

Incident Analysis Report

1. Alarm Information

- **Alarm ID / Case No:** 008
- **Alarm Source:** SIEM / IDS
- **Alarm Description:** Access to Gambling Website Detected – temp.sh
- **Timestamp:** [e.g., 2025-08-24 13:20 CET]

2. IOC Information

- **IOC Type:** temp.sh
- **IOC Value:** temp.sh
- **IOC Location:** [France]

3. OSINT Investigation

VirusTotal

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

URLscan.io

- Result: No malicious classification, website considered clean.
- <https://urlscan.io/result/0198db81-bc4f-7085-a0c3-8267b7db6c59/>

The screenshot shows the urlscan.io interface for the URL <http://temp.sh/>. The main header includes links for Home, Search, Live, API, Blog, Docs, Pricing, and Login. Below the header, the URL is displayed as 51.91.79.17 with a red flag icon and a 'Public Scan' button. The submission details show it was submitted on August 24, 2025, from CH (Switzerland) and scanned from FR (France). The navigation bar below the header includes Summary, HTTP (2), Redirects, Links (4), Behaviour, Indicators, Similar, DOM, Content, API, and Verdicts.

Summary:

- This website contacted 1 IPs in 1 countries across 1 domains to perform 2 HTTP transactions.
- The main IP is 51.91.79.17, located in France and belongs to OVH OVH SAS, FR. The main domain is temp.sh.
- TLS certificate: Issued by E5 on August 19th 2025. Valid for: 3 months.

Verdict: [temp.sh](#) scanned 767 times on urlscan.io [Show Scans 767](#)

Live information:

- Google Safe Browsing: [No classification for temp.sh](#)
- Current DNS A record: 51.91.79.17 (AS16276 - OVH OVH SAS, FR)

Screenshot: A preview of the website's content, which appears to be a temporary file upload page for [Temp.sh | Temporary File Upload](#).

4. Analysis & Assessment

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

5. Conclusion / Decision

- **Decision:** [True Positive](#)
- **Category:** Access to Gambling Website
- **Risk Level:** Low (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.