Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 124 (2017) 664–671

Procedia Computer Science

www.elsevier.com/locate/procedia

4th Information Systems International Conference 2017, ISICO 2017, 6-8 November 2017, Bali, Indonesia

Typosquat Cyber Crime Attack Detection via Smartphone

Zakiah Zulkefli, Manmeet Mahinderjit Singh*, Azizul Rahman Mohd Shariff, Azman Samsudin

School of Computer Sciences,University Sains Malaysia 11800 Penang, Malaysia

Abstract

A Smartphone is a multi-purpose device that can act as both mediums of communications and entertainment due to the availability of various sensors and services, such as SMS, NFC and Bluetooth. Through these functionalities, Smartphone owner can exchange information to each other by sharing links or even files. However, an attacker see these as an advantage to perform an Advanced Persistent Threat (APT) attack. APT is an attack which incorporates both social engineering attack and malware. In this paper, the authors will shed light on how APT attack through spear phishing can occur in Smartphone and how to detect it. First, the authors will examine the tactics that can be used by the attacker to perform a successful social engineering attack. Then, based on the discussion that has been made, the authors have used a machine learning algorithm to classify whether a certain URL is a phish or not. Lastly, the authors have evaluated the propose technique using machine learning and obtained more than 90% accuracy. This proves , that the proposed technique would able to help mitigating APT attack through spear phishing in the Smartphone.

Peer-review under responsibility of the scientific committee of the 4th Information Systems International Conference 2017.

Keywords: Advanced Persistent Threat (APT); Cyber Crime; Typosquat; Smart Phone; Decision Tree

1. Introduction

Advanced Persistent Threat (APT) attack is a carefully planned attack that involved both social engineering and malware, where spear phishing is the most popular method that has been used by the attacker [1]. The attacker will send email to the targeted victim by including link(s) to the targeted web or malicious attachment (e.g. Trojan horse). In order to achieve a high chance of success, the spelling of the link or URL will have high similarity with the link that the victim's frequently accessed to. This is known as typosquatting or url hijacking. Unlike computer, where the

* Corresponding author. Tel.: +604-6535346[2].; fax: +0-000-000-0000 .
E-mail address: manmeet@usm.my

1877-0509
Peer-review under responsibility of the scientific committee of the 4th Information Systems International Conference 2017
10.1016/j.procs.2017.12.203

spear phish is likely to happen through email, there are various mediums that can be used to perform the social engineering attack in Smartphone. For example, in 2013, a Tibetan activist had become one of the targeted victims by a sophisticated attacker through Smartphone [2]. The attacker used the social engineering attack by sending email with Android application's file (.apk) attached. Once the victim has downloaded the file and executed it, the application will act as a backdoor that sends several information to the attacker. This event proof that Smartphone can be used as a medium to perform a sophisticated and well planned attack.

This era, Smartphone has been widely adopted as a personal device to be used in the working environment or known as Bring Your Own Device (BYOD), thus it is very important to protect the device from becoming the next target of an APT. However, there are still lack of research in this area. Most of the research on APT attacks are focused on malware features [8,7,21,22,23] and not on the URL features. Thus, this research will explore how APT attack can occur in Smartphone through url hijack and how to detect it. There are three main objectives of this research. First, to investigate the how APT attack through spear phishing could happen in Smartphone. Second, to propose an enhanced tool for spear phish detection by examine the URL and website features. This proposed technique is called LESSIE, LabEl baSed Spear phIsh dEtection. Third, to further employ the LESSIE and make evaluation by using machine learning technique. The main contribution of this research is a technique on detecting an APT attack through spear phishing on Smartphone by examining the URL that has been received.

This research can be divided into five sections. In Section 2, the research will highlight about how APT can occur in Smartphone and the related works on how to detect phishing website. Then, in Section 3, the research will discuss about LESSIE's components and the experimental setup. In Section 4, the research will discuss about the results that have been obtained and its evaluation. Lastly, in Section 5 will conclude the research's finding.

2. State-of-art

Adopting Smartphones as personal device to be used in a working environment or BYOD might bring benefit towards employee. However, not all of the organizations are aware of the needs to implement security policy on the BYOD in order to prevent information leakage that can happen due to the employee's behaviour and different level of awareness [3]. In this section, the research will discuss in details on how an APT attack can occur in Smartphone and methods that can be used in order to detect it.

2.1. Advanced Persistent Threat (APT) : Definition And Methods

Advanced Persistent Threat (APT) is a sophisticated attack that involves social engineering and malware. In general, the APT attack can be divided into three stages, where each of it are chained together and keep repeating until the attacker has gained the information that they want. They are information gathering, social engineering attack and malware. Previously, there are several real cases of APT attacks that have been reported [4, 5]. APT leave huge impacts to the affected party in term of monetary gain, security and trust relationship. Hence, it is very important to prevent the threat from happening

An APT attack can happen through spear phishing, exploiting the web infrastructure through SQL injection and exploiting the social network [6]. The likelihood and impact of spear phishing attack on BYOD is the highest [7] where, 91% spear phishing of APT attack occur through email [1]. Thus, APT through spear phishing has become the main focus of this research. In this section, details on how the spear phish attack occurs in Smartphone will be discussed.

2.1.1 Spear phish attack in Smartphone

In Smartphone, the medium of spear phishing are email, services and sensors. These sensors are used as a medium to transferring file from one device to another, share services (e.g. connect to headphone) and communication. However, it can be exploited by the attackers in order to perform a spear phish attack by sending malware in the form of .apk file to the targeted victim or sharing malicious links. For example, sending a SMS or MMS that contains URL with/or attachment with it by using content that the user familiar with, transferring malicious file with bluetooth, scanning NFC tag or QR code which later lead the user to a malicious website to download certain document or drive-by-download. Compared to malware, victims usually more prone to click on a URL as malware requires request access