The Recognization and Methods of Prevention of SPAM

垃圾邮件（SPAM）的认识和防范方法

黎宙 （广州荔湾成人中等专业学校 430074）

摘要：本文介绍了垃圾邮件（SPAM）的由来、危害性、其形成的基本原理，并提出了具体相应的识辨、防范方法。

关键词：垃圾邮件（SPAM） UCE（unsolicited commercial email） UBE（unsolicited bulk email） 邮件地址 邮件攻击 群发 反垃圾邮件组织

1 引言

中国正日益成为新的垃圾邮件（SPAM）发源地。来自中国的垃圾邮件有两种：一种来源于中国的企业，基本都是中文邮件，内容大多是盗版软件、中文网站、电子产品的广告，第二类垃圾真正的起源并不在中国，而是在美国，只不过由于中国的一些邮件服务器安全性能较差、管理松懈，因而这些来自美国的垃圾邮件便利用中国的邮件服务器进行转发。

海外一些民间垃圾邮件监控机构--如美国的非盈利性机构"邮件滥用预防系统"（简称MAPS)以及英国的UNX都加强了针对中国的监控措施。其中UNX最近已决定将负责为本国近200家ISP提供骨干网服务的中国电信所拥有的全部IP地址列入黑名单；而MAPS定期编制的RBL垃圾邮件黑名单上目前有2800个IP地址，有5%是中国的地址，其中被列入完全阻止名单的有国内著名的ISP：163.net、263.net等。

2 垃圾邮件（SPAM）的危害

2.1 垃圾邮件对网络的破坏

2000年2月8日到10日，一伙神通广大的神秘黑客在三天时间里接连袭击了互联网上包括雅虎、美国有线新闻CNN、世界最著名的网络拍卖行eBay、风头最劲的购物网站Amazon.com等在内的五个最热门的网站，并且造成这些网站瘫痪长达数个小时，黑客使用了一种名为"拒绝服务"的入侵方式，在不同的计算机上同时用连续不断的服务器电子请求来轰炸网站，在袭击进行最高峰的时候，网站平均每秒钟要遭受一千兆字节数据的猛烈攻击，这一数据量相当于普通网站一年的数据量！面对如此猛烈的攻击，技术人员却束手无策，只能眼睁睁地看着泛滥成灾的电子邮件垃圾死死地堵住了用户们上网所需的路由器。

2.2 垃圾邮件导致封杀行为产生

早在1997年，垃圾邮件已经开始泛滥了，利用封锁IP地址的手段来制止垃圾邮件传播的方法开始盛行，那时中国互联网还不是非常发达，所以电子邮件遭遇封杀事件多是出现在网络技术先进的欧美。随着此类事件的增多，1999年一些发达国家开始制定有关的法律来限制此类事件的发生，目前美国有18个州通过了制止垃圾邮件的法律，欧洲已有16个国家通过了相关法律。而最关键的是在欧美发送垃圾邮件，特别是职业发送者，往往会受到比较严厉的法律制裁，2000年随着中国互联网的发展，垃圾邮件的传播开始出现在中国这个网络技术日益发达、但相关法律还不够健全的国家。从那时起，国际反垃圾邮件（Mail－Abuse）等组织的黑名单上就没少出现中国互联网企业的名字，新浪、网易、搜狐、163邮局、263、21cn等国内主要邮件服务商都曾上榜，从那时开始，国外的企业和组织开始了对中国电子邮件的封杀。如果断绝东西方电邮传送，对以网络为基础，正与传统经济元素有机融合迅速成长的中国新经济将造成重大打击。据统计，我国网上用户约为3370万，平均每个用户拥有E－mail账号2.2个。随着中国加入世界贸易组织，中国的对外交流活动将呈上升趋势，对外邮件也将大幅增加，如果中国电子邮件遭遇全面封杀的话，对国外企业与组织也是巨大的损失。目前，中国电子邮件将遭全面封杀事件已经引起了社会、企业和政府的广泛关注。

