THREAT INTELLIGENCE CAPSTONE PROJECT

Target: Densastate.gov.ng (Densa State Government)
Prepared by: David Kiridi
Date: May 2025

Executive Summary

This report presents the findings of a cyber threat intelligence exercise conducted on the domain **densastate.gov.ng**, the official online presence of the Densa State Government. The objective was to assess the organization's public-facing digital footprint using open-source intelligence (OSINT) tools to uncover potential vulnerabilities and threat exposure.

Through tools such as **theHarvester**, **crt.sh**, **WHOIS**, **BuiltWith**, **VirusTotal**, and the **Wayback Machine**, the investigation revealed over 30 exposed subdomains, a publicly listed administrative contact, outdated DNS protections, use of a widely targeted WordPress CMS, and missing SPF/DMARC email authentication protocols.

These findings indicate a large attack surface and potential gaps in foundational cybersecurity hygiene. Recommendations are made to join recognized threat intelligence communities such as FIRST, GFCE, and MISP to enhance collaboration, monitoring, and response capacity. The information gathered will support the security risk analysis to follow in Part Two of the capstone project.

OBJECTIVE

The objective of this phase is to gather and analyze publicly available cyber threat intelligence related to Densastate.gov.ng. Using OSINT tools, the goal is to assess the organization's public exposure, identify potential vulnerabilities, and lay the foundation for risk analysis in subsequent phases.

IDENTIFIED CYBER THREAT INTELLIGENCE SOURCES USED

As required, below are six major sources of cyber threat intelligence used during the OSINT phase of this project. Each source provided valuable insights into the target organization’s external exposure:

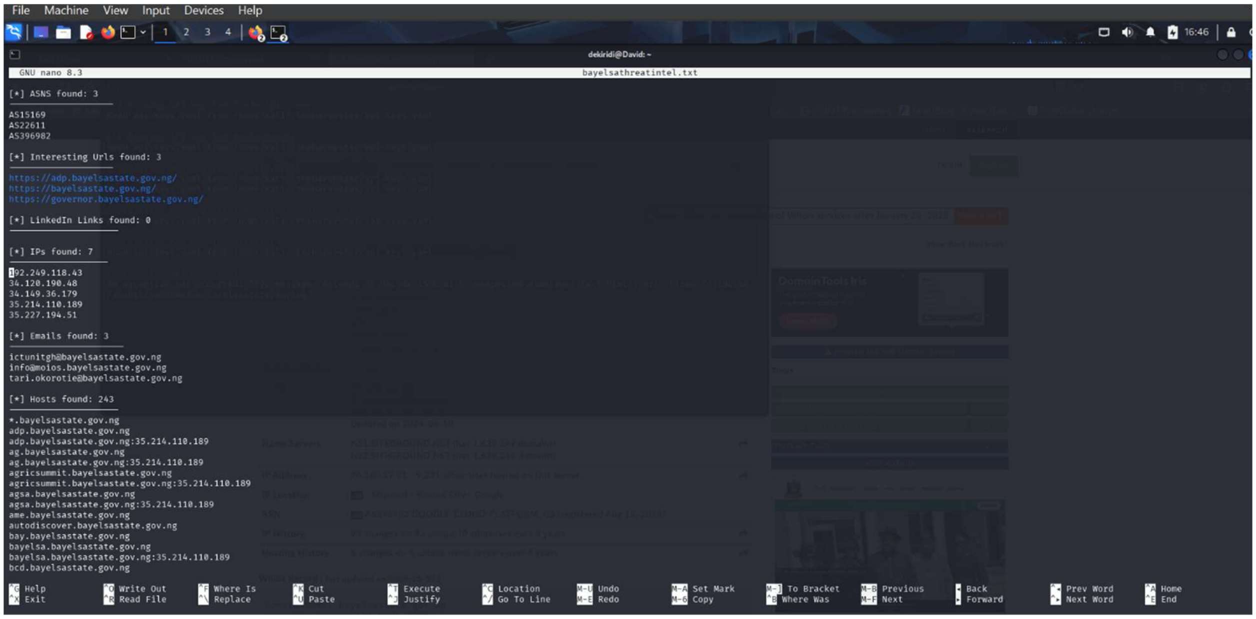
1. **theHarvester** – for collecting emails, subdomains, IPs, and DNS info.
2. **WHOIS Lookup** – to retrieve domain registration and administrative data.
3. **crt.sh (Certificate Transparency Logs)** – to enumerate SSL certificates and subdomains.
4. **BuiltWith / Wayback Machine** – to analyze the current and historical website technology and content structure.
5. **VirusTotal** – to check domain/IP reputation and scan for malware indicators.
6. **Google Dorking / Manual Search** – to discover publicly accessible documents and metadata leaks.

