

# 外发垃圾邮件阻断策略研究<sup>①</sup>

吴翔毅

(华侨大学信息化建设与管理处, 福建泉州, 362000)

**摘要** 为了解决电子邮箱被盗用于外发垃圾邮件, 电子邮件服务器IP被列入实时黑名单列表, 严重影响电子邮件正常通信的问题, 本文提出了一系列阻断外发垃圾邮件的策略, 包括事前预防、检测, 事中及时识别、阻断和事后安全审计的三级防控策略。实践结果表明, 采用该方案能及时发现、阻断用户外发垃圾邮件, 将外发垃圾邮件行为扼杀在萌芽状态, 避免被列入实时黑名单列表, 保障邮件系统访问流畅。

**关键词** RBL; 垃圾邮件; 阻断策略; 管理

## Strategy to Block Sending Spam

Wu Xiangyi

(Department of Information Construction and Management, Huaqiao University, Quanzhou, Fujian, 362021, China)

**Abstract** In order to solve the problem of sending spam, the e-mail server IP is listed in the real-time blacklist, which seriously affects the normal communication of e-mail. This paper proposes a series of strategies to block sending spam, including pre-detection, prevention, timely identification, blocking and post-event safety audit. The practice results show that the use of this scheme can timely detect and block sending spam, nip the spam behavior in the bud, avoid being included in the real-time blacklist, and ensure smooth access to the mail system.

**Keywords** RBL; Spam; Blocking Strategy; Management

### 1 引言

电子邮件系统作为我国很多高校师生生活、学习、教学和科研创新发展的重要工具之

一, 常常被外部攻击者非法利用, 通过邮件系统漏洞、“钓鱼”邮件、暴力破解等手段攻击, 进行邮箱盗号, 对外发送垃圾邮件。

因外发垃圾邮件, 我国高校的电子邮件服

<sup>①</sup>本文系福建省中青年教師科研項目“自建成郵件系統外發垃圾郵件阻斷策略研究與實現”(項目編號: JAT200002)的研究成果之一。

务器 IP 被反垃圾邮件组织列入 RBL (Real-time Black List, 实时黑名单列表) 的事件时有发生。不少高校邮箱向海外邮箱发送邮件被拒收, 很大一方面的原因是被列入了 RBL<sup>[1]</sup>。高校邮箱外发的垃圾邮件主要是外部攻击者发送的。

本文提出了一系列的管理策略和技术手段, 贯彻“三分技术、七分管理”的方针, 将外发垃圾邮件行为扼杀在萌芽状态, 避免被列入 RBL, 保障邮件系统访问流畅。

## 2 邮箱信息盗用手段

邮箱地址可从多种渠道获得<sup>[2,3,4]</sup>, 如直接购买、机器自动采集、客户资源、邮件订阅、会员注册、暴力枚举等方式, 邮箱密码窃取的途径有网络通信监听、“钓鱼”网站诈骗、撞库、字典猜解、暴力破解、社会工程学分析、密码心理学破解甚至植入计算机病毒、木马、间谍软件, 屏幕记录、键盘监控等。

## 3 邮箱被盗带来的问题

盗用者除了利用被盗邮箱对外发送垃圾邮件、“钓鱼”邮件, 更恶劣的会利用通讯录及邮箱内往来邮件, 骗取同事、朋友等熟人信任, 发送欺诈邮件, 造成经济损失或个人隐私泄漏。

盗用者利用被盗邮箱多批次, 频繁发送垃圾邮件, 会导致邮件服务器发信 IP 地址被列入 RBL, 从而导致全域邮箱用户外发邮件被拒, 影响全域用户的正常使用。

邮箱被盗还可能导致其他信息系统被入侵, 一旦被入侵可能会导致其他信息系统个人数据丢失。

## 4 高校邮箱安全管理难点

对大部分国内高校而言, 往往开设了教职工邮箱、公务邮箱、学生邮箱、校友邮箱等,

邮箱大多在师生入校时批量创建, 密码往往与学工号、证件号码相关, 用户数量大, 不活跃用户多, 弱密码用户持久存在, 极易被盗, 且不易被发现。与此同时, 教育行业面临严重的盗号威胁, 而在邮箱系统盗号问题上, 暴力破解是目前的突出难题。教育行业成为攻击者暴力破解攻击的主要攻击目标<sup>[5]</sup>。不少师生安全意识薄弱, 警惕性不高, 在针对性“钓鱼”作案上, 容易上当提交邮箱和密码等个人信息, 账号被盗问题严重, 排查效率低。

