



DNS attacks could be a warning shot

11/04/02

*By William Jackson,
GCN Staff*

Last month's concerted denial-of-service attack on the Internet's Domain Name System root servers, though unsuccessful, was a sign of things to come.

"The incident is significant not because it was effective but because it represents an escalation," said Ted Julian, chief strategist for Arbor Networks Inc. of Lexington, Mass. "Decades of information security experience tells us we're not done yet."

The Internet's distributed nature helped it survive the attacks with little impact. But that same nature leaves it just as vulnerable as before.

"If you run a DNS server, there is no real economic incentive to keep it secure," consultant and GCN columnist John McCormick said. He said he believes the federal government should help secure the backbone by regulation, by funding research or by leveraging its buying power to spur security improvements.

The attacks hit the 13 DNS root servers, which translate uniform resource locators into numerical IP addresses. The root servers, operated by a variety of government, commercial and educational organizations around the world, are only the top DNS layer. Most Internet traffic is in fact handled by local servers that cache frequently requested addresses without going to the root servers.

Flooded root servers

The attack began ramping up about 4 p.m. Eastern time on Oct. 21, according to network monitor Matrix NetSystems Inc. of Austin, Texas. It said Internet Control Message Protocol traffic flooded the root servers from a distributed network of attack machines and spiked to more than 10 times the normal volume.

That produced "periods of zero reachability for many of the root servers and an increase in packet loss for the worldwide DNS network approaching 10 percent," compared with normal packet loss levels of less than 1 percent, Matrix NetSystems reported.

Average reachability for users dipped only to about 94 percent. Two days later, packet loss from continuing attacks was about 4 percent, and reachability was about 97 percent.

"If all the DNS root servers were taken down, people might not notice it for hours, maybe a day," Julian said.

The most seriously affected root servers were:

- A and J—VeriSign Global Registry Services of Herndon, Va.
- G—Defense Department Network Information Center in Vienna, Va.
- H—Army Research Laboratory in Aberdeen, Md.

- I—Autonomica AB in Stockholm
- K—Reseaux IP Europeens Network Coordination Centre in London
- M—Widely Integrated Distributed Environment project in Tokyo.

Server operators mitigated the effect by disabling response to ICMP echo traffic. The FBI's National Infrastructure Protection Center is still investigating the attacks.

Although similar distributed attacks have been occurring for several years, and DNS root servers have been targeted, "this is the first time I am aware of that all of them were attacked at once," Julian said.

Denial-of-service attacks against specific Web servers have been successful at shutting down traffic. But root servers could be vulnerable to more serious attacks, such as corruption of key address lists.

John Pescatore, Internet security research director for Gartner Inc. of Stamford, Conn., said government could improve security of the infrastructure by requiring that the service providers with whom it does business filter out spoofed IP addresses.

Packets used in denial-of-service attacks often disguise their sources with false IP addresses. Ingress and egress filtering would make such attacks more difficult, he said.

Pescatore also recommended that the proposed Homeland Security Department make the public-private National Secure Telecommunications Advisory Council the lead organization for critical infrastructure protection.

© 2003 PostNewsweek Tech Media, a division of Post Newsweek Media