CTF Challenge Proposal: CEO's Mobile Mystery

Difficulty: Medium-Hard

What we want: We aim to create a realistic scenario where a CEO's mobile phone gets infected. As a cybersecurity specialist, you need to uncover how the phone was infected, what caused the infection, and so much more.

The story: After a dramatic altercation that involved the CEO throwing his old phone at John, the CEO obtained a new phone. John was dismissed that day. Initially, everything seemed normal, but soon sensitive company data that only the CEO had access to began appearing online. The CEO has summoned your team of cybersecurity specialists to uncover the mystery. Your primary objectives are to identify the **package name** of the malicious application, **the command and control server**, and determine which **tool** was used to craft such **malware**.

The flag format will be constructed using the answers to the following questions:

- What is the package name of the malicious application?
- Identify the C2 (Command and Control) server.
- What tools were used to craft the malware?

Example: **CTF{answer1_answer2_answer3}**

What the investigators will get:

- A full capture of the mobile device using Oxygen Forensics

Tools that can be used for analysis:
Android Studio, Oxygen Forensics Viewer, adb, apktool, dex2jar, jd-gui, VirusTotal, google, etc..

Steps for solving:

- **Initial Assessment:** Begin by examining the files provided. It's crucial to scrutinize the downloads, browser history, and emails to determine how the infection was introduced to the system.
- **Malware Analysis:** Once the entry point of the infection is identified, focus on analyzing the application involved in the attack (after identifying it). This involves decompiling the app, conducting static and dynamic analyses. During the application analysis, determine to which command and control server the application is exfiltrating the company's data.
- **Investigate application:** Analyze how the application was developed by searching for specific tool patterns and other indicators that might suggest the methods and tools used in crafting the malware.

P.S. This is our preliminary proposal. While we are developing the CTF, some aspects of these steps, tools, or the story presented may change slightly (though hopefully not too much).