



"Keylogger: Un vistazo al lado oscuro del teclado"

Autor: Steven Vallejo Sacoto

Carrera: Tecnología Superior en Ciberseguridad

Docentes: Boris Suquilanda, Marcelo Monteros, Fabián Chuqui

Fecha: 17 de febrero de 2025

Introducción



¿Cuál es el propósito de este proyecto y de qué trata?

Objetivos



Objetivo principal:

Desarrollar una aplicación con keylogger en Android que capture las pulsaciones del teclado con fines educativos.

Objetivos específicos

1. Concientizar e informar a los usuarios.

2. Desarrollar aplicativo keylogger con datos que se compila en un servidor

3. Crear un correo malicioso con ingeniería social que permite distribuir la aplicación simulada.

4. Demostrar cómo funciona un keylogger en un dispositivo Android y analizar el impacto potencial de este tipo de malware.

Justificación

Relevancia del estudio: Relación con Ciberseguridad en la nube, Continuidad del negocio y Ciberseguridad en Tecnologías y Sistemas de información.

Beneficio educativo: Simulación de ataques para alertar al consumidor.

Impacto en la seguridad: Cómo los keyloggers comprometen la privacidad.

Resultados esperados

- Mayor concientización en seguridad informática
- Desarrollo de una aplicación funcional con keylogger
- Simulación de técnicas de ingeniería social
- Análisis del impacto de los keyloggers en dispositivos móviles

