CNNIC 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

2012

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
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
TCP	Transmission Control Protocol	传输控制协议
TTL	Time To Live	生存时间
UDP	User Datagram Protocol	用户数据报协议

1、前言

域名系统（Domain Name System，DNS）是互联网重要的基础设施，目前大多数的互联网应用，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。对域名系统的安全检测一方面有助于对域名服务器安全状态进行完整、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）即开始从多角度对整个域名服务体系的配置情况和安全态势进行检测与分析，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 基于此方面已有工作，2012 年在全国范围内部署了更为广泛的检测节点，并设计开发了故障、配置、性能和流量等多角度的检测项，以对域名服务体系的根域名服务系统、顶级权威域名服务系统、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检测和客观评估。

2、摘要

周期性的重复检测及分析结果显示：

1) Linux 和 BIND 为权威及递归服务器所采用的最主要的操作系统和域名解析软件，但 BIND 的版本应答比例普遍较高，具有一定安全隐患；
2) 根域名服务系统的协议支持完善，安全保障较好。此外，由于采用了全球范围内的镜像部署，可提供稳定高效的解析服务；
3) 顶级权威域名服务系统的冗余配置较好，保证了稳定的解析性能，但对 DNSSEC 及相关配套协议的支持还有待进一步完善；
4) 二级及以下权威域名服务系统分布广泛，服务器配置状态参差不齐，主要在 DNSSEC 和服务器冗余配置方面应进一步加强；
5) 递归域名服务系统的主要问题为端口随机性设置仍有待加强。此外，虽然递归域名服务器对 EDNS0 的支持已经较为普遍，但并未有效配置以支持大数据包，仍有 94%以上的服务器仅支持 512bytes 以内的数据包。

3、域名服务安全状况

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，主要由基础运营商运行管理。具体架构如图 1 所示。

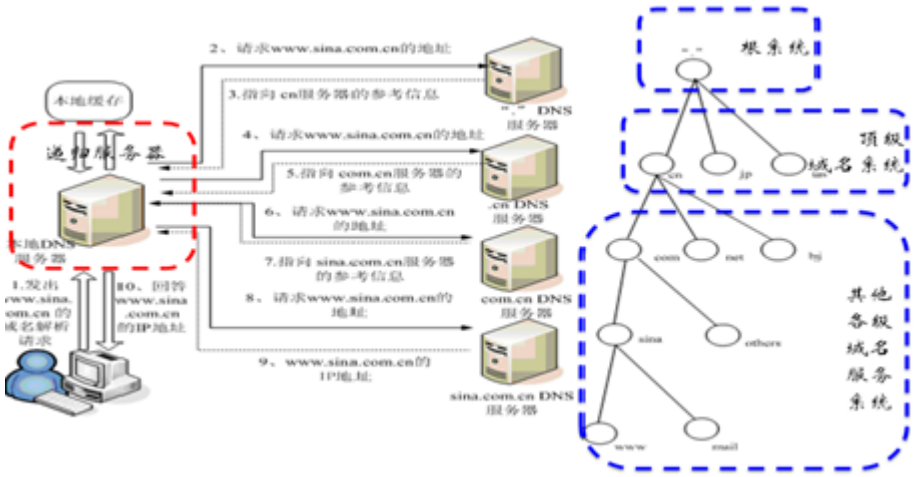

图 1 域名服务体系的构成

根据域名服务体系构成及其各部分的服务模式，本报告从域名服务体系各系统的底层操作系统和 DNS 软件到上层的域名服务架构，以及服务器的功能配置和解析性能进行检测，以期全面反映域名服务体系的安全配置情况和运行状态。

3.1 根域名服务系统

3.1.1 简介

DNS 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 DNS 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 2012 年 12 月 17 日，域名系统 13 个根服务器在全球的镜像节点数量共 348 个，其分布如图 2 所示，中国大陆有 F 根、I 根、J 根和 L

根的镜像节点。

图 2 根镜像全球分布情况

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	4
C	Cogent Communications	IPv4: 192.33.4.12	2149
D	University of Maryland	IPv4: 128.8.10.90 IPv6: 2001:500:2D::D	27
E	NASA Ames Research Center	IPv4: 192.203.230.10	297
F*	ISC	IPv4: 192.5.5.241 IPv6: 2001:500:2f::f	3557
G	U.S. DOD NIC	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*	Autonomica	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

[1] 注：“*”表示在中国境内具有该服务器镜像节点。

L*	ICANN	IPv4: 199.7.83.42 IPv6: 2001:500:3::42	20144
M	WIDE Project	IPv4: 202.12.27.33 IPv6: 2001:dc3::35	7500

3.1.2 DNSSEC

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，必须在从根区域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，所有根服务器都支持 NSEC3，从而避免区文件被遍历、枚举的风险。

3.1.3 IPv6 和 TCP

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。由此可见，根服务器的 IPv6 和 TCP 支持已经较为完善。

3.1.4 服务架构

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 Anycast 机制在全球范围内广泛部署镜像节点。截至 2012 年 12 月 11 日，全球共有 348 个 DNS 根服务器镜像节点，除了由 Information Sciences Institute 运维的 B 根和由 University of Maryland 运维的 D 根外，其他 11 个根服务器均在全球范围内部署了广泛的镜像节点，具体分布如图 3 所示。

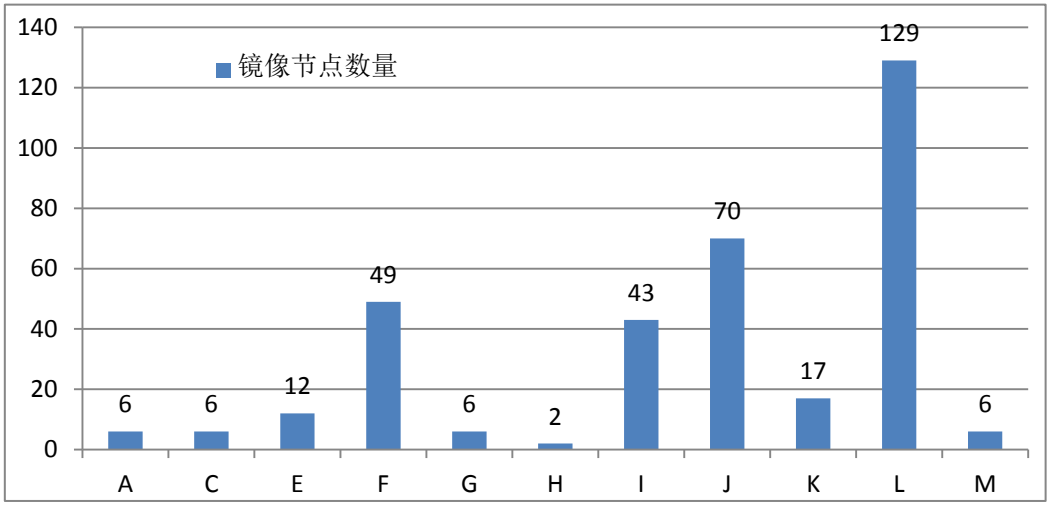

图 3 根服务器镜像部署情况

3.1.5 查询时延

根域名服务系统采用 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 根服务节点，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检测节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，本报告对分布在全国范围内的 39 个检测节点的探测结果取平均值，具体结果如图 4 所示。

