UNIVERSITI TEKNOLOGI MARA

COOPERATIVE NETWORK BEHAVIOR ANALYSIS MODEL FOR MOBILE HTTP BOTNET DETECTION

MEISAM ESLAHI

Thesis submitted in fulfillment
of the requirements for the degree of
Doctor of Philosophy

Faculty of Electrical Engineering

February 2017

ABSTRACT

Recently, BYOD or Bring Your Own Device has become one of the most popular methods for enterprises to provide mobility and flexibility in workplaces. The emergence of new technologies and features of mobile devices makes them integral part of every aspect of daily business activities. On the other hand, mobile devices are not well protected compared to computers and their users pay less attention to security updates and solutions , therefore, these new capabilities (e.g. high internet speed and processing power) have motivated the attackers to migrate to mobile infrastructures. Thus, mobile security has become a crucial issue in BYOD or Bring Your Own Device as the employees use their own mobile devices to access an organization data and systems. The mobile attacks and threats come in different forms, such as viruses and worms. However, Mobile Botnets or MoBots are more dangerous as they pose serious threats to mobile devices and communication networks. Bot and Botnets are sophisticated form of organized cyber-crime, which infect different targets (e.g. computers or mobile devices) without attracting the users' attention, which subsequently communicates with each other by using a Command and Control (C&C) mechanism. The main intention of Botnets is to steal the private and personal information (e.g. Zeus and Zitmo) or sensitive information of organizations (e.g. Flame and Stuxnet), thus, several techniques such as encryption and use of standard protocols (e.g. HTTP and Port 80) employed by Botmasters to develop fool-proof C&C mechanism which are difficult to detect. For instance, the AnserverBot, DroidDream, Geinimi, and DroidKungFu are the real world examples of mobile Botnets that use HTTP protocol to hide their activities amongst normal web traffic and stealthily communicate with C&C servers. In fact, Botmasters configure the Bots with regular interval to periodically visit a certain websites contains their updated instructions. Although the periodic behavior of HTTP Bots has been significantly used as a detection measure, most of current studies can detect Bots with fixed interval only. This research proposed a decision tree based model to identify the level of periodicity of HTTP and WEB activities in order to classify them into several categories such as Non-periodic, Periodic, Weak Periodic, Uniform Periodic and Strong periodic. Based on the literature this is the first reported use of classification to categorize the periodic C&C traffic. The results show that the proposed model is able to classify the communication patterns with 95% accuracy and very low rate of false positive of 1.2 % only. However, the level of periodicity alone is not a sufficient factor to detect mobile HTTP Botnets as there are numbers of normal applications such Gmail session, auto refresh pages, and etc. that may pose the same periodic pattern as Botnets. Thus, in addition to this model, a cooperative model using feed forward neural network is also proposed to look for any evidence of mobile Botnet activities. The proposed cooperative detection model is significantly able to detect the mobile HTTP Botnets with 97.8 % of accuracy and 0.5% false positive only.

ACKNOWLEDGEMENTS

Thank God, the most Gracious and Merciful, for all the blessings bestowed on me. The submission of this dissertation marks the end of a somewhat long journey in my pursuit of Ph.D. degree at the Universiti Teknologi MARA (UiTM), Malaysia. The journey would have been difficult if not for all the help, understanding and kindness of many people.

Without doubt, I would like to express my sincere gratitude to my supervisors, Dr. Habibah Hashim and Dr. Nooritawati Md. Tahir for their kindness to take me under their charge to conduct this research. Their patience and encouragement gave me the motivation to work on this research until its successful completion. Their guidance and readiness to share their knowledge have greatly contributed to the direction I should take and what I should do to achieve my goal. I cannot thank them enough, and it is hoped the Malay way of expressing how I feel says it all "Ribuan Terima Kasih".

While doing my studies and research in UiTM, one can say that one is never working alone. I have the friendship, goodwill and support of my course-mates and friends, who have never hesitated to offer their advice and moral support when it is needed.

