


# Android Botnets: A Proof-of-Concept Using Hybrid Analysis Approach

Ahmad Karim, Bahauddin Zakariya University, Pakistan

Victor Chang, Teesside University, UK

 <https://orcid.org/0000-0002-8012-5852>

Ahmad Firdaus, Faculty of Computer Systems and Software Engineering, Malaysia

## ABSTRACT

Mobile botnets are gaining popularity with the expressive demand of smartphone technologies. Similarly, the majority of mobile botnets are built on a popular open source OS, e.g., Android. A mobile botnet is a network of interconnected smartphone devices intended to expand malicious activities, for example; spam generation, remote access, information theft, etc., on a wide scale. To avoid this growing hazard, various approaches are proposed to detect, highlight and mark mobile malware applications using either static or dynamic analysis. However, few approaches in the literature are discussing mobile botnet in particular. In this article, the authors have proposed a hybrid analysis framework combining static and dynamic analysis as a proof of concept, to highlight and confirm botnet phenomena in Android-based mobile applications. The validation results affirm that machine learning approaches can classify the hybrid analysis model with high accuracy rate (98%) than classifying static or dynamic individually.

## KEYWORDS

Botnet Detection, Hybrid Analysis, Mobile Botnet, Mobile Malware

## INTRODUCTION

Although Android OS being an open source has promoted mobile applications developers, yet malware programmers have also contributed to exploit its open source nature to carry out malicious acts. McAfee, an antimalware platform, has diagnosed more than 700K mobile malware in the second quarter of 2014 (Weafer, 2014). Another report (Chebyshev, 2016) published in 2016 discovered that Internet access on smartphone devices had exceeded 61% in the first quarter of 2015. This study also revealed that 60.85% of Android users had started Internet access on their smartphone devices. Consequently, the similar growth is observed in malware program construction, i.e., 40,267 new mobile malware variants were analyzed and diagnosed by the security agencies at the end of 2015 (Millman, 2015). In Q2 2016, it was observed that Android was used by 86.2% of smartphone users (Paul,

DOI: 10.4018/JOEUC.2020070105

This article, originally published under IGI Global's copyright on July 1, 2020 will proceed with publication as an Open Access article starting on January 21, 2021 in the gold Open Access journal, Journal of Organizational and End User Computing (converted to gold Open Access January 1, 2021), and will be distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

2017). Similarly, its widespread adaptation to other platforms such as televisions, tablets, wearable, and vehicles opened the new dimensions for multi-platform attacks. In the similar pace, IoT (Internet of Things) would be the next target for malware programmers. A more recent report (BILIĆ, 2017) states that the growth of mobile malware is constantly increasing since 2013. On average 200 new malicious code variants have been discovered per month during 2015, this number rose to 300 per month by the end of 2016. As a result, on average 400 new malicious code variants are expected to evolve by the end of 2017 (Weafer, 2016).

Mobile botnet or SMARTbot (Karim, Salleh, & Khan, 2016) is a malevolent action which is inspired from traditional botnets (PC based). The basic motive behind botnet is to gain illegitimate access to someone's personal device (smartphone, tablets, etc.) and makes this device compromised by a bot binary (app). After becoming the part of a bot network, another pivotal role (botmaster) is responsible for controlling this device remotely and to initiate various attacks using some command and control (C&C) channel. Consequently, these devices are then participating in numerous malicious activities including DDoS, ransom, making premium calls, sending text messages and emails without user's consent.

