2024 第二季度 企业邮箱 安全性研究报告

Coremail | CACTER × 中睿天下

2024年7月出品

Coremail | CACTER 中睿天下

2024 年第二季度企业邮箱安全性研究报告

组长

林延中

主要编写人员

刘磊　江嘉杰　伍伟彬　黄楚斯

《2024 年第二季度企业邮箱安全报告》是由广东盈世计算机科技有限公司与北京中睿天下信息技术有限公司携手呈现。我们特别感谢 Coremail 邮件安全人工智能实验室和中睿天下邮件安全响应中心的专家们，他们对本报告的编写提供了专业的指导和宝贵的建议。

Coremail 邮件安全人工智能实验室（Email Security AI Lab，简称“AI 实验室”）是在 Coremail 的广泛应用场景、丰富大数据资源和顶尖科技人才的支持下成立的。AI 实验室致力于在电子邮件安全防护领域实现 AI 技术的创新应用，包括自然语言处理、计算机视觉和大语言模型等前沿技术。通过这些技术，我们旨在提升电子邮件的安全性，为企业提供更加可靠的保障。

一、2024 年 Q2 垃圾邮件概况分析

（一）国内企业邮箱垃圾邮件增长态势明显，境外源大比重加剧挑战

根据 Coremail 邮件安全人工智能实验室数据显示，2024 年第二季度，国内企业邮箱用户共收到 9.1 亿封垃圾邮件，总量无论是环比（上升 24.9%）还是同比（上升 40.6%），呈大幅度增长态势，其中接近 70%的垃圾邮件来自境外，进一步加剧了防护的难度与复杂性。

