2023第一季度
企业邮箱安全性研究报告

Coremail × 中睿天下

2023年4月出品

2023 年第一季度企业邮箱安全性研究报告

目录

一、2023 年 Q1 垃圾邮件宏观态势 4
（一）垃圾邮件数量走势 4
（二）垃圾邮件 IP 来源宏观分析 6
（三） 垃圾邮件发送&接收源 TOP100 域名行业分布 7
二、2023 年 Q1 钓鱼邮件宏观态势 9
（一）钓鱼邮件数量走势 9
（二） 钓鱼邮件 IP 来源宏观分析 10
（三）钓鱼邮件发送&接收源 TOP100 域名行业分布 12
三、2023 年 Q1 暴力破解宏观态势 13
（一）暴力破解数量走势 13
（二）暴力破解 IP 来源宏观分析 15
（三）暴力破解受害者行业分布 16
四、2023 年 Q1 典型恶意邮件案例 18
（一）垃圾钓鱼邮件主题 TOP10 18
（二）“工资补贴”成钓鱼邮件最大诱饵 19
五、中睿天下溯源深度案例 22
（一）某快递到达详情确认 22
（二）邮箱系统提醒 26
附录 1 CACTER 邮件安全网关产品介绍 29
附录 2 邮件安全人工智能实验室介绍 32

Coremail | 邮件安全

组长

林延中

主要编写人员

江嘉杰 刘骞 朱腾蛟 邱嘉娜 李雨恒 伍伟彬

《2023 年第一季度企业邮箱安全报告》由广东盈世科技计算机有限公司与北京中睿天下信息技术有限公司联合为您提供，本联合报告的编撰获得了 Coremail 邮件安全人工智能实验室、中睿天下邮件安全响应中心相关专家的悉心指导和宝贵建议，在此表示感谢。

Coremail 邮件安全人工智能实验室（Email Security AI Lab，以下简称“AI 实验室”），依托于 Coremail 丰富的应用场景、海量大数据与一流科技人才，专注于将自然语言处理、计算机视觉、大型语言模型等 AI 智能技术应用于电子邮件安全防护领域的创新突破。

一、2023 年 Q1 垃圾邮件宏观态势

（一）垃圾邮件数量走势

垃圾邮件一直是企业邮箱用户 “长盛不衰”的问题。2023 年初，各类垃圾邮件总量同比和环比均呈现上升态势，迎合国内逐渐放开疫情管控的大环境，垃圾邮件正在死灰复燃。据 Coremail 邮件安全人工智能实验室的监测数据显示，2023 年 Q1 全国企业邮箱用户共收到各类垃圾邮件 7.13 亿封，在 2022 年 Q4 短暂的回落后，又开始持续增长，相比 2022 年 Q4 环比增长 21.19%，对比去年 Q1 同比增长 5.55%。

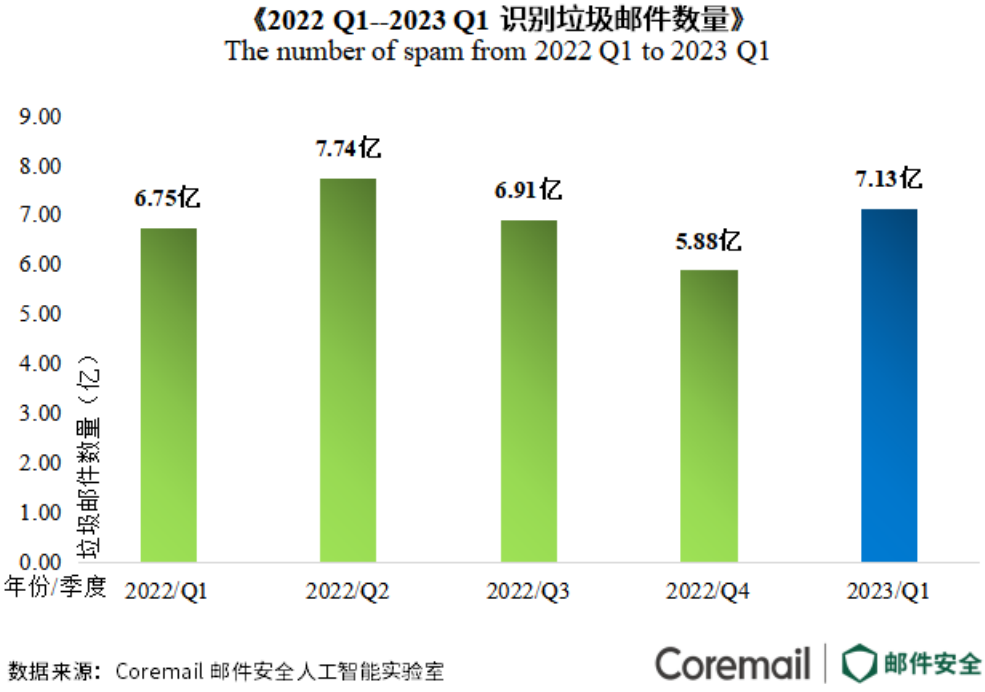


图 1 2022 Q1-2023 Q1 垃圾邮件数量走势

同时，7 成左右的垃圾邮件发送源 IP 归属地来自境外，发送超过 4.96 亿封，环比增长 29.17%，境外垃圾邮件发送量一直处于高速增长的状态。而国内垃圾邮件发送量也有小幅增长，发送超过 2.16 亿封垃圾邮件，环比增长 5.89 个百分点。

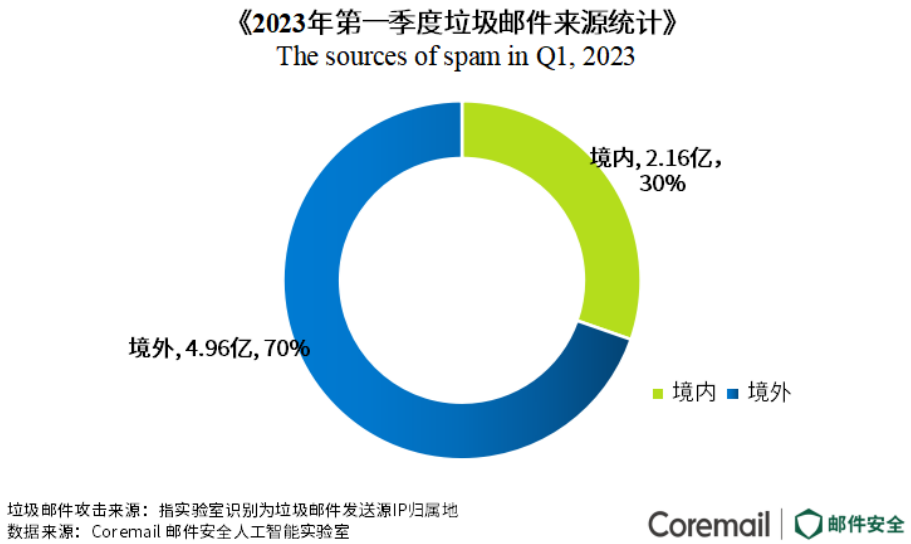


图 2 2023 年第一季度垃圾邮件来源

企业邮箱用户 Q1 收到的邮件类型中，正常邮件的总量和普通垃圾邮件的总量趋近，还有相当一部分邮件占比为钓鱼邮件、谣言反动类、色情赌博类邮件等，导致垃圾邮件总量整体超过正常邮件数量，给邮箱用户造成了很大困扰。

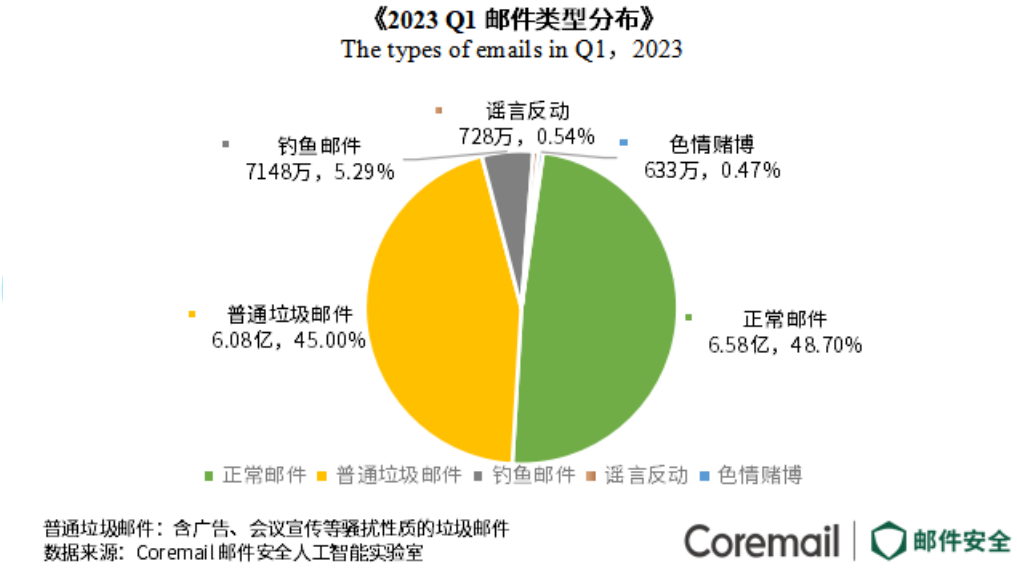


图 3 2023 年 Q1 邮件类型分布

垃圾邮件的泛滥严重影响着网络服务业者或企业的邮件服务器运作，侵占了网络传输资源。亟需高度重视邮件系统安全保护工作，提升电子邮件系统的安全防护能力，共同维

护良好的邮件安全生态环境，保障人民财产安全。

（二）垃圾邮件 IP 来源宏观分析

在 2023 年第一季度，境外垃圾邮件来源 TOP10 发生了些许变化，**排名第一的是美国（1300.4 万），再次登顶垃圾邮件攻击榜榜首，尽管其在第四季度略有下降。**其次是英国（997.8 万）、俄罗斯取代法国成为第三（642 万）、荷兰（401.5 万）和印度尼西亚（380.7 万）。