2.3 垃圾邮件对企业的影响

最新的的调查显示，企业收到的电子邮件中，竟有28%为垃圾邮件。英国电邮防毒企业Message Labs在调查中发现，有三分之一的企业抱怨他们收到了不想收到的电子邮件；有三分之二的企业表示他们正试图通过修改有关政策解决垃圾邮件泛滥的问题。调查报告指出，企业雇员通常每日花费10分钟的时间清理收件箱内的垃圾邮件，照这一数字计算，每日由此造成的损失可达每100位雇员4.7万英镑。Message Labs公司指出，通过调查可以看出，越来越多的企业已经开始意识到垃圾邮件会浪费企业IT资源，降低生产效率，一些企业已经采取了解决方案。垃圾邮件所费不赀：一项统计报告指出ISP业者为了对抗垃圾邮件，平均每个用户必须花费2块美金

成本。该项报告并指出垃圾邮件将影响传输速度30%以上。

3 认识垃圾邮件

3.1 什么是垃圾邮件

垃圾邮件（SPAM）也称作UCE（unsolicited commercial email）或UBE（unsolicited bulk email），顾名思义就是不请自来、有商业企图的Email，未经收件者同意，即大量散发的邮件，信件内容多半以促销商品为意图，是某些想利用Internet致富的人，藉以散播广告或色情的媒介。相同的信息，在互联网中被复制了无数遍，并且一直试图着强加给那些不乐意接受它们的人群。大部分垃圾邮件是商业广告，关乎一些可疑的产品，"迅速发财"诀窍，或准合法性质的服务。它的发送者几乎不用花什么钱---费用大都由收件人或邮递者来支付了。它们是企业相当头痛的问题。网络资源被这些毫无价值的信件，利用来分类、储存和寄发，而那些含着重大商机的E-mail却被淹没在垃圾邮件中。日积月累会造成企业财力与生产力的亏损。

电子邮件攻击主要有两种方式：一是电子邮件轰炸和电子邮件"滚雪球"，也就是通常所说的邮件炸弹，指的是用伪造的IP地址和电子邮件地址向同一信箱发送数以千计、万计甚至无穷多次的内容相同的垃圾邮件，致使受害人邮箱被"炸"，严重者可能会给电子邮件服务器操作系统带来危险，甚至瘫痪；二是电子邮件欺骗，攻击者佯称自己为系统管理员（邮件地址和系统管理员完全相同），给用户发送邮件要求用户修改口令（口令可能为指定字符串）或在貌似正常的附件中加载病毒或其他木马程序。

3.2 垃圾邮件的起源与历史

垃圾邮件是Internet技术发展的产物，与其他先进技术一样，在为人类服务的同时，不可避免的被另外一些人用作相反目的。

首次关于垃圾邮件的记录是1985年8月一封通过电子邮件发送的链锁信，一直持续到1993年，1993年6月份，在Internet上出现了名为"Make Money Fast"的电子邮件。历史上比较著名的SPAM事件是1994年4月份，Canter和Siegel的法律事务所把一封信发到6000多个新闻组，宣传获得美国国内绿卡的法律支持。这是第一次使用Spam一词来称呼垃圾邮件，用来描述新闻或电子邮件的主动性发布。同时，垃圾邮件也开始引起了人们的注意。一些触觉敏锐的商人立刻意识到了电子邮件带来的商机，许多人开始利用电子邮件作商业广告，95年5月有人写出了第一个专门的应用程序Floodgate，可以自动把邮件发给大批的人。紧接着在8月份，就有人拿两百万个邮件地址来出售。垃圾邮件越来越多与商业联系起来，并引起人们的反感。96年4月，人们开始使用UCE(Unsolicited Commercial Email)来称呼垃圾邮件，并开始积极想办法阻止垃圾邮件在Internet上泛滥。

到了96年3月，有人提出了SpamBlock的方法，例如使用REMOVE.TO.REPLY的工具来过滤邮件地址。随着过滤垃圾邮件技术的发展以及人们对发送垃圾邮件者的谴责，垃圾邮件制造者们(spammer)采取了更隐蔽的技术，比如伪造信头中的发件人，域名、邮件地址等，然而这些方法还是逃不出IP地址的过滤。于是，垃圾邮件的制造者又开始寻找更为安全的做法，97年3月，他们开始把目光转向OPEN RELAY。OPEN RELAY是当时解决Internet邮件路由的一种很好的方法，但存在可被spammer利用的安全漏洞。很快大部分商业垃圾邮件就开始利用别人的邮件服务器使用转发的办法来发送spam。这样做的另一个原因是可以盗用别人的资源，节省邮件发送者的钱。在过去的几年里，人们已经越来越多的意识到控制Internet上垃圾邮件的重要性，世界各地成立了很多组织来反垃圾邮件，MAPS，ORBS，SpamCorp，Junckemail.org等，从技术和法律上不断努力着。

