中国顶级域名根服务器昨出现大面积故障

网站集体“跳闸”网民担心被“钓鱼”

焦点

本报记者 **胡晓晶**

“QQ邮箱为什么打不开了？”“网上买东西买到一半怎么断了？”“网上抢火车票眼看要成了怎么‘跳闸’了？”昨天一天，从上午的QQ邮箱等“腾讯系”服务用不了，到下午的包括百度、京东、新浪等诸多站点的访问“抓瞎”，使不少网民都处于“干着急”状态。据悉，前者的问题出在“网络系统故障”，后者的问题更严重，涉及到了服务器之“根”。这让关键词“网络故障”昨天排上微博热门排行榜榜首，话题量超过164万条。

三分之二DNS瘫痪

昨天上午9时30分过后，记者一登录QQ邮箱，页面就显示“503 : HTTP Error 503”，Error 503为服务器出错的一种返回状态；而在QQ上传输文件无论是在线或离线，均显示“传输失败”。随后记者进一步了解到，QQ空间、QQ音乐、QQ秀、广点通、QQ群共享文件、企业邮箱、微云等也受到了影响。接近中午12时，腾讯官方发表声明证实服务器出现故障，并承认了是“由于网络系统故障”。直到下午1时30分过后，上述各项服务才逐步恢复。

紧接着，昨天下午3时左右开始，出现了更大面积的上网故障，包括百度、京东、腾讯、新浪等诸多站点访问均受影响。直到下午5时左右，国内访问根服务器才基本恢复正常。据多家DNS服务商透露，这是全国所有通用顶级域的根服务器出现了异常，导致国内大部分用户无法正确解析域名，对全国互联网链接造成系统性影响。据域名服务商DNSPod创始人吴洪声分析：此次故障情况非常严重，受此影响预计全国有三分之二的DNS处于瘫痪状态。

“李鬼”警察在指路

此次出现故障的是顶级域名.COM。在互联网中，供一些特定组织使用的顶级域，以其代表组织英文名称的头几个字母代表，通用顶级域名包括以.COM、.NET和.ORG结尾的常用域名等。

根服务器是管理全球互联网的主目录。全世界的根服务器只有13台，其中10台设置在美国，另外各有一台设置于英国、瑞典和日本。所有根服务器均由美国政府授权的互联网域名与号码分配机构ICANN统一管理。打比方说，就好比全球有13个交警负责在网上指路，但万一有几个交警被“李鬼”替换了，就会影响到全球的网上“问路”和“指路”，网民上网就找不到该去的正确地址。

360网站卫士测试发现，昨天下午很多网站都被解析到了同一个IP地址——65.49.2.178；而乌云-漏洞报告平台进一步指出，就是这个位于国外的IP，此前有发送垃圾邮件及其他有政治目的的黑客活动；来自金山毒霸的分析则认为，该IP位于美国北卡罗莱纳州卡里镇Dynamic Internet Technology公司，从目前看该事件极可能是黑客攻击行为。

三类人群受影响最大

在昨天的DNS事件中，受影响最大的是网购族、办公族和春运族，故障导致了电商网站无法正常访问，网上办公受影响，在春运高峰期大量用户无法通过网站订到春运车票。

至于网民最关心的对支付宝和网银账号会不会造成威胁，360监测显示，由于DNS事件会直接造成网站无法访问，大量网购和交易也同时中断，所以目前尚未发现因此被劫持IP及钓鱼事件。网银安全专家提醒，如果用户在网银支付操作到中途时遇断网，应在网络恢复后第一时间查看账户明细，如发现差错及时与商户或银行沟通。

360网站安全专家董方指出，由于根域名服务器主要分布在美国、日本和欧洲，我国对根域名几乎没有掌控权，如果根域名出现问题，将影响我国所有域名解析和网站访问。因此，国家需要建立一套完整的DNS监控系统。普通网民无法事先预警和防范，所以只能在故障发生后通过修改本地DNS解析服务器，即把自己电脑的DNS设置成“8.8.8.8”等办法来正常上网；但一旦网络恢复正常后，还是建议使用运营商提供的DNS服务器地址。

