**Passive Threat Intelligence Report**

Date: 2025-05-26

Primary Tool Used: theHarvester

Target Organization: The Hapuna Financial Limited

TI ANALYST: UCHE ABIODUN ENIOLA

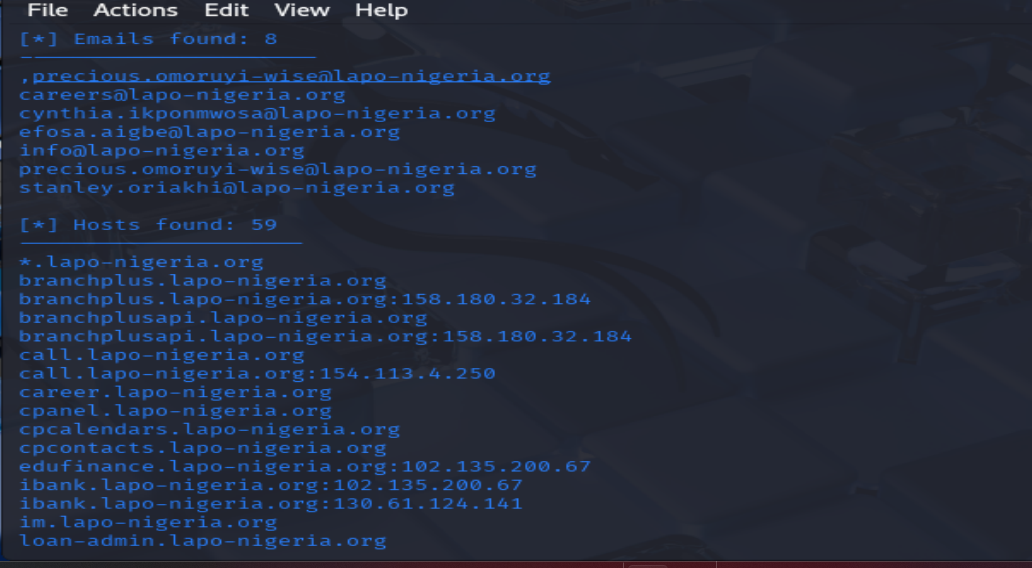
### ****Executive Summary****

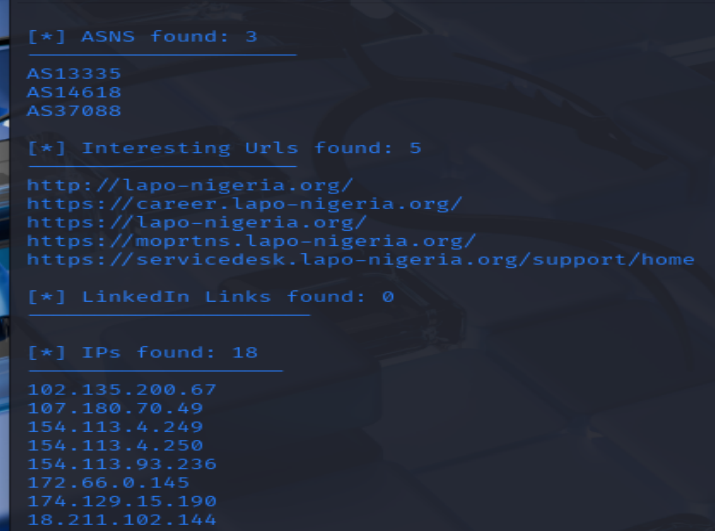
This report presents the findings of a passive reconnaissance assessment conducted on Hapuna, a FINTECH organization dedicated to improving financial access for low-income households through services such as savings and loans. The assessment was designed to identify publicly available information that could potentially expose the organization to cybersecurity threats.

Using passive intelligence-gathering techniques, specifically through the use of theHarvester, the project focused on enumerating accessible data without directly interacting with or scanning Hapuna’s infrastructure. The scope of this reconnaissance included email addresses, subdomains, IP addresses, and other publicly indexed metadata.

The objective of this exercise was not only to catalog potential exposures but also to evaluate the security implications of such information being available to threat actors. Based on the findings, this report provides actionable recommendations to reduce Hapuna’s public footprint and limit the risk of exploitation through social engineering, phishing, infrastructure mapping, or targeted attacks.

The following picture below shows the output using theHarvester an OSINTS Tool.





