ABSTRACT

MALWARE ANALYSIS ON EVIL-DROID USING TELEGRAM APPLICATION WITH REVERSE ENGINEERING METHOD

By

Nadya Sadira Verdayani

20102276

The whole of society is facilitated by technology. Technology has made developments in the world drastically, for example, communicating with fellow humans using smartphones. The hardware must use an internet connection. It is usually used by users to search for a variety of information on the Internet. It could trigger a malware attack. The Internet has positive benefits, such as making it easier to find information, and negative effects, such as misusing sensitive data by inserting malware into applications. The research was carried out due to the absence of experiments from previous studies because many internet users are not fully aware of the negative impact. From there, users can learn the functionality of the evil-droid malware after being infiltrated into the Telegram application and diving into the testing using MobSF. The analysis is carried out manually using JADX and MobSF automatically, with the aim of analyzing the change of code on the telegram as soon as malware is embedded and performing an analogy of the results of the analysis. This research using the reverse engineering method is carried out with static analysis aimed at obtaining code that is already infected with malware. In the results obtained in this study, there are 7 permissions that have been found to be analyzed automatically and manually: SEND_SMS, RECEIVE_SMS, WRITE_SETTINGS, SET_WALLPAPER, WRITE_CALL_LOG, READ_SMS, and RECORD_AUDIO. Analysis using JADX included the addition of 10 new classes, namely a, b, c, d, e, f, g, MainBroadcastReceiver, MainService, and Payload, which included backdoor parts. Code obtained to set up connections, manage TCP network connections, and hide application icons. MobSF was able to locate modifications and additional code, but MobSf failed to detect the existing class as a whole, but it detected two classes associated with the malware.

Keywords: Malware, Evil-Droid, Backdoor, Telegram