Malware and Antivirus Procedures

Xin Luo
Mississippi State University, USA

Merrill Warkentin
Mississippi State University, USA

INTRODUCTION

The last decade has witnessed the dramatic emergence of the Internet as a force of inter-organizational and inter-personal change. The Internet and its component technologies, which continue to experience growing global adoption, have become essential facilitators and drivers in retailing, supply chain management, government, entertainment, and other processes. However, this nearly-ubiquitous, highly-interconnected environment has also enabled the widespread, rapid spread of malware, including viruses, worms, Trojan horses, and other malicious code. Malware is becoming more sophisticated and extensive, infecting not only our wired computers and networks, but also our emerging wireless networks. Parallel to the rise in malware, organizations have developed a variety of antivirus technologies and procedures, which are faced with more challenging tasks to effectively detect and repair current and forthcoming malware. This article surveys the virus and antivirus arena, discusses the trends of virus attacks, and provides solutions to existing and future virus problems (from both technical and managerial perspectives).

BACKGROUND

Global networks and client devices are faced with the constant threat of malware attacks which create burdens in terms of time and financial costs to prevent, detect, repel, and especially to recover from. Viruses represent a serious threat to corporate profitability and performance, and accordingly, this constant threat of viruses and worms has pushed security to the top of the list of key issues (Palmer, 2004). Computer virus attacks cost global businesses an estimated $55 billion in damages in 2003. Companies lost roughly $20 billion to $30 billion in 2002 from the virus attacks, up from about $13 billion in 2001 (Tan, 2004). Sobig.F virus, for instance, caused $29.7 billion in economic damage worldwide (Goldsborough, 2003) (see Tables 1 and 2). Mydoom and its variants have infected 300,000 to 500,000 computers (Salkever, 2004), and Microsoft has offered $250,000 for information leading to the arrest of the worm writer (Stein, 2004). The most recent Sasser worm has infected millions of users including American Express (AMEX), Delta Airline Inc. and some other Fortune 500 companies. And Netsky-D worm has caused $58.5 million in damages worldwide (Gaudin, 2004). Furthermore, CSX, the biggest railroad company in USA, had to suspend its services in the metropolitan Washington DC area due to the activity of Nachi worm in 2003. Air Canada cancelled its flights because its network failed to handle the amount of traffic generated by the Nachi worm. Many organizations, whether high, medium, or low profile, such as The Massachusetts Institute of Technology (MIT) and the U.S. Department of Defense have been the victims of viruses and worms. (For more perspective on the financial impact of malware, see Tables 1-4 and Figures 1-2.)

Since the early 1990s, computer viruses have appeared in the world of IT and become more changeable and destructive in recent years, as today's computers are far faster, and as the vulnerabilities of the globally connected Internet are being exploited. Today's hackers can also easily manipulate existing viruses so that the resulting code might be undetectable by antivirus application; they may even insert malicious code into files with no discernable trace to be found, regardless of digital forensics examiner's competence and equipment (Caloyannides, 2003).

A virus is a piece of programming code usually disguised as something else that causes some unexpected and usually undesirable event. Viruses, unlike

Table 1. Top 10 viruses in 2003

Rank	Virus	Percentage of reports
1	W32/Sobig-F	19.9%
2	W32/Blaster-A	15.1%
3	W32/Nachi-A	8.4%
4	W32/Gibe-F	7.2%
5	W32/Dumaru-A	6.1%
6	W32/Sober-A	5.8%
7	W32/Mimail-A	4.8%
8	W32/Bugbear-B	3.1%
9	W32/Sobig-E	2.9%
10	W32/Klez-H	1.6%
Others		25.1%

Source: Sophos.com (http://www.sophos.com)

Table 2. Number of security incidents reported to CERT from 1995-2003

1995	1996	1997	1998	1999	2000	2001	2002	2003
2,412	2,573	2,134	3,374	9,859	21,756	52,658	82,094	137,529

Source: Computer Economics (http://www.computereconomics.com/article.cfm?id=936)

Figure 1. Number of security incidents reported to CERT from 1995-2003

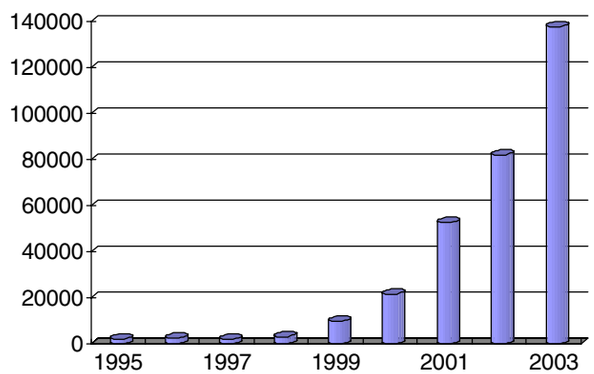

Figure 2. Annual global financial impact of major virus attacks 1995-2003

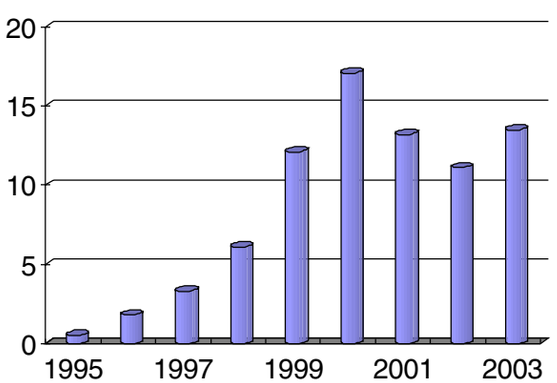

Table 3. Annual global financial impact of major virus attacks 1995-2003

Year	Impact ($U.S.)
2003	$13.5 Billion
2002	11.1 Billion
2001	13.2 Billion
2000	17.1 Billion
1999	12.1 Billion
1998	6.1 Billion
1997	3.3 Billion
1996	1.8 Billion
1995	500 Million

Source: Computer Economics

http://www.computereconomics.com/article.cfm?id=936

worms, must attach themselves to another file (typically an executable program file, but can infect dozens of file types, including scripts and data files with embedded macros) in order to propagate. When the host file is executed, the virus's programming is also executed in the background. Viruses are often designed so that they can automatically spread to other computer users (Harris, 2003) by various