## 5 阻断策略

根据高校邮件系统运维中遇到的常见问题, 提出以下管理和技术策略。

### 5.1 事前预防策略

#### (1) 密码策略

强制使用强密码。本研究所用的电子邮件系统允许强制使用强密码, 禁止弱口令用户进行 Web 登录, 若需使用客户端收发邮件, 建议启用客户端专用密码, 系统可生成一个或多个高强度密码专用于邮件客户端 (例如 Outlook、Foxmail、各类邮箱 App 等) 的登录。

批量开设师生邮箱时采用随机强密码。很多高校每年都要为新职工、学生开设邮箱, 密码往往采用特定的字母加证件号码或学号某几位之类的有规律的密码, 若个人信息泄露了, 密码也就容易被窃取。可编写脚本从统一身份认证系统同步信息, 使用随机密码开设邮箱。用户首次使用时通过手机短信找回密码。

启用二次登录双因素认证。在高校中全面实施双因素认证, 有一定的难度, 可配合信任登录, 由使用者从已登录过的设备中选择信任的设备, 从信任设备上登录可免除二次登录验证, 但仅限于 Web 端, 本研究所使用的生产

系统，无法在客户端上使用二次登录验证，当启用双因素认证时，客户端需使用随机生成的复杂密码。启用双因素认证可极大解决密码被盗问题，但使用客户端收发邮件，对于木马监听、通讯传输链路上监听明文密码等方式依然无能为力。

(2) 最小权限策略

将最小权限原则应用于邮箱日常管理。默认关闭自动转发、客户端通信功能，调低收件人数量。邮箱按组分类，根据需要赋予不同的单封邮件收件人数阈值、每日发送邮件总量阈值、自动转发、邮箱客户端收发信功能等。根据使用活跃度再设正常、禁止外发邮件、禁用等策略，考虑到部分用户合理的群发需求，设置群发组，给予较大的收件人数、调高检测阈值，加强审计。

也可以考虑正常邮件通道和群发邮件通道分开，若群发邮件导致 IP 进入 RBL，可不影响正常通道的邮件外发。

(3) 通信策略

针对网络通信链路上的监听、流量镜像、安全检测等行为，启用 HTTPS、SMTPS、POP3S、IMAPS，HTTP 自动跳转 HTTPS，限制 SMTP，禁用 POP3、IMAP，对通信内容进行加密传输。数据经过加密后，通过监听仍然可以得到传送的信息，但显示的是经过加密后的乱码。

(4) 日常维护策略

高度重视邮件系统安全保护工作，加强运行维护管理，落实专人负责。按照相关法律法规、政策要求，落实网络安全等级保护制度和技术防护措施，组织开展邮件系统技术检测和渗透性攻击测试，查找安全漏洞，及时升级服务器系统和邮件系统漏洞补丁，防范系统级漏洞，做好日志留存和审计，及时发现、修复存在的安全隐患。执行系统定期巡检脚本，包括弱密码账户巡检，对弱密码用户发送通知，限期修改为高强度密码。

5.2 事前检测策略

本课题项目还通过对电子邮件系统运行日志及数据库数据的挖掘，根据校外 IP 登录邮箱数、邮箱登录校外 IP 数、非常用登录地点数、校外 IP SMTP 和 Web 登录总次数、弱口令邮箱 Web 验证后是否修改密码、是否符合邮箱日常使用习惯等因素，建立了盗用邮箱模型、外发垃圾邮件发现模型，设计了一套外发垃圾邮件阻断系统。

该系统根据数据挖掘模块得到的盗用邮箱模型，定时统计 Web 访问日志和数据库中当天的 SMTP、IMAP、POP、Web 登录记录，发现盗用邮箱行为，并进行阻断和通知。

对生产系统近三年来的数据挖掘，共确认有 621 个邮箱被盗用，被盗用邮箱统计信息如表 1 所示：

表 1 被盗用邮箱统计

检测因素	数量	占比
邮箱在多个IP登录	123	19.8%
一个IP登录多个邮箱	227	36.6%
大量发送邮件	213	34.3%
没有发送邮件	331	53.3%

统计结果显示,有 53.3% 的邮箱被盗当天并没有发送邮件行为,事先禁用邮件外发,避免被盗邮箱外发垃圾邮件,避免被列入 RBL。

检测修改密码、非常用地登录、设置自动转发等行为,进行短信提醒。

### 5.3 事中识别、阻断策略

采用本课题项目所设计的外发垃圾邮件阻断系统,定时检测当天的 MTA 日志及数据库中当天的 SMTP、IMAP、POP、Web 登录记录,根据数据挖掘模块得到的外发垃圾邮件模型,发现外发垃圾邮件行为,自动禁用该用户邮箱外发邮件功能,避免继续外发垃圾邮件,发送邮件、短信通知用户和管理员。

