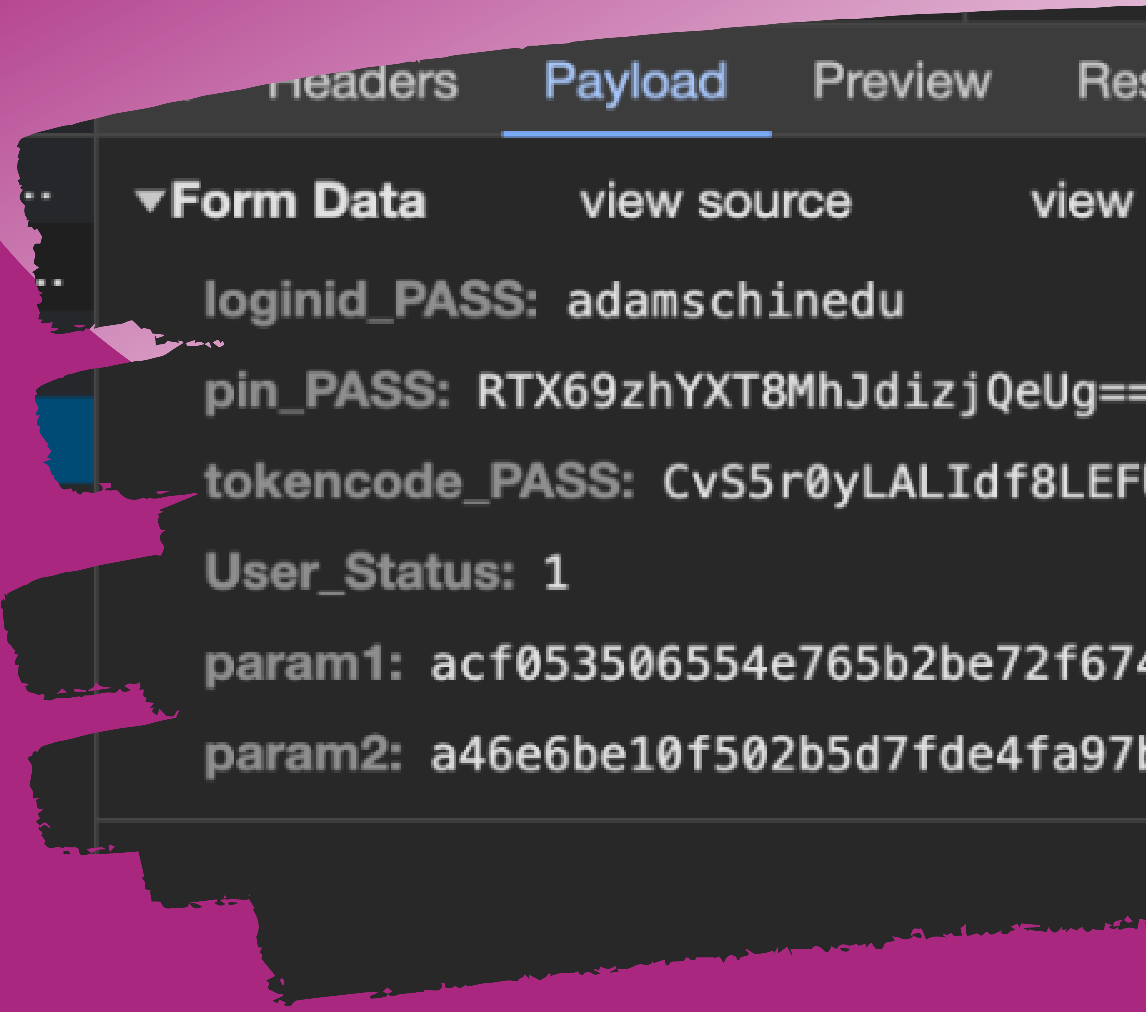
cyber plural
...focus on cybersecurity

2024 | Q1 Report

Cyber Incident Reports, Major CVEs & Threat Intel.



▾Form Data

loginid_PASS: adamschinedu

pin_PASS: RTX69zhYXT8MhJdizjQeUg==

tokencode_PASS: CvS5r0yLALIdf8LEF

User_Status: 1

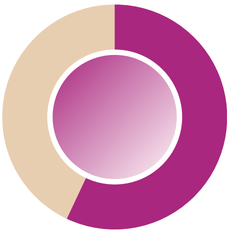
param1: acf053506554e765b2be72f67

param2: a46e6be10f502b5d7fde4fa97

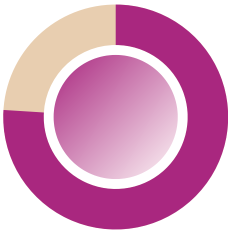
cyber plural
...focus on cybersecurity

cyberplural.com
hello@cyberplural.com

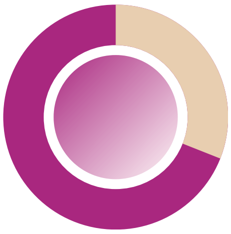
2024 | Q1 at a glance



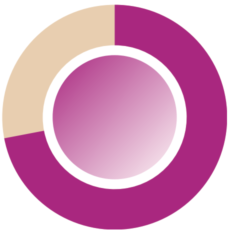
The problem of unreported cyber incidents persists into the first quarter of 2024 in Nigeria. Failure by organizations and businesses to disclose cyber incidents could erode the digital trust essential for society and create additional openings for threat actors to exploit vulnerabilities



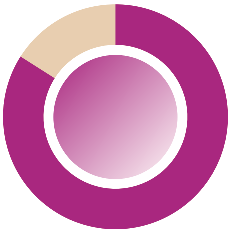
Throughout Q1 of 2024, the ALPHV, Rhysida, Lockbit and Medusa ransomware groups have continued to create significant disruptions across numerous organizations in both the United States and Europe. Their activities have been observed to have a widespread impact, posing a significant challenge to the cyber landscape in these regions.



The first quarter of 2024 saw a worrying trend in cyber threats linked to state-sponsored actors. Several high-profile incidents underscored this rise in activity. These events collectively paint a concerning picture of state-sponsored actors actively targeting various entities and employing diverse tactics.

