A year later, DDoS attacks still a major Web threat

By Robert Lemos
Staff Writer, CNET News.com
February 7, 2001, 12:00 AM PT
http://news.com.com/2009-1001-252187.html

Even the Internet has a sense of fate.



Can the Internet combat DDoS attacks?
Chris Rouland, research director, Internet Security Systems

At 9:15 a.m. on Feb. 7, 2000, AT&T researcher Steve Bellovin walked up to the podium at the North American Network Operators' Group and started a talk. His topic: How a relatively unknown type of Internet attack couldn't be stopped by current technology.

Less than an hour later, Yahoo seemingly dropped off the Internet, as the company's servers were targeted with the very attack that Bellovin had warned about.

A year later, the network security researcher said major e-commerce and information sites worldwide remain vulnerable because "there are (still) no strong defenses deployed."

The DDoS (distributed denial of service) attack that knocked out Yahoo used a host of hacked servers--dubbed "slaves" or "zombies"--to inundate a Web site or Internet-connected server with data, effectively stopping the server's ability to respond to Web page requests or other access attempts. The attack could not be easily pinpointed, as data seemingly came from 50 or more points across the Internet. Simple DoS (denial of service) attacks only come from one source, though attackers can make data appear to come from multiple sources.



Two days later, eBay, Amazon.com, Buy.com, ZDNet, CNN.com, E*Trade and MSN.com joined Yahoo, dropping off the Web for hours at a time. The attacks affected other sites as well. Overall, Internet traffic slowed by as much to 26 percent, according to Net performance watcher Keynote Systems.

Internet still vulnerable
Though repeated attacks have increased awareness of the problem, and technologies for dealing with a DoS attack are seemingly on their way, last year's messes are only the tip of the iceberg, said Tom Anderson, chief technology officer of Asta Networks, one of three companies that have popped up in the last year to offer remedies for DoS attacks and other Internet threats.

"The attacks have become more sophisticated. We have seen a little bit more of the iceberg, but there is a lot more to come," he said.

Two weeks ago, Microsoft became the latest proof when it suffered a router glitch and two DoS attacks that left access to the company's Web properties spotty at best.

The outage followed attacks on worldwide Internet Relay Chat, or IRC, servers that collapsed parts of the service for hours at a time.

And the problem is not going away. At least one tester of anti-DoS technology--a major Internet provider--has estimated that anywhere from 5 to 10 percent of the traffic on its networks is, in reality, data sent by vandals intent on a DoS attack.

"The attacks have gone from just Web servers to enterprises and infrastructure," said Anderson. "We cannot become more complacent."



Solutions on the way?
Several groups are attempting to work together to fight denial-of-service attacks.

The Internet Engineering Task Force has started working on a technology to trace back the origin of a piece of

data to its source. So-called ICMP Traceback Messages, or itrace, could turn DoS attackers from anonymous vandals into easily tracked criminals.

Other groups are forming to share information about attacks, to be better prepared to defend against them.

The Information Technology Association of America, with 19 other major technology companies, has formed the Information Technology Information Sharing and Analysis Center, or IT-ISAC. The center hopes that by sharing attack data, members will be better prepared for future DoS attacks--among other Internet threats--and able to track attacks to the source.

Such tracking is very difficult today, because the tools used by the vandals who start such attacks can be modified to appear to come from a completely different source than the real one. Called "IP spoofing," such a technique requires every company whose server routes data to cooperate to pinpoint the attacker.

Without such cooperation, an attacker may be difficult to find, but stopping the attack is possible, said Phil London, CEO of Mazu Networks, another start-up that believes it can prevent DoS attacks.

"The Holy Grail is to have an ubiquitous deployment all throughout the Internet," he said. "But we don't believe that is completely necessary to provide (DoS prevention) services to our customers."

London and his competitors--Asta Networks and the newly announced Arbor Networks--believe their customers are more interested in keeping their connection to the Internet up and working rather than prosecuting an attacker.

Ted Julian, chief technology officer of Arbor Networks, agrees. "Customers' first priority is to make these things go away. They just want to keep on doing business."

Everyone must work together

While that's true, others believe the problem won't be solved without Internetwide cooperation.



"I think the only solution is to trace things back and turn them off, and that requires a lot of cooperation," said the manager of research and development for network security company @Stake, who would only use his old-school hacker handle "Weld Pond."

"Any technology like these has to be widely deployed," he added. "It has got to be a community effort."

DoS attacks seem to--and in some cases, actually do--come from dozens or hundreds of locations at the same time. Without Internet service providers cooperating, tracking the attacks is impossible.

Cooperation has become critical because the Internet is still rapidly growing, and more, rather than fewer, mistakes are being made, said Weld Pond.

"There are more and more machines out there," he said. "And to me, that means more and more vulnerable machines. The attacks on Microsoft have shown that these people are more than willing and more than able."

Until companies act together to make the Internet more reliable, business on the Net a waiting game.

Go to **Front Door** | **Enterprise** | **Search** | **One Week View**