International Journal of Digital Information and Wireless Communications (IJDIWC) 1(3): 682- 687
The Society of Digital Information and Wireless Communications, 2012(ISSN 2225-658X)

Investigation of Malware Defence and Detection Techniques

Farid Daryabar
Asia Pacific University College of Technology and Innovation
Technology Park Malaysia Kuala Lumpur, Malaysia
farid0fx@yahoo.com

Ali Dehghantanha
Asia Pacific University College of Technology and Innovation
Technology Park Malaysia Kuala Lumpur, Malaysia
ali_dehqan@ucti.edu.my

Hoorang Ghasem Broujerdi
Asia Pacific University College of Technology and Innovation
Technology Park Malaysia Kuala Lumpur, Malaysia
hoorang@ucti.edu.my

Abstract—Malwares are considered as a major threat vector which can be potentially caused huge damage to both network infrastructure as well as network applications.

In this paper, different techniques such as repacking, reverse engineering and hex editing for bypassing host-based Anti Virus (AV) signatures are illustrated, and the description and comparison of different channels and methods when malware might reach the host from outside the networks are demonstrated. After that, bypassing HTTP/SSL and SMTP malware defences as channels are discussed. Finally, a new malware detection technique base on honeynet systems is discussed and its strengths and weaknesses were highlighted.

Keywords: Malware defences, Bypassing malware, Honeynet, Anti Viruses, Penetration Testing.

I. INTRODUCTION

Nowadays, almost every organisation depends on information such as financial, political, etc. By using the Internet protocols these information are transferred through the Internet and almost all internal networks are connected to the Internet directly or indirectly. In the internal networks there are many important systems such as Supervisory Control and Data Acquisition (SCADA) and bank databases, etc [1].

The term malware, which is also called malicious code and malicious software, refers to an executable file or application that are covertly injected to systems. Malware can be Trojan horses, Rootkits, and Backdoors. The main purpose of the malware is compromising the systems' Confidentiality, Integrity and Availability (CIA) [1].

Malware is executed on the internal networks and it provides full controlling the systems by its author when it is on the victim systems. Attacks with malware are the most expensive incidents for the companies and organisations [2].

In general, AV products detect malware in two methods, which are listed below:

1) Signature-based
2) Behavioral based

Signature-based works on the byte or binary patterns, and hashes of the known malware and hashes are saved in a large database of the AV products [3]. The result of comparison between the database of signatures and a program shows that the program is a malware or not [3]. False-positives in the comparison are almost impossible because the signatures are unique[4]. Malware creators often create various versions of a malware to avoid detecting them from AV signature-based method. Therefore, difficulty of the method is egregious when a new version of the malware is created. To prevent the problem, AV vendors utilize generic signatures [4]. Generic signatures method attempt to recognize the whole families of the malware, e.g. by creating a signature for a code segment that is shared by different versions of a malware [4].

Behavioral based detection methods recognize malware either by looking at the codes earlier than it is run or the AV runs it on a virtual sandbox environment to find a malicious activity [4]. By utilizing these methods, it is not needed to have a big database of binary patterns and hashes because the malware is simply recognized by its behavior. Occurring false positives in these methods are more common; therefore, these techniques are not often used [5]. Examples of these activities or behaviors are injection into privileged processes, alteration of critical operating system (OS) or AV files and keystroke logging [5].

Study about bypassing the malware detections considers on protecting the companies' systems. The consideration is based on the functionality of the malware that it cause the malware changes itself to prevent of detection. After that more researches about how to change existing malware to bypass detection have been done [5]. When a specimen malware has been found, the AV vendors can realize a signature or behavior show in the malware by analyzing the malware. To change existing malware to bypass AVs products, attacker is able to find the signature and the behavior, which AV vendors have realized, and then the attacker changes the malware to bypass the defences. Therefore, here AV vendors provide advantages for the attackers [5].

At first, the power rates of AV defences to recognize malware and changing malware's signatures in order to pass the AVs and the gateways are discussed. Then, bypassing 41 AV's programs by simple codes and description of how to detect malware before the malware gets in to the host are given. At the end, because of writing a new malware is the