中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

国家域名安全联盟

中国域名服务安全状况与态势分析报告

2013

中国互联网络信息中心
国家域名安全联盟

目录

专业术语表

缩略语	英文全称	中文全称
ccTLD	Country Code Top Level Domain	国家与地区顶级域名
CDN	Content Delivery Network	内容分发网络
DNS	Domain Name System	域名系统
DNSSEC	DNS Security Extensions	域名系统安全扩展
DLV	DNSSEC Lookaside Validation	域名系统安全旁路认证
DoS	Denial of Service	拒绝服务攻击
DS	Delegation Signer	授权签名者
gTLD	General Top Level Domain	通用顶级域名
IANA	Internet Assigned Numbers Authority	互联网数字分配机构
ICANN	Internet Corporation for Assigned Names and Numbers	互联网名称与数字地址分配机构
IPv4	Internet Protocol version 4	互联网协议第四版本
IPv6	Internet Protocol version 6	互联网协议第六版本
ISC	Internet Software Consortium	互联网系统协会
TCP	Transmission Control Protocol	传输控制协议
TLD	Top Level Domain	顶级域名
TTL	Time To Live	生存时间
UDP	User Datagram Protocol	用户数据报协议

1、前言

域名服务系统是互联网的重要基础设施，目前大多数互联网应用，如网页浏览、电子邮件、文件传输等，都依赖域名系统来实现网络资源的寻址和定位。整个域名服务体系包括提供域名服务的所有域名系统，由两大类别、四个环节组成：第一类是权威域名解析服务系统，包括根域名服务系统、顶级域名服务系统和其他各级域名服务系统三个环节。权威域名服务系统由各级域名持有者管理，负责维护和保存各级权威域的域名信息，并且接受递归服务器的查询请求。第二类是递归域名解析服务系统，它们面向终端用户提供域名查询服务。具体架构如图 1 所示。

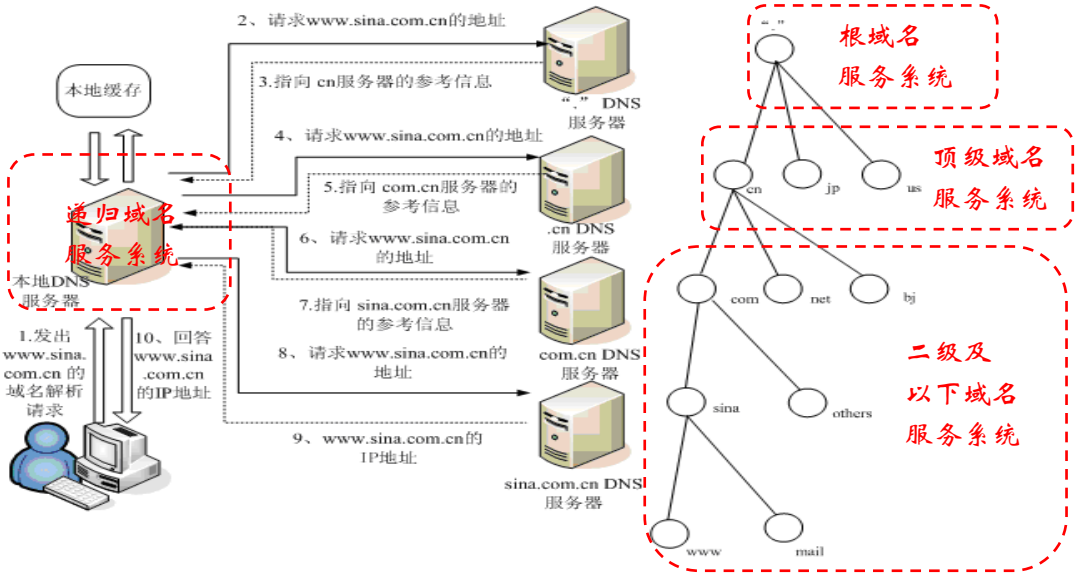

图 1 域名服务体系的构成

对我国域名基础设施网络安全的监测一方面有助于对我国域名系统安全状态进行完整、精确、深入的把握，另一方面也可以借助于域名系统安全状况进行我国互联网安全态势的分析和评估。

自 2009 年起，中国互联网络信息中心（以下简称 CNNIC）就开始对整个域名服务体系的配置情况和安全态势进行多角度的监测分析。为了对域名服务体系的运行状态和安全配置情况进行更为准确、客观的了解，CNNIC 基于自身建设的国家域名安全监测平台，在全球范围内部署了广泛的监测节点，截至 2013 年 12 月，该平台所拥有的监测点数已达到 46 个，其中海外监测点 2 个。同时，我

们还设计开发了故障、配置、性能和流量等多角度的监测项，以对域名服务体系的根域名服务系统、顶级域名服务系统、二级及以下权威域名服务系统和递归域名服务系统的运行状态和安全状况进行全面监测和客观评估。

2、摘要

经过周期性的重复监测及分析，我国域名基础设施网络安全状况主要存在以下特点：

1) 各级权威及递归域名服务器使用 Linux/Unix 操作系统的比例均高于 80%，选择 ISC BIND 作为域名解析软件的比例均在 90%以上。另外，BIND 软件版本应答比例较去年有所降低，但总体依然较高，具有一定安全隐患；
2) 根域名服务系统协议支持完善，安全保障较好，较去年新增 38 个镜像服务器，监测显示，根域名服务器的平均解析速度较去年提升了 3%；
3) 顶级域名服务系统的冗余配置较好，递归开启比率降低至 0.5%，进一步提升了抗攻击能力，对相关协议的支持情况较去年有了明显提升，其中 DNSSEC 支持率达到 46.4%；
4) 二级及以下权威域名服务系统在解析性能和协议支持程度方面较去年均有所提升，但是 16.8%的服务器仍然开启了递归服务，具有一定安全风险；
5) 递归域名服务系统在 DNSSEC 支持率和端口随机性程度方面有所改善，但仍然存在较大的提升空间，此外大数据包支持比率由去年的不足一成提高到了今年的超过一半；
6) 总体而言，国内递归域名服务器的总体安全状况要好于全体递归域名服务器，国内重点权威域名服务器的总体安全状况要好于全部权威域名服务器。

3、域名服务安全状况

3.1 根域名服务系统

3.1.1 简介

域名服务系统通过层次化的形式管理域名数据，从而以分阶段的方式将人们可以记住的域名转换为计算机使用的数字以寻找其对应的目的地。根域名服务系统作为提供域名权威数据的入口，其服务器数量和分布对互联网域名解析服务性能和安全稳定有很大的影响。截至 2013 年 12 月 31 日，域名系统 13 个根服务器在全球的镜像节点数量共 386 个(较去年同期新增 38 个)，其中中国大陆有 F 根、I 根、J 根和 L 根共计 4 个镜像节点。

根服务器的运营管理者及对应的 IP 和 AS 号如表 1 所示。

表 1 根服务器主要情况[1]

根服务器	运营者	IP地址	AS号
A	VeriSign, Inc.	IPv4: 198.41.0.4 IPv6:2001:503:BA3E::2:30	19836
B	Information Sciences Institute	IPv4: 192.228.79.201 IPv6: 2001:478:65::53	none
C	Cogent Communications	IPv4: 192.33.4.12	2149
D	University of Maryland	IPv4: 199.7.91.13 IPv6: 2001:500:2D::D	27
E	NASA Ames Research Center	IPv4: 192.203.230.10	297
F*	Internet Systems Consortium, Inc.	IPv4: 192.5.5.241 IPv6: 2001:500:2f::f	3557
G	U.S. DOD Network Information Center	IPv4: 192.112.36.4	5927
H	U.S. Army Research Lab	IPv4: 128.63.2.53 IPv6:2001:500:1::803f:235	13
I*	Netnod	IPv4: 192.36.148.17 IPv6:2001:7fe::53	29216
J*	VeriSign, Inc.	IPv4: 192.58.128.30 IPv6: 2001:503:C27::2:30	26415
K	RIPE NCC	IPv4: 193.0.14.129 IPv6: 2001:7fd::1	25152
L*	ICANN	IPv4: 199.7.83.42	20144

