DECEPTISENSE

(BASED ON DECEPTI CONCEPT IN CYBERSECURITY)

BY:- AARYA GHOSALKAR

https://github.com/AaryaGhosalkar/DECEPTISENSE

What is DeceptiSense?

DECEPTISENSE is a cybersecurity deception tool that embeds hidden tracking mechanisms into decoy documents.

When a malicious user interacts with the decoy (e.g., clicking a hidden link), it triggers an alert system that:

- Logs the interaction via a local web beacon
- Sends a real-time SMS alert via Twilio
- Collects potential forensic intelligence

This enables early breach detection without relying on conventional signature-based defenses.

What is Twilio?

Twilio is a cloud communication platform that allows software developers to programmatically send and receive messages, phone calls, emails, and more.
In the context of DECEPTISENSE:

- Twilio is used to send instant SMS alerts when the decoy link is accessed.
- The alert contains information like:

1. The decoy ID (decoy1)
2. Timestamp of access

- This enables real-time threat detection, even when you’re away from the system.

How DECEPTISENSE Works

DECEPTISENSE is built using three key Python modules working together to deliver real-time detection and alerting:

1. decoy_generator.py
   - Generates a Word document embedded with a hidden link:
   - http://localhost:5000/beacon?id=decoy1
   - Can be seeded in cloud drives, emails, or network shares.

2. app.py (Beacon Server)
   - Runs a Flask web server on a secure channel (VPN or local network).
   - Listens for requests to the beacon URL.
   - When triggered, it:
     - Logs the request
     - Calls the SMS alert function
     - Displays a confirmation page (“Tracked on Webpage”)

3. sms_alert.py
   - Contains the logic to send SMS alerts using Twilio.
   - Called by app.py whenever a decoy is accessed.
   - Sends attacker ID, time, and decoy name to your phone.

Why Would the Market Love This?

- Proactive Defense: Detects attackers before damage is done.
- Low False Positives: Unlike traditional tools, any interaction with the decoy is almost certainly malicious.
- Cost-Effective: Runs locally and uses inexpensive cloud communication (Twilio).
- Integration-Ready: Can be embedded in email attachments, internal shares, or honeypots.
- Intelligence Gathering: Reveals attacker behavior and entry vectors.

Importance in Today's Cybersecurity Landscape

In a world where perimeter-based security is no longer sufficient:

- Insider Threats are rising.
- Zero-Day Exploits bypass firewalls and AV.
- Traditional SIEMs are noisy and slow to respond.

DECEPTISENSE fits into Zero Trust and Deception Technology frameworks, offering a lightweight, fast, and reliable alert system.

Technologies Used

- Python Flask (backend server)
- Twilio (SMS alerting)
- HTML (embedded in the fake document)
- Localhost server simulation
- Microsoft Word or similar editor for decoy crafting

Future Enhancements

- Use ngrok or a VPS to make the beacon globally accessible.
- Log attacker IP, browser info, and geo-location.
- Email alerts, Discord bots, or Slack integration.
- Multiple beacon types: image, JS, or iframe traps.
- Dashboard for activity monitoring.

Summary

- DECEPTISENSE turns the table on attackers.
- Simple but effective alerting system.
- Real-time response improves reaction time.
- Scalable and adaptable to many environments.

THANK YOU