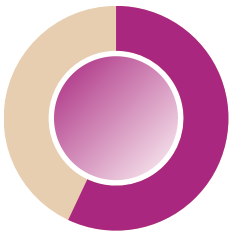


2023 | Q2 Report

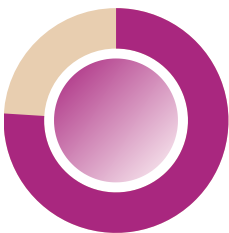
Cyber Incident Reports, Major CVEs &
Threat Intel.



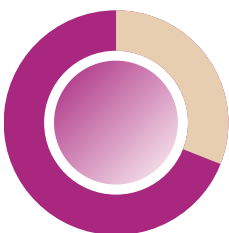
2023 | Q2 at a glance



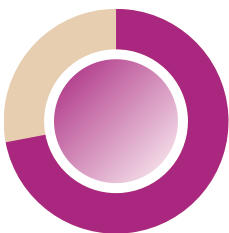
Multiple cyber incidents have gone unreported in Q2 of 2023 in Nigeria. We observed that if organizations/businesses continue this way, it might end up eroding the digital trust on which society relies and give more advantages to threat actors.



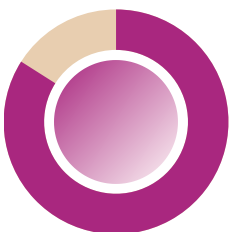
CVEs from 2021, 2022 and Q1 and Q2 of 2023 are still being exploited. Government, schools, and businesses were targets of multiple breaches and ransomware attacks in Q2. The focus is on supply chain attacks, data espionage, ransomware, and hacktivism.



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

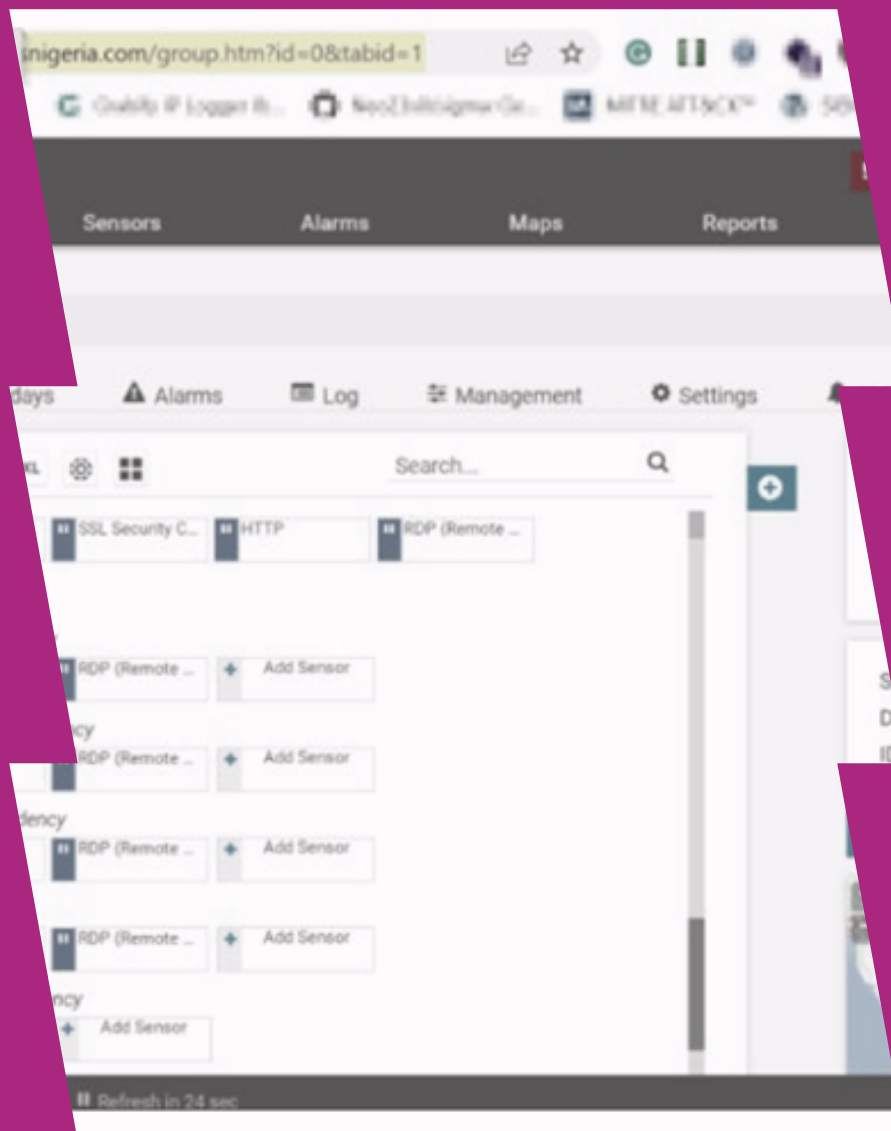


Threat Intelligence Ops reveals misconfigurations leading to sensitive data leakage on critical systems and facilities in Nigeria. Our reports have helped block these leakages and fix these vulnerabilities to ensure a safer cyberspace.



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

Threat Actor Groups Targeting Vulnerabilities in Routers - Connecting it with PRTG



Threat Actor Groups Targeting Vulnerabilities in Routers - Connecting it with PRTG

A recent [advisory](#) from CISA talked about threat actor groups targeting vulnerabilities in routers, especially those of Cisco-made. Our CTI team decided to take a deeper look at this advisory and how that can be applicable to our space here in Nigeria, and others in the African Region.