[1] 注：“*”表示在中国境内具有该服务器镜像节点。

		IPv6: 2001:500:3::42	
M	WIDE Project	IPv4: 202.12.27.33 IPv6: 2001:dc3::35	7500

3.1.2 协议支持

随着网络攻击技术的发展及 DNS 漏洞的频繁出现，攻击者已经大大缩短了劫持 DNS 查找过程的任一步骤所需的时间，从而可以更快地取得对会话的控制以实施某种恶意操作。若要在长期内消除此漏洞，唯一的解决方案是以端到端的形式部署 DNSSEC 协议。开发 DNSSEC 技术的目的之一是通过对 DNS 数据进行数字签名来抵御此类攻击，从而使用户确信所接收到的数据有效。但是，为了从互联网中彻底消除该漏洞，必须在从根区到最终域名的查找过程中的每一步部署 DNSSEC。

因此，作为 DNSSEC 信任链的根源，根服务器是否支持 DNSSEC 对于整个 DNS 服务体系部署 DNSSEC 至关重要。检测结果显示，根服务器都已经部署了 DNSSEC 服务（ICANN 于 2010 年已宣布，根区完成 DNSSEC 签名）。数据加密算法为 RSA/SHA-256。此外，所有的根服务器都支持 NSEC3，从而避免区文件被遍历、枚举的风险。

IPv6 的普及离不开 DNS 对 IPv6 的支持。根服务器中有 3 个还未支持 IPv6，分别为 C、E、G 节点。

此外，在现行 DNS 标准中，数据包大小被控制在 512Byte 以下，通过一个 UDP 数据包进行传输。如果 DNS 支持 IPv6 的话，在 DNS 请求的应答当中，IPv6 地址就会与 IPv4 地址一起发送过来。这样一来，返回的信息量自然就超过了 512Byte，而 DNS 服务器在交换超过 512Byte 的数据时应采用 TCP 代替 UDP。检测结果显示，所有的根服务器都支持 TCP 协议。

图 2 显示的是根域名服务器的协议支持比例分布情况。可见，根域名服务器在协议支持程度方面与去年相比没有发生变化。

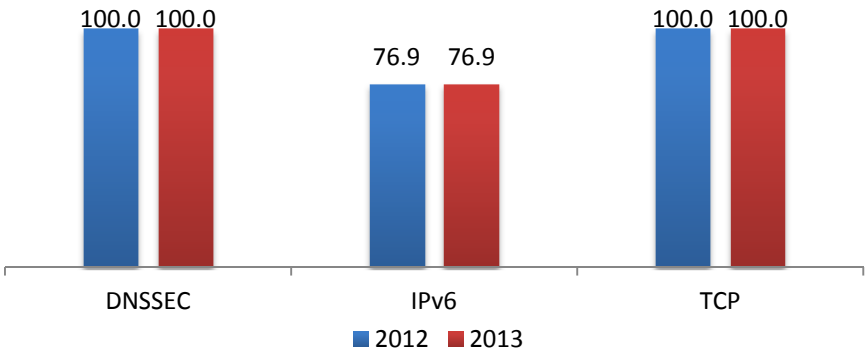

图 2 根域名服务器协议支持比例情况（%）

3.1.3 服务性能

为了保证全球 DNS 服务的高可用性以及抗攻击能力，根服务器采用 BGP Global AnyCast 技术[2]在全球范围内广泛部署镜像节点。截至 2013 年 12 月 31 日，全球共有 386 个根服务器镜像节点(较去年同期新增 38 个)，除了由 Information Sciences Institute 运维的 B 根以外，其他 12 个根服务器均在全球范围内部署了广泛的镜像节点。图 3 所示为 13 个根服务器各自所部署的镜像数量分布情况。

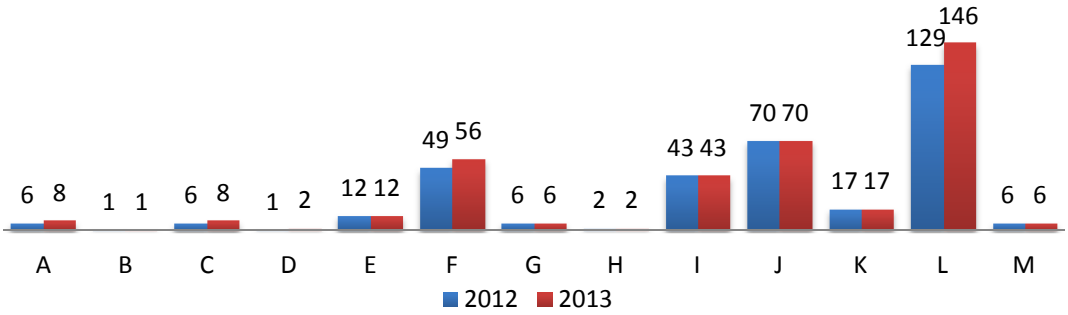

图 3 根服务器部署镜像数量分布情况

根域名服务系统采用 BGP Global AnyCast 机制保证多个镜像节点对于用户访问的透明性，该机制会将用户的 DNS 查询引导到距其最近的 DNS 根镜像节点，从而起到了一定的负载均衡作用。因此，根服务器查询时延的大小对于监测点的位置有直接的依赖性。为了全面反映国内互联网用户访问根服务器的时延，本报告对分布在全球范围内的 46 个监测点的探测结果取平均值，具体结果如图 4 所示。从中可以看出，大部分根域名服务器的查询时延较去年都有了一定程度的减少。

[2]DNS 多点部署 IP Anycast＋BGP 实战分析：http://tech.sina.com.cn/b/2010-01-25/15341227860.shtml

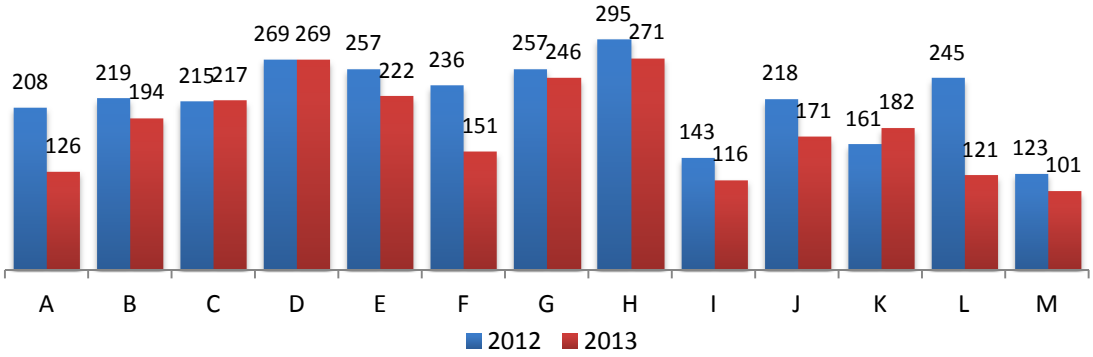

图 4 根域名服务器查询时延分布情况（毫秒）

中国早在 2003 年就拥有了第一个根服务器的镜像——F 根镜像，这是由 ISC 和中国电信共同建立的。2005 年，I 根的管理机构 Autonomica 在 CNNIC 设立了中国第二个根镜像。2006 年，原中国网通与美国 Verisign 公司正式开通 J 根的中国镜像服务器。此外，CNNIC 于 2012 年又部署了国内第一个 L 根镜像节点。这四个根的镜像节点也成为我国境内 DNS 查询请求最主要的根域名服务节点。

