Threat Intelligence Investigation - Findings

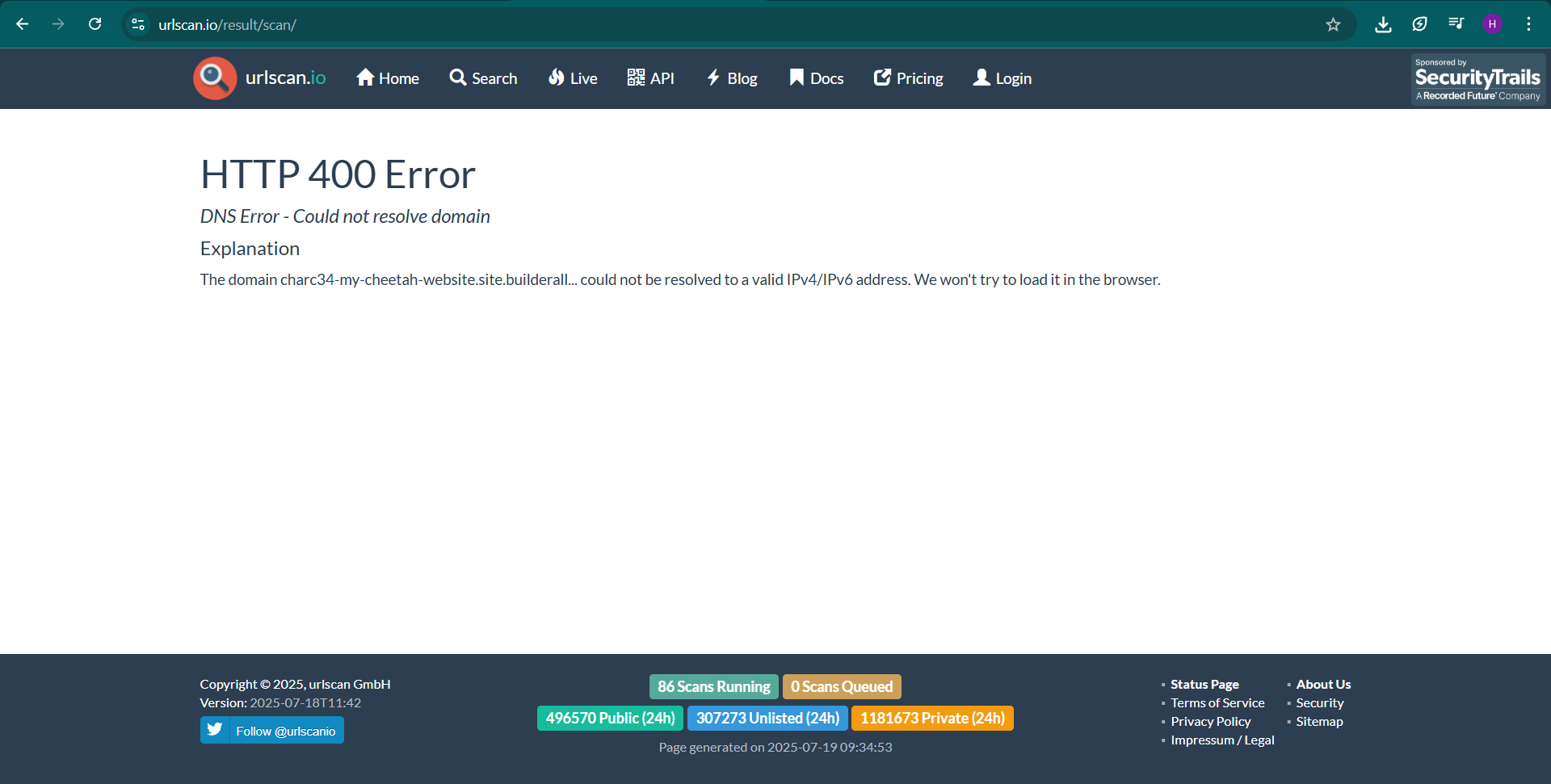
This document contains findings from the analysis of suspicious URLs using various open-source threat intelligence tools such as Urlscan.io, Abuse.ch, and Cisco Talos Intelligence.

