Chapter XI
Viruses and Virus Protection in Cybercafés

Alex Ozoemelem Obuh
Delta State University, Nigeria

ABSTRACT

The objective of this chapter is to give an insight to virus, virus infection, and prevention in cybercafés. Specifically, it gives the meaning of virus, types of viruses, classification of viruses, sources of viruses in cybercafés, why cybercafé systems are vulnerable to attacks or infections, how to detect virus infections or symptoms of virus infection in cybercafé systems or networks, virus prevention and control, and future trends. It is argued that with the advent of WiFi technologies, virus writers can launch their dubious malcode from just about anywhere in the world, and as such there exist a form of cyber-terrorism that cannot be easily stopped.

INTRODUCTION

As computers gained in popularity in the early 1980's, more and more individuals started writing their own programs. Advances in telecommunications provided convenient channels for sharing programs through open-access servers such as BBS—the bulletin board system. Eventually, university BBS servers evolved into a global data bank and were available in all developed countries. The first *Trojans* appeared in large quantities; programs that could not self-replicate or spread, but did damage systems once downloaded and installed.

The widespread use of Apple II computers in 1981 predetermined this machine's fate in attracting the attention of virus writers. It is not surprising that the first large-scale computer

virus outbreak in history occurred on the Apple II platform.

Elk Cloner spread by infecting the Apple II's operating system, stored on floppy disks. When the computer was booted from an infected floppy, a copy of the virus would automatically start. The virus would not normally affect the running of the computer, except for monitoring disk access. When an uninfected floppy was accessed, the virus would copy itself to the disk, thus infecting it, too, slowly spreading from floppy to floppy. The Elk Cloner virus infected the boot sector for Apple II computers. In those days, operating systems were stored on floppy disks: as a result the floppies were infected and the virus was launched every time the machine was booted up. Users were startled by the side effects and often infected friends by sharing floppies, since most people had no idea what viruses were, much less how they spread.

The Elk Cloner payload included rotating images, blinking text and joke messages like:

Elk cloner: *The program with a personality it will get on all your disks it will infiltrate your chips yes, it's cloner it will stick to you like glue it will modify ram, too send in the cloner!*

Len Eidelmen first coined the term 'virus' in connection with self-replicating computer programs. On November 10, 1983, at a seminar on computer safety at Lehigh Unversity, this grandfather of modern computer virology demonstrated a virus-like program on a VAX11/750 system. The program was able to install itself to other system objects. A year later, at the seventh annual information security conference, he defined the phrase 'computer virus' as a program which is able to 'infect'other programs by modifying them to install copies of itself.

The first global IBM-compatible virus epidemic was detected in 1986. Brain, which infected the boot sector, was able to spread practically worldwide within a few months. The almost total lack of awareness in the computing community of how to protect machines against viruses ensured Brain's success. The Brain virus was written by a 19 year old Pakistani programmer, Basit Farooq Alvi, and his brother Amjad, and included a text string containing their names, address, and telephone number. According to the virus's authors, who worked in sales for a software company, they wanted to gauge the level of piracy in their country. Aside from infecting a disc's boot sector and changing the disk name to '© Brain,' the virus did nothing; it had real payload, and did not corrupt data. Unfortunately, the brothers lost control of their so-called experiment and Brain spread worldwide.

Interestingly enough, Brain was also the first '*stealth virus*.' When an attempt to read the infected sector was detected, the virus would display the original, uninfected data.

That same year, a German programmer, Ralf Burger, invented the first programs that could copy themselves by adding their code executable DOS files in COM format. The working model of the program, named Virdem, was introduced by Burger in December 1986 in Hamburg at an underground computer forum, the Chaos Computer Club. Though most of the hackers at the event specialized in attacking VAX/VMS systems, they were still interested in the concept.

The objective of this chapter is to give the meaning of virus, types of viruses, classification of viruses, sources of viruses in *cybercafés*, why *cybercafé* systems are vulnerable to attacks or infections, how to detect virus infections or symptoms of virus infection in *cybercafé* systems or networks, virus prevention and control, and future trends.

Virus

Fred Cohen (1983) defined a computer virus as "a program that can 'infect' other programs by modifying them to include a version of itself." This means that viruses copy themselves, usu-