



The **Measurement Factory's fifth annual DNS Survey** is a Pandora's box of both frightening and hopeful results. Of particular interest is the enormous growth in the number of Internet-connected name servers, largely attributable to the introduction by carriers of customer premises equipment (CPE) with embedded DNS functionality. This equipment represents a significant risk to the rest of the Internet, as without proper access controls, it facilitates enormous DDoS attacks.

On the hopeful side, DNSSEC adoption has begun accelerating, and the percentage of name servers open to zone transfers is significantly lower. The Microsoft DNS Server's presence on the Internet is dramatically diminished. Below is a summary and assessment of the most interesting results.

- **NEUTRAL: Current estimate of 16.3 million name servers on the Internet** (up from 11.7 million in 2007) **represents a 40% increase in 2 years**
 - Explosion in population of "non-traditional" name servers (proxies embedded in CPE, etc.)
 - Consequences:
 - Population of name servers increases dramatically as more people get broadband (because so many broadband access devices have built-in DNS proxies)
 - People in the DNS business need to call for minimum standards for embedded DNS proxies such as support for query ACLs and source port randomization
- **VERY DISTURBING: 79.6% of the name servers in our random sample are open to recursion**
 - Consequences:
 - Enormous population of open recursive name servers
 - These name servers can be used in DDOS attacks
- **POSITIVE: Percentage of Microsoft DNS Servers is now almost negligible** (down to .37% from 2.74% in 2007)
 - Microsoft is almost extinct as an external name server, likely due to greater awareness of the risks of exposing Windows computers to the Internet
 - This is positive, but we still haven't done a great job securing the name servers that *are* exposed to the Internet
- **POSITIVE: Percentage of zones with one or more name servers open to zone transfers decreased to 16% from 31% (in 2008)**
 - Administrators are paying closer attention to configuration of external DNS servers, realizing that they need to configure ACLs to prevent zone transfers, which can leave them open to DOS attacks.
- **POSITIVE: The number of DNSSEC signed zones increased significantly, by approximately 300%**
 - Signed zones rose from 45 in 2008 to 167 this year; this indicates that momentum in DNSSEC adoption is increasing. This could be the result of Kaminsky vulnerability and support for DNSSEC in parent zones (.org, which was included in this year's survey) is signed).
 - As simplified solutions, such as Infoblox's, help automate management of signed zones, we hope to see this number increase substantially in the next year
 - Further adoption of DNSSEC among parent zones (such as the root zone and *net*, both planned for 2010) will also help encourage adoption
 - Most common configuration parameters:
 - 96.2% of signed zones use RSA keys with SHA-1
 - 94.6% of signed zones use separate ZSKs and KSKs
 - 86.8% of signature validity periods are 30 days (+/- 1 day)
 - 29.7% of KSKs are 1024 bits long
 - 50.6% of KSKs are 2048 bits long
 - 8.2% of KSKs are 4096 bits long
 - 84.3% of ZSKs are 1024 bits long
 - Choice of key length indicates how difficulty in cracking the key, but overhead increases with longer keys, because the encryption takes longer and responses are larger

- **NEUTRAL: IPv6 adoption increased to .7% from .44 (in 2008), but still remains low**
 - While one might argue that people still aren't concerned about diminishing IP address space, this is also due to the fact that registrars don't make it easy to add IPv6 addresses to a zone's delegation
- **NEUTRAL: SPF was stable at about 12.2%** (fairly level with 12.6% in 2007)
 - This may indicate that adoption has stalled

Conclusions

- Carriers need to pay more attention to the default configuration and security features (e.g., source port randomization, ACLs, etc.) of CPE that they deploy
- Likewise, customers should insist on CPE with secure default configurations and adequate security features
- Administrators should prepare themselves for DNSSEC; adoption is already accelerating and will continue to accelerate as top-level zones are signed. There are new solutions that can help organizations more easily deploy and support DNSSEC.
- Administrators should be sure to employ best practices
 - Upgrade to the most recent version of BIND
 - Make sure you use a solution that performs port randomization to protect against the Kaminsky cache poisoning vulnerability
 - Consider appliances with easy upgrade/options
 - Separate internal and external name servers
 - Separate authoritative and recursive name servers
- Registrars should make it easier for people to include IPv6 addresses in their delegations

References

- The DNS Advisor tool performs more than 53 DNS tests:
<http://dnsadvisor.infoblox.com>
- DNSSEC Best Practices Architecture whitepaper:
<http://www.infoblox.com/library/l-genLibrary.cfm?section=l-whitepapers&libld=251>
- DNSSEC webinar featuring Dan Kaminsky, NIST's Scott Rose and Cricket Liu:
<http://www.infoblox.com/library/l-genLibrary.cfm?section=l-webinars>
- DNS Best Practices Resources:
<http://www.infoblox.com/library/dns.cfm>
- Cricket's Blog:
<http://www.cricketondns.com/>
- Cricket on Twitter:
<http://twitter.com/cricketondns>
- NIST "Secure Domain Name System Deployment Guide":
http://csrc.nist.gov/publications/drafts/800-81-rev1/nist_draft_sp800-81r1-round2.pdf

About Infoblox

Infoblox is a manufacturer of appliances – used by over 3,200 organizations worldwide, including over 130 of the Fortune 500 – that deliver utility-grade domain name resolution (DNS), IP address assignment and management (IPAM/DHCP), and other related services.