**Sources and Tools Used**

In the course of this project, several open-source intelligence (OSINT) platforms and threat intelligence communities were leveraged to assess the level of public exposure of Hapuna Financial Ltd. These sources provided passive insights into the organization’s infrastructure, email footprint, and external reputation.

**Threat Intelligence & OSINT Sources**:

**LinkedIn** – Used to identify publicly listed employees, roles, and email naming conventions for potential social engineering vectors.

**VirusTotal Community** – Analyzed shared indicators of compromise (IOCs) such as domains, IPs, or file hashes associated with Hapuna.

**Twitter** – Monitored for threat reports, credential leaks, or attacker chatter mentioning the organization.

**ISACs (Information Sharing and Analysis Centers)** – Reviewed financial sector threat reports relevant to Hapuna’s operational environment.

**AlienVault OTX** – Cross-referenced domains, IPs, and email addresses for threat activity or known malicious associations.

**AbuseIPDB** – Checked IPs related to Hapuna for any history of malicious behavior or abuse reports.

**Tools Utilized for Exposure Assessment**:

**Shodan.io** – Scanned publicly available internet-connected systems associated with Hapuna for exposed services and misconfigurations.

**MITRE ATT&CK Framework** – Mapped observed behaviors or exposure risks to known adversarial techniques for clearer risk context.

**Hunter.io** – Used to identify valid and exposed corporate email addresses across public records and data breaches.

**crt.sh** – Searched for SSL/TLS certificates issued to Hapuna subdomains, revealing additional infrastructure.

**Spyse (SecurityTrails)** – Provided historical DNS, port scanning data, tech stack information, and IP-to-domain mapping to identify potential forgotten or vulnerable assets.

**GREYNOISE**: This finds out if an IP address is part of known scanning or botnet activity.

**Information Exposure Assessment: Hapuna Financial Ltd**

The passive reconnaissance exercise conducted against Hapuna Financial Ltd revealed that a significantamount of organizational data is publicly availableonline, across various platforms and intelligence sources. While no direct scanning was performed, multiple exposures were identified through passive means alone, which present real risks from a security point.

1. Social Media Exposure

Platforms like LinkedIn revealed a list of employees, job roles, and potential email naming conventions

This can be exploited for social engineering or spear-phishing attacks targeting executives or high-privilege users

2. Online Infrastructure & Metadatal

Through tools like theHarvester, crt.sh, and Hunter.io, numerous subdomains and email addresses were passively discovered.

Services like Shodan.io and SecurityTrails exposed IP addresses and open ports associated with Hapuna’s web infrastructure.

Certificate transparency logs from crt.sh provided insights into past and present digital certificates issued to the organization’s subdomains — which may include test or staging environments.

3. Threat Intelligence Reports

AlienVault OTX and AbuseIPDB contained entries indicating that none Hapuna-associated IPs had been flagged for abuse in the past.

**Here** are the list of threat intelligence-sharing communities and organizations that I recommended for Hapuna Financial Ltd, as a fintech to improve its cyber defense posture:

1. FS-ISAC (Financial Services Information Sharing and Analysis Center)
2. FIRST (Forum of Incident Response and Security Teams)
3. MISP Project (Malware Information Sharing Platform)
4. AfricaCERT or National CERT (e.g., Nigeria CERT - ngCERT)
5. CTA (Cyber Threat Alliance)

**SECURITY RISK ASSESSMENT**

A Security Risk Assessment is the process of identifying, analyzing, and evaluating risks that could potentially affect the confidentiality, integrity, and availability of Hapuna Financial Ltd's information systems and data.

**Threat Classifications Based on Extracted Information**

Targeted Phishing & Email Attacks  
Exposed emails and naming patterns can be used for phishing, especially if attackers know names, roles, and departments from LinkedIn or public reports.

Reconnaissance for Infrastructure Attacks  
Knowing IP addresses, subdomains, and SSL certificates gives attackers a map of Hapuna’s digital infrastructure to plan more direct attacks like web exploitation or brute-forcing login portals.

Brand Damage & Trust Loss  
If malicious actors impersonate Hapuna (e.g., spoof emails using discovered addresses), it can lead to fraud, loss of customer trust, or regulatory issues.

