邮件服务器被列入黑名单的解决办法

黄福[1]，何黎明[2],
1．江西铁通计费中心　江西 330002
2. 江西省政务信息网网管中心　江西 330046

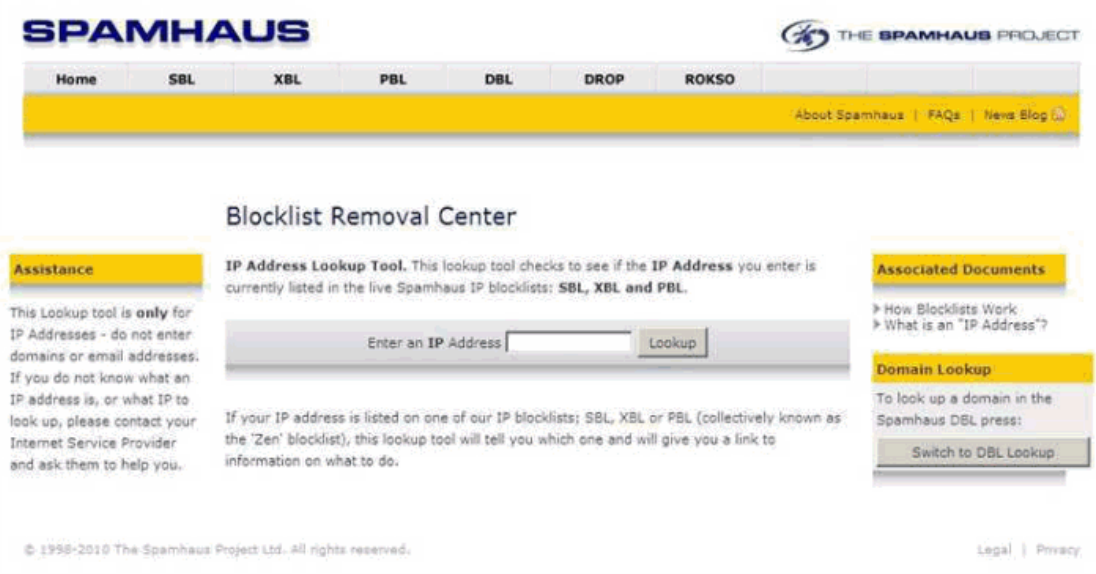
随着企业邮箱在企事业单位的广泛应用，让广大企事业单位最头疼的事情就是自己企业的邮件服务被莫名的列入黑名单，让好好的一个邮件系统不能正常使用。我们单位的邮箱也碰到过这样让人很郁闷的事情。为了能让单位的邮件服务器从黑名单中去除，让邮件系统正常工作，我在将近一个月的时间里做了大量的工作，总算让邮件服务器恢复正常了。下面我就简单介绍让邮件系统恢复正常我做了哪些工作，在这之前我认为有必要先介绍下邮件黑名单是怎么回事，这样大家对我所做的工作会有一个更好的理解。

