THREAT INTELLIGENCE ANALYSIS PROJECT

Conducted by: David Kiridi

Target: Densastate.gov.ng

(Densa State Government)

Introduction

Densa State Government is known for its oil wealth and natural beauty. The government delivers essential services through digital platforms vital to governance, education, healthcare, and infrastructure. In response to the surge in cyber threats driven by the increasing dependence on online services, I was tasked as a threat intelligence analyst to conduct a comprehensive threat intelligence analysis on the domain Densastate.gov.ng.

Objective of the Assessment

- Identify vulnerabilities in Densa State Government’s digital infrastructure.
- Analyze potential threat actors.
- Recommend strategies to strengthen cybersecurity posture

Sources and Tools Used

theHarvester – Email and subdomain enumeration

WHOIS Lookup - Domain registration, contacts, and expiration data

Crt.Sh – Certificate transparency analysis

Wayback Machine – Historical snapshots/ Technology stack profiling

VirusTotal – Malware and reputation checks

Google Dorking – Public document and data exposure discovery

KEY FINDINGS

theHarvester – Discovered 30+ subdomains, IP addresses, email naming conventions, and DNS structure

WHOIS Lookup- Publicly exposed admin contacts; DNSSEC (Domain Name System Security Extensions) not enabled

crt.sh – Wildcard certificates issued for 30+ subdomains

VirusTotal – Domain clean, one malware detected.
Google Dorking – Publicly accessible PDFs with metadata (usernames, software versions).

Wayback Machine –

- Revealed WordPress CMS (Content Management System), PHP backend, and Google Compute Engine hosting.
- Wayback Machine showed the domain was archived 103 times between May 2021 and May 2025.

Contd of Wayback machine.
MIME-type data captured:

- text/HTML: 1,765 captures
- application/JavaScript: 904 captures
- image/jpeg: 530 captures
- 474 unique URLs indexed

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, High 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 (GCP) Google Cloud Platform	Shared IP space with other tenants	Cross- contamination risks, IP blacklisting	Service disruption, Degradation 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, and potential user data compromise.

THREAT ACTOR PROFILING

S/N	Threat Actor / Group	Aliases	Target Sectors	Tactics & Tools	Notable Attacks
1	WINNTI GROUP (CHINESE ORIGIN)	BARIUM, BLACKFLY, WICKED PANDA	Government, Software Vendors, Gaming, Pharmaceuticals, Education	Supply chain attacks, backdoors (e.g., ShadowPad, Winnti malware), DLL sideloading, C2 channels	- 2017 Cleaner supply chain attack \n - 2020 APT41 indictments by U.S. DOJ \n - Attacks on video game publishers and telecoms.
2	FIN7 (RUSSIAN ORIGIN)	CARBANAK GROUP	Financial, Hospitality, Retail	POS malware (Carbanak), phishing kits, backdoors	Targeted banks, restaurants (Chipotle, Arby's, Red Robin)
3	LAZARUS GROUP (NORTH KOREA ORIGIN)	HIDDEN COBRA	Government, Banks, Cryptocurrency	Ransomware, backdoors, wiper malware	Sony Pictures Entertainment Attack (2014): Destructive attack and data leak in retaliation for the film "The Interview, Bank of Bangladesh ”CLICK HERE”
4	WIZARD SPIDER (RUSSIAN ORIGIN)	UNC1878, RYUK GROUP, TRICKBOT GANG	Government, Healthcare, Education, Financial Services, Logistics	Ransomware (Ryuk, Conti), malware (TrickBot, BazarLoader), Cobalt Strike	- 2018–2021 global Ryuk ransomware attacks U.S. hospitals hit during COVID-19 \n- Conti attacks on Costa Rican government (2022)
5	APT33 (IRANIAN)	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 . Use of wiper malware similar to Shamoon.

Threat Actor: Wizard Spider

01

Cybercrime group specializing in ransomware (Ryuk, Conti)

02

Targets government and healthcare sectors

03

Uses phishing, TrickBot, and BazarLoader for access and spread

04

Encrypts systems and demands ransom payments

TTP MAPPING WITH MITRE ATT&CK (WIZARD SPIDER)

This section analyzes Wizard Spider, a financially driven cybercriminal group targeting government and critical infrastructure.

Given the vulnerabilities in the Bayelsa State Government’s domain, they pose the highest threat through ransomware (Ryuk, Conti), malware loaders (TrickBot, BazarLoader), and phishing campaigns enabling lateral movement and data encryption.

Their sophisticated and disruptive attacks warrant deeper analysis using the MITRE ATT&CK framework.

TTP MAPPING WITH MITRE ATT&CK (WIZARD SPIDER)

TACTICS	MITRE ID	DESCRIPTION
Reconnaissance	Search Open Sites (T1593)	Uses search engines and public data to discover subdomains and infrastructure.
	Gather Victim Org Info (T1591)	Collects organization details to craft targeted phishing
Resource Development	Acquire Infrastructure (T1583)	Registers domains and servers for phishing and C2(Command and Control)
	Obtain Capabilities (T1588)	Uses off-the-shelf malware like TrickBot.
Initial Access	Phishing (T1566)	Delivers malicious attachments to gain initial foothold.
Execution	Command & Scripting Interpreter (T1059)	Executes malicious scripts using PowerShell or batch files.
Persistence	Registry Run Keys / Startup Folder (T1547.001)	Establishes persistence by modifying registry keys

TTP MAPPING WITH MITRE ATT&CK (WIZARD SPIDER)

TACTICS	MITRE ID	DESCRIPTION
Privilege Escalation	Exploitation for Privilege Escalation (T1068)	Exploits vulnerabilities to gain elevated access.
Defense Evasion	Obfuscated Files or Information (T1027)	Encrypts or disguises payloads to avoid detection
Credential Access	Credential Dumping (T1003)	Extracts credentials from memory or system files.
Discovery	System Information Discovery (T1082)	Collects OS, software, and hardware information.
Lateral Movement	Remote Services (T1021)	Uses RDP(Remote Desktop Protocol) and SMB(Server Message Block) to spread across systems internally.
Collection	Data from Local System (T1005)	Gathers sensitive files from infected systems.
Exfiltration	Exfiltration Over C2 Channel (T1041)	Sends stolen data to attacker-controlled servers.
Impact	Data Encrypted for Impact (T1486)	Encrypts files with ransomware to extort payment.

Risks to Densa State Government

- Disruption of essential public services.
- Data breaches affecting citizens.
- Financial loss from ransom payments due to high risk from threat actors like Wizard Spider, who exploit these weaknesses.
- Website Exploitation: Vulnerabilities in the widely targeted WordPress CMS platform can bring about Reputational damage and public distrust.

Recommendations

- ❖ Implement SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting & Conformance).
- ❖ Regular updates for CMS (Content Management System) and plugins
- ❖ Remove sensitive metadata from documents
- ❖ Staff training on phishing and cyber hygiene
- ❖ Join threat intelligence sharing networks [FIRST (Forum of Incident Response and Security Teams), MISP (Malware Information Sharing Platform)].

Conclusion

Cyber risks are real and growing for government institutions. Proactive cybersecurity measures are critical. Collaboration and awareness will enhance resilience.