网络域名不能再只认.COM

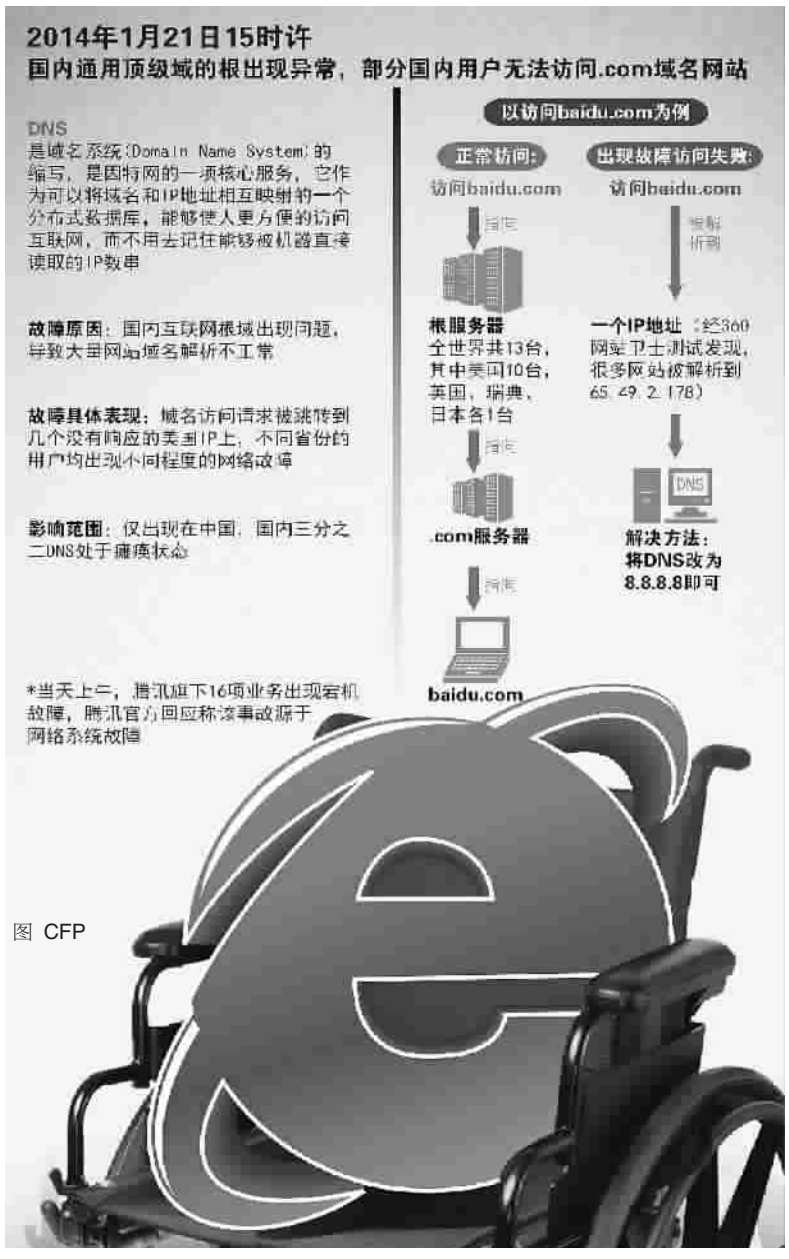

图 CFP

昨天下午，全国所有通用顶级域的根出现异常，导致部分国内网民无法访问.COM域名网站，对国内互联网造成严重影响。上海市信息化专家委员会委员、华东师范大学计算机应用研究所教授顾君忠分析指出，由于国内解析.COM域名的根服务器在美国，无论技术故障还是黑客攻击，大洋彼岸的域名解析服务器若有风吹草动，国内网络事故难免。

互联网上相互寻找，就像现实生活中一样，需要记住彼此的“门牌号”。这些网络“门牌号”由一长串枯燥的数字代码来标识，即IP地址，记起来相当困难。为此，科学家们贴心地给网络IP地址编写了一整套通俗易记的英文名字。对于普通网民来说，想要在网络上查网页、发邮件或浏览微博，只需记住并输入简单易懂的英文字母——网络域名。从网络域名到IP地址之间复杂海量的“翻译工作”，则交由网络背后一层层的域名解析服务来完成。