从图 4 中也可以看出，相对于其他根服务器，上述 4 个在国内拥有镜像的根服务器的查询时延明显较小，这也表明根服务器镜像在国内的部署可以有效提升我国互联网连接根服务器的响应速度。

3.2 顶级域名服务系统

3.2.1 简介

根据国际互联网域名体系的构成，当前顶级域名共包含四类：通用顶级域名（gTLD）、国家与地区顶级域名（ccTLD）、基础设施类顶级域名（infrastructure，目前仅有.arpa）和实验性顶级域（test）。其中通用顶级域 gTLD 可细分为组织主办类（sponsored），通用类（generic），及限制通用类（generic-restricted）。根据 IANA 的统计，截至 2013 年 12 月 31 日，全球域名服务体系共包含 383 个 TLD，较去年同期新增 54 个 TLD，其中绝大部分是新通用顶级域（New gTLD）[3]。

3.2.2 系统软件

监测显示，顶级域名服务器普遍采用了 Linux 或者 Unix 操作系统，两者所占比例达到 99%以上。顶级域名服务器所采用的 DNS 软件比例分布情况如表 2 所示。可以看出，绝大部分顶级域名服务器都采用了 ISC BIND 软件，比例高达 95.9%，较去年略有提升（去年比例为 93.04%）。值得注意的是，这些采用 ISC BIND 软件的顶级域名服务器，它们当前的 BIND 版本普遍存在过低的问题，主要以 9.2.3rc1~9.4.0a0 为主，而 ISC BIND 软件的当前稳定版本为 9.8.6，因此应立即升级到当前最新版本。此外，38.1%的 BIND 软件开启了版本应答功能，相比去年增加了 0.7 个百分点，具有一定的安全隐患，应当引起足够的重视。

表 2 顶级域名服务器 DNS 软件比例分布情况

软件类型	2012年所占比例（%）	2013年所占比例（%）
ISC BIND	93.0	95.9
VeriSign ATLAS	5.1	2.4
UltraDNS	0.8	1.3
DJ Bernstein TinyDNS	0.8	0.2
JHSOFT simple DNS plus	0.1	0.1
Nominum ANS	0.2	0.1

[3] 随着 ICANN 于 2012 年 1 月开放新通用顶级域（New gTLD）申请，未来还将有无数新通用顶级域诞生并写入根区。

3.3.3 协议支持

顶级域名服务器的协议支持分布情况如图 5 所示。可见，和去年相比，顶级域名服务器的协议支持程度均有了明显的提升。

随着业界对于 DNSSEC 的努力推动，各顶级域名管理机构陆续开始部署 DNSSEC 服务。截至 2013 年 12 月 31 日，已有 46.4%的顶级权威域实现了 DNSSEC 签名，与去年相比提升了 15.4 个百分点。其中所支持的加密算法，以 RSA/SHA-256 和 RSASHA1-NSEC3-SHA1 为主，两者占到了 89%。依然采用传统的 NextSECure（NSEC）机制的 DNSSEC 顶级域名服务器比例占到了 26.1%，具有区文件被遍历、枚举从而泄露所管理的域名解析数据的风险，该比例相比去年上升了 6.1 个百分点，应当引起足够重视。

IPv6 支持比率由去年的 43.4%提升到今年的 58.9%，TCP 支持比率由去年的 56.6%猛增至 92.1%，这种变化有助于加速下一代互联网的过渡进程。

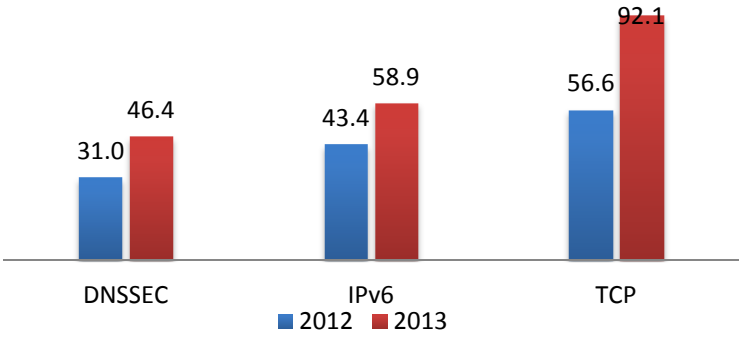

图 5 顶级域名服务器协议支持程度分布情况（%）

3.3.4 服务性能

监测显示，顶级域名服务器均具有冗余配置[4]，但是顶级域名服务器的总体冗余程度相比去年略有下降，平均每个顶级域所拥有的服务器数量由去年的 5.6 个减少为今年的 5.2 个，具体情况如图 6 所示。

[4] 注：本报告以一个顶级域所具有的服务地址数量表示其冗余性程度。

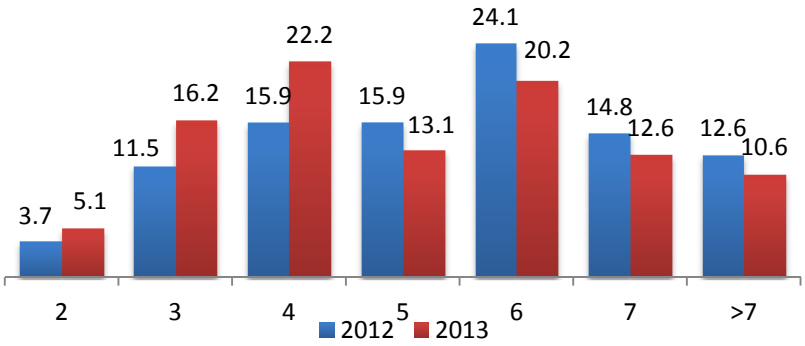

图 6 顶级域名服务地址数量比例分布情况（%）

权威域名服务器开启递归服务具有易遭受 DoS 攻击的风险。监测显示，顶级域名服务器的递归服务开启比例由去年的 1.6%减少为今年的 0.5%，总体抗攻击能力进一步提高。

部署多台权威域名服务器能够起到增强权威域名服务鲁棒性和抗攻击能力的效果。但检测显示，15.5%的 TLD 域名具有数据不一致的问题，即同一个顶级域的多台权威域名服务器数据不完全相同，这将会导致客户端从不同服务器查询得到不一致的 DNS 信息[5]。

服务器如果设置较大的 TTL，有可能会使客户端接收到过期的 DNS 缓存数据，但如果 TTL 设置过小，权威域名服务器将会因为频繁的 DNS 更新和区传输导致较大的开销，顶级权威域的 TTL 设置分布如图 7 所示。