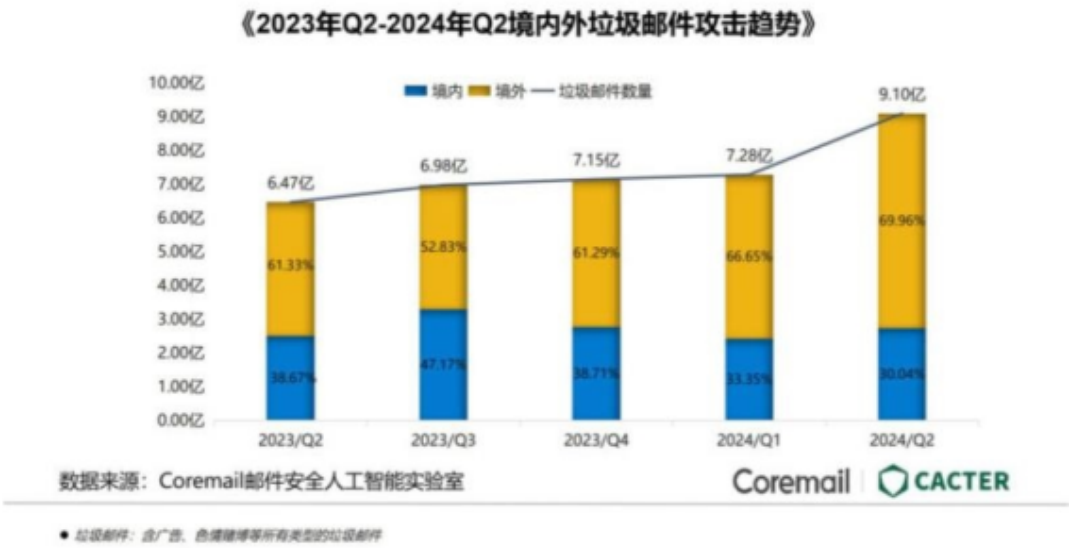

图 1 2023 Q2-2024 Q2 境内外垃圾邮件攻击趋势

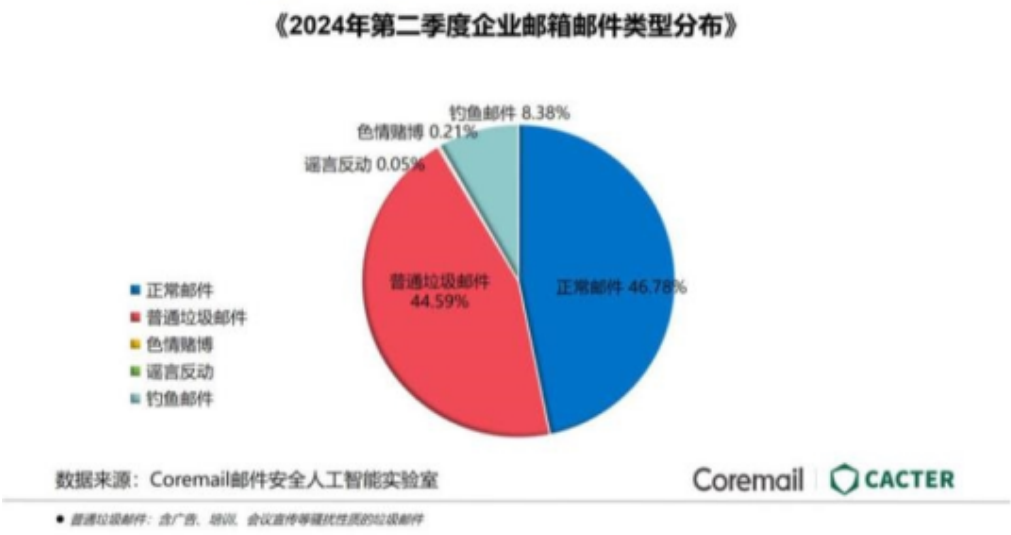

图 2 2024 年 Q2 企业邮箱邮件类型分布

在 2024 年第二季度企业邮箱用户收到的邮件构成中，正常邮件以 46.78%的占比（共

计 7.99 亿封）主导了邮件流量，然而，不容忽视的是，垃圾邮件的侵扰依然严重，其数量高达 7.62 亿封，占据了总邮件量的 44.59%。各单位组织仍需要继续加强对垃圾邮件、钓鱼邮件和诈骗邮件的防范措施。

（二）境外垃圾邮件攻击激增：美国及欧洲国家成主要威胁源

在 2024 年第二季度中，美国依旧是境外垃圾邮件的主要来源国，其次是乌克兰与马来西亚，为新的垃圾邮件攻击源，可能是境外垃圾邮件发送者，改变了攻击策略，选择了不同的邮件发送源或发件人地址，我们仍需加快提升国内网络防护能力。

图 3 2024 年第二季度全球垃圾邮件攻击源 TOP 10 国家

在国内范围内，垃圾邮件攻击也几乎无处不在，尤其在经济繁荣的区域更为突出。具体来说，北京市（约 2448.3 万封）、上海市（约 1103.3 万封）、浙江省（约 887.8 万封）和广东省（855.5 万封），属于人口密集区和经济中心，信息技术基础设施方面较为发达，为大规模的垃圾邮件攻击提供了便利条件。

图 4　2024 年 Q2 国内十大垃圾邮件攻击源头省份

（三）TOP100 垃圾邮件分析：教育行业为主要攻击目标

经 AI 实验室分析 TOP100 发送&接收垃圾邮件的域名，不难发现，教育行业仍然是垃圾邮件的主要攻击目标，接收量达 3.32 亿封。邮件是教育科研项目、教学数据、师生信息等敏感信息的承载体，教育行业的邮件安全更加不容忽视。

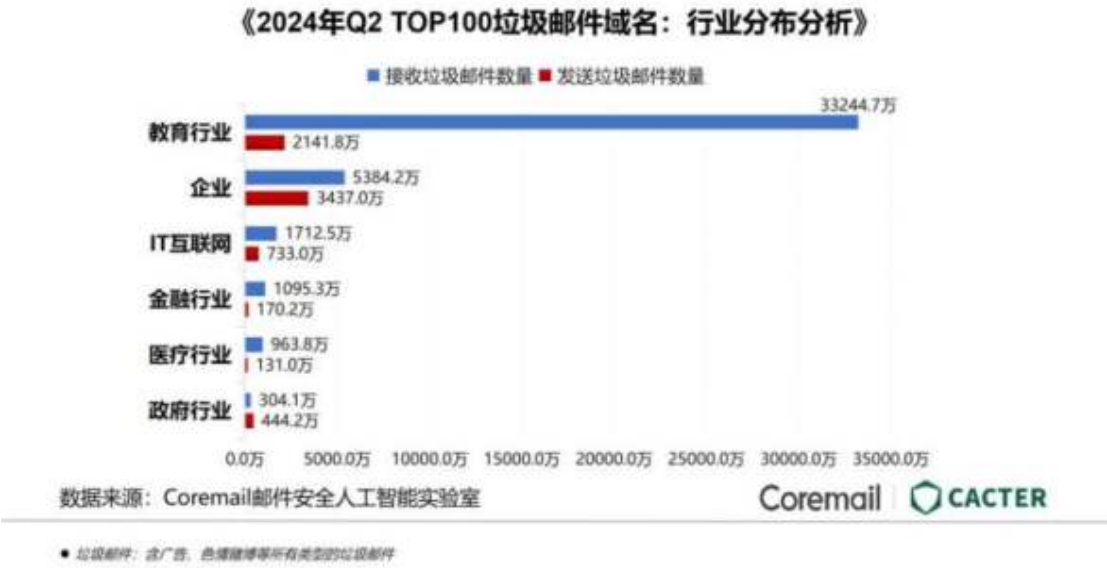

图 5 2024 年 Q2 TOP100 域名发送&接收垃圾邮件数量行业分布

面对教育领域持续增长的垃圾邮件困扰，提出以下建议给各位邮件系统管理员：

1. **设置有效的邮件过滤和防护机制：**学校和教育机构应使用针对垃圾邮件的有效过滤和防护技术，如使用邮件安全网关，及时拦截和清除垃圾邮件，减少对教育行业的干扰和危害。

