GitHub - ics-iot-bootcamp/cerberus_research: Research tools for analysing Cerberus banking trojan.

By lotusexpeditor

Archived: 2026-04-05 19:34:20 UTC

Related research paper : https://github.com/ics-iot-bootcamp/cerberus_research/blob/master/cerberus_research_paper.pdf

This repository currently has two tools that can be used.

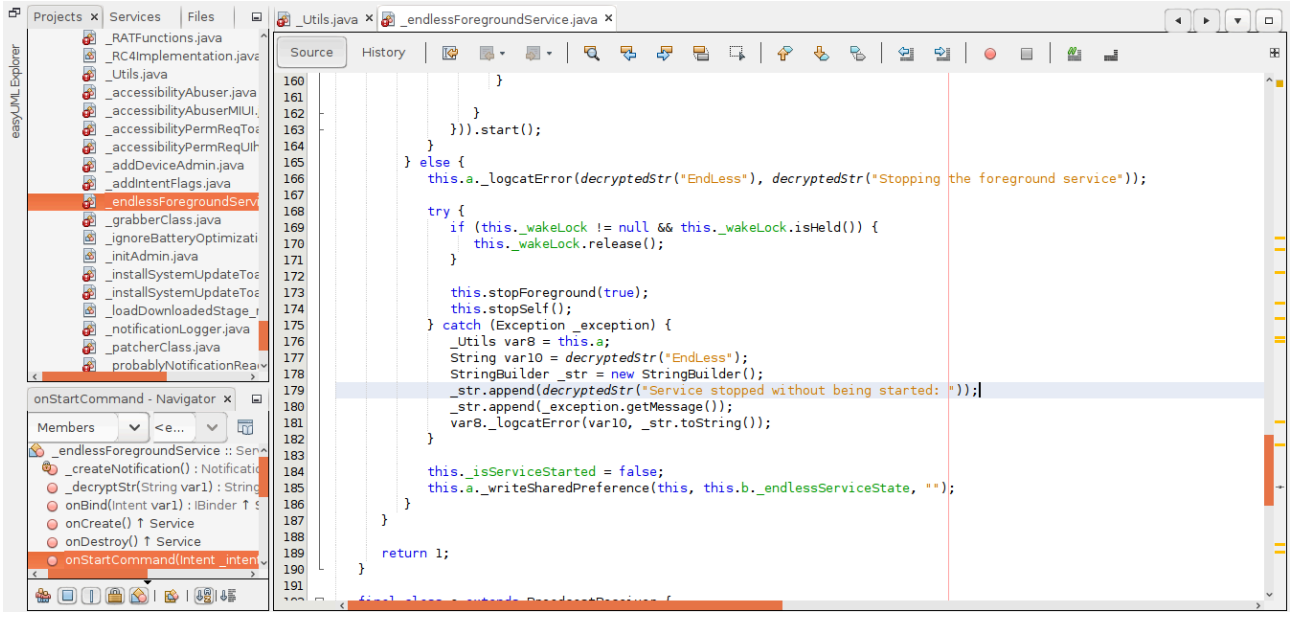
Hercules: Hercules automatically finds decryption key for actual DEX of the given Cerberus sample, decrypts it, then decrypts configuration parameters in the actual payload. All statically, in seconds.

queryCerberus: Partial implementation of the Cerberus banking trojan C2 communication.

---

cerberus_full_package contains Cerberus source code that distributed to premium members of originated forum. Credits: DC8044

Initial analysis shows that the Android V2 in the source package **is not the latest version** in the wild. It lacks Android 10 improvements. Our research paper covers latest version of the malware. According to leftover files, looks like their development team uses a private GitHub repository.



-Latest version contains Endless Foreground Service taken from;
https://robertohuertas.com/2019/06/29/android_foreground_services/

-Communication parameters of latest version are abbreviated. In this one they aren't.

Stay Safe & Healthy.

Regards, Cyberwise Research Task Force (Cyberwise - RTF).