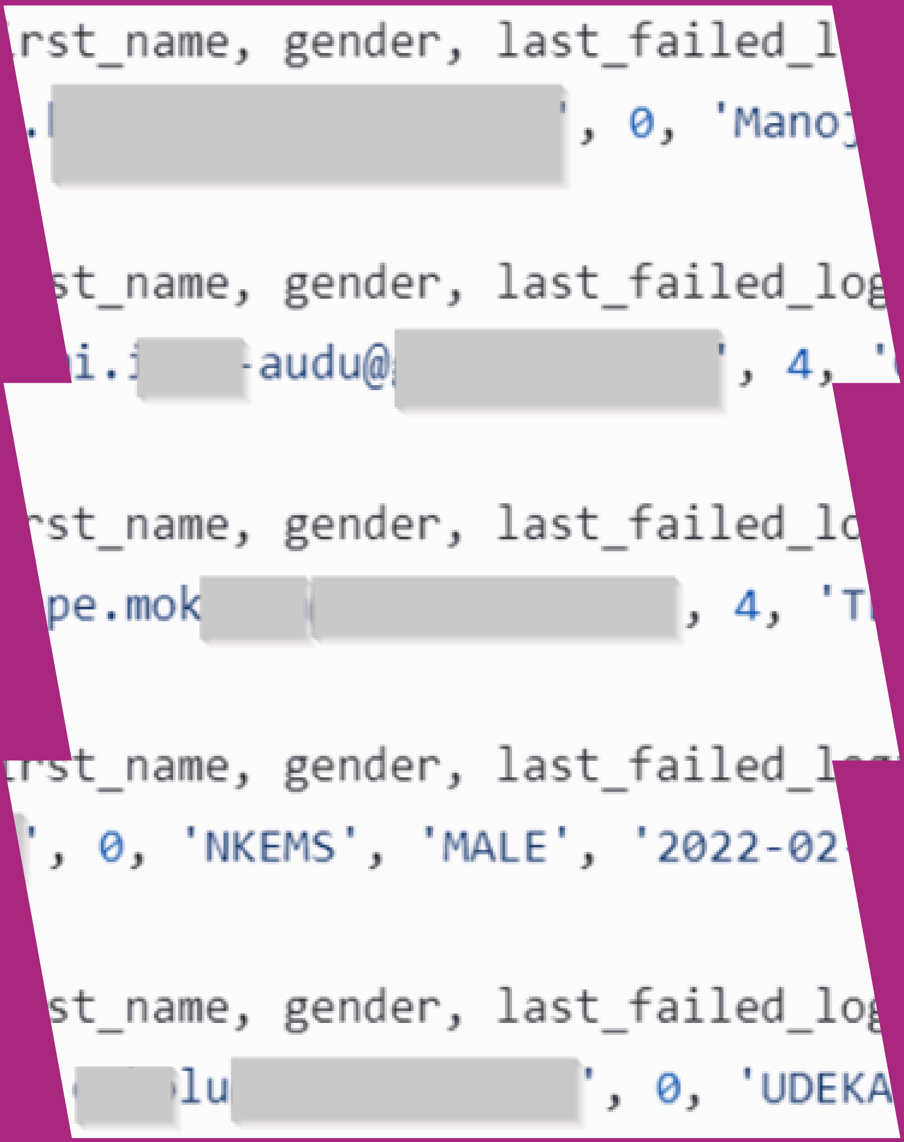


Proactive measures by our Threat Intelligence Ops stopped leaks of sensitive data from vital Nigerian systems. Their vigilance is key to creating a safer digital space, as the team continue to share intel with sectoral CERTs like ngCERT, Whitehat.NG, and CERRT.ng



Digital banking scams are on the rise. Banks are asking customers to update their National Identification Number (NIN) for security reasons, but scammers are taking advantage. They create fake bank websites that look real and trick people into giving up their personal information.

GitHub: The Silent Data Harvesting Tool and Its Impact on Data Privacy and Security



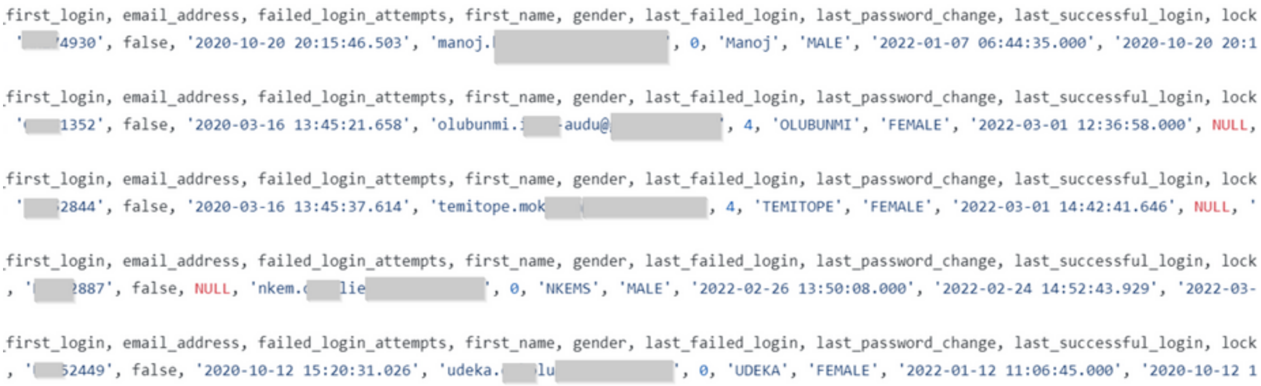
```
rst_name, gender, last_failed_l
.[redacted]', 0, 'Mano

st_name, gender, last_failed_log
i.[redacted]-audu@[redacted]', 4, '

rst_name, gender, last_failed_lo
pe.mok[redacted] [redacted], 4, 'T

rst_name, gender, last_failed_l
', 0, 'NKEMS', 'MALE', '2022-02

st_name, gender, last_failed_log
[redacted]lu[redacted]', 0, 'UDEKA
```

2024 | Q1 Report

cyberplural.com

GitHub: The Silent Data Harvesting Tool and Its Impact on Data Privacy and Security