There are two most common analysis strategies exist, static and dynamic analysis. In static analysis, structural properties of program code are observed including permission usage, CFGs, function call graphs and API calls, etc. For static analysis, reverse engineering tools (Lukan, 2012) are deployed to disassemble program code (Schmidt et al., 2009) or directly fetching parameters from executable binaries (Petsas, Voyatzis, Athanasopoulos, Polychronakis, & Ioannidis, 2014; Yousafzai et al., 2016). In contrast, dynamic analysis requires execution of malware binaries in a secure environment (called sandbox) to extract runtime behavior of these applications. Following are some of the parameters which are of interest during dynamic analysis: (a) file operations (b) network traces (c) initiated services (d) HTTP and DNS traffic etc. Currently, some mobile malware detection approaches (Arp, Spreitzenbarth, Hubner, Gascon, & Rieck, 2013; Chen, Rong-Cai, ZHENG, Jia, & Li-Jing, 2016; Fereidooni, Conti, Yao, & Sperduti, 2016; Yang, Wang, Ling, Liu, & Ni, 2017) are introduced targeting either program code or runtime execution traces. However, at a higher level of abstraction, these approaches are targeting mobile malware detection rather than mobile botnet. This is the extension of our previously proposed approaches (Ahmad Karim & Shah, 2015; Karim, Salleh, Khan, Siddiqua, & Choo, 2016) in a way that it can highlight the need for a hybrid analysis framework for the detection of botnet mobile binaries.

In this paper, we will investigate and highlight the problem of the mobile botnet by comparing botnet properties of known botnet applications with existing malware families and benign samples.

Thus, the basic motive of this research is to confirm the existence of mobile botnet phenomenon in Android-based system which is continuously progressing with the technological advancements. Moreover, we argued that hybrid analysis systems can detect mobile botnet binaries more accurately. Consequently, mobile botnet problem may supersede traditional PC based botnets if the precautionary measures have not been devised timely. Overall the paper objectives are summarized as follows:

- To strengthen the existing efforts (mobile malware detection in general) towards mobile botnet (C&C) detection by identifying, highlighting and comparing the properties of known mobile botnets with existing malware and benign applications;
- We have divided our hybrid analysis framework into three different categories for mobile applications which includes botnet, malware and benign set of applications. Through this setup, we need to observe the most inherent properties and ongoing trends of mobile applications having botnet capabilities;
- Our claim of a hybrid analysis is more efficient to detect mobile botnet malware is verified by machine learning approaches;
- Conclusively, we have provided some guideline steps to avoid this growing hazard.

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: [www.igi-global.com/article/android-botnets/256145](http://www.igi-global.com/article/android-botnets/256145)

## Related Content

---

### In or Out: An Integrated Model of Individual Knowledge Source Choice

Yinglei Wang, Darren Meister and Peter H. Gray (2013). *Innovative Strategies and Approaches for End-User Computing Advancements* (pp. 40-60).

[www.irma-international.org/chapter/out-integrated-model-individual-knowledge/69611](http://www.irma-international.org/chapter/out-integrated-model-individual-knowledge/69611)

### Studying the Translations of NHSnet

Edgar A. Whitley and Athanasia Pouloudi (2002). *Advanced Topics in End User Computing, Volume 1* (pp. 158-176).

[www.irma-international.org/chapter/studying-translations-nhsnet/4430](http://www.irma-international.org/chapter/studying-translations-nhsnet/4430)

### E-SERVCON and E-Commerce Success: Applying the DeLone & McLean Model

Jung-Yu Lai (2014). *Journal of Organizational and End User Computing* (pp. 1-22).

[www.irma-international.org/article/e-servcon-and-e-commerce-success/116693](http://www.irma-international.org/article/e-servcon-and-e-commerce-success/116693)

### Asynchronous Learning Using a Hybrid Learning Package: A Teacher Development Strategy in Geography

Kalyani Chatterjea (2008). *End-User Computing: Concepts, Methodologies, Tools, and Applications* (pp. 594-610).

[www.irma-international.org/chapter/asynchronous-learning-using-hybrid-learning/18210](http://www.irma-international.org/chapter/asynchronous-learning-using-hybrid-learning/18210)

### Towards Smart Transportation System: A Case Study on the Rebalancing Problem of Bike Sharing System Based on Reinforcement Learning

Guofu Li, Ning Cao, Pengjia Zhu, Yanwu Zhang, Yingying Zhang, Lei Li, Qingyuan Lian and Yu Zhang (2021). *Journal of Organizational and End User Computing* (pp. 35-49).

[www.irma-international.org/article/towards-smart-transportation-system/276375](http://www.irma-international.org/article/towards-smart-transportation-system/276375)