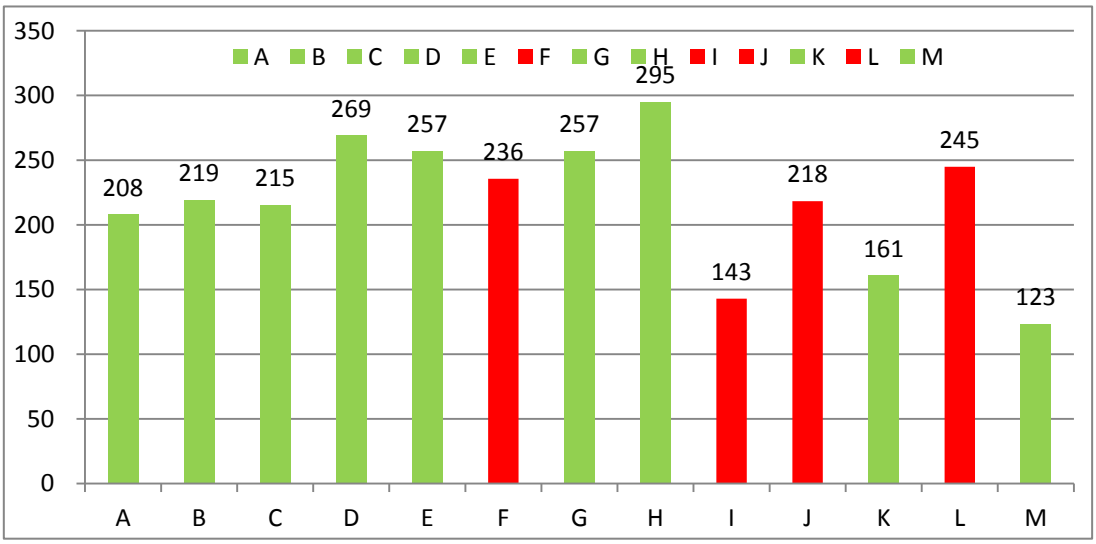

图 4 根服务器查询时延分布情况（毫秒 ms）

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。2011 年，CNNIC 在北京新增一个 F 根镜像。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。

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，顶级域名分为四类：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（目前仅有.arpa）和实验性顶级域。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），当前全球域名服务体系共有 329 个 TLD。

3.2.2 DNS 软件

顶级权威域名服务器所采用 DNS 软件分布如表 2 所示。采用 BIND 的比例高达 93.04%，版本区间 9.2.3rc1-9.4.0a0 内的比例为 98%。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，37.4%的 BIND 软件开启版本应答功能，具有一定的安全隐患。

表 2 顶级权威服务器的 DNS 软件分布

软件类型	软件版本	所占比例
DJ Bernstein TinyDNS	1.05	0.29%
ISC BIND	8.3.0-RC1 -- 8.4.4	0.49%
	9.2.0rc7 -- 9.2.2-P3	1.08%
	9.2.3rc1 -- 9.4.0a0	91.47%
JHSOFT simple DNS plus		0.10%
Meilof Veeningen Posadis		0.10%
NLnetLabs NSD	1.2.3 -- 2.1.2	0.20%
	2.1.3	0.20%
Nominum ANS		0.20%
UltraDNS	2.7.0.2 -- 2.7.3	0.78%
VeriSign ATLAS		5.10%

3.2.3 DNSSEC

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，至今已有 31%的顶级权威域实现了 DNSSEC 签名，对于所支持的加密算法，均为 RSASHA1-NSEC3-SHA1 和 RSA/SHA-256。其中有 91 个 TLD 已经在根区发布了其对应的 DS 记录，其中有 3 个 TLD 也同时向 ISC 的 DLV 提交了 DS 记录，分别为.am，.kg 和.ua。

但是有 20%的 DNSSEC 顶级权威域名服务器未支持 NSEC3 而采用传统的 NSEC 机制，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。

