ABSTRACT

Current technological and information advances in smartphones is directly proportional to the risks it produces. There have been many cases of data or information theft, such as: Credentials, PINs, and OTPs. This is caused by Hacker attacks that send payloads in the form of malicious scripts that are injected into Android applications. Hackers usually send these malicious applications through social media and email. To address this, an analysis is needed with the aim of knowing the capabilities of the malware so that smartphone users who have installed this application know how to mitigate it so that the data or information they have is not successfully obtained by Hacker. This research focuses on analysis the influence of Virtual Private Networks (VPNs) and vulnerabilities on Android applications infected with command and control (C&C) malware. The scenario in this research is to simulate on an Android smartphone by limiting the network segmentation for the environment used. The results of this study show that the Creator application has a security score of 49/100 with medium risk, the Wedding Invitation application has a security score of 31/100 with high risk, and the J&T Invoice Check application has a security score of 52/100 with medium risk based on the Open Web Application Security Project (OWASP) application security standardization. VPNs have a 100% success rate in protecting devices against C&C attacks, but experience a decrease in network service quality, namely: download -24.87 Mbps and upload -14.91 Mbps. Based on the TIPHON standard, the internet network service quality produced from the three VPNs is excellent and falls into the perfect category with an index of 4 based on the percentage of packet loss produced.

Keywords: *OTP, Payload, PIN, Malware, Mobile Security Framework, Smartphone, Virtual Private Network, Vulnerability*