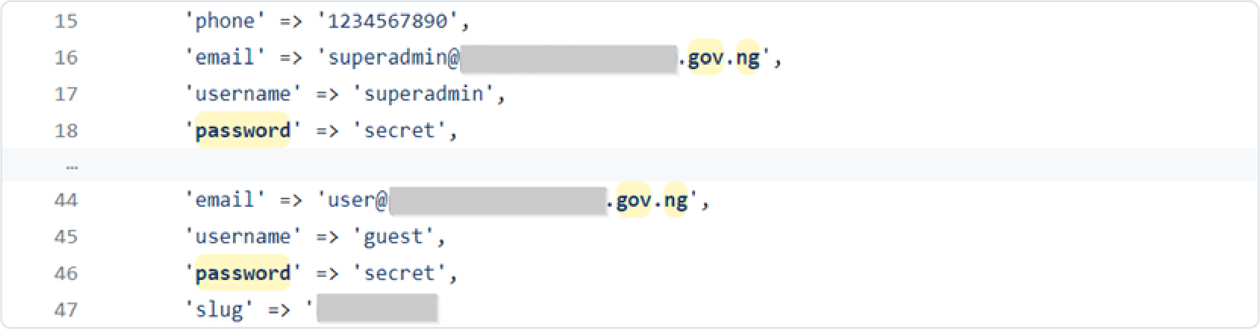
GitHub has long been known as a platform for collaborative software development and version control, but it has also quietly evolved into a significant source of data harvesting. The vast amount of code, documentation, and other content hosted on GitHub provides a rich trove of information that can be exploited for data mining and analysis. While this may have some benefits for developers and researchers, it also raises concerns about data privacy and security.



```
first_login, email_address, failed_login_attempts, first_name, gender, last_failed_login, last_password_change, last_successful_login, lock
 '[redacted]4930', false, '2020-10-20 20:15:46.503', 'manoj.[redacted]', 0, 'Manoj', 'MALE', '2022-01-07 06:44:35.000', '2020-10-20 20:1

first_login, email_address, failed_login_attempts, first_name, gender, last_failed_login, last_password_change, last_successful_login, lock
 '[redacted]1352', false, '2020-03-16 13:45:21.658', 'olubunmi.[redacted]audu@[redacted]', 4, 'OLUBUNMI', 'FEMALE', '2022-03-01 12:36:58.000', NULL,

first_login, email_address, failed_login_attempts, first_name, gender, last_failed_login, last_password_change, last_successful_login, lock
 '[redacted]2844', false, '2020-03-16 13:45:37.614', 'temitope.mok[redacted], 4, 'TEMITOPE', 'FEMALE', '2022-03-01 14:42:41.646', NULL, '

first_login, email_address, failed_login_attempts, first_name, gender, last_failed_login, last_password_change, last_successful_login, lock
, '[redacted]2887', false, NULL, 'nkem.[redacted]lie[redacted]', 0, 'NKEMS', 'MALE', '2022-02-26 13:50:08.000', '2022-02-24 14:52:43.929', '2022-03-

first_login, email_address, failed_login_attempts, first_name, gender, last_failed_login, last_password_change, last_successful_login, lock
, '[redacted]52449', false, '2020-10-12 15:20:31.026', 'udeka.[redacted]lu[redacted]', 0, 'UDEKA', 'FEMALE', '2022-01-12 11:06:45.000', '2020-10-12 1
```

Fig 1. Personal Information of Users found in applications logs.

One of the primary ways in which GitHub serves as a data harvesting tool is through the collection of public repositories. These repositories often contain sensitive information such as API keys, credentials, and other proprietary data that can be inadvertently exposed. Additionally, the commit history of repositories can reveal patterns of development, code changes, and potentially sensitive information about the development process.

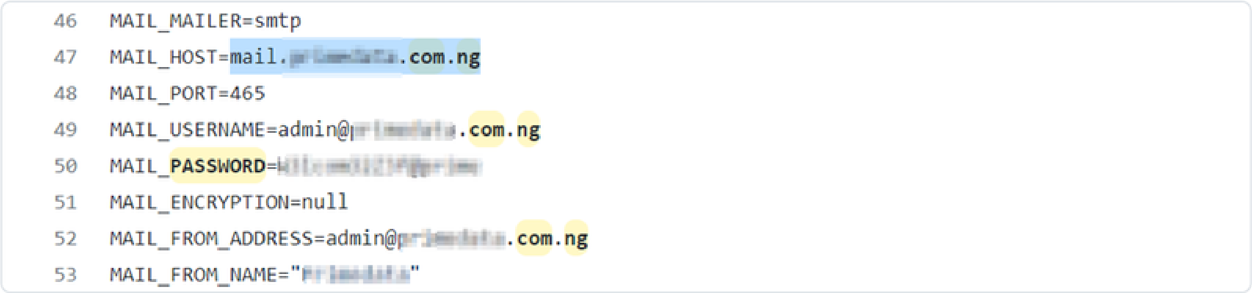


```
        'phone' => '1234567890',
        'email' => 'superadmin@[redacted].gov.ng',
        'username' => 'superadmin',
        'password' => 'secret',
...
        'email' => 'user@[redacted].gov.ng',
        'username' => 'guest',
        'password' => 'secret',
        'slug' => '[redacted]
```

Fig 2. Portal Administrative Dashboard credential found

Furthermore, GitHub's web interface and API make it easy to search for and access large amounts of code and other content, allowing for the extraction of data on a massive scale. This data can then be used for various purposes, including profiling developers, identifying trends in software development, and even extracting sensitive information.

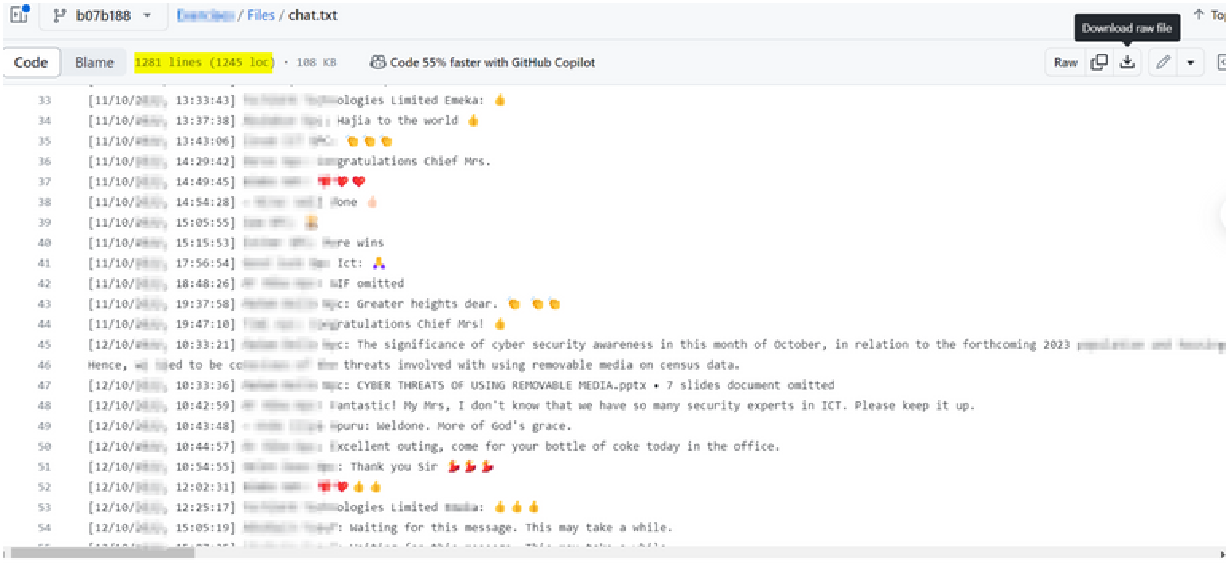
The impact of GitHub's data harvesting on data privacy and security is significant. Developers and organizations may unknowingly expose sensitive information through their public repositories, leading to potential security breaches and data leaks. Additionally, the use of harvested data for profiling and analysis raises concerns about privacy and the potential misuse of information.



```
MAIL_MAILER=smtp
MAIL_HOST=mail.[redacted].com.ng
MAIL_PORT=465
MAIL_USERNAME=admin@[redacted].com.ng
MAIL_PASSWORD=[redacted]
MAIL_ENCRYPTION=null
MAIL_FROM_ADDRESS=admin@[redacted].com.ng
MAIL_FROM_NAME="[redacted]"
```

Fig 3. Email credential found in the public repo.