# URL 1 Findings

1. **URL:** https://charc34-my-cheetah-website.site.builderall...

2. **Scan Tool:** Urlscan.io

3. **Scan Date:** 19-07-2025

4. **Key Findings:**  
 - DNS Error: Domain could not be resolved (likely removed or inactive).  
 - No IP address found.  
 - 

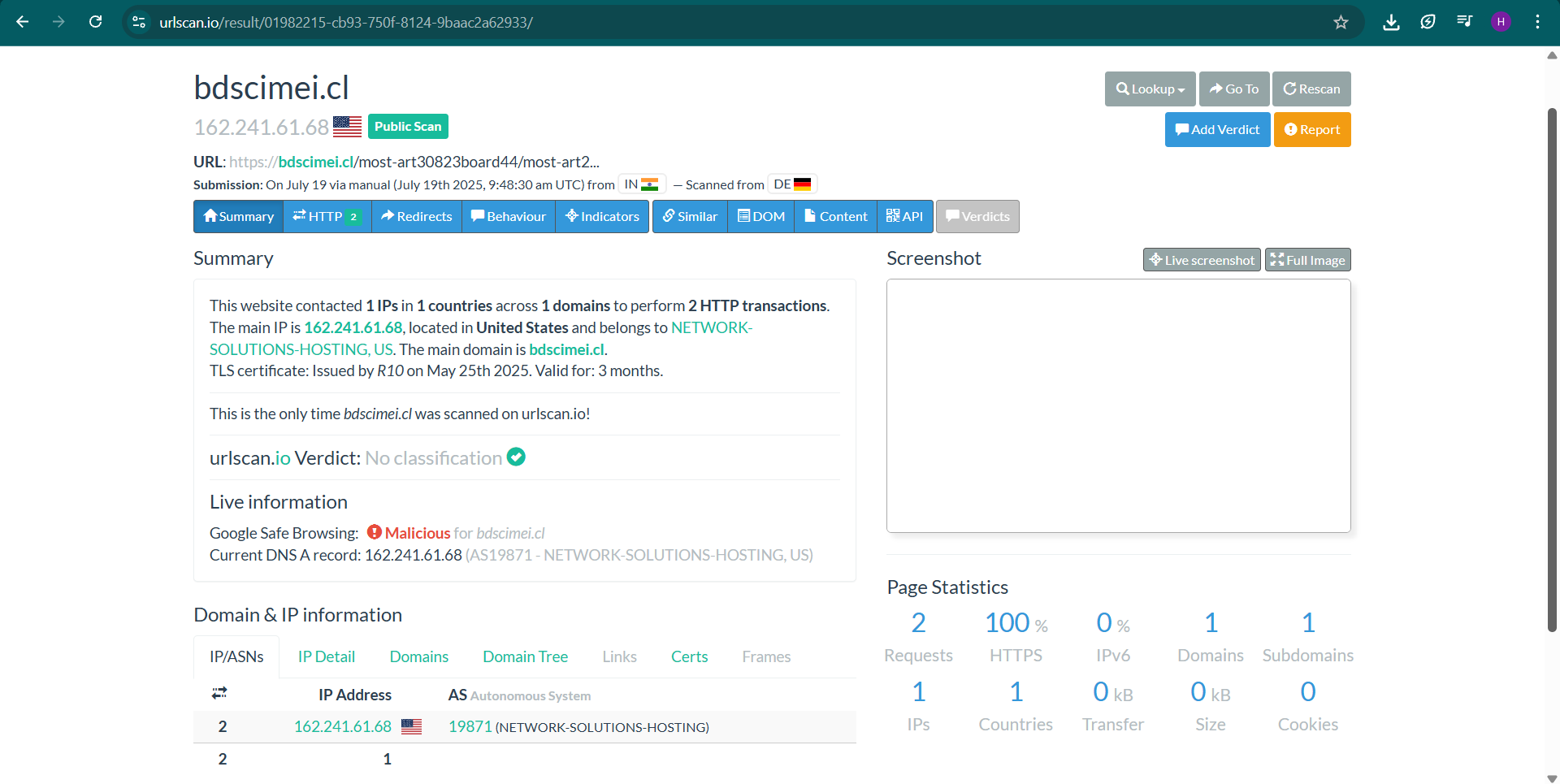
5. **Risk Level:** Unknown (inactive now, but previously flagged as phishing).

