**在发送端遏制垃圾邮件的一种轻量级的方法**

Wouter Willem de Vries, Giovane Cesar Moreira Moura, and Aiko Pras

特文特大学

远程信息处理及信息技术中心

电气工程学院、数学与计算机科学

通信系统设计与分析(DACS)

荷兰，恩斯赫德

w.w.devries@student.utwente.nl, {g.c.m.moura,a.pras}@utwente.nl

# 摘要

当今互联网上的电子邮件交流中，大约有90-95%被垃圾邮件占据，这是一个远远未被解决的问题。每年，因为垃圾邮件造成的损失估计高达870亿美元。打击垃圾邮件时,大多数人的关注点集中在了接收端, 而且解决方法通常要求较高的资源消耗。在本文中,我们提出一个方法来解决这些缺点。我们建议：（1）在发送端过滤传出的电子邮件（2）使用轻量级的技术来检查邮件是否为垃圾邮件。此外，在荷兰的一家托管服务提供商的帮助下，我们已经评估了这些技术中在发送端上两个不同数据集之中检测垃圾邮件的准确度。这种方法得到的结果表明，通过在发送端进行简单的检查，我们可以显著减少在互联网上垃圾邮件的数量。

# 1介绍

当今互联网上的电子邮件交流中，大约有90-95%被垃圾邮件占据[1,2]。企业不得不花费计算机和网络资源，人力工时来应对这些不请自来的电子邮件，而这将导致经济上的损失。每年，因为垃圾邮件造成的损失估计高达870亿美元[3]。

为什么会互联网上会出现这么多的垃圾邮件的原因是成本

发送一封电子邮件的成本几乎为零。据估计，传输垃圾邮件比接收它便宜10000倍[4]。此外，电子邮件协议对于电子邮件的发送没有任何的安全限制，这导致互联网上的任何一台机器都可能是一台潜在的垃圾邮件服务器。

为了打击数量庞大的垃圾邮件，接受者依靠接收端技术，如在电子邮件客户端使用自动过滤或使用邮件服务器过滤器（比如SpamAssassin等软件）。尽管在一定程度上有效，这些技术目前仍有一大缺点：就是异常的耗费资源[5]。鉴于此，很多时候，ISP（互联网服务提供商）们没有遵守非常严格的要求的话[6]，就被迫更​​多的在前期拒收电子邮件来防止过滤邮件服务器超载。反过来，这种方法可能会导致误报，导致合法的电子邮件被拒绝。因此，这样的攻击性技术可能危及电子邮件通信的可靠性并且也不能过滤所有的垃圾。

面对与发送和过滤垃圾邮件相关的这些问题，本文提出了一种新的方法来打击垃圾邮件，即专注于在发送端过滤垃圾邮件，而不是采用耗费资源的传统的解决方案。由于发送垃圾邮件是如此便宜，而在接受端检测又极度耗费资源，为什么不通过阻止垃圾邮件发送来解决问题呢？如果我们能显著抑制垃圾邮件的传输，那么收到的电子邮件的数量会大大降低。

为了检测在发送端的垃圾邮件，我们提出采用四种就CPU周期而言不耗费资源的技术。这些技术着重于根据电子邮件的核心属性，如宣传URL（advertised URL’s）检测垃圾邮件。为了评价这些技术的有效性，我们已经进行了一系列的在一家大型荷兰的托管服务提供商的生产网络上的测试。

本文的其余部分内容如下：第2节我们介绍背景和当前ISP采用的打击垃圾邮件的解决方案，以及这些解决方案各自的缺点。接着，在第3节我们提出我们的建议，利用低资源消耗技术，在发送端打击垃圾邮件。之后，在第4节，我们展示了这些技术的有效行评估。为达目的，我们所使用的数据来自于一家荷兰的托管服务提供商的真实网络。最后，在第5节，我们将提出结论以及未来的工作。