Credential Reuse Attacks  
Public email addresses, especially when leaked in data breaches found on platforms like Hunter.io, can lead to credential stuffing if employees reuse password

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Categories** | **Information founds** | **Threat** | **Potential Risk** | **Vulnerabilities** | **Mitigations** |
| URL | 5 Interesting URLs both HPPT and HTTPS such as <https://career.Hupuna-nigeria.org>, <https://moprtns.Hapuna-nigeria.org> etc | Web portal visible then spies may gather information frm exposed interfaces | Atack surface mapping, this helps attacker to know where to target, unauthorized access especially if the URL leads to admin panels. | It can lead to login brute force or fuzzing attack using, Sensitive data exposure because the query string may contain passwords or user information. | Validate permissions, there should be authentication and authorization in place, HTTPS should be enabled to encrypt URL parameters. |
| IPs Addresses | 18 IPs address found:  102.135.200.67  18.211.102.144  172.66.0.145 to mention few. | DDos Attack which can disrupt services by flooding with traffic, Insider threat | Attacker can scan for open ports and vulnerability using SHODAN, unauthorized access to internal system, Data breach and reputation damage. Exposure of internal services or improperly secured ports | Outdated Apache/ SSH can be used (unpatched Services) Scanning and exploitation. | Firewall rules, IP whitelisting, Cloudflare (a cloud security services), Regular patch, penetration testing, IDS & IPS implementation. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| HOST | 59 Host names to found [link](https://crt.sh/?q=webmail.lapo-nigeria.org) | Port scanning and service enumeration (e.g., SSH, HTTP)  Exploitation of unpatched services using known CVEs  Access via default configurations or weak credentials  Exposure of admin panels or misconfigured web services | Some subdomains may be less secure and attractive to attackers | DNS reconnaissance  Social engineering via known hostnames  Automated scanning by threat actors and bots | Use firewalls and allowlists to restrict access to critical systems. Regularly scan for exposed assets using tools like Nmap, Shodan, or Censys, Remove unused or test environments from public exposure. |
| ASN | 3 ASNS were found:  AS13335  AS14618  AS37088 | Full-range ASN scanning for vulnerable hosts  Exposure of internal infrastructure if IP block is known  Targeting by threat actors based on ASN reputation (e.g., government, banking sector ASNs) | Traffic redirection, denial of service, or man-in-the-middle attacks at the ISP/network level. | Malicious actors can attempt to advertise routes that belong to ASN.  May lead to traffic redirection, surveillance, or blackholing of services.  A known ASN might reveal the hosting in AWS, Azure, etc., giving attackers info about underlying cloud platforms | Use cloud-based infrastructure that masks ASN details.  Subscribe to ASN threat monitoring services  Avoid static ASN ownership for sensitive environments if possible. |
|  |  |  |  |  |  |
| Email | Employees Email found: precious.omoruyi-wise@Hapuna-nigeria.org  careers@Hapuna-nigeria.org  cynthia.ikponmwosa@Hapuna-nigeria.org  ebusiness@Hapuna-nigeria.org  info@Hapuna-nigeria.org  jane.doe@Hapuna-nigeria.org | Email phishing, social Engineering, spear phishing, DDos | Unauthorized access. | Credential stuffing, Email spoofing, Business Email Compromise. | Train employees on phishing awareness and impersonation threats, use alias or generic emails, Enforce MFA (Multi-Factor Authentication) on all systems. |
|  |  |  |  |  |  |

**Threat Actors and Relevance to Fintech Sector**

The following threat actors have been active recently and possess tactics and techniques that align with the types of information discovered in this passive intelligence report. Given that the target organization is a fintech institution (state microfinance bank), the actors below represent relevant and realistic threats:

1. **Lazarus Group (North Korea)**

* Tactics: Spear-phishing, supply chain attacks, malware deployment
* Techniques: T1566.001 (Phishing with attachments), T1059 (Command and Scripting Interpreter), T1071 (Application Layer Protocol)

2. **FIN7 (Carbanak) (Eastern Europe)**

* Tactics: Malware delivery via email, lateral movement, data exfiltration
* Techniques: T1204 (User Execution), T1027 (Obfuscated Files), T1003 (Credential Dumping)

3. **TA505 (Unknown (likely Russia-linked)**

* Tactics: Mass phishing campaigns, ransomware deployment
* Techniques: T1486 (Data Encrypted for Impact), T1055 (Process Injection), T1047 (WMI Execution)

4. **APT38 (North Korea)**

* Tactics: Banking system manipulation, SWIFT network exploitation
* Techniques: T1140 (Deobfuscate/Decode Files), T1041 (Exfiltration Over C2 Channel), T1036 (Masquerading)