THREAT INTELLIGENCE TOOLS USED

The following tools were used to collect intelligence on densastate.gov.ng. Each tool served a unique purpose in revealing the organization’s external footprint and threat exposure:

1. theHarvester

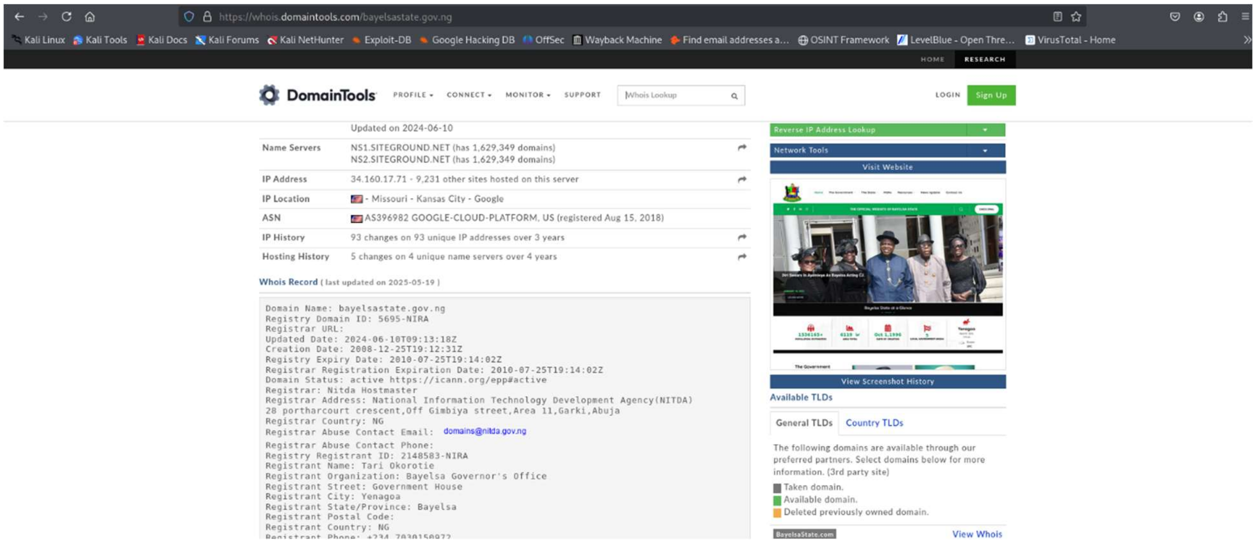
- **Purpose:** Automated collection of emails, subdomains, IPs, and DNS info.
- **Findings:** Discovered 30+ subdomains, IP addresses, email naming conventions, and DNS structure.
- **Implication:** Helped build an accurate map of the organization’s attack surface.



```
  GNU nano 8.3                                  bayelsathreatintel.txt

[*] ASNS found: 3
____________________

AS15169
AS22611
AS396982

[*] Interesting Urls found: 3
____________________

https://adp.bayelsastate.gov.ng/
https://bayelsastate.gov.ng/
https://governor.bayelsastate.gov.ng/

[*] LinkedIn Links found: 0
_____________________


[*] IPs found: 7
___________________

192.249.118.43
34.120.190.48
34.149.36.179
35.214.110.189
35.227.194.51

[*] Emails found: 3
______________________

ictunitgh@bayelsastate.gov.ng
info@moios.bayelsastate.gov.ng
tari.okorotie@bayelsastate.gov.ng

[*] Hosts found: 243
_____________________

*.bayelsastate.gov.ng
adp.bayelsastate.gov.ng
adp.bayelsastate.gov.ng:35.214.110.189
ag.bayelsastate.gov.ng
ag.bayelsastate.gov.ng:35.214.110.189
agricsummit.bayelsastate.gov.ng
agricsummit.bayelsastate.gov.ng:35.214.110.189
agsa.bayelsastate.gov.ng
agsa.bayelsastate.gov.ng:35.214.110.189
ame.bayelsastate.gov.ng
autodiscover.bayelsastate.gov.ng
bay.bayelsastate.gov.ng
bayelsa.bayelsastate.gov.ng
bayelsa.bayelsastate.gov.ng:35.214.110.189
bcd.bayelsastate.gov.ng

^G Help      ^O Write Out  ^F Where Is  ^K Cut    ^T Execute  ^C Location  M-U Undo  M-A Set Mark  M-] To Bracket  M-B Previous  ^B Back     ^◂ Prev Word  ^A Home
^X Exit      ^R Read File  ^\ Replace   ^U Paste  ^J Justify  ^/ Go To Line  M-E Redo  M-6 Copy  ^B Where Was  M-F Next  ^F Forward  ^▸ Next Word  ^E End
```

