A Static Approach towards Mobile Botnet Detection

Shahid Anwar*

Faculty of Computer Systems and Software Engineering
Universiti Malaysia Pahang
Gambang, Malaysia
shahidanwar.safi@gmail.com

Jasni Mohamad Zain

Faculty of Computer Systems and Software Engineering
Universiti Malaysia Pahang
Gambang, Malaysia
jasni@ump.edu.my

Zakira Inayat

Computer Science and Information Technology
University Malaya Kuala Lumpur, Malaysia
University of Engineering & Technology Peshawar, Pakistan
zakirainayat@uetpeshawar.edu.pk

Ahmad Karim

Computer Science and Information Technology
University Malaya
Kuala Lumpur, Malaysia
ahmadkarim1@yahoo.com

Riaz Ul Haq

Faculty of Computer Systems and Software Engineering
Universiti Malaysia Pahang
Gambang, Malaysia
rias.ullah@gmail.com

Aws Naser Jabir

Faculty of Computer Systems and Software Engineering
Universiti Malaysia Pahang
Gambang, Malaysia
awscomputer2009@gmail.com

***Abstract*— The use of mobile devices, including smartphones, tablets, smart watches and notebooks are increasing day by day in our societies. They are usually connected to the Internet and offer nearly the same functionality, same memory and same speed like a PC. To get more benefits from these mobile devices, applications should be installed in advance. These applications are available from third party websites, such as google play store etc. In existing mobile devices operating systems, Android is very easy to attack because of its open source environment. Android OS use of open source facilty attracts malware developers to target mobile devices with their new malicious applications having botnet capabilities. Mobile botnet is one of the crucial threat to mobile devices. In this study we propose a static approach towards mobile botnet detection. This technique combines MD5, permissions, broadcast receivers as well as background services and uses machine learning algorithm to detect those applications that have capabilities for mobile botnets. In this technique, the given features are extracted from android applications in order to build a machine learning classifier for detection of mobile botnet attacks. Initial experiments conducted on a known and recently updated dataset: UNB ISCX Android botnet dataset, having the combination of 14 different malware families, shows the efficiency of our approach. The given research is in progress.**

Keywords*— *Botnets; Mobile Botnets; Android Botnets; Static Technique; Detection Technique;