Phishing Domain & Malicious URL Investigation Report

Suspicious URL: hxxp://www.info-resmi888.blogspot[.]com/login
Abused Subdomain: info-resmi888.blogspot[.]com
Parent Domain: blogspot.com (Legitimate – Google Blogger)
Hosting Platform: Blogspot (Google Blogger)
Resolved IP Address: 192.178.155.132
ASN: AS15169 – Google LLC
Threat Type: Phishing (Credential Harvesting)

Domain Context
The parent domain blogspot.com is a legitimate and long-established domain owned by Google. The phishing activity originates from a user-created subdomain, which does not require domain registration. Threat actors commonly abuse free and trusted hosting platforms to host phishing pages.

DNS & Hosting Analysis
DNS analysis revealed that the phishing URL resolves to IP address 192.178.155.132, which belongs to Autonomous System AS15169 operated by Google LLC. The content is hosted on Blogspot, a shared blogging platform. Due to the use of shared Google infrastructure, direct attribution of the hosting IP to the threat actor is not possible. Such platforms are frequently abused by attackers to host phishing pages while leveraging the trust associated with legitimate services.

VirusTotal Analysis
Detection Ratio: 15 / 93
Categories: Phishing, Malicious, Suspicious

Conclusion
Based on OSINT analysis, the investigated URL exhibits strong indicators of phishing activity and is likely intended for credential harvesting.