At first, the advisory pointed out how the adversary use two different attacks to target Cisco routers. One is the exploitation of the Simple Network Monitoring Protocol (SNMP) - a tool that allows network administrators to monitor and configure network devices remotely. The tools can be abused to steal sensitive network information and subsequently penetrate a network.

Over time certain misconfiguration and availability of such software that can leverage this protocol (SNMP) to scan the entire network, meaning that poor configuration such as using default or easy-to-guess community strings, can make a network susceptible to attacks.

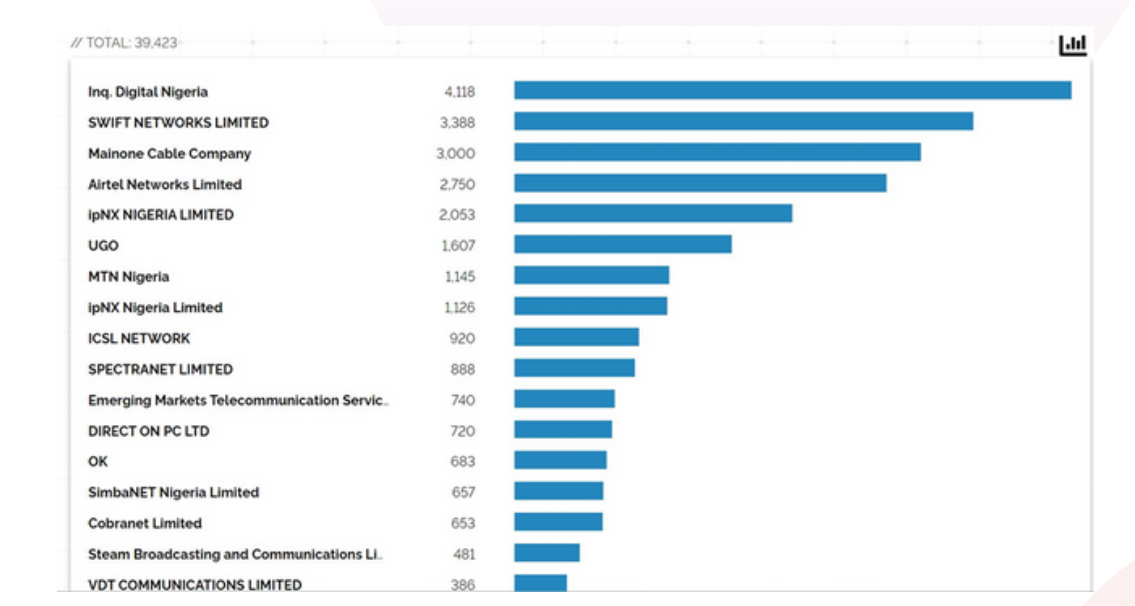
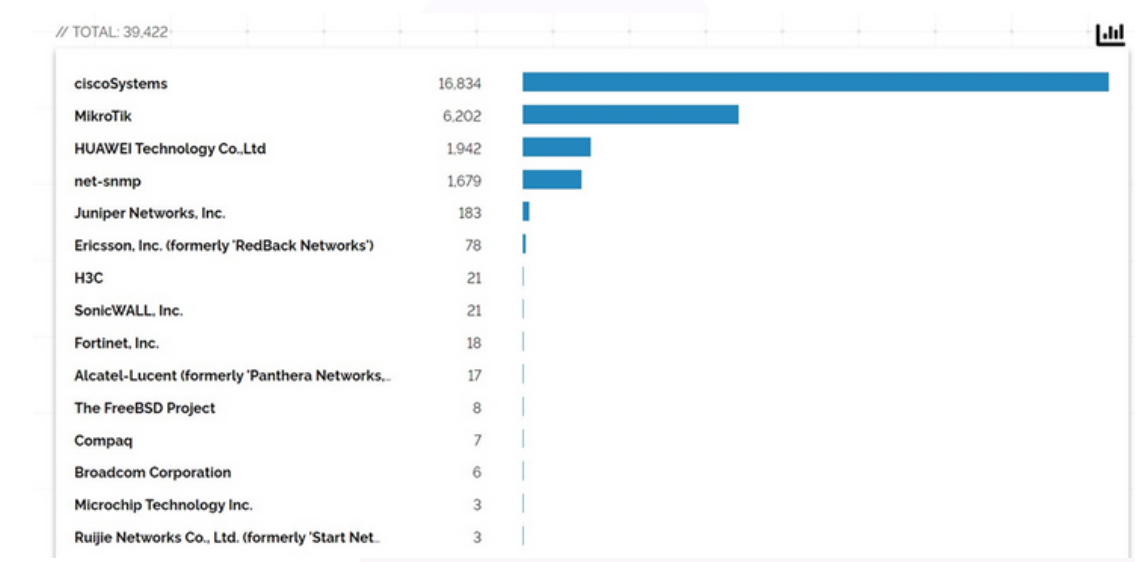
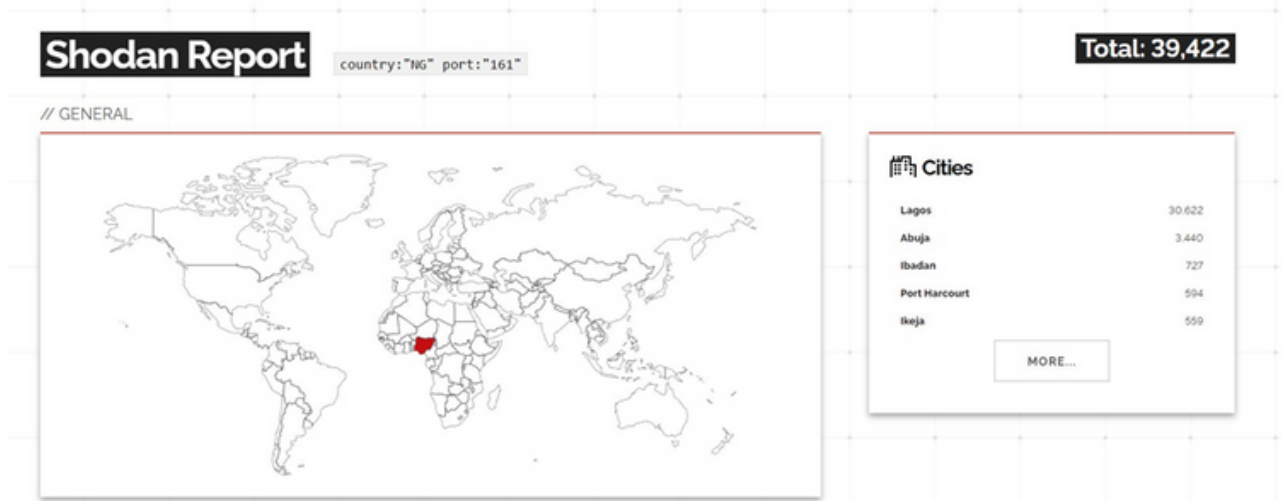
“Weak SNMP community strings, including the default ‘public,’ allowed APT28 to gain access to router information.”