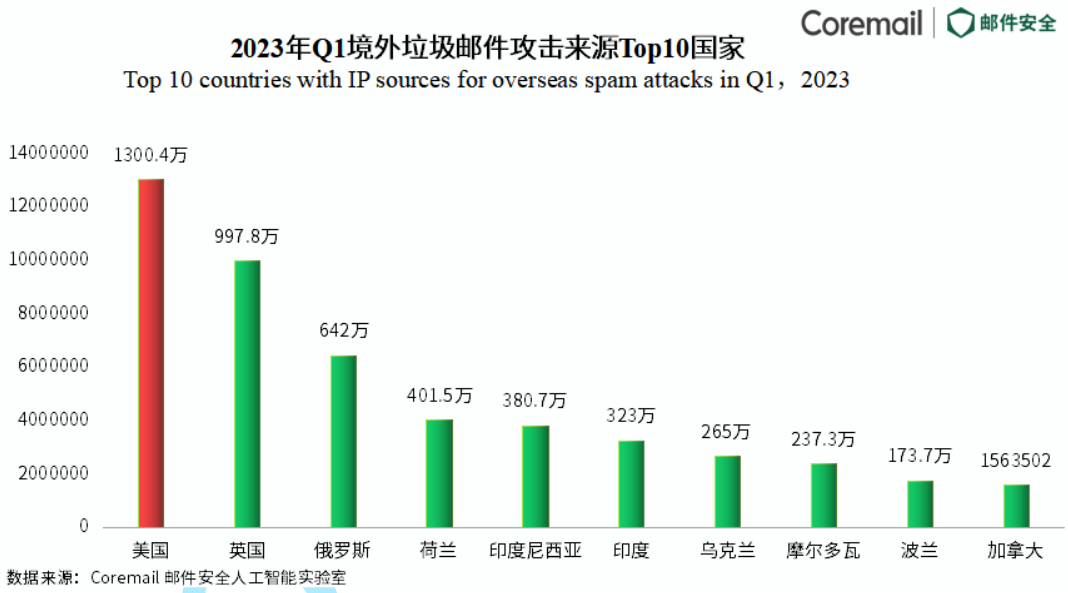


图 4 2023 年 Q1 境外垃圾邮件攻击来源 Top10 国家

来自中国归属地的垃圾邮件数量来源 TOP10 中，来自北京市、广东省、浙江省、上海市、香港特别行政区的发送量占据前五。**北京稳居高位，垃圾邮件发送量为 2825.8 万，创阶段新高，环比增超 200%。**

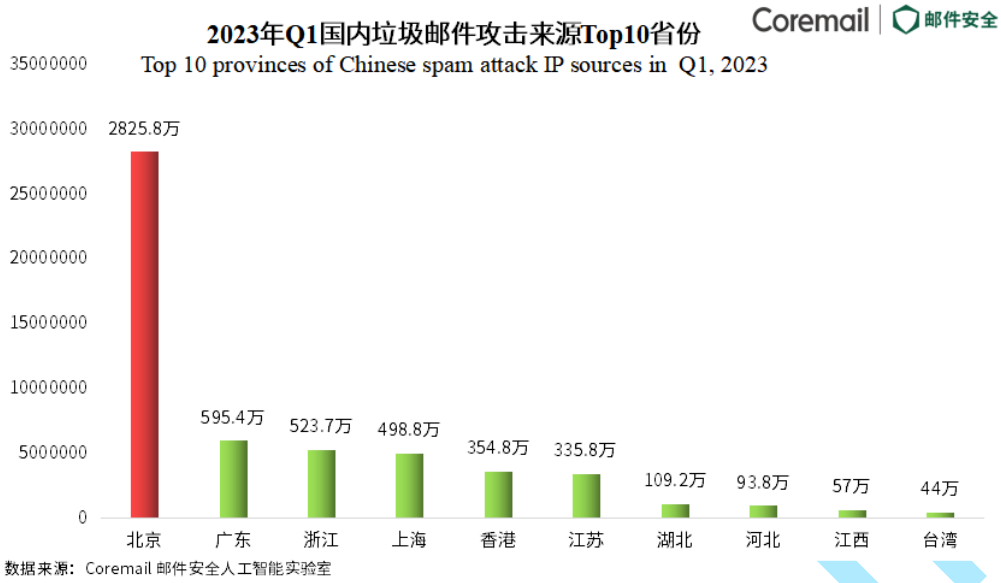


图 5 2023 年 Q1 国内垃圾邮件攻击来源 Top10 省份

（三）垃圾邮件发送&接收源 TOP100 域名行业分布

为了更好地分析垃圾邮件对企业邮箱使用的影响，AI 实验室对发送&接收垃圾邮件 TOP100 域名的用户行业进行了分析。据显示，**来自企业域名发送的垃圾邮件占比 65.72%，发送垃圾邮件数量达到 5333.7 万，这主要跟企业持续大量投放营销广告有关。**

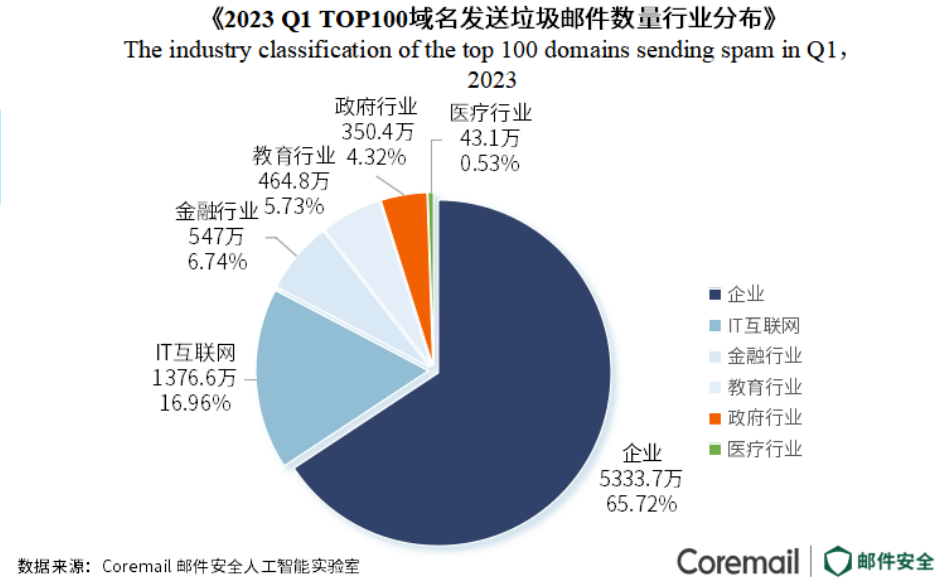


图 6 2023 年 Q1 TOP100 域名发送垃圾邮件数量行业分布

而在 TOP100 域名接收垃圾邮件源中，**教育行业接收量达到 1.59 亿封（62%），居于高位，教育行业仍然是垃圾邮件的重灾区**，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不容忽视，在此建议各位高校管理员能在日常邮箱运维中，增强垃圾邮件的过滤手段，同时有序组织反钓鱼演练，在拦截垃圾邮件的同时，持续提高用户的安全意识，形成垃圾邮件防护的完整闭环。

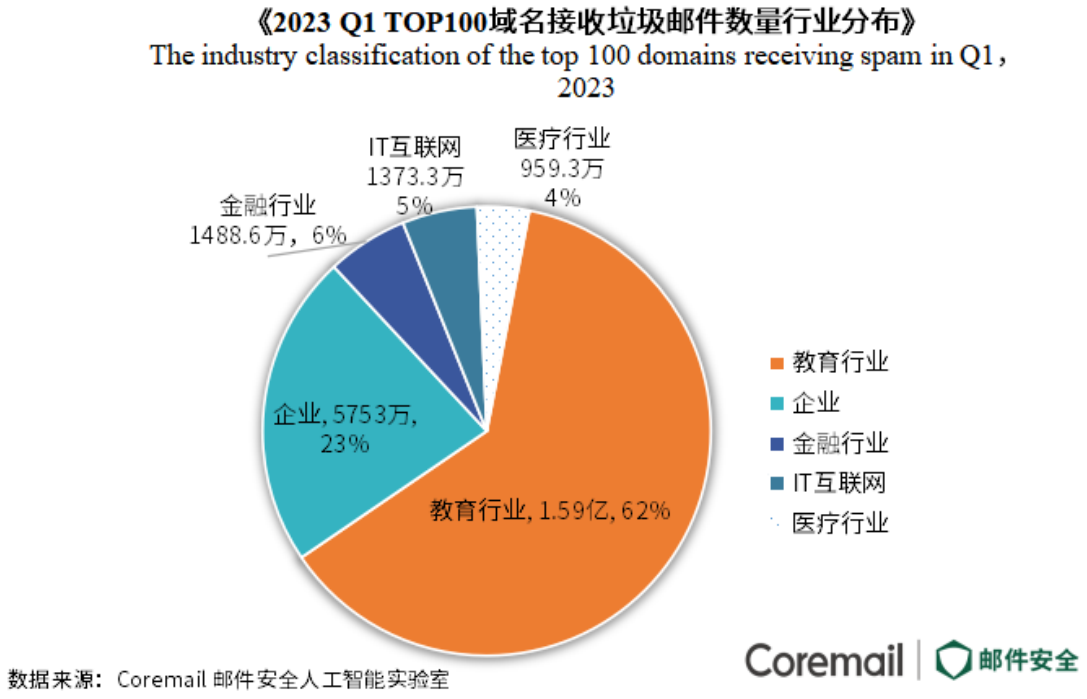


图 7 2023 年 Q1 TOP100 域名接收垃圾邮件数量行业分布

二、2023 年 Q1 钓鱼邮件宏观态势

（一）钓鱼邮件数量走势

钓鱼邮件包含恶意欺诈信息的邮件，包括 OA 钓鱼邮件、鱼叉邮件、钓鲸邮件、CEO 仿冒邮件和其他各类钓鱼欺诈邮件，但不包括带毒邮件、非法邮件等。黑产团伙会根据社会热点新闻、如人才补贴、银行年审、外贸快递、财务结算确认等多种主题引诱点击邮件中的钓鱼链接，目的就是为了盗取金钱。