2. **开展反钓鱼培训：**提高师生的网络安全防范意识，通过定期的模拟练习，教会他们如何识别并防御垃圾邮件和诈骗链接。

3. **强化信息与账号防护：**普及并推广个人信息加密及强密码使用的重要性，防止信息泄露成为钓鱼邮件攻击的跳板。

4. **推动高校安全合作：**鼓励高等学府间的威胁情报共享，及时交流最新的邮件安全策略和防御技巧，共同提高校园网络的安全防护水平。

二、2024 年 Q2 钓鱼邮件攻击动态

（一）境外钓鱼邮件激增与隐蔽的境内攻击源

在频发的网络安全攻击事件中，钓鱼攻击往往是黑客们的首选。2024 年以来，钓鱼邮

件数量持续增长，第二季度企业邮箱用户收到的钓鱼邮件数量达 1.43 亿，威胁态势依旧严峻，其中境外发送源达 56.23%，然而据 AI 实验室此前分析，虽然发件来源是境外，但钓鱼邮件中的文本、行文规范均符合国内的中文使用习惯，且钓鱼网站也都以仿冒境内网站为主，由此说明部分攻击的真实来源应是境内，只不过攻击者使用了境外服务器做为跳板，最终导致钓鱼邮件的境外来源数量远高于境内。

图 6 2023 Q2-2024 Q2 境内外钓鱼邮件攻击趋势

（二）国际邮件安全环境复杂严峻，北京为国内主要风险源

近年来，随着互联网的快速扩张与全球化进程的加速，邮件安全议题日益凸显其重要性。我国正面临境外钓鱼攻击的不断攀升，数据揭示美国作为钓鱼邮件的主要发源地，其攻击比例较俄罗斯高出显著的 60.7%。

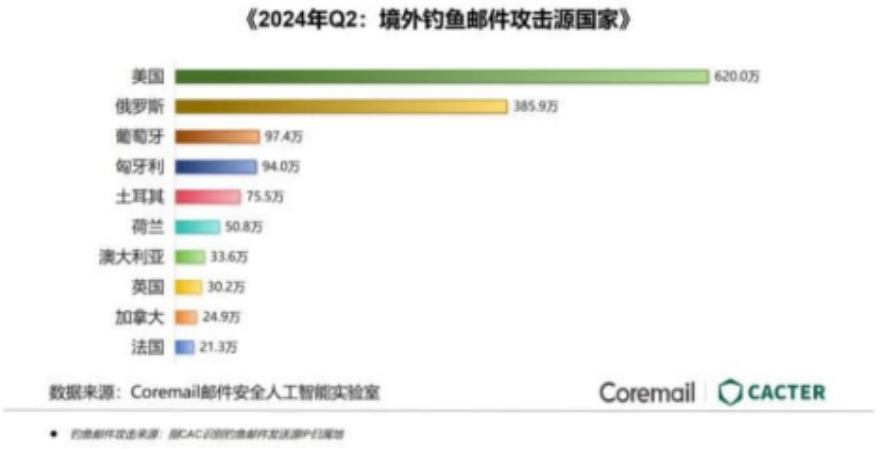

图 7　2024 Q2 境外钓鱼邮件攻击来源 Top10 国家

从国内的钓鱼邮件攻击态势来看，第二季度国内各地的钓鱼邮件攻击均有上升的趋势，其中北京为钓鱼邮件的主要来源，发出钓鱼邮件攻击次数达到 286.5 万次。此外香港跃居前三，成为了活跃来源，让黑客团体更易进行网络钓鱼活动。