# 2背景和当前解决方案打击垃圾邮件

在本节中，我们将展示一个垃圾邮件发送者进行传播时使用的技术的研究此外，我们还将提供一个相关工作和现存的抵制垃圾邮件方案的回顾。

## 2.1背景

目前，垃圾邮件发送者轻松并且广泛的发送垃圾邮件，同时还能保持大半甚至完全的匿名性的方法主要有三种：直接发送垃圾邮件，邮件中继，和僵尸网络[8,9]。直接垃圾邮件发送者是那些使用自己的邮件服务器发送大量的垃圾邮件的人。这些人的主要特点是他们没有试图隐瞒他们的活动和身份，他们从有限的IP地址发送着大量的垃圾邮件。其中的一些人已被列入“已知垃圾邮件操作列表”（ROKSO）[10]，所以ISP可以识别并拒绝他们，有时直接垃圾邮件发送者甚至不惜采取劫持整个IP前缀的方法[11]如果他们需要连接到接收端。

另一种方法是当邮件服务器中配置允许任何用户（不管其授权与否）发送电子邮件时打开邮件中继。这可以使垃圾邮件发送者几乎匿名的发送垃圾邮件,只有配置邮件服务器的运营商能找到垃圾信息散布者的身份。举例而言,Sendmail5是一个默认配置开放的中继站[8]。许多缺乏经验的管理员都会犯这个配置错误,所以垃圾邮件发送者会积极的搜索互联网上的开放中继站。幸运的是越来越多的邮件服务器软件将默认配置改成了安全的,这个麻烦才有所改善。

最后,第三种更有效的发送垃圾邮件的方法是使用僵尸网络。僵尸网络由许多受到攻击的主机（称为僵尸电脑）[12]组成。垃圾邮件发送者会保持与中央控制服务器的连接。这些主机通常为一些感染了电脑病毒而不自知的windows终端用户[13,14] 所有。通过控制服务器，垃圾邮件发送者就可以命令这些主机发送垃圾邮件了。此方法发展迅速，它提供了一个便宜的，分布式完全匿名的方式来发送垃圾邮件。

在文献中,垃圾邮件主机根据产生的垃圾邮件数量进行分类。Pathak et al. [15] 通过建立一个开放的中继站并统计三个月时间内收集的垃圾邮件的统计数据，对垃圾邮件发送者的行为进行了研究。他们观察到有两种流行的垃圾邮件主机:大量垃圾邮件发送者(HVS)和垃圾邮件发送者(LVS)。LVS是一个包含大量的主机,每台主机发送少量垃圾邮件的集合(好比僵尸网络的僵尸电脑)。相比之下,HVS则只有少量的主机,每台主机发送大量的垃圾邮件(好比直接垃圾邮件发送者)。

## 2.2当前ISP采用的打击垃圾邮件的解决方案

ISP都对阻止垃圾邮件在他们的网络里传输越来越感兴趣，这主要是由于技术和法律方面的原因。举例来说，由于管理糟糕的网络最终会导致其身名扫地。ISP们会冒险的将整个垃圾邮件的IP范围列入黑名单，甚至使得他们无法传递客户的合法电子邮件。此外，在未来几年，由于IPv6[16]的崛起，IP黑名单作为在接收端的防御方法预计效果会更小（有更大的可能会误报）。关于法律方面的原因，一些政府已经立法要求检测，约束和处罚垃圾邮件发送者。例子包括2003年美国的CAN-SPAM法案[17]和2003年澳大利亚的SPAM法案[18]。

在实践中，ISP打击垃圾邮件时通常使用以下解决方案：

-为终端用户阻止SMTP端口;

-速率限制（例如，每小时的电子邮件的最大数量）;

-使用SpamAssassin等工具过滤发出的电子邮件。

最简单、最激进的对抗垃圾邮件的方法是为终端用户阻止SMTP端口,以及只允许连接到ISP的邮件服务器。

由于发送电子邮件时，SMTP不会强制执行安全限制，互联网上的任何计算机可以用作邮件服务器[19]。阻止来自ISP网络以外的连接使用SMTP端口25可以防止垃圾邮件进入其他邮件服务器，但不能阻止垃圾邮件进入ISP自己的邮件服务器。这种方法的缺点是，它严重地限制了终端用户出于不同的目的使用不同的邮件服务器的行为。

另一种方法则是坚持限制一个客户端每小时可以发送和接收的电子邮件的最大数量。这个方法非常基础而且对LVS并不有效，因为每个LVS在很长一个时段只发送少量的电子邮件 [20]。此外，合法的电子邮件活动（比如通讯）也将触发这种措施。