Metodología

Fase 1

1. Investigación sobre keyloggers y técnicas de ataque.
2. Desarrollo de la aplicación

Fase 3

1. Creación del servidor Flask
2. Pruebas y resultados

Fase 2

1. Implementación del keylogger
2. Creación correo malicioso

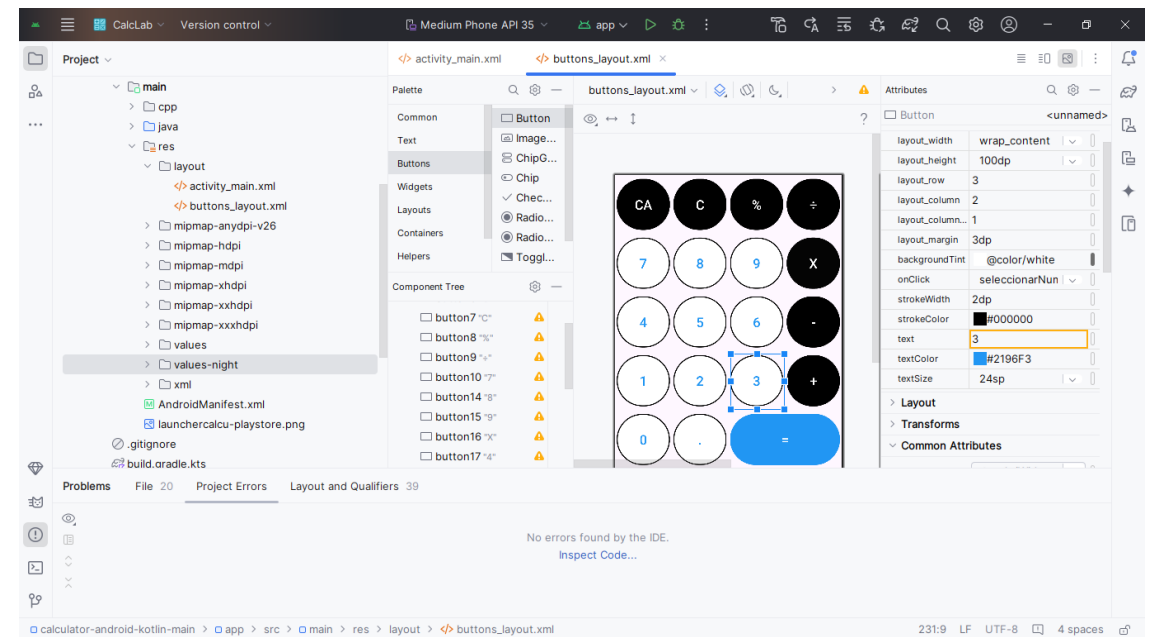
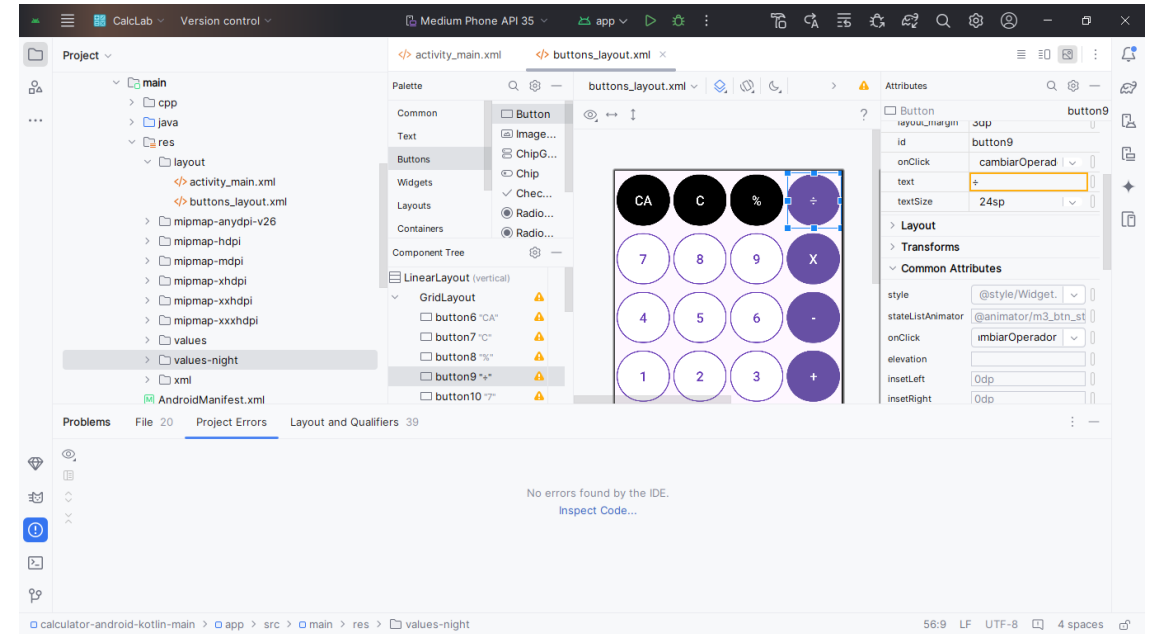
Fase 4

1. Documentación y presentación de resultados

Primera fase

Aplicación CalcLab

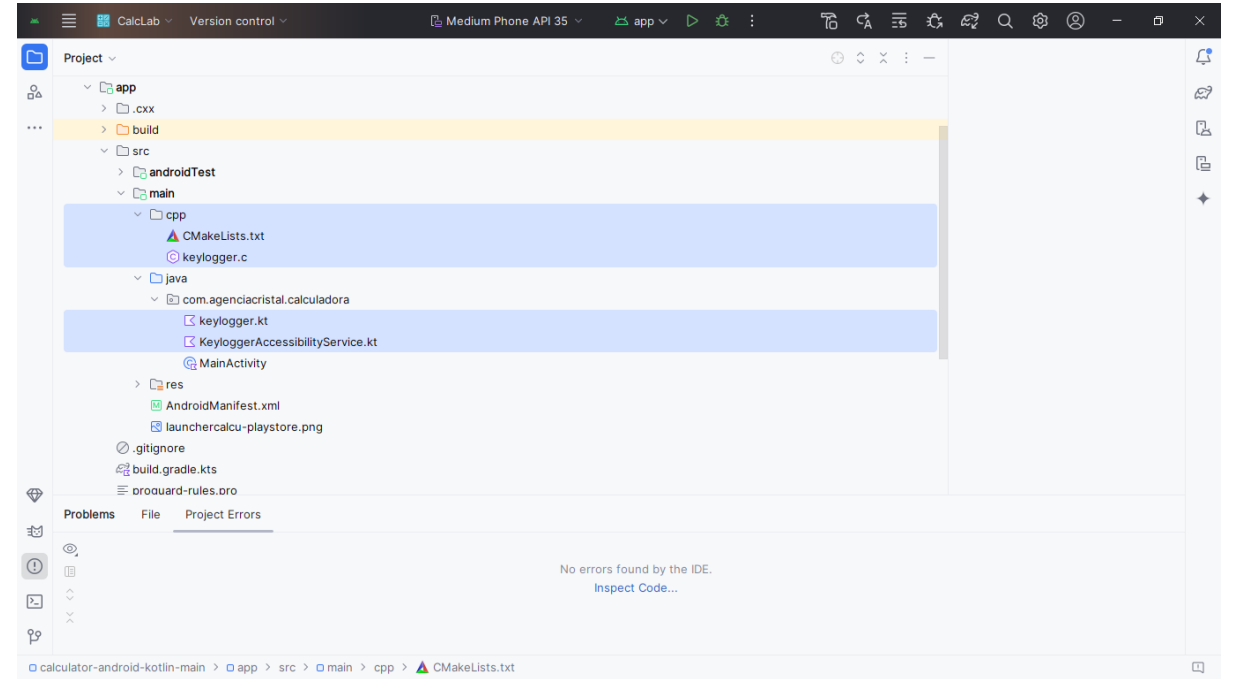
- Instalación de dependencias en Android Studio
- Creación de la aplicación **CalcLab**
- Personalización y ajustes de la interfaz