Two was, how over time, attackers have leveraged outdated software, operating systems in the host, and network infrastructure to compromise the entire organization.

Looking at these two, we dig to understand the coverage of this product and protocol within our space, and we have the following statistics from Shodan;

- We have almost 40K internet-facing devices with SNMP ports on them. Not to talk of those being used internally
- Cisco Systems led the chart! Almost 17K devices were Cisco made, Followed by Mikrotik.
- Majority shareholders of such ports as per ISP holding them down for personal use and customer use.

Threat Actor Groups Targeting Vulnerabilities in Routers - Connecting it with PRTG



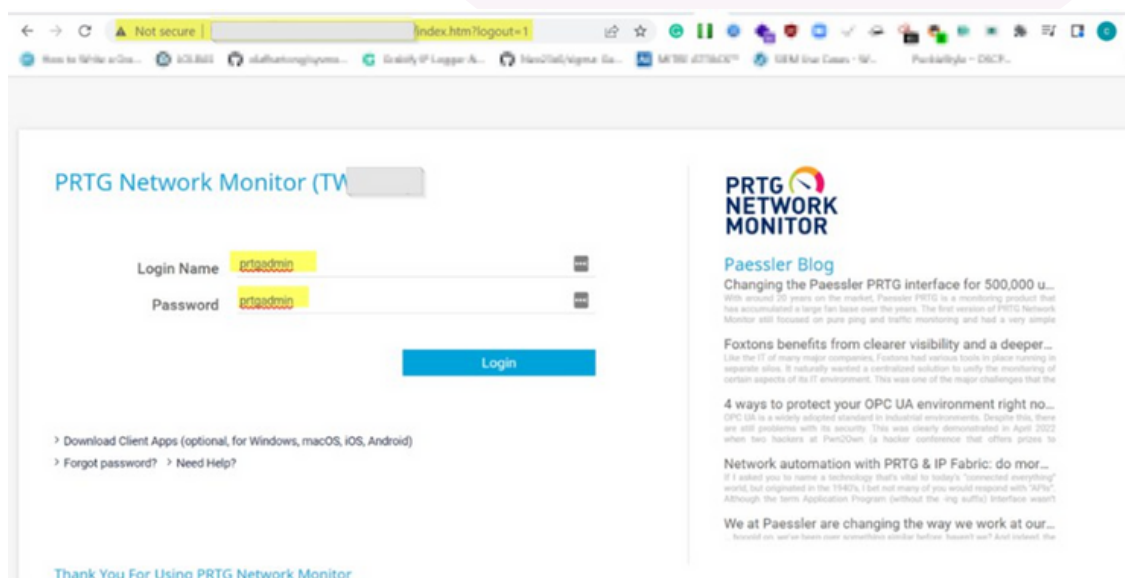
Threat Actor Groups Targeting Vulnerabilities in Routers - Connecting it with PRTG

Another interesting fact about the SNMP protocol is the need to Remember that SNMP versions 1, 2, and 2c present the highest level of risk because community strings are communicated in clear text, and can be used by attackers during an attack.

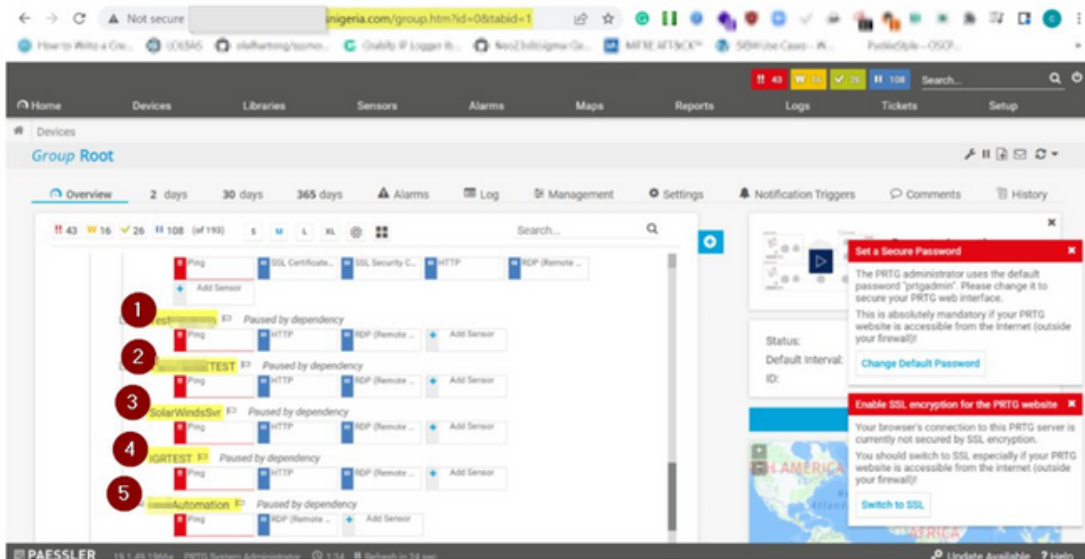
- We were able to find out that over 10K out of the 40K identified internet-facing assets are running version 1, some had version 3 combined



