GRC RISK REPORT

Case Study

Hidden Communication via PNG Steganography in CTF Challenge "Stepic"

Report ID: GRC-2025-STEG-001

Date: 28 July 2025

Prepared by: Divyanshu Kumar

Confidentiality Level: Internal – For Security & Awareness Use

1. Executive Summary

This report investigates a simulated security incident based on the "Stepic" CTF forensics challenge. The scenario demonstrates how a seemingly benign PNG image can be used to covertly transmit secret data via LSB (Least Significant Bit) steganography, bypassing traditional file inspection and forensic methods.

Such covert techniques highlight the growing sophistication of data exfiltration methods and emphasize the importance of incorporating advanced analysis tools and awareness in modern cybersecurity governance. This report maps the identified risks and controls against ISO/IEC 27001 and CERT-In frameworks.

2. Incident Description

Attack Vector:

LSB steganography embedded in upz.png using Stepic, a Python-based steganography library.

Scenario Simulated:

A potential insider or adversary shares a PNG file containing a hidden message (flag) through an image-sharing channel. The image successfully evades traditional DLP and forensic tools like strings, exiftool, binwalk, steghide, zsteg, etc.

Detection Gap:

PNG files, though common, are unsupported by many default stego tools (e.g., Steghide doesn’t support PNG). This creates a blind spot for organizations that rely only on metadata or format-specific inspection.

Outcome in Simulation:

Secret flag was successfully extracted using:

```
pip install stepic
python3
 import stepic
 from PIL import Image
 img = Image.open("upz.png"
 hidden_data = stepic.decode(img)
 print(hidden_data)
```

3. Risk Analysis

Attribute	Description
Asset at Risk	Confidential messages, intellectual property, sensitive operational data
Threat Agent	Insider, external adversary, or malicious attacker with access to uploads
Vulnerability	Absence of deep steganalysis tools; trust in standard forensic routines
Impact (I)	High – Secret data exfiltration or command & control can go undetected
Likelihood (L)	Medium – Most orgs do not scan all images for LSB steganography
Overall Risk (IxL)	High

4. ISO 27001 & CERT-In Control Mapping

Framework	Control Reference	Title/Requirement
ISO 27001	A.8.23	Use of Secure Communication Channels
ISO 27001	A.6.5	Information Security Awareness & Training
ISO 27001	A.5.9	Threat Intelligence
ISO 27001	A.5.27 / A.5.28	Security Event Response & Management
CERT-In	Section 2(e)	Reporting of incidents involving data exfiltration
CERT-In	Section 4	Maintain forensically sound logs (180 days)

5. Root Cause Analysis

a) Lack of advanced steganalysis and DPI (Deep Packet Inspection) for image uploads.

b) Over-reliance on traditional file inspection tools (which do not support PNG LSB extraction).

c) Absence of user training regarding covert communication channels and file anomalies.

d) No automated alerts for anomalous file sizes or upload patterns.

6. Remediation Plan

Action Item	Priority	Owner
Integrate steganalysis (LSB & format-aware) tools	High	IT Security
Conduct specialized user awareness on covert channels	High	Security Training
Tune SIEM for large/abnormal image upload/downloads	Medium	SOC
Actively monitor upload endpoints for suspicious files	Medium	IT Security
Develop incident response for steganography incidents	High	IR Team

7. Policy & Compliance Recommendations

a) Update digital asset and media upload policies to include mandatory steganalysis scans for high-risk channels.

b) Add covert channel threats (steganography, protocol tunneling) to periodic security awareness and tabletop exercises.

c) Document findings and risks in the ISMS Risk Register.

d) Ensure incident reporting mechanisms capture covert exfiltration or C2 scenarios.

8. Conclusion

The "Stepic" challenge reveals a potent blind spot for many security programs: image-based steganography. Organizations should enhance their GRC posture by adopting advanced detection tooling, strengthening user awareness, and rigorously applying controls aligned to ISO 27001 and CERT-In guidelines. Failure to address such risks could result in undetected data loss or weaponization of innocent files for adversarial purposes.