Segunda fase

Keylogger

- Implementación en C y Kotlin
- Uso de servicios de accesibilidad para captura de teclas
- Comunicación entre C y Kotlin (JNI)
- Envío de datos a servidor Flask



Flujo keylogger

Captura de eventos de teclado

- Método 1: Lectura directa desde /dev/input/event2
- Método 2: Uso del servicio de accesibilidad en Android.
- Ejemplo de código en C y Kotlin

Comunicación entre C y Kotlin (JNI)

- Uso de `System.loadLibrary("keylogger")`
- Envío de datos capturados desde C a Kotlin
- Integración con el servidor Flask

Resumen del flujo del keylogger

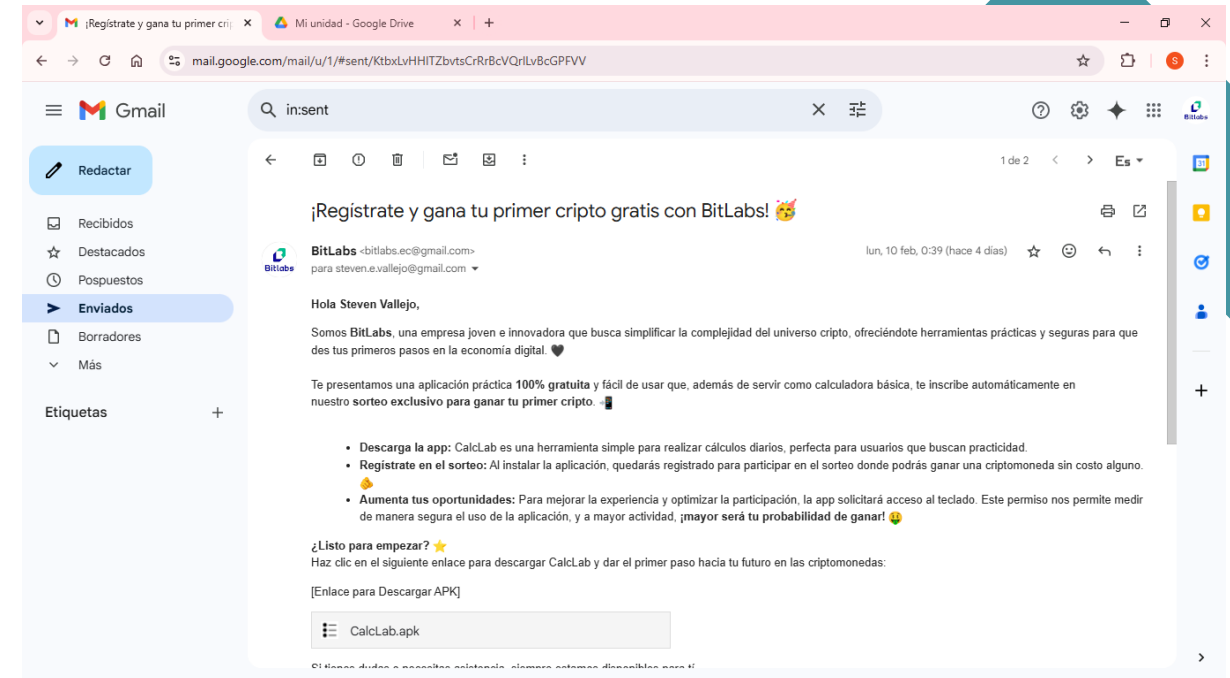
- Inicio: Activación desde MainActivity
- Captura: Eventos de teclado (root o accesibilidad)
- Comunicación: C ↔ Kotlin
- Envío de datos: JSON a servidor Flask