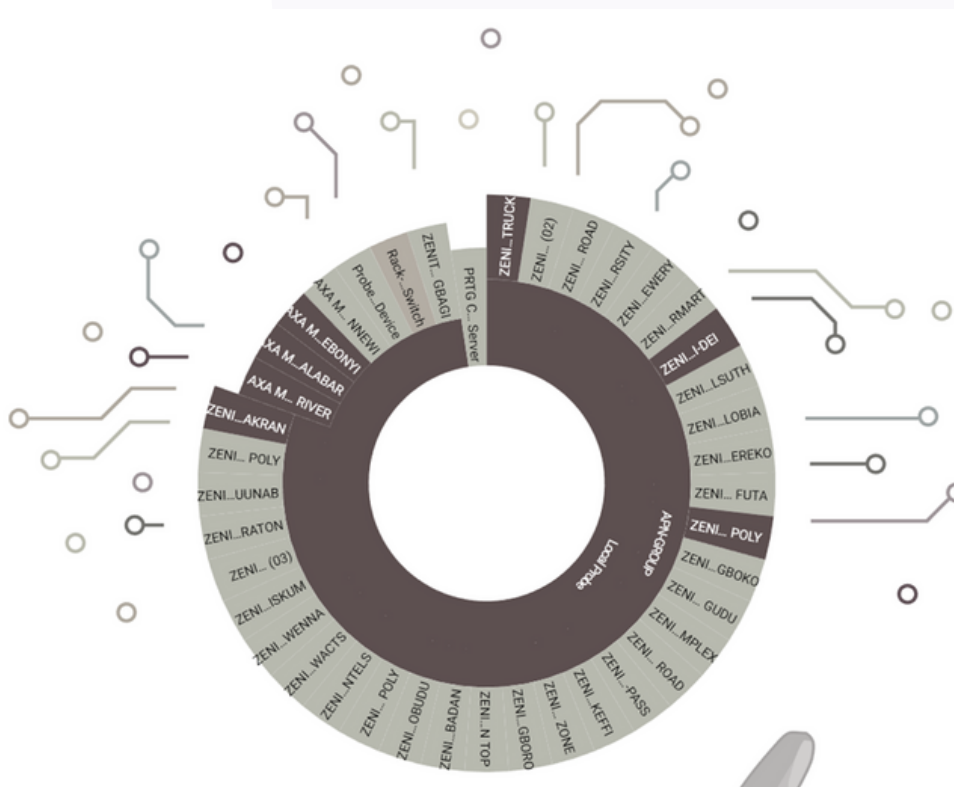
Linking this to a popular network monitoring tool called PRTG known to leverage the SNMP port on network devices and host for data collections; which is commonly deployed by organizations in Nigeria, we were able to chain it up with a PoC as we have seen some organizations leaving it misconfigured thereby exposing their internal system. This is the POC of what an attacker can do with it; enumerations and discovery.



Threat Actor Groups Targeting Vulnerabilities in Routers - Connecting it with PRTG



As of this writing, more of these servers are currently exposed. And considering its relationship with SNMP, and the type of information it can provide an attacker; it would be a gold mine for malicious threat actors to learn of the internal network of their target without even doing any work; as this just got served on a platter of Gold.

