



PRESS RELEASE

Media Contact:

Jennifer Jasper
Infoblox
408.625.4309
jjasper@infoblox.com

Sixth Annual DNS Survey Reveals Most Businesses are Vulnerable to Cache Poisoning Attacks and Network Downtime

Stalled DNSSEC Adoption and DNS Server Deployment Diversity Represent Biggest Concerns

SANTA CLARA, Calif., Dec. 6, 2010 — Infoblox, a market leading developer of advanced [network infrastructure control](#) solutions, and The Measurement Factory, experts in performance testing and protocol compliance, today announced results from [the sixth-annual survey of DNS infrastructure](#) on the public Internet.

“This year’s survey results along with recent related outages like those experienced by [Rollingstone.com](#) and [Comcast](#) should represent a huge wake-up call for any organization with an Internet presence,” commented Cricket Liu, Vice President of Architecture at Infoblox and author of O’Reilly & Associates’ *DNS and BIND*, *DNS & BIND Cookbook*, and other titles. “Despite years of highlighting the vulnerability of the Domain Name System (DNS) and a long history of publicized downtime associated with DNS vulnerabilities, organizations are still not taking DNS security seriously. We are nowhere near what’s required to prevent criminals from wreaking havoc with online business. 2011 has to be the year for DNSSEC deployment or organizations will have no one to blame but themselves if they become victims.”

Startling DNSSEC Statistics

Survey results reveal that while DNSSEC adoption percentages appear to have increased dramatically by 340 percent this year, the actual number of zones that have been signed is very small: .02 percent. This indicates that the vast majority of organizations with an Internet presence are vulnerable to attacks. Of the .02 percent of zones that are DNSSEC-signed, 23

percent of them failed validation due to expired signatures. This underscores that DNSSEC (including re-signing) needs to be as automated as possible to avoid accidental denial of service.

Furthermore, survey results reveal that some fundamental DNS capabilities required for DNSSEC adoption – TCP queries and support for [Extension Mechanisms for DNS \(EDNS0\)](#) – are not fully deployed. All these figures cause great concern that there is significant work to do before the industry is ready for DNSSEC and the Internet and enterprises alike are protected.

DNS Server Diversity Prevents Single Points of Failure

Additional survey findings revealed that topological diversity of authoritative name servers is an ongoing issue, with almost 75 percent of all name servers advertised in a single autonomous system; this presents a single point of failure that can impact availability of many organizations' Internet presence in the event of a fault or problem with routing infrastructure.

These Statistics Have Big Implications

DNS servers are essential network infrastructure that map domain names (e.g., yahoo.com) to IP addresses (e.g., 66.94.234.13), directing Internet inquiries to the appropriate location. Domain name resolution conducted by these servers is required to perform any Internet-related request from Web browsing, email and ecommerce to cloud computing.

Should an enterprise or organization's DNS systems become compromised by attacks, the results can be devastating, ranging from loss of a company's Web presence, inability of employees to access any outside Web services, and perhaps most damaging, redirection of Web and email traffic to bogus sites, resulting in data loss, identity theft, ecommerce fraud and more.

Making matters worse, Cybercrime estimates are only growing. In a 2009 report, [The Internet Crime Complaint Center \(IC3\)](#), a partnership between the FBI and the National White Collar Crime Center, indicated that cyber crime complaints increased 22.3 percent compared to 2008 – and those are just the reported cases – illustrating the continued growth of cyber-crime.

DNSSEC: Offers Protection, *If* Adopted

Most security experts agree that the Domain Name System Security Extensions (DNSSEC), a suite of IETF specifications for securing information provided by DNS, represent the best means to protect against cyber-criminal activities launched at DNS servers. DNSSEC implements an automated trust infrastructure, enabling systems to verify the authenticity of DNS information, and foils attackers' attempts to direct users to alternate sites for collection of credit card information and passwords, to redirect email, or otherwise compromise applications.

Matt Larson, Vice President of DNS Research at [VeriSign](#), commented: “DNSSEC is an essential tool in sealing DNS vulnerabilities and mitigating DNS cache poisoning attacks that undermine the integrity of the DNS system. Especially as top-level zones, including .NET imminently and .COM early next year, are signed, DNSSEC offers the best protection for all organizations with a presence on the Internet.”

Calls to Action

Based on these statistics, there are some clear calls to action for organizations with external DNS servers:

- [Assess DNS infrastructure](#) and immediately take the necessary steps to make it more secure and diverse, following [best practices](#).
- Educate themselves about DNSSEC; view this [DNS Security Page](#) to find tutorials, links to deployment guides, and other resources; and,
- Familiarize yourself with [new solutions](#), such as those provided by Infoblox that can help organizations more easily deploy DNSSEC and automate maintenance.

To view complete 2010 DNS Survey results visit: <http://www.infoblox.com/dnssec>.

About Infoblox

Infoblox is an industry leading developer of network infrastructure control solutions. Infoblox’s unique technologies, including the Infoblox Grid™—a real-time, data distribution technology—increase network availability and control, while automating time-consuming manual tasks associated with network infrastructure services like domain name resolution ([DNS](#)), IP address management ([IPAM](#)), network change and configuration management ([NCCM](#)) and network discovery, among others. Infoblox solutions are used by over 4,500 organizations worldwide, including more than one third of the Fortune 500. The company is headquartered in Santa Clara, Calif., and operates in more than 30 countries.

About The Measurement Factory

The Measurement Factory provides a variety of products and services related to Internet testing and measurement, with a current focus on DNS, HTTP, and ICAP. Most of the Factory’s products are available under open-source licenses. For more information, call +1-303-938-6863, email info@measurement-factory.com, or visit www.measurement-factory.com.

###