ISP最常用的方法是使用SpamAssassin等电子邮件过滤器来过滤传入的电子邮件。 SpamAssassin在消息报头和内容进行了一系列的测试来判断其是否为垃圾邮件[21]。它采用Bayesian过滤，DNS黑名单检查，以及其他的技术。这种方法的主要缺点是就CPU周期而言非常损耗资源[22]。此外，它通常用于接收端，因此不能过滤发出的邮件消息。

总之，现有的解决方案的主要缺点是：（1）对终端用户而言非常莽撞，（2）以现代垃圾邮件处理方法而言效率低下（3）价格昂贵。为了填补这一领域空白，在这项研究中，我们将提出了一个轻量级的方法来过滤传出的电子邮件。

# 3建议的解决方案

找出现有解决方案的缺点后，我们现在提出我们提案，我们的方案有两大支柱：（1）在发送端过滤发出的邮件（2）使用轻量级技术检查邮件是否为垃圾邮件。主要优点是我们可以以低成本在垃圾邮件抵达目标服务器之前对其进行检测和阻止。

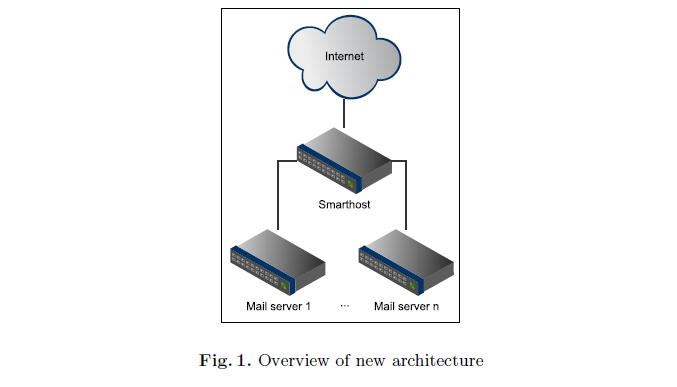


图1表示了我们的解决方案的架构。在此图中，一个ISP有一定数量的负责处理该电子邮件交流的邮件服务器。当他们收到来自客户的电子邮件时，不是直接发送其他邮件服务器，而是转发给同一网络中的另一台主机（图中的智能主机（Smarthost））。智能主机负责鉴别发出的邮件是否为垃圾邮件，并将垃圾邮件过滤掉。

为了实现这种电子邮件信息的分类，我们建议使用轻量级技术。我们的想法是在对每一条消息进行快速的检查的同时仍然能有良好的过滤效果。为达目的，我们提出了基于电子邮件核心属性的过滤方法，这种方法就CPU周期而言要求资源很少。核心属性通常是电子邮件内不能被轻易修改的元素，比如宣传URL。这些元素可以用于制定判断标准，同时确保该标准对服务器资源[22]是轻量级的。例如，可以在DNS查询的同时检查一个宣传URL是否为垃圾邮件所用，这几乎不占用服务器的处理能力。

在本文中，我们提出以下技术来分类一封电子邮件：

- 发件人策略框架检查（SPF）：ISP的邮件服务器应仅从由ISP实际掌控托管域发送电子邮件。如果收到一封要通过ISP的邮件服务器，却不是从ISP实际掌控托管域发送的电子邮件，这封邮件就应当被自动舍弃。为了执行这项验证程​​序，过滤器需要检查包含ISP掌控的托管域的DNS文本文件。

- URL黑名单检查：智能主机应对照实时黑名单检查电子邮件的URL。这些黑名单包含垃圾邮件发送者在活动时使用的URL。这些黑名单的实例包括：URIBL, SURBL, DayOld Bread, Spamhaus,Outblaze,以及AbuseButler。这样做的主要优点是，通过一次DNS查询，过滤器就可以确定宣传URL是否被用于垃圾邮件。

- 谷歌安全浏览（GSB）[23]：除了黑名单列表提供的URL，过滤器还应检查不符合谷歌安全浏览服务的网址。该服务允许我们通过谷歌自己的恶意主机列表检查实际的宣传URL。

- 全来源地址检查：对每一个消息，过滤器应检查来源地址字段，以验证它是否存在。通过连接到的MX域名记录并发出SMTP的RCPT TO命令（对于该命令，邮件服务器将回复一段SMTP 250或550码[19]，从而揭示地址是否存在），这项检查可以被迅速执行。然而，由于这种发送者标注可能会被滥用[24]，我们建议只在前两个检查表明电子邮件有问题时执行此检查。这样，这个检查将只在服务器所有者的过滤器上执行。包含非有效地址的消息将被丢弃。

