

Incident Analysis Report

1. Alarm Information

- **Alarm ID / Case No:** 005
- **Alarm Source:** SIEM / IDS
- **Alarm Description:** Phishing from t.co/ElqtWuBpW6
- **Timestamp:** [e.g., 2025-08-24 13:20 CET]

2. IOC Information

- **IOC Type:** t.co/ElqtWuBpW6
- **IOC Value:**
- **IOC Location:** [unknown]

3. OSINT Investigation

VirusTotal

- Result: Detected by 1 AV engine (No confidence).
- <https://www.virustotal.com/gui/url/715a463d18f652e0f461ac2f73baf6ea7d673005de01d49c53ce339b8717ae2a/detection>

The screenshot shows the VirusTotal analysis page for the URL https://twitter.com/safety/unsafe_link_warning?unsafe_link=https://animaldiscoveries.click/wp-admin/xxx/link.html. The page displays the following information:

- Community Score:** 0 / 97
- Detections:** 1 LOW 1 (Crouching Yeti: Appendices)
- Details:** No security vendors flagged this URL as malicious.
- URL:** https://twitter.com/safety/unsafe_link_warning?unsafe_link=https://animaldiscoveries.click/wp-admin/xxx/link.html
- Status:** 200
- Content type:** text/html; charset=utf-8
- Last Analysis:** 1 day ago
- Crowdsourced context:** HIGH 0, MEDIUM 0, LOW 1, INFO 0, SUCCESS 0
- Security vendors' analysis:**
 - Abusix: Clean
 - Acronis: Clean
 - AllLabs (MONITORAPP): Clean

AbuseIPDB

- Result: no reports

- <https://www.abuseipdb.com/check/199.45.154.176>

4. Analysis & Assessment

- VirusTotal result not found.
- AbuseIPDB result not found.

5. Conclusion / Decision

- **Decision:**  **False Positive**
 - **Category:** Phishing
 - **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.