2. WHOIS Lookup

- **Purpose:** Domain registration, contacts, and expiration data.
- **Findings:** Publicly exposed admin contacts; DNSSEC not enabled.
- **Implication:** Vulnerable to social engineering and DNS spoofing.



	Updated on 2024-06-10
Name Servers	NS1.SITEGROUND.NET (has 1,629,349 domains) NS2.SITEGROUND.NET (has 1,629,349 domains)
IP Address	34.160.17.71 - 9,231 other sites hosted on this server
IP Location	- Missouri - Kansas City - Google
ASN	AS396982 GOOGLE-CLOUD-PLATFORM, US (registered Aug 15, 2018)
IP History	93 changes on 93 unique IP addresses over 3 years
Hosting History	5 changes on 4 unique name servers over 4 years

Whois Record (last updated on 2025-05-19)

```
Domain Name: bayelsastate.gov.ng
Registry Domain ID: 5695-NIRA
Registrar URL:
Updated Date: 2024-06-10T09:13:18Z
Creation Date: 2008-12-25T19:12:31Z
Registry Expiry Date: 2010-07-25T19:14:02Z
Registrar Registration Expiration Date: 2010-07-25T19:14:02Z
Domain Status: active https://icann.org/epp#active
Registrar: Nitda Hostmaster
Registrar Address: National Information Technology Development Agency(NITDA)
28 portharcourt crescent,Off Gimbiya street,Area 11,Garki,Abuja
Registrar Country: NG
Registrar Abuse Contact Email:  domains@nitda.gov.ng
Registrar Abuse Contact Phone:
Registry Registrant ID: 2148583-NIRA
Registrant Name: Tari Okorotie
Registrant Organization: Bayelsa Governor's Office
Registrant Street: Government House
Registrant City: Yenagoa
Registrant State/Province: Bayelsa
Registrant Postal Code:
Registrant Country: NG
Registrant Phone: +234 7030150972
```

Available TLDs

General TLDs | Country TLDs

The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

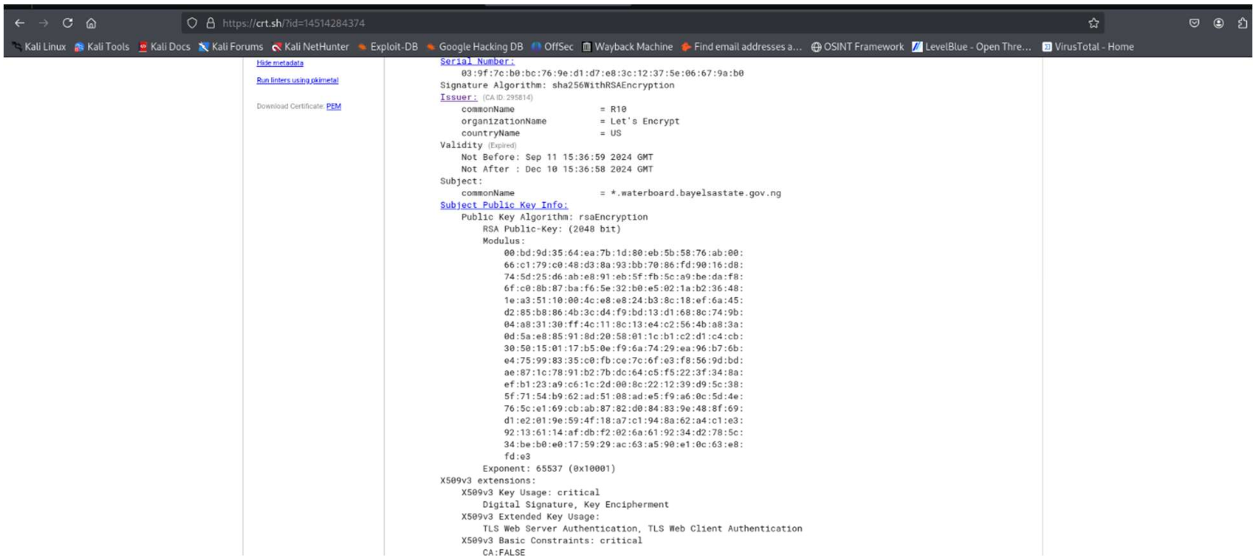
▨ Taken domain.
🟩 Available domain.
🟧 Deleted previously owned domain.