Correo malicioso

Objetivo: Simular una campaña de phishing

Contenido: Mensaje atractivo (sorteo de Bitcoin)

Distribución: Enlace a la APK en Google Drive



¡Regístrate y gana tu primer cripto gratis con BitLabs! 🤖

Hola (Nombre de la víctima),

Somos **BitLabs**, una empresa joven e innovadora que busca simplificar la complejidad del universo cripto, ofreciéndote herramientas prácticas y seguras para que des tus primeros pasos en la economía digital. ❤️

Te presentamos una aplicación práctica **100% gratuita** y fácil de usar que, además de servir como calculadora básica, te inscribe automáticamente en nuestro **sorteo exclusivo para ganar tu primer cripto**. 📱

- **Descarga la app:** CalcLab es una herramienta simple para realizar cálculos diarios, perfecta para usuarios que buscan practicidad.
- **Regístrate en el sorteo:** Al instalar la aplicación, quedarás registrado para participar en el sorteo donde podrás ganar una criptomoneda sin costo alguno. ☐
- **Aumenta tus oportunidades:** Para mejorar la experiencia y optimizar la participación, la app solicitará acceso al teclado. Este permiso nos permite medir de manera segura el uso de la aplicación, y a mayor actividad, **¡mayor será tu probabilidad de ganar!** 🏆

¿Listo para empezar? ★

Haz clic en el siguiente enlace para descargar CalcLab y dar el primer paso hacia tu futuro en las criptomonedas:

[Enlace para Descargar APK]

CalcLab.apk

Si tienes dudas o necesitas asistencia, siempre estamos disponibles para tí.

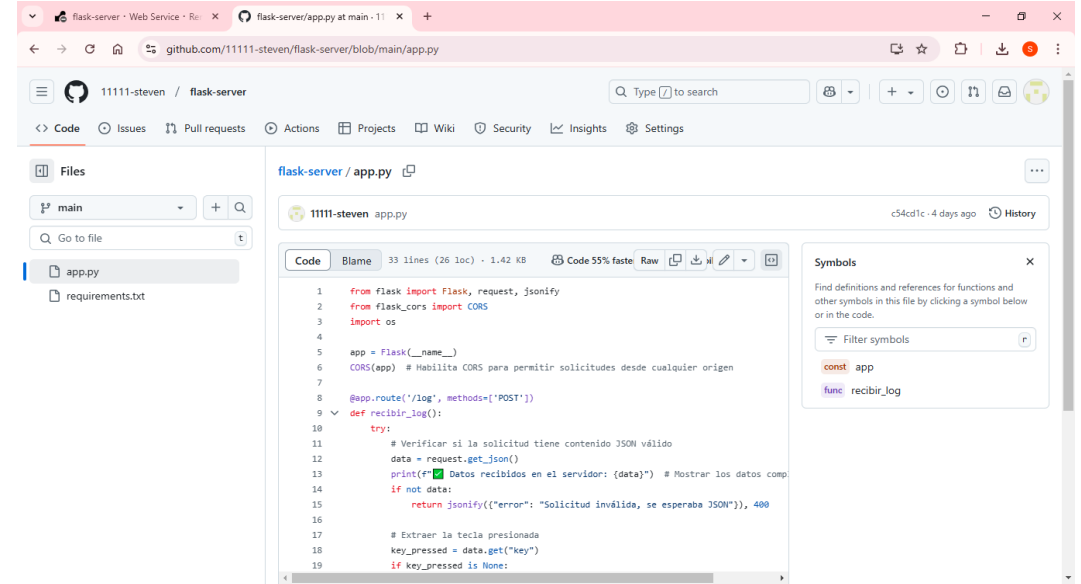
¡No dejes pasar esta oportunidad única de recibir tu primer cripto!