1、什么是邮件黑名单？

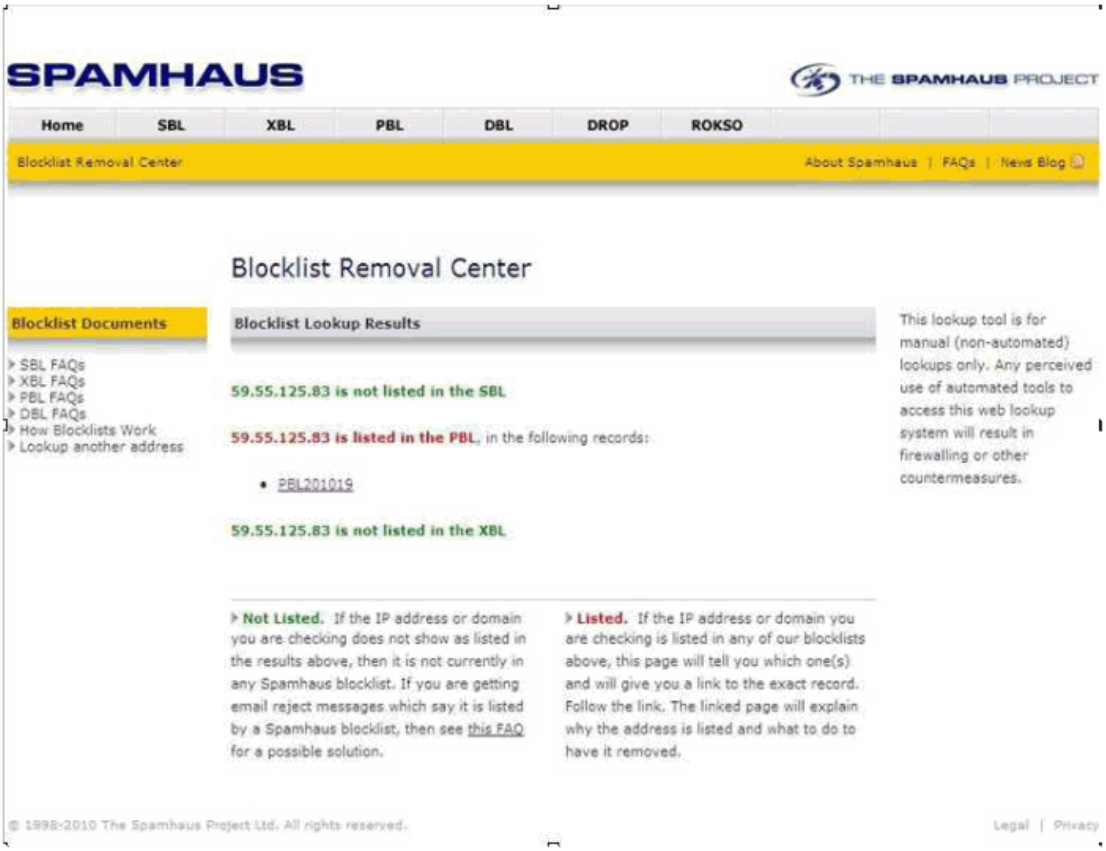
随着互联网的不断普及和扩大，在它带给人们方便的时候，也给了一些黑客从事非法活动提供了很隐蔽的方式。黑客经常利用一些木马、病毒程序从事非法活动，对企事业单位经常会造成不可想象的损失。而这些可恶的木马、病毒程序常常隐藏在邮件当中，而这些邮件我们称之为垃圾邮件。为了让垃圾邮件对人们造成的损失降到最低，人们使用了各种办法，其中一个办法就在全球建立了多个反垃圾邮件的网站，这些网站制定一些垃圾 邮件检测规则，凡是属于这些规则的邮件都属于垃圾邮件，当来自一个邮件服务器的垃圾邮件过多时，这些网站就会将这个邮件服务器列入黑名单，禁止这个邮件服务器向外发送邮件。

2、如何确定邮件服务器被列入黑名单？

通过上一段的介绍，大家应对邮件黑名单有个大致的了解，那怎么样才知道自己企业邮件服务器被列入黑名单了呢？方法很简单，当某天你发邮件时，接收方告知你没有收到你发的邮件，这时你应该立刻进入你的邮箱收件列表，这时如果你的收件列表有一封由一封来至企业邮箱服务器发给你的错误信息邮件（标题类似：failure notice），打开该邮件，正文会列出一段英文信息：Hi. This is the deliver program at x.com(邮件服武器域名)I'm afraid I wasn't able to deliver your message to the following addresses.This is a permanent error; I've given up. Sorry it didn't work out.abc@x.com(发件人的邮箱)550 #5.7.1 Your access to submit messages to this e-mail system has been rejected.--- Attachment is a copy of the message.这些英文信息表示你的服务器可能出现问题，不能将邮件投递出去。如果你邮件里真出现了上面所讲的邮件，那么恭喜你，你们企业邮件服务器十有八九被某个反垃圾网站列入了黑名单，这个时候你马下进入下面这个地址网站：http://www.spamhaus.org/lookup.lasso，出现如下图所示：



在中国大陆的邮件服务器如果被列入黑名单，一般会在这个网站上查找得到。要确认自己企业邮件服务器是否被列入了黑名单，在 Enter an IP Address 输入框内输入你邮件服务器的 IP 地址，点击 Lookup 按钮查询你的邮件服务器 IP 是否被列入了黑名单，如下图所示：



在上图显示的查询结果中，出现了**"59.55.125.83 is not listed in the SBL"** 、**"59.55.125.83 is listed in the PBL**, in the following records:PBL201019"、**"59.55.125.83 is not listed in the XBL"**三行信息。这三行信息表示我们所查