在频发的安全攻击事件中，钓鱼攻击往往是黑客的首选。值得关注的是，自 2022 年第三季度以来，钓鱼邮件发送数量持续增长。2023 年 Q1，Coremail AI 实验室识别出的**企业钓鱼邮件数量持续走高，突破七千万，环比增长 7.3 个百分点，相较去年同期钓鱼邮件总量上升了 17.89%，威胁的态势依然十分严峻。**

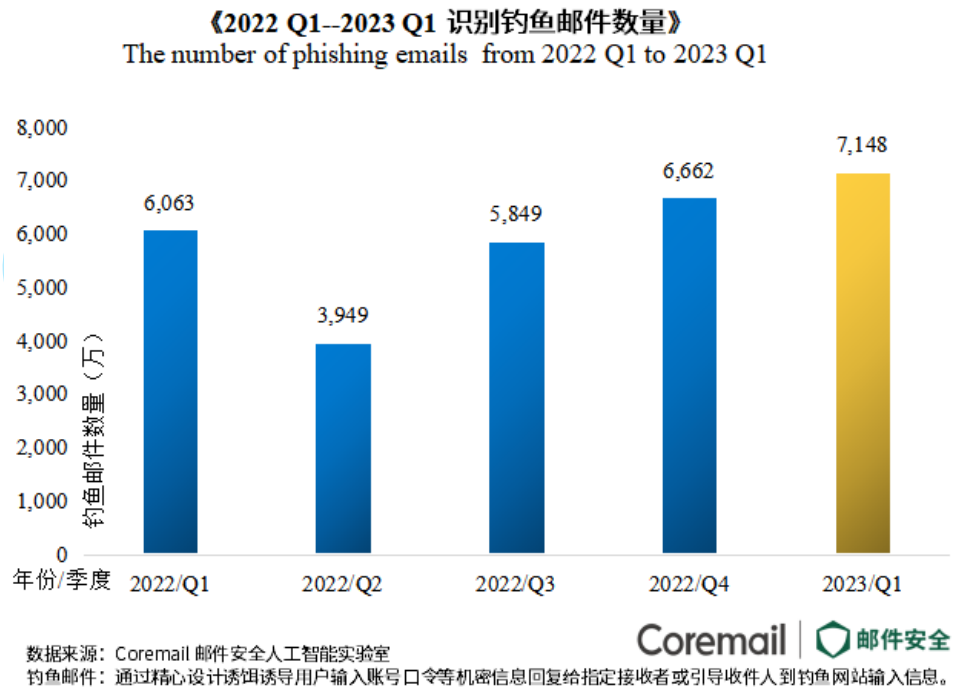


图 8 2022 Q1-2023 Q1 钓鱼邮件数量趋势

从 2022 全年数据而言，全国企业邮箱用户共收到各类钓鱼邮件约 425.9 亿封，这意味着平均每天约有 1.2 亿封钓鱼邮件被发出和接收，每位用户每月会收到约 20 封钓鱼邮件。网络钓鱼攻击事件逐年增加，钓鱼邮件数量在 2022 年短暂抑制后，再次增长，企业用户面临的潜在经济损失不可估量。（数据来源：《2022 年中国企业邮箱安全性研究报告》，Coremail&奇安信联合发布）

（二） 钓鱼邮件 IP 来源宏观分析

就钓鱼邮件的发送源分布而言，Q1 境外的钓鱼邮件数量有所下降，而境内发送钓鱼邮件数量攀升至 3 千万（占比 42%），环比 2022 第四季度增长 104.8%，境内钓鱼邮件攻击态势不可小觑。据 AI 实验室此前分析，虽然钓鱼邮件发信来源是境外，但邮件中的文本、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，由此说明部分钓鱼攻击的真实来源应是境内。

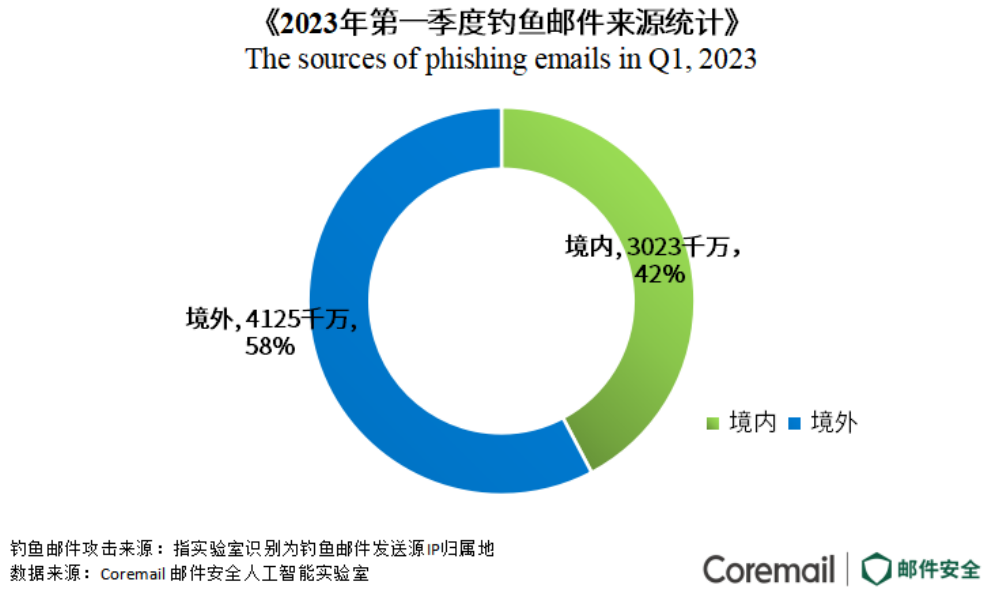


图 9 2023 Q1 钓鱼邮件来源统计

我国遭受来自境外的钓鱼攻击持续增加，而美国是针对中国钓鱼攻击的最大来源国。被用来钓鱼的美国 IP 来源最多，始终保持排名第一，钓鱼攻击的目标主要是针对中国企业。

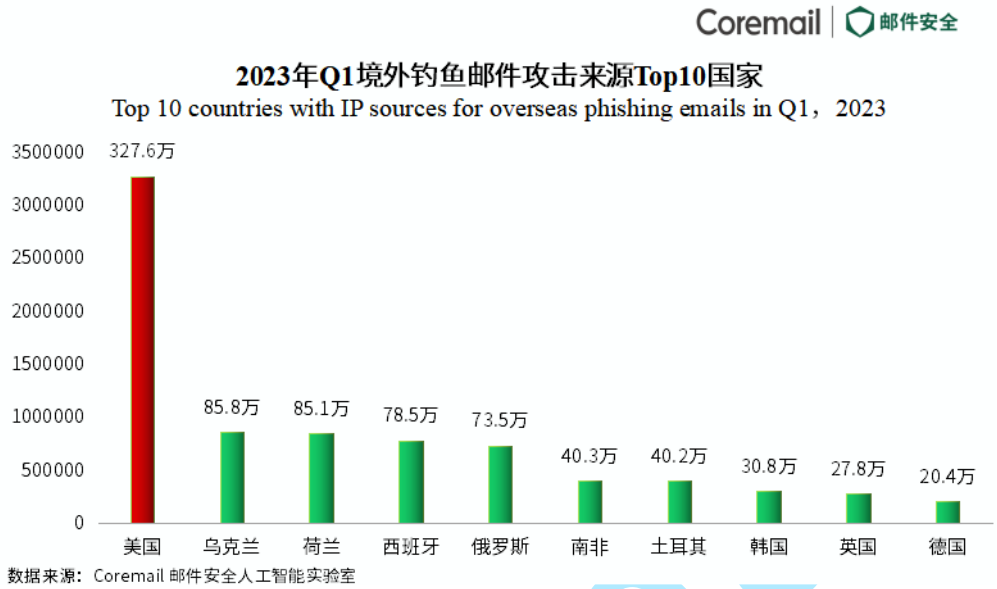


图 10 2023 Q1 境外钓鱼邮件攻击来源 Top10 国家

从国内的钓鱼邮件攻击态势来看，第一季度国内各地的钓鱼邮件攻击均有上升的趋势，其中上海市发送的钓鱼邮件数量最多，发出钓鱼邮件攻击次数达到 250.2 万次，替代北京位居第一。

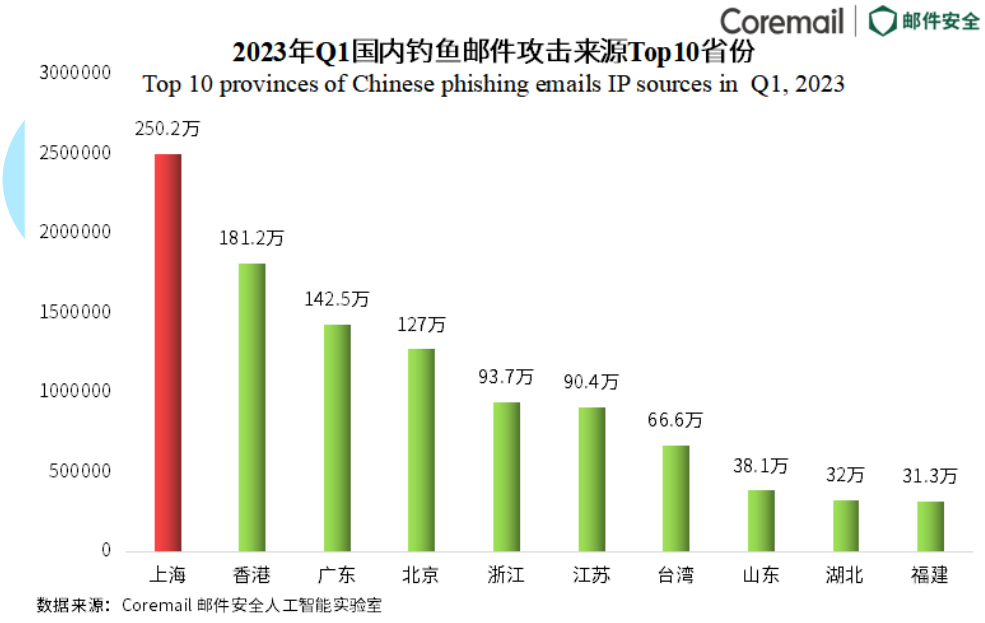


图 11 2023 Q1 国内钓鱼邮件攻击来源 Top10 省份

（三）钓鱼邮件发送&接收源 TOP100 域名行业分布

国内发送钓鱼邮件数量最多的行业是企业。国内钓鱼邮件受害者所在行业也比较集中，收到的钓鱼邮件数量排名 TOP100 域名的行业中，教育行业排名第一，约占钓鱼邮件总数的 53%（1.34 亿封）；企业排名第二，约占 35%；排名第三的行业为金融行业，占 7%。

