“百度被黑”事件分析与对策研究报告

（文/中国电子商务研究中心搜索引擎分析师 卜梓琴）

一、事件概述：

2010 年 1 月 12 日上午 6 点左右起，全球最大中文搜索引擎百度突然出现大规模无法访问，主要表现为跳转到一雅虎出错页面、伊朗网军图片，出现“天外符号”等，范围涉及四川、福建、江苏、吉林、浙江、北京、广东等国内绝大部分省市。

这次百度大面积故障长达 5 个小时，也是百度 2006 年 9 月来最大一次严重断网事故，在国内外互联网界造成了重大影响，后百度公告称域名在美注册商处遭非法篡改，正在处理。

二、事件过程：

透过百度“被黑”表象，经中国电子商务研究中心搜索引擎分析师卜梓琴全程跟踪分析，其大致攻击过程解剖如下：

1、2010 年 1 月 12 日上午约 6 点起，百度域名 DNS 服务器被劫持更换，同时主域名已经被解析到一个荷兰的 IP；

2、域名被更换后，访问百度时页面自动跳转到一租用雅虎服务器的空间；该 IP 的网站实际使用英文 yahoo 下的租用空间，因此访问百度旗下网站时，会出现英文 yahoo 的出错信息页面；

3、由于页面请求数量过于庞大导致雅虎服务器瘫痪或者流量超限，服务器瘫痪；

4、服务器瘫痪后，访问百度的网民页面自动跳转到雅虎的提示页面；

5、在超限之前，部分网民伊朗网军的黑客页面，攻击者在百度首页自称是“Iranian Cyber Army”的组织承认篡改了百度主页，并留下阿拉伯文字；

6、2010 年 1 月 12 日上午，国内大部分城市用户和海外用户只能通过未被劫持的备用域名 www.baidu.com.cn 访问；

7、2010 年 1 月 12 日上午近 10 点，百度相关人士出面表示，故障“还在查，目前原因不知”，此前均表示不知情或拒接电话；

8、2010 年 1 月 12 日上午约 11 点起，部分地区陆续恢复正常访问；

9、下午起，百度正在陆续恢复域名解析，所以也出现了各地逐渐恢复访问的情况；

10、根据解析速度，如不出意外，全世界将在 48 小时内全部恢复访问。

二、劫持过程：

域名劫持只能在特定的网络范围内进行，所以范围外的域名服务器(DNS)能还回正常 IP 地址。

对此，中国电子商务研究中心搜索引擎分析师卜梓琴认为，攻击者正是利用此点在范围内封锁正常 DNS 的 IP 地址，使用域名劫持技术，通过冒充原域名以 E-MAIL 方式修改公司的注册域名记录，或将域名转让到其他组织，通过修改注册信息后在所指定的 DNS 服务器加进该域名记录，让原域名指向另一 IP 的服务器，让多数网民无法正确访问，从而使得某些用户直接访问到了恶意用户所指定的域名地址。

其一般步骤如下：

1、获取劫持域名注册信息：首先攻击者会访问域名查询站点，通过 MAKE CHANGES 功能，输入要查询的域名以取得该域名注册信息。

2、控制该域名的 E-MAIL 帐号：此时攻击者会利用社会工程学或暴力破解学进行该 E-MAIL 密码破解，有能力的攻击者将直接对该 E-MAIL 进行入侵行为，以获取所需信息。

3、修改注册信息：当攻击者破获了 E-MAIL 后，会利用相关的 MAKE CHANGES 功能修改该域名的注册信息，包括拥有者信息、DNS 服务器信息等。

4、使用 E-MAIL 收发确认函：此时的攻击者会在信件帐号的真正拥有者之前，截获网络公司回溃的网络确认注册信息更改件，并进行回件确认，随后网络公司将再次回溃成功修改信件，此时攻击者成功劫持域名。

三、影响分析：

（一） 对百度自身影响分析

“全球最大中文搜索网站”技术形象有损，该事件或将引发进一步的攻击。百度作为中国代表性的互联网企业，却遭受多次被黑事件，且这次故障恢复时间长达 5 小时，折射出百度对安全技术投入和应急准备明显不足。

而包括国外网络军队在内的各种黑客看到百度是如此的脆弱，可能会发起对国内网络更大规模的攻击。

（二） 对其他搜索引擎影响分析

百度无法访问后，谷歌、爱问、有道、搜搜、中国雅虎等其他搜索引擎访问量都出现激增情况，而且 “百度”成谷歌今日上升最快关键词。“此消彼长”，这也从另一面说明搜索市场整体竞争剧烈。

另据权威“搜索榜”（top.toocle.com）数据监测显示，2010 年 1 月 11 日各主流搜索引擎份额分别为，百度占 55.65%，谷歌占 17.93%，搜狗、搜搜、微软 bing 和有道分别占 7.72%，7.61%、7%和 4.08%。对此，我们预计 1 月 12 日“搜索榜”份额甚至排名将出现重大变化，谷歌等其他搜索引擎的访问量与份额比例有望明显上升。

