DYNAMIC ANALYSIS OF ANROID MALWARE USING DROIDBOX

A Thesis

Submitted to the Graduate School

of

Tennessee State University

In

Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in

Computer, Information and Systems Engineering

Graduate Research Series No._____

Priya Chaurasia

November 9, 2015

DYNAMIC ANALYSIS OF ANDROID MALWARE USING DROIDBOX

A Thesis

Submitted to the Graduate School

of

Tennessee State University

In

Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in

Computer, Information and Systems Engineering

Priya Chaurasia

November 9, 2015

To the Graduate School:

We are submitting a thesis by Priya Chaurasia entitled “DYNAMIC ANALYSIS OF ANDROID MALWARE USING DROIDBOX”. We recommend that it be accepted in partial fulfillment of the requirements for the degree, Master of Science in Computer, Information and Systems Engineering.

Sachin Shetty
Chairperson

Tamara Rogers
Committee Member

Liang Hong
Committee Member

Accepted for the Graduate School:

Alex Sekwat
Dean of the Graduate School

DEDICATION

I dedicate this thesis to my family and to my advisor Dr. Sachin Shetty for their valuable support. Thank you for believing in me. It is also dedicated to the faculty and staff of Electrical and Computer Engineering. I am deeply grateful for the support. Thank you all.

-e.a.t-

ACKNOWLEDGEMENTS

First and foremost I want to thank God for giving me strength and courage to successfully complete this research work.

I express my deepest gratitude to my thesis advisor and mentor Dr. Sachin Shetty, for his valuable guidance and support. He has always given a very beneficial direction to my research work. He has always motivated, corrected and encouraged me as need be.

I would also like to present my sincere appreciation to my committee members Dr. Liang Hong and Dr. Tamara Rogers for their support. I am also grateful to Dr. Devgan, for his assistance and inputs in writing this thesis. My sincere gratitude goes to the entire Electrical and Computer Engineering Department, for offering their support and time whenever I approached them.

Moreover, I would like to express gratitude to my fellow students and researchers in the Computer, Information and Systems Engineering Lab for helping me in different aspects. They were big source of hope and courage in the times of my despair.

Last but not the least; I want to say special thanks to National Science Foundation for funding my research work.

-e.a.t.-

ABSTRACT

PRIYA CHAURASIA. Dynamic analysis of Android Malware using DroidBox (under the direction of DR. SACHIN SHETTY)

With advent of technology, Smartphones have become an integral parts of our lives. Android is one of the most popular open source operating system used in Smartphones.It is also used by technology companies which require ready made, low cost and customizable operating system. Android's open nature has not only invited large community of developers but hackers as well. According to Forbes report, 97% of Mobile Malware in the year 2014 was on Android. Dynamically analyzing the Android Malware using DroidBox will not only provide an insight to this problem but also help in combating.

Mobile sandboxes are gaining popularity as they are able to overcome deception by executing malware in an isolated environment. DroidBox is an excellent mobile sandboxing tool to dynamically analyze the malware. We will utilize it as a base for porting to the recent version of Android. Porting would not only help in effective detection but also putting defenders way ahead in combating evasive mobile malware through an improved version of DroidBox.

Dynamic analysis of Android malware would collect the output generated by the DroidBox consisting of file system access, network activity, interacting with operating system, data sent, data received logs. We will implement porting of DroidBox which will not only help in combating malware but will be effective against all the existing sandboxes. In this thesis, defense strategies applied by Android Malware to thwart dynamic analysis is also investigated.