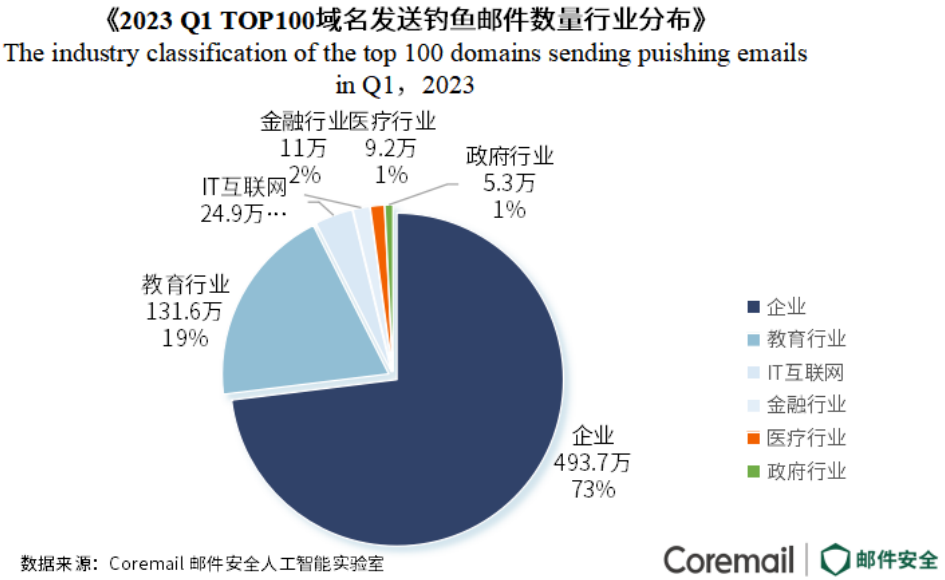


图 12 2023 Q1 TOP100 域名发送钓鱼邮件数量行业分布

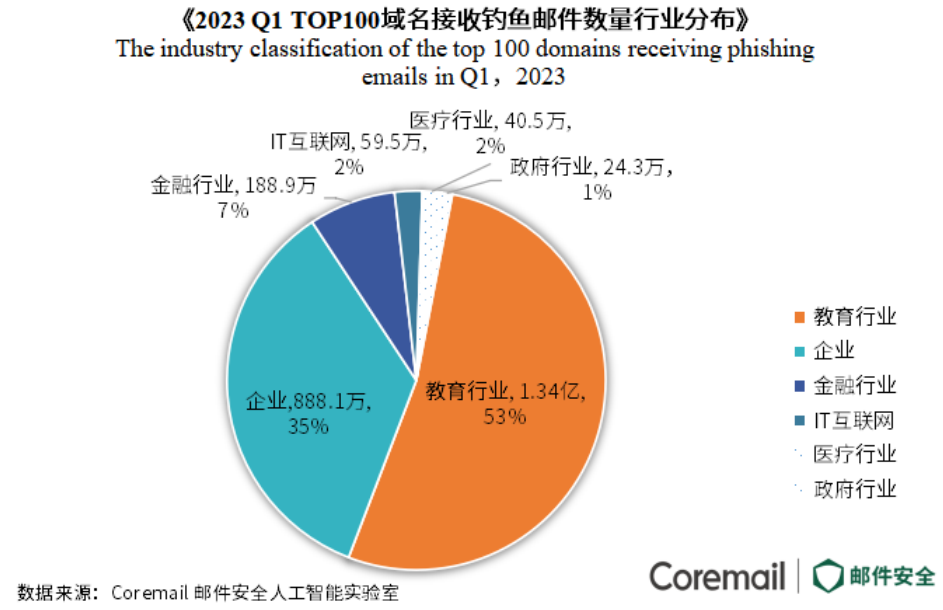


图 13 2023 Q1 TOP100 域名接受钓鱼邮件数量行业分布

三、2023 年 Q1 暴力破解宏观态势

（一）暴力破解数量走势

在邮箱系统盗号问题上，暴力破解是目前的突出难题。根据 AI 实验室监测，Q1 全国企业级用户遭受超过 17.45 亿次暴力破解，无差别的暴力破解攻击从去年 Q4 开始有相当幅度的下降趋势，但在今年 2-3 月，全域暴力破解攻击次数又开始回升。

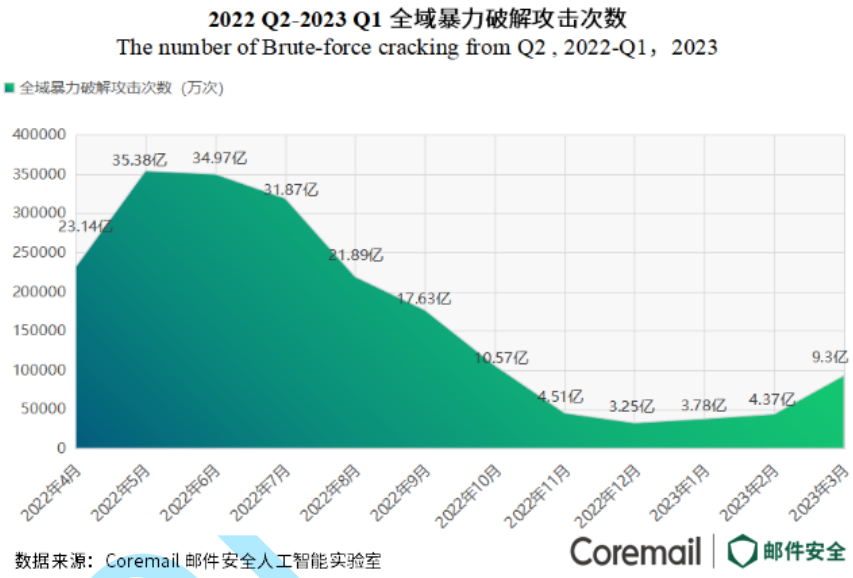


图 14 2022 Q2-2023 年 Q1 全域暴力破解攻击次数

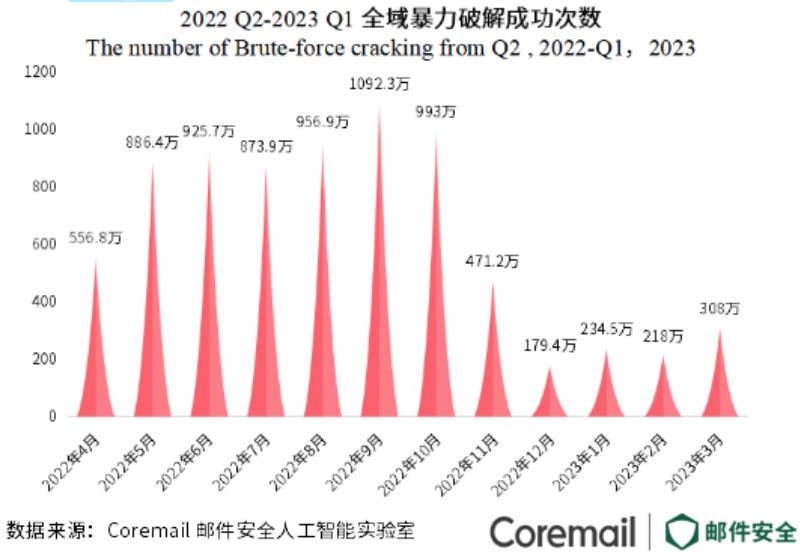


图 15 2022 Q2-2023 年 Q1 全域暴力破解成功次数

根据 Coremail 邮件安全专家推测，该攻击趋势可能有以下几个原因供参考：

（1） **前期攻击者在尝试探测用户的真实账号。**在这个过程中，攻击者并不确定哪些是用户正常使用的账号，只能尝试反复攻击多个具有特定命名规则或字典中的账号。在密码字典长度恒定的前提下，此时攻击的总数量与被攻击账号呈正比关系，所以 Q2~Q3 攻击暴破次数处于一个较高的水平。

（2） **在 Q4，攻击者进入了精准攻击阶段。**精准攻击意味着攻击者把攻击对象从广泛的、不确定的猜测对象转换为局部的、可能性较高的确定对象。在密码字典没有明显量级变化时，攻击对象数量大量减少，导致 Q4 的攻击暴破次数出现了明显的梯度下跌。

（3） **在 Q4，攻击者同时也进入了成果转换阶段。**在成功盗取了一批账号后，主要工作重心进行了部分转移。所以出现 2022 年 Q4 钓鱼邮件数量明显高于同年其他季度，但攻击暴破次数明显下降的迹象。

（4） **在 2023 年 Q1，攻击暴破次数出现了回升。**初步判断为受害者经历去年 Q4 的被盗账号进行成果转换后，增强了对应账号的防护。攻击者只能另寻其他防守薄弱的账号进行攻击，攻击手段又回到了之前的广撒网式攻击。

（5） 按照上述的说明，可以明显看出攻击者的攻击爆破规律：**广撒网、精准攻击、成果转换。**基于这个规则，下一个季度将是攻击爆破次数的高峰期，建议提前做好对应的账号安全防范。比较有效的做法是针对外部 IP 的认证制定严格的策略，针对内部账号的行为进行严格的监测。

（二）暴力破解 IP 来源宏观分析

据 AI 实验室的数据显示，暴力破解 IP 主要来源于国内。Q1 国内暴力破解主要来源于江苏省和安徽省，Coremail 拦截分别达到 5.2 亿次、4.64 亿次。

