5 February 2003
Updated: 12:24 GMT

The Register

Biting the hand that feeds IT

Search The Register

Go!

Register Services
- Register ISP
- Reg Jobsearch
- Reg Reader Research
- Reg Merchandise
- IT-minds bookstore

Sections
- Front Page
- Software
- Enterprise Systems
- Servers
- Storage
- Personal Hardware
- Semiconductors
- Internet
- Security
- Virus News
- Business
- Networks
- Bootnotes
- This Week's Headlines

- Wireless
- 3G
- Broadband
- The Mac Channel
- Channel Flannel
- Small Business
- BOFH
- Letters
- Site News
- Contact us

Dud queries swamp US Internet Root servers

By Joe Baptista

Posted: 05/02/2003 at 09:47 GMT

Broken queries are swamping US Internet servers with unnecessary traffic. A detailed analysis of 152 million messages received on Oct. 4, 2002 by one of the root servers in California showed that only 2 per cent of the queries were legitimate.

The Cooperative Association for Internet Data Analysis (CAIDA) at the San Diego Supercomputer Center (SDSC) which conducted the research is trying to understand why the roots get so many broken queries from Internet service providers.

DNS root servers provide a critical service to Internet users by mapping text host names to numeric Internet Protocol (IP) addresses. The 13 roots are operated by a mix of volunteers and U.S. government agencies. The U.S. Department of Commerce is the agency responsible for managing the root system which serves most Internet users.

"If the system were functioning properly, it seems that a single source should need to send no more than 1,000 or so queries to a root name server in a 24-hour period," said CAIDA researcher Duane Wessels. "Yet we see millions of broken queries from certain sources."

CAIDA researchers speculate that 70 per cent of the bad requests are due to misconfigured packet filters, firewalls, or other security mechanisms intended to restrict network traffic. Twelve per cent of the illegitimate traffic however could not be explained and was for nonexistent top-level domains, such as ".elvis", ".corp" and "localhost".

.elvis is alive and well and living in an Alternative Root Universe

CAIDA’s results are no surprise to Bradley Thornton, a root server operator at PacificRoot and director of the Top Level Domain Association, an organization of domain operators. He operates the “.corp” alternative TLD for the business community.

The "localhost" queries are to be expected, he says. A computer can have many names - but all computers use "localhost" on the Internet as the host name of the local loopback interface. "The localhost naming convention is an Internet standard and the localhost errors represent misconfigured DNS settings at the user or ISP level,” he says. The rest of the "nonexistent" illegitimate traffic is a vote of confidence in the "inclusive namespace" (i.e. alternative TLDs) which Thornton helped pioneer.

"There may only be one Internet," explains Thornton, "but we now have many namespaces and that’s confusing the legacy root system." Top-level domains in the U.S. roots include country codes such as ".uk" for England, ".ca" for Canada, or ".us" for the United States, as well as generic domains such as ".com", ".net", and ".edu". There are some 300 top level domains in the US root but inclusive namespace has over 10,000 listed.

Thornton thinks that inclusive namespace user activity is the cause of much of the rogue traffic. "Anytime one of our users publishes a URL from our namespace or any namespace in email or via the web that link becomes available to potentially millions of U.S. root users. When those users clicks one of our URLs a query is generated."

This explains the dud traffic discovered by CAIDA, he says. In the inclusive namespace universe ".corp" is a busy top level domain and Thornton speculates that ".elvis" is alive and well and living in some unknown root system heaven.

According to KC Claffy, a resident research scientist at CAIDA, traffic originating from the inclusive namespace system is “likely part” of the results. But Wessels, the project leader, emphasized “there was not much evidence of alternative (inclusive namespace) TLDs” in the data collected.

Thornton disagrees: "the data clearly shows we’re having an effect." A TLD only needs an average of 10,000 hits in the root to show significant activity based on the CAIDA data of 3 million legitimate queries for 300 listed TLDs, he argues.

"CAIDA reports that “.corp” got 51,000 queries and that's very significant evidence,” he says. ®

Joe Baptista is involved in the running of dot-god.com, the "official domain registry for web addresses ending in .god and .satan".

Related Link

CAIDA Press Release