（三） 对门户网站影响分析

调查显示：目前搜索引擎给门户网站带来的流量占到 20%左右，部分甚至占到 40%，而其中百度带来的流量要占 70%，google 大于 20%。

百度无法访问后，四大门户、各大行业网站等均遭受不同程度的损失，流量受到一定影响，由于百度访问障碍时间较长，从明天的 alexa 排名来看，国内门户网站将普遍会略有所下降。

在此次百度被黑事件里，四大门户中流量较大的腾讯、新浪受到影响较少，预计流量将

下降大约在 5%左右，而搜狐和网易受到的影响可能会稍大些，预计流量将会下降 10%左右。

（四） 中小网站影响分析

中小网站由于搜索引擎依赖度较高，遭受的直接影响最大，如音乐类搜索方面，主要集中于百度（百度 MP3）、搜狗、中搜等多家综合搜索引擎带来的下载量，而百度就占到 80%左右。

此外，这次百度被黑事件将明显对数百万中小网站造成心理上的负面影响。

（五） 对网民影响分析

百度等知名互联网企业遭受域名劫持，使得普通用户上网安全更难保障，黑客极容易将木马等恶意程序植入。但同时，该事件对网民上网安意识与防范意识起到了警示作用。

（六） 对客户影响分析

百度尽管用“凤巢”替代竞价排名,但其商业模式还是点击产生付费,在这次长达5小时的被黑事件中，将会对数十万的百度企业客户造成心理上的负面影响，若在线模式被黑客入侵，将会遭受惨重的损失，甚至在被黑客连续的攻击下无法持续经营，破产关门。

（七） 对互联网业界影响分析

（1）**DNS 根服务器设置：**因为 DNS 服务是互联网的基础服务，不是个人或者小公司负责的业务，所以 DNS 被劫持再次说明国内的基础服务安全防范意识不高。除了日常做好服务器基础安全漏洞的跟进和修复外，更需提高互联网安全意识。

（2）**网络安全警钟：**从现象上看，这次百度被黑 baidu.com 这个域名在根域解析上被黑客控制（这个域名是美国管理的），不只是国内的互联网厂商需要增强防范意识，而是整个国际互联网社会同样面临着网络安全威胁。

（3）**域名争论：**百度域名遭篡改本质原因在于域名注册商系统存在漏洞，域名注册商是美国的 REGISTER.COM。律师于国富认为，百度应该起诉位于美国的国际域名管理机构。此前，另一家互联网巨头 QQ 已经将域名从国外转移到国内。这次被攻击事故发生后，百度方面是否会立即采取转移行动也成为了业界关注的焦点。

四、相关案例：

（一） 2000 年 8 月 31 日 新浪网曾“被黑”;

（二） 2006 年 9 月 12 日，百度遭黑客攻击，导致百度搜索服务在全国各地出现了近 30 分钟的故障，在对百度服务器执行“Ping”命令时发现域名丢包率达到 100%;

（三） 2008 年 12 月 2 日，中国中央电视台的官方网站 CCTV 的音乐频道被一名自称“小波”的黑客侵入并修改了页面，并留下挑衅的字语。

（四） 2009 年 8 月，Twitter 和社交网站 Facebook 分别遭遇黑客攻击，致使 Twitter 服务瘫痪，而 Facebook 也严重受创，服务速度大为减慢;

（五） 2009 年 5 月，美国网络搜索引擎巨头 Google 遭遇黑客攻击，其阿尔及利亚、波多黎各和摩洛哥、乌干达等地的域名主页均发生过被黑客劫持的情况;

五、分析师十大观点：

对此重大突发性事件，长期关注搜索引擎与网络营销的中国电子商务研究中心搜索引擎分析师卜梓琴给出以下评论与独家观点（欢迎新闻媒体与各界人士引用或讨论）：

（1）暴露了国内互联网企业安全隐患。“百度被黑”事件本身暴露了我国互联网企业诸多问题，不仅是事先安全防范意识和监控措施，还有在出现突发性故障后的应急反应机制方面，所以互联网企业需自身提高技术创新与突破，掌握核心技术；提高技术监管与防范，设置预警方案，比如技术处理方案、设置备用域名、公关关系处理方案等；

（2） 互联网域名服务器安全性未受到应有重视。此次攻击黑客利用了 DNS 记录篡改的方式。根本原因在于目前互联网域名的 DNS 管理服务器安全性未受到应有的重视。并提醒称，目前绝大多数域名都存在类似安全风险，使得 DNS 存在很多安全隐患。