用  $x_1$ 、 $x_2$ 、 $x_3$ 、 $x_4$ 、 $x_5$ 、 $x_6$ 、 $x_7$ 、 $x_8$  分别表示校外 IP 登录的邮箱数、邮箱登录的校外 IP 数、非常用登录地点数、校外 IP SmtP 和 Web 登录总次数、弱口令邮箱 Web 登录是否修改密码(是=0,否=1)、是否符合邮箱日常使用习惯(是=0,否=1)、邮箱发送邮件总数的平方、邮箱发送邮件主题数。 $a_1$ 、 $a_2$ 、 $a_3$ 、 $a_4$ 、 $a_5$ 、 $a_6$ 、 $a_7$ 、 $a_8$  分别表示  $x_1$ 、 $x_2$ 、 $x_3$ 、 $x_4$ 、 $x_5$ 、 $x_6$ 、 $x_7$ 、 $x_8$  的权重。

$$\text{Score} = \sum_{k=1}^n a_k x_k \quad k \in [1, 8]$$

当  $\text{Score} \geq$  外发垃圾邮件预警阈值时,若邮箱尚未禁用外发功能,则发送预警信息给系统管理员。当  $\text{Score} \geq$  外发垃圾邮件阻断阈值时,若邮箱尚未禁用外发功能,则进行阻断和通知。

### 5.4 事后审计策略

编写脚本实现事后审计,以自然日为单位进行审计,结果通过邮件发送给管理员。

审计内容包括同一主题的邮件数量、IP 登录邮箱数、邮箱登录 IP 数、邮箱发送邮件总数、IP 发送邮件总数、邮箱退信等统计数据

Top 10 信息和 Sender Score 对邮件服务器 IP 地址的评分值、是否被列入常见 RBL 名单、达预警值的邮箱等。

审计弱密码验证成功,但未修改密码的邮箱。因生产环境对 Web 登录进行弱口令检测,若是弱口令,则需修改为强密码后才能进入系统,若登录验证成功,但未修改密码,则构成异常使用,判定为入侵行为。

审计不活跃用户,对超过一年未使用的邮箱,给予禁止外发邮件的限制,在修改密码后自动恢复外发邮件功能。超过五年未使用的教职工邮箱给予禁用使用,校友邮箱数据进行备份后删除。

### 5.5 安全教育

加强宣传工作。为了提高校内师生信息安全素养,加强安全宣传、培训和演练等。

通过微信公众号推送、邮件群发、OA 系统发布安全提醒通知等多方面举措并行,为师生提供多种形式的安全科普和建议,不断强调不明邮件不轻信,不明链接和附件不点开,弱密码要避开,公私要分开。让师生掌握基本的防病毒、防“钓鱼”、防窃取的安全知识,具备分辨和处理“钓鱼”邮件、垃圾邮件的能力。用户安全素养提高可以大大降低被“钓鱼”成功的风险。

开展反“钓鱼”演练,“钓鱼”邮件演练的效果是非常显著的。根据《2021 企业邮件“钓鱼”演练分析报告》数据显示,长期坚持进行安全意识培训和有计划的模拟“钓鱼”邮件演练可以帮助各行业把人的风险因素降到最低<sup>[6]</sup>。可以视实际情况,每年开展 1 至 2 次反“钓鱼”演练。通过演练,能够检验和大幅度提高师生用户的警惕性和辨别能力,提升师生的安全防范意识。

## 6 结束语

本策略的贯彻执行,近一年来邮箱被盗数量与投入执行之前相比减少了近 90%,Sender Score 组织对本研究所用的生产系统外发邮件服务器的 IP 地址评分长期在 95 分以上,甚至因收集到的垃圾样本数量不足,达不到其评分标准,而不予以评分,极大降低了被列入 BRL 的风险。

## 参考文献

- [1] 霍跃华. 高校邮箱向海外发送邮件被拒收问题探究 [EB/OL]. <https://xdjy.cumtb.edu.cn/info/1016/1164.htm>.
- [2] 冯登国, 张敏, 李昊. 大数据安全与隐私保护 [J]. 计算机学报, 2014, 37(1).
- [3] Coremail, 奇安信. 中国企业邮箱安全性研究报告 [EB/OL]. (2022-9-8). <https://community.icoremail.net/article/599>.
- [4] 李媛. 大数据时代个人信息保护研究 [D]. 重庆: 西南政法大学, 2017.
- [5] Coremail, 中睿天下. 2022Q2企业邮箱安全态势观察 [EB/OL]. (2022-8-19). <https://www.cacter.com/news/719>.
- [6] Coremail. 2021企业钓鱼演练报告 [EB/OL]. (2022-5-6). <https://www.cacter.com/news/691>.