ABSTRACT

Smartphone usage advance greatly in the society nowadays, especially smartphone with Android Operating System and IOS . Smartphone usually used to surf and browsing on the internet, taking photos, recording videos, listening to music, online banking transaction and the most interesting were social media. Along with the increasing usage of smartphone, new need rose that is power or electricity to be able relative easily accessed to charge up smartphone battery.

In this research, Android malware was designed to be planted in the smartphone to steal user's data and send it back to the microcontroller. Stolen data were smartphone information, SMS, contacts, email and webview. By exploiting permissions function granted on the Android Programming, malware able to access user's sensitive data in the smartphone. To smoothen data stealing process, malware was inserted into a normal Application to avoid user's suspicions.

Product of this research is a malware with the ability to steal user's data on the smartphone and send it back to the microcontroller. Data transmission use serial communication. From the text file processing until transmission data into the microcontroller each of them need average time of 7523.6 per 50 SMS, 45013.83 ms per 30 contact , 4502.93 ms per 3 webview dan 30010.66 ms per 20 email. The data sent have the probability of damage caused by interruption of the users while transmission data were on going.

Kata kunci : *android, malware, root, serial communication, security system*