“由于这一整套域名解析的概念和算法由美国提出，到目前为止，域名解析的根服务器依然在大洋彼岸。”顾君忠告诉记者，这就意味着只要在网络上使用.COM域名，即使是寻找隔壁人家的网络地址，网络域名的解析数据也得先漂洋过海往返一趟美国，才能到达邻家网址。通俗一点说，只要还使用国际最广泛流行的通用域名格式.COM，“互联网之根”就一直在美国。近年来，包括中国、欧盟等国家和地区在内的互联网科学家多次提议，互联网应用已经无所不在，域名解析根服务器扎根于某一国家存在隐患，或许可以考虑迁往联合国。

其实，因域名解析服务器故障导致的大面积断网，屡见不鲜。2010年，为百度提供域名解析服务的托管商被黑客入侵，当天数小时内，网民无法正常登录网站。不管被黑客攻击劫持，还是服务器自身的技术故障，一旦域名解析服务出现问题，对网民的直接伤害首先是大面积断网，另一个大的风险则是被钓鱼网站欺诈。“这就有点像灯火通明的大楼里忽然停电两分钟，小偷很可能趁黑上门、浑水摸鱼。这对网络金融安全无疑十分危险。”

目前情况下，若要尽可能躲避类似断网，有赖于更多的网站和网民启用.CN中文域名。“因为.CN中文域名的根服务器在国内，家门口的服务器出毛病了，维护起来也便当。最起码，关键时刻不必盲目地受制于人。”顾君忠指出，淘宝、腾讯、支付宝、新浪微博等网民常用的网站和互联网应用，一般都同时注册了相应的中文域名。可能是着眼全球商业战略，推广营销时重金砸向了拖着.COM“尾巴”的网址，用户几乎都不知它们也有相应的中文域名，基本也不会主动使用。

“遭遇域名解析故障，若使用.COM域名，再具吸引力的网络应用和服务也只能‘望洋兴叹’。可喜的是，国内政府、教育机构和科研院所等网站基本都使用的是中文域名网址，未受昨天下午的网络事故影响，相应的信息安全风险也随之规避。”　本报记者 **马亚宁**

近年全国范围网络故障事件一览

2006年12月27日
台湾地震震断海底光缆

受南海海域发生强烈地震影响，多条国际海底通信光缆发生中断，造成中国大陆至台湾地区、美国、欧洲等方向的通信线路大量中断，国际港澳台互联网访问质量受到严重影响，包括雅虎等国际网站无法访问。此外，国际港澳台话音和专线业务也受到一定影响。

2009年5月19日
暴风DNS受攻击大范围断网

自21时起，江苏、河北、山西、广西、浙江等省陆续出现互联网网络故障，部分互联网用户的服务受到影响，用户网速极慢以致无法上网。工信部发布通报确认，此次故障原因是由于暴风网站的域名解析系统受到网络攻击出现故障，导致电信运营企业的递归域名解析服务器收到大量异常请求而引发拥塞。

2010年1月12日
百度域名被劫持事件

在中国内地大部分地区和美国、欧洲等地都无法以任何方式正常登录百度网站，长达8个小时，是百度成立以来最严重的服务器故障事件。原因是百度被自称是伊朗网军（Iranian Cyber Army）的黑客组织入侵，百度域名baidu.com的WHOIS传输协议被无故更改，网站的域名被更换至雅虎属下的两个域名服务器，修改时间为2010年1月11日。部分网民更发现网站页面被篡改成黑色背景以及伊朗国旗，同时显示“This site has been hacked by Iranian Cyber Army”（该网站已被伊朗网军入侵）字样以及一段阿拉伯文字，然后跳转至英文雅虎主页。

2011年2月21日
中国电信大规模网络故障

下午3时开始，部分电信用户反馈，网速一度非常缓慢，很多网页甚至无法打开。电信网络不稳定情况涉及全国许多省市，北京、上海、湖南、河南、广东、四川、甘肃、内蒙等地都出现断网现象。据不完全统计，此次断网累计时间持续近3小时，给不少网友带来诸多不便。上海电信客服人员称是由于前一天发现网络线路出现故障，电信进行了宽带维修所致。

马亚宁 整理