2023 IEEE 8th International Conference On Software Engineering and Computer Systems (ICSECS) | 979-8-3503-1093-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICSECS58457.2023.10256304

Cloud of Word vs DroidKungfu: Performance Evaluation in Detecting Root Exploit Malware with Deep Learning Approach

Che Akmal Che Yahaya
Faculty of Computing and Information Technology
Tunku Abdul Rahman University of Management and Technology
Kuantan, Pahang, Malaysia
cheakmal@tarc.edu.my

Ahmad Firdaus*
Faculty of Computing,
Universiti Malaysia Pahang Al-Sultan Abdullah
Pekan, Pahang, Malaysia
firdausza@ump.edu.my

Azlee Zabidi
Faculty of Computing,
Universiti Malaysia Pahang Al-Sultan Abdullah
Pekan, Pahang, Malaysia
azlee@ump.edu.my

Noor Akma bt Abu Bakar
Faculty of Industry and Management,
Universiti Malaysia Pahang Al-Sultan Abdullah
Gambang, Pahang, Malaysia
noorakmaab@ump.edu.my

Mukrimah bt Nawir
Faculty of Computing and Information Technology
Tunku Abdul Rahman University of Management and Technology
Kuantan, Pahang, Malaysia
mukrimah@tarc.edu.my

Philimal Normelissa Ani Abdul Malek
Faculty of Computing and Information Technology
Tunku Abdul Rahman University of Management and Technology
Kuantan, Pahang, Malaysia
philimal@tarc.edu.my

***Abstract*—Android mobile malware is a type of malware that execute malicious activities (stealing and collecting data and running programs without the user's knowledge) in victims' Android mobile device. There are several types of malware, for instance; 1) Root exploit; 2) Botnet; 3) Trojan; and 4) Ransomware. Among these, root exploit is the most dangerous as it is able to gain control over the root privileges of an operating system (OS) stealthily, avoids security software scanning, and further installs other types of malware. Moreover, there are multiple types of root exploit families that attack Android, such as Droidkungfu, Droiddream, and Asroot. However, Droidkungfu possesses the highest number of samples among other families and able to survive with updated versions (version one until six). Therefore, the updated version could be increasing in the future. Furthermore, finding the best features in detecting root exploit is challenging, as the categories (permission, system calls, and intent) are many to choose from. Moreover, finding the ideal number of features is challenging as well, as it is able to affect machine learning detection. Thus, this study focuses to develop a solid model to predict undiscovered Droidkungfu by converting all the codes in images and adopted a Convolutional neural network (CNN) with Word of Cloud (WoC) to discover features automatically without considering the categories and number of features in the code. Among all parameters in evaluation, the highest result is 96 % accuracy in predicting unknown Droidkungfu and proved to detect new versions of this family in the future.**

***Keywords*—root exploit, Android, static analysis, convolutional neural network, deep learning**

I. Introduction

Android provides a wide range of prices; from cheapest to the most expensive which can be considered affordable to be bought by anyone. The increment of Android devices between users globally has triggered several malware attacks (observe location, install the application without the victim's awareness, and stealing information). Since OS is an open source, many attackers exploits the Android for their own attentions and benefits. Attackers aiming for Android is that it is an open-source operating system (OS), which is available to all people who are interested to investigate it. All types of malwares (root exploit, botnet, and trojan) are aiming at Android for private and money purposes. Root exploit is one of the malware types that take over the initial root privilege stealthily and gains control of the Android OS [1]. Once the attackers have gained control of the Android, they can install different types of malwares to carry out their malicious attacks. Worst, the attackers also refer to the rooting community to bypass the security of the OS. The rooting community is a group that finds ways to root Android to block advertisements, tweaks, and installs cool system-level modifications and uninstall bloatware [2]. By obtaining guide from them, the attackers are able to update their root exploit with a variety of new updated ways with different Android devices. There are many families of root exploit, for example, 1) Droidkungfu; 2) Droiddream; 3) Asroot.

The number of Droidkungfu increases exponentially with a new updated version year by year. It surpasses other root exploit families and mark the first root exploit that have the highest number of samples. These samples were detected by security practitioners from universities and security companies. Nevertheless, it is possible to assume that there are many versions of Droidkungfu that are still undiscovered yet. Therefore, in order to detect the undiscovered version of it, typically the security researchers adopt two types of analysis, which are dynamic and static.

The contributions of this paper are as follows:

1. Root exploit is the most dangerous among all types of malwares (botnet, trojan, and ransomware). This is because, once it gains control of the operating system (OS), it is able to install all types of malware stealthily [3].

2. As Droidkungfu family of root exploit keep on evolving and producing new and updated version year by year, there is a need to develop a unique machine learning model to detect this type of family.