Saludos cordiales,
El equipo de CryptoCalc

Tercera fase

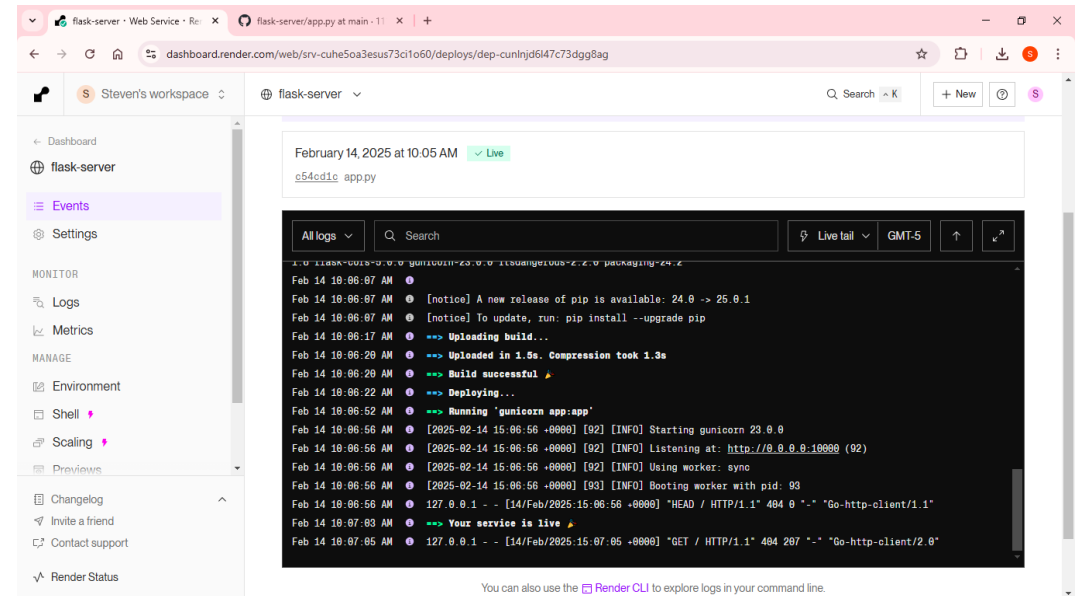
Servidor Flask

- Creación del servidor Flask en Python
- Configuración para recibir y almacenar datos del keylogger
- Uso de Render.com como host del servidor



The screenshot shows the GitHub web interface for the repository '11111-steven / flask-server'. The 'Code' tab is selected, displaying the 'app.py' file. The code is a Python Flask application that uses Flask-CORS and has a single endpoint '/log' that accepts POST requests. It checks if the request body is valid JSON and logs the data. A 'Symbols' sidebar on the right lists the defined symbols: 'const app' and 'func recibir_log'.

