Chapter XIII
Prevention and Handling of Malicious Code

Halim Khelafa
University of Wollongong in Dubai, United Arab Emirates

ABSRACT

The purpose of this chapter is to provide a wide spectrum of end users with a complete reference on malicious code or malware. End users include researchers, students, as well as information technology and security professionals in their daily activities. A particular effort aims at educating users about malware, enhancing organization capabilities for preventing as well as handling malicious code incidents when they occur, and preparing them for tomorrow's new types of malware, as well as the new types of safeguards they should consider. First, the author provides an overview of malicious code, its past, present, and future. Second , he presents methodologies , guidelines and recommendation on how an organization can enhance its prevention of malicious code, how it should respond to the occurrence of a malware incident, and how it should learn from such an incident to be better prepared in the future. Finally, the author addresses the issue of the current research as well as future trends of malicious code and the new and future means of malware prevention.

INTRODUCTION

The information age has revolutionized all sectors of human activity: business, health care, education, even entertainment. However, this has come with a price; these enhancements bring about new threats from an ever technically sophisticated group of hackers. Stevens (2006) distinguishes four major types of attacks: network intrusions, viruses, worms, rootkits, and poisoning of the Domain Name Service. Tremendous losses can result from suck attacks. According to the FBI computer crime and security survey of 2005, losses due to viruses accounted for US$42,787,667 out of a total loss of US$130,104,542. In addition, the respondents to the survey have consistently put

viruses as the type of attacks with the highest occurrences (more than 70%). Virus is a concept used by the general public. A more appropriate description would be malicious code or malware. Even though, some authors make a difference between malware and malicious code, the terms will be used interchangeably because of the convergence of the different malware vectors.

The term *malicious code* is a recent term in the taxonomy of information security. It can be defined as any program or piece of code that interferes with the proper operation of a computer or a network. The categories of malicious code are no longer restricted to viruses, worms, and Trojan horses, but new breeds of malicious code have emerged with the development of the Internet in general and online business activities in particular. Hoefemeyer (2004) asserts that malicious code attacks are quite similar to biological ones, with one crucial difference: the propagation of malware infections is significantly faster than biological ones thanks to the Internet. In matters of hours,

Figure 1. Financial impact of malware estimated in billions of U.S. dollars (Anonymous, 2005)

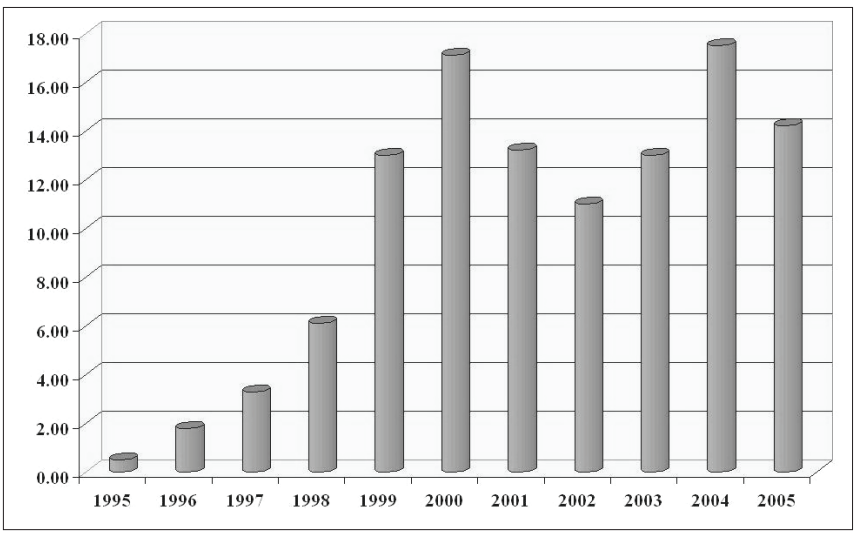

Figure 2. Percentage of financial impact of malware (Anonymous, 2005)