5. **EvilCorp (Russia)**

* Tactics: Dridex malware distribution, ransomware-as-a-service
* Techniques: T1059.003 (Windows Command Shell), T1499 (Endpoint Denial of Service), T1105 (Ingress Tool Transfer)

6**. Silence Group (Russia)**

* Tactics: ATM cash-out, email phishing, reconnaissance on financial institutions
* Techniques: T1592 (Gathering Vulnerability Information), T1083 (File and Directory Discovery), T1210 (Exploitation of Remote Services)

Here are several notable historical breaches and high-impact campaigns attributed to North Korean threat actors, particularly APT38, Lazarus Group, and APT37

1. Bangladesh Bank Heist (2016) – APT38

* Target: Bangladesh Central Bank (via SWIFT network)
* Impact: ~$81 million USD stolen (attempted $951 million)
* Method: Compromised internal banking systems, created fraudulent SWIFT transactions, used malware and custom tools to delete transaction logs.
* Relevance to FinTech: Demonstrated capability to breach and manipulate core financial systems, not just endpoints.

2. Sony Pictures Hack (2014) – Lazarus Group

* Target: Sony Pictures Entertainment
* Impact: Destruction of data, leaks of confidential emails, unreleased films, and sensitive employee information
* Method: Wiper malware (Destover), spear-phishing
* Motivation: Political retaliation (release of “The Interview” film)
* Significance: Marked the transition of North Korea from espionage to destructive attacks.

3. WannaCry Ransomware Attack (2017) – Lazarus Group

* Target: Global (over 200,000 systems in 150+ countries)
* Impact: Estimated damages in the billions; affected NHS UK, FedEx, Renault, etc.
* Method: Ransomware propagated via EternalBlue exploit (Windows SMBv1 vulnerability)
* Attribution: US, UK, and other governments officially attributed this to North Korea.
* Relevance: Shows DPRK’s ability to conduct global financial disruption.

4. Bank of Chile Attack (2018) – APT38

* Target: Banco de Chile
* Impact: $10 million USD stolen
* Method: Attackers gained access to internal systems and attempted to cover their tracks with wiper malware.
* Relevance: Similar attack style to Bangladesh Bank – targeted, strategic financial theft.

5. Mobile Espionage – APT37 (Reaper)

* Target: South Korean government officials, defectors, journalists
* Impact: Espionage and surveillance, not direct financial gain
* Method: Android spyware, phishing, zero-days
* Relevance: Demonstrates versatility of DPRK threat actors — from cybercrime to cyberespionage.

North Korea’s state-sponsored actors are among the most financially and politically motivated threat groups globally. They’re known for:

**Financial theft (APT38)**

**Destructive attacks (Lazarus)**

**Espionage (APT37)**

These attacks have shifted global cybersecurity policy and proven that fintech organizations are high-value targets.

**Most Dangerous Threat Actor to Fintech: APT38**

**APT38** – The Greatest Threat to Fintech

APT38, a North Korea-linked threat actor, stands out as the most relevant and dangerous to fintech institutions, especially banks and microfinance institutions, for the following reasons:

1. **Direct Targeting of Financial Systems**

Unlike many other groups that use generic phishing or ransomware, APT38 specifically targets the financial sector, focusing on:

Banking systems

Payment platforms

SWIFT networks.

This aligns directly with a state microfinance bank’s core operation.

2. **High-Impact, High-Skill Attacks**

APT38 is known for:

Stealing hundreds of millions through carefully planned attacks.

Bypassing financial controls, exploiting core banking apps, and manipulating transactions.

Using techniques like masquerading (T1036) and C2 exfiltration (T1041) to stay hidden for long durations.

3. **Sophisticated Reconnaissance and Persistence**

They are skilled at:

Infiltrating bank networks months in advance.

Living off the land with legitimate tools.

Using malware designed specifically for financial transactions and fund manipulation.