BayelsaState.com View Whois

3. Certificate Transparency Logs (crt.sh)

- **Purpose:** Discovery of SSL-issued subdomains.
- **Findings:** Wildcard certificates issued for 30+ subdomains.
- **Implication:** Increases attack surface; potential for subdomain takeovers.

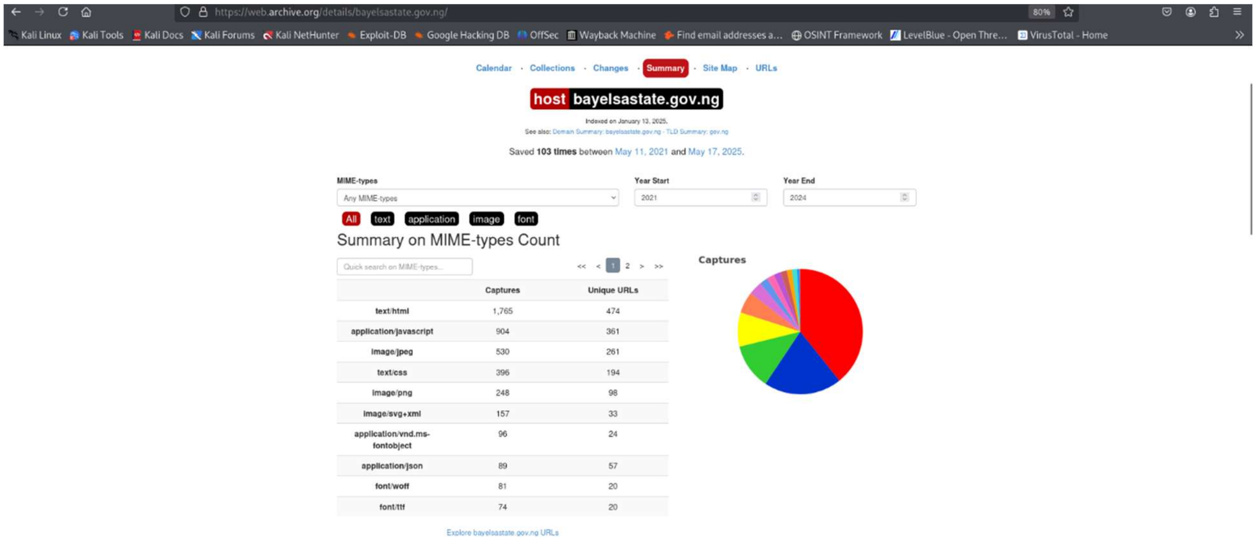
Example Certificate Insight:
A wildcard SSL certificate was discovered for the subdomain **waterboard.densastate.gov.ng**, issued by Let’s Encrypt. The certificate, valid from September 11, 2024, to December 10, 2024, had expired at the time of review. Wildcard certificates allow coverage of all subdomains under the specified domain. If one subdomain is compromised, the entire namespace could be at risk.



```
Serial Number:
    03:9f:7c:b0:bc:76:9e:d1:d7:e8:3c:12:37:5e:06:67:9a:b0
Signature Algorithm: sha256WithRSAEncryption
Issuer: (CA ID: 295814)
    commonName                = R10
    organizationName          = Let's Encrypt
    countryName               = US
Validity (Expired)
    Not Before: Sep 11 15:36:59 2024 GMT
    Not After : Dec 10 15:36:58 2024 GMT
Subject:
    commonName                = *.waterboard.bayelsastate.gov.ng
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        RSA Public-Key: (2048 bit)
        Modulus:
            00:bd:9d:35:64:ea:7b:1d:80:eb:5b:58:76:ab:00:
            66:c1:79:c0:48:d3:8a:93:bb:70:86:fd:90:16:d8:
            74:5d:25:d6:ab:e8:91:eb:5f:fb:5c:a9:be:da:f8:
            6f:c0:8b:87:ba:f6:5e:32:b0:e5:02:1a:b2:36:48:
            1e:a3:51:10:00:4c:e8:e8:24:b3:8c:18:ef:6a:45:
            d2:85:b8:86:4b:3c:d4:f9:bd:13:d1:68:8c:74:9b:
            04:a8:31:30:ff:4c:11:8c:13:e4:c2:56:4b:a8:3a:
            0d:5a:e8:85:91:8d:20:58:01:1c:b1:c2:d1:c4:cb:
            30:50:15:01:17:b5:0e:f9:6a:74:29:ea:96:b7:6b:
            e4:75:99:83:35:c0:fb:ce:7c:6f:e3:f8:56:9d:bd:
            ae:87:1c:78:91:b2:7b:dc:64:c5:f5:22:3f:34:8a:
            ef:b1:23:a9:c6:1c:2d:00:8c:22:12:39:d9:5c:38:
            5f:71:54:b9:62:ad:51:08:ad:e5:f9:a6:0c:5d:4e:
            76:5c:e1:69:cb:ab:87:82:d0:84:83:9e:48:8f:69:
            d1:e2:01:9e:59:4f:18:a7:c1:94:8a:62:a4:c1:e3:
            92:13:61:14:af:db:f2:02:6a:61:92:34:d2:78:5c:
            34:be:b0:e0:17:59:29:ac:63:a5:90:e1:0c:63:e8:
            fd:e3
        Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Key Usage: critical
        Digital Signature, Key Encipherment
    X509v3 Extended Key Usage:
        TLS Web Server Authentication, TLS Web Client Authentication
    X509v3 Basic Constraints: critical
        CA:FALSE
```

