

# 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>

Vendor	Result	Notes
Abusix	Clean	
ADMINUSLabs	Clean	
AlienVault	Clean	
Anti-AVL	Clean	
BitDefender	Clean	
Certego	Clean	
Acronis	Clean	
AI Labs (MONITORAPP)	Clean	
alphaMountain.ai	Clean	
benkow.cc	Clean	
Blueliv	Clean	
Chong Lua Dao	Clean	

### URLscan.io

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

The screenshot shows the URLscan.io interface for the domain [www.bitalih.com](http://www.bitalih.com/). Key details from the analysis include:

- Submitted URL:** <http://www.bitalih.com/>
- Effective URL:** <https://www.bitalih.com/>
- Submission:** On August 24 via manual (August 24th 2025, 9:50:08 am UTC) from CH (Switzerland) — Scanned from CH (Switzerland)
- Summary:** This website contacted 30 IPs in 9 countries across 24 domains to perform 294 HTTP transactions. The main IP is 2606:4700::6812:7bb, located in and belongs to CLOUDFLARENET, US. The main domain is [www.bitalih.com](http://www.bitalih.com).
- TLS certificate:** Issued by GlobalSign RSA OV SSL CA 2018 on April 10th 2025. Valid for: a year.
- Scans:** www.bitalih.com scanned 19 times on urlscan.io. [Show Scans 19](#)
- Verdict:** No classification (green checkmark)
- Live information:**
  - Google Safe Browsing: [No classification for www.bitalih.com](#)
  - Current DNS A record: 104.18.6.187 (AS13335 - CLOUDFLARENET, US)
  - Domain created: March 11th 2020, 16:37:25 (UTC)
  - Domain registrar: NAMECHEAP INC

## 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.