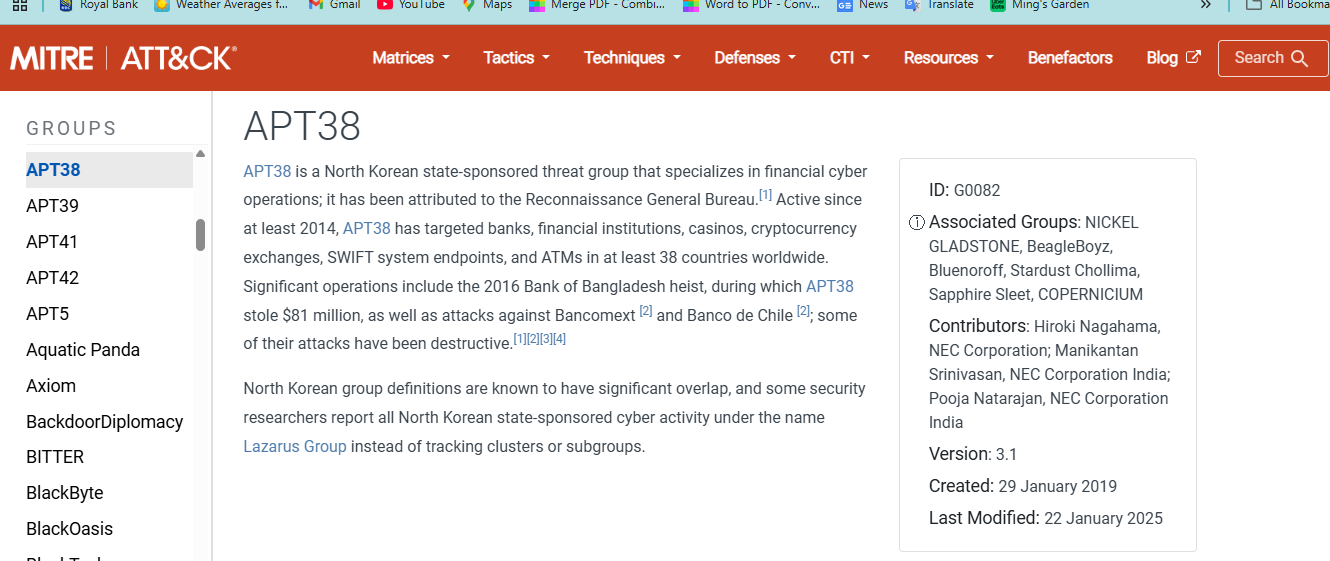
**APT38** is the greatest threat to Hapuna Financial Ltd or any fintech organization due to their:

Focused attacks on core banking infrastructure.

Deep knowledge of payment systems.

Proven history of successful, large-scale financial thefts.

More on Mitre ATT&CK MAPPING IN DETAILS HERE [LINK](https://attack.mitre.org/groups/G0082/)



**APT38 (North Korea) - MITRE ATT&CK Techniques**

| **Technique ID** | **Technique Name** | **Tactic Category** | **Description** |
| --- | --- | --- | --- |
| **T1036** | Masquerading | Defense Evasion | Spoofing the names or locations of files and processes to appear legitimate. |
| **T1041** | Exfiltration Over C2 Channel | Exfiltration | Transferring stolen data through an existing command-and-control channel. |
| **T1140** | Deobfuscate/Decode Files or Info | Defense Evasion | Decoding or unpacking files to execute or analyze them without detection. |
| **T1059** | Command and Scripting Interpreter | Execution | Execution of malicious code via PowerShell, Bash, or script interpreters. |
| **T1071** | Application Layer Protocol | Command and Control (C2) | Using common protocols like HTTPS, DNS for C2 traffic to evade detection. |
| **T1566.001** | Phishing: Spearphishing Attachment | Initial Access | Delivering malware through targeted email attachments to gain access. |
| **T1003** | OS Credential Dumping | Credential Access | Extracting stored passwords and hashes from memory or files. |
| **T1027** | Obfuscated Files or Information | Defense Evasion | Hiding malicious content using encoding, encryption, or compression. |

This table provides a comprehensive view of **APT38's** tactics and techniques, emphasizing how they:

Gain access through phishing,

Maintain stealth using obfuscation and masquerading,

Exfiltrate data through stealthy channels,

Execute malicious code while evading detection.

Their tools and actions remain hidden (T1036, T1140),

Data is exfiltrated without triggering standard outbound monitoring (T1041).

**Recommendations**

- Remove unnecessary exposure of email addresses on public sites.

- Apply SPF, DKIM, and DMARC on domains to prevent email spoofing.

- Regularly audit subdomain exposure and decommission unused ones.

- Use web application firewalls (WAFs) and VPNs to restrict access.

- Monitor public threat intelligence feeds for leaks associated with company domains.

