**IDEA GROUP PUBLISHING** **ITB11408**

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 chapter appears in the book, *Managerial Guide for Handling Cyber-Terrorism and Information Warfare* by Lech J. Janczewski and Andrew Colarik © 2005, Idea Group Inc.

## Chapter 5

# Denial of Service Threat

In the early 1960s, programmers used to play *memory games* on a computer. The objective of the game was to disable as much of the operating system memory as possible in order to make their opponents unable to run their applications. In those days it was not anticipated that the whole idea would reemerge some 35 years later to become one of the most treacherous concepts in disabling vast computer networks. Denial of Service (DOS) attacks are here to stay for the foreseeable future.

In the previous chapter, we discussed the issue of physical protection as perhaps the most direct threat to IT from terrorist groups or individuals. The attacks could be either direct against the IT resources, which is less probable, or collateral, resulting from attacks against the other targets physically located nearby. On the other hand, DOS attacks are purely IT-based and may be classified as a typical information warfare tool. They can also be used by cyber-terrorists.

So what classification of DOS attacks is justified? To be employed as a suitable cyber-terrorist tool, we believe that a number of conditions must apply. Among them are the following:

- An attack should not involve lengthy preparations and should not require a considerable amount of funds.
- The essence of a terrorist attack is to inflict as much damage as possible.

- The damage should be spectacular, noticeable, and understandable by a wide audience. Unauthorized electronic transfer of funds may cause a lot of damage to the bank, but may not be noticed. As a matter of fact, banks usually try to keep the publicity about such attacks at a minimum.

DOS attacks and their offspring, Distributed Denial of Service (DDOS) attacks fulfill these conditions in the IT domain, they are relatively easy to launch, and the destruction they inflict can be spectacular.

## The Nature of DOS and DDOS Attacks

The idea behind DOS and DDOS attacks is very simple: to force a target system to become overloaded with activities that reduce its capacity to process legitimate tasks. These activities are arranged in such a way that starting one triggers an avalanche of other activities. An example of a DOS attack is the so-called *Christmas Tree* worm. When it was first launched through the IBM network in Europe in the early 1970s, it was not intended as a DOS attack. The initial idea was to spread the picture of a Christmas tree on the screens of computers connected to the network. To accomplish this task, the Christmas Tree software extracted the addresses of the correspondents from the target machine and forwarded to them the tree picture. As a result, the whole network was saturated with pictures of a Christmas tree on every screen, and there was no room in memory for any other jobs to be processed.

A typical DOS attack may be successful against a small Web site, but a powerful site like Amazon.com or eBay.com can easily handle such a flood of messages. As a result, the idea of the DDOS attack was conceived. The DDOS concept is as follows:

- The attacker first decides which type of DDOS attack to use, against which site to use it, and when it will be implemented. There are many different DDOS attacks (e.g., UDP flood, ICMP flood, SYN flood, SMURF), which will be presented later in the text.
- The attacker then must find a number of hosts that are used later as launching pads against the victim site. Security of these sites must be questionable and allow the implantation of the attacking software (usually