Incident Analysis Report

1. Alarm Information

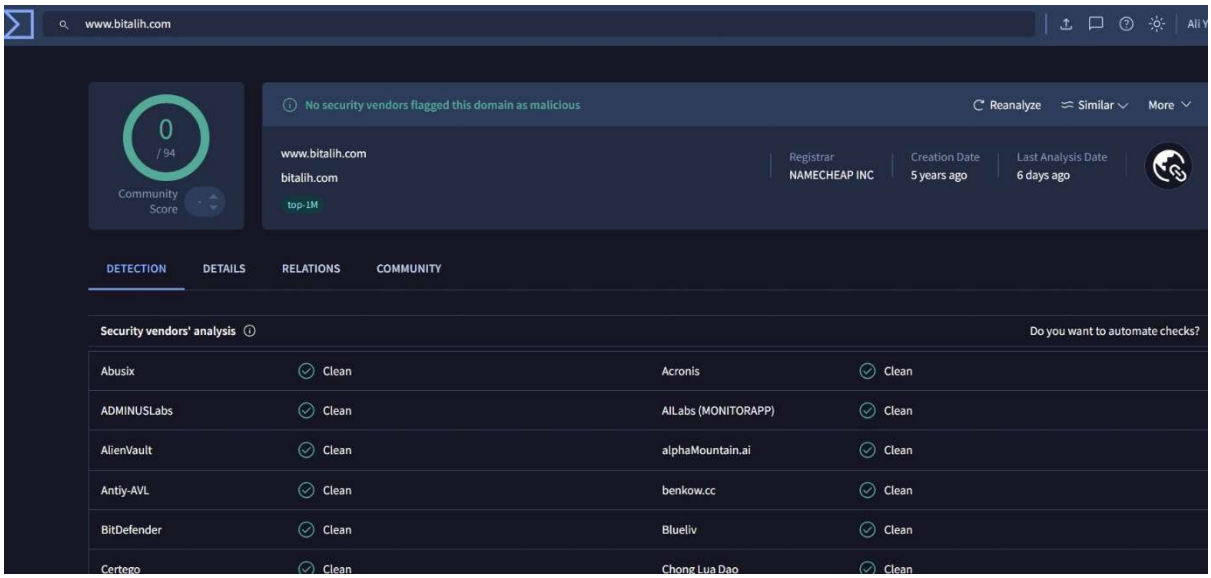
- **Alarm ID / Case No:** 007
- **Alarm Source:** SIEM / IDS
- **Alarm Description:** Access to Gambling Website Detected – www[.]bitalih[.]com
- **Timestamp:** [e.g., 2025-08-24 13:20 CET]

2. IOC Information

- **IOC Type:** www[.]bitalih[.]com
- **IOC Value:** www[.]bitalih[.]com
- **IOC Location:** [USA]

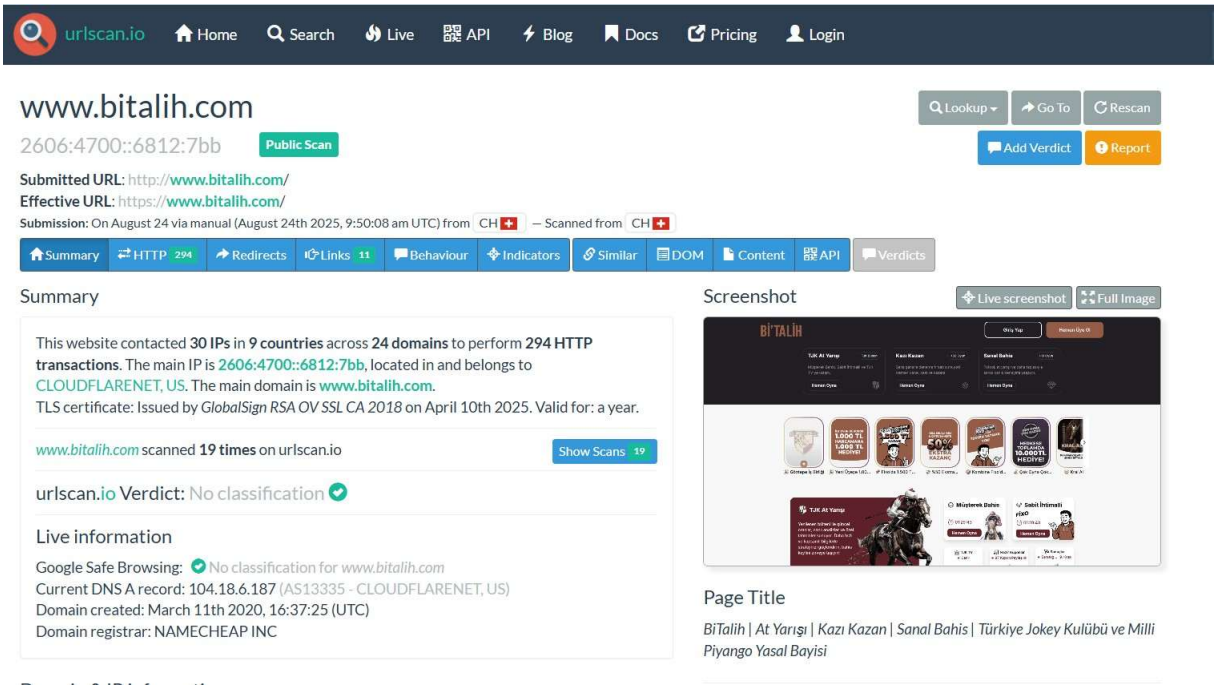
3. OSINT Investigation

VirusTotal

- Result: Detected by 1 AV engine (low confidence).
- https://www.virustotal.com/gui/domain/www.bitalih.com
- 

URLscan.io

- Result: No malicious classification, website considered clean.
- https://urlscan.io/result/0198db7c-3b95-71a8-973d-02a4bebebb3d/



-

4. Analysis & Assessment

- VirusTotal result alone is weak evidence.
- URLscan.io No malicious classification, website considered clean.

5. Conclusion / Decision

- **Decision:** ✅ **False Positive No Threat Detected**
- **Category:** Access to Gambling Website Detected
- **Risk Level:** None (based on organization's classification)

---

6. Recommended Actions

1. Block the IP address on firewall / IPS.
2. Review SIEM logs for additional login attempts from the same source.
3. Correlate failed logins with user accounts for potential compromise attempts.
4. Consider implementing automated blocking rules for IPs with high abuse scores.