4. **BuiltWith Wayback Machine**

- **Purpose:** To analyze both current and historical structure, technologies, and public exposure.
- **Findings:**
- BuiltWith revealed WordPress CMS, PHP backend, and Google Compute Engine hosting.
- Wayback Machine showed the domain was archived 103 times between May 2021 and May 2025.
- MIME-type data captured:
    - text/html: 1,765 captures
    - application/javascript: 904 captures
    - image/jpeg: 530 captures
    - 474 unique URLs indexed
- **Implication:** Archived content may expose deprecated or forgotten URLs, metadata, and historical vulnerabilities exploitable by attackers.



host bayelsastate.gov.ng

Indexed on January 13, 2025.

See also: Domain Summary: bayelsastate.gov.ng - TLD Summary: gov.ng

Saved **103 times** between May 11, 2021 and May 17, 2025.

MIME-types: Any MIME-types

Year Start: 2021

Year End: 2024

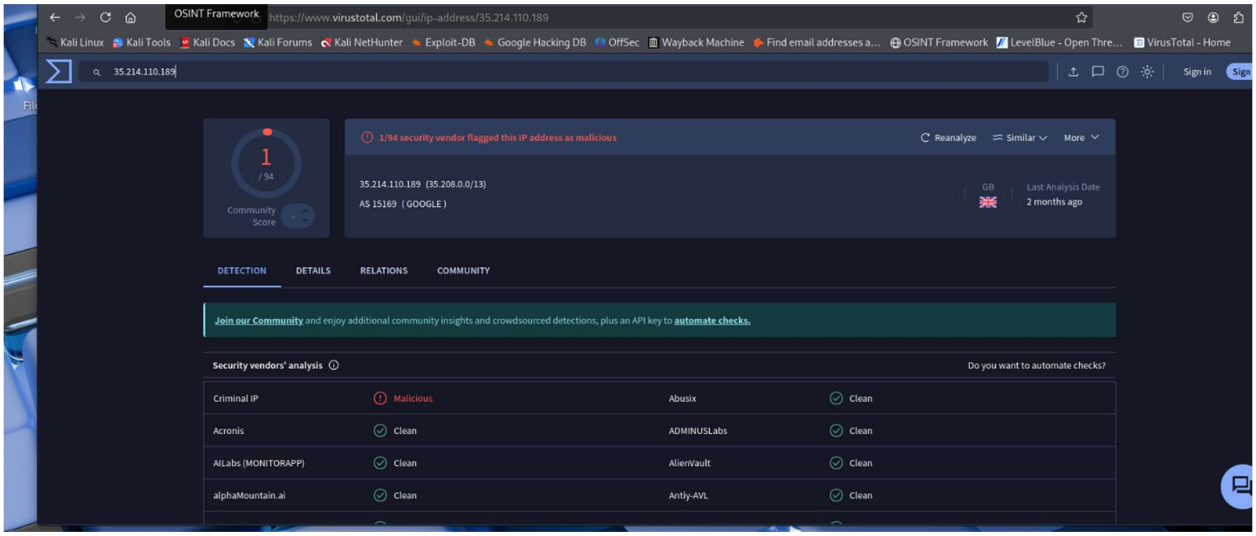
Summary on MIME-types Count

	Captures	Unique URLs
text/html	1,765	474
application/javascript	904	361
image/jpeg	530	261
text/css	396	194
image/png	248	98
image/svg+xml	157	33
application/vnd.ms-fontobject	96	24
application/json	89	57
font/woff	81	20
font/ttf	74	20

Explore bayelsastate.gov.ng URLs

5. VirusTotal

- **Purpose:** Scan IP/domain for malware or blacklist status.
- **Findings:** Domain clean, one malware detected.
- **Implication:** Positive hygiene, but shared IP risks persist.



1 / 94

1/94 security vendor flagged this IP address as malicious

35.214.110.189 (35.208.0.0/13)
AS 15169 (GOOGLE)

GB

Last Analysis Date: 2 months ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Criminal IP	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean

6. Google Dorking / Manual Search

- **Purpose:** Discovery of exposed documents and metadata.
- **Findings:** Publicly accessible PDFs with metadata (usernames, software versions).
- **Implication:** Useful for profiling and social engineering.

RECOMMENDED INTELLIGENCE-SHARING ORGANIZATIONS

To enhance threat detection, collaboration, and response, Densa State Government is advised to join these professional cybersecurity communities:

1. **FIRST (Forum of Incident Response and Security Teams)**
   Global CSIRT collaboration, threat sharing, and incident response coordination.
2. **GFCE (Global Forum on Cyber Expertise)**
   Multilateral platform for public-sector cyber capacity building.
3. **MISP Project Community**
   Open-source threat intelligence platform for structured IOC sharing.
4. **APCERT (Asia Pacific CERT)**
   Model collaborative CERT community with public-sector participation.