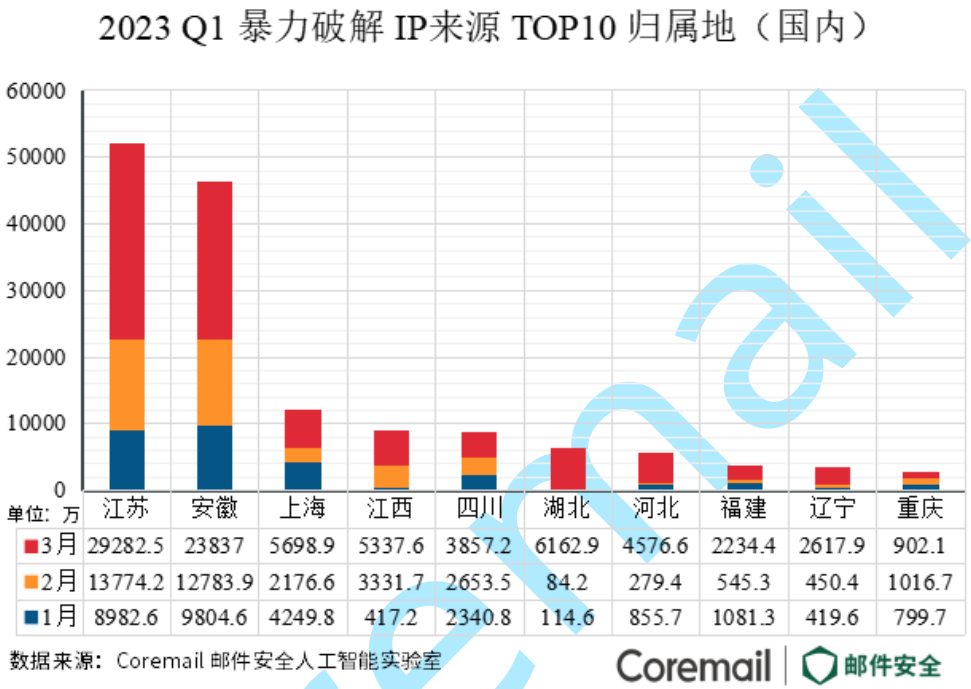


图 16 2023 年 Q1 全域暴力破解 IP 来源 TOP10 归属地（国内）

来自境外的暴力破解 IP 中，美国暴力破解 IP 来源占据榜首，第 1 季度 Coremail 合计拦截来自美国的 2692 万次暴力破解，欧盟排名第二（2013.6 万次），亚太地区跻身前三（1115.2 万次）。

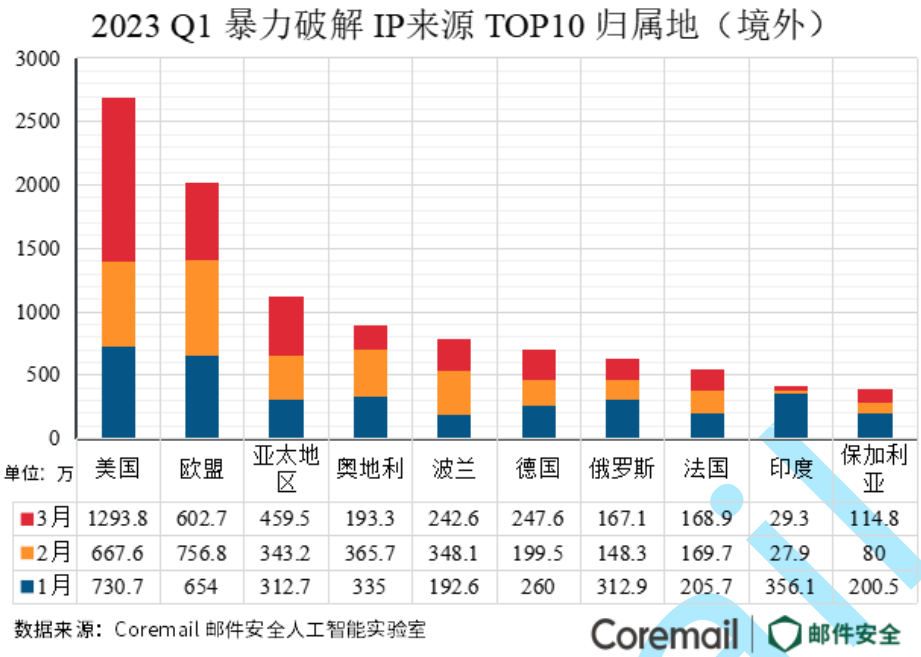


图 17　2023 年 Q1 全域暴力破解 IP 来源 TOP10 归属地（境外）

（三）暴力破解受害者行业分布

第 1 季度全国企业级用户遭受超过 17.45 亿次暴力破解，Coremail 对各行业面临的邮件威胁压力进行深度分析，无论是接收钓鱼邮件数量、接收垃圾邮件数量、被暴力破解攻击次数，**发现暴力破解攻击的行业目标比较集中，教育行业、企业和 IT 互联网是主要受灾区，**而教育行业遭受的威胁最大。大量高校师生的邮箱账号使用初始密码，且有大批学生邮箱始终处于非活跃状态，极易被盗，且不易被发现。

黑产攻击者通过暴力破解拿到账号，从撒网攻击到利用潜伏账号进行收割，攻击者会使用被盗账号大量发送垃圾邮件或进行针对性钓鱼攻击。

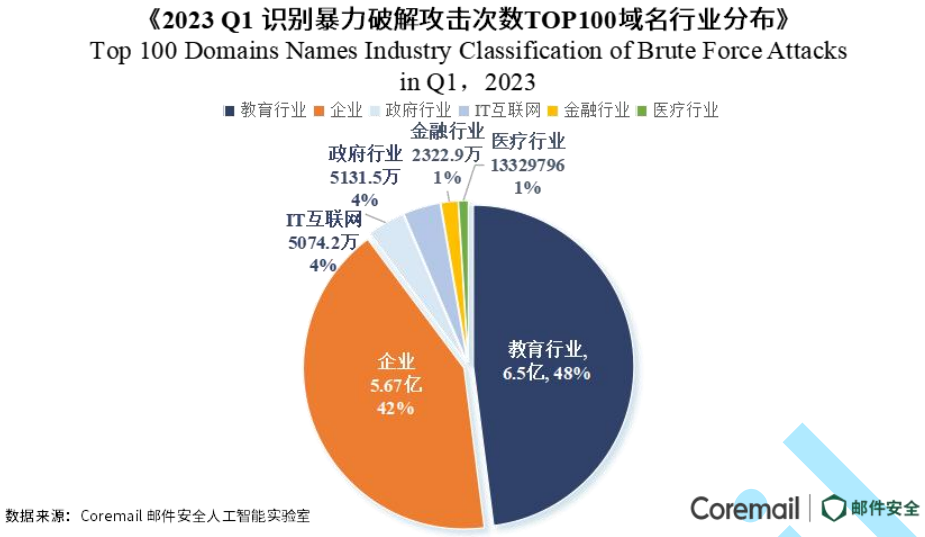


图 18 2023 年 Q1 识别暴力破击攻击次数 TOP100 域名行业分布

我国双一流高校长期面临着严重的邮件威胁，黑产团伙妄图通过钓鱼邮件、盗号等手段获取高校机密性科研材料，或对师生进行钱财诈骗。面对越来越有针对性的邮件攻击，高校应该从邮件服务器端、个人终端和安全意识等多方面入手进行防护。

对于邮件服务端，可以通过增加邮件网关来加强对钓鱼邮件的防护，同时需要强制开启二次认证和客户端专用密码来防止账号被盗；对于用户终端，要正确安装防毒软件；在用户安全意识培养方面，可以通过钓鱼攻击演练来加深用户的印象。

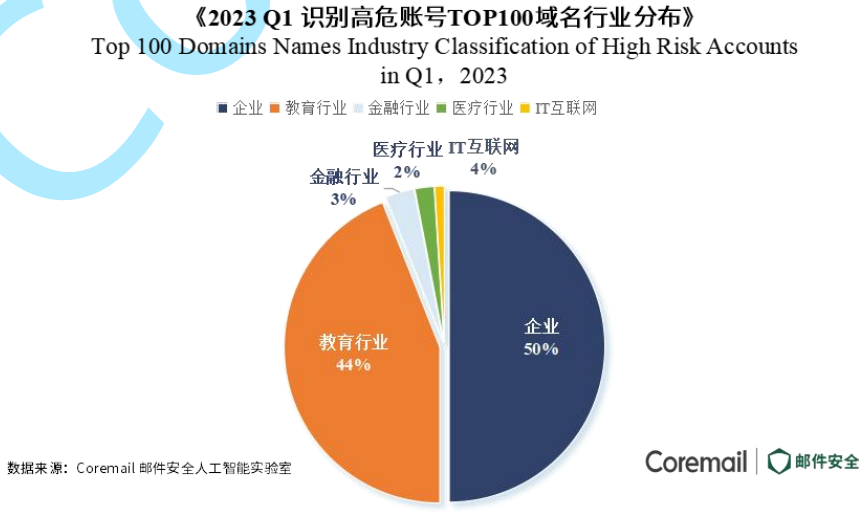


图 19 2023 年 Q1 识别高危账号 TOP100 域名行业分布

四、2023 年 Q1 典型恶意邮件案例

（一）垃圾钓鱼邮件主题 TOP10

如下表所示，AI 实验室分别统计分析了 2023 年第一季度垃圾邮件、钓鱼邮件主题 TOP10。可以发现，在钓鱼邮件中，**工资补贴类诈骗邮件依然活跃，且黑产分子结合时事，在 3 月份的时候出现了仿冒个人所得税申报的钓鱼邮件，邮箱用户务必提高反钓鱼意识，避免损失财物。**

2023 年第一季度垃圾邮件主题 TOP10		
序号	垃圾邮件主题	邮件数（万封）
1	顶峰设计：PPT 美化与设计服务	1447.7
2	POWER BI 商业大数据分析&可视化呈现 、Excel 高效数据管理与图表应用	1080.4
3	《客户服务的管理与投诉处理技巧》《演示之道——PPT 的商务设计与呈现技巧》	1062.5
4	五星服务：客户服务创新与投诉处理、赢在中层：中层（MTP）管理技能提升	986.7
5	《项目全过程管理控制与实践》《销售渠道建设与管理》	934.1
6	订单已派送	681.7
7	《大客户开发与维护策略技巧》《行政管理实操训练》	661.2
8	【报名中！】2023 年中级经济师（人力资源方向）	418.7
9	《基于战略导向的薪酬与绩效管理》《行政管理实操训练》	392.2
10	【招生中】2023 年中级经济师（人力资源）	382.8

