CircleID™
THE INTERNET ADDRESSING NETWORK

Home | Subscribe | Archives | Submit | About | Contact | Feedback

Previous Articles

Tell A Colleague

Email This Article | Subscribe To CircleID | Read Feedback

DDoS Attack: What The Media Did Not Tell You

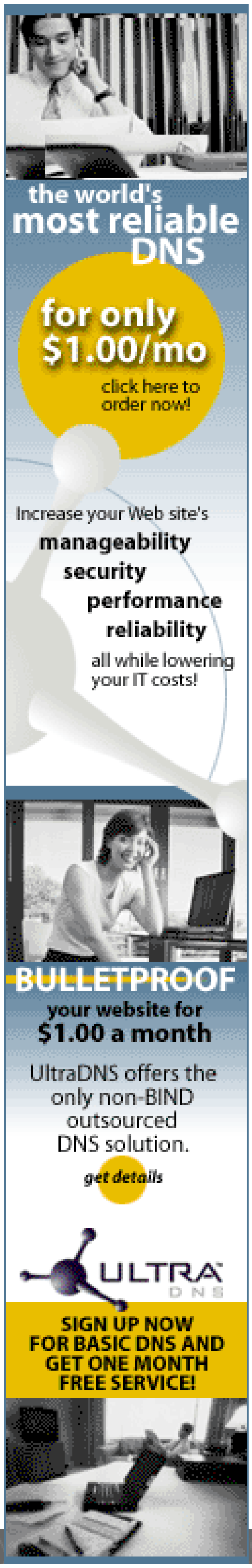
November 20, 2002 | By Joe Baptista | Article Feedback

On Monday, October 21, a "distributed denial of service" (DDOS) attack struck 9 out of the 13 root servers operated by a number of contractors on behalf of the United States Department of Commerce (USG). The next day, the Washington Post reported, "The heart of the Internet sustained its largest and most sophisticated attack ever."

This claim was only partially true. The classic hacker attack was indeed the largest ever witnessed in 20 years of root history -- in fact, it was the first attack against the roots.

But claims that the attack was "sophisticated" were bogus. Most network operators were of the opinion that the attack showed a serious ignorance of the domain name system (DNS) and general network operations. A great deal more damage could have been done if the individuals responsible had targeted the DNS directly. At worst the attack was a test or probe for a potential future attack.

The root servers struck by the attack assist computers in translating Internet domain names, such as www.circleid.com, to numeric equivalents used by computers. These servers provide the primary roadmap for 70% of all Internet communications. The remaining 30% of the net now uses competing root service providers who bypass the USG root system.



They were not under attack.

According to statements by U.S. Federal Bureau of Investigation (FBI) director Robert Mueller, the incident lasted about an hour and originated from computers in the United States and Korea. Most often, computers used in the DDOS assaults are commandeered by hackers either manually or remotely with the help of automated software tools that scan millions of computers for known security holes. These computers often belong to unsuspecting home users. An FBI spokesperson confirmed that the incident was still under investigation.

Fortunately, despite its size, the attack had no impact on the Internet, and no users or computers were affected. The USG root server system contains only 258 top-level domains, of which 243 are ccTLDs (country code top-level domains) and the rest are generic top-level domains (gTLDs) like .com, .org and .net. In comparison to many Internet root server systems, the USG is the smallest. As a result of its limited size, most of the information contained in that root is cached by Internet Service Providers (ISPs) and refreshed every 48 hours. Under those circumstances, Internet users would not have noticed the one-hour attack even if all 13 roots had been successfully blocked the entire time. There simply was not enough time for the cache records at ISPs to expire long enough for anyone to notice.

Petri Helenius was one of the first people to witness and report the attack in progress. He notified the networking community that the DDOS attack was not "causing any serious operational problems" but was slowing things down. Helenius is a telecommunications expert whose company developed the ROMmon (Robust Online Metric MONitoring) system that alerted Mr. Helenius to the intrusion. Helenius notified the North American Network Operators' Group (NANOG) by email at 21:29 UTC. "I remember spending some time before sending off the email," said Helenius. "And, trying to figure out specifics and failing to get further, I sent the email."