5. **ISACA (Information Systems Audit and Control Association)**
   Provides cyber risk governance training, threat reports, and best practices.

PART TWO: SECURITY RISK ASSESSMENT

S/N	Asset / Area	Vulnerability	Threat	Potential Risk
1	Admin/Tech Contact Info (WHOIS)	Public exposure of names and phone numbers	Social engineering, phishing, impersonation	Unauthorized access or fraudulent communications
2	Email Infrastructure	Missing SPF (Sender Policy Framework) and DMARC (Domain-based Message Authentication, Reporting and Conformance) records	Email spoofing, phishing	Impersonation of government domains, phishing success rates
3	Subdomains (e.g.,**waterboard**)	Wildcard certificates, lack of DNSSEC (Domain Name System Security Extensions**)**	Subdomain takeover, DNS spoofing	Service hijacking, data theft, credential harvesting

4	Content Management System (WordPress)	Possible outdated plugins or themes	Web exploitation SQLI (Structured Query Language) code is injected into a website's input field to **access or manipulate the database**, RCE (Remote Code Execution) Complete takeover of the system if exploited successfully, XSS (Cross-Site Scripting) Can **steal session cookies, login credentials, or perform actions on behalf of a user** without their consent.	Website defacement , loss of integrity and public trust
5	Exposed Documents (PDFs)	Metadata leaks (usernames, internal software info)	Social engineering, profiling	Identity spoofing, targeted phishing campaigns
6	Hosting Infrastructure	Shared IP space with other tenants	Cross-contamination	Service disruption, degradation

	(GCP) **Google Cloud Platform**		risks, IP blacklisting	in email delivery
7	Expired SSL Certificates	*.waterboard.densastate.gov.ng expired cert	Man-in-the-Middle (MiTM) attacks, expired trust	Browser errors, insecure communication, potential user data compromise

Recommended Controls / Mitigation Recommendation

1. Redact or mask WHOIS records via registrar or government managed DNS infrastructure.
2. Implement Sender Policy Framework (SPF) and Domain-based Message Authentication, Reporting and Conformance (DMARC) policies for email security.
3. Replace wildcard certificates with scoped ones, monitor CT logs, enable DNSSEC for domain integrity.
4. Ensure WordPress core, themes, and plugins are regularly updated, apply WAF (Web Application Firewall).
5. Sanitize documents before publication, disable metadata retention in office document settings.
6. Request dedicated IP from cloud provider or restrict access via firewall and IAM.
7. Monitor certificate expiry dates, automale SSL renewal and audit certificate transparency logs.