3.2.4 IPv6 和 TCP

顶级权威域名服务器对 IPv6 和 TCP 协议的支持情况如图 5 所示。

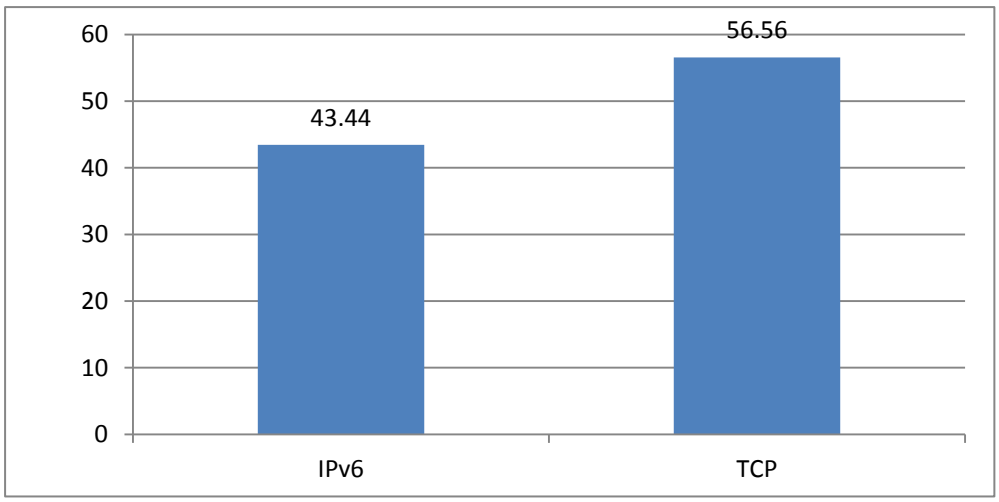

图 5 顶级权威服务器的 IPv6 和 TCP 支持性（%）

可见，顶级权威服务器的 IPv6 和 TCP 支持比较完善。

3.2.5 服务架构

TLD 的权威服务器均具有冗余配置[2]，具体情况如图 6 所示。

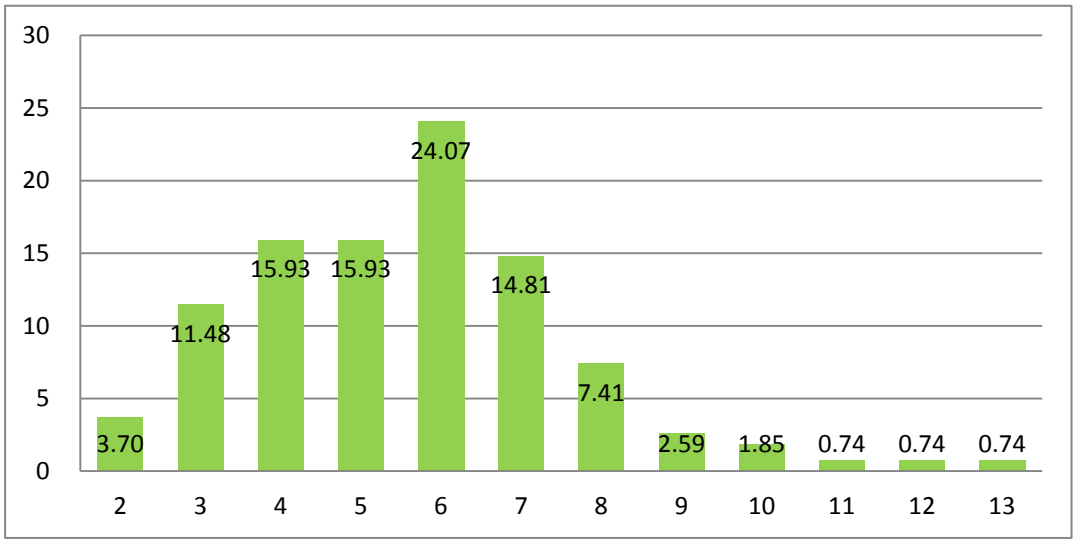

图 6 服务器冗余性分布（%）

但是 1.6%的权威服务器仍然开启递归服务，这种配置缺陷具有易遭受 DoS 攻击的风险。

3.2.6 解析性能

部署多台权威服务器能够起到增强权威解析服务鲁棒性和抗攻击能力的效

[2] 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。

果。但检测显示，16%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[3]。

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。

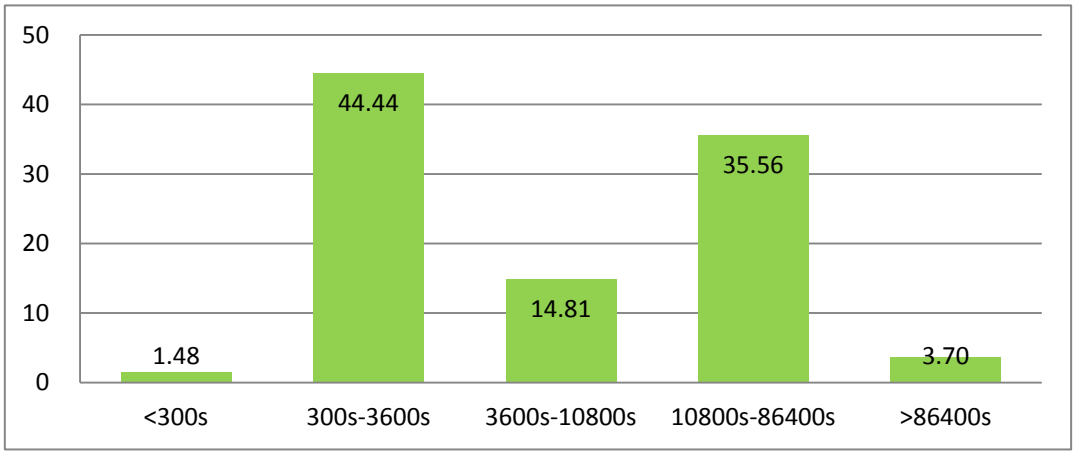

图 7 顶级权威域的 TTL 设置分布（%）

顶级权威域名服务器的查询时延分布如图 8 所示。

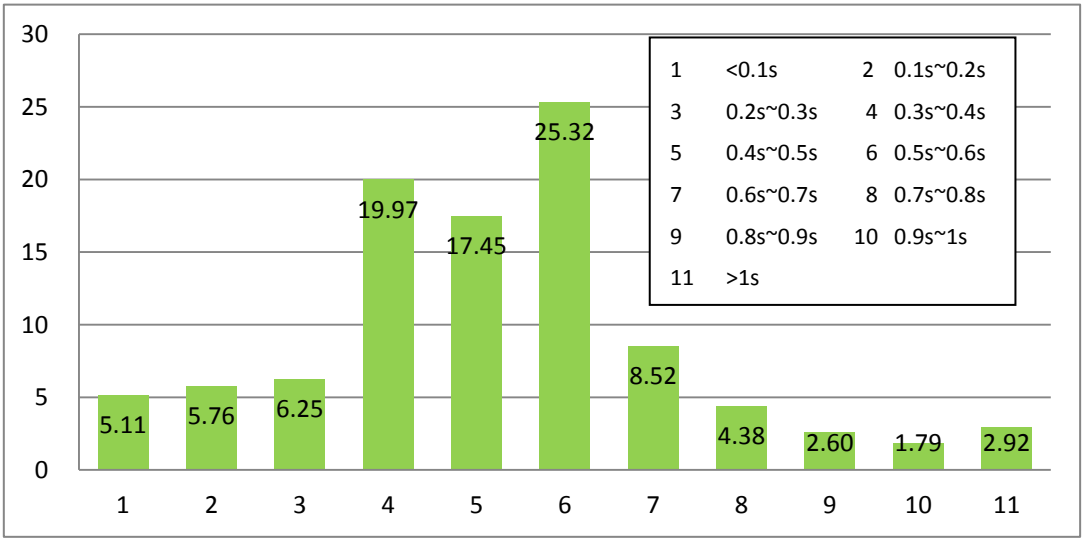

图 8 顶级权威服务器查询时延分布（%）

由于顶级权威域的运维和管理都较为成熟完善，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。

[3] 注：不排除检测时发生区传输等影响区数据的操作。

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 顶级域下的超过 1.2 亿个二级及以下域名作为检测对象。

3.3.2 操作系统和 DNS 软件

Linux 为权威服务器使用的最主流的操作系统类型，所占比例高达 70.9%。BIND 在所有 DNS 软件中所占比例绝对领先，为 92.17%。具体分布如表 3 所示。

表 3 二级及以下权威服务器的 DNS 软件分布

软件类型	软件版本	所占比例
DJ Bernstein TinyDNS	1.04	0.04%
	1.05	5.14%
ISC BIND	4.9.3 -- 4.9.11	0.04%
	8.1-REL -- 8.2.1-T4B	0.04%
	8.3.0-RC1 -- 8.4.4	0.47%
	9.1.0 -- 9.1.3	0.02%
	9.2.0a1 -- 9.2.2-P3	0.02%
	9.2.0rc4 -- 9.2.2-P3	0.02%
	9.2.0rc7 -- 9.2.2-P3	0.56%
	9.2.3rc1 -- 9.4.0a0	91.20%
JHSOFT simple DNS plus		0.49%
Microsoft Windows DNS	2000	0.70%
	2003	0.06%
	NT4	0.04%
NLnetLabs NSD	2.1.3	0.02%
Nominum ANS		0.02%
PowerDNS	2.8 -- 2.9.3	0.02%
	2.9.4 -- 2.9.11	0.06%
Sam Trenholme MaraDNS		0.04%
TZO Tzolkin DNS		0.02%

UltraDNS	2.7.0.2 -- 2.7.3	0.02%
XBILL jnamed (dnsjava)		0.02%
bboy MyDNS		0.95%

但有 91%的 BIND 服务器使用的版本为 9.2.3rc1-9.4.0a0。此外，40%的 BIND 软件仍开启版本应答功能，具有一定的安全隐患。

3.3.3 DNSSEC

虽然 DNS 根区和顶级域的 DNSSEC 部署已经比较广泛，但是二级及以下的权威域中仅有 0.25%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，所支持的加密算法分布如图 9 所示。

