DNS解析故障的那些事儿—安全小课堂第三十二期

2016-11-04 京东安全应急响应中心

安全小课堂第三十二期

DNS就相当于邮差，他能够准确将酒店的地址对应到经纬度，方便他人顺利的找到酒店。DNS解析故障就好比邮差病了，除了他没人知道经纬度和地址的对应关系，自然也就找不到酒店。本期，我们来聊一聊DNS解析故障的那些事儿。

本期我们邀请到
河图安全的安全专家Vern
白帽子小飞侠
大家欢呼
ヽ(*°▽°*)ノ

/ 01 /

豌豆妹

什么是DNS解析故障？

小新 

对于DNS解析故障，首先得先了解什么是DNS，DNS故名思义就是域名解析系统，主要是IP地址和域名的对应关系，举个简单的例子，IP就好比一个酒店的经纬度，域名就相当于酒店地址包含国家、县市区、街道门牌号，方便别人能够找到你。DNS就相当于邮差，他能够准确将酒店的地址对应到经纬度，方便他人顺利的找到酒店。DNS解析故障就好比邮差病了，除了他没人知道经纬度和地址的对应关系，自然也就找不到酒店。

/ 02 /

豌豆妹

出现DNS解析故障的原因呢？

柴可夫斯基 

通常有以下几种原因：
1、DNS服务器本身出现问题， 比如前一段时间美国的DNS服务商DRY的DNS被DDOS的事件，就造成了美国大范围的网站无法访问；
2、DNS配置问题引发的问题，如：域名或者IP设置错误等；
3、 客户机或者服务器本地的hosts文件配置不当等。

哆啦A梦 

个人认为有以下几点：网站是否域名设置错误；网站空间是否存在问题；本地host文件存在问题；DNS投毒攻击；以及恶意DNS服务器设置等。

/ 03 /

豌豆妹

解决DNS解析故障的使用工具有哪些呢？

葫芦娃 

一般常见的工具有： nslookup、 host、 dig，还有ettercap。

/ 04 /

豌豆妹

能说说DNS解析故障的严重性么？

小丸子

正常网站无法打开严重影响网站正常运营，恶意的解析还能造成钓鱼攻击。如果本地运营商DNS没有被污染，那么只会导致用户电脑看不到啦。简而言之就是，找不着路和带错路。

/ 05 /

豌豆妹

求分享DNS解析故障的修复方法呢~

葫芦娃

本地查看host文件和本地DNS地址设置是否正常 。打开cmd输入nslookup命令行窗口中会显示出当前系统所使用的DNS服务器地址接下来输入你无法访问的站点对应的域名。例如输入www.baidu.com，假如不能访问的话，那么DNS解析应该是不能够正常进行的，我们会收到DNS request timed out，timeout was 2 seconds的提示信息。这说明我们的计算机确实出现了DNS解析故障。ipconfig查看DNS地址是否正确，还可以尝试执行ipconfig /flushdns命令清除本地缓存，windows的话在c:\windows\system32\drivers\etc里面查看host文件里的网址与IP对应是否正确。如果遇到了DNS污染遇到这种问题时，可以依次单击“开始→运行”命令，在系统运行框中执行“net stop dnscache”命令，临时关闭客户端系统DNS缓存功能，这样就能正常访问自己想要的站点内容了。

小新

1、查看是否存在解析故障。如：nslookup jd.com 如果不能正常返回jd.com的ip 或者返回的jd.com的IP异常，即说明存在故障。

2、查看DNS服务器。如：ipconfig -all 找到本地的DNS服务器，尝试更换成其它DNS服务器，如问题解决，说明是本地的DNS服务的问题，继而去排查DNS服务器是否存在问题，或者也可以尝试更改本地的host文件直接添加真实IP和域名地址，如：111.206.227.118 jd.com, 继而观察是否能够继续访问。

排查思路通常是：

1、有没有存在解析问题；

2、是不是本地客户端的问题，包括host的配置；

3、是不是DNS服务器的问题，有没有被DDOS，有没有配置出错，有没有被劫持和污染。

豌豆妹

好嘞~谢谢小伙伴们的耐心解答呢！咱们下期见~

微信公众号：jsrc_team
新浪官方微博：
京东安全应急响应中心

固定栏目

技术分享 | 安全意识 | 安全小课堂