### ****References****

MITRE ATT&CK Framework – Tactics, Techniques, and Procedures (TTPs)  
https://attack.mitre.org

Shodan Search Engine – Discovering exposed internet-connected devices  
<https://www.shodan.io>

AlienVault Open Threat Exchange (OTX) – Community-based threat intelligence  
https://otx.alienvault.com

Hunter.io – Email discovery and validation  
<https://hunter.io>

crt.sh (Certificate Transparency Log Search**)** – SSL/TLS certificate enumeration  
<https://crt.sh>

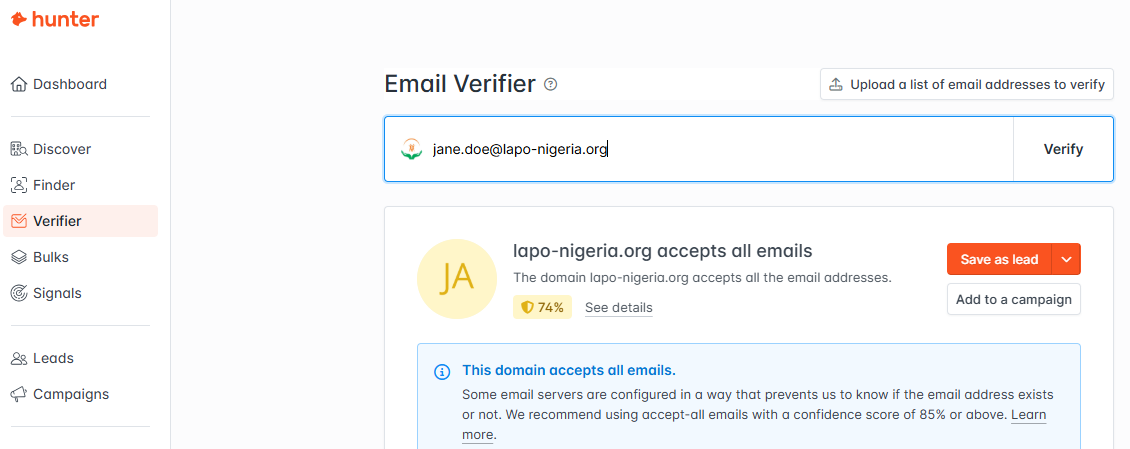
Have I Been Pwned – Breach and credential exposure database  
<https://haveibeenpwned.com>

VirusTotal Community – Threat detection from file, domain, and URL analysis  
<https://www.virustotal.com>

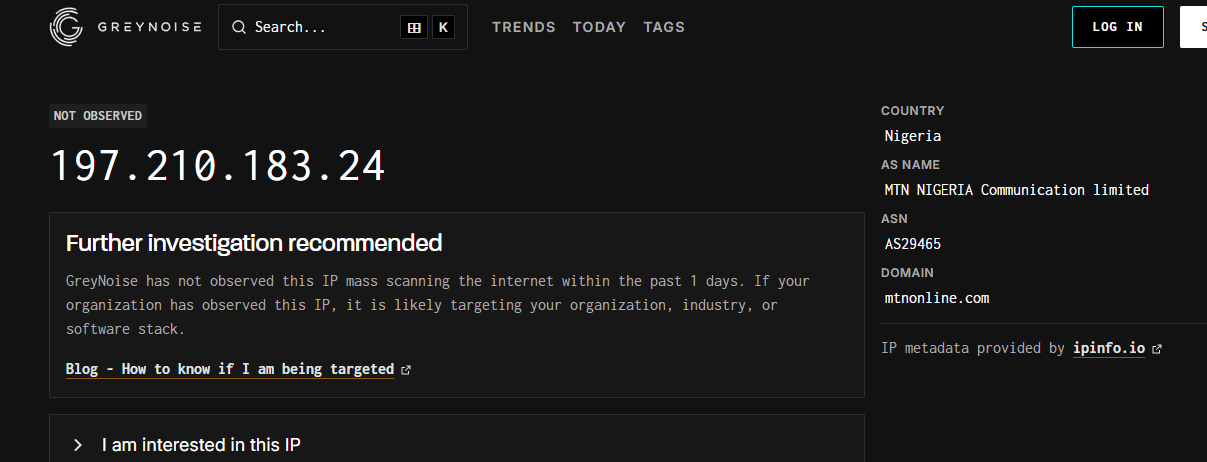
AbuseIPDB – IP reputation and abuse reports  
<https://www.abuseipdb.com>

