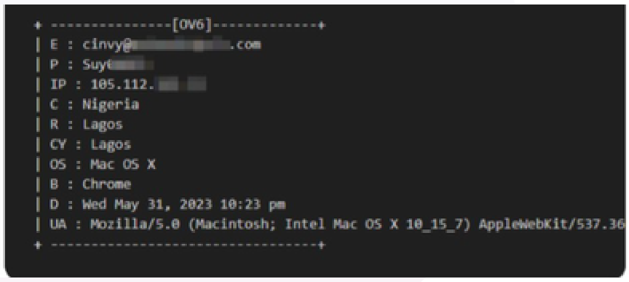
Info Stealer Malware Infests Organizations in Nigeria

The use of cracked operating systems and software has contributed to the high rise of infection on personal laptops and other mobile devices. Info stealers malware like Racoon, RedLine, Pony, and Agent Tesla activities have been observed during proactive monitoring by the SOC Team across industry vertical, as well as incident response engagement where info stealers malware capability were seen packaged into ransomware code ahead of the data exfiltration and encryption activities during ransomware deployment.

A recent report by Group-IB revealed the discovery of a new web-based control panel called W3LL. This control panel is used by cybercriminals to manage various types of malware, including banking trojans, ransomware, and information stealers. The W3LL panel is being offered for sale on the dark web and is marketed as a "one-stop shop" for managing malware campaigns. The discovery of this control panel highlights the growing sophistication of cybercriminals and the need for businesses to take proactive measures to protect their systems and data from these types of attacks.



```
+ ---------------[OV6]-------------+
| E : dpa@[redacted].com
| P : @Password[redacted]
| IP : 105.112[redacted]
| C : Nigeria
| R : Lagos
| CY : Lagos
| OS : Mac OS X
| B : Chrome
| D : Wed May 31, 2023 7:00 pm
| UA : Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
+ ---------------------------------+
```



```
+ ---------------[OV6]-------------+
| E : cinvy@[redacted].com
| P : Suy[redacted]
| IP : 105.112.[redacted]
| C : Nigeria
| R : Lagos
| CY : Lagos
| OS : Mac OS X
| B : Chrome
| D : Wed May 31, 2023 10:23 pm
| UA : Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
+ ---------------------------------+
```

To protect against Info stealer malware and other types of malware, organizations in Nigeria must take proactive measures to improve their cybersecurity posture. This includes implementing robust and proactive cybersecurity controls that are risk-based. It also includes providing regular cybersecurity training to employees to raise awareness of the risks associated with cyber-attacks and how to prevent them.

In conclusion, the Info stealer malware is a significant threat to organizations in Nigeria. It is important for businesses to take proactive steps to protect themselves from these types of attacks

September 2023

Organizations Breached / Experienced Ransomware Attack

- Government of Nova Scotia
- Air Canada’s Internal network breached
- Lanka Government Cloud (LGC) - Sri Lanka
- Israeli hospital Mayanei HaYeshua
- The city of Seville, Spain
- Cyberport Network Breach
- American Resort, Casino and Hotel chain MGM
- Auckland University of Technology

Critical CVEs Reported

- VMware vRealize CVE-2023-34039
- Netgear - CVE-2023-41182 and CVE-2023-41183
- Apple CVE-2023-41061 and CVE-2023-41064

Interesting Highlight

- The FBI successfully dismantled the long-standing Qakbot (Qbot) malware operation known as "Duck Hunt," which has been active since at least 2008.
- Trojan (Spyware) was distributed through modified versions of the Telegram and Signal Android apps, which were made available on the Play Store.
- Microsoft issued a warning about a fresh phishing campaign being carried out by a group known as Storm-0324. This initial access broker group employs email-based infection vectors and typically sells access to ransomware operations such as FIN7.
- The International Criminal Court was targeted in a cyber-attack that has impacted its information systems.
- Greater Manchester Police confirmed that a data breach has occurred due to a suspected ransomware attack on Digital ID, a third-party identity card supplier.

2023 | Q3 Recommendations

- MFA is a necessary security measure for all user accounts, as passwords alone do not offer full protection anymore.
- Keep your Vulnerability Management Program current with all the available patches for the vulnerabilities that were identified in Q2.
- Users' behaviour should be measured and improved by a cybersecurity awareness program that can enable them to act as a defensive force for the organization, which should be invested in.
- Critical servers and other essential resources should be hardened and proper network segmentation should be enforced throughout the enterprise
- Breach & attack simulation activities, purple teaming engagement, and drills can help you discover and resolve gaps in security control's effectiveness, people and process in advance of threat actors
- To ensure that the security of data is not jeopardized by any gaps at any time, all organizations must review their third-party relationships and contracts on a regular basis.
- A plan for incident response and proactive monitoring of the system are essential to ensure effective detection and handling of security incidents.

cyber
plural
...focus on cybersecurity

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

Do you need help with any of the recommendations, feel free to consult and use our services.

Contact US

web

cyberplural.com

email

hello@cyberplural.com

blog

blog.cyberplural.com

social

cyberplural