Project 2 - Suspicious Deb package

Description

We found a deb file being distributed inside the Campus that may be suspicious. A formal evaluation was not conducted, but the name and version do not match the original package, and the signature is incorrect. Can you help finding what is going on and if there are other things to look for?

We need to know:

- Do we really have a malware?
- How the malware works and why a deb is used?
- Are other hosts involved?
- What is the potential impact to our organization?

As this was found inside the Campus, the use of the University VPN may be required.

Describe the strategies you follow (traces, logs, static and dynamic analysis approaches), assumptions, dead ends, tools used, features of the malware, and if possible, provide a clear reconstruction of the malware operation, and of the major algorithms. Include screenshots whenever relevant.

As always: Be careful and do not trust this file. Use VMs, sandboxes or other confinement strategies.

The files are here

Rules

The use of automated tools to scan the application is allowed. However, grading will mostly consider your work and your analysis, not on the raw results.

This project is expected to be authored by the students enrolled in the course. The use of existing code snippets, applications, or any other external functional element without proper acknowledgement is strictly forbidden. If any content lacking proper acknowledgment is found in other sources, the current rules regarding plagiarism will be followed.

The use of AI tools is allowed. If this is the case, include the prompts in your report.

The delivery should be composed of a ZIP, containing a written report and support files (logs, screenshots, scripts).

The report should have the the following structure:

- Executive summary
- Major findings
- Indicators of Compromise
- Detailed description of the files

2024

PREVIOUS
Project 1 - Android Reversing

Last updated on 27 Mar 2024