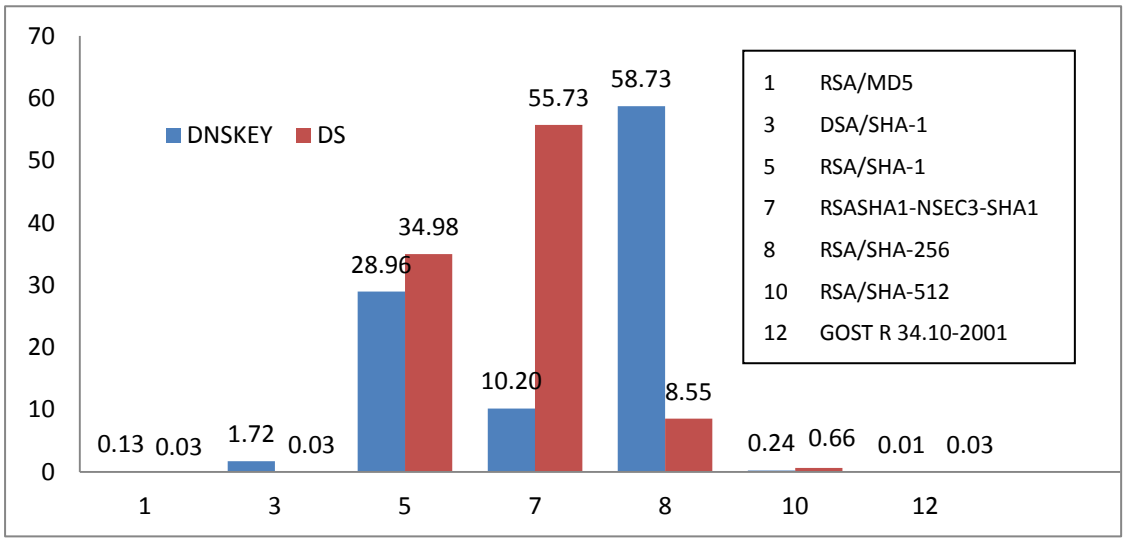

图 9 支持 DNSSEC 的二级及以下各级权威域的加密算法分布（%）

此外，有 39.7%的 DNSSEC 权威服务器未支持 NSEC3 而采用传统的 NSEC 机制。

3.3.4 IPv6 和 TCP

二级及以下各级权威域名服务器对 IPv6 和 TCP 协议的支持情况如图 10 所示。

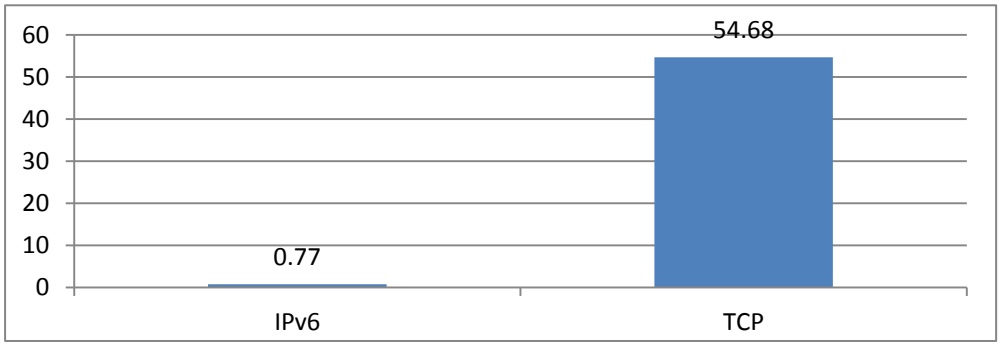

图 10 二级及以下各级权威服务器的 IPv6 和 TCP 支持情况（%）

由此可见，二级及以下各级权威的 IPv6 和 TCP 支持率仅为 0.77%和 54.68%，未能很好的支持 DNS 的演进。

3.3.5 服务架构

在服务冗余方面，二级及以下各级权威域配置较好，具体情况如图 11 所示。

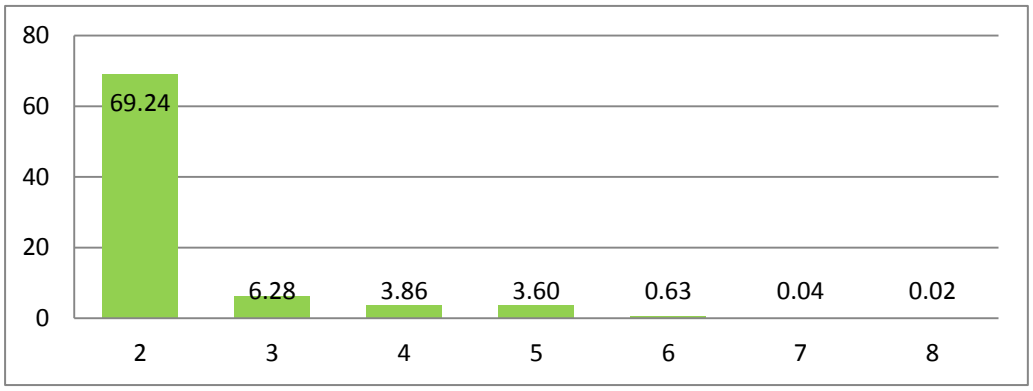

图 11 二级及以下各级权威服务器冗余性分布（%）

但是 15.9%的权威服务器仍然开启递归服务，这种配置缺陷具有易遭受 DoS 攻击的风险。

3.3.6 解析性能

二级及以下权威域名的 TTL 设置分布如图 12 所示。

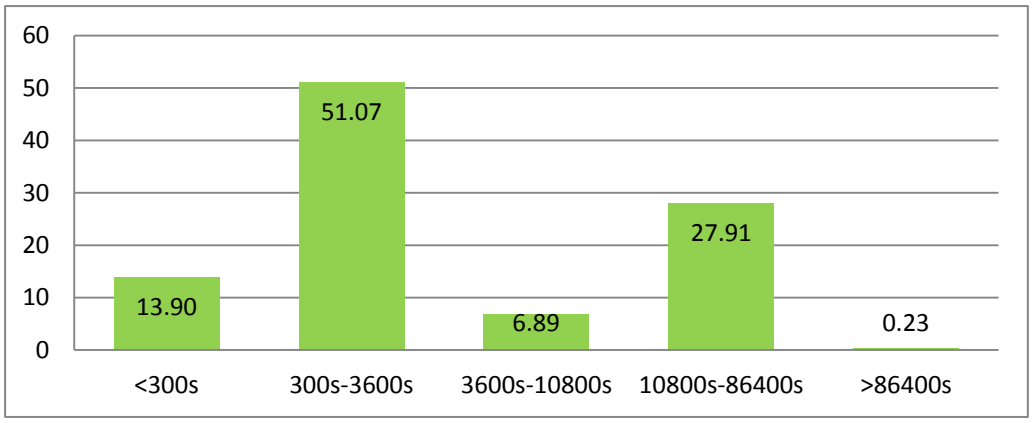

图 12 二级及以下各级权威域名 TTL 设置分布（%）

服务器的查询时延分布情况如图 13 所示。

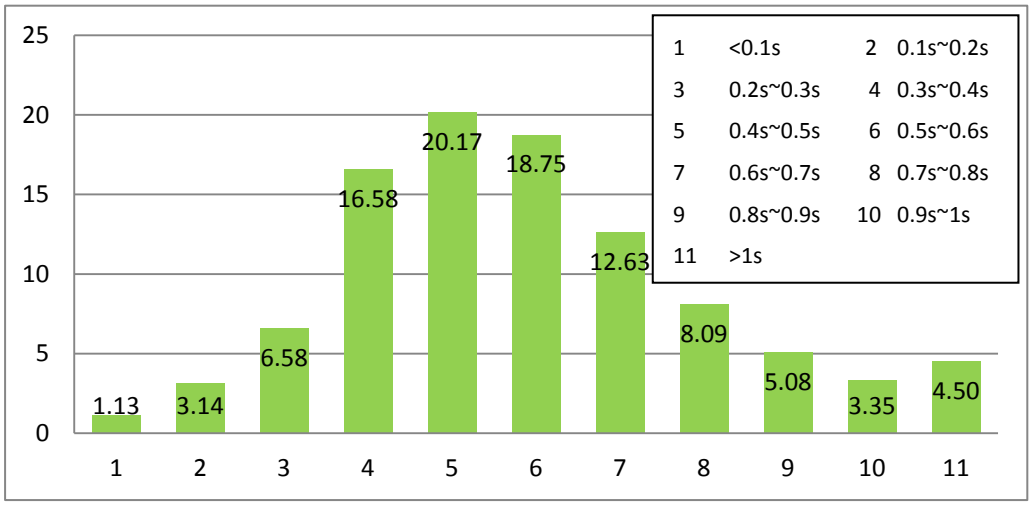

图 13 二级及以下各级权威服务器查询时延分布（%）

由于二级及以下各级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。

3.3.7 .CN 重点域名权威服务器检测结果

为了能够更加全面深入的了解.CN 域名体系的整体安全状态，本报告从.CN 顶级域区文件中抽样选择了 300 个来自政府机构、金融机构、教育机构、网络运营商以及涉及到国计民生行业的重点域名，对其权威服务器配置情况进行扫描。结果显示，.CN 重点域名权威服务器所用 Linux 比例为 42%。DNS 软件中，采用各版本 BIND 软件所占比例为 94%，但是，其中有高达 30%的 BIND 服务器均开启了版本应答，存在一定的安全隐患。

