Mobile Botnet Detection: A Deep Learning Approach Using Convolutional Neural Networks

Title	Mobile Botnet Detection: A Deep Learning Approach Using Convolutional Neural Networks
Publication Type	Conference Paper
Year of Publication	2020
Authors	Yerima, S. Y., Alzaylaee, M. K.
Conference Name	2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)
Date Published	June 2020
Publisher	IEEE
ISBN Number	978-1-7281-6690-2
Keywords	Android (operating system), Android botnet detection, Android Botnets, Android platform, Androids, Botnet, botnet apps, Botnet detection, botnets, CNN-based approach, CNN-based model, composability, convolutional neural nets, convolutional neural networks, Deep Learning, feature extraction, Forestry , Humanoid robots, invasive software, ISCX botnet dataset, learning (artificial intelligence), machine learning, machine learning classifiers, malicious apps, Metrics, mobile botnet detection, mobile computing, mobile devices, mobile operating systems, pattern classification, program diagnostics, pubcrawl, resilience, Resiliency, smart phones, static app features

Abstract

Android, being the most widespread mobile operating systems is increasingly becoming a target for malware. Malicious apps designed to turn mobile devices into bots that may form part of a larger botnet have become quite common, thus posing a serious threat. This calls for more effective methods to detect botnets on the Android platform. Hence, in this paper, we present a deep learning approach for Android botnet detection based on Convolutional Neural Networks (CNN). Our proposed botnet detection system is implemented as a CNN-based model that is trained on 342 static app features to distinguish between botnet apps and normal apps. The trained botnet detection model was evaluated on a set of 6,802 real applications containing 1,929 botnets from the publicly available ISCX botnet dataset. The results show that our CNN-based approach had the highest overall prediction accuracy compared to other popular machine learning classifiers. Furthermore, the performance results observed from our model were better than those reported in previous studies on machine learning based Android botnet detection.

URL https://ieeexplore.ieee.org/document/9139664
DOI 10.1109/CyberSA49311.2020.9139664
Citation Key yerima_mobile_2020

Android (operating system) Android botnet detection Android Botnets Android platform Androids botnet botnet apps Botnet detection botnets CNN-based approach CNN-based model composability convolutional neural nets convolutional neural networks deep learning feature extraction Forestry Humanoid robots invasive software ISCX botnet dataset learning (artificial intelligence) machine learning machine learning classifiers malicious apps Metrics mobile botnet detection mobile computing mobile devices mobile operating systems pattern classification program diagnostics pubcrawl resilience Resiliency smart phones static app features