询的 IP 地址不在 SBL、XBL 黑名单列表中，而在 PBL 列表中。那么 SBL、XBL、PBL 究竟是什么呢？我们这里做个简单的介绍。

SBL(The Spamhaus Block List)：它是已经经过验证的垃圾邮件源及确有垃圾邮件发送行为的实时黑名单列表。它也是 spamhaus 最主要的项目之一，由分布在全世界 9 个国家 的,每周 7 天，每天 24 小时进行列入新记录和删除记录的工作。所以，这个列表可信度高使用人数也多。如果你被列入算是严重事件，被列入后，需要你的 ＩＳＰ（电信或是网通）的ＩＰ管理人员去和 Spamhaus 联系才有可能移除。

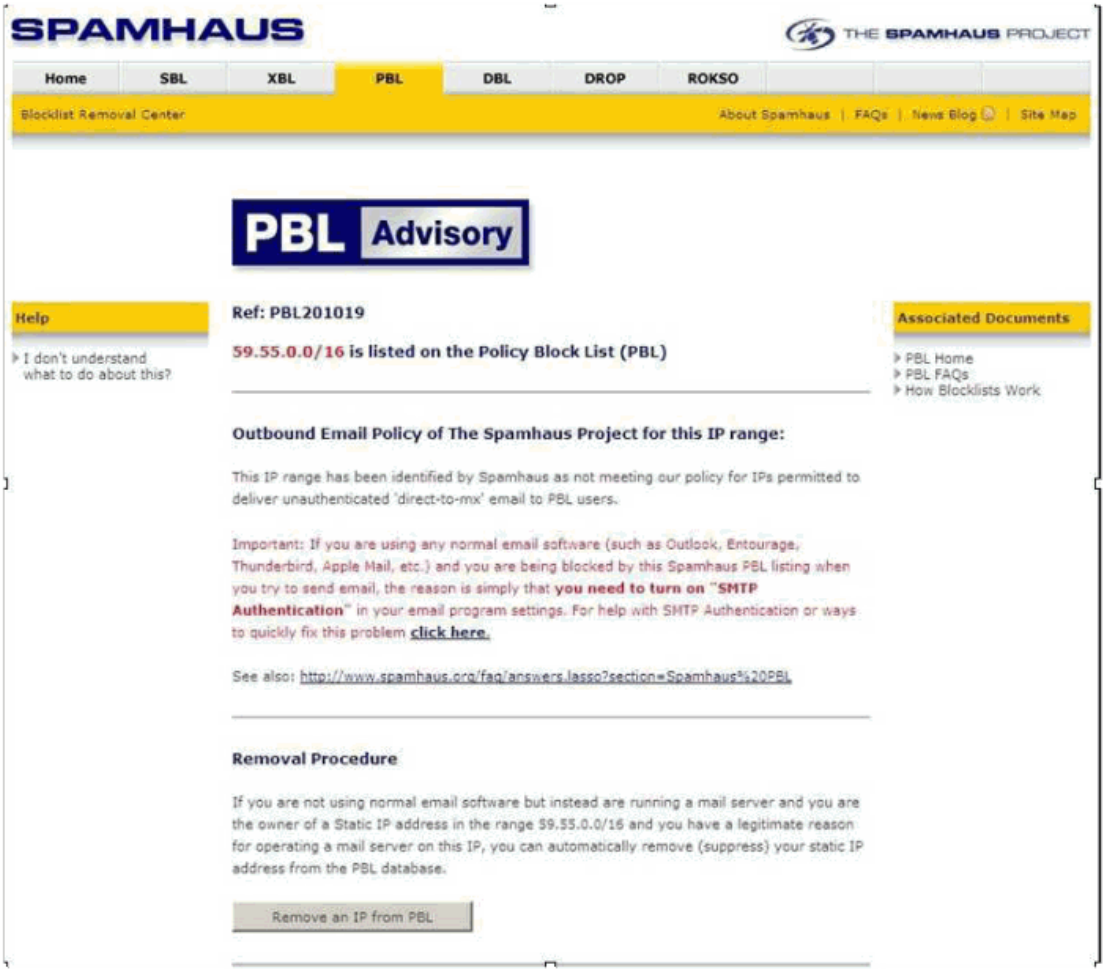
XBL(Exploits Block List)：它是针对因为安全问题被劫持（比如僵尸机）或是蠕虫/病毒，带有内置式垃圾邮件引擎和其他类型的木马来发垃圾邮机器的实时黑名单ＩＰ列表。它 的数据主要来源于两个合作组织：cbl.abuseat.org 及 www.njabl.org.因为被列入 XBL 的服务器大多为被第三方劫持利用，所以有可能导致误判断。