I would like to express my gratitude and love to my family for their care and understanding when I was doing my research. To the two special women in my life, my mother and my wife Maryam Var Naseri, your boundless love, and for your confidence in me, you have been my pillars of strength and determination to help me to carry on, and if I have succeeded, then you have been a big part of my success, and I dedicate it to both of you together with my love.

TABLE OF CONTENT

	Page
CONFIRMATION BY PANEL OF EXAMINERS	ii
AUTHOR'S DECLARATION	iii
ABSTRACT	iv
ACKNOWLEDGEMENTS	v
TABLE OF CONTENT	vi
LIST OF TABLES	xii
LIST OF FIGURES	xiv
LIST OF ABBREVIATIONS	xvi
CHAPTER ONE: INTRODUCTION	1
1.1 Background	1
1.2 Current Byod Security Models	2
1.2.1 Mobile Device Management (MDM)	2
1.2.2 Mobile Application Management (MAM)	4
1.2.3 Mobile Information Management (MIM)	4
1.3 Why Current Models Are Not Sufficient?	5
1.4 Research Motivation	6
1.5 Statement Of Problem	7
1.6 Research Questions	8
1.7 Research Objectives	9
1.8 Significance Of The Study	9
1.9 Thesis Scope	9
1.10 Thesis Organization	10
CHAPTER TWO: LITERATURE REVIEW	12
2.1 Introduction	12
2.2 Botnets And Organized Cybercrimes	12
2.2.1 DDoS	13
2.2.2 Spamming	14

CHAPTER ONE
INTRODUCTION

1.1 BACKGROUND

The advanced capabilities of new mobile devices (e.g. smart phones) and tablets along with high speed Internet has motivated organizations to use them in the workplace. Bring Your Own Device or BYOD is a new phenomenon in which employees connect their personal mobile devices to an enterprise network to access the corporate information and conduct daily business functions. It simply allows users to engage more with work-related activities by using any specific endpoint devices and smartphone which is independent of time and geographical position [1].

Thus, the BYOD has brought significant convenience and advantages to business activities such as work efficiency and flexibility [2]. In addition, BYOD offers cost efficiency for organizations as they do not need to provide any devices for employees. Therefore, the number of companies using the productivity benefits of personally-owned computing devices is increasing in global scale as it significantly increases the mobility of employment in addition to satisfaction and productivity [3]. Figure 1.1 depicts the growth rate of BYOD in different countries.

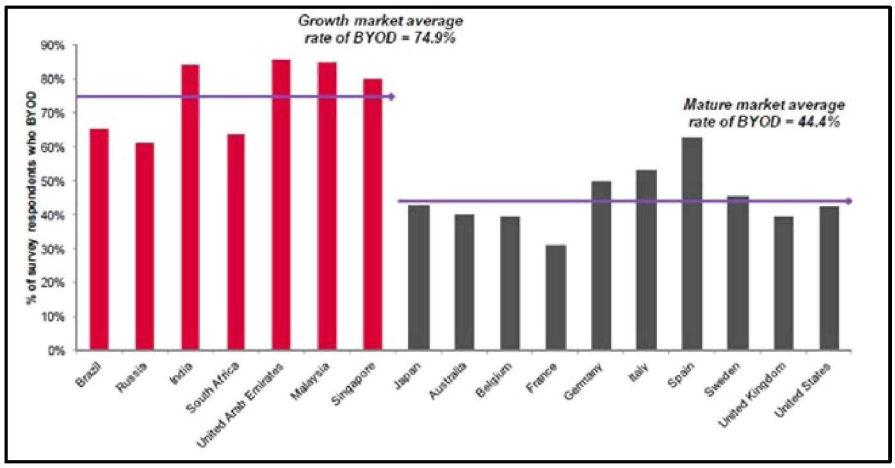

Figure 1. 1: The BYOD Growth Market [4]

Despite the aforementioned benefits achieved by BYOD, the global security state of mobile devices, services and networks is at a critical condition. As depicted by Figure 1-1, there are numbers of high-growth countries in terms of using their own devices in the workplace. However, the number of employees who follow the policies