.CN 重点域名权威服务器的协议支持情况如图 14 所示。

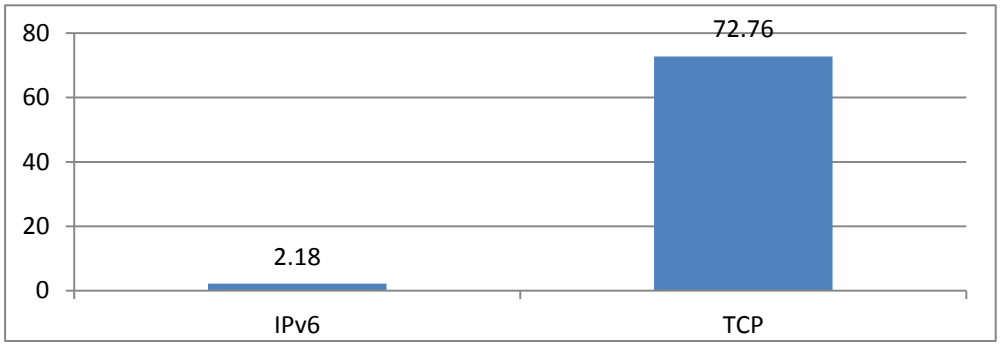

图 14 .CN 重点域名权威服务器的 IPv6 和 TCP 支持情况（%）

由此可见，.CN 重点域名对于 IPv6 的支持性有待进一步加强。

此外，有 24.5%的服务器开启递归服务，存在遭受 DoS 攻击的风险。重点域名的 TTL 设置情况如图 15 所示。

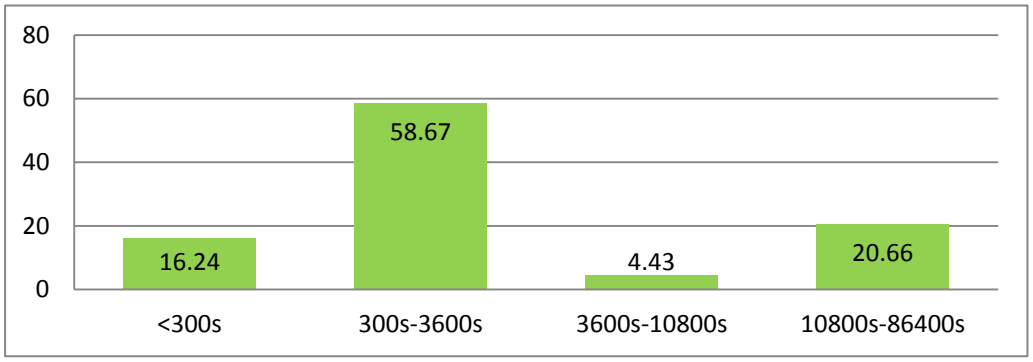

图 15 .CN 重点域名的 TTL 设置分布（%）

由此可见，大部分重点域名的 TTL 设置较大，域名权威数据稳定。此外，超过 95%的重点域名权威服务器的解析时延均小于 100ms，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 顶级域名权威服务器连续 7 天日志中的递归服务器作为检测样本，进行如下检测。

3.4.2 操作系统和 DNS 软件

Linux 是递归服务器所采用的主要操作系统类型，所占比例达到 51.8%。所采用的 DNS 软件中，BIND 所占比例高达 93.5%，其中以 9.2.3rc1—9.4.0a0 软件最多，占所有 BIND 软件的 96%，具体分布如表 4 所示。

表 4 递归服务器的 DNS 软件分布

软件类型	软件版本	所占比例
ATOS Stargate ADSL		0.09%
Cisco CNR		0.04%
DJ Bernstein TinyDNS	1.05	0.81%
ISC BIND	4.9.3 -- 4.9.11	0.09%
	8.1-REL -- 8.2.1-T4B	0.43%
	8.3.0-RC1 -- 8.4.4	1.20%
	9.1.0 -- 9.1.3	0.04%
	9.2.0a1 -- 9.2.2-P3	0.09%
	9.2.0rc7 -- 9.2.2-P3	2.01%
	9.2.3rc1 -- 9.4.0a0	89.62%
JHSOFT simple DNS plus		0.30%
Microsoft Windows DNS	2000	1.07%
	2003	0.13%
NLnetLabs NSD	1.0 alpha	1.20%
Nominum CNS		1.79%
Paul Rombouts pdnsd		0.09%
PowerDNS	2.9.4 -- 2.9.11	0.04%
Raiden DNSD		0.13%
VeriSign ATLAS		0.34%
bboy MyDNS		0.09%
robtex Viking DNS		0.09%

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，39.34%的 BIND 软件仍开启版本应答功能。

3.4.3 协议支持程度

递归服务器对 DNSSEC 的支持率仅为 0.29%，而对 TCP 的支持率为 61.3%。对 EDNS0 的支持率为 96.16%。但对于大数据包的支持仍不乐观，如图 16 所示。

