Chapter 20
Limitation of COTS Antiviruses: Issues, Controversies, and Problems of COTS Antiviruses

Sidney Lima
Federal University of Pernambuco, Brazil

ABSTRACT

Malware (amalgam between the words malicious and software) aims to access a device without the permission of its owner. Undoubtedly, antiviruses are the most popular mechanism in relation for information security. They are present on 95% of personal computers and are associated with combating malicious applications. Technically, the modus operandi of the COTS antiviruses is for the most part the identification of the executable malicious in their datasets nominated blacklist. The major problem with the strategy, adopted by COTS antiviruses, is that in order to detect a new malware, some machines must have already been infected. In order to demonstrate the inefficiency of COTS antiviruses, the authors evaluate the accuracy of conventional antiviruses. On average, the 86 main worldwide antiviruses were able to detect 54.84%, 34.95%, 42.17%, and 16.82% of Portable Executable (PE), Java, JavaScript, and PHP malwares, respectively. Thus, traditional antiviruses have severe limitations when dealing with cyber-pandemic caused by malware.

INTRODUCTION

Malware (amalgamation of malicious and software) aims to access a device without the permission of its owner. The term employed for anti-malware tools is antivirus, not anti-malware, although the virus is only a subcategory of malware. In addition to virus, there are other categories of malware such as Worm, Backdoor, Trojan Horse, Spyware, Rootkit, Ransomware and Botnet.

The damage caused by malware amounts to billions of dollars, as well as the billionaire industry that combats these threats. Just as cyber-criminals are always creating or trying to find new ways to quickly bypass the security of as many people as possible, the industry tries to completely immunize its customers, or at least minimize the damage suffered in the shortest possible time.

DOI: 10.4018/978-1-7998-5728-0.ch020

Research by MCSI (Microsoft Computing Safety Index WorldWide Report) estimates that, worldwide, the financial impact due to malware, Social Engineering or other forms of attacks related to digital identity theft exceeded $23 billion in 2013 alone (Microsoft, 2013). In that year, the amount spent to repair damage to professional reputation, caused by digital scams, was around $4.5 billion. In addition, it is estimated that the time lost due to corrupted, stolen or deleted information by malwares, in 2013 alone, was close to 180 thousand years (Microsoft, 2013).

With the ascent of social networks and with people increasingly connected through mobile devices, confidentiality of information accepts an important role in maintaining the dignity, finances and mental health of legitimate users. From malware infection, a person or institution can have irrecoverable losses. As for a person, their bank passwords, social networks, photos or intimate videos can be shared in World Wide Web, which will affect his/her finances, dignity and mental health. In other side, an institution may have its vital data inaccessible and/or information from its customers and employees stolen.

Then, due to the losses, which are largely irreversible, more and more investments are being made in digital security through new technologies associated with antivirus, firewalls and biometrics. It is estimated that antivirus services are present in 95% of personal computers, while firewall services are activated by 84% of Internet users and 82% have automatic updates activated on their Microsoft OS (Operating System) (Microsoft, 2013).

The promised protection is not always fulfilled. One of the explanations concerns the retrograde methods of COTS antiviruses. One method is the blacklist, a reactive method where the client's suspicious file is compared to a previously catalogued threat dataset. The major problem with this strategy, adopted by COTS antiviruses, is that in order to detect a new virtual pest, it is required that some machines have already been infected. It is important to emphasize that it is not only enough the detection and elimination of the malicious application for the victim to be free of its action. Besides the elimination of malware, it is necessary to undo all its malfeasances, such as having disabled the victim's defense mechanisms, including firewall, security plugins and the antivirus itself. Such disinfection of malware is technically named vaccine. Then, the strategy of waiting for the victim to become infected and subsequently reporting an anomalous behavior from their device is not appropriate.

In addition, some commercial antiviruses share this suspicious executable in small chunks. Thus, if one or more chunks of the suspect executable are present in the antivirus database (blacklist), then it is classified as malware. It should be noted that the comparison between suspect application chunks and the antivirus database may become impractical because millions of malwares are created annually (VirusShare, 2020). Then, investigating the presence of parts of a suspect executable in all the millions of malicious samples is possibly an unfeasible computational problem since this task could last for months or years.

As a general rule, antiviruses are just catalogs of malware. Antiviruses scan the computer comparing suspicious files with their catalogs (blacklist). If a malware is not contained on its blacklist, the COTS antivirus will not detect this malicious application. It should be emphasized that malware will only be present on a blacklist if it has a very wide range. By range, it is denoting that the symptoms of a certain malware are reported by a large number of users. It is assumed that it is not economically viable for COTS antivirus to allocate physical and human resources to create the vaccine for a low-range malware.

In case of a suspicious application, the customer submits to the quarantine period. Instead of a controlled environment (SandBox), the suspicious application is investigated on the client's own private computer. If malware is confirmed, the victim will suffer the malfeasance caused by the malicious application. Thereafter, the COTS antivirus blacklisted the application that was once quarantined. In