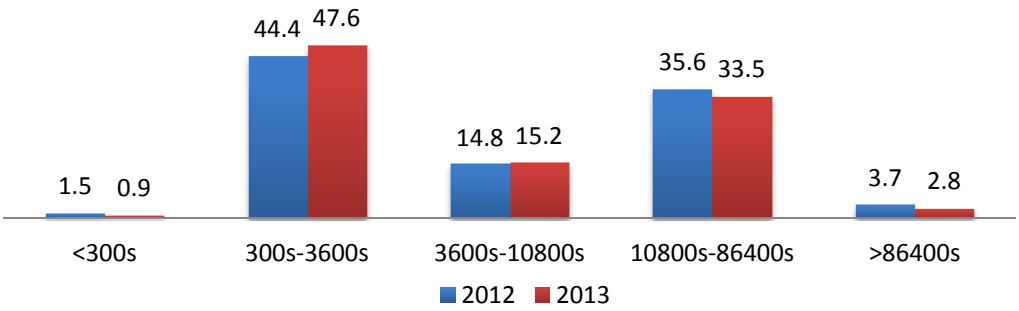

图 7 顶级域的 TTL 设置比例分布情况（%）

顶级域名服务器的查询时延分布如图 8 所示。由于顶级域名服务器的运维和管理都相对成熟，不仅整体配置和功能实现较为完善，查询时延也较平稳、服务状态良好。

[5] 注：不排除检测时发生区传输等影响区数据的操作。

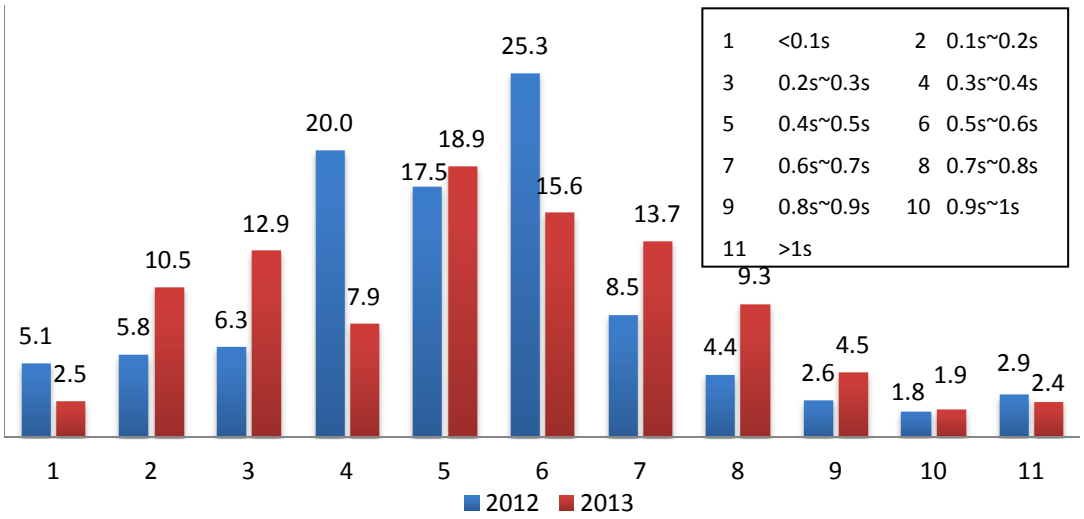

图 8 顶级域名服务器查询时延比例分布情况（%）

3.3 二级及以下权威域名服务系统

3.3.1 简介

二级及以下权威域名服务系统的基础建设普遍比较薄弱，运维能力也参差不齐。而其中一些域名服务器，如运行重点域名的服务器或运行重要信息系统的域名服务器，其所提供的权威数据直接影响到互联网用户各种应用的开展，一旦发生问题后果非常严重。为了抽样了解二级及以下权威域名服务系统的安全状态，本报告选择在中国境内使用最广泛的.CN、.COM 和.NET 三大顶级域下的超过1.3 亿个二级及以下域名作为监测对象，以下是详细的监测结果。

3.3.2 系统软件

Linux/Unix 为二级及以下权威域名服务器使用的主流操作系统类型，所占比例高达 85.9%，较去年有了明显提高（去年比例为 70.9%）。ISC BIND 在所有DNS 软件中所占比例绝对领先，为 91.45%。具体分布如表 3 所示。与顶级域名服务器面临的问题相同，大部分 BIND 服务器使用的是位于区间 9.2.3rc1~9.4.0a0 的较旧版本。此外，28%的 BIND 软件仍开启版本应答功能（去年该比例为 40%），具有一定的安全隐患。

表 3 二级及以下权威域名服务器 DNS 软件比例分布情况

软件类型	2012年所占比例（%）	2013年所占比例（%）
ISC BIND	92.17	91.45
DJ Bernstein TinyDNS	5.18	4.64
bboy MyDNS	0.95	2.58
JHSOFT simple DNS plus	0.49	0.5
Microsoft Windows DNS 2000	0.7	0.33
PowerDNS	0.08	0.09
UltraDNS	0.02	0.06
Nominum ANS	0.02	0.04
Microsoft Windows DNS 2003	0.06	0.03
NLnetLabs NSD	0.02	0.02
Other	0.31	0.26

3.3.3 协议支持

监测显示，虽然根域和顶级域的 DNSSEC 部署已经比较广泛，但是二级及以下权威域中仅有 0.26%部署了 DNSSEC 服务，这也是整个 DNS 业界期望整体实现 DNSSEC 功能、避免安全孤岛的工作重点所在。对于已经签名的区域，同样以 RSA/SHA-256 和 RSASHA1-NSEC3-SHA1 为主，两者占到了 95.8%。依然采用传统的 NSEC 机制的 DNSSEC 权威服务器由去年的 60.3%减少为今年的 4.1%，有效的降低了域名解析数据的泄露风险。

同时，二级及以下权威域的 IPv6 和 TCP 支持率与去年相比，都有了一定的提升，分别达到了 14.6%和 81.7%。

二级及以下权威域名服务器的协议支持比例情况如图 9 所示。

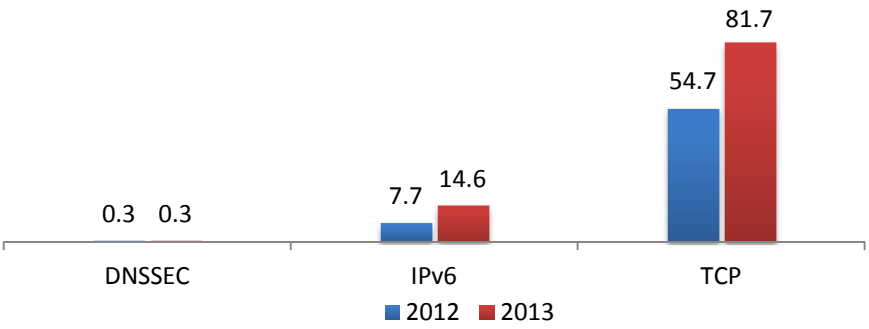

图 9 二级及以下权威域名服务器协议支持比例情况（%）

3.3.4 服务性能

在服务冗余方面，73.8%的二级及以下权威域具有冗余配置，但是二级及以下权威域的总体冗余程度相比去年略有下降，平均每个域所拥有的服务器数量由去年的 2.2 个减少为今年的 2.0 个，具体情况如图 10 所示。

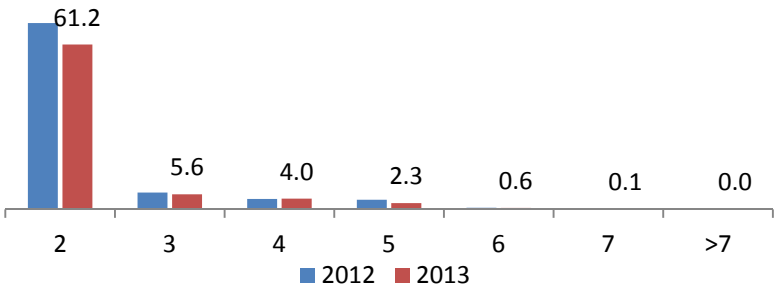

图 10 二级及以下权威域服务地址数量比例分布情况（%）

另外，16.8%的服务器仍然开启了递归服务（去年比例为 15.9%），这种配置缺陷具有易遭受 DoS 攻击的风险。

二级及以下权威域名的 TTL 设置分布如图 11 所示。

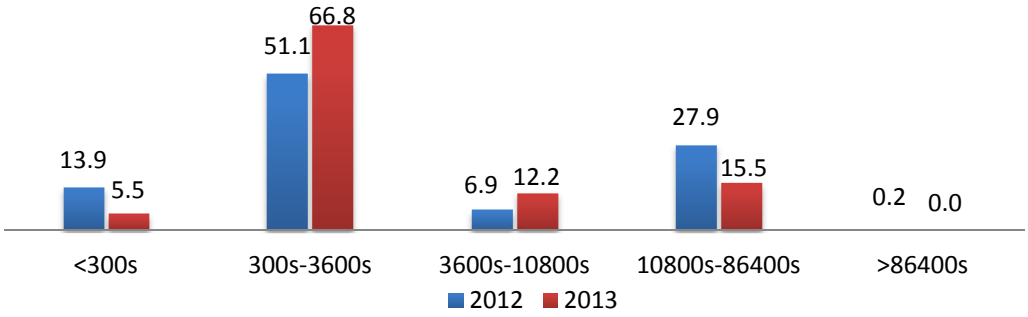

图 11 二级及以下权威域名 TTL 设置分布（%）

二级及以下权威域名服务器的查询时延分布情况如图 12 所示。可见，由于二级及以下权威域的服务能力和运维水平参差不齐，因此服务器的查询时延分布较广、差别很大，查询时延在 0.1 秒以内的服务器占到了 36.8%，相比去年有了大幅度提升，表明二级及以下权威域名的解析性能和服务水平在不断提升，同时监测点所处网络环境的改善也是产生该结果的部分因素。