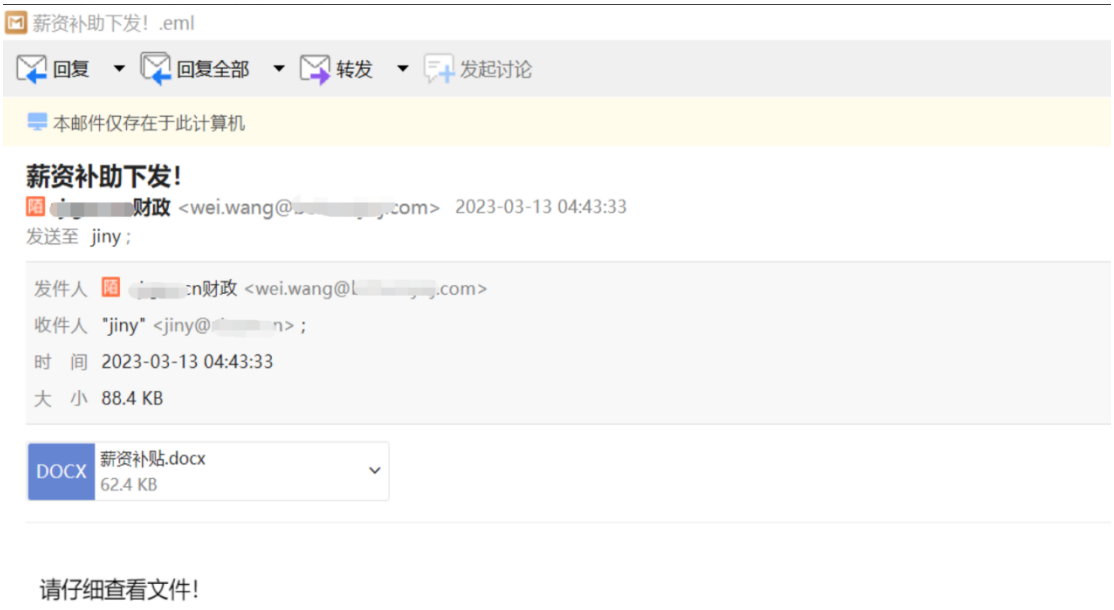
2023 年第一季度钓鱼邮件主题 TOP10		
序号	钓鱼邮件主题	邮件数（万封）
1	2023 年个人劳动（补贴）通知，查看下图查收	106.2
2	回复：邮箱安全升级重要公告！关系到用户的正常使用！（请务必仔细阅读）	97.1
3	邮箱安全升级重要公告！关系到用户的正常使用！（请务必仔细阅读）	91
4	转自：2023 年第一季度工薪补助登记统计相关补充材料	86.6
5	回复:邮箱安全升级重要公告！关系到用户的正常使用！（请务必仔细阅读）	59.5
6	隔离区邮件通知目录摘要/Spam notification Abstract	54.7
7	第一季度补•贴	52.8
8	《2023 财政通知》	44.5
9	新的邮件请查收！	43.5
10	个人劳动（补贴））已下发，请查看下图查收	43.3

（二）“工资补贴”成钓鱼邮件最大诱饵

诈骗邮件详情

Coremail 从 2021 年 12 月开始披露关于黑产团伙冒充国家相关部门下发补贴的钓鱼邮件，主题基本为【工资补贴通知】【《2023 财务补贴声明》】等，该组织通过诱导受害者输入银行卡及密码进行实时诈骗，中睿天下该邮件进行了深度溯源，邮件正文是工资补贴通知，在正文中放置了一张二维码图片，诱导收件人扫描正文中二维码，邮件附件的内容

和邮件正文一样，并未携带病毒和可执行文件。



在过去的 2 年时间，此类补贴诈骗钓鱼邮件不仅日益猖獗，攻击手法也不断变种。2022 年，Q2~Q3 攻击手法转变为先盗号，使用被盗账号伪装为公司“财务部”“人事部”等公司内部相关人员，向域内大量传播诈骗邮件，利用域内邮箱的高信用度躲避反垃圾反钓鱼检测、骗取“同事”的信任。主题也发展为【XX 月份补贴发放通知】【XXX+补贴】【XXX 集团财务部-关于发布最新补贴通知】，此诈骗邮件在去年 5 月份甚至导致了某门户邮箱网站员工受骗，引发了广泛讨论。

而 2023 年 Q1，黑产团伙偏向使用不同的文案逃避邮件系统厂商反钓鱼检测。Q4 常见的钓鱼主题有【2023 年第一季度个人劳动补贴】、【薪资补助下发】等，且黑产分子结合时事，在 3 月份的时候出现了仿冒个人所得税申报的钓鱼邮件，同时正文更多使用图片形式插入，对厂商的反垃圾反钓鱼图片 OCR 引擎产生较大考验。

防护策略

1. 不要轻易在可疑网站中输入个人身份证信息、银行卡号、密码。
2. 提高密码策略要求，设置域内必须使用强密码，并建议进行弱密码扫描，及时修改弱密码以防邮箱被盗。
3. 提高警惕，收到相关补贴通知类邮件请务必进行单位内部确认；切勿轻易点击邮件中的可疑链接或扫描二维码!
4. 建议订阅【防暴卫士】和【邮件安全情报】，最大化邮件威胁感知能力，能有效缓解账号破解威胁；
5. 请确保您的反垃圾功能正常开启或使用 CACTER 邮件安全网关进行拦截防护。

6. 建议进行【反钓鱼演练】，对公司重要岗位职工（财务、管理层）进行安全意识教育；

7. 积极举报威胁邮件，携手共建邮件安全环境；举报邮箱:cac-team@coremail.cn。

8. 如遇可疑情况，可拨打 96110 咨询求助；或下载国家反诈中心 APP，关注广州反诈服务号，学习防骗知识，防诈反诈。

五、中睿天下溯源深度案例

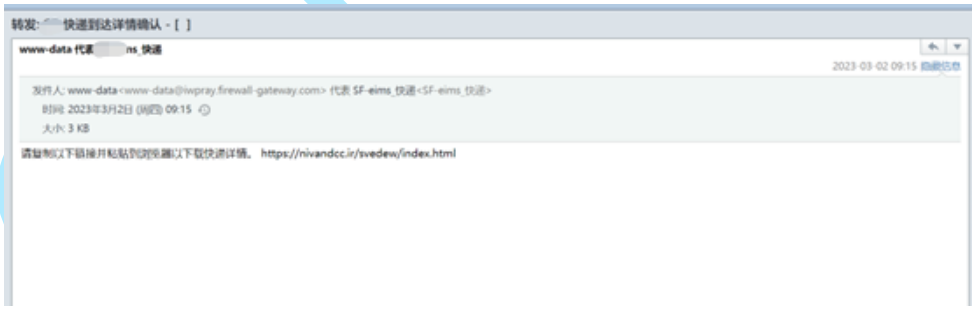
（一）某快递到达详情确认

邮件溯源分析报告

邮件分析

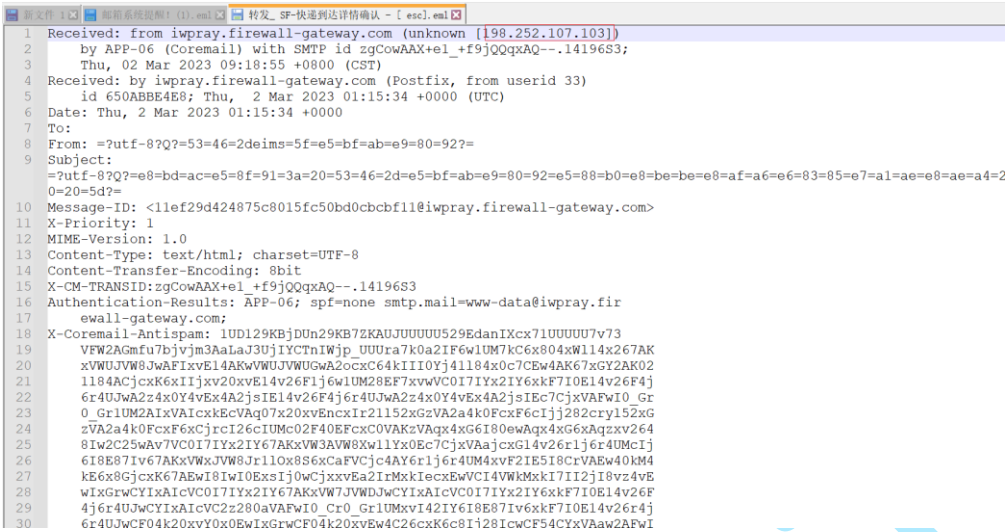
概述：发件人邮箱地址 IP 为 198.252.107.103，归属地为中国/香港。钓鱼链接未发现后续跳转，域名可伪造。域名关联多个恶意木马程序。