（3） 搜索引擎市场竞争机制有待进一步完善。搜索引擎是互联网的一个核心节点，是网民上网不可缺少的工具。在短时间内，而百度作为中国搜索引擎的“旗舰”，被破坏后的替代品竟是谷歌，国内其他搜索引擎有道等没有扮演谷歌的角色。

（4） 互联网产业网络安全亟待进一步加强。互联网战场是未来各国必争之地，未来的“网络战争”也很有可能打响。互联网产业直接影响该国的社会和经济等诸多领域，甚至造成大面积的行业瘫痪，这影响不亚于国家基础产业和战略产业被人牵制、乃至控制。

（5） 即使企业网站安全级别很高，技术精良，但仍存在薄弱环节，需进一步调整、巩固和加强互联网结构。

（6） 从该事件引发的种种“连锁反应”，也从侧面反映了搜索引擎作为用户使用全球互联网的一“节点”的重要地位。而百度，无疑已深入中国网民的生活，与网友的生活密不可分。换句话说，互联网已经深入到每个人的工作、学习、商务、休闲的每一个环节。

（7） 因为百度庞大的用户群体、市场占有率等因素以及媒体关注度，使他具有很高的媒体关注度，若加之百度运作合理，百度极有可能成为“2010 十大网络事件”，若百度运作得到，力挽狂澜，还有可能成为网络营销的经典案例。

（8）面对当前国际政治经济局势的错综复杂，部分极端分子通过攻击一些具有全球影响力的大网站的手段来彰显自己的影响力、开展政治宣传、甚至向异己示威并进行要挟，其影响力效果，甚至可能不亚于制造一个类似 911 的事件。

（9）由于目前我国没有 DNS 根服务器（全世界 13 台 DNS 根服务器均设在美国），我国的 DNS 请求实际上由一台台镜像服务器负责处理，镜像服务器分布于世界各地，由国家专属机构负责维护。

（10）众所周知，国际互联网技术和游戏规则都是美国人制定和把控的，我们没有核心技术。与 2009 年 5 月 30 日轰动一时的“微软封杀五国 MSN 服务事件”（事件详情：http://b2b.toocle.com/zt/msn/）道理如出一辙，这次“百度事件”再次提醒并鞭策我们：落后与被动只能处处挨打，中国的互联网企业不仅需要不断提高技术创新与监管力度，还是牢牢把握互联网话语权和规则制定权，争取自主知识产权，才能加强信息安全，也才能使得我们的互联网产业是真正自主可控，也才能长期稳定、持续与健康发展的。

六、名词解释：

1、**域名劫持**：是在劫持的网络范围内拦截域名解析的请求，分析请求的域名，把审查范围以外的请求放行，否则直接返回假的 IP 地址或者什么也不做使得请求失去响应，其效果就是对特定的网址不能访问或访问的是假网址。

2、DNS：是“域名系统” (Domain Name System) 的缩写，该系统用于命名组织到域层次结构中的计算机和网络服务。在 Internet 上域名与 IP 地址之间是一对一（或者多对一）的，域名虽然便于人们记忆，但机器之间只能互相认识 IP 地址，它们之间的转换工作称为域名解析，域名解析需要由专门的域名解析服务器来完成，DNS 就是进行域名解析的服务器。

3、**根服务器**：要用来管理互联网的主目录，全世界只有 13 台。1 个为主根服务器，放置在美国。其余 12 个均为辅根服务器，其中 9 个放置在美国，欧洲 2 个，位于英国和瑞典，亚洲 1 个，位于日本。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，负责全球互联网域名根服务器、域名体系和 IP 地址等的管理。美国政府对其管理拥有很大发言权。

4、**中国电子商务研究中心**：本报告编制机构中国电子商务研究中心，是我国最早创办、也是目前唯一家以专注研究与传播电子商务、搜索引擎、网络营销、中小企业等为己任的第三方机构。通过在线平台(b2b.toocle.com)，研究中心日均发布各类行业动态稿件、分析研究文章与行业报告数百篇，每日吸引了来自全球的百余万电子商务相关用户群体访问。经三年多积累，目前已发展成为我国电子商务领域最具影响力的专业研究机构和新兴传播平台。

5、**联系分析师**：卜梓琴：互联网分析师；重点研究分析搜索引擎、网络营销、网络广告、网络推广、搜索引擎优化等互联网应用领域TEL：0571-85337326；E-mail：bzq1@netsun.com；MSN：zjyhshdf2163.com；详情访问研究中心网站：b2b.toocle.com。

6、**相关报告**：《中国互联网外资控制调查报告（2009版）出炉》
http://b2b.toocle.com/b2bimages/dcbg.pdf（全文下载地址）
“微软封杀五国MSN服务事件”解读，详情：http://b2b.toocle.com/zt/msn/

报告发布：中国电子商务研究中心

发布时间：2010年1月12日星期二