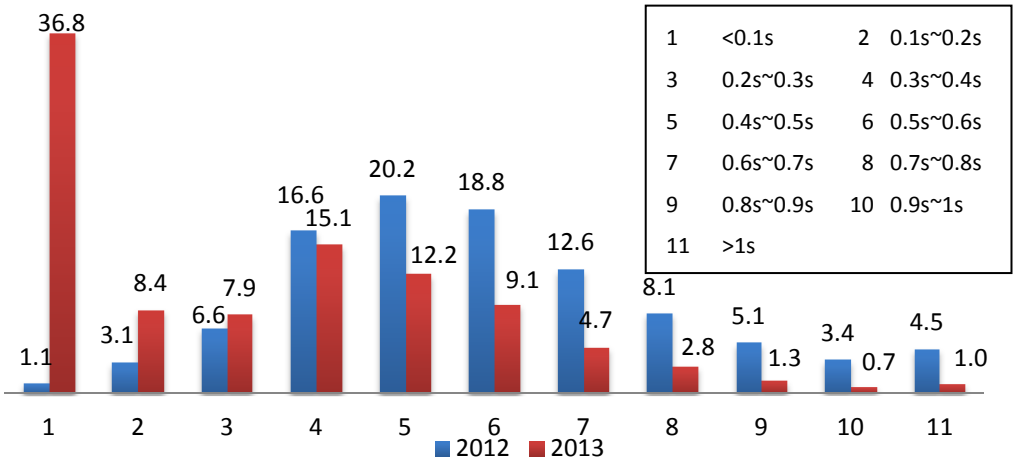

图 12 二级及以下权威域名服务器查询时延比例分布情况（%）

3.3.5 国内重点权威域名服务系统

3.3.5.1 简介

为了能够更加全面深入的了解我国域名体系的整体安全状态，本报告还抽样

选择了约三百个来自政府机构、金融机构、网络运营商以及涉及到国计民生行业的热门域名，对其权威域名服务器的安全配置情况进行了监测。

3.3.5.2 系统软件

监测显示，我国重点权威域名服务器采用 Linux 或 Unix 操作系统的比例为 80.7%。DNS 软件中，采用各版本 BIND 软件所占比例为 94.16%，但是，仍然有 23.2%的 BIND 服务器开启了版本应答，存在一定的安全隐患（去年该比例为 30%）。

3.3.5.3 协议支持

国内重点权威域名服务器的协议支持情况如图 13 所示。

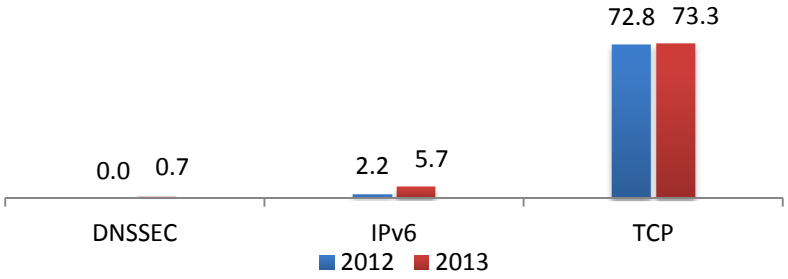

图 13 国内重点权威域名服务器协议支持情况（%）

由此可见，国内重点域名对于 IPv6 以及 DNSSEC 的支持性相比去年略有提高。此外，仍然有 10.15%的服务器开启了递归服务，存在遭受 DoS 攻击的风险（去年该数据为 24.5%）。

3.3.5.4 服务性能

在服务冗余方面，92.5%的国内重点权威域名具有冗余配置，总体冗余程度较高。

此外，有 10.2%的服务器开启递归服务，较去年有所降低（去年比例为 24.6%），仍然存在遭受 DoS 攻击的风险。

国内重点域名的 TTL 设置情况如图 14 所示。由此可见，大部分国内重点域名的 TTL 设置较大，域名权威数据稳定。

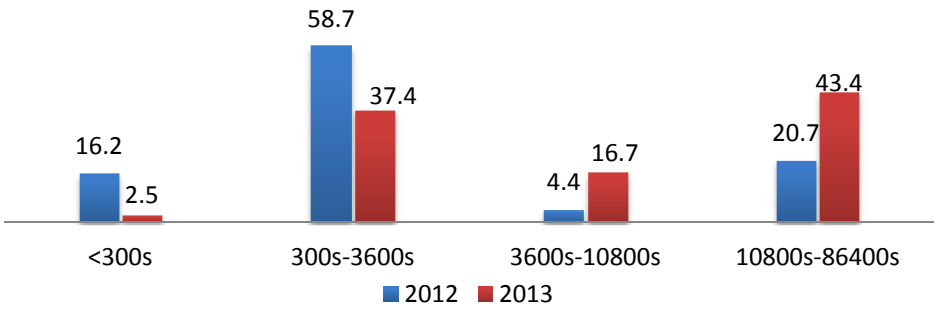

图 14 国内重点域名 TTL 设置比例分布情况（%）

此外，大约 73.5%的重点权威域名服务器的解析时延均小于 100 毫秒，具有良好的服务性能。

3.4 递归域名服务系统

3.4.1 简介

递归域名服务系统作为和客户端直接交互的环节，其配置情况和运行状态对于用户所获取到的 DNS 解析数据的完整性、正确性和及时性有直接的影响。为了解全球范围内的递归服务器配置情况和运行状态，本报告以.CN 顶级域名服务器连续七天日志中出现的递归域名服务器作为监测样本[6]进行了监测，以下是详细的监测结果。

3.4.2 系统软件

递归域名服务器采用 Linux 或者 Unix 操作系统的比例达到 94.9%。所采用的 DNS 软件中，BIND 所占比例高达 96.36%，其中同样以 9.2.3rc1—9.4.0a0 软件最多，占到所有 BIND 版本的 97.6%，具体分布如表 4 所示。由此可见，BIND 在所有 DNS 软件中所占比例绝对领先，但有很大比例的 BIND 服务器仍使用较旧版本。此外，仍有 38.9%的 BIND 软件开启了版本应答功能（去年该数据为 39.3%）。

表 4 递归域名服务器 DNS 软件比例分布情况

软件类型	2012年所占比例（%）	2013年所占比例（%）
ISC BIND	93.5	96.36
NLnetLabs NSD	1.2	2.07
Microsoft Windows DNS 2000	1.07	0.66
JHSOFT simple DNS plus	0.3	0.35
Raiden DNSD	0.13	0.18
bboy MyDNS	0.09	0.07
DJ Bernstein TinyDNS	0.81	0.05
robtex Viking DNS module	0.09	0.03
Cisco CNR	0.04	0.03
PowerDNS	0.04	0.03
Nominum CNS	1.79	0.03
Microsoft Windows DNS 2003	0.13	0.02
Other	0.81	0.12