我们的智能主机采用的这四种技术对CPU方面的要求很低，特别是与bayesian技术相比。我们的想法是组合使用这些技术以获得更好的分类效果，从而使我们有一个可伸缩的邮件过滤器。在下一节中，我们将对提出的技术的有效性做一个检测。

# 4评价过滤技术的准确度

为了获得对所提出的过滤器有效性的了解，我们在一家荷兰大型托管服务提供商的基础架构中进行分析。由于隐私问题，我们无法提供概念验证的实现测试，因为这意味着要检查用户的传出的电子邮件（要求预授权）。为了克服这个问题，我们在现实生活中的电子邮件服务器进行了两个不同的测试来验证我们提出的技术的有效性。

这些测试是在两个不同的数据集进行的：

- 数据集A - SpamAssassin的日志文件：这些日志是通过分析邮件服务器接收到的邮件得到的。我们共汇总了一周的日志文件。

- 数据集B - 从美国在线（AOL）接收到的电子邮件反馈报告（EOR）：AOL提供给ISP们使使其了解正在他们的网络中传递的垃圾邮件的服务[25]。对于每一个被鉴定为垃圾邮件的AOL用户。AOL将会发送一封EOR到其始发ISP处。报告将包含垃圾邮件的报头和内容。我们汇总一个月的这些报告，这意味着我们有一组发送端的垃圾邮件来分析。该组仅包​​含324 EFR报告;但应该注意到的是，这些报告构成了实际上大多数的垃圾邮件。

在接下来的小节，我们将提出各技术获得的成果。

## 4.1 SPF检测垃圾邮件的精度

发件人策略框架检查（SPF）已在AOL EFR数据集上被执行。对于每一个接收到的报告，我们提取了垃圾邮件来源地址的域部分，然后我们检查该域名是否包含在指向托管服务提供商的邮件服务器的SPF记录中。如果该域没有SPF记录或SPF记录允许任何邮件服务器发送电子邮件，我们就使用建议的回退机制;我们解决了一份www.domain.tld的记录，并检查了该IP地址是否由托管服务提供商掌控。

表1给出了发件人策略框架的准确性检验结果：正如人们所看到的，在报告期内，我们收到了324封AOL EFR报告。其中，有125封可以被安装了SPF的电子邮件服务器避免。这使我们有38.6％的准确度。但是，我们应该强调的是，这并不意味着该方法并不好。这仅仅意味着这些垃圾邮件的38.6％是由非授权域发送的。为了达到更好的结果，该技术应与本文所提到的全部四种技术结合使用。

**表1 2009年12月从EOR中提取的结果**

|  |  |  |  |
| --- | --- | --- | --- |
| **AOL EFR 报告** | **SPF拦截** | **来源地址拦截** | **GSB拦截** |
| 324 | 125 (38.6%) | 324 (100%) | 165 (50.9%) |

## 4.2黑名单检测垃圾邮件的准确性

为了评估URL黑名单检查的准确性，我们使用的数据集A（SpamAssassin接收电子邮件的日志文件）。有了这个记录，我们可以通过比较接受到的垃圾邮件的总数（使用SpamAssassin的几种技术获得）以及仅仅由于实时黑名单而别判别为垃圾邮件的数量，来简单地得到黑名单检测垃圾邮件的准确性。尽管我们只是在接收邮件集里进行了这个实验，但可以预期的是，在发出邮件集中也可以得到类似的结果。，因为这种方法是独立于邮件源/目的服务器的。

通过表2中可以看到测试黑名单检测垃圾邮件分类的准确性得到的结果。例如，SpamAssassin在1月8日（原文为5日，当为疏误）共将7016封电子邮件归为垃圾邮件。其中有5164（原文为51664，按表修正）封邮件仅使用黑名单就可以判别。说明使用该技术具有73.6%的准确性。

从我们连续8天收集到的数据分析结果，我们可以观察到仅采用实时黑名单可以将36053封电子邮件归类为垃圾邮件。根据这个结果，该方法总体准确度达到了74.4％。即使它并不像我们预期的那样高，但通过与之后的技术相结合，这个数字还可以继续上升。

