**Crear un documento donde se exponga cómo ha sido posible extraer dinero de la víctima a través del portal de inversiones, usando los métodos descritos en el proyecto, posible vía de entrada por las que se han comunicado con la víctima.**

De acuerdo con el presente proyecto, el primer paso para poder extraer dinero de los clientes es extrayendo información como usuarios y contraseña de sitio de **Exchange de criptomonedas**, la vía para comunicarse con las víctimas sería mediante envío de correo fraudulento o phishing aunque también pudo haberse enviado por SMS.

En nuestro caso se creó una página similar a la original del sitio : **https://www.coinex.com/signin** , la mism

a que fue subida a Heroku, en la siguiente URL: [**https://mysterious-bastion-81992.herokuapp.com**/](https://mysterious-bastion-81992.herokuapp.com/)

**SITIO CLONADO: SITIO REAL:**

Graphical user interface, text, application, chat or text message

Description automatically generatedGraphical user interface, text, application, chat or text message

Description automatically generated

En esta página se pudiera obtener usuario y contraseña, lo cual sería muy importante para el siguiente paso dentro de obtener información valiosa para el cliente.

En la siguiente página se pudiera descargar la apk la misma que se encontraría en nuestro caso publicada en a URL de Heroku antes mencionada:



En esta pantalla el cliente puede descargar la apk de **Coinex,** pero esta contiene un **RAT** para poder extraer informacióntales como acceso a la cámara, acceso a los SMS, acceso a la llamada, acceso a captura de pantalla, geolocalización, grabación de audio, etc.

Esto permitiría acceso completo al celular infectado para poder retirar dinero de los usuarios de sitios como el Exchange de criptomonedas.