3.3 判断垃圾邮件

虽然垃圾邮件可能以任何形式出现，但还是有迹可寻，以下是其特点：

- "提供天下没有白吃的午餐"，当你收到各项难以置信的中奖通知、特价优惠...等好消息时得提高警觉。通常这些发信者本身的Mail address也是造假的，也就是说当愤怒的收件者回信加以指责时，他们却可充耳不闻。
- 邮件内容的文法或错字百出。
- 频繁使用大写字体和惊叹语词。
- 他们会要求收件者来电提出停止寄件通知。但这是另一个阴谋，当你拨出电话时，你会

发现对方转换另一个方式对你实行更强力的电话行销，更糟的，这会是个高计费电话。

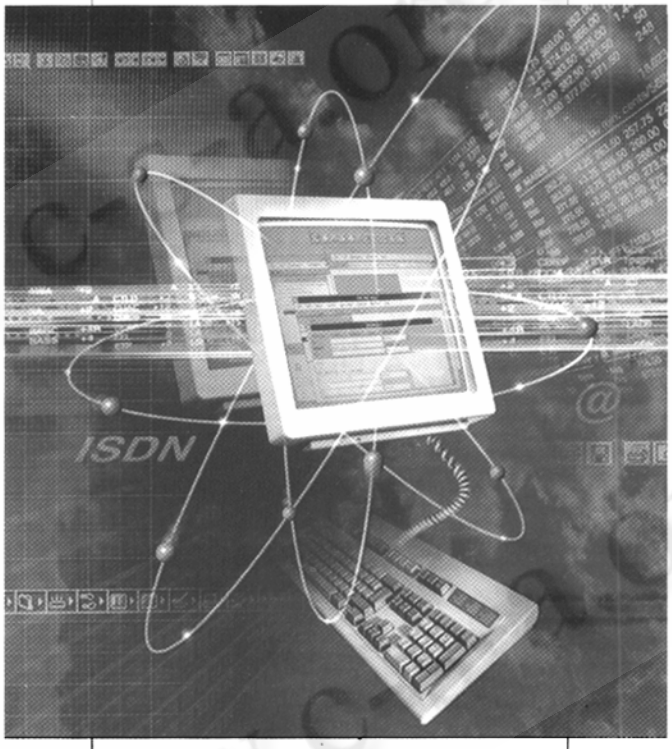
• 大部分的内容为广告或电话服务。

4 防范垃圾邮件

收发电子邮件是网友们使用频率最多的互联网应用之一，在享受电子邮件方便快捷服务的同时，还要防范垃圾邮件和邮件炸弹的侵害。

4.1 垃圾邮件取得邮件地址的方法

网站向规范的营销组织购买电子邮件地址列表，很多见钱眼开的互联网公司搜集用户的电子邮件地址，有人需要就出售给他们。因此，每次你在网站中填写表格，输入自己的邮件地址时，或者是当你在网上读完一个不错的笑话，想要转发给朋友时，你都将置身于暴露邮箱地址的危险下。取得名单的渠道相当多，比如：



• 有些程序会自动从新闻讨论区的表头基本资料取得 E-Mail

• 收集其他电子媒体订阅名单

• 使用 web-crawling 程序寻找 HTML 文件的 "mail to:" 码

• 在线 E-mail 目录

• 在线聊天室

• 购买 E-mail 名单（也许你曾经自某项调查、网络活动或电子贺卡中填过 Email，这些将成为有些人士的一项 "卖点"）

• 有许多不请自来的信件都会有 " 移除名单 " 的相关注明，但却有一些不肖者利用这个渠道来确认名单的准确性，也就是说，当你回复信件的同时，你的名单可能被放入另一个 mailing list，而这些大量的回复信件也形成另类的垃圾邮件。有一些 web-based 的组织，企图藉着 " 移除名单 " 的方式全球性收集名单。现在，有一个方法让他们的企图失效，那就是不要填写正确的 Email address。

