Evolution Study of Android Botnets

Heloise Pieterse and Ivan Burke

Abstract:
Smartphones continue to excel in the 21st century due to the constant improvements of mobile technology. Advances in smartphones, such as increased computing power, improved device-to-device communication and the option of installing additional third-party applications, have led to a sharp rise in their popularity. This popularity, combined with the extensive adoption of smartphones by the general public, has now drawn the attention of mobile malware developers. On popular platforms, such as Android, malware have grown exponentially since the detection of the first mobile Trojan horse in 2010. Android malware families detected during 2013 displayed capabilities that revealed the transition from traditional computer-based botnets to the Android platform. To effectively mitigate or defend against Android botnets, an insightful understanding of them is required. This paper aims to characterise existing Android malware families that display botnet functionality, allowing for the development of proper mitigation and anti-botnet solutions. The contributions of this paper are two-fold. Firstly, the Android malware collection presented in this paper includes 20 families, which covers the majority of malware families displaying botnet behaviour, ranging from their debut in December 2010 to the recent ones discovered in December 2013. These families are thoroughly characterised based on their detailed behaviour breakdown, including propagation methods, command and control channels, and attack strategies. Secondly, an evolution-based study of representative Android botnet families is performed, revealing the rapid growth of Android botnets and the pressing need for anti-botnet solutions. The characterisation of the Android malware families and the subsequent evolution-based study reveal the sophistication of Android botnets. These identifiable characteristics can, however, be incorporated into new and existing mitigation solutions to defend and protect against Android botnet infections. The outcome of this study show that Android botnets are real and a current threat to smartphone users and that there is a need for proper anti-botnet solutions on mobile platforms.

Keywords: Android, Android botnets, mobile botnets, smartphones, mobile malware.