In the previous article in this series, we looked at stopping spurious outbound traffic. In this article, I review methods for stopping inbound DDoS traffic.

* * *

One approach for stopping the stream of fraudulent packets generated by DDoS tools is exemplified by the solutions offered by Captus Networks. Their CaptIO device (<http://www.captusnetworks.com/product_overview.html>) is a specialized processor that recognizes DDoS traffic before it reaches the protected network. CaptIO removes the spurious packets from the data stream before the routers and firewalls can be disturbed. No user intervention is required, and the rule that blocks the junk is removed automatically when the attack subsides. Depending on the model, these devices can service 9 to 12 networks. As I mentioned in an earlier article, this approach resembles the solutions for handling heavy data communications traffic back in the early 1980s, when some mainframe and minicomputers still allowed every single character to interrupt the main processor; manufacturers added specialized communications controllers that handled all the character-by-character interrupts and passed completed command or data strings to the main CPU only when a line delimiter (e.g., CR/LF) was encountered. The major advantage to the CaptIO approach is that adaptation to the attack packets is much quicker than anything a human being could do, thus staunching a DDoS attack before it reaches noticeable levels.

Asta Networks recently announced its Vantage System (<http://www.astanetworks.com/news/press/relief.html>) for fighting DDoS; according to its press release, "Vantage System is composed of Sensors, network appliances that collect traffic data from key routers, and Coordinators, servers that aggregate and analyze data from the Sensors to construct an overall view of network activity for the network operator or engineer. Several phases of analysis are conducted to provide all the actionable knowledge Network Operations Centers need to immediately detect an attack, locate its source, and counter it with the most appropriate measures to ensure continued flow of good traffic."

* * *

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.