4.2 垃圾邮件的源头

垃圾邮件一般采用了群发软件发送，发信人的地址是可以任意伪造的，查看信头可以让您找到真正的发件人，查看信头的方法是：

(1) 如果您是在 web 页面上看邮件的话，直接打开邮件，点击信件显示页面上方菜单中的 " 原文 "，就可以看到信头。

(2) 如果是用 Outlook Express 来收信的话，指向邮件，不要打开，点击鼠标右键，看信件的属性，再点击详细资料，就可以看到信头。如果有 sender 的话，sender 后面就是真正的发件人；如果没有 sender，最后一个 received from 就是发件人所用的 SMTP 服务器。

4.3 防范垃圾邮件

有效地防范垃圾邮件和邮件炸弹的方法如下：

(1) 不要把您的邮件地址在 Internet 页面上到处登记，不要随便公开你的电子邮件地址。需要注意的是最好不要在新闻组(News)、论坛(Forum)、公告板(BBS)等这些流量较高的服务尚公开您的电子邮件地址(特别是你的 ISP 的电子邮件地址，如果实在有必要公开的话建议申请免费的转信的电子邮件地址)，因为有很多的软件可以自动收集这些新闻组文章或者论坛中出现的电子邮件地址，一旦成为这些垃圾邮件清单中的一员，如果这些不怀好意的收集者用于出售这些电子邮件地址牟利的话，很不幸，您将可能源源不断地被这些垃圾邮件所追随；

(2) 不要回复垃圾邮件。这是一个诱人进一步上当的花招，很多的垃圾邮件发送者为了能够验证邮件地址是否有效，往往以一种非常抱歉地语气说，如果您不需要我们的邮件，请向某地址写信，我们将立刻停止向您发送邮件。这是，最好的方法是不理不问，直接将发送人地址加入拒收邮件发送者清单。对于许多来自提纲免费邮件列表服务的垃圾邮件，虽然已有加入列表时候的确认环节，但是很多时候我们还是遇到被某邮件列表加入，这时候我们可以向邮件列表服务商投诉，直至将你从垃圾邮件列表中清除甚至该邮件列表被服务商剔除。

(3) 发现收集或出售电子邮件地址的网站或消息，请告诉相应的主页提供商或主页管理员，将您删除，以避免邮件地址被他们利用，卖给许多商业及非法反动用户。给 Internet 服务提供商(ISP)、反垃圾邮件组织等写申诉信，如果您无法通过 Who is 查询到域名所有者的地址或者根本就得不到回复的话，您可以试验一个按照默认 " 游戏规则 "，接收投诉垃圾邮件地址投诉的信息地址：abuse@domanname.com 或者直接给 webmaster @domainname.com 写信，你可以试一试。如果在国外的服务商，该方法应该是很奏效的，一般发送者将会受到处罚甚至遭遇法律的制裁。这样呢就不必担心会再次收到来自同一来源的电子邮件垃圾了。

反垃圾邮件组织列表：

• CAUCE http://www.cauce.org/index.html

• Network Abuse Clearinghouse http://www.abuse.net/

• Forum for Responsible http://www.spamfree.org/

• Zdnet's article http://www.zdnet.com/filters/printerfriendly/0,6061,2245511-77,00.html

• Jesse Berst http://www.zdnet.com/anchordesk /story/story_3921.html

(4) 建议您用专门的邮箱进行私人通信，而用其他邮箱订阅电子杂志。应尽量分门别类地使用免费邮箱。互联网上有许多提供免费邮件服务的网站，应申请多个免费信箱，对于不同用途，譬如与亲朋好友通信、订阅电子邮件列表、杂志社投稿等，分门别类地使用不同的信箱。正如股市中的一句俗语所说的，"不要把鸡蛋放在一个篮子里"。这样可以保证在某个邮箱遭受邮件炸弹或垃圾邮件攻击时，其他邮箱仍可正常使用，降低了风险。

(5) 应尽量减少使用ISP提供的信箱，或者干脆将它"束之高阁"，因为ISP信箱的密码往往与上网帐户的密码相同，这样可以避免上网密码的泄露或ISP信箱遭受邮件炸弹的攻击带来不必要的损失。而且国内一些地方的ISP提供的免费邮箱当邮件超过一定体积时收取保管费，就曾经有人因使用Netscape内置的软件收发邮件，因其缺省选项为"在服务器保留备份"，导致一个月的保管费高达1000元；