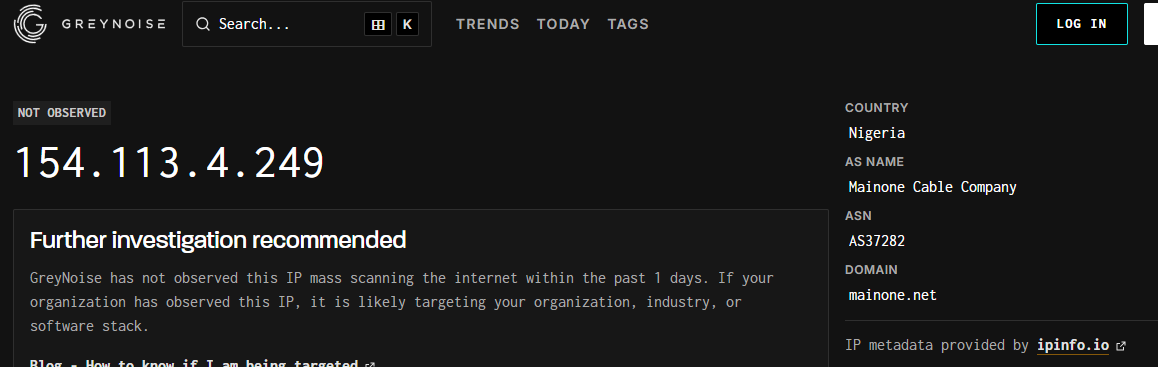
**Appendix: Screenshots and Visual Evidence**

**Figure 1: Hunter.io** – Used to identify valid and exposed corporate email addresses across public records and data breaches.