# URL 2 Findings

1**. URL:** https://bdscimei.cl/most-art30823board44/most-art2...

2. **Scan Tool:** Urlscan.io

3. **Scan Date**: 19-07-2025

4. **Key Findings:**  
 - IP Address: 162.241.61.68 (USA)  
 - ASN: AS19871 [Network Solutions Hosting]  
 - Verdict: Google Safe Browsing flagged it as Malicious.  
 

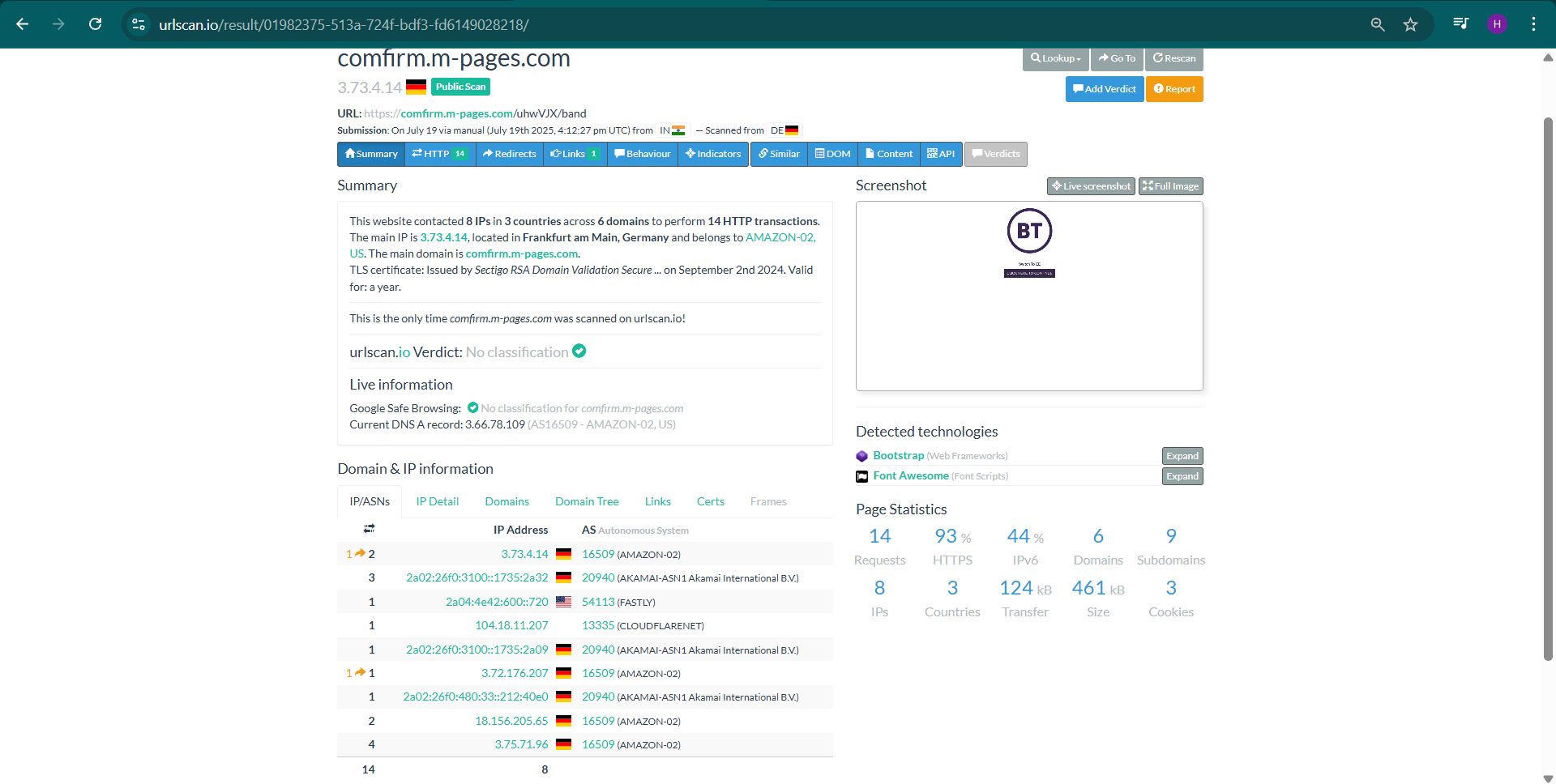
5. **Risk Level:** High

# URL 3 Findings

1. **URL:** https://comfirm.m-pages.com/uhwVJX/band

2. **Scan Tool:** Urlscan.io

3. **Scan Date:** 19-07-2025

4. **Key Findings:**  
 - IP Address**:** 3.73.4.14 (Frankfurt am Main, Germany)  
 - ASN: AS16509 (Amazon-02, US)  
 - Google Safe Browsing: No classification found (not flagged yet).  
 

5. **Risk Level:** Medium: (The site contacted multiple domains, which can be suspicious, but no direct malicious flag yet).

