Detecting DNS censorship without an internal vantage point.

Will Scott, Sujit Packiaraj, Arvind Krishnamurthy
University of Washington
{wrs,sujitp,arvind}@cs.washington.edu

ABSTRACT

One challenge in detecting online censorship is the need for vantage points within the censoring domains. We focus on the specific subproblem of DNS blacklisting, where servers in a particular administrative domain are instructed not to resolve requests for specific sites. We find that for this problem internal vantage points are not needed, since public DNS servers in a given domain can be directly queried. Previous work[2] has leveraged this insight in the context of a single country.

We query several thousand potentially sensitive domains taken from known blacklists (such as [1] and wikileaks) against publicly available DNS servers. After removing servers with erratic behavior and conservatively defining availability as whether an IP address was returned by a server, simple statistics were used to determine if a subpopulation of measurements from a single administrative domain significantly differ from the larger population. This paper presents a condensed result, showing that the technique can be effective in identifying this type of censorship. We limit our coverage to the 59 countries in which we found at least 30 accessible DNS servers, and determine censorship to occur when the subpopulation's mean availability is more than four standard deviations below that of the general population. We consider these results to be a lower bound, and allude to future research opportunities including how the same technique might be used to monitor widely blocked domains.

BODY

DNS censorship can be detected through anomalies when querying public DNS servers. At least 13 countries block otherwise available sites.

REFERENCES

[1] B. Edelman and J. Zittrain. Empirical Analysis of Internet Filtering in China. *Berkman Center for Internet & Society, Harvard Law School*, 2005. cyber.law.harvard.edu/filtering/china.

[2] G. Lowe, P. Winters, and M. Marcus. The Great DNS Wall of China. Technical report, NYU, 2007. cs.nyu.edu/~pcw216/work/nds/final.pdf.

Volume 2 of Tiny Transactions on Computer Science