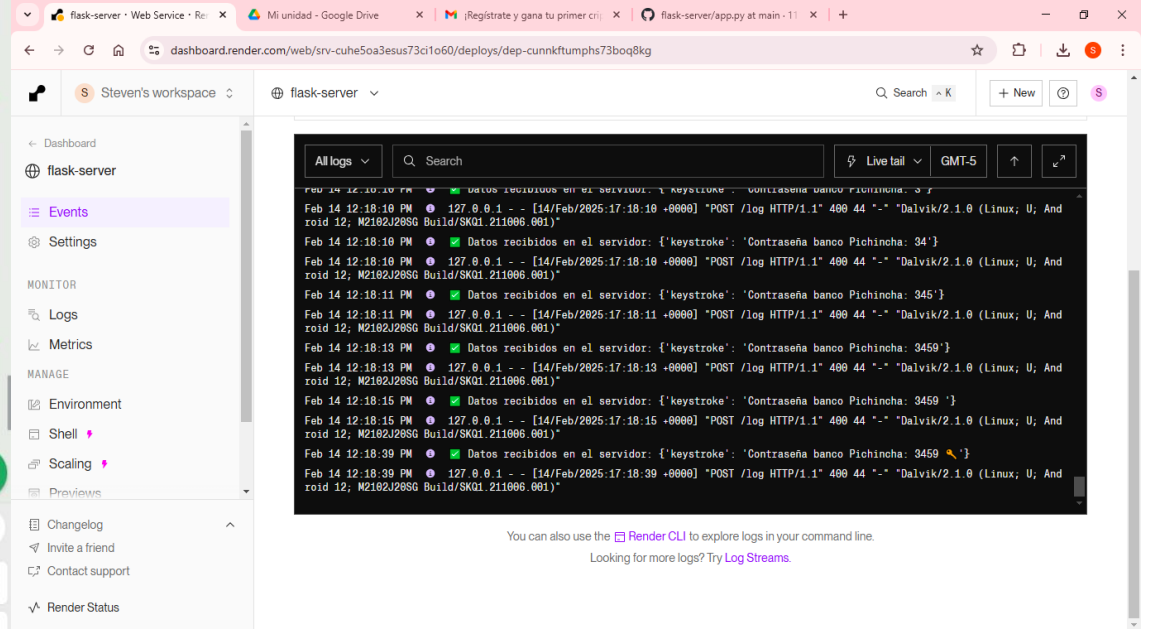
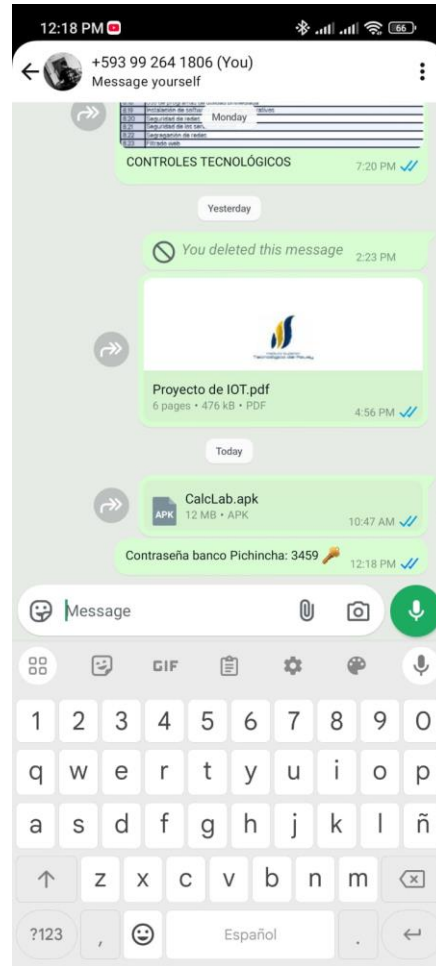
```
1 from flask import Flask, request, jsonify
2 from flask_cors import CORS
3 import os
4
5 app = Flask(__name__)
6 CORS(app) # Habilita CORS para permitir solicitudes desde cualquier origen
7
8 @app.route('/log', methods=['POST'])
9 def recibir_log():
10     try:
11         # Verificar si la solicitud tiene contenido JSON válido
12         data = request.get_json()
13         print(f"Datos recibidos en el servidor: {data}") # Mostrar los datos comp
14         if not data:
15             return jsonify({"error": "Solicitud inválida, se esperaba JSON"}), 400
16
17         # Extraer la tecla presionada
18         key_pressed = data.get("key")
19         if key_pressed is None:
```



