In the previous article in this series, we looked at stopping inbound DDoS traffic at the enterprise level. In this final article, I point to a couple of products that stop spurious traffic upstream, at the Internet Service Provider level.

* * *

A different location in the Internet is used by other anti-DDoS tools: the upstream Internet Service Providers. The TrafficMaster system from Mazu Networks sits on large-bandwidth pipes upstream from the protected system; this positioning is advantageous because data collection can be carried out on data streams that are directed to many different customers of the ISP. Such central monitoring allows rapid identification of attack patterns when there are multiple targets. The TrafficMaster Inspector module is capable of monitoring up to OC-12 bandwidth (622 Mbps) with no slowing of throughput. The TrafficMaster Enforcer module is essentially a single-purpose firewall dedicated to eliminating spurious traffic identified as a DDoS attack.

Arbor Networks produces the Peakflow DoS tool, which also works upstream. This specialized product is designed for carriers with large bandwidth, although it can also be applied to enterprise networks. As I understand it, this system does rely on human intervention for effective blocking of DDoS traffic; in the caption to a diagram of the system process, the company writes, "1. Traffic enters the Service Provider network. 2. Monitor: Peakflow DoS Collectors analyze traffic for anomalies without disrupting traffic flow to routers. 3. Detect: Peakflow DoS collectors create and forward unique anomaly fingerprints to Peakflow DoS Controllers. 4. Trace: Peakflow DoS Controllers then quickly trace the attack to its source. 5. Filter: Peakflow DoS Controller recommends filters, which the network engineer can implement to stop the attack before it brings down key routers, firewalls and/or the entire network."

NetScreen Technologies Inc. manufactures high-speed network security devices, including anti-DDoS systems. There is an impressive list of White Papers on the site; unfortunately, one has to register for the privilege of reading their White Papers by providing full contact information. Since there appears to be no privacy policy listed on their site -- and I checked thoroughly -- I declined to do so. However I did write to NetScreen before sending the draft article to NetworkWorld Fusion and got a very courteous and concerned response from Mr Jeff Wenker, Manager of Public Relations for the firm. Mr Wenker assured me that the company is working on a privacy policy and categorically stated that they "do not share any of the information visitors submit with
parties unaffiliated with NetScreen."

In conclusion, there are several methods available for interfering with the wretched behavior of irresponsible fools and scoundrels who spew their fraudulent packets all over the Internet to cause harm to others. The more sites there are that respond effectively to such denial-of-service attacks, the more likely that law enforcement will be able to use log files to track down the perpetrators and prosecute them for these outrages.

As for me, I run two firewalls on my PC and automatically update my antivirus software and my PestPatrol software to catch and remove malicious software of all kinds.

I encourage everyone to do their part in fighting this scourge.

* * *

Disclaimer: the author has no financial or any other interests in the companies named in this article. All references are for information purposes only and are not to be construed as product endorsements.

* * *

In the next and last article in this series, we will look at methods of stopping a flood attack at the upstream ISP level.

* * *

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.