In the previous article in this series, we looked at some of the fundamental reasons that systems on the Internet are so vulnerable to such attacks. In this article, I review some methods for interfering with DDoS by stopping the spurious outbound traffic.

* * *

The best description I have found of how to fight DDoS at its root is the document "Help Defeat Denial of Service Attacks: Step-by-Step, Revision: 1.41" from the System Administration and Network Security (SANS) Institute <http://www.sans.org/dosstep/index.htm>. This guide enumerates and explains the steps in setting up barriers to harmful flows of spurious packets designed to cause trouble for recipients. The topics are as follows:

1. Egress filtering to stop spoofed IP packets from leaving your networks
   1.1 Deny invalid source IP addresses
   1.2 Deny private and reserved source IP addresses
2. Stop your network from being used as a broadcast amplification site
   2.1 Disable IP directed broadcast on all systems
   2.2 Test your network to determine if it is an amplification site
   2.3 Require that vendors disable IP directed broadcast by default


To track and destroy zombie programs on intermediate systems, one can use the PestPatrol software <http://www.pestpatrol.com> from SaferSite. This program has been developed to attack malicious non-viral programs; among the crew at SaferSite are my good friends Bob Bales, Pete Cafarchio, Don Krysakowski, Pam Martin, Barbara Rose David Stang and others -- folks I have known for years from our involvement in the early days of the National Computer Security Association (NCSA). The categories of pests that PestPatrol can identify and remove are listed at <http://www.pestpatrol.com/PestPatrol/PestPatrolCategories.asp>; in particular, the program recognizes and destroys 138 DoS tools and 24 DDoS tools. The Web site provides a searchable database <http://www.pestpatrol.com/PestPatrol/pestdatabase.asp> that allows anyone to find detailed information about all sorts of pests.

* * *

In the next article in this series, we will look at stopping inbound DDoS traffic.

* * *
M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services.

Copyright © 2001 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.