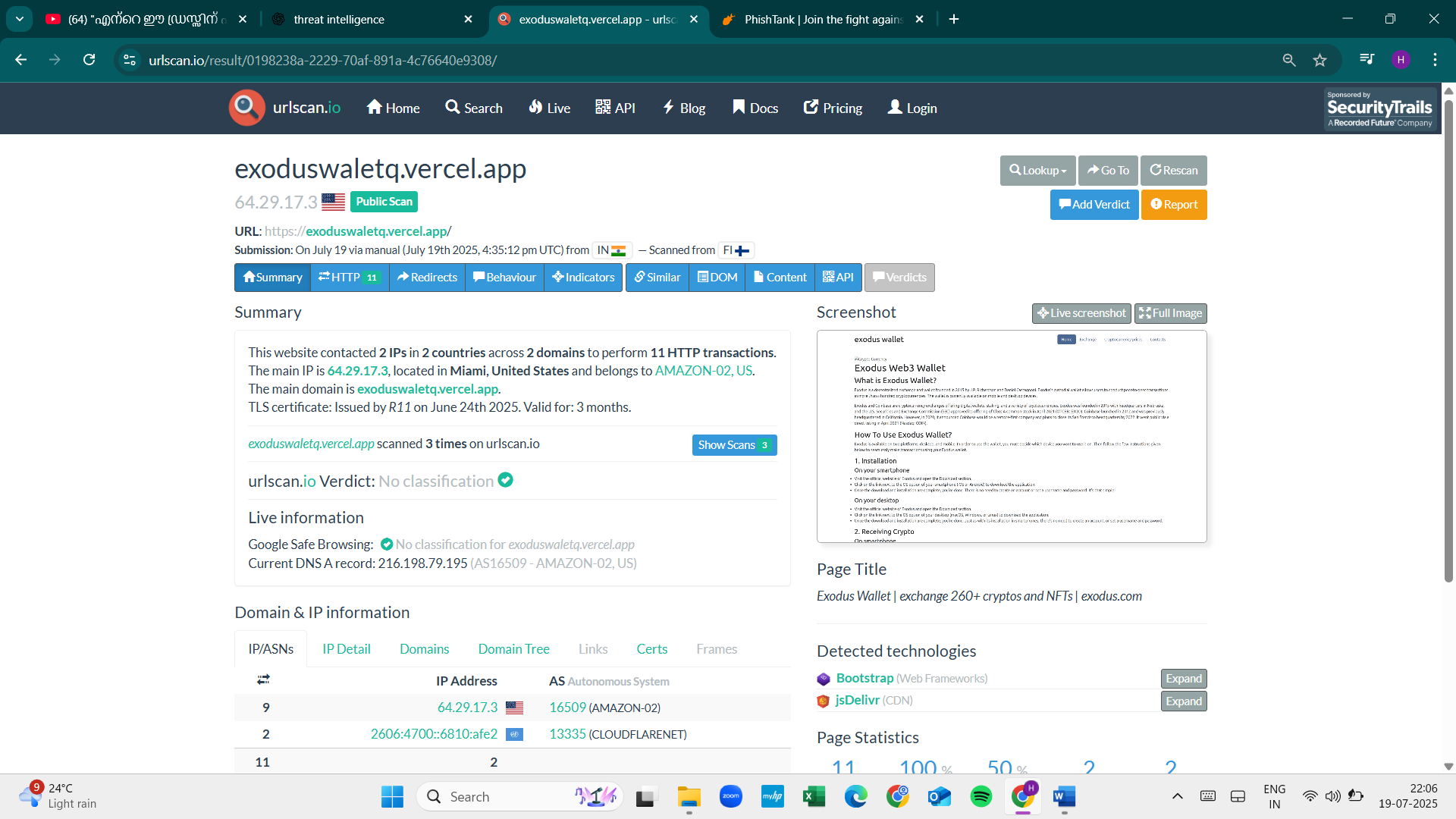
# URL 4 Findings

1. **URL:** https://exoduswaletq.vercel.app/

2. **Scan Tool:** Urlscan.io

3. **Scan Date:** 19-07-2025

4. **Key Findings:**  
 - IP Address: 64.29.17.3 (Miami, USA  
 - ASN**:** AS16509 (Amazon-02)  
 - Google Safe Browsing: No classification yet.



5. **Risk Level:** Medium (Suspicious name "exoduswallet," might be targeting cryptocurrency users).

