ABSTRACT

BACKDOOR-APK MALWARE ANALYSIS USING REVERSE ENGINEERING METHOD

Oleh

Aufa Salsabila Nahrowi 20102040

Malware attacks are dangerous attacks and can harm most victims. One malware attack is by exploiting the Android operating system using a backdoor attack. The backdoor attack was carried out using the Backdoor-apk malware on the Turbo VPN application installed on the Android operating system. This research is used to identify the behavior of Backdoor-apk malware and determine the vulnerability of an application due to the insertion of a backdoor in the Android operating system. This analysis was carried out automatically using MobSF and manually using JADX to determine changes and additions to source code in applications that had been inserted with malware. Then, a comparison of each analysis was carried out using the reverse engineering method. The results show that there are 36 permissions with 19 changes from the two analyses. In the automatic analysis MobSF security score changed from 38/100 to 34/100 and in the source code analysis there were 3 additional problems (issues) and differences in file information. In the JADX manual analysis, a malware folder was found in the free/vpn/unblock/proxy/turbovpn package and there was a source code change in AppContext.java which was indicated as a payload hook.

Keywords : Malware, Backdoor, Backdoor-apk, Reverse Engineering.