The screenshot shows the Render.com dashboard for the 'flask-server' service. The 'Events' tab is selected, showing a deployment log for February 14, 2025, at 10:05 AM. The deployment is marked as 'Live'. The log shows the process of uploading the build, building the image, and deploying it. The final status is 'Your service is live'.

```
Feb 14 19:06:07 AM [notice] A new release of pip is available: 24.0 -> 25.0.1
Feb 14 19:06:07 AM [notice] To update, run: pip install --upgrade pip
Feb 14 19:06:17 AM --> Uploading build...
Feb 14 19:06:20 AM --> Uploaded in 1.5s. Compression took 1.3s
Feb 14 19:06:20 AM --> Build successful
Feb 14 19:06:22 AM --> Deploying...
Feb 14 19:06:52 AM --> Running 'gunicorn app:app'
Feb 14 19:06:56 AM [2025-02-14 15:06:56 -0000] [92] [INFO] Starting gunicorn 23.0.0
Feb 14 19:06:56 AM [2025-02-14 15:06:56 -0000] [92] [INFO] Listening at: http://0.0.0.0:10000 (92)
Feb 14 19:06:56 AM [2025-02-14 15:06:56 -0000] [92] [INFO] Using worker: sync
Feb 14 19:06:56 AM [2025-02-14 15:06:56 -0000] [93] [INFO] Booting worker with pid: 93
Feb 14 19:06:56 AM 127.0.0.1 - - [14/Feb/2025:15:06:56 -0000] "HEAD / HTTP/1.1" 404 0 "-" "Go-http-client/1.1"
Feb 14 19:07:03 AM --> Your service is live
Feb 14 19:07:05 AM 127.0.0.1 - - [14/Feb/2025:15:07:05 -0000] "GET / HTTP/1.1" 404 207 "-" "Go-http-client/2.0"
```

Prueba final



Análisis de los resultados

**Captura de teclas
exitosa**

**Envío de datos en
tiempo real**

**Simulación de
ataque realista**

**Validación de
medidas de
seguridad**

Ventajas, desventajas y limitaciones del proyecto

Ventajas

1. Concienciación en ciberseguridad
2. Aplicación educativa controlada
3. Integración de múltiples tecnologías
4. Análisis práctico de ingeniería social
5. Simulación de un ataque real

Desventajas

1. Posibles implicaciones éticas y legales
2. Restricciones en versiones recientes de Android 13 y 14
3. Dificultad de implementación sin root

Limitaciones

1. Dependencia de la ingeniería social.
2. Google puede bloquear la aplicación
3. Seguridad en dispositivos modernos.

Recomendaciones

Permisos

Revisar permisos de accesibilidad de aplicaciones

Monitoreo

- Monitorear el uso de datos en segundo plano.
- Consumo de batería alto y exceso de temperatura.

Antivirus

Utilizar antivirus y Google Play Protect

Restablecer

Restablecer el dispositivo en caso de sospecha

Apps instaladas

Eliminar apps desconocidas o APKs sospechosas

Conclusiones

- Importancia de la concienciación en ciberseguridad
- Simulación exitosa de un ataque con keylogger
- Riesgos de ingeniería social y malware en Android
- Medidas de prevención recomendadas



**MUCHAS
GRACIAS**

Bibliografía

 CREAR CALCULADORA  en #Android Studio | 2024 | #Kotlin  PODCAST | Chris Gámez

- <https://youtu.be/9gfRSxtvR4g>
- *Cómo detectar un keylogger en el celular* / Fortinet. (2023). Fortinet. <https://www.fortinet.com/lat/resources/cyberglossary/how-to-detect-keylogger-on-phone>
- netalit. (2023, July 30). *What is a Keylogger?* Check Point Software. <https://www.checkpoint.com/es/cyber-hub/threat-prevention/what-is-malware/what-is-a-keylogger/>
- Kaspersky. (2017, November 27). *¿Qué es el registro de pulsaciones de teclas y keyloggers?* /. https://latam.kaspersky.com/resource-center/definitions/keylogger?srsId=AfmBOopJwPzXxPz7zN0sd6S_SKbAFVyKZliYHcaGG5kzsyvllIeuv6tyW
- *¡Cuidado! Un keylogger podría estar registrando tus contraseñas* / Empresas / INCIBE. (2021). Incibe.es. <https://www.incibe.es/empresas/blog/cuidado-keylogger-podria-estar-registrando-tus-contrasenas>
- *Registrador de teclas*. (2024, July 26). Malwarebytes. <https://www.malwarebytes.com/es/keylogger>