[6] 只考虑日查询量连续七天超过百次的递归服务器，共计约 9.2 万台。

3.4.3 协议支持

递归域名服务器的协议支持情况如图 15 所示，与去年监测结果相比，DNSSEC、TCP 以及 EDNS0 的支持率都有了一定程度的提升，其中 DNSSEC 支持率较去年提升了一倍多，但总体仍然偏低。

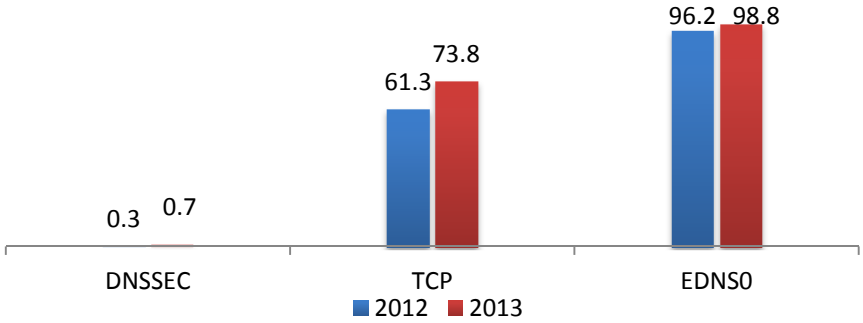

图 15 递归域名服务器协议支持比例情况（%）

另外，递归域名服务器对于大数据包的支持情况相比去年有了明显改善，支持超过 512 字节的大数据包的比例从去年的不足 6%猛增至今年的 53.9%，如图 16 所示。

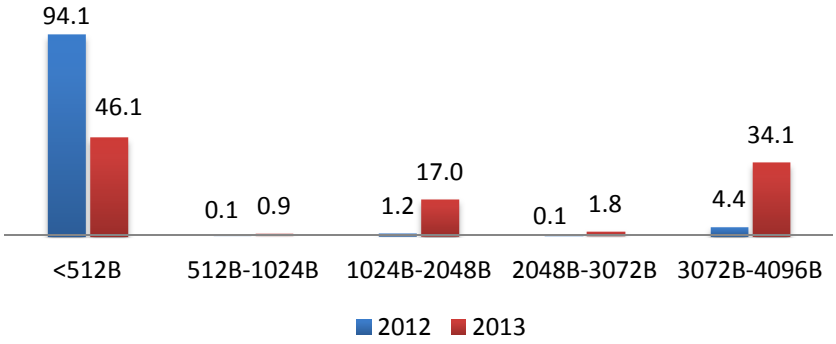

图 16 递归域名服务器最大数据包支持比例分布情况（%）

长期以来，递归域名服务器一直受到缓存中毒攻击的威胁，而其中主要的原因就是递归域名服务器的端口随机性不足，从而提高了中毒攻击的成功率，图 17 所示为递归域名服务器的端口随机性程度比例分布情况。

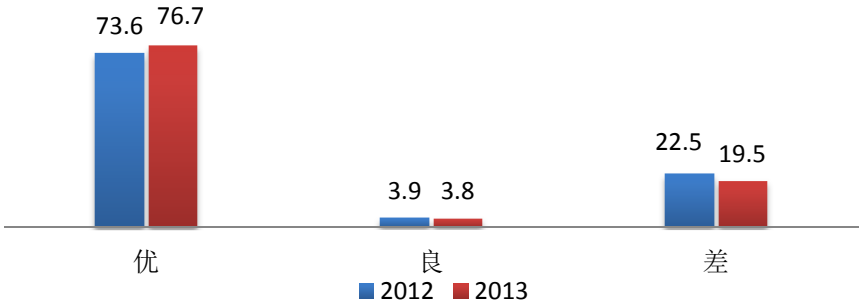

图 17 递归域名服务器端口随机性程度比例分布情况

3.4.4 服务性能

递归域名服务器的查询时延比例分布情况如图 18 所示。由此可见，递归域名服务器查询时延比例分布情况与去年的监测结果基本一致，整体上递归域名服务器的查询时延差异较大。

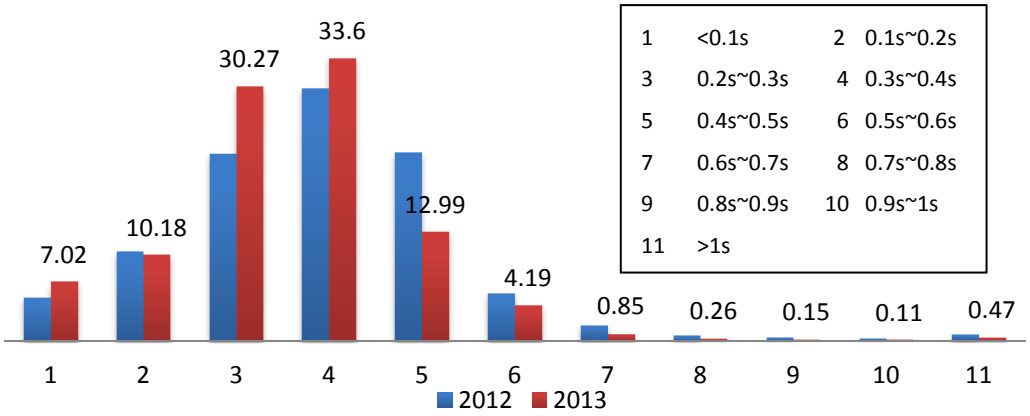

图 18 递归域名服务器查询时延比例分布情况（%）

3.4.5 国内递归域名服务系统

3.4.5.1 简介

本报告还对位于国内的递归域名服务器作了抽取（共计大约八千台），并对其进行了针对性的监测。以下是相关监测结果展示。

3.4.5.2 系统软件

结果显示，国内递归域名服务器使用 ISC BIND 软件的比例为 95.9%，同样以版本 9.2.3rc1—9.4.0a0 居多，占到所有 BIND 软件版本的 95.7%，其中 BIND 版本应答比例为 30.2%，略低于全球递归域名服务器的 BIND 版本应答比例（38.9%）。

3.4.5.3 协议支持

国内递归域名服务器的协议支持情况如图 19 所示。

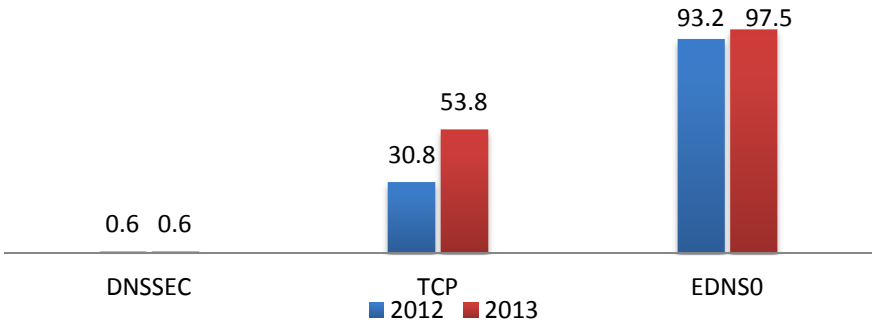

图 19 国内递归域名服务器协议支持比例分布情况（%）

由此可见，国内递归域名服务器对于 EDNS0 的支持已经非常广泛，但是对于 TCP 支持低于全球平均水平（73.8%）。另外，国内递归域名服务器的 DNSSEC 支持率同样偏低，仅有 0.64%。值得注意的是，国内递归域名服务器对于大数据包的支持情况较去年相比有了明显改善，支持超过 512 字节的大数据包的服务器从去年的不足 10%猛增至今年的超过 50%，具体如图 20 所示。