In a recent finding, our team discovered a chat log from an organization's WhatsApp group that was uploaded to a public repository by one of their former interns. This mistake led to the internal communication of the group becoming public, potentially exposing sensitive information and conversations. This incident highlights the real-world impact of data harvesting on GitHub and underscores the urgent need for improved data privacy and security measures.



b07b188
[redacted] / Files / chat.txt
Code
Blame
1281 lines (1245 loc) · 108 KB
Code 55% faster with GitHub Copilot
Download raw file
Raw
↑ To

```
[11/10/[redacted], 13:33:43] [redacted]ologies Limited Emeka: 👍
[11/10/[redacted], 13:37:38] [redacted] Hajia to the world 👍
[11/10/[redacted], 13:43:06] [redacted] 👏👏👏
[11/10/[redacted], 14:29:42] [redacted]gratulations Chief Mrs.
[11/10/[redacted], 14:49:45] [redacted] ❤️❤️❤️
[11/10/[redacted], 14:54:28] [redacted] one 👍
[11/10/[redacted], 15:05:55] [redacted]
[11/10/[redacted], 15:15:53] [redacted] re wins
[11/10/[redacted], 17:56:54] [redacted] Ict: 🙏
[11/10/[redacted], 18:48:26] [redacted] IF omitted
[11/10/[redacted], 19:37:58] [redacted]c: Greater heights dear. 👏 👏👏
[11/10/[redacted], 19:47:10] [redacted]gratulations Chief Mrs! 👍
[12/10/[redacted], 10:33:21] [redacted]c: The significance of cyber security awareness in this month of October, in relation to the forthcoming 2023 [redacted]
Hence, [redacted]ed to be co[redacted] threats involved with using removable media on census data.
[12/10/[redacted], 10:33:36] [redacted]c: CYBER THREATS OF USING REMOVABLE MEDIA.pptx • 7 slides document omitted
[12/10/[redacted], 10:42:59] [redacted] antastic! My Mrs, I don't know that we have so many security experts in ICT. Please keep it up.
[12/10/[redacted], 10:43:48] [redacted]puru: Weldone. More of God's grace.
[12/10/[redacted], 10:44:57] [redacted] xcellent outing, come for your bottle of coke today in the office.
[12/10/[redacted], 10:54:55] [redacted]: Thank you Sir 💃💃💃
[12/10/[redacted], 12:02:31] [redacted] ❤️❤️👍👍
[12/10/[redacted], 12:25:17] [redacted]ologies Limited [redacted]: 👍👍👍
[12/10/[redacted], 15:05:19] [redacted]: Waiting for this message. This may take a while.
```

Fig 4. WhatsApp Chat Log of an organization found in a public repository of former Intern

To mitigate the impact of GitHub's data harvesting on data privacy and security, developers and organizations should be vigilant about the content they publish on GitHub. This includes regularly auditing repositories for sensitive information, using tools to scan for potential vulnerabilities, and implementing access controls to limit exposure of sensitive data.

In conclusion, while GitHub has become a valuable resource for collaborative software development, its role as a silent data harvesting tool raises important concerns about data privacy and security. Developers and organizations must be proactive in protecting sensitive information and mitigating the risks associated with data harvesting on GitHub.

January 2024

Organizations Breached / Experienced Ransomware Attack

- EquiLend, a Wall Street stock-lending firm.
- Ukrainian Online Bank Monobank
- Foxsemicon Integrated Technology Inc
- National Bank of Angola
- Water for People - nonprofit organization
- US Largest mortgage lender LoneDepot
- SEC official X account hijack
- Multiple Ukrainian state-owned entities, including Naftogaz, the Postal Service, and Railway Services.

Critical CVEs Reported

- VMware - CVE-2023-34063
- Citrix addressing CVE-2023-6549,
- Atlassian - CVE-2023-22527
- GitLab - fixes CVE-2023-7028

Interesting Highlight

- Researchers found that the threat group UTA0178, associated with China, has been actively exploiting two zero-day vulnerabilities (CVE-2023-46805 and CVE-2024-21887) in Ivanti Connect Secure & Ivanti Policy Secure gateways, allowing remote authentication bypass and code execution
- Microsoft detected an attack by the Russian state-sponsored actor Midnight Blizzard (Nobelium), who used a password spray attack to access a small number of corporate email accounts, including those of senior leadership, cybersecurity, and legal personnel.
- The LockBit ransomware group has taken credit for a cyber-attack targeting Foxsemicon Integrated Technology Inc. (FITI), a major semiconductor manufacturer in Taiwan.
- The National Bank of Angola confirmed a cyber-attack that caused a minimal impact on its infrastructure and data. Although no specific group has claimed responsibility, researchers discovered that access to the bank's systems was advertised for sale on a cybercriminal forum in 2022.

cyber plural
...focus on cybersecurity

Cyber Security Resilience in Nigeria: A Call to Action for Incident Reporting and Collaboration

2024 | Q1 Report

cyberplural.com

Cyber Security Resilience in Nigeria: A Call to Action

In the era of digital interconnectedness, Nigeria's digital landscape is witnessing rapid growth, accompanied by a surge in cyber security threats. As the most populous nation in Africa with over 122 million internet users, Nigeria stands at a critical juncture where the adoption of technology is reshaping industries and government operations. However, the prevalence of cyber security lapses poses a significant risk to the nation's digital infrastructure, necessitating a multifaceted approach to fortify its cyber defenses.

Navigating Cyber Security Challenges

Cyber security lapses in Nigeria are often attributed to vulnerabilities stemming from outdated software, social engineering tactics, and inadequate security practices. The absence of a robust cyber security culture further compounds these risks, leaving organizations vulnerable to a myriad of cyber threats such as data breaches, malware attacks, phishing scams, denial-of-service incidents, and data exfiltration.

Real-World Impacts

Recent security incidents in Nigeria underscore the severity of cyber security breaches, leading to financial losses, reputational damage, and diminished trust in the digital ecosystem. Reports reveal that a significant percentage of Nigerian organizations have fallen victim to cyber-attacks, with ransomware groups like Mallox and ALPHV targeting both private and government entities across various sectors.

Strengthening Incident Reporting

Timely incident reporting is crucial in mitigating cyber security risks and minimizing the impact of potential breaches. Establishing streamlined channels for reporting security incidents and vulnerabilities can enable swift response and remediation efforts, safeguarding critical assets and information.

Facilitating Sectoral CERT Collaboration

Collaboration with sectoral Computer Emergency Response Teams (CERTs) plays a pivotal role in enhancing cyber resilience across industries. By fostering information sharing, best practices dissemination, and coordinated response strategies, sectoral CERTs can bolster the collective defense posture of organizations within specific sectors by working with national CERT (ngCERT).

Embracing MSSP Partnerships

Partnering with Managed Security Service Providers (MSSPs) offers organizations access to specialized expertise, advanced threat intelligence, and round-the-clock monitoring capabilities. By leveraging MSSP services, businesses can augment their internal security operations, detect emerging threats proactively, and respond to incidents effectively, thereby enhancing their overall cyber security posture.