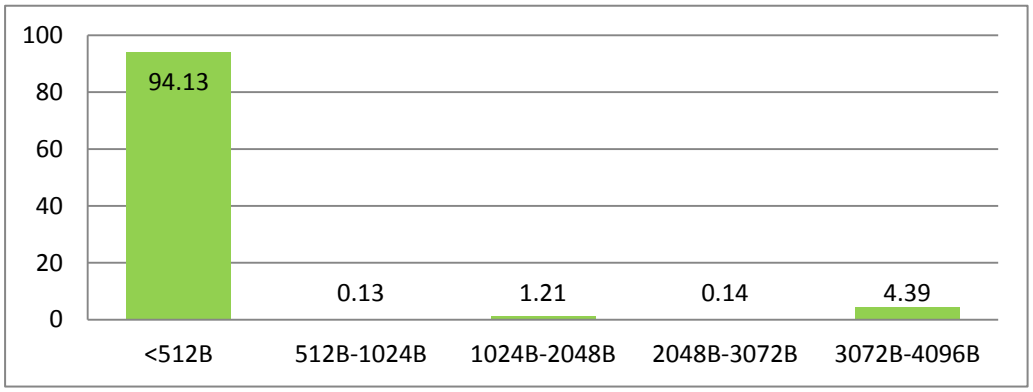

图 16 递归服务器对最大数据包支持分布（%）

长期以来，递归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 所示为递归服务器的端口随机性分布。

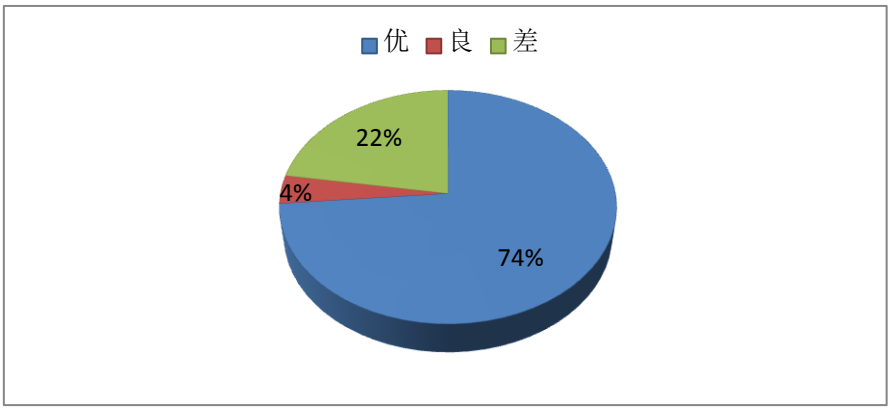

图 17 递归服务器端口随机性分布

3.4.4 查询时延

递归服务器的查询时延分布如图 18 所示。由此可见，递归服务器解析时延差异较大。

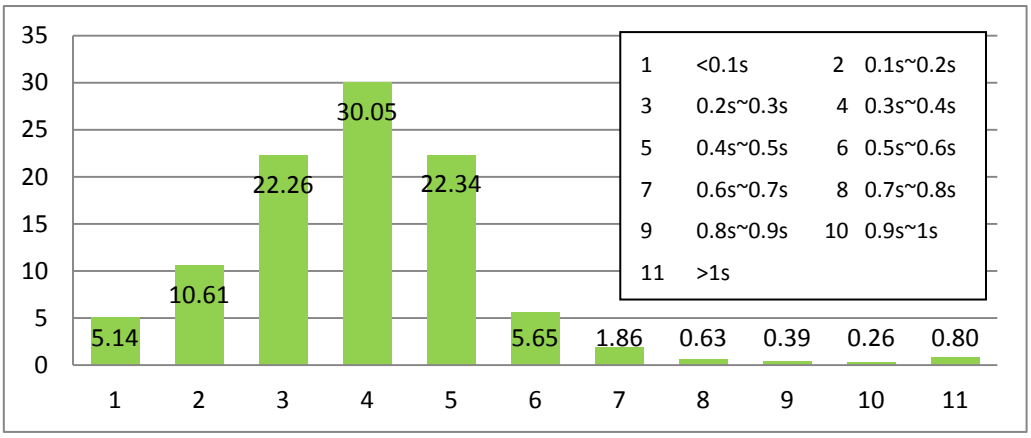

图 18 递归服务器查询时延分布（%）

3.4.5 国内递归服务器检测结果

本报告抽样选择了 26000 个国内运行的递归服务器，对其配置情况进行针对性的检测。结果显示，递归服务器 BIND 软件的比例为 87.4%。BIND 版本应答比例为 19.8%，低于全球递归服务器的 BIND 版本应答比例。其协议支持情况如图 19 所示。