The alarms went off at ROMmon at 20:46 (UTC) and the threshold for escalation was crossed at 20:49. The situation dropped "below radar" at 22:01. Helenius pointed out, "the timestamp is a little later than the fact (attack) due to the averaging of the system that (ROMmon) does before it's happy."

Paul Vixie, a root operator, confirmed to NANOG that the DDOS attack was an Internet Control Message Protocol (ICMP) request. ICMP messages are used in the processing of datagrams through which Internet systems communicate. This was the first clue to network operators that the people behind the attack had no clue as to how to effectively take out the roots. If the attackers had focused their computer power on generating bogus queries to port 53, used by roots to provide domain name service, the attack might have been successful -- provided that it was sustained for more than one hour. Vixie successfully blocked the DDOS traffic he was getting with the assistance of his backbone providers. Other operators, however, were not as successful in defending their systems against the attack.

If the attackers had instead targeted the much larger databases used by the .com servers, users would have noticed the incident and it could have gotten ugly. The .com domain servers operated by VeriSign contain millions of domain names, and are queried more often than the roots. If this had been the scenario, the one-hour attack would have had significant repercussions and most of the Internet would have been unreachable, though it was reported on NANOG that the primary root server operated by VeriSign had been unreachable at times during the DDOS attack. Still, there are lots of clues here that the attackers had computer power behind them but did not take full advantage of it. If the attackers had wanted the world to notice, they should have attacked the .com servers. Or maybe it was just a warning, as some have speculated.

The month of October has seen a number of possible attacks against the roots, and this may not have been the first one. CAIDA, the Cooperative Association for Internet Data Analysis, has been monitoring the performance of root and gTLD servers since January 2002, using passive monitors located at the University of California in San Diego and in San Jose. Their report on the DDOS attack indicates that "unusual behavior" in the roots was detected as early as October 7. The report suggests that a series of probes in October preceded the attack.

Speculation by officials that the attack was a warning may be credible under these circumstances. As attacks go, this one was a failure: no one except the experts noticed. Thus, it could have been a short test to see how the system responded. Expect more incidents like these in future.

The attack, however, should come as no surprise to ICANN (Internet Corporation for Assigned Names and Numbers), the Department of Commerce contractor responsible for root security. Over the years, ICANN has been warned that the existing root infrastructure was vulnerable to attack, but the warnings have been largely ignored. Now, however, ICANN President Louis Touton insists that the attacks "make it important to have increased focus on the need for security and stability of the Internet." ICANN's Security and Stability Advisory Committee quickly moved in to investigate the incident. The committee is expected to produce a report on securing the edge of the USG Domain Name System network.

Informed sources at ICANN expect that the committee will initially recommend that ISPs take steps to prevent packets with forged IP addresses from being used in DDOS attacks. This, however, does not directly address the problem of preventing a potential outage of the root system. It is, rather, an attempt to protect the root servers from attack. But don't expect ICANN's recommendations to be widely deployed. It's a difficult process to get ISPs worldwide to do the work required. Rather, expect DDOS to remain a fact of life on the net for now. There are technical solutions available, and technicians and scientists are working to solve the DDOS problem. Until then, taking control of root operations at the user or ISP level is a more logical approach to avoiding any potential interruption to service.

To survive a sustained DDOS attack against the roots, the best solution an ISP has is to run its own system and eliminate any dependence on the US government for basic internet services. It would also be prudent for other primary namespaces like .com. Unfortunately, though, it would require a considerable amount of resources -- the .com zone file alone is well over a gigabyte in size. But the root file is very manageable and can easily be run on an ISP's local domain name servers.

In fact, large ISP's facilities and co-location sites don't rely on the USG for service. They run their own roots, and some mirror the USG root on their local domain servers. ISPs and individual users also have the option of leaving the USG root by switching to private root service providers.

Joe Baptista is a managing director of The dot.GOD Registry, Limited a not for profit provider of network infrastructure, and domain names inclusive namespace. Joe is also involved in Internet governance as a member of the General Assembly of the Domain Name Supporting Organization (DNSO) of The Internet Corporation for Assigned Names and Numbers (ICANN). Joe has been interviewed by the leading Canadian newspapers, radio and television on various Internet issues.

Home | Subscribe | Archives | Submission | About | Contact | Feedback

Interested in submitting your articles? Learn More
Please send us your Feedback & Error Reports. Thank You.