**表2 2010年1月从连续8天的SpamAssassin日志提取的结果**

|  |  |  |  |
| --- | --- | --- | --- |
| **日期** | **垃圾邮件** | **黑名单拦截** | **准确性** |
| 2010/1/2 | 5149 | 3703. | 71.9% |
| 2010/1/3 | 5493 | 4291 | 78.1% |
| 2010/1/4 | 5132 | 3991 | 77.8% |
| 2010/1/5 | 6601 | 4934 | 74.7% |
| 2010/1/6 | 6600 | 4953 | 75.0% |
| 2010/1/7 | 7125 | 5110 | 71.7% |
| 2010/1/8 | 7016 | 5164 | 73.6% |
| 2010/1/9 | 5331 | 3907 | 73.3 |
| 总数 | 48447 | 36053 | 74.4% |

## 4.3通过检查全部来源地址检测垃圾邮件的准确性

检查全部来源地址的测试在数据集B（AOL EFR）上进行。

对于每一封接收到的报告，我们通过连接到的MX来源地址域名记录并发出SMTP的RCPT TO命令。对于该命令，邮件服务器会回复SMTP 250或550代码，从而揭示该地址是否存在。拦截命中则由不存在的来源地址构成。

表1给出了来源地址法的准确性。可以看到，被AOL报告的全部324封电子邮件消息均被检测为假邮件地址。这一结果好于预期。我们猜测这些地址可能是由僵尸电脑在传播垃圾邮件时随机产生的。这些结果表明，这项技术足够处理来自AOL的EFR报告。

## 4.4 GSB黑名单检测垃圾邮件的准确性

为了测试GSB检测垃圾邮件的准确性，我们采用数据B. 对于每一封接收到的报告，我们使用GSB检测器宣传URL。由于报告是手工处理的，以及垃圾邮件发送时间与收到EFR报告存在时间间隔，垃圾邮件传播与我们手工处理EFR之间会有大约24-48小时的间隔。尽管如此，我们可以看到使用GSB检测垃圾邮件仍有50.9％的准确性，如表1所示。

## 4.5所有技术结合使用的整体准确性

为了获得更好的垃圾邮件分类效果，上文中提到的四种技术可以以某种方式结合起来。但在本次研究中我们并未能够实现。因为我们的数据集来自于不同的数据源（数据集A来自于分析发送端的邮件。数据集B来自于分析接收端的邮件）。

但是，在部署我们的技术是，应该将四种技术都用于分析发送端发出的邮件一边它们能够被结合使用。然而，如何将它们最有效的结合起来还亟待实验性的测试，这也是我们未来的工作。尽管如此，我们仍然希望将这些技术结合起来能有更好的结果。

# 5结论和未来的工作

在本文中，我们提出了一个新的解决方案，使互联网服务供应商和托管商得以较低的成本显著抑制垃圾邮件在其网络内传输。我们的建议主要基于两点：（1）在发送端过滤传出的电子邮件（2）使用轻量级的技术来检查邮件是否为垃圾邮件。主要优点是，我们可以以较低的成本检测并阻止垃圾邮件达到目标服务器。此外，该解决方案只需要进行一些修改，就可以简单地给互联网服务供应商和托管商部署。

基于一家荷兰大型托管服务提供商的基础架构内的分析，我们对提出的四种不同的过滤技术的准确性作出了评价。其中表现最好的两种技术分别达到了74.4％和100％的准确性。尽管这些结果是在相对较小的数据集内获得的，但它们仍是非常鼓舞人心：

例如，仅仅通过检查黑名单，我们就可能减少70%甚至更多的发送端垃圾邮件的产生。如果互联网服务供应商和托管服务提供商开始使用这样的方法（由于法律，信誉等原因），我们就可以在无形之中从源头减少大部分垃圾邮件的产生

通过这种方法，我们可以减少处理垃圾邮件的人力、硬件、网络资源消耗，因为大多数垃圾邮件都不会传输到其它网络。

至于今后的工作，我们打算实现和部署一个原型来测试方法的实时性能和有效性。此外，我们打算在一个更大的数据集进行这种分析，并确定使用这四种技术检测垃圾邮件最合适的方案。

接下来，我们将比较四种技术结合配置与更传统的方法，如纯粹使用SpamAssassin的检出率。我们打​​算通过在同一组包含垃圾邮件和垃圾消息的数据集上同时部署两种方案来实现比较。最后，我们将监测和分析系统资源的使用情况。