Summary

The Densa State Government's public infrastructure presents several low-to-moderate security risks, primarily due to poor email hygiene, exposed admin data, outdated certificates, and reliance on widely attacked platforms like WordPress. With appropriate mitigations, including modern email protections, better SSL management, and hardening of web and cloud infrastructure, the government can significantly reduce its cyber risk posture.

PART THREE: THREAT ACTOR PROFILING

S/N	Threat Actor / Group	Aliases	Target Sectors	Tactics & Tools	Notable Attacks
1	WINNTI GROUP	APT41, BARIUM, BLACKFLY, WICKED PANDA	Government, Software Vendors, Gaming, Pharmaceuticals, Education	Supply chain attacks, backdoors (e.g., ShadowPad, Winnti malware), DLL sideloading, C2 channels	- 2017 CCleaner supply chain attack \n - 2020 APT41 indictments by U.S. DOJ \n - Attacks on video game publishers and telecoms. "CLICK HERE"
2	FIN7	Carbanak Group	Financial, Hospitality, Retail	POS malware (Carbanak), phishing kits, backdoors	Targeted banks, restaurants (Chipotle, Arby's, Red Robin) "CLICK HERE'
3	Lazarus Group	Hidden Cobra	Government, Banks, Cryptocurrency	Ransomware, backdoors, wiper malware	Sony Pictures breach, WannaCry (2017), Bank of Bangladesh "CLICK HERE"
4	WIZARD SPIDER	UNC1878, Ryuk Group,	Government, Healthcare, Education, Financial	Ransomware (Ryuk, Conti), malware (TrickBot,	- 2018–2021 global Ryuk ransomware attacks \n -

		TrickBot Gang	Services, Logistics	BazarLoader), Cobalt Strike	U.S. hospitals hit during COVID-19 \n - Conti attacks on Costa Rican government (2022)”CLICK HERE”
5	APT33	Elfin, Holmium, Peach Sandstorm	Aerospace, Oil & Gas, Government, Defense Contractors	Spear phishing, custom malware (DropShot, TurnedUp), credential theft	2016–2019: Espionage against Saudi and U.S. aerospace and energy firms \n - Use of wiper malware similar to Shamoon. “CLICK HERE”

Summary

Each of these actors represents a credible threat due to their established history of targeting public institutions, use of advanced tools, and alignment with geopolitical or financial motives relevant to governments like Densa State.

PART THREE:

TTP MAPPING WITH MITRE ATT&CK (WIZARD SPIDER)

Introduction:

In this section, we examine the tactics, techniques, and procedures (TTPs) of Wizard Spider, a financially motivated cybercriminal group with a known history of targeting government, healthcare, and critical public infrastructure. Based on the digital footprint and vulnerabilities identified in Densa State Government’s domain, Wizard Spider poses the greatest operational threat due to their use of ransomware (Ryuk, Conti), malware loaders (TrickBot, BazarLoader), and remote access tools.

Wizard Spider's campaigns often begin with phishing, followed by the deployment of malware that allows for lateral movement and data encryption across enterprise networks. Their attacks are sophisticated, disruptive, and financially devastating — making them the most relevant threat actor for deeper analysis using the MITRE ATT&CK framework.

TTP MAPPING FOR WIZARD SPIDER USING MITRE ATT&CK

1. Reconnaissance: Search Open Sites (T1593)
   Description: Uses search engines and public data to discover subdomains and infrastructure.
   MITRE Link
   Reconnaissance: Gather Victim Org Info (T1591)
   Description: Collects organization details to craft targeted phishing.
   MITRE Link
2. Resource Development: Acquire Infrastructure (T1583)
   Description: Registers domains and servers for phishing and C2.
   MITRE Link
   Resource Development: Obtain Capabilities (T1588)
   Description: Uses off-the-shelf malware like TrickBot.
   MITRE Link
3. Initial Access: Phishing (T1566)
   Description: Delivers malicious attachments to gain initial foothold.
   MITRE Link
4. Execution: Command & Scripting Interpreter (T1059)
   Description: Executes malicious scripts using PowerShell or batch files.
   MITRE Link
5. Persistence: Registry Run Keys / Startup Folder (T1547.001)
   Description: Establishes persistence by modifying registry keys.
   MITRE Link
6. Privilege Escalation: Exploitation for Privilege Escalation (T1068)
   Description: Exploits vulnerabilities to gain elevated access.
   MITRE Link
7. Defense Evasion: Obfuscated Files or Information (T1027)
   Description: Encrypts or disguises payloads to avoid detection.
   MITRE Link