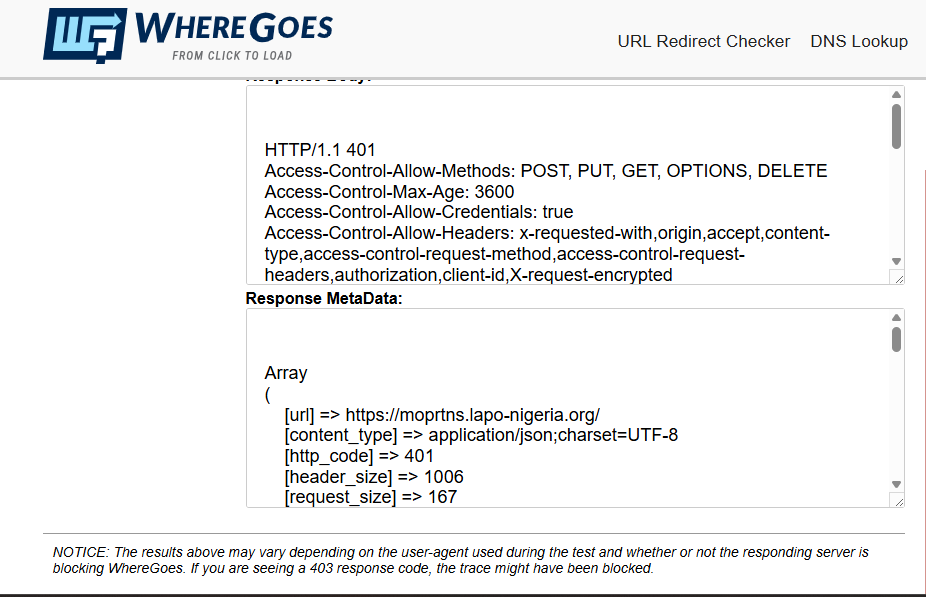


**FIGURE 2**: GREYNOISE: This finds out if an IP address is part of known scanning or botnet activity.

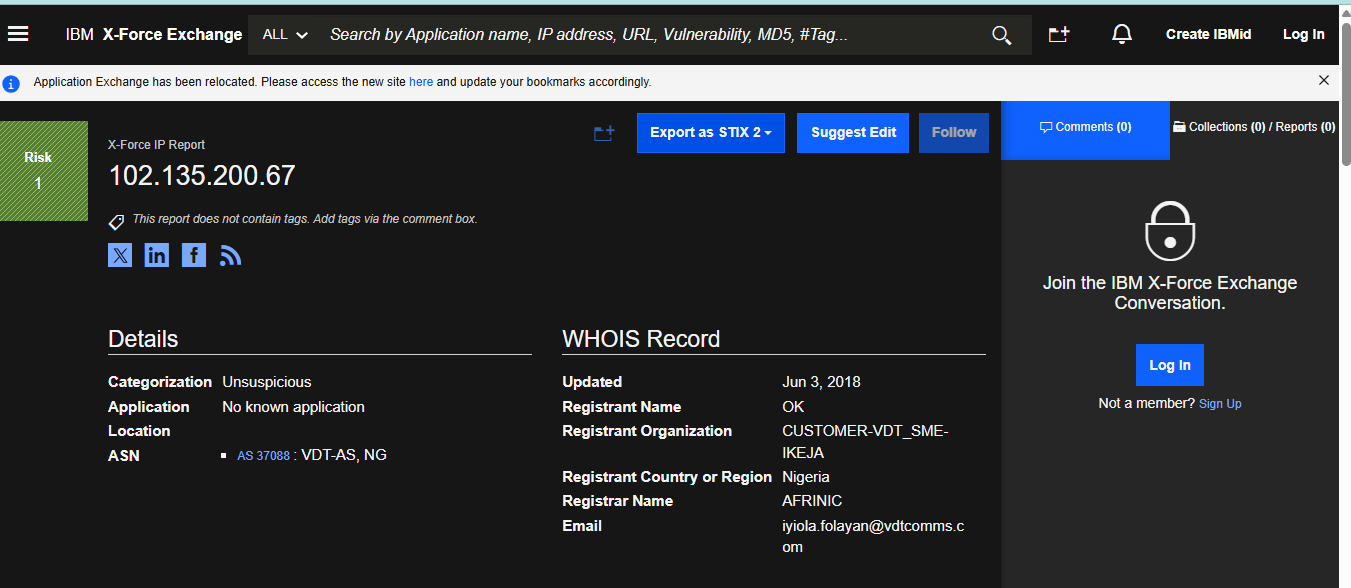




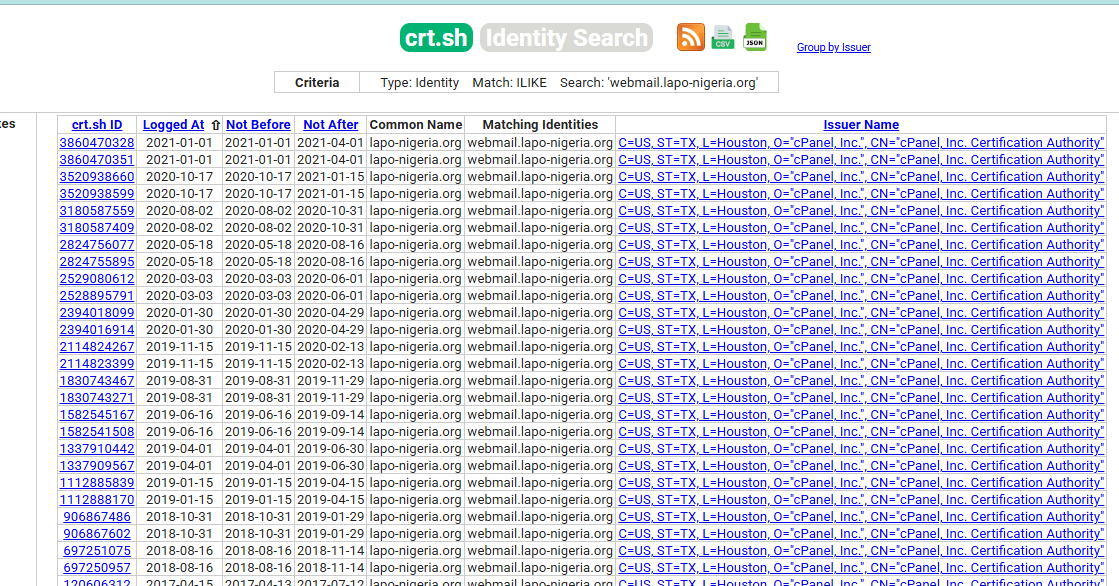
**FIGURE 3**. URL REDIRECT CHECKER: A **URL Redirect Checker** is a tool that **tracks and analyzes the full redirect path** of a URL. It shows you each hop the browser or HTTP client takes before reaching the final destination.



**FIGURE 4**: **WHOIS** is a protocol and database that provides information about **domain name registrations.**



**FIGURE 5:** Searched for SSL/TLS certificates issued to Hapuna subdomains, revealing additional infrastructure.



.