

|  |
| --- |
| Research Paper : DeceptiSense – A Cybersecurity Decoy Detection System |
|  |
| May 13  Institution : Mulund College of Commerce Affiliation: Digisuraksha Parhari Foundation  Authored by: Aarya Ghosalkar |

Title: DeceptiSense – A Cybersecurity Decoy Detection System

1. Abstract

DeceptiSense is a lightweight, stealthy cybersecurity deception tool designed to detect and alert on unauthorized access attempts through decoy file monitoring. The system creates realistic-looking decoy documents with embedded tracking links. When accessed by a potential intruder, these decoys silently trigger an alert mechanism via SMS, providing information such as IP address and device location. This tool simulates real data traps to enhance security visibility in both personal and enterprise environments.

2. Introduction

Cyber threats have evolved, and attackers often bypass traditional antivirus or firewall protections. DeceptiSense leverages a proactive deception strategy by deploying bait files (decoys) that appear genuine but are monitored for interaction. The primary goal is to detect intrusions early, even before any damage is done.

3. Objectives

• Design a system to create realistic decoy documents.

• Trigger an alert whenever the decoy is accessed.

• Send alert details via SMS including IP and location.

• Operate in stealth mode without alerting the attacker.

• Ensure persistence (running even after reboot).

4. Tools & Technologies Used

|  |  |
| --- | --- |
| Technology | Purpose |
| Python | Core programming |
| Flask | Backend server (beacon trap) |
| Twilio API | SMS alerts |
| docx (python-docx) | Decoy file generation |
| Windows VBS | Stealth startup automation |
| IPinfo API | IP-based geolocation |

5. System Architecture

Step 1: Generate a decoy Word document with a hyperlink.

Step 2: Run a Flask server silently in the background.

Step 3: When the hyperlink is clicked, it sends a GET request.

Step 4: Flask receives the beacon and triggers the SMS alert.

Step 5: The system logs the attacker’s IP address and approximate location.

6. Modules

a) decoy\_generator.py

• Creates a Word document with professional layout.

• Embeds a hyperlink labeled “Click here”.

b) app.py

• Lightweight Flask server that receives beacon hits.

• Extracts and logs attacker IP and location.

c) sms\_alert.py

• Uses Twilio API to send an alert message.

• Includes timestamp, IP, and location.

d) Stealth Mechanism (VBS script)

• Ensures app.py runs in the background on every startup.

• Eliminates need to open terminal manually.

7. Implementation Screenshots

• Decoy document appearance

• Flask terminal logs

• SMS alert received on phone

• IP/location info

• Folder structure of project

8. Results

• Successfully received SMS alert when decoy was accessed.

• Logged attacker’s IP and estimated location.

• Verified persistence after reboot (Flask auto-started).

• No user-visible terminal windows (runs silently).

9. Challenges Faced

• Embedding clickable hyperlinks in .docx with formatting.

• Sending SMS without exposing credentials.

• Hiding Python execution from attacker.

• Location accuracy limited to IP-based services.

10. Future Scope

• Add email alert integration.

• Capture device details like OS fingerprint.

• Extend to decoy spreadsheets or PDFs.

• Deploy across enterprise machines using GPO.

11. Conclusion

DeceptiSense offers a practical and powerful way to detect unauthorized file access. By integrating deception, automation, and real-time alerts, it enhances security visibility and provides an early warning system for potential intrusions. It’s lightweight, non-intrusive, and effective.

12. References

• https://twilio.com/docs/sms

• https://python-docx.readthedocs.io

• https://flask.palletsprojects.com/

• https://ipinfo.io/