8. Credential Access: Credential Dumping (T1003)
   Description: Extracts credentials from memory or system files.
   MITRE Link
9. Discovery: System Information Discovery (T1082)
   Description: Collects OS, software, and hardware information.
   MITRE Link
10. Lateral Movement: Remote Services (T1021)
    Description: Uses RDP and SMB to spread across systems internally.
    MITRE Link
11. Collection: Data from Local System (T1005)
    Description: Gathers sensitive files from infected systems.
    MITRE Link
12. Exfiltration: Exfiltration Over C2 Channel (T1041)
    Description: Sends stolen data to attacker-controlled servers.
    MITRE Link
13. Impact: Data Encrypted for Impact (T1486)
    Description: Encrypts files with ransomware to extort payment.
    MITRE Link

CONCLUSION

The cyber threat intelligence assessment of densastate.gov.ng reveals that the Densa State Government's public-facing infrastructure contains several vulnerabilities that increase its exposure to cyber threats. These include missing email authentication protocols, outdated certificates, unprotected metadata, subdomain misconfigurations, and the use of a widely targeted WordPress CMS platform. When combined, these elements create a large attack surface attractive to sophisticated threat actors.

Among the actors profiled, **Wizard Spider** presents the most credible and immediate threat. This group specializes in ransomware campaigns that exploit many of the same weaknesses identified in this project—particularly email spoofing, credential harvesting, and lateral movement within vulnerable public systems. Their tactics align strongly with the Densa State Government's current gaps in email, CMS, and network infrastructure security.

By implementing the proposed mitigation measures and proactively engaging with global threat intelligence communities, Densa State can significantly improve its cybersecurity posture and resilience.

RECOMMENDATIONS

To reduce cyber risk exposure, the following strategic and technical actions are strongly recommended:

1. Strengthen Email Security

- Implement **SPF**, **DKIM**, and **DMARC** to prevent spoofing and impersonation.
- Enforce anti-phishing awareness training for staff.

2. Replace Wildcard Certificates

- Use **domain-scoped certificates** for individual subdomains.
- Automate renewal processes and monitor **certificate transparency logs**.

3. Improve DNS and Hosting Controls

- Enable **DNSSEC** to protect domain integrity.
- Request dedicated IPs from the cloud provider to avoid shared risks.

4. Secure WordPress and Plugins

- Regularly update all **core CMS components** and plugins.
- Deploy a **Web Application Firewall (WAF)** and configure proper access controls.

5. Sanitize Publicly Shared Files

- Strip metadata from office documents before uploading.
- Review all indexed documents using tools like **Google Dorking** to assess exposure.

6. Monitor and Log Activity

- Implement **continuous monitoring**, endpoint detection (EDR), and SIEM tools to detect intrusions early.

7. Join Threat Intelligence Networks

- Engage with cybersecurity communities such as:

    - **FIRST** – for coordinated incident response and global threat updates.
    - **GFCE** – for public-sector cyber capacity building.
    - **MISP** – for structured threat intelligence sharing (IOCs, TTPs).
    - **ISACA** – for governance, risk frameworks, and professional training.
    - **APCERT** – for regional collaboration and alert sharing.

REFERENCES

1. MITRE ATT&CK – Wizard Spider Group (G0102)
2. MITRE ATT&CK Techniques:

    - T1566 – Phishing
    - T1021 – Remote Services
    - T1059 – Command and Scripting Interpreter
    - T1486 – Data Encrypted for Impact

3. Mandiant – APT41 / Winnti Group Profile
4. MITRE – FIN7 Threat Group (G0046)
5. CISA – Lazarus Group Threat Alert
6. MITRE – APT33 Group (G0065)
7. VirusTotal – Domain Intelligence Platform
8. crt.sh – Certificate Transparency Log Search
9. theHarvester – OSINT Email & Domain Collection Tool
10. BuiltWith – Website Technology Profiler
11. Internet Archive – Wayback Machine