# 参考文献

1. Sophos. 28封合法电子邮件中仅有一封…… (June 2008),

http://www.sophos.com/pressoffice/news/articles/2008/07/dirtydozjul08.html

2. Spamhaus. 有效地垃圾邮件过滤法 (January 2010),

http://www.spamhaus.org/effective\_filtering.html

3. Soma, J., Singer, P., Hurd, J.: SPAM Still Pays: CAN-SPAM的失败

Act of 2003 and Proposed Legal Solutions. Harv. J. on Legis. 45, 165–619 (2008)

4. Lieb, R.: 让垃圾邮件发送者在你行动之前付出代价(July 2002),

http://www.clickz.com/1432751

5. McGregor, C.: 使用SpamAssassin控制垃圾邮件

Linux J. 153, 9 (2007)

6. Mori, T., Esquivel, H., Akella, A., Mao, Z.M., Xie, Y., Yu, F.: 预验收垃圾邮件检测的有效性

University of Wisconsin Madison, Tech. Report

TR1650 (2009)

7. de Vries, W.W.:对不请自来的大量电子邮件的传输限制

In: Proceedings of the twelth Twente Student Conference on Information Technology (2010)

8. Stern, H.: 现代垃圾邮件工具的总结.

In: Proc. of the fifth conf. on email and

anti-spam (2008)

9. Sperotto, A., Vliek, G., Sadre, R., Pras, A.: 在网络层杜绝垃圾邮件.

In: Oliver, M., Sallent, S. (eds.) EUNICE 2009. LNCS, vol. 5733, pp. 208–216.Springer, Heidelberg (2009)

10. Spamhaus. 著名的垃圾邮件操作记录(January 2010),

<http://www.spamhaus.org/rokso/>

11. Ballani, H., Francis, P., Zhang, X.: 前缀劫持和截获的研究

in the Internet. ACM SIGCOMM Computer Communication Review 37(4), 276

(2007)

12. Fabian, M.A.R.J.Z., Terzis, M.A.:我的僵尸网络比你（甚至你们）的更大: 为什么规模估计仍充满挑战.

In: Proceedings of the 1st USENIX Workshop on Hot Topics in Understanding Botnets, Cambridge, USA (2007)

13. Chiang, K., Lloyd, L.:一个关于rustock rootkit和spam bot的研究案 In: The First Workshop in Understanding Botnets (2007)

14. Mendyk-Krajewska, T., Mazur, Z.: 软件漏洞及网络安全的问题。

In: Internet-Technical Development and Applications, p. 233 (2009)

15. Pathak, A., Hu, Y.C., Mao, Z.M.: 从一个独特的有利位置偷看垃圾邮件发送者的行为。

In: LEET 2008: Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats, pp. 1–9. USENIX Association, Berkeley (2008)

16. RIPE Labs. IPV6时代的垃圾邮件 (March 2010),

http://labs.ripe.net/content/spam-over-ipv6

17. United States of America. 2003年Can-spam法案(2003),

http://uscode.house.gov/download/pls/15C103.txt

18. Australasian Legal Information Institute. 澳大利亚2003SPAM法案 (2003),

http://www.austlii.edu.au/au/legis/cth/consol\_act/sa200366/

19. Klensin, J.: 简单邮件传输协议 (April 2001),

http://www.ietf.org/rfc/rfc2821.txt

20. Pathak, A., Qian, F., Hu, Y.C., Mao, Z.M., Ranjan, S.: 僵尸网络的垃圾邮件活动还将长久持续：证据，影响和分析。

In: Proceedings of the eleventh international joint conference on Measurement and modeling of computer systems, pp. 13–24. ACM, New York (2009)

21. OBrien, C., Vogel, C.: 比较CBDF电子邮件过滤及SpamAssassin。In: Proceedings of the 7th Annual CLUK Research Colloquium (2004)

22. Pras, A., Wanrooij, W.: 隔绝来自坏邻居的垃圾邮件

International Journal of Network Management (2009)

23. Google. 谷歌安全浏览 (January 2010),

http://code.google.com/apis/safebrowsing/

24. UCEProtect. 发件人标注 – 它为何被滥用(January 2010),

http://www.backscatterer.org/?target=sendercallouts

25. AOL.给互联网服务提供商们的电子邮件反馈报告(January 2010),

http://postmaster.aol.com/cgi-bin/fbl.pl