Driving a Culture of Cyber Resilience

Promoting a culture of cyber resilience requires a concerted effort from all stakeholders, including government agencies, private enterprises, and individual users. Investing in cyber security awareness programs, training initiatives, and incident response exercises can empower organizations and individuals to recognize and mitigate cyber threats effectively.

Charting the Path Forward

As Nigeria continues its digital transformation journey, prioritizing incident reporting mechanisms, fostering collaboration with sectoral CERTs, and forging partnerships with MSSPs are essential steps in safeguarding the nation’s digital assets. By embracing a proactive approach to cyber security, Nigeria can navigate the evolving threat landscape with confidence and resilience.

Organizations must prioritize cyber security and adopt proactive measures to safeguard their digital assets. By partnering with *CyberPlural MSSP*, businesses can strengthen their cyber defenses, enhance their incident response capabilities, and position themselves for a secure and resilient future in the face of evolving cyber threats.

cyber plural
...focus on cybersecurity

February 2024

Organizations Breached / Experienced Ransomware Attack

- American Prince George's County Public Schools (PGCPS)
- Truck and Trailer Rental company U-Haul
- Alleged Compromised of 600K French Social Security accounts (CAF)
- US IT service firm Technica
- Italian cloud service provider CloudFire
- AnyDesk Software GmbH
- Ukrainska Pravda

Critical CVEs Reported

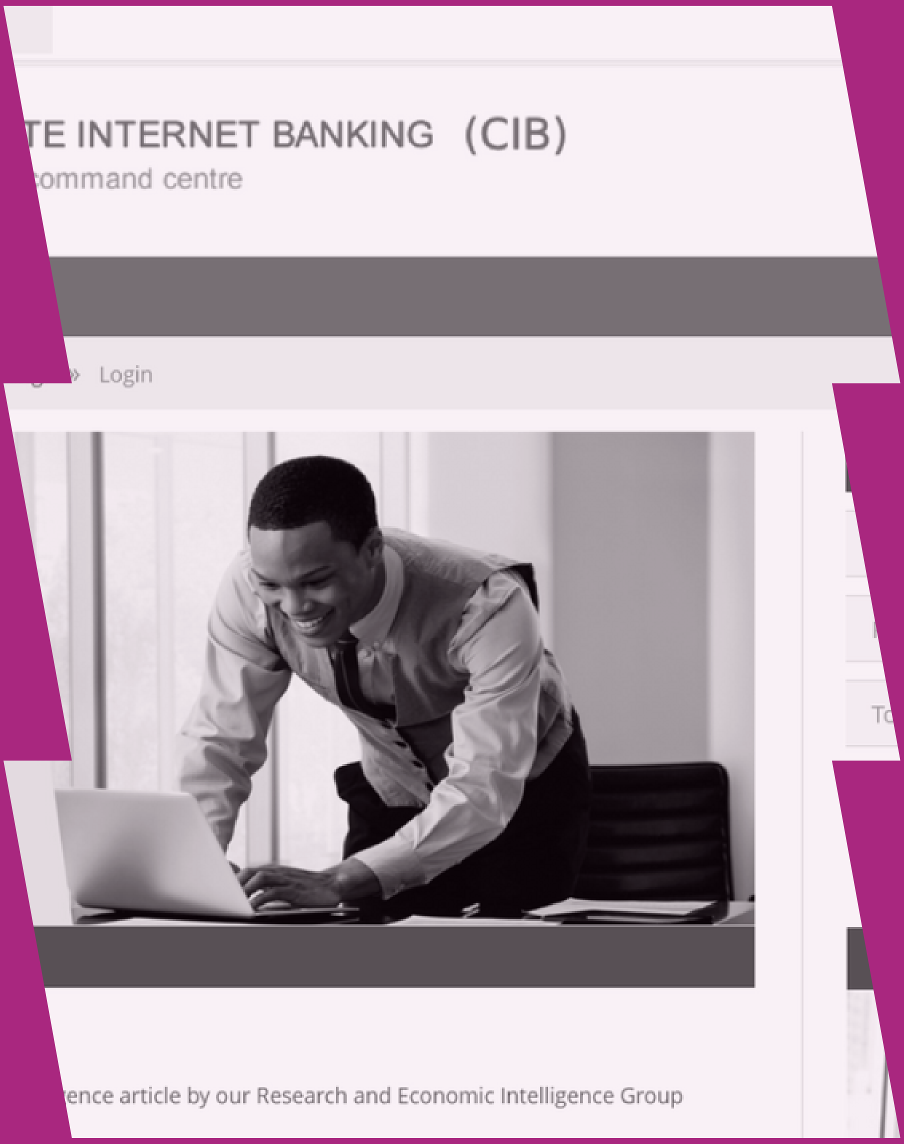
- ConnectWise - CVE-2024-1709
- Mozilla Firefox
- Joomla - CVE-2024-21725
- Microsoft's Patch Tuesday - CVE-2024-21412 and CVE-2024-21351

Interesting Highlight

- The financially driven advanced group DarkCasino has been actively leveraging the Microsoft Defender SmartScreen bypass vulnerability (CVE-2024-21412) in its targeted campaigns against financial market traders.
- The release of confidential documents from Anxun Information Technology Co., Ltd. (i-SOON), a Chinese IT and cybersecurity company, revealed insights into China's state-sponsored cyber espionage activities.
- Dutch intelligence agencies uncovered a cyber espionage campaign carried out by Chinese state-backed hackers targeting the Dutch Defense Ministry. Exploiting a Fortinet vulnerability (CVE-2022-42475), the attackers sought to breach the unclassified military research network.
- In a coordinated international law enforcement effort named 'Operation Cronos', the LockBit ransomware group, which has been responsible for widespread attacks since late 2019, was dismantled by the UK's National Crime Agency, the FBI, and Europol.
- The Philippines has reported the prevention of an attempted breach into the email systems of the country's president and government.

cyber plural
...focus on cybersecurity

Stay Secure, Stay Informed: A Look into Deceptive Practices Targeting Bank Customers.