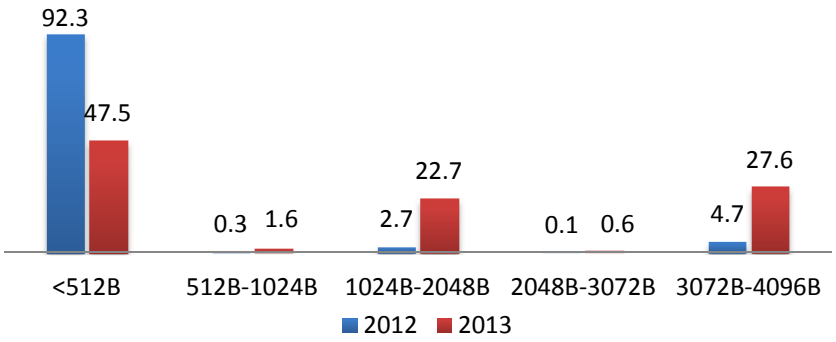

图 20 国内递归域名服务器最大数据包支持比例分布情况（%）

国内递归域名服务器的端口随机性程度比例分布情况如图 21 所示，该结果

和去年的监测结果基本一致，但整体上低于全球平均水平。

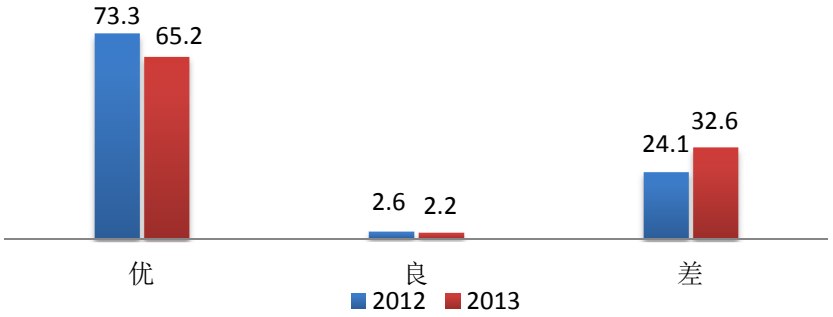

图 21 国内递归域名服务器端口随机性程度比例分布情况

3.4.5.4 服务性能

国内递归域名服务器的查询时延分布如图 22 所示。由此可见，国内递归域名服务器查询时延比例分布情况与去年的监测结果基本一致，查询时延大部分分布在 300 毫秒以内，整体解析性能良好。

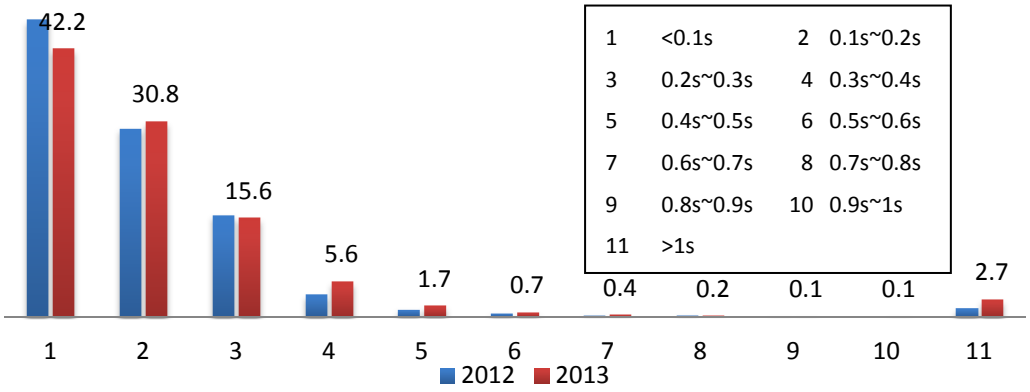

图 22 国内递归域名服务器查询时延比例分布情况（%）

4、域名服务安全评估

域名服务体系安全评估旨在针对域名体系特定环节，选择恰当的检测项并进行归一化处理，然后根据域名系统常见安全威胁进行检测项的权重设置，从而通过量化以实现对该系统整体安全状态的客观、准确评估。

4.1 权威域名服务系统

权威服务器主要用于维护和提供 DNS 权威数据，其可能遭受的攻击包括 DoS 攻击、数据篡改等，对权威服务器的安全评估主要考虑权威系统服务架构、服务器配置、安全功能支持以及服务器性能四个方面。安全指标如表 5 所示。

表 5 权威服务安全指标

安全指标值	含义
0≤#<0.4	服务安全差，如存在配置漏洞
0.4≤#<0.7	服务安全良，如无配置漏洞
0.7≤#≤1	服务安全优，如具有若干安全防护配置

根据测试结果，得出图 23 所示的权威域名服务安全状态分布。

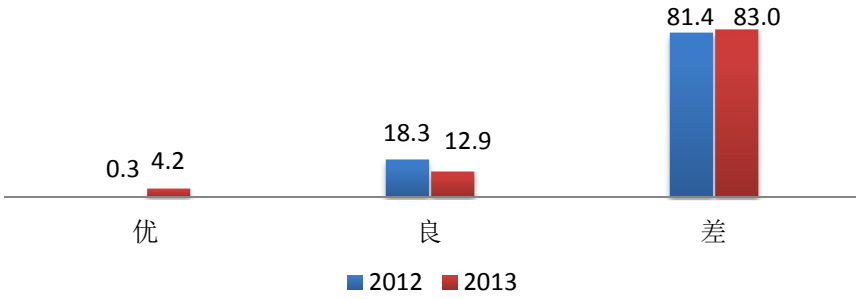

图 23 权威域名服务安全状态分布（%）

由此可见，和去年的监测数据相比较，安全状态为差的权威域名服务器比例仍占据八成以上，配置漏洞现象在权威域名服务器中普遍存在。另外，安全状态为优的权威域名服务器比例略有提升，由去年的 0.3%升至今年的 4.17%。

