

GitHub - LaurieWired/StrangeLoop: This contains notes, slides, and code for my Strange Loop talk

By LaurieWired

Archived: 2026-04-05 18:27:44 UTC



Unmasking the Godfather

Welcome to a deep-dive analysis of the notorious Godfather Android banking trojan. This repository contains notes, slides, and code related to my Strange Loop 2023 talk "Unmasking the Godfather".

In this presentation, I provide a reverse-engineering walkthrough to demystify one of the most contemporary threats in the mobile banking industry.

Prerequisites

If you'd like to follow the session interactively, ensure you have these tools installed and their respective source codes downloaded:

- **JADX** - Java Decompiler/Disassembler for Android. Available [here](#).
 - **Ghidra** - C/C++ Decompiler/Disassembler. Available [here](#).
 - **Docker-Android** - A reliable Android emulator. Available [here](#).
 - **Recaf** - An emerging Java bytecode editor. Available [here](#).
-

Presentation Slides

The slides accompanying the talk can be found in the repository at the following link:

- [UnmaskingTheGodfather.pdf](#)
-

Marked Up Sample

My fully marked up Godfather Sample can be found at the following link:

- [marked_up_godfather_jadx](#)
-

Supplementary Resources

Additional references to supplement the content of this talk:

- [Comprehensive Anubis Banker Analysis \(Work-in-Progress\)](#)
 - [How to Hook Android Methods with Frida](#)
 - [Guide to Running an Android ARM Emulator](#)
-

Malware Sample Links

Explore and analyze these real-world samples of the Godfather and other Android banking trojans:

Godfather Samples

- [Sample 1](#)
- [Sample 2](#)

Other Android Banking Trojans

Cerberus

- [Sample](#)

Anubis

- [Sample](#)

Sharkbot

- [Sample](#)
-

Anubis Leaked Source Code

Access the complete Android Anubis source code [here](#).

Archive Password: `infected`

Source: <https://github.com/LaurieWired/StrangeLoop>