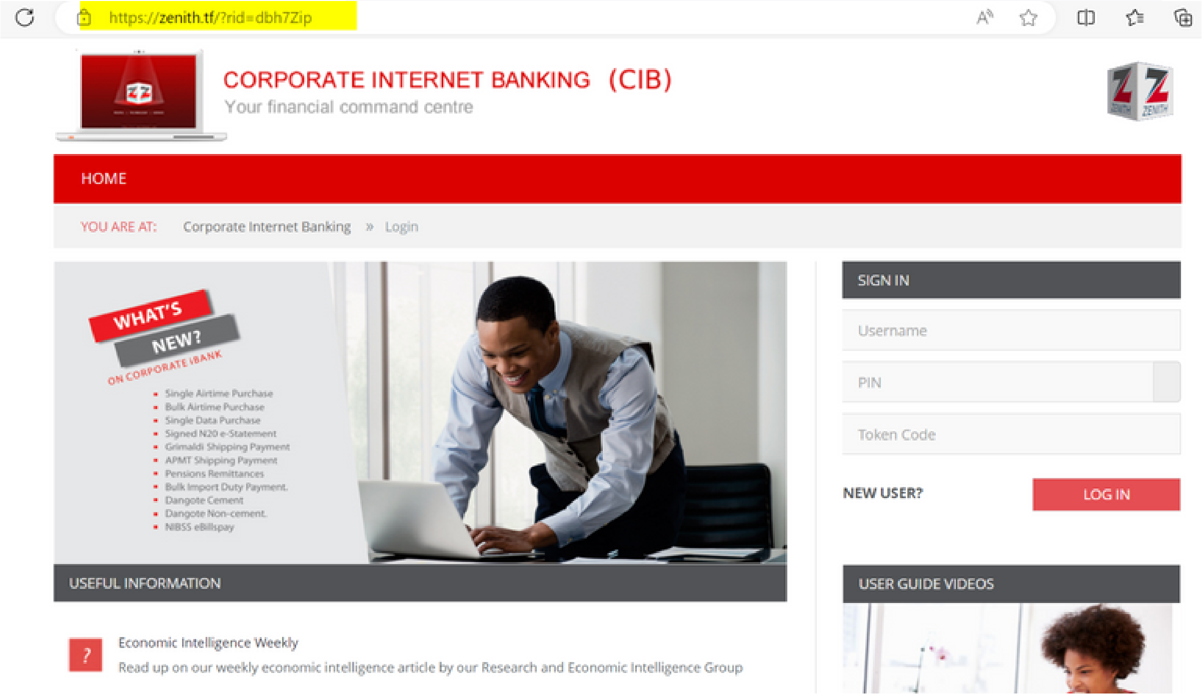

TE INTERNET BANKING (CIB)
ommand centre
» Login
To
ence article by our Research and Economic Intelligence Group

A Look into Deceptive Practices Targeting Bank Customers

In the current landscape of digital banking, a concerning trend has emerged that puts account holders at risk of falling victim to sophisticated cyber scams. Banks are now urging their customers to update their account information by submitting their National Identification Number (NIN), a move aimed at enhancing security measures. However, this well-intentioned process has inadvertently opened the door for threat actors specializing in Business Email Compromise (BEC) and phishing scams to exploit unsuspecting users.

Phishing Meets Timing

These malicious actors have been quick to capitalize on the situation by setting up fake or replica versions of corporate banking websites to deceive individuals into divulging their personally identifiable information. By mimicking the legitimate interfaces of banks, these fraudulent websites trick users into entering sensitive data, such as login credentials, token codes, and NINs, under the guise of security compliance.



https://zenith.tf/?rid=dbh7Zip

CORPORATE INTERNET BANKING (CIB)
Your financial command centre

YOU AREAT: Corporate Internet Banking » Login

WHAT'S NEW? ON CORPORATE IBANK

- Single Airtime Purchase
- Bulk Airtime Purchase
- Single Data Purchase
- Signed N20 e-Statement
- Grimaldi Shipping Payment
- APMT Shipping Payment
- Pensions Remittances
- Bulk Import Duty Payment.
- Dangote Cement
- Dangote Non-cement.
- NIBSS eBillspay

USEFUL INFORMATION

Economic Intelligence Weekly
Read up on our weekly economic intelligence article by our Research and Economic Intelligence Group

SIGN IN

Username

PIN

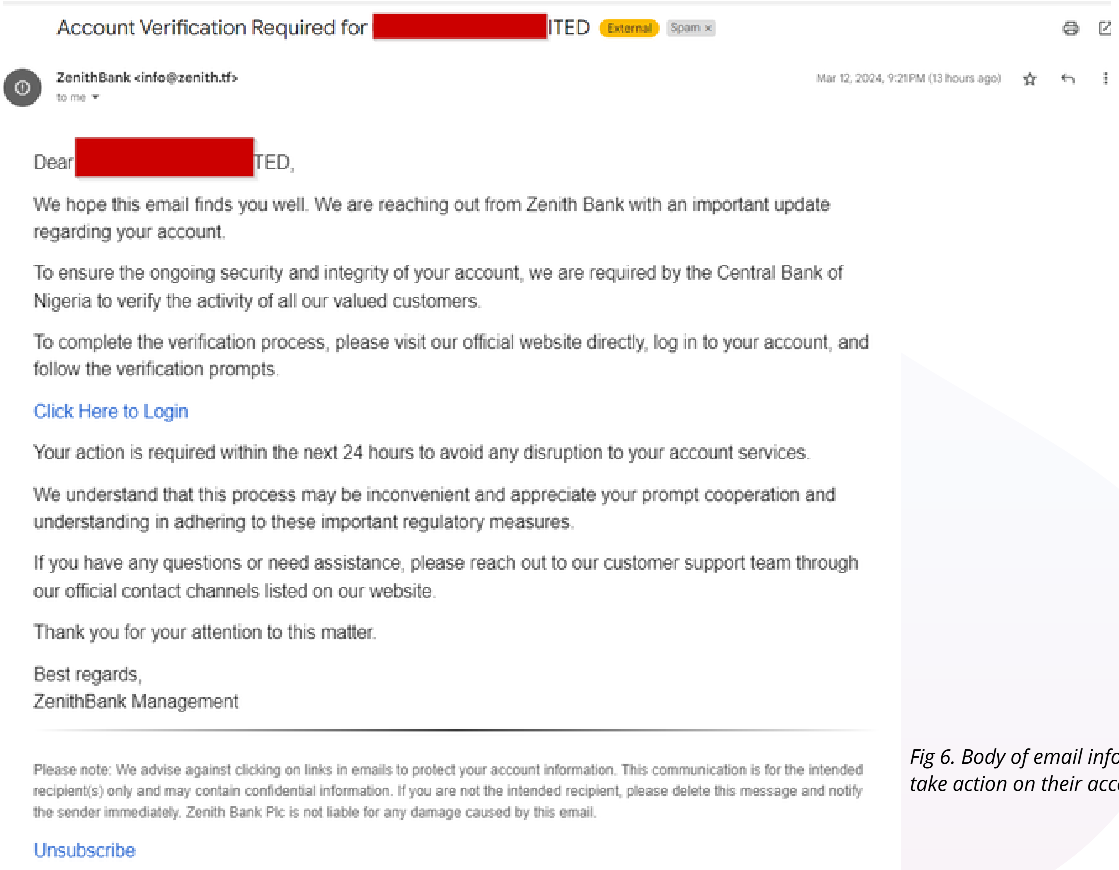
Token Code

NEW USER?

Fig 5. Link from the Phishing Email sent to corporate account owners.

A Look into Deceptive Practices Targeting Bank Customers

Recently, our vigilant team stumbled upon a server that had been specifically configured to facilitate these deceptive practices. Recognizing the imminent threat posed by these fraudulent activities, we undertook a thorough investigation to uncover the indicators of compromise (IoC) associated with such malicious endeavours.