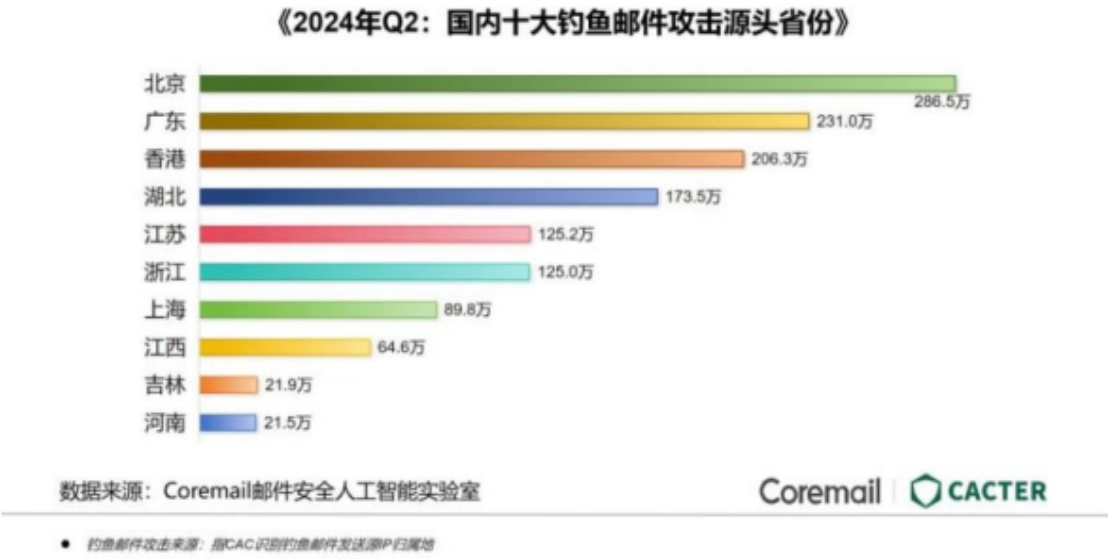

图 8　2024 Q2 国内钓鱼邮件攻击来源 Top10 省份

（三）TOP100 钓鱼攻击分析：教育与企业为攻击热点

如图，通过 Q2 钓鱼邮件发送&接收源 TOP100 域名行业分析，国内钓鱼邮件受害者所在行业比较集中，收到的钓鱼邮件数量排名 TOP100 域名的行业中，教育排名第一，约占钓鱼邮件总数的 60%（3914.1 万封）；企业排名第二，约占 26%（1713.4 万封）；排名第三的行业为 IT 互联网，占 5%（329.1 封）。

图 9　2024 Q2 TOP100 域名发送&接收钓鱼邮件数量行业分布

大规模邮件通讯所涉及的大量高价值信息和账号资产，以及员工和用户端安全意识和培训水平参差不齐的现状，导致企业和教育类机构成为网络攻击的重要目标。攻击者可以运用社会工程学手段，通过伪装成相关角色（例如老师、合作伙伴、客户或上级主管）的身份，针对性地向特定用户发送钓鱼邮件，从而提高攻击的成功率。

三、2024 年 Q2 垃圾钓鱼邮件案例

（一）垃圾邮件 TOP10：教育培训为主攻手段

第二季度的垃圾邮件数据揭示了当前邮件诈骗和垃圾邮件发送者采用的主要策略。以下为主题排名前十的垃圾邮件，以及其各自的邮件数量：

2024 年 Q2 热门垃圾邮件主题榜 TOP10

序号	垃圾邮件主题	邮件数（封）
1	【火热招生中】2024 年人力资源管理师	2562.3 万
2	re:我是陈*飞，为企业提供礼品采购的企业	1080.5 万
3	re:鼓励客户比价的企业礼品采购服务！	1076.9 万
4	2024 年最全课程汇总（增：线上证书课，包括中级经济师，HRBP 证书……）	1014.9 万
5	大客户开发与维护策略技巧	588.7 万
6	成交的秘密——高业绩顾问式销售技巧	539.6 万
7	中层经理管理能力提升	419.9 万
8	为了您自身的安全，我强烈建议您阅读这封电子邮件。	367.2 万
9	【火热招生中】2024 年中级经济师（人力资源）	346.2 万
10	Sales Notification	315.9 万

（二）钓鱼邮件 TOP10：官方伪装通知依然是主流

钓鱼邮件常伪装为系统通知或发票诈骗，这增加了账户被劫和数据泄露的风险。

2024 年 Q2 热门钓鱼邮件主题榜 TOP10

序号	钓鱼邮件主题	邮件数（封）
1	关于邮件系统的通知	393.4 万
2	为了您自身的安全，我强烈建议您阅读这封电子邮件。	151.7 万
3	お支払い金額のお知らせ	103.1 万
4	【电子发票】您收到一张新的电子发票[发票号码:980750**]	92.2 万
5	邮件管理系统	91.6 万
6	邮件管理系统通知	87.5 万
7	ご利用明細更新のお知らせ	81.6 万
8	《薪酬津贴登记发放须知》	81.4 万
9	核内邮件管理	80.2 万
10	待办申报表	79.2 万

（三）Q2 垃圾钓鱼邮件典型案例样本

1、补贴诈骗通知类持续威胁

图 10　2024 Q2 垃圾钓鱼邮件案例 1

图 11　2024 Q2 垃圾钓鱼邮件案例 2

图 12　2024 Q2 垃圾钓鱼邮件案例 3