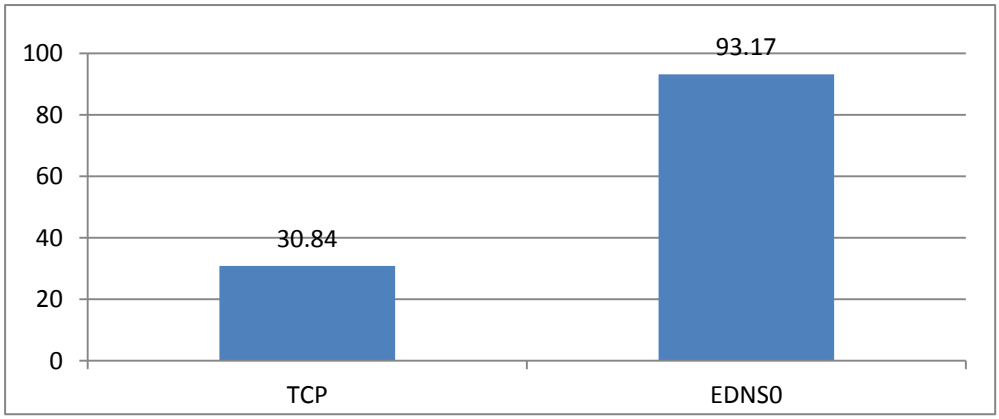

图 19 国内递归服务器协议支持情况（%）

由此可见，递归服务器对于 EDNS0 的支持已经非常广泛，但是对于大数据包的支持却不容乐观，具体如图 20 所示。

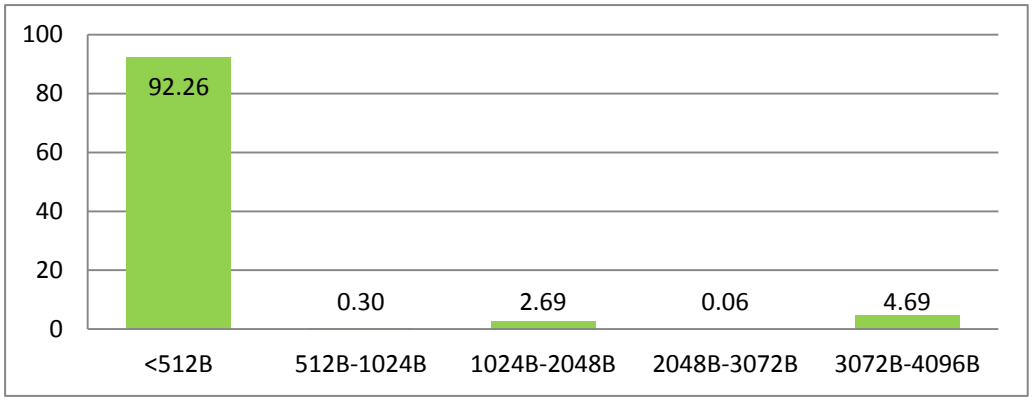

图 20 国内递归服务器对最大数据包支持分布（%）

国内递归服务器的端口随机性分布如图 21 所示，该结果和全球递归服务器的端口随机性状况基本一致。

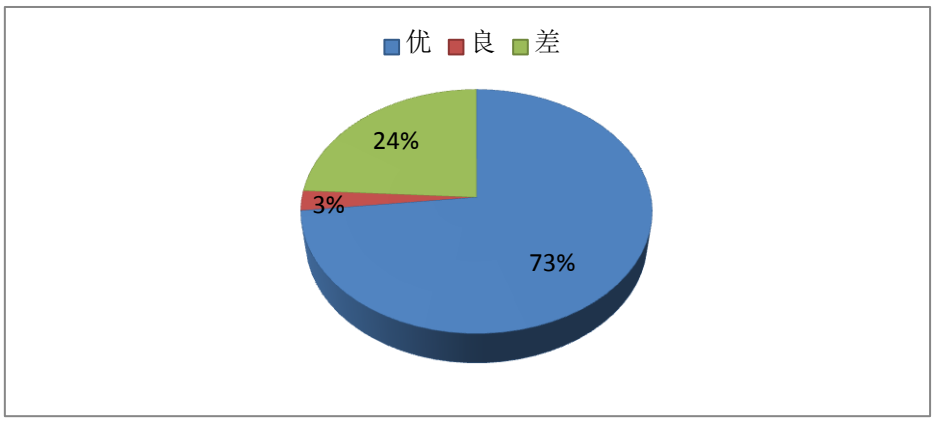

图 21 国内递归服务器端口随机性分布

国内递归服务器的查询时延分布如图 22 所示。

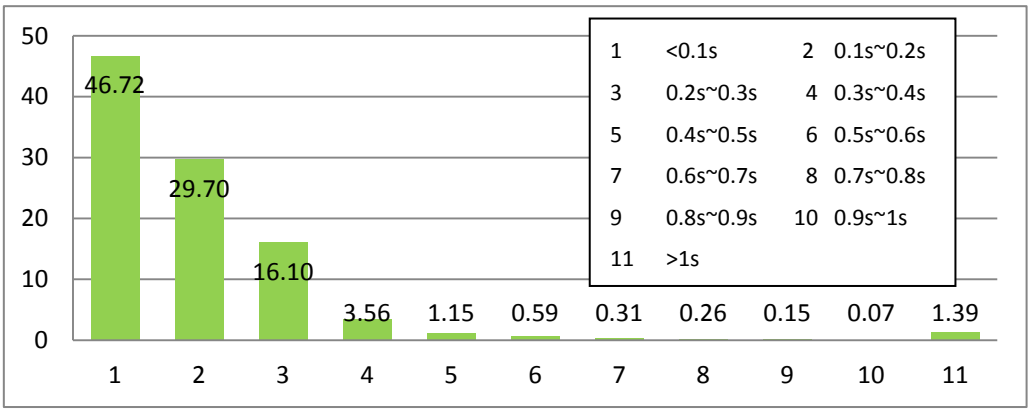

图 22 国内递归服务器查询时延分布（%）

由此可见，国内递归服务器查询时延基本分布在 300ms 以内，整体解析性能良好。

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 权威服务安全状态

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 所示的权威服务安全状态分布。

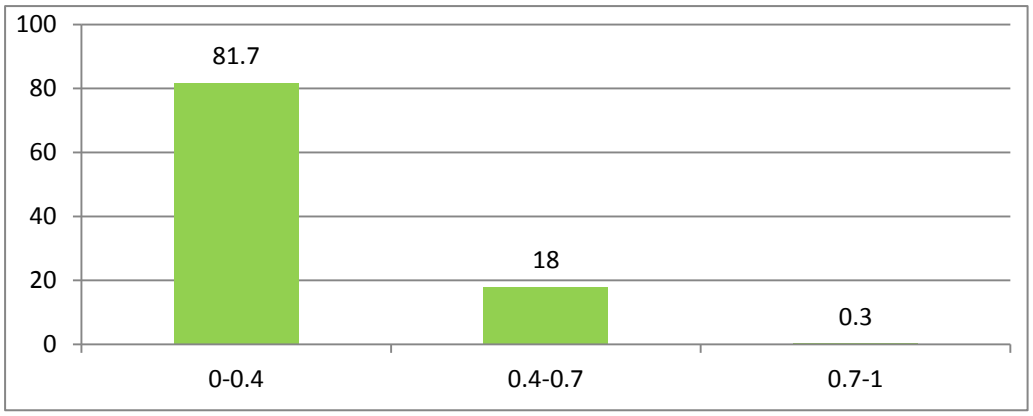

图 23 权威服务安全状态分布（%）

由此可见，大部分权威服务器安全状态差，具有一定的配置漏洞。

各国家和地区的权威服务器平均安全状态如图 24 所示。

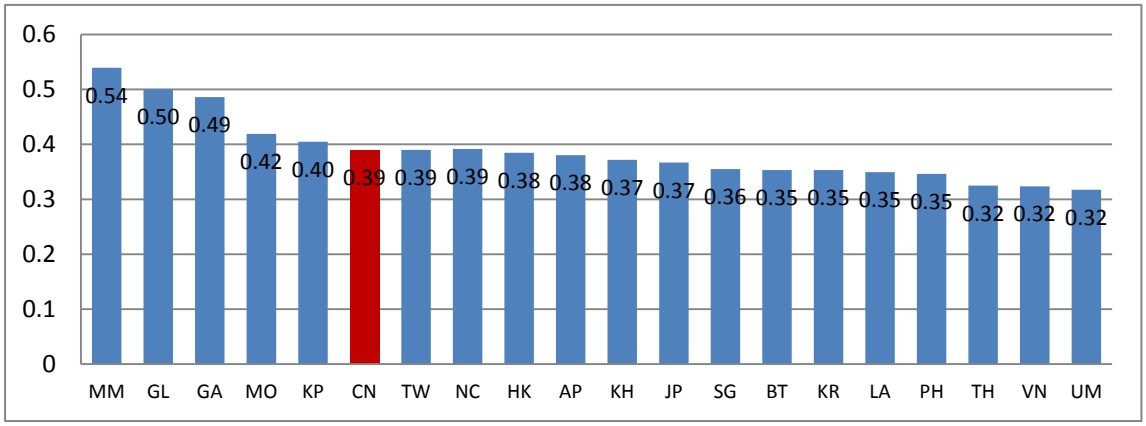

图 24 各国家和地区的权威服务平均安全状态分布

中国境内权威服务器平均安全指标为 0.39，安全状态差。

对于 CN 重点域名，其安全状态分布如图 25 所示。

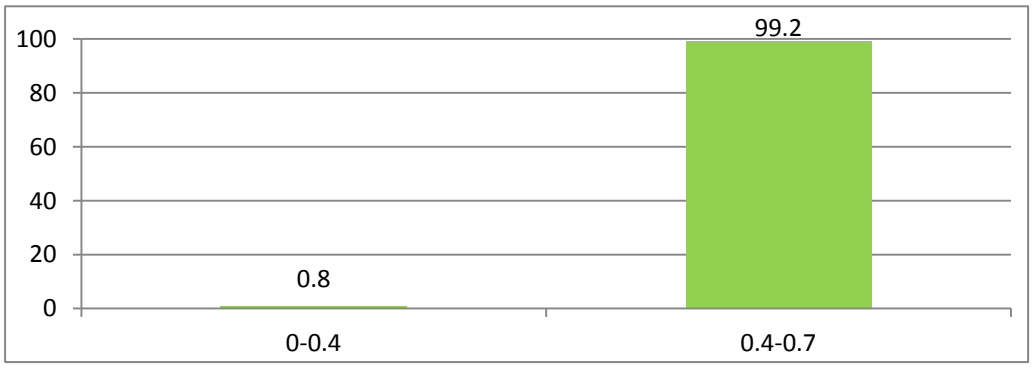

图 25 CN 重点域名安全状态分布（%）

由此可见，CN 重点域名权威服务器配置较为完善，安全状态良好。

4.2 递归服务安全状态

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 所示的递归服务安全状态分布。

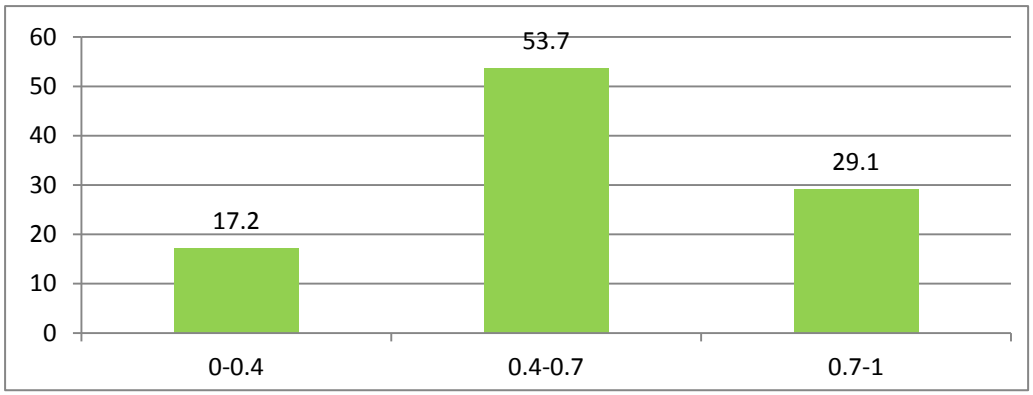

图 26 递归服务安全状态分布（%）

由此可见，递归服务器安全状态整体较好。

各国家和地区的递归服务器平均安全状态如图 27 所示。

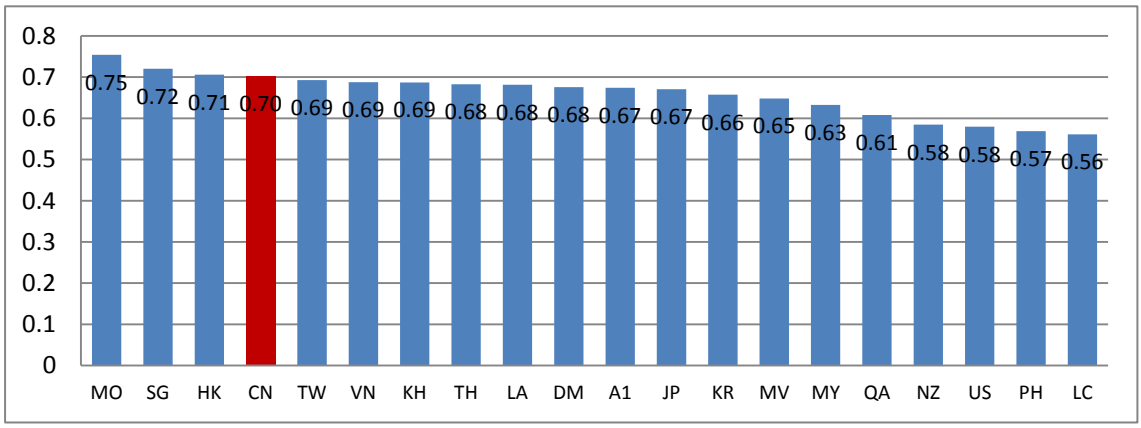

图 27 递归服务安全状态分布

中国境内大部分递归服务器在配置和运维方面都较规范，其平均安全指标为 0.70，安全状态为优。

中国境内的递归服务器安全状态具体分布如图 28 所示。

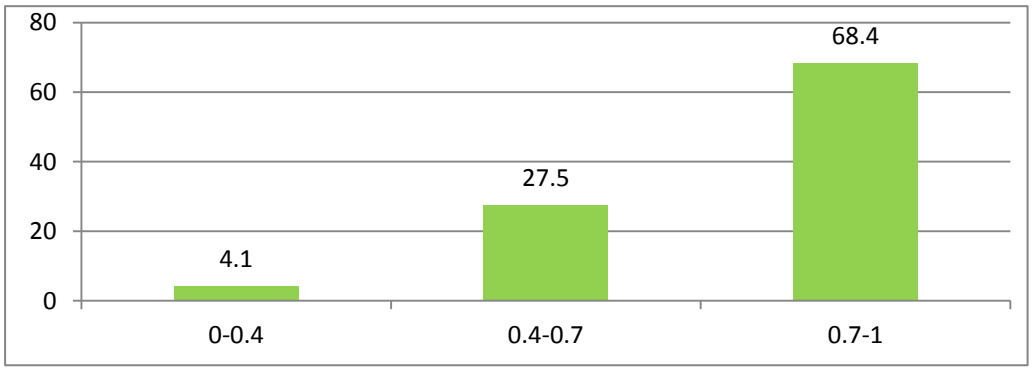

图 28 国内递归服务安全状态分布（%）

由此可见，递归服务器的安全状态相对较好。但也有少部分服务器存在一定

的安全配置漏洞。

5、域名服务安全态势分析

域名服务包含了权威域名服务和递归域名服务，域名服务器的正确、安全和可靠运行对于整个互联网的正常运作至关重要。本报告的检测结果表明，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均存在不同程度的安全隐患。对于国内域名服务体系，权威域名服务器安全状态整体较差，但.CN 重点域名的安全状态良好。此外，递归服务器的安全状态整体较好。

结合本报告检测结果，全球域名服务体系应着实加强如下方面的工作，以全面应对 DNS 的不断演进，特别是 DNSSEC 部署步伐的加快和 IPv6 普及程度的深入：

