Chapter XX
Malware:
Specialized Trojan Horse

Stefan Kiltz
Otto-von-Guericke University, Germany

Andreas Lang
Otto-von-Guericke University, Germany

Jana Dittmann
Otto-von-Guericke University, Germany

ABSTRACT

The Trojan horse can be used in cyber-warfare and cyber-terrorism, as recent attacks in the field of industrial espionage have shown. To coordinate methods of defence a categorisation of the threat posed by Trojan horses in the shape of a list of tuples is proposed. With it, a set (consisting of methods for the distribution, activation, storage, means of execution, communications, malicious functionality) can be defined, which describes the Trojan horse by its features. Each of these aspects can be accompanied by methods of self-defence (e.g., armouring or encryption) against detection and removal by protection software. The list of tuples and therefore the categorisation of the Trojan horse properties is a vital first step to develop and organise counter measures against this kind of threat. A new category of Trojan horses, the special and universal Trojan horse, is proposed. This type of malware is particularly well suited for cyber-warfare and cyber-terrorism, as it unlikely to be picked up by common protection software (e.g., virus scanner). To achieve this, a Trojan horse is tailor-made for one special attack of a particular computer system and can provide espionage or sabotage functionality. If it is not used on large-scale attacks, anti-malware software producers will have little or no chance to extract a signature for this code. Systems being spied upon without notice can deliver vital information for the attacker. In addition, the attacker can choose to permanently or temporarily disrupt IT-infrastructure (e.g., denial-of-service, destruction of hardware). The universal Trojan horse can be updated by the attacker to achieve an extended functionality which makes it universal. The above-proposed list of tuples can be a tool to describe such special and universal Trojan horses which will be introduced in the full item description.

INTRODUCTION

Trojan horses as a special kind of malware (malicious software) have been around for quite some time. The threat prosed by this sort of program should not be underestimated. Therefore, the manufacturers of antivirus software today offer means to detect and, if possible, to remove Trojan horses from a computer system. But they almost exclusively rely on signatures to detect this sort of program. If a carefully crafted Trojan horse is used only once or at least very rarely, chances are that this piece of malware will remain undetected, simply because no one could record a signature for this particular code and integrate that signature in antivirus databases. Such a Trojan horse can be used in cyber warfare and cyber terrorism, as recent attacks in the field of industrial espionage have shown (Neumann, 1997).

This chapter will show the threat posed by this subcategory of Trojan horses. It will then propose ways to systematically describe the characteristics of this type of malware. Such a classification can be the first step to finding suitable countermeasures against that type of malware.

BACKGROUND

Trojan horses as a special form of malware got their name from the tales of Greek mythology, where an entire army was hidden in an enormous wooden horse that was given as a present to the people of the city of Troy. The gift provided a means to bypass the heavily defended outer wall and attack the city from the inside (Trojan War, 2005).

Similarly, computer programs pretending to be useful to the user and also having hidden, undocumented and malicious features are called Trojan horses. Or as Matt Bishop (Trojan War, 2005, p. 614) defined: "A Trojan horse is a program, that has overt (documented and known) functions as well as covert (undocumented and unexpected) functions."

Trojan horses often use the techniques of social engineering. That means that the user is tricked into installing and running the program. All the automated defenses, such as firewalls, e-mail spam filters, and so forth, are of no use because the user insists on running the program.

MAIN THRUST OF THE CHAPTER

The Special and Universal Trojan Horse

With Trojan horses having been around for some time, the authors will now focus on a new and dangerous subcategory of Trojan horses, the special and universal Trojan horse (Dittman & Lang, 2004). This type of malware is particularly well suited for cyber warfare and cyber terrorism, as it unlikely to be picked up by common protection software (e.g., virus scanner). To achieve this, a Trojan horse is tailormade for one special attack on a particular computer system and can provide espionage or sabotage functionality. If it is not used on large-scale attacks, antimalware software producers will have little or no chance to extract a signature for this code. Systems being spied upon without notice can deliver vital information for the attacker. In addition, the attacker can choose to permanently or temporarily disrupt information technology (IT) infrastructure (e.g., denial-of-service, destruction of hardware).

The authors define a special and universal Trojan horse as follows: "A special and universal Trojan horse is a specialised piece of code that is purpose built to attack a particular computer system in such a way that it allows the attacker unauthorised and universal access to the victim computer system." What makes this Trojan horse *special* is the choice of properties of the code that is tailored to the demands of the system being attacked. Such a Trojan horse is also *universal* in that allows the attacker to reconfigure the functionality of the code at run time.

Although some protection mechanisms (e.g., firewalls) allow for blind blocking, that is, defense against a threat without prior detection, in order to detect Trojan horses, it is often necessary to detect