Account Verification Required for [redacted]ITED

ZenithBank <info@zenith.tf>
to me

Mar 12, 2024, 9:21 PM (13 hours ago)

Dear [redacted]TED,

We hope this email finds you well. We are reaching out from Zenith Bank with an important update regarding your account.

To ensure the ongoing security and integrity of your account, we are required by the Central Bank of Nigeria to verify the activity of all our valued customers.

To complete the verification process, please visit our official website directly, log in to your account, and follow the verification prompts.

Click Here to Login

Your action is required within the next 24 hours to avoid any disruption to your account services.

We understand that this process may be inconvenient and appreciate your prompt cooperation and understanding in adhering to these important regulatory measures.

If you have any questions or need assistance, please reach out to our customer support team through our official contact channels listed on our website.

Thank you for your attention to this matter.

Best regards,
ZenithBank Management

Please note: We advise against clicking on links in emails to protect your account information. This communication is for the intended recipient(s) only and may contain confidential information. If you are not the intended recipient, please delete this message and notify the sender immediately. Zenith Bank Plc is not liable for any damage caused by this email.

Unsubscribe

Fig 6. Body of email informing users to take action on their account update

As responsible digital citizens, all bank customers must remain vigilant and cautious when navigating online banking platforms. To safeguard against falling prey to these nefarious schemes, users should exercise due diligence by verifying the authenticity of banking websites, scrutinizing email communications for signs of phishing attempts, and refraining from sharing sensitive information unless certain of the legitimacy of the request.

By staying informed and proactive in our cybersecurity practices, we can collectively combat the insidious efforts of threat actors seeking to exploit unsuspecting individuals. Remember, when it comes to safeguarding your personal information in the digital realm, vigilance is key.

Technical Analysis of the Phishing Page

The phishing page seems to be an exact copy of the original login page, down to the customer support widget at the bottom.

But they only seem like an exact copy at first glance, the difference between the phishing page and the actual login page, purely by a matter of the goal the attackers are trying to achieve, will always be the form.

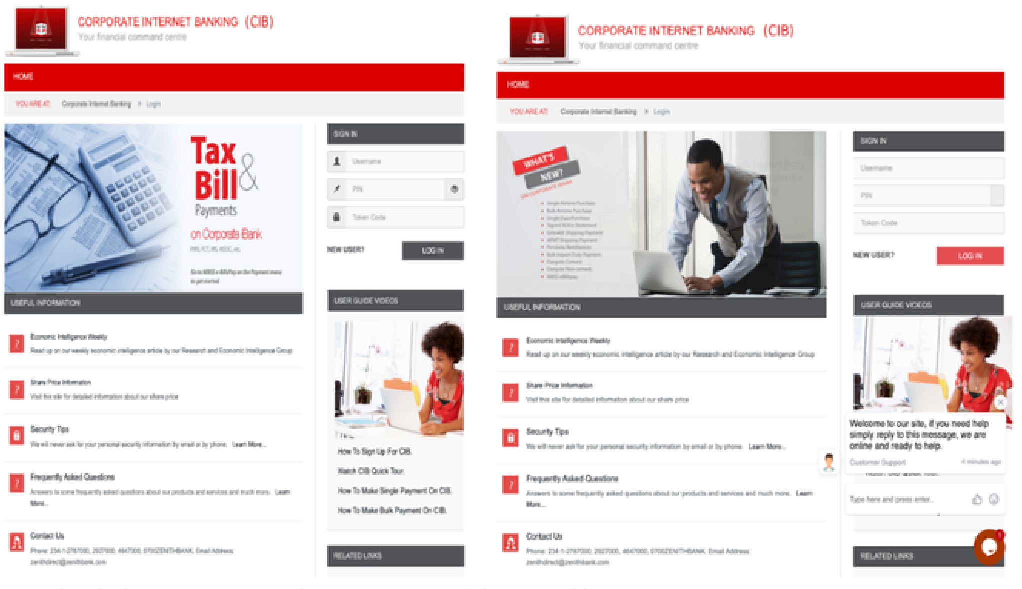
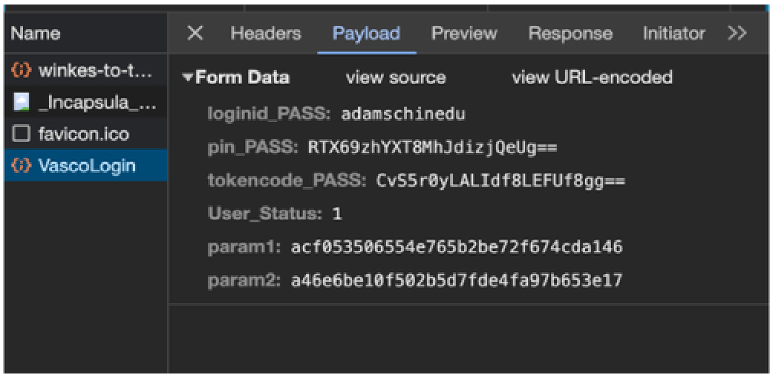

CORPORATE INTERNET BANKING (CIB)
Your financial command centre
HOME
SIGN IN
Username
PIN
Token Code
NEW USER?
LOG IN
Tax & Bill Payments on Corporate Bank
USEFUL INFORMATION
USER GUIDE VIDEOS
Economic Intelligence Weekly
Share Price Information
Security Tips
Frequently Asked Questions
Contact Us
How To Sign Up For CIB.
Watch CIB Quick Tour.
How To Make Single Payment On CIB.
How To Make Bulk Payment On CIB.
RELATED LINKS
CORPORATE INTERNET BANKING (CIB)
Your financial command centre
HOME
WHAT'S NEW?
SIGN IN
Username
PIN
Token Code
NEW USER?
LOG IN
USEFUL INFORMATION
USER GUIDE VIDEOS
Economic Intelligence Weekly
Share Price Information
Security Tips
Frequently Asked Questions
Contact Us
Welcome to our site, if you need help simply reply to this message, we are online and ready to help.
Customer Support
Type here and press enter..
RELATED LINKS

Fig 7.The phishing page seems to be an exact copy of the original login page

Visually, the only difference is the icons but this indicates that the code for the form itself has been altered. To test how the two forms work, we'll attempt logging in using an alter ego. "***Adams Chinedu"***