TABLE OF CONTENTS

LIST OF FIGURES

Table of Figure (Continue)

LIST OF TABLES

LIST OF ACRONYMS AND ABBREVIATIONS

IT	Information Technology
SMS	Secure Messaging Service
OS	Operating Systems
SQL	Structured Query Language
DVM	Dalvik Virtual Machine
UI	User Interface
APK	Application Package
JAR	Java Archive
SEMP	System Engineering Management Plan
IPC	Inter Process Communication
SDK	Software Development Kit
JSON	JavaScript Object Notation

CHAPTER I

INTRODUCTION AND NEED ANALYSIS

1.1 INTRODUCTION

Internet has become an integral part of our lives. There are over 3.1 billion Internet users in the year 2015 which would be approximately 40% of the total world's population. Right from shopping to watching movies, we are completely dependent on it [1].The past decade has seen an unprecedented growth in the field IT and Internet. E-commerce sites have also grown exponentially which in turn has invited Cyber criminals. Traditionally, IT supported business in terms of increasing efficiency and performance but now it being has being transformed into independent business. It is predicted that number of jobs in IT is going to rise by 22% till 2020. US had a market of over 348.9 billion in 2013 of E-commerce. Such a huge turnover of this industry has brought increase in malicious activities. Cyber criminals have used this tremendous opportunity to gain profit financially from this newly established cyber world. As per the Internet Security report by Symantec, one of the leading organizations in the area of malware security. There has been over 60,000 recorded vulnerabilities over the two decades from over 19,000 vendors representing 54,000 or more products which is alarming. Over the years as Internet has advanced and as more and more people have started using it, it is not confined to computers but there's shift in the paradigm. We are gradually moving away from computers to mobile devices [2].

Smartphones have started replacing computers and are gaining huge popularity. As the technology is advancing, the smartphones are not confined just for making calls or sending messages. The sky is the limit, we use it browsing web, social networking, online banking, online shopping, Starbucks coffee, storing credit card details, personal information and the list is endless [3]. You can be a naïve user and still order everything with the touch of a screen. It is estimated that by the end of year 2014-15, the number of smartphones users are going to surpass the number of desktop/computers users worldwide. The graph bel

shows a steady rise in the number of Smartphone users worldwide. The popularity of smartphones has evoked interest from Cyber criminals and made it a haven for malicious activities.

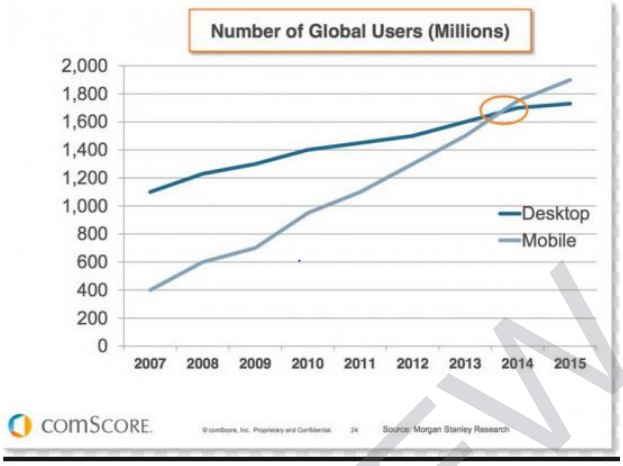

Figure 1.1 Mobile phone users Vs Desktop users [4]

There has been numerous research in the field of smartphone security. Researchers have been studying mobile phone security for years. Initially, the analysis was confined to proof of concept but the malware now has become a real threat. A recent study conducted to categorize the malicious malware activities in smartphones involved stealing user credentials, sending premium rate SMS messages, credential theft, SMS spam, search engine optimization and ransom [5]. As the smartphones are getting more advanced in the software and hardware, the malwares are also evolving. The first malware named Trojan-SMS.Android.fakeplayer was detected by Kaspersky in the year 2010 on Google's Android phone [6]. There's no looking back after that incident.

The traditional method use to detect and analyze malware samples are error prone and time consuming. Therefore, it is required to automate the analysis technique. Dynamic analysis of malware samples would allow us to detect suspicious, possibly malicious applications more effectively. Compared to static analysis, dynamic analysis results are not hindered by obfuscation techniques used by the application which in turn provides more accurate results [7].