Attack on domain name servers fails

October 23rd, 2002
By Robert Lemos, CNET News.com

An assault on all 13 domain-name service root servers attempts to shut down the address books of the Internet. An attempt to cripple the computers that serve as the address books for the Internet failed on Monday.

The so-called distributed denial-of-service attack leveled a barrage of data at the 13 domain-name service root servers beginning around 1 pm PDT on Monday and apparently is ongoing, according to Internet performance measurement company Matrix NetSystems. Traffic from several Internet service providers have been slightly delayed, but because the domain name system is spread out and because the 13 root servers are the last resort for address searches, the attack had almost no effect on the Internet itself.

"There was never an end user that said there was a problem," said Paul Vixie, chairman of the Internet Software Consortium, a group that supports the open-source software on which many domain name servers run.

The group also administers one of the 13 computers -- specifically, the "F" server -- that routinely matches Internet addresses. Like the telephone book, domain name servers match a name with a number. They also are layered like a virtual onion, so that a user who wants to go to specific address, such as "cnet.com", will first attempt to get the information from a local server. If the domain is not found, then the request gets bumped up to a domain name server for the top-level domain, such as ".com".

Requests should only rarely consult the root servers. Most requests that the ISC's "F" server sees are from poorly designed networks that don't cache the previous answers for information, Vixie said.

"We answer a request and then two milliseconds later get another request from the same user for the same domain," he said.

While Vixie took issue with reports that the attack had been the "largest ever", he did say that aspects of the data flood made it unusual. "There have been (previous) attacks against the root domain servers -- yes," he said. "But it is rare to have attacks against all 13 at the same time."

The Internet Software Consortium's "F" server responds to more than 270 million domain-name service queries each day, according to its site.

The 13 domain-name service root servers are designated "A" through "M". The most affected servers, according to Internet performance firm Matrix NetSystems, were the "A" and "J" servers owned by VeriSign Global Registry Services in Herndon, Virginia, the "G" server owned by the US Department of Defense Network Information Center in Vienna, Virginia, the "H" server at the US Army Research Lab Aberdeen, Maryland, the "I" server located in Stockholm, the "K" server located in London and the "M" server in Tokyo.

Still, the results were not severe. According to Matrix NetSystems, the peak of the attack saw the average reachability for the entire DNS network dropped only to 94 percent from its normal levels near 100 percent.

About 4,000 denial-of-service attacks hit the Internet in the average week, according to data collected by the Cooperative Association for Internet Data Analysis. Many of those are aimed at domain name servers.

Attacks that broadly affect the Internet are rare. In April 1997, a misconfigured router advertised itself to the Internet as the quickest gateway to every other server and caused a ripple that affected communications for several hours.

Domain News Archive

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
2003	13	10	13	5	0	0	0	0	0	0	0	0
2002	0	0	0	0	0	0	1	0	3	14	9	27