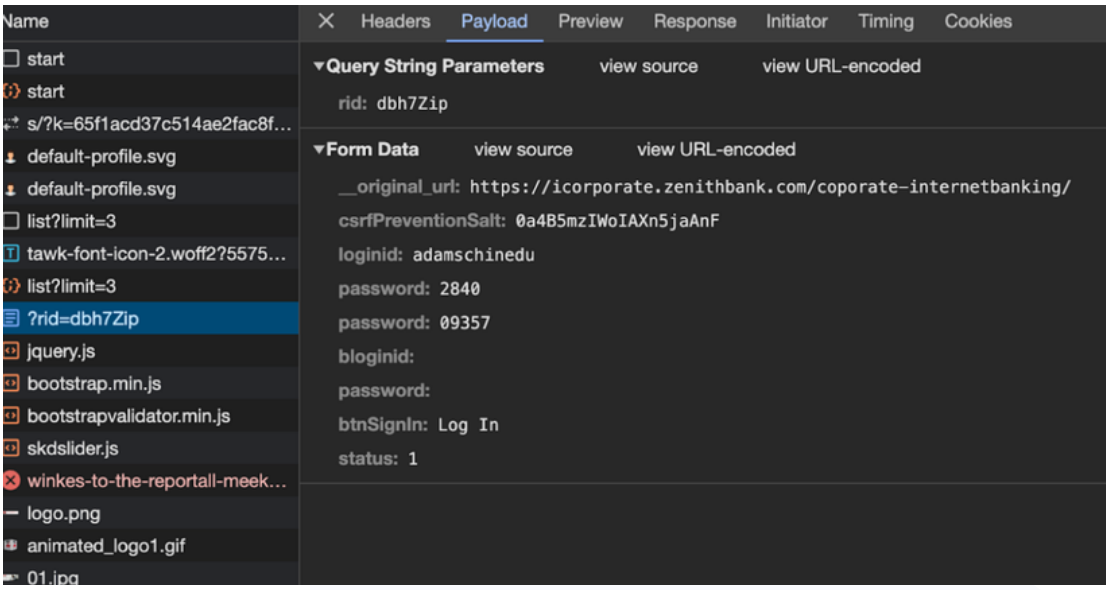
After "Logging in", the form will send the data to the server and this is how ***we get the endpoint where all the data is sent.***



```
▾Form Data        view source        view URL-encoded
    loginid_PASS: adamschinedu
    pin_PASS: RTX69zhYXT8MhJdizjQeUg==
    tokencode_PASS: CvS5r0yLALIdf8LEFUf8gg==
    User_Status: 1
    param1: acf053506554e765b2be72f674cda146
    param2: a46e6be10f502b5d7fde4fa97b653e17
```

Fig 8. Legitimate Zenith Bank Corporate Banking Login Form

The legitimate Zenith Bank form passes the user, then ***the pin and token as encoded values*** along with what I suspect to be ***csrf hashes.***



```
start
start
s/?k=65f1acd37c514ae2fac8f...
default-profile.svg
default-profile.svg
list?limit=3
tawk-font-icon-2.woff2?5575...
list?limit=3
?rid=dbh7Zip
jquery.js
bootstrap.min.js
bootstrapvalidator.min.js
skdslider.js
winkes-to-the-reportall-meek...
logo.png
animated_logo1.gif
01.jpg
```

```
▾Query String Parameters
  rid: dbh7Zip
▾Form Data
  __original_url: https://icorporate.zenithbank.com/coporate-internetbanking/
  csrfPreventionSalt: 0a4B5mzIWoIAXn5jaAnF
  loginid: adamschinedu
  password: 2840
  password: 09357
  bloginid:
  password:
  btnSignIn: Log In
  status: 1
```

Fig 9. Phishing Page Form on – https[:]//zenith[.]tf/?rid=dbh7Zip

The phishing page on the other hand takes the original url of the page it is pretending to be (probably to use as a target url when the details are entered)

The existence of this variable also ***alludes to this page being set up by a tool***, since if it were a one-off, the developer would have hardcoded a value in the code instead.

The request also passes on the **rid query parameter** that can be seen in the **URL bar**. This probably is an identifier for the target that received the phishing link.

Indicator of Compromise

https[:]//zenith[.]tf/?rid=dbh7Zip
188.114.96[.]2
info@zenith[.]tf
https[:]//zenithbankplc[.]zom.ng
188.114.97[.]0, 188.114.96[.]0, 2a06:98c1[:]3120::c
https[:]//zenith[.]com.pt/?keyname=ewCgchx
https[:]//secure[.]zenith.it[.]com/coporate-internetbanking/RVFFA5W
secure[.]zenith, it[.]com
104.21.43[.]207, zenith-support@server7-nigeria[.]xyz
server7-nigeria[.]xyz, https[:]//zenith[.]com[.]pt/?keyname=9JCqtKX
https[:]//z[.]plc[.]pm/?keyname=NzYuQkM, https[:]//zenith[.]tf/?keyname=bqRqrIw

March 2024

Organizations Breached / Experienced Ransomware Attack

- UnitedHealth Group
- Houser LLP Data Breach
- Duvel Moortgat Brewery
- Japanese Tech Company Fujitsu
- CISA Breach - Exploitation of Ivanti
- Paysign Investigating data breach
- Walmart's Spark
- Swiss Tech and IT vendor Xplain
- France's Unemployment Agency

Critical CVEs Reported

- VMware (CVE-2024-22252 – CVE-2024-22255
- Cisco - CVE-2024-20337
- Adobe - CVE-2024-20756, CVE-2024-20755, and CVE-2024-20752

Interesting Highlight

- Threat actor groups, including Black Basta and Bl00dy Ransomware gangs, have been exploiting major vulnerabilities in ConnectWise ScreenConnect software, identified as CVE-2024-1708, 2024-1709..
- The French unemployment agency has revealed that data from 43 million individuals has been exposed as a result of a cyber-attack on the agency.
- Nemesis Market, a major darknet marketplace for narcotics, weapons, and stolen data, was seized in Operation Dark Hunt. Advanced digital forensics techniques were employed in a collaborative law enforcement effort to execute the takedown.
- CISA alerted of the exploitation of known vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure gateways. These vulnerabilities (CVE-2023-46805, 2024-21887, and 2024-21893) could enable threat actors to bypass authentication, create malicious requests, and execute unauthorized commands with elevated privileges

2024 | Q1 Recommendations

- Breach & attack simulation activities, purple teaming engagement, and drills can help you discover and resolve gaps in security control’s effectiveness, people and process in advance of threat actors
- Keep your Vulnerability Management Program current with all the available patches for the vulnerabilities that was identified in Q4 of 2023.
- To ensure that the security of data is not jeopardized by any gaps at any time, all organizations must review their third-party relationships and contracts on a regular basis.
- Critical servers and other essential resources should be hardened and proper network segmentation should be enforced throughout the enterprise
- MFA is a necessary security measure for all user accounts, as passwords alone do not offer full protection anymore.
- Users’ behaviour should be measured and improved by a cybersecurity awareness program that can enable them to act as a defensive force for the organization, which should be invested in.
- A plan for incident response and proactive monitoring of the system are essential to ensure effective detection and handling of security incidents.

cyber plural
...focus on cybersecurity

Don't let cybersecurity slow you down. We build and implement resilient cyber plans so you can focus on what matters most - growing your business.

Need guidance on these security improvements? Our team has the expertise to consult and implement the best plan for you

Contact US

web

cyberplural.com

email

hello@cyberplural.com

blog

blog.cyberplural.com

social

cyberplural