PBL(The Policy Block List):它主要是包含动态ＩＰ及哪些允许未经验证即可发送邮件的ＳＭＴＰ服务器的ＩＰ地址段。这一个列表最明显的特点就是提供了一个ＩＰ地址移除的自 助服务，ＩＰ它列入后，可以自己申请移除。所以就算是被 PBL 列入，影响并不大，请要使用移除功能移除即可。

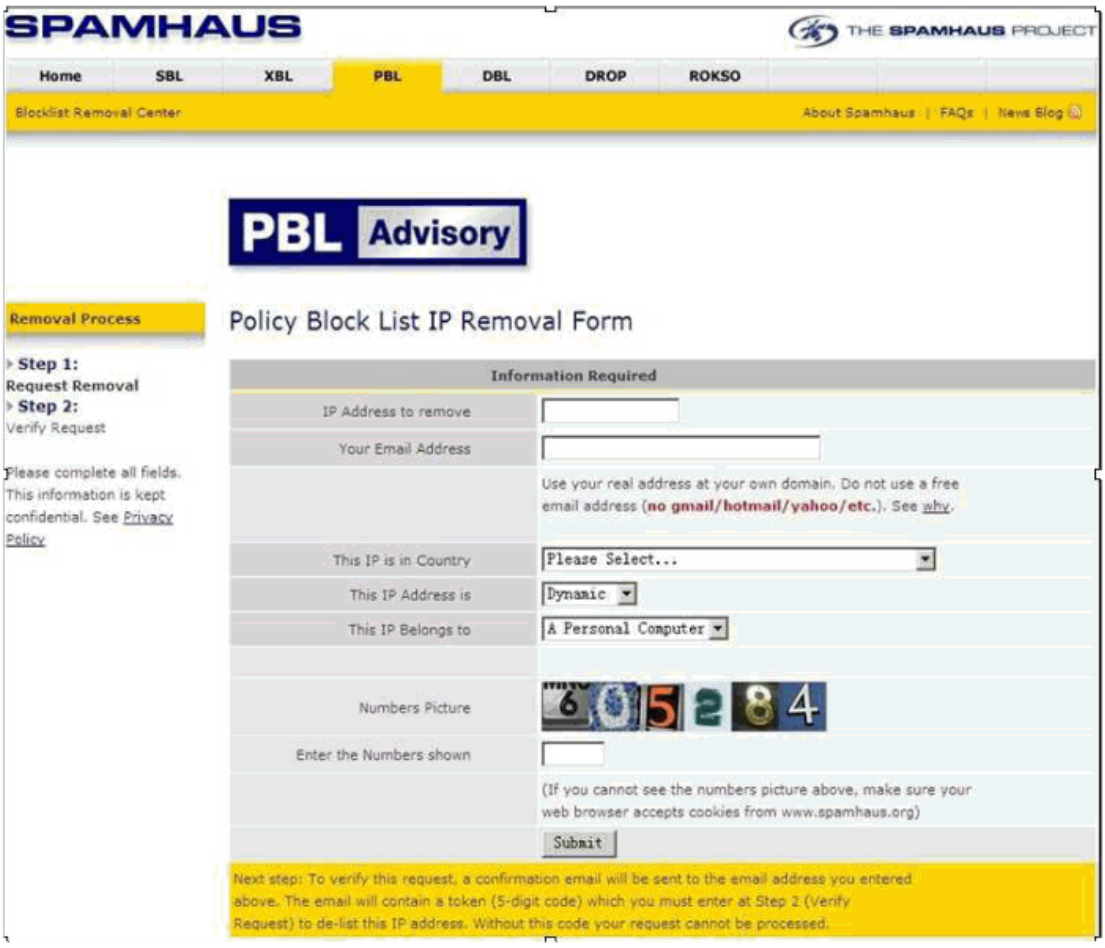
3、如何将邮件服务器从黑名单中移除？

如果你们企业邮件服务器 IP 被列入了 SBL、XBL、PBL 中任意一个说明被列入了黑名，从而导致邮件发送不出去。那么如何将企业邮件服务器从黑名单列表中移除，使邮件服务器恢复正常。下面我就以我本人的经历讲述我是如何使我们企业邮件服务器从黑名单列表中移除。

