Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 9, September 2013, pg.247 – 255

RESEARCH ARTICLE

Performance Base Static Analysis of Malware on Android

Khyati Rami[1], Vinod Desai[2]

[1]Ph.D Research Scholar, Mewar University, Rajasthan, India

[2]Department of Computer Application, Kadi Sarva Vishwa Vidyalaya, Gujarat, India

Abstract— According to a Gartner study (Gartner, 11/2010), Android is now the No. 2 worldwide mobile operating system and will challenge Symbian for No.1 position by 2014. In addition to Android's large market share, the number of Android applications is growing at a fast rate. There are currently more than 100,000 Android applications available (Techeye, 26/11/2010). With the increasing numbers of applications available for Android; spyware is becoming a real concern. Several malicious applications, ranging from fake banking applications to an SMS Trojan embedded into a fake media player, have already been discovered on the Android Market since the beginning of this year. However, there are other forms of malware that may also emerge. What about hiding spyware in the background of a well-known application? For example, imagine an application claiming to be the latest version of a famous Twitter client, which actually runs spyware in the background and uploads all private data to the attacker. The purpose of this paper will be to explore a study of static analysis on Android and provide real case malware attack scenarios. Reverse engineering will be used, because most users do not check the permissions of the applications loaded onto their mobile device.

Keywords: - Malware; Static analysis; translator; Reverse Engineering

Full Text: http://www.ijcsmc.com/docs/papers/September2013/V2I9201339.pdf