1）服务器的操作系统和 DNS 软件应进行及时升级，保证对最新漏洞的及时修补。对采用 BIND 的 DNS 服务器，应关闭软件的版本应答功能，提供一定程度的安全保证；

2）测试表明，实施 DNSSEC 后（以 RSA/SHA1 算法、密钥长度 ZSK 为 1024、KSK 为 2048 为例），权威区文件增大 4 倍，网络带宽增大为 4.5 倍，CPU 使用率增大 7%，内存容量增大 205%；递归服务器 DNS 应答包增大 5 倍，网络带宽增大 5 倍，CPU 使用率增大 20%，内存占用率增大 66.7%。因此，随着新 gTLD 申请的开放，应加快对 DNSSEC 技术的培训和实际部署测试，以及时发现 DNSSEC 大规模部署之后密钥更新和数据加密操作中存在的故障；

3）IPv6 成为下一代互联网的基本特征，DNS 系统对于 IPv6 资源记录和过渡环境的全面支持需要进一步完善；

4）对于大数据包的支持不仅能使 DNS 平滑支持 DNSSEC 和 IPv6，也为 DNS 以后的演进奠定基础，这不仅需要协议层面的功能支撑，而且需要整个网络环境对于大数据包的传输支持；

5）DNS 已经成为互联网恶意攻击的主要对象之一，因此，在服务架构方面增强 DNS 抗高强度 DoS 攻击能力不仅是提高 DNS 权威服务体系生存性的有效方法，还能够为物联网、CDN 等需要大规模、高性能 DNS 解析支撑的新型应用

环境提供基本支持；

6）DNS 服务器本身的解析能力和网络环境的具体情况都会对客户端感受到的 DNS 解析性能造成影响，因此，优化 DNS 解析性能应配合整个网络环境的优化和升级。

6、国家域名安全联盟年度报告

2012 年 3 月 27 日，由工业和信息化部通信保障局作为指导单位，由 CNNIC 国家域名安全中心发起的“国家域名安全联盟”（以下简称联盟）在京正式成立。CNNIC 作为联盟秘书处，负责联盟日常事务的处理和协调、会议召集、突发事件处理等。本着自愿加入的原则，截至目前已有 45 家国内域名注册管理机构和域名注册服务机构加入该联盟，成为联盟的正式成员单位，并依照联盟章程享有相应的权利和义务。

自成立以来，联盟依照联盟章程面向联盟成员开展了以下几方面工作：

（一）DNS 抗攻击设备免费发放和试用活动。此项举措得到了广大联盟成员单位的积极响应和参与。截至 2012 年底，联盟已陆续为北京新网互联科技有限公司、北京新网数码信息技术有限公司、成都西维数码科技有限公司、杭州电商互联科技有限公司、厦门易名科技有限公司共计五家成员单位完成了设备发放和上线部署工作，在提高相关单位域名服务稳定性、提高抵御攻击能力方面发挥了重要作用。今后，联盟还将根据联盟成员的需求和反馈情况，继续推进此项工作。

（二）域名系统安全预警信息、安全事件分析、域名行业安全动态等方面信息的共享工作。截至 2012 年底，联盟已面向广大联盟成员累计推送《DNS 安全信息与动态报告》15 期，通报 DNS 高危漏洞 5 次，提高了联盟成员对域名系统安全事件的预防和发现能力，得到了广大联盟成员的充分认可和肯定。

（三）面向联盟成员开展域名安全监测和域名应用检测服务。今年六月，联盟向 43 家成员单位发送了《CN 域名权威服务器安全检测报告》，同时逐月提供针对性的《域名不良应用检测服务报告》。截至 2012 年底，已为联盟成员推送 5 期总计 258 份检测报告，累计检测域名 1700 万次，检出疑似不良应用域名 99 个。此项服务加强了联盟成员对自身域名系统整体运行情况以及所属域名应用情

况的整体了解和把控，得到了广大联盟成员的积极反馈。

在新的一年里，联盟将继续开展和深入以上各项工作，同时积极拓展更多的服务形式，推进各成员单位间的协作创新，为促进域名行业安全、健康、快速的发展创造更加有利的环境。

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