# URL 5 Findings

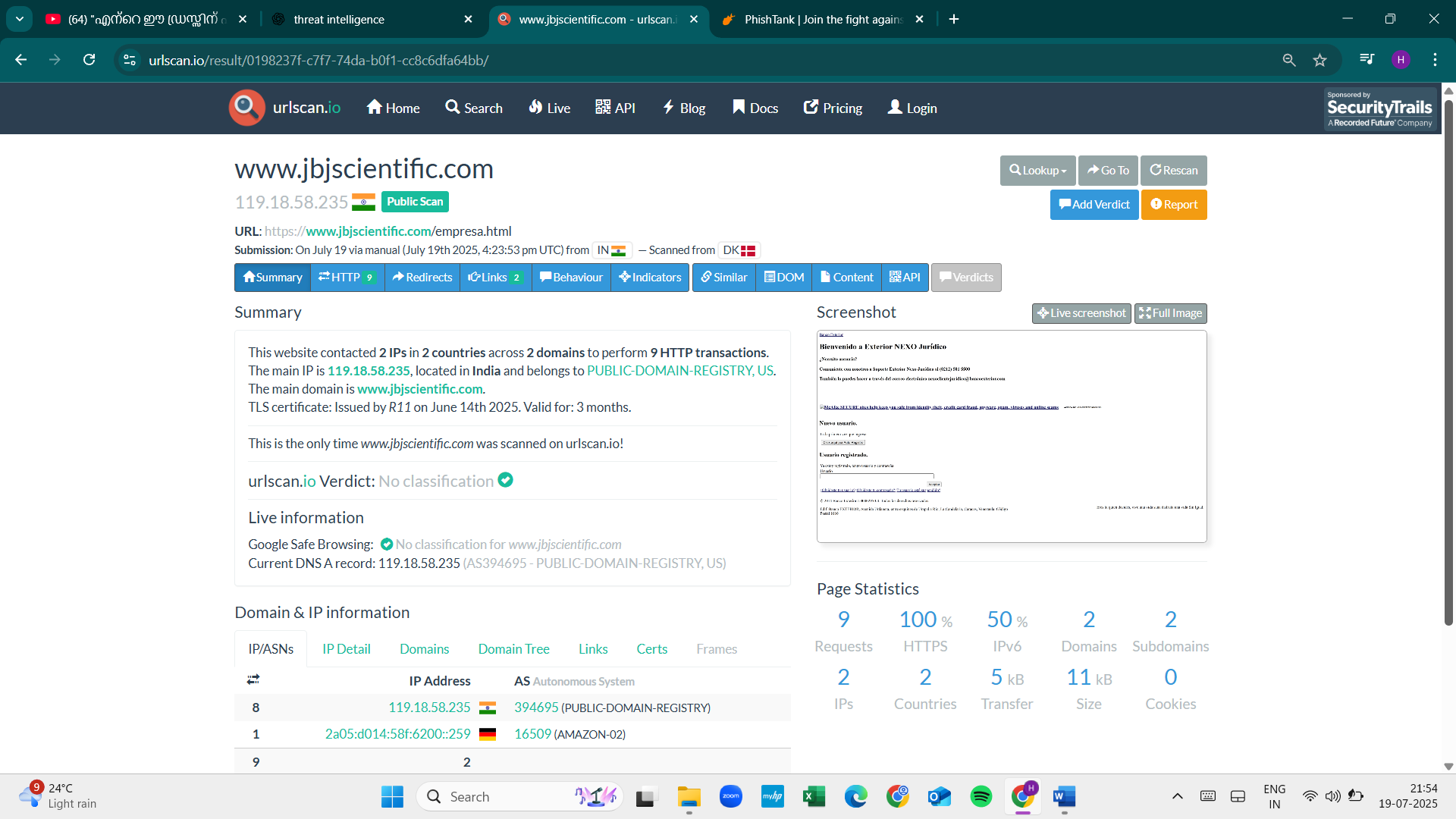
1. **URL:** https://www.jbjscientific.com/empresa.html

2. **Scan Tool:** Urlscan.io

3. **Scan Date:** 19-07-2025

4. **Key Findings:**  
 - IP Address: 119.18.58.235 (India)  
 - ASN: AS394695 (Public Domain Registry, US)

- Google Safe Browsing: No classification yet.



5. **Risk Level:** Medium (not flagged but suspicious domain behavior).

| **S.No** | **URL (From PhishTank)** | **IP Address** | **ASN** | **Google Safe Browsing Verdict** | **Risk Level** |
| --- | --- | --- | --- | --- | --- |
| 1 | https://charc34-my-cheetah-website.site.builderall... | N/A (Domain not resolved) | N/A | Could not resolve | Low (inactive domain) |
| 2 | https://bdscimei.cl/... | 162.241.61.68 (US) | AS19871 (Network Solutions Hosting) | **Malicious** | **High** |
| 3 | https://confirm.m-pages.com/... | 3.73.4.14 (Germany) | AS16509 (Amazon-02) | No classification | Medium |
| 4 | https://www.jbjscientific.com/... | 119.18.58.235 (India) | AS394695 (Public Domain Registry) | No classification | Medium |
| 5 | https://exoduswaletq.vercel.app/... | 64.29.17.3 (US) | AS16509 (Amazon-02) | No classification | Medium |

**Conclusion**

From the analysis of 5 suspicious URLs (collected from PhishTank) using **Urlscan.io**, the following findings were observed:

* **1 URL was flagged as malicious** by Google Safe Browsing.
* **Most domains exhibited suspicious behavior**, such as contacting multiple IPs or being linked to cloud hosting services often misused for phishing.
* **Short-lived TLS certificates** (3 months) were commonly found, which is typical of phishing sites.
* **Risk levels** were assigned based on malicious verdicts, domain behavior, and hosting information.