当我发现我们单位邮件服务器发送邮件，发送不去的时候，并收到邮件服务器报错邮件，我立马感觉我们邮件服务器可能被列入了黑名单，我马上进入 spamhaus 网站查询，结果发现我们邮件服务器 IP 被列入了 PBL 黑名单了。为了解除 PBL 黑名单列表，我立马点击”**59.55.125.83 is listed in the PBL**”下面”PBL201019“，进入申请移除步骤，如下图：



点击上图"Remove an IP from PBL"按钮，进入下一步，选择"I have read and I have understood this page"表示对这些协议已经清楚了，然后点击"Remove IP Address..."按钮，进入下一步,如下图：



填写上图列出的一些信息，这里要特别提醒注意的是，在“IP Address to remove”信息框内填写的是要从黑名单列表中删除的邮件服务器 IP 地址；在“Your Email Address” 的信息框内填写申报人的邮箱，该邮箱必须是该企业的一个邮箱。填写完相关信息，点击”Submit”提交，进入下一个步骤，并在“Enter your 5-digit code”中输入 5 位数字，这 5 位数字从哪获得，就是从上一步中我们填写邮箱中获得，最后点击”Finish”按钮完成申请流程。

4、总结

在我完成移除黑名单申请后一天，我们单位的企业邮箱恢复了正常。正当我以为这个问题已经解决了的时候,一个星期之后我们单位的企业邮箱又出现了发不了邮件的情况，现象和之前出现的情况一样。于是我又按前面方法再次将企业邮件服务器从黑名单中删除，可是没过多久邮件又发不出去了，就这样来来回回折腾了好几次，最后我想这不是解决办法，于是我就到网上查找了相关资料。资料上讲述如果企业邮件服务器多次被列入黑名单，很可能是企业内部有电脑中毒了，自动向外发送垃圾邮件，所以就导致企业邮件服务器反复被列入黑名单，必须找出中毒的电脑，将病毒清除干净。于是我就利用抓包软件，对单位内网发往外部的数据流进行抓包分析，对分析有问题的数据，我跟踪到电脑，并将该电脑做一个彻底清理。经过对单位电脑彻底清查，并对所有电脑做了安全加固，我再一次提交申请解除黑名单。

可是这次提交申请解除黑名单后，没过多久又出现了邮件发不出去的情况，于是我怀疑是不是单位又有哪些电脑中毒了，于是我又通过抓包分析，可是经过分析并没有发现异常数据，这让我十分郁闷，到底是怎么回事呢？为了找出原因所在，我通过找资料，请教高人，终于发现了症结所在。

这里我先简单介绍下我们单位关于邮件服务器部署的一个网络结构。我们的邮件服务器部署在防火墙内部，自己本身网卡配置的内部 IP(这里简称 IPn1)，在防火墙上配置了一个外网 IP（这里简称 IPw1）与 IPn1 对应。另外在防火墙上配置了一个出口默认外网 IP（这里简称 IPw2）,所有防火墙内部电脑和服务器（包括邮件服务器）向外发送消息都通过 IPw2，而单位外部的邮件则发送给 IPw2，再通过防火墙转发到 IPn1。

通过上面的介绍，大家可能认为这样一个网络结构应该没有什么问题，但是我们仔细看就会发现问题。邮件服务器发邮件时是通过 IPw2 出去的，而收邮件确实通过 IPw1，这就造成了一台邮件服务器拥有两个不同的外 网 IP.这就无意中造成了邮件 IP 欺骗情况，对于邮件 IP 欺骗的情况反垃圾邮件网站都会将其列入黑名单中。

在知道真正原因之后，我立马在防火墙上修改了配置，让邮件服务器收发都走 IPw1,这样就避免了形成邮件 IP 欺骗的情况。

通过上面的工作，邮件服务器再也没有出现发不出邮件的情况，至此邮件服务器被列入黑名单的问题彻底解决。

作者：黄福

简历：工程师，江西铁通计费网络系统维护。

详细通信地址：南昌市二七西街 53 号

邮编：330002

联系电话：13767102998

E-mail：huangfu0614@163.com

作者：何黎明

简历：工程师，负责江西省政务信息网骨干网的设计规划与维护。

详细通信地址：南昌市省府大院西二路 3 号江西省信息中心网络部

邮编：330046

联系电话：13807044628

E-mail：heliming@jiangxi.gov.cn