各国家和地区的权威域名服务器平均安全状态如图 24 所示。

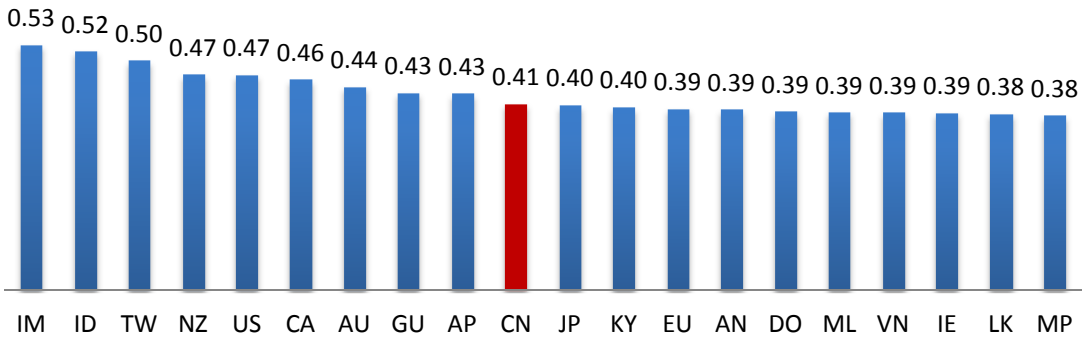

图 24 各国家和地区的权威域名服务平均安全状态分布情况

中国境内的权威域名服务器平均安全指标为 0.41，安全状态为良，较去年分值（0.39）略有提升。

对于国内重点权威域名服务器，其安全状态分布如图 25 所示。

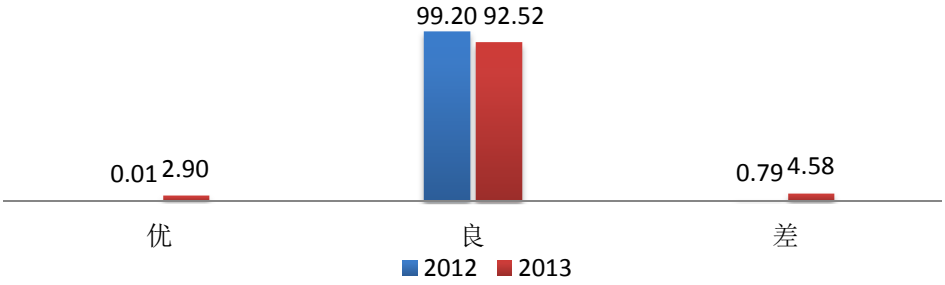

图 25 国内重点权威域名安全状态分布情况（%）

由此可见，国内重点权威域名服务器的安全状况相对优于全体权威域名服务器的总体安全状况，大部分国内重点权威域名服务器配置较为完善，安全状态良好。

4.2 递归域名服务系统

递归服务器发起 DNS 解析操作，并对所获取到的权威数据进行缓存，其可能遭受的攻击包括 DoS 攻击、缓存中毒等，对递归服务系统的安全评估主要考虑服务器配置、安全功能支持以及服务器性能三个方面，安全指标如表 6 所示。

表 6 权威服务安全指标

安全指标值	含义
0≤#<0.4	服务安全差，如存在配置漏洞
0.4≤#<0.7	服务安全良，如无配置漏洞

0.7≤#≤1	服务安全优，如具有若干安全防护配置

根据测试结果，得出图 26 所示的递归域名服务安全状态分布。可见，递归域名服务器安全状态整体较好。

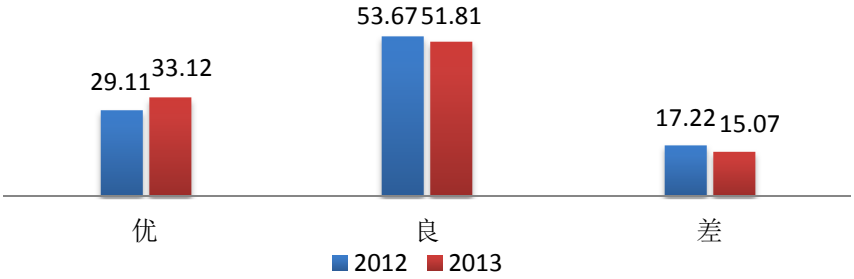

图 26 递归域名服务安全状态分布情况（%）

各国家和地区的递归域名服务器平均安全状态如图 27 所示。

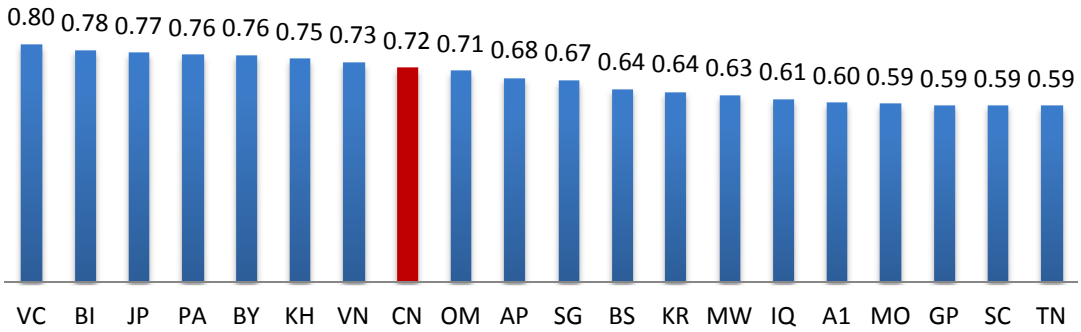

图 27 递归域名服务安全状态分布情况

中国境内大部分递归域名服务器在配置和运维方面都较规范，其平均安全指标为 0.72，相比去年同样有略微提升（去年为 0.70），安全状态为优。

中国境内的递归域名服务器安全状态具体分布如图 28 所示。

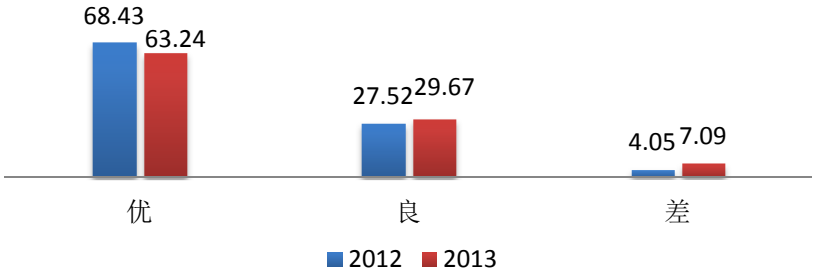

图 28 国内递归域名服务安全状态比例分布情况（%）

由此可见，国内的递归域名服务器的安全状况相对优于全体递归域名服务器的总体安全状况，但也有少部分服务器存在一定的安全配置漏洞。

另外，可以发现，权威域名服务器和递归域名服务器的安全评估结果存在一

定差异，递归域名服务器的安全评估结果相对较好。由于针对递归域名服务器和权威域名服务器安全状况的评价标准不同，且各自的监测范围存在较大差异（权威域名服务器涉及到三大顶级域下的超过 1.3 亿的所有域名，而递归域名服务器这里只针对.CN 顶级域连续七天日查询量超过百次的共计约 9.2 万台递归域名服务器，这些繁忙的递归域名服务器往往具备较高的安全管理水平），因此导致了上述结果的出现。

5、我国域名基础设施安全态势分析

基于域名系统的重要性和其在互联网领域牵一发动全身的地位，对我国域名服务体系进行整体的安全监测和运行分析,不仅可以为国家提供第一手的域名服务系统情况，还可以根据监测分析，向国家提出对域名服务系统、对网络安全、以及互联网建设和治理方面的建议，从而有效地增强国家对互联网的管控能力，促进互联网产业健康有序地发展，从根本上提升我国域名体系的安全保障能力，具有显著的社会意义。

本报告的监测结果表明，我国权威域名服务和递归域名服务在配置管理和运行维护方面仍然存在不同程度的安全隐患，但整体安全状况相比去年有略微提升。总体来看，我国权威域名服务和递归域名服务的安全状况均优于世界平均水平，但仍存在较大的提升空间。

结合本报告监测结果，我国域名基础设施安全态势呈现出以下几方面显著特点：

1）除根域名服务以外的其他各级域名服务仍然存在不同程度的安全问题，表现在系统软件、协议支持和服务性能等各个方面，但总体来看，各级域名服务的安全状况相比去年都有了一定的改善。

2)我国域名系统对于 IPv6 协议支持程度进一步提升，这有助于加速基于 IPv6 的下一代互联网的过渡进程，同时域名系统对于 IPv6 资源记录和过渡环境的全面支持还需要进一步加强。

3）虽然 DNSSEC 服务在根区已部署数年，目前在顶级域名服务器中的部署比率也已接近半数，但在二级及以下权威域名服务器和递归域名服务器中的部署程度仍然严重匮乏，这也将是今后 DNSSEC 部署推进工作的重点所在。

4）今年以来，有 50 多个新通用顶级域正式入根生效，未来还将有更多的新通用顶级域涌入。由于新通用顶级域的运营服务经验相对不足，因此新通用顶级域的安全管理将是今后域名安全领域的一个重要议题。

地址：北京中关村南四街四号中国科学院软件园1号楼一层
7*24小时客户服务咨询电话：+86-10-58813000
传真：86-10-58812666
邮政地址：北京349信箱6分箱 CNNIC
邮政编码：100190
网址：http://www.cnnic.cn
http://中国互联网络信息中心.中国
电子邮件：ndsa_public@cnnic.cn