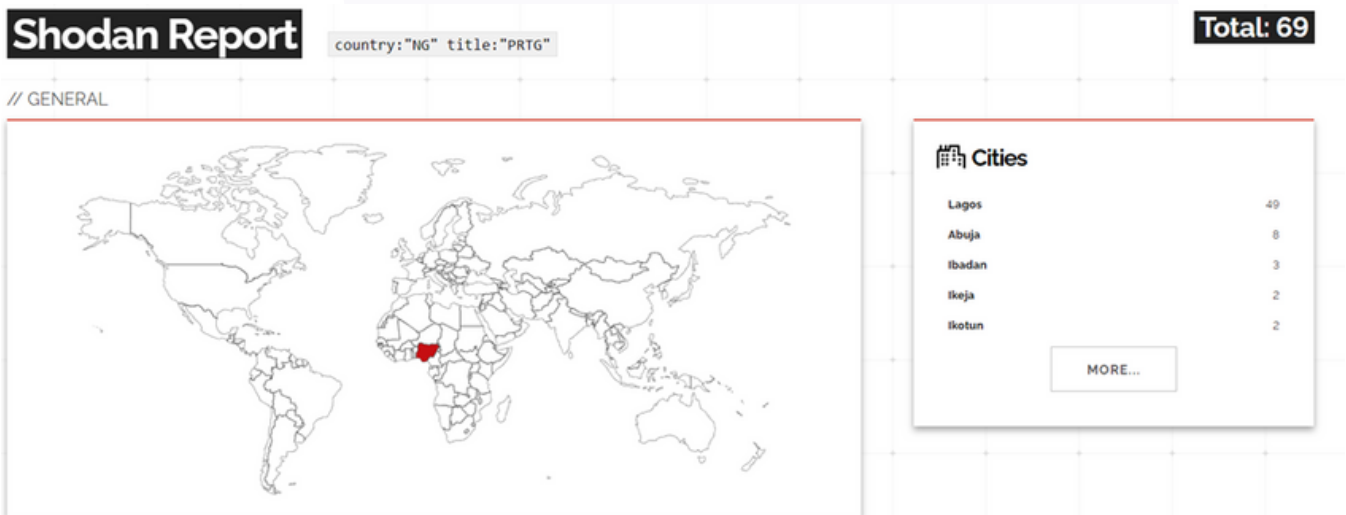


Threat Actor Groups Targeting Vulnerabilities in Routers - Connecting it with PRTG

We urge organizations, businesses with similar infrastructure and services to apply the following key recommendations & advice.

- Organizations with services that are largely dependent on this protocol should apply security best practices around the management of SNMP ports & their usage.
- The use of older versions and misconfiguration are key issues that must be highlighted, and those not using the port should take them off.
- PRTG dashboard access should be reconfigured from the default.
- Continuous vulnerability management should apply to all assets, whether internal or external facing that is under the purview of all organizations and businesses.

As of 23rd April 2023, the count of devices with this PRTG product was 71 after which two devices left as contained in the image below taken on 25th April 2023. Mostly owned and used by ISPs*



April 2023

Organizations Breached / Experienced Ransomware Attack

- The American Bar Association (ABA)
- Capita, London UK
- Two Major Automotive Manufacturers Hyundai and Toyota
- South Korean National Tax Service
- Kodi Media Player
- Netherlands' national railway company, NS
- City of Oakland, California
- Evotec, a German biotech company

Critical CVEs Reported

- Cisco and VMware Products
- Microsoft, Apple
- Enterprise vendor SAP
- Nexx IoT
- VM2, a popular Javascript Library

Interesting Highlight

- A global operation called Cookie Monster shut down Genesis Market, a major site for stolen data and device identities, and arrested 119 of its users.
- Anonymous Sudan, a sub-group of the Russian hacktivists Killnet, has been behind several DDoS attacks on various countries, motivated by anti-Muslim sentiments.
- Hackers used 3CX Desktop App, a VoIP app for Windows and macOS, to spread malicious versions in a big supply chain attack.
- A new attack in Azure Active Directory exploits a common misconfiguration and can affect apps like Bing.com, allowing hackers to access and change search results.

Twice beaten, no shy. Ransomware in Nigeria - The lessons we did not learn.



Ransomware in Nigeria - The lessons we did not learn.

‘No official information yet, but we have seen some leakage of alleged compromise of a certain Nigeria organization as released by a ransomware threat group in the dark web’ – This was a statement from a member of our Threat Intel Team This was on the afternoon of April 16th, 2023.

ALPHV

Blog Collections

A little background from what we know before this time...

A week earlier, we got some intel and notification of intrusion on certain facilities which has to do with the usage of Cobalt Strike in its post-exploitation as documented by the CyberPlural’s Team. This introduced a couple of questions as to whether the country is being targeted towards this time as a similar incident had been previously captured by the team in 2022, just a few days after the Bet9ja incident became news.

Basically in 2022, the following happened;

- Bet9ja Ransomware Incident
- ALPHV / Blackcat was stated to be responsible
- Cobalt Strike Post-Exploitation Tool observed around certain facilities in Nigeria.
- Bet9ja was updating stakeholders on their progress throughout the incident and provided assurance to customers on their progress to restoring. (This single act was documented to have prevented similar attacks in other organizations)

Cobalt strike is a legitimate and powerful post-exploitation tool known for its abuse by cybercriminals targeting organizations’ networks and always part of the tools used in the MOs for this particular ransomware group that is getting their second publicly disclose hit in Nigeria (ALPHV / Blackcat). And it will interest you to know that FBI documentation carrying the MOs of this ransomware group captured it as shown below.

Technical Details

BlackCat/ALPHV ransomware leverages previously compromised user credentials to gain initial access to the victim system. Once the malware establishes access, it compromises Active Directory user and administrator accounts. The malware uses Windows Task Scheduler to configure malicious Group Policy Objects (GPOs) to deploy ransomware. Initial deployment of the malware leverages PowerShell scripts, in conjunction with Cobalt Strike, and disables security features within the victim’s network. BlackCat/ALPHV ransomware also leverages Windows administrative tools and Microsoft Sysinternals tools during compromise.

Ransomware in Nigeria - The lessons we did not learn.

This background reinforces our belief that the publication date of this compromise on the leakage site of ALPHV is not the same as the real incident date, and is very far from the initial date of entry. The ransomware deployment part of the incident might have happened earlier, maybe a week earlier putting it at the first week of April at best.

Considering the phases involved in a successful and sophisticated compromise as this which cut across the adversary gaining initial access to the network, the conduct of internal recon of the alleged victim's networks, finding important data and laterally moving across different connected business segments networks down to exfiltration of the data, confidential business data as we come to find out wouldn't be just an overnight work. The start of this journey to the end might have taken months before the ransomware deployment.