原件预览详情如下图所示：



源码分析

分析邮件源码可以发现发送邮件的 IP 地址为 198.252.107.103



```
Received: from iwpray.firewall-gateway.com (unknown [198.252.107.103])
    by APP-06 (Coremail) with SMTP id zgCowAAX+e1_+f9jQQqxAQ--.14196S3;
    Thu, 02 Mar 2023 09:18:55 +0800 (CST)
Received: by iwpray.firewall-gateway.com (Postfix, from userid 33)
    id 650ABBE4E8; Thu,  2 Mar 2023 01:15:34 +0000 (UTC)
Date: Thu, 2 Mar 2023 01:15:34 +0000
To:
From: =?utf-8?Q?=53=46=2deims=5f=e5=bf=ab=e9=80=92?=
Subject:
=?utf-8?Q?=e8=bd=ac=e5=8f=91=3a=20=53=46=2d=e5=bf=ab=e9=80=92=e5=88=b0=e8=be=be=e8=af=a6=e6=83=85=e7=a1=ae=e8=ae=a4=20=20=5d?=
Message-ID: <11ef29d424875c8015fc50bd0cbcbf11@iwpray.firewall-gateway.com>
X-Priority: 1
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 8bit
X-CM-TRANSID:zgCowAAX+e1_+f9jQQqxAQ--.14196S3
Authentication-Results: APP-06; spf=none smtp.mail=www-data@iwpray.fir
    ewall-gateway.com;
X-Coremail-Antispam: 1UD129KBjDUn29KB7ZKAUJUUUUU529EdanIXcx71UUUUU7v73
    VFW2AGmfu7bjvjm3AaLaJ3UjIYCTnIWjp_UUUra7k0a2IF6w1UM7kC6x804xWl14x267AK
    xVWUJVW8JwAFIxvE14AKwVWUJVWUGwA2ocxC64kIII0Yj41l84x0c7CEw4AK67xGY2AK02
    1l84ACjcxK6xIIjxv20xvE14v26F1j6w1UM28EF7xvwVC0I7IYx2IY6xkF7IOE14v26F4j
    6r4UJwA2z4x0Y4vEx4A2jsIE14v26F4j6r4UJwA2z4x0Y4vEx4A2jsIEc7CjxVAFwI0_Gr
    0_Gr1UM2AIxVAIcxkEcVAq07x20xvEncxIr21l52xGzVA2a4k0FcxF6cIjj282cry152xG
    zVA2a4k0FcxF6xCjrcI26cIUMc02F40EFcxC0VAKzVAqx4xG6I80ewAqx4xG6xAqzxv264
    8Iw2C25wAv7VC0I7IYx2IY67AKxVW3AVW8Xwl1Yx0Ec7CjxVAajcxG14v26r1j6r4UMcIj
    6I8E87Iv67AKxVWxJVW8Jr1lOx8S6xCaFVCjc4AY6r1j6r4UM4xvF2IE5I8CrVAEw40kM4
    kE6x8GjcxK67AEwI8IwI0ExsIj0wCjxxvEa2IrMxkIecxEwVCI4VWkMxkI7II2jI8vz4vE
    wIxGrwCYIxAIcVC0I7IYx2IY67AKxVW7JVWDJwCYIxAIcVC0I7IYx2IY6xkF7IOE14v26F
    4j6r4UJwCYIxAIcVC2z280aVAFwI0_Cr0_Gr1UMxvI42IY6I8E87Iv6xkF7IOE14v26r4j
    6r4UJwCF04k20xvY0x0EwIxGrwCF04k20xvEw4C26cxK6c8Ij28IcwCF54CYxVAaw2AFwI
```

查询此 ip 发现其归属地为中国/香港

当前IP	198.252.107.103 (rDNS: 198.252.107.103-static.reverse.arandomserver.com)
地理位置	中国/香港
行为位置	-
定位商圈	-
定位经纬度	
运营商	hawkhost.com
应用场景	数据中心
地区中心经纬度	22.396428,114.109497

经初步判断此 ip 可能为攻击者的网络出口地址，或者代理转发地址。

对该 ip 进行开源情报查询，发现此 ip 被标注恶意

钓鱼链接

邮件正文显示诱导链接为 https://nivandcc.ir/svedew/index.html

在三月份开展溯源工作时，页面仍可以访问预览如下，而在此次报告发布时显示“此帐户

已被暂停”。

测试暂未发现此网站有跳转现象，解析此域名 ip 为 195.201.55.155，

```
C:\Users\Administrator>nslookup nivandcc.ir
服务器:  bogon
Address:  172.16.120.16

非权威应答:
名称:    nivandcc.ir
Address:  195.201.55.155
```

查询此 IP 归属地点来自德国/萨克森自由州/法尔肯施泰因。

数据	地理位置信息(数据来源于企业版)
当前IP	195.201.55.155 (rDNS: static.155.55.201.195.clients.your-server.de)
地理位置	德国/萨克森自由州/法尔肯施泰因
行为位置	-
定位商圈	-
定位经纬度	
运营商	hetzner.com
应用场景	数据中心
地区中心经纬度	50.475005,12.364975

且查询此域名发现 spf 校验为软拒绝，即此域名可以伪造，该域名无可继续追溯价值。

```
C:\Users\Administrator>nslookup -q=txt nivandcc.ir
服务器:  bogon
Address:  172.16.120.16

非权威应答:
nivandcc.ir     text =

        "v=spf1 ip4:78.46.90.183 ip4:69.162.96.186 +a +mx +ip4:216.245.198.154 ~all"
```

根据开源情报发现该 ip 关联多个恶意木马程序，包括 Emotet 恶意软件木马病毒、Generic 盗号木马等。

Trojan.Generic 属于一种常见的盗号木马，启动后会从体内资源部分释放出病毒文件，有些在 WINDOWS 下的木马程序会绑定一个文件，将病毒程序和正常的应用程序捆绑成一个程序，释放出病毒程序和正常的程序，用正常的程序来掩盖病毒。

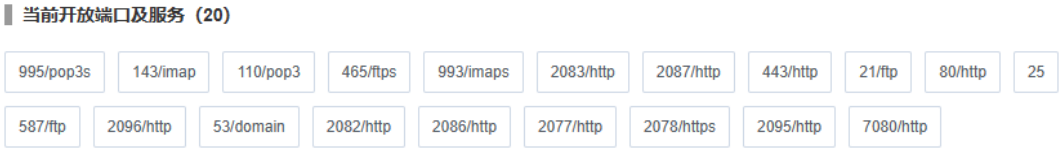
样本	扫描时间	多引擎检出	木马家族和类型	威胁等级
1e6a750b72a26d86f381a2c0bffe1d1d…	2022-12-03 03:37:45	8/22	Emotet 木马	恶意
ef4173f23c13bfc8241c2e2c28c2ba93…	2022-12-02 04:34:25	7/22	Generic 木马	恶意
4726642cd0ef16ffb727e16315a06ac2…	2022-12-02 04:34:22	8/22	Emotet 木马	恶意
4ecffc5cf391651bac6f513e16b484963…	2022-12-02 02:37:58	7/22	Generic 木马	恶意
71b59f7ff1c58e58298ce70803ad9439…	2022-12-02 01:28:21	8/22	Emotet 木马	恶意

Emotet 是一种计算机恶意软件程序，最初是作为一种银行木马病毒开发的。其目的是访问外部设备并监视敏感的私有数据。Emotet 会骗过基本的防病毒程序并保持隐匿。一旦被感染，该恶意软件会像计算机蠕虫病毒一样传播，并试图渗透到网络中的其他计算机。Emotet 主要通过垃圾电子邮件传播。相应的电子邮件包含恶意链接或受感染的文档。如果您下载文档或打开链接，则其他恶意软件会自动下载到您的计算机上。

通信样本 (264)　相关域名 (11)

域名	发现时间	更新时间	微步标签
armannahalpersian.ir	2022-07-10	2023-02-16	钓鱼 恶意软件 Emotet银行木马
mail.armannahalpersian.ir	2022-07-10	2023-02-16	钓鱼 恶意软件 Emotet银行木马
www.armannahalpersian.ir	2022-07-10	2023-02-16	钓鱼 恶意软件 Emotet银行木马
mail.rravagh.com	2022-09-01	2022-10-15	钓鱼
rravagh.com	2022-09-01	2022-10-15	钓鱼

判断该 ip 为攻击者购买使用国外服务器 ip，该服务器开放 995/pop3s、443、80 等多个端口。



（二）邮箱系统提醒

邮件分析

邮件头

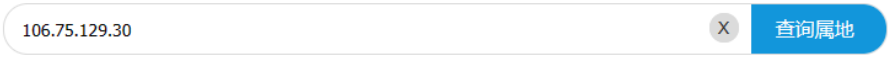
```
Received: from mail.wxltec.com (unknown [106.75.129.30])
    by APP-08 (Coremail) with SMTP id 0ACowACnrOwQLwFkjNq6AQ--.694S2;
    Fri, 03 Mar 2023 07:19:44 +0800 (CST)
Received: from rlljowddp (unknown [180.110.209.251])
    by mail.wxltec.com (Postfix) with ESMTPSA id 0080A3A2A01D7
    for <>; Fri,  3 Mar 2023 07:04:47 +0800 (CST)
Message-ID: <4741f0711a5d8bb32ab5f4f603c7c644@wxltec.com>
From: =?utf-8?B?57O757uf566h55CG5ZGY?= <test@wxltec.com>
To:
Subject: =?utf-8?B?6YKu566x57O757uf5o+Q6YaS77yB?=
Date: Fri, 03 Mar 2023 07:04:21 +0800
X-Priority: 3
X-Mailer: Qadlaaaa Hsawkpbls 72.36
MIME-Version: 1.0
Content-Type: text/html;
    charset="utf-8"
Content-Transfer-Encoding: base64
X-CM-TRANSID:0ACowACnrOwQLwFkjNq6AQ--.694S2
Authentication-Results: APP-08; spf=none smtp.mail=test@wxltec.com;
X-Coremail-Antispam: 1UD129KBjvdXoW7Wr18ArWDCr4kurWxJry5Jwb_yoWDGrb_ZF
    ykJr1vkFs7Z3W5A340valkGr18K3ZrWF40vayUZa97Aw48G3W8Zr4Yy34YyF47Ga42q3ZI
    qanxZry3WFy7ZjkaLaAFLSUrUUUUUb8apTn2vfkv8UJUUUU8Yxn0WfASr-VFAUDa7-sFnT
    9fnUUIcSsGvfJTRUUU1zAYjsxI4VWDJwAYFVCjjxCrM7AC8VAFwI0_Jr0_Gr1lIIY67AE
    w4v_Jr0_Jr4l8cAvFVAK0II2c7xJM28CjxkF64kEwVA0rcxSw2x7M28EF7xvwVC0I7IYx2
    IY67AKxVWUJVWUCwA2z4x0Y4vE2Ix0cI8IcVCY1x0267AKxVWUJVW8JwA2z4x0Y4vEx4A2
    jsIE14v26r4UJVWxJrl184ACjcxK6I8E87Iv6xkF7I0E14v26r4UJVWxJrl1nx0E6VACY4
    xI67k04243AVACY4xI67k04243AVAKzVAKj4xI6x02cVCv0xWle2I262IYc4CY6c8Ij28I
    cVAaY2xG8wAqx4xG62kEwI0EbcxfMc02F40En4AKxVAvwIkv4cxYr2415I8CrVC2j2CE0s
    8v4I0Ex7kE8s41Yx0E2Ix0cI8IcVAFwI0_Jrv_JF1lYx0Ec7CjxVAajcxGl4v26rlj6r4U
    McIj6I8E87Iv67AKxVW8Jr0_Cr1UMcvjeVCFs4IE7xkEbVWUJVW8JWACjcxG0xvY0x0EWI
    xGrwACjcxG0xvY0x0EWIxGrVCF72vEw4AK0wACY4xI67k04243AVAKzVAKj4xxM4xvF2IE
```

