Security Incident Analysis Report: Smishing Attempt Investigation

1. Incident Summary

On February 25, 2025, at 16:22, a suspicious SMS was received by a user(myself), claiming to be a delivery notification that required immediate action. The message included a link (hxxp://intpro[.]icu) prompting the user to update their delivery location within 12 hours to avoid order cancellation. Given the urgency and unknown sender, an investigation was conducted to determine if this was a **SMS phishing** (**smishing) attack**.

2. Threat Identification

- **Message Content:**

  "Kindly update your delivery location within 12 hours, otherwise we will proceed to return the product."

- **Sender Details:** Random mobile number, not associated with any known delivery service.
- **Suspicious URL:** hxxp://intpro[.]icu
- **Timestamp:** February 25, 2025, at 16:22
- **Attachments:** None

Red Flags:

1. **Urgency Tactic:** Threatens order return within 12 hours to force immediate action.
2. **Unknown Sender:** Uses a random mobile number instead of an official company name.
3. **Suspicious URL:** Domain does not match any known delivery service.
4. **Newly Registered Domain:** Created on the same day of the SMS received.

3. Technical Analysis

To verify if the URL was malicious, the following tools were used:

Tool	Findings
VirusTotal	1 vendor flagged the URL as malicious
URLScan.io	- The site contacted 68 IPs across 8 countries - Performed 282 HTTP transactions, indicating aggressive tracking - Primary domain resolves to stockx.com (potential impersonation)
Whois Lookup	- Domain created on the same day (Feb 25, 2025) - Registered with Gname.com, linked to spam domains - Uses generic DNS servers (SHARE-DNS)

Final Conclusion: The URL is likely a phishing site, designed to steal user credentials or distribute malware.

4. Potential Impact

If a victim clicks the link and enters their details:

1. **Credential Theft** – Attackers could steal personal or banking information.
2. **Malware Installation** – The website could trigger downloads of malicious software.
3. **Financial Loss** – If payment details are entered, they could be misused.

5. Mitigation & Recommendations

For End Users:

- Do NOT click unknown links in SMS messages.
- Verify deliveries directly with the e-commerce or courier service.
- Report smishing messages to mobile carriers and security teams.

For Security Teams (SOC/IT):

- Blacklist the phishing URL in email/SMS security filters.
- Monitor network traffic for access attempts to intpro[.]icu.
- Conduct awareness training on social engineering attacks.

6. Conclusion

Through structured analysis, we confirmed that this SMS was a **smishing attack** attempting to deceive users into clicking a phishing link. The **newly registered domain, suspicious HTTP activity, and malicious reputation** confirm that the link is **dangerous**.

Final Verdict: Malicious – Users should avoid this link and report the SMS immediately.