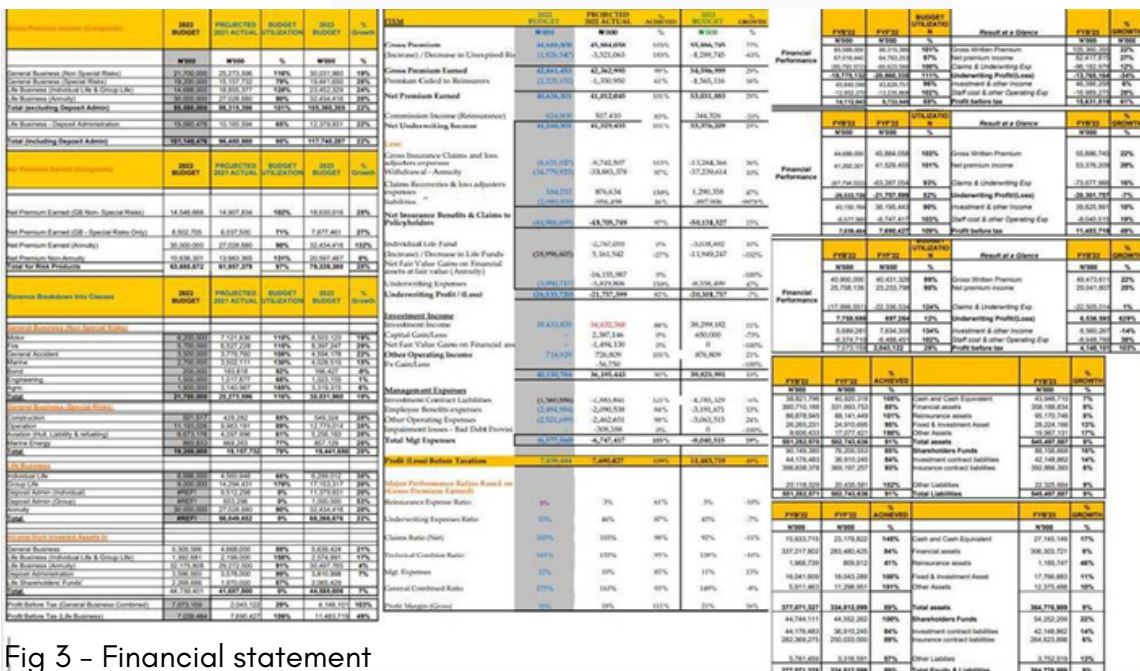


Fig 3 - Financial statement

This data as contained in Fig 3 above and 4 and 5 below indicated the ALPHV group was not bluffing about what they were currently holding on the alleged victim, thousands of customer's personal data and business-related data. Information on the leak site indicated that what was currently published is just a part of the stolen data, and if management (of the alleged victim's company) did not contact soon will warrant the release of others.

Ransomware in Nigeria - The lessons we did not learn.

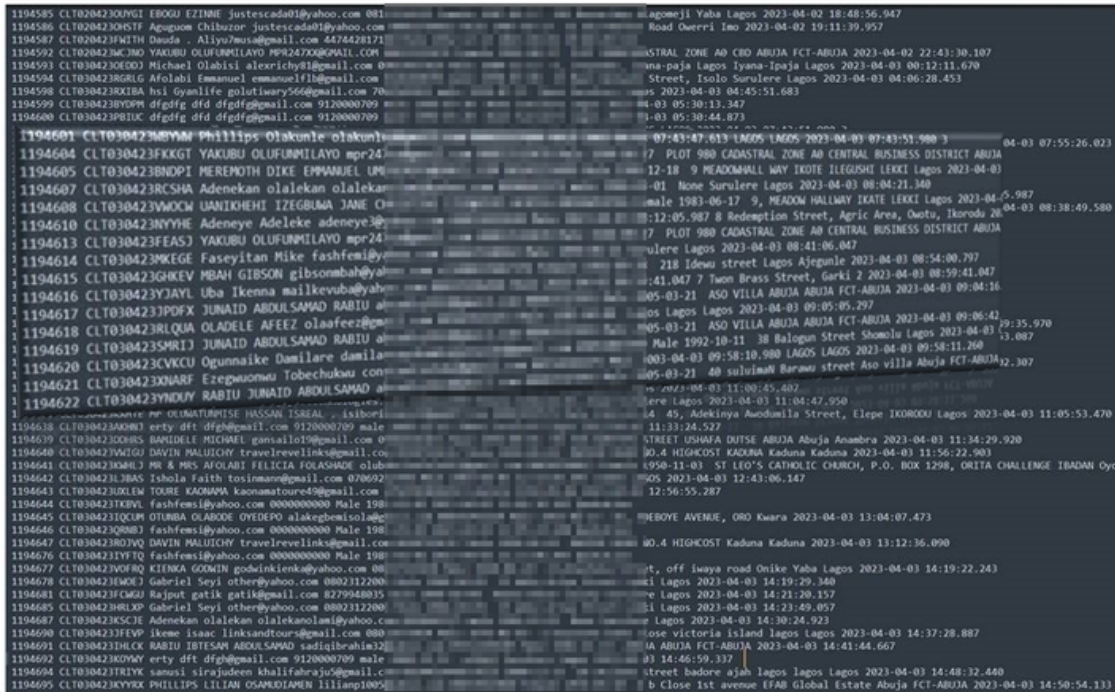


Fig 4 - Personally Identifiable Information of Customers.



Fig 5 - Passports as used by customers as a means of identity validations for enabling services offered.

Ransomware in Nigeria - The lessons we did not learn.

On one hand, we were expecting an official statement on this incident from the alleged victim. The statement was to guide customers in ensuring they are protected from secondary attacks such as phishing & social engineering, as well as stakeholders getting to know of the progress the organization is making in restoring and becoming operational.

