Chapter 11
Information Security Governance:
The Art of Detecting Hidden Malware

Mamoun Alazab
Australian National University, Australia

Paul Watters
University of Ballarat, Australia

Sitalakshmi Venkatraman
University of Ballarat, Australia

Moutaz Alazab
Deakin University, Australia

ABSTRACT

Detecting malicious software or malware is one of the major concerns in information security governance as malware authors pose a major challenge to digital forensics by using a variety of highly sophisticated stealth techniques to hide malicious code in computing systems, including smartphones. The current detection techniques are futile, as forensic analysis of infected devices is unable to identify all the hidden malware, thereby resulting in zero day attacks. This chapter takes a key step forward to address this issue and lays foundation for deeper investigations in digital forensics. The goal of this chapter is, firstly, to unearth the recent obfuscation strategies employed to hide malware. Secondly, this chapter proposes innovative techniques that are implemented as a fully-automated tool, and experimentally tested to exhaustively detect hidden malware that leverage on system vulnerabilities. Based on these research investigations, the chapter also arrives at an information security governance plan that would aid in addressing the current and future cybercrime situations.

INTRODUCTION

A number of criminal justice agencies and organisations are increasing rapidly (Khan, Wiil, & Memon, 2010) and they share responsibility for detecting and stopping digital crime (Kruse & Heiser, 2001). The Regional Computer Forensics Laboratory (RCFL) of the Federal Bureau of Investigation (FBI), in their annual report (RCFL, 2008), stated that 1,756 TBs of data was processed in USA for computer forensic analysis in the year 2008 alone. It was only one year

DOI: 10.4018/978-1-4666-2083-4.ch011

earlier (RCFL, 2007), they had announced that the amount of data to be examined per criminal case would increase by 35% annually, which was immediately surpassed in the subsequent year. In addition, according to recent reports (RSA, 2011) 2010 has witnessed new threats with increased level of sophistication in the attacks, targeting employees in enterprises globally. Only recently there has been a high rise in smartphone malware that warrant further forensic investigations. With online crime escalating to great heights in the form of hidden malware, both in quantity as well as in sophistication of stealth techniques being adopted to inflict computing devices, digital forensics and information security governance have become a major challenge worldwide (Stolfo, Wang, & Li, 2007; Venkatraman, 2010).

Digital forensics is the science of preserving, identifying, extracting, analysing and documenting evidence found in computing devices at crime scenes so that this evidence may be used in a court of law (Vacca, 2005). It also answers questions and attempts to provide full descriptions of a digital crime scene. In computing systems, the primary goals of digital forensic analysis are fivefold: i) to identify all the unwanted events that took place, ii) to ascertain their effect on the system, iii) to acquire the necessary evidence to confirm malicious activity, iv) to prevent future incidents by detecting the malicious techniques used and v) to recognize the incitement reasons and intention of the attacker for future predictions. The focus of this research is on the third goal, to acquire the necessary digital electronic evidence to confirm malicious events that may have occurred on computing devices. Also in this chapter we will illustrate the variety of stealth strategies adopted by malware authors to hide the maliciousness in the devices including smartphones. Based on our experimental investigations performed successfully, we propose detection techniques to identify hidden malware in a systematic method that facilitates in arriving at an information security governance plan that would help in developing, implementing and continuously reforming malware forensic techniques.

Overall, this chapter aims to investigate two main questions with regard to research in digital forensics. Firstly, we need to identify what are the infection strategies undertaken by malicious authors, since that forms the basis of any further investigation that could be fruitful in digital forensics. Secondly, we need to adopt innovative techniques and examine how they could detect hidden malware. Therefore, this chapter is focused on an important research study of the current issues in digital forensics.

The organisation of the remainder of the chapter is as follows. Section 2 provides the trends in malware attacks and the escalated infections due to the recent emergence of smartphones. Section 3 describes current techniques used in data analysis following which previous research work conducted in digital forensics is described in section 4. Our main contributions in this chapter are two-fold: i) to unearth and report the various new strategies employed by malicious authors through our experimental investigations, described in section 5, and ii) to present our proposed innovative techniques that we have implemented as a fully-automated tool to successfully detect unknown and hidden malware, as explained in section 6. In section 7, we provide an information security governance plan derived based on the research study conducted, and finally, a brief summary and conclusions are provided in section 8.

MALWARE ATTACK TRENDS

The continued growth and diversification of the Internet has resulted in the increasing sophistication of tools and methods used to conduct computer system attacks and intrusions (Venkatraman, 2010). Among these attacks, Malware or malicious software is one of the biggest threats posing the digital world (Alperovitch, 2011; RSA, 2011). With more and more use of computers, portable