从邮件头可以发现最开始发送邮件的 IP 地址为 180.110.209.251，归属地为中国/江苏/南京/浦口区，威尼斯水城(第四街区)。

当前IP	180.110.209.251
地理位置	中国/江苏/南京/浦口区
行为位置	中国/江苏/南京/浦口区
定位商圈	威尼斯水城(第四街区)
定位经纬度	118.74419,32.14371
运营商	chinatelecom.com.cn
线路	电信
应用场景	家庭宽带
地区中心经纬度	32.060255,118.796877

这可能是攻击者的网络出口地址，也可能是代理。

邮件最后一次转发投递是通过 106.75.129.30，归属地为中国 广东 广州。



归属地	中国 广东 广州	上报纠错
运营商	优刻云	
iP类型	数据中心	

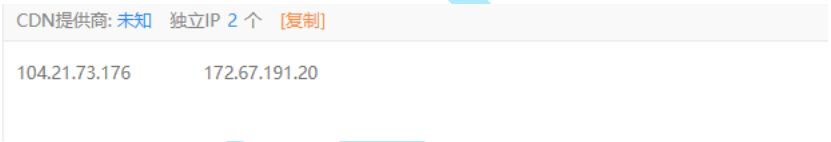
钓鱼链接

https://www.dbgfbsd56.top，在三月份开展溯源工作时，页面仍可以访问预览如下，而在此次报告发布时显示“没有找到站点”。

根据开源情报查询该域名发现确为恶意域名

相关恶意关联信息如下

查询该域名，对 www.dbgfbsd56.top 进行多 ping 后发现该域名存在 cdn，无法进行下一步的查询



附录 1 CACTER 邮件安全网关产品介绍

广东盈世计算机科技有限公司旗下品牌包含 Coremail 及 CACTER 邮件安全。2021 年，正式成立邮件安全事业部，专注于一站式解决所有邮件安全问题，产品涵盖邮件安全网关、CAC2.0 反钓鱼防盗号、邮件数据防泄露 EDLP、安全海外中继、重保服务、反钓鱼演练等。客户涵盖国务院新闻办公室、国家科技部、国家财政部、中科院、清华大学、北京大学、人民银行、建设银行、交通银行、华润集团、南方电网、美的集团等。

CACTER 邮件安全网关介绍

2021 年，Coremail 邮件安全事业部推出 CACTER 邮件安全网关，网关基于 CAC 大数据中心，实时拦截垃圾广告，钓鱼邮件，病毒邮件，BEC 诈骗邮件，拦截有效率达到 99.8%，支持邮箱品牌包括 Coremail、Exchange、O365、Gmail、IBM Domino、lotus notes。

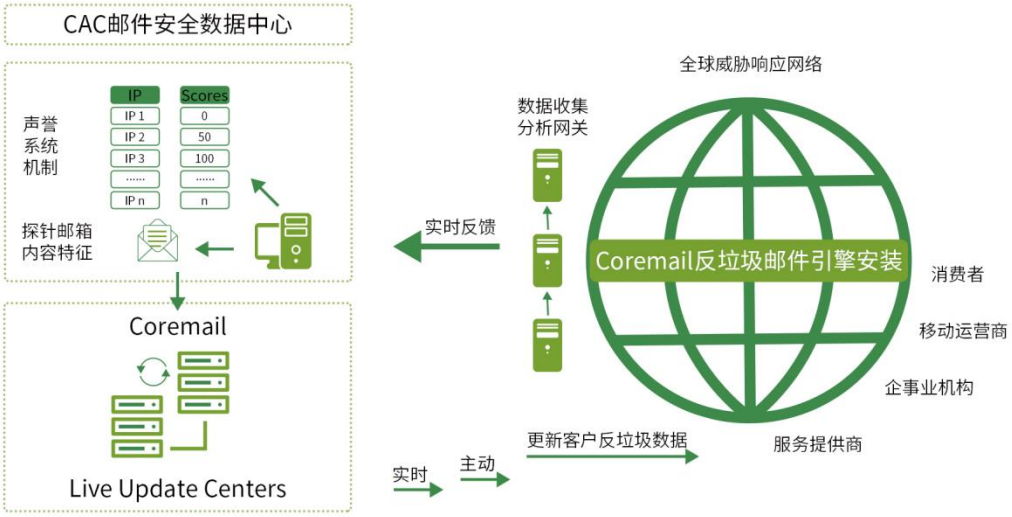
产品优势

1 恶意邮件精准隔离

CACTER 邮件安全网关融合了多项自主研发的世界领先级反垃圾邮件技术，并使用国内外知名反病毒引擎，对进入网关的邮件进行多维分析，确保钓鱼邮件、病毒邮件、垃圾邮件被隔离到网关，保障邮件系统不受恶意邮件威胁。

2 检测能力实时更新

CACTER 邮件安全网关拥有全国最大的邮件安全数据中心，基于数亿恶意邮件样本，通过部署百万探针邮箱搜集恶意邮件数据，实时更新邮件检测引擎规则，为客户提供最新邮件防护。



3 恶意链接保护

使用 CACTER 邮件网关后，管理员可开启恶意链接保护功能，对投往邮件系统的每一封邮件的链接进行保护。首次过滤+二次检测防护，事前拦截、事中提醒、事后追溯结合，为邮件系统的邮件安全保驾护航。

4 加密附件检测

病毒查杀：Coremail 与多家反病毒厂商合作，对邮件的附件进行多重查杀，同时，病毒库支持智能实时升级

附件检测：部分病毒邮件使用加密压缩的附件，能够绕过反病毒检测，如近期泛滥的 Emotet 病毒邮件攻击。

内容检测：CACTER 网关能够拆解文档类型的附件，包括 PDF、word、Excel 并执行文本指纹检查，有效识别附件型的垃圾邮件。

沙箱检测：网关内置云沙箱检测可在独立、隔离的环境中自动化检测恶意代码、可执行文件、恶意软件、判断是否有异常网络行为、创建进程等高级威胁。

5 邮件一键召回

主要针对新型变种威胁邮件绕过反垃圾反钓鱼反病毒引擎检查，甚至是云沙箱检测，

成功投递至邮件系统无法撤回时，企业管理员可以启用 CACTER 邮件安全网关的邮件召回功能，一键召回已经投递至邮件系统的威胁，守护邮箱系统安全最后一道防线。

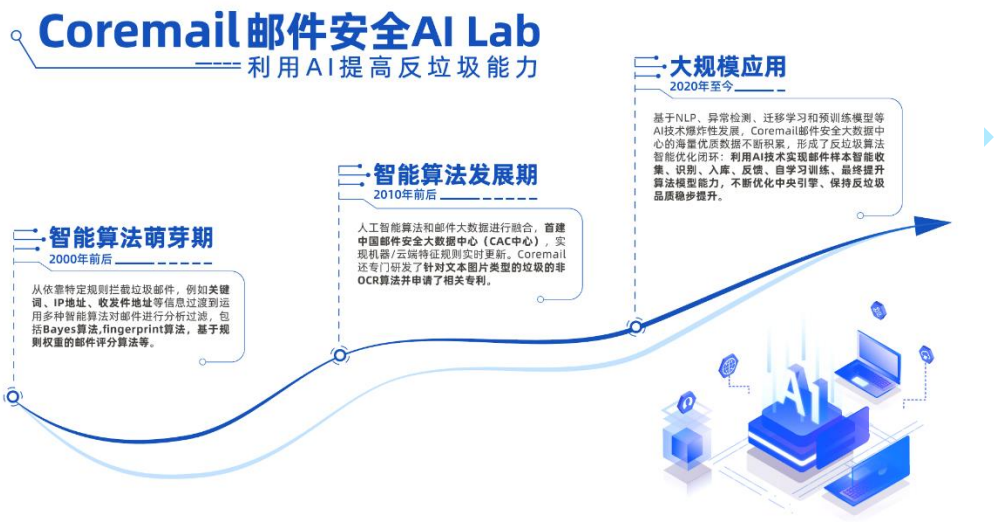
CACTER 邮件安全网关采用当今世界上先进的反垃圾邮件技术，包括自研算法——基于神经网络的垃圾邮件过滤算法、IP 信誉评估机制、实时邮件指纹检查、邮件评分技术、发信行为分析、机器学习算法等，经过多层次过滤，CACTER 邮件安全网关可以高达 99.8%的垃圾邮件拦截率，低于 0.02%的误判率。

多种部署，支持信创

CACTER 邮件网关可提供云/软件/硬件多种部署方式，为 Coremail、Exchange、O365、Gmail、IBM Domino、lotus notes 等市面主流邮件系统提供防护。

附录 2 邮件安全人工智能实验室介绍

Coremail 邮件安全人工智能实验室（Email Security AI Lab），依托于 Coremail 丰富的应用场景、海量大数据与一流科技人才，专注于将自然语言处理、计算机视觉、大型语言模型等 AI 智能技术应用于电子邮件安全防护领域的创新突破。



目前邮件安全人工智能实验室已在反垃圾领域取得可喜成果，形成了反垃圾算法智能优化闭环：基于 AI 技术实现邮件样本智能收集、识别、入库、反馈、自学习训练、最终提升算法模型能力，不断优化中央引擎、保持反垃圾品质稳步提升。