Such a statement has also been seen in the past to have helped protect other businesses and organizations operating in the same space and industry as the alleged victim of such an ugly incident.

After four days of waiting, no official statement from any quarter and we already concluding the ALPHV group might as well start releasing the rest of the data or maybe some transactions might have exchanged hands which might make the alleged victim publication to be removed from their site; any of these two was possible at the time.

To cap it all; In 2023 similar incidents as in 2022 took place as highlighted below:

- Another Ransomware Incident
- ALPHV / Blackcat claimed responsibility as the leak site has it documented, and sample data released.
- Cobalt Strike Post-Exploitation tool observed around certain facilities in Nigeria.
- The alleged victim went political with the breach notification on the incident.

It is important we note that acknowledging cyber incidents, vulnerabilities and issuing a breach notification as it should, does not make our organization weaker but what we do after knowing about the incident, as this differentiates an organization that will not become a victim of another attack in the future to those that are likely to be again.

In the end, organizations and societies that tend to be political with cyber incidents are likely to diminish the trust and confidence their customers and peers have in them thereby eroding the digital trust on which the society of the 21st century is expected to thrive on.

May 2023

Organizations Breached / Experienced Ransomware Attack

- [Swedish-Automation Company ABB](#)
- The City of Dallas, Texas
- [Suzuki Motorcycles](#)
- Virginia-based Bluefield University
- [The Japanese automaker Toyota](#)
- Arnold Clark, one of Europe's largest car retailers
- [T-Mobile](#)
- Western Digital
- HWL Ebsworth

Critical CVEs Reported

- VMware Workstation and VMware Fusion - marked CVE-2023-20869
- Apple (AirPods and Beats)
- WordPress Elementor Plugin
- Cisco - (CVE-2023-20159, CVE-2023-20160, CVE-2023-20161)

Interesting Highlight

- Fake video-editing sites lure users into downloading malware that steals their information.
- MalasLocker ransomware attacks [Zimbra servers](#), locks files and emails, and asks for charity donations.
- Researchers have reported on DarkCloud info-stealer, which is currently being distributed via spam emails. [DarkCloud](#) is designed to steal account credentials stored on infected systems
- [PaperCut servers](#) exploited to deliver CIOP and LockBit ransomware, patch available. Microsoft warns of a recent wave in the exploitation of CVE-2023-27350, a critical-severity remote code execution vulnerability in PaperCut
- [Obsidian ORB ransomware](#) hits Windows and asks for gift cards.

OWA - Several servers are still vulnerable to Proxy Attack Chain



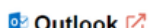
OWA - Several servers are still vulnerable to Proxy Attack Chain

The ProxyLogon, ProxyShell, ProxyNotShell, and OWASSRF exploit chains were used to attack Microsoft Exchange servers across a range of sectors including real estate, law firms, manufacturing, consulting, wholesale, and arts and entertainment.

ProxyShell is a way of hacking Exchange servers without login or password by using three flaws in the system. It can run any command on the server through the internet.

To summarize those exploits:

- CVE-2021-34473: Allows 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 to run PowerShell commands
- CVE-2021-31207: This vulnerability leverages the New-MailboxExportRequest cmdlet in order to export the user mailbox to an arbitrary file location, which can be used to write a web shell on the Exchange server.
- CVE-2021-34473, CVE-2021-26858, CVE-2021-26857, CVE-2021-26855, CVE-2021-31207, CVE-2021-31206, CVE-2021-34523, CVE-2021-27065



102.104.100.100
inb.letazuma.com
AutoDiscover
hq-exc2
Layer3 Limited
Nigeria, Abuja

SSL Certificate

Issued By:
Common Name:
Sectigo RSA Domain
Validation Secure Server
CA

Organization:
Sectigo Limited

Issued To:
Common Name:
inb.letazuma.com

Supported SSL Versions:
TLSv1.2

Vulnerabilities

CVE-2021-34473
CVE-2021-31206
CVE-2021-34523
CVE-2021-31207

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

2023-05-06T16:13:43.111709



41.104.100.100
www.mail.letazuma.com
mail.letazuma.com
ipNX NIGERIA LIMITED
Nigeria, Abuja

SSL Certificate

Issued By:
Common Name:
Go Daddy Secure
Certificate Authority - G2

Organization:
GoDaddy.com, Inc.

Issued To:
Common Name:
mail.letazuma.com

Organization:
Etazuma Mining &
Industries Ltd

Supported SSL Versions:
TLSv1, TLSv1.1,
TLSv1.2

Vulnerabilities

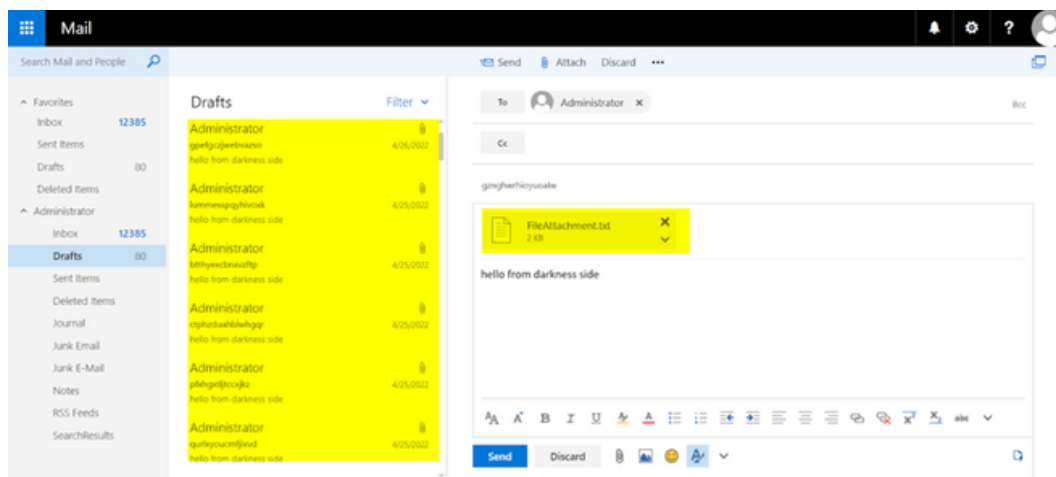
CVE-2021-34473
CVE-2021-26858
CVE-2021-26857
CVE-2021-26855
CVE-2021-31207
CVE-2021-31206
CVE-2021-34523
CVE-2021-27065

