IDEA GROUP PUBLISHING **ITB13035**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This paper appears in the publication, *Digital Crim and Forensic Science in Cyberspace*
edited by Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis, and Drakoulis Martakos

Chapter II

Malware: An Evolving Threat

Steven Furnell, University of Plymouth, UK

Jeremy Ward, Symantec EMEA, UK

Abstract

In the two decades since its first significant appearance, malware has become the most prominent and costly threat to modern IT systems. This chapter examines the nature of malware evolution. It highlights that, as well as the more obvious development of propagation techniques, the nature of payload activities (and the related motivations of the malware creators) is also significantly changing, as is the ability of the malware to defeat defences. Having established the various facets of the threat, the discussion proceeds to consider appropriate strategies for malware detection and prevention, considering the role of modern antivirus software, and its use alongside other network security technologies to give more comprehensive protection. It is concluded that although malware is likely to remain a significant and ever-present threat, the risk and resultant impacts can be substantially mitigated by appropriate use of such safeguards.

Introduction

Malicious software (malware) such as worms, viruses, and Trojan horses are now amongst the most readily recognised threats to computing systems. Indeed, malware has been the principal computer security problem for the PC generation, and has certainly

dominated the scene since mass adoption of the Internet began in the mid-1990s. However, the beginnings of the malware problem go back significantly beyond this. For example, while the precise origins of Trojan horse programs are unknown, the ultimate arrival of worms and viruses can be linked back to the earliest thinking about self-replicating systems, such as the proposal of "cellular automata" (von Neumann, 1948). Such "automata" introduce the concept that information can be encoded with simple rules in such a way that it is able to self-replicate and spread throughout a system. Effectively it is this concept that was used by Watson and Crick when, five years later, they published the structure of DNA— the molecule which encodes the information used to replicate organic life-forms. Some 30 years later, security researcher Frederick Cohen first used the term 'computer virus' to describe a self-replicating piece of code within an IT system (Cohen, 1994). In an interesting parallel development, Richard Dawkins' book *The Selfish Gene* (Dawkins, 1976), introduced the concept that all living organisms are the "puppets" of self-replicating pieces of code. These are the concepts that lie behind the examination of the evolution of the malware threat which is the subject of this chapter.

The discussion in this chapter aims to examine the evolution of the malware threat, and the consequent demands that it now raises in terms of protection. The next section presents some of the core terminology, and highlights the prevalence of the malware threat in relation to current systems. The third section considers the range of motivations that may lead to malware being written and released, which gives an insight into the reasons for the threat. The fourth section examines the ways in which malware has evolved, focusing upon the techniques that it may use to harm systems, as well as those that it uses to propagate and ensure its own survival. Having identified a clear threat, the next section identifies the various measures that should be considered in order to detect and prevent malware, including safeguards at both the system and network levels to provide a comprehensive overall strategy. The chapter concludes with an overall summary and thoughts on the future outlook. It should be noted that the discussion does not seek to address the software level implementation and functionality of the malware. However, readers interested in these aspects can find relevant information in a number of published sources (Skoudis & Zeltser, 2003; Harley, Slade, & Gattiker, 2001).

Background

At a general level, the term "malware" can denote any piece of computer code that has a malicious or unwanted effect on an IT system or network. While there are literally thousands of individual examples of malware, the key categories are typically considered to be the following:

- **Virus:** A replicating program that enters a system by infecting "carrier" materials such as disks, files, or documents. A virus may carry a payload, which will activate at some point after infection, causing unwanted and often damaging effects. It is worth noting that the term "virus" is often misused as a generic label for all forms