(6) 设置垃圾邮件过滤器。如果您在web页面看到有垃圾邮件，可以点击信件显示页面上方菜单中的"拒收"，此垃圾邮件的发件人将自动进入您的拒收发件人列表中，以后凡是来自此地址的邮件将不能发送到您的信箱中。或在web页面上，进入您的邮箱后，点击左边菜单中的"垃圾邮件过滤器"或者点击"配置"中的"邮件规则"，在上面的"拒收发件人列表"中填入要拒收的发件人的Email地址，多个地址之间以逗号分隔，然后点击更新键即可，以后这些发件人所发的邮件就不能进入您的邮箱。或者点击下面"收件过滤器"中的"新建"，您可以在这里设置您需要的邮件规则，如："设置"如果邮件来源包括"--"@abc.net"，则所有邮件地址后缀为"@abc.net"的邮件都将被拒收。"如果邮件主题包括"--"法轮功"，则所有邮件标题中带有"法轮功"字样的信都将被拒收。(注意：选择哪个条件，一定要在该条件前面的小方框内打勾，此邮件规则才会生效)。

(7) 规范邮件的使用

① 认真使用邮件发送列表。只把邮件发送给真正需要这些信息的人。收到这些没有用的电子邮件的人应该写一个"礼貌的提醒"作为回复，以温和的态度让这些职业性垃圾邮件制造者知道：尽管他们得到了邮件受众的工作支持，但是他们本不需要把这个特定的邮件发给这个特定的收件人人或者收件人名单。

② 鼓励邮件发送人在发送邮件前仔细考虑到底他们要发的特定邮件有多大必要发送。

③"停止友好的攻击"，不要编写或者发送笑话，连锁信或者其他业务无关的电子邮件。

④ 最后一封电子邮件的末尾应该留下信息以示暂告一段落。例如使用"现在都解决了"、"不需要再行动支持了"，或者"不用回复了"。

⑤ 建议公司投资开发内部网络软件以促进远程团队合作和沟通。对于团队协作而言，聊天室，BBS，甚至即时信息传送都比电子邮件更加有效率。

5 写在最后

在CNNIC2001年7月发布的统计报告中，其中有一条是在一年内用户计算机被入侵的情况：47.1%被入侵过，43.0%没有被入侵过，9.9%不知道。而在2002年1月发布的统计报告中，在过去一年内用户计算机被入侵过的达到63.3%，没有被入侵过为29.9%，6.8%不知道。显然，在过去一年中，被入侵过的计算机越来越多，而这种情况意味着被入侵的服务器数量也在随之增加。CNNIC工作人员在接受采访时认为，中国网民的个人防备意识与国外相比有很大的差距，而专门从事网络管理的人员也由于知识、经验的缺乏，导致自己网络被别人攻击时还不知道的情况时有发生。

防范垃圾邮件，提高工作效率，避免损失，需要靠每个人的努力，提高意识，在使用电子邮件这一现代化技术的同时也不要给别人制造更多的垃圾邮件。

参考资料

1 http://www.sina.com.cn 2001/11/03 12:29 新浪科技。

2 http://tech.sina.com.cn 2000/08/25 新浪科技。

3 http://www.sina.com.cn 2000/02/11 02:27 半岛晨报。

4 htttp://www.dayoo.com 2002-03-11 18:03:26 大洋网。

5 http://www.sina.com.cn 2002/01/25 10:58 赛迪网。

6 http://www.sina.com.cn 2001/12/22 11:25 北京青年报。

7 http://www.sina.com.cn 2001/12/17 10:37 新浪科技。

8 http://www.sina.com.cn 2001/11/08 07:47 日经BP社。

9 http://www.sina.com.cn 2001/09/13 15:14 赛迪网。

10 http://www.sina.com.cn 2000/04/07 04:12 ChinaByte。

11 http://www.sina.com.cn 2000/02/11 02:27 半岛晨报。

12 张公忠：《现代网络技术教程》。电子工业出版社，2000.1。

13 信息管理系列编委会：《网络安全管理》。中国人民大学出版社，201.7。