HTTP/1.1 200 OK
Cache-Control: no-cache, no-store
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-IIS/8.5
request-id: b81a0a04-680d-47ac-9f7b-18f3738f5b42
X-Frame-Options: SAMEORIGIN
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sat, 29 Ap...

2023-04-29T03:28:16.656853

OWA - Several servers are still vulnerable to Proxy Attack Chain

Several attempts in the past to exploit the popular proxy-chain vulnerabilities (Proxy Shell, Proxy Logon, Proxy Oracle) were observed during an Incident Response in the draft of Administrator Inbox as shown below;



The ProxyLogon attack is a cyberattack that exploits a vulnerability in Microsoft Exchange Server that allows an attacker to bypass the authentication and impersonate the admin. The attacker can then execute arbitrary commands on the server, such as installing a web shell to gain persistent access, stealing data, or launching further attacks.

Microsoft released patches and a one-click fix to mitigate the vulnerability, but many Exchange servers remained unpatched and vulnerable to the attack.

```

--$ python3 proxyshell.py -u https://[redacted]:[redacted]
[+] Determining number of Exchange backend servers...
[+] Exchange Backend Servers: ['[redacted]-ex01.[redacted].tals.com', '[redacted]-ex02.[redacted].tals.com']
[+] [redacted]-ex01.[redacted].tals.com - version: 15.2.221.18
[+] [redacted]-ex01.[redacted].tals.com - version short: Exchange Server 2019 RTM Mar21SU
[+] [redacted]-ex01.[redacted].tals.com - user: NT AUTHORITY\SYSTEM
[+] [redacted]-ex01.[redacted].tals.com - sid: S-1-5-18
[+] [redacted]-ex002.[redacted].tals.com - version: 15.2.221.12
[+] [redacted]-ex002.[redacted].tals.com - version short: Exchange Server 2019 RTM
[+] [redacted]-ex002.[redacted].tals.com - user: [redacted]\[redacted]-EX01$
[+] [redacted]-ex002.[redacted].tals.com - sid: S-1-5-21-1104
[+] Successfully parsed SID via backend request: S-1-5-21-[redacted]
[+] Attempting to retrieve Active Directory emails...
[+] Enumerated 110 possible UserMailbox LegacyDNs from Active Directory
[+] Enumerated 100 possible User LegacyDNs from Active Directory
[+] Enumerated SMTP domains: {'outlook.com', '[redacted].tals.com', '[redacted].health.com', '[redacted].com', '[redacted].com', 'gmail.com', 'yahoo.com'}
[+] Attempting to retrieve SID for /o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]
[+] Successfully parsed SID via UserMailbox object: S-1-5-21-[redacted]
[+] Attempting to discover SID via 49 builtin email combinations
[+] Retrieved LegacyDN: /o=[redacted].TALS/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=74e946a251d54d2783927e816aef0793-Administ
  
```

- To block access to endpoints or strings that may be vulnerable, a WAF/Web Platform (IIS or reverse proxy) should be used.
- You should probably review vendor (Microsoft) guidance
- Reviewing your exchange servers for IOCs, checking log files for activity, and checking for web shells that may have been dropped are some steps you may want to take.

Organizations Breached / Experienced Ransomware Attack

- United States' largest dental insurer, MCNA
- Greece's Ministry of Education
- Jimbos Protocol
- Japanese Pharmaceutical Giant Eisai
- Beverly Hills Plastic Surgery
- The Estonia-based cryptocurrency wallet service Atomic Wallet
- America CalPERS and CalSTRS
- The Louisiana Office of Motor Vehicles (OMV) and the Oregon DMV Services

Critical CVEs Reported

- Zyxel Networks
- ISC on Bind 9
- Cisco
- MOVEit Transfer (CVE-2023-34362)

Interesting Highlight

- ALPHV says it hacked Reddit and took 80GB of data. The group claims to be behind the attack on Reddit, which was disclosed by the company in February 2023.
- The LockBit ransomware, which attacked more organizations than any other in 2022, was reviewed by CISA. The report says that the group targeted over 1,700 US organizations since 2020 and got about \$91M from US victims only as ransom payments
- Cyclops Group is a new provider of ransomware services that can be found on dark web forums. It can attack Windows, Linux, and macOS systems. Cyclops also has a different binary for stealing data.
- The Nigerian Data Protection Act, of 2023 is a new law that regulates how personal data is collected, used, and protected in Nigeria. It replaces the previous regulations under the NITDA Act and aims to promote data privacy, security, and accountability.

2023 | Q2

Recommendations

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



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

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

Contact US

web

cyberplural.com

email

hello@cyberplural.com

blog

blog.cyberplural.com

social



#BeProactive