Coremail CACTER 奇安信 新一代网络安全领军者

2024 中国企业邮箱安全性研究报告

THE REPORT

2025年3月出品

Coremail CACTER

奇安信 新一代网络安全领军者

编写组

组长

林延中 裴智勇

主要编写人员

朱腾蛟 江嘉杰 黄楚斯

《中国企业邮箱安全性研究报告》由广东盈世计算机科技有限公司与奇安信集团联合为您提供，本联合报告的编撰获得了 Coremail 邮件安全人工智能实验室、Coremail 邮件安全大数据中心以及奇安信行业安全研究中心相关专家的悉心指导和宝贵建议，在此表示感谢。

主要观点

- 不论是从企业邮箱注册域名数、活跃用户数、还是邮件收发量等方面来看，国内企业级电子邮箱应用市场，都呈现出持续、稳定发展的态势。尽管垃圾邮件、钓鱼邮件的总量也有小幅增长，但带毒邮件数量已经呈现出逐年下降的趋势。这主要得益于邮件安全技术，特别是邮件反病毒技术的持续进步。
- 邮箱盗号问题仍然十分严重。2024 年，全国被盗企业邮箱账户多达 1074 万个，占全年活跃企业邮箱账号总量的 5.37%。由被盗企业邮箱账号发出的垃圾邮件多达 822.5 亿封。特别值得关注的是，邮箱盗号问题已经成为商业机密泄露、商业邮件诈骗等高危安全风险事件频发的重要诱因。同时，由“盗号”+“同域钓鱼”的攻击方式，也已经成为钓鱼邮件攻击的流行手段。
- 来自全球的邮件安全威胁仍然十分严峻。整体而言，全球垃圾邮件源呈现“核心收缩、边缘扩张”的态势，中美虽仍为主导但控制力减弱，东欧、东南亚等地区逐渐形成新的次级策源地，除 Top5 外的中小规模垃圾邮件源国在加速扩容，反监测技术扩散趋势明显。
- 邮箱账号盗取已形成了专门的黑色产业，盗号测试信是黑产盗取账号成功的重要标志；黑产暴力破解使用的口令字典，大部分通过目标邮箱账号名变形生成，其他占比达到 73.2%。
- 域名劫持技术被大范围应用于邮件攻击，预计未来几年内，此类攻击还有可能愈演愈烈。企业想要减少此类攻击造成的损害，应当在邮件防护系统中谨慎设置邮箱域名的白名单。
- 生成式 AI 成钓鱼邮件内容重要生产者，越来越多的攻击者正在使用生成式 AI，更加快速地制作更有针对性的恶意邮件文案内容。邮件攻击者，开始采用 AI 技术进行自动化的邮件攻击，主要体现在目标人群选择、投放策略制定和口令爆破攻击等方面。

摘　要

- 截至 2024 年底，国内注册的企业邮箱独立域名约为 530 万个，活跃的国内企业邮箱用户规模约为 2 亿。
- 2024 年，全国企业邮箱用户共收发各类电子邮件约 8188.4 亿封。其中，正常邮件占比 46.8%、普通垃圾邮件 38.3%、钓鱼邮件 9.2%、带毒邮件 5.4%、谣言邮件 0.08%，色情、赌博等违法信息推广邮件约 0.17%。
- 从正常邮件的发送量上来看，工业制造类企业全年发送的邮件数量最多，约为全国邮件发送总量的 18.7%，排名第一；交通运输占比 16.7%，排名第二；其次是媒体占比为 12.6%；教育培训、IT 信息技术、互联网等也都是邮件发送量较多的行业。
- 从域名归属来看，国内企业邮箱收到的所有垃圾邮件、钓鱼邮件和带毒邮件，美国都是最大的海外发送源。同时，自 2022 年以来，俄罗斯、乌克兰也成为头部的恶意邮件发送源。
- 2024 年，由于某些中文邮件黑产团伙的突然活跃，国内企业邮箱收到的钓鱼邮件数量同比大幅增长 30.8%。年度最为流行的三种钓鱼邮件类型分别是补贴/退税（32.1%）、升级/扩容（25%）和身份验证/备案（15.6%），三者之和占到了所有钓鱼邮件总量的 72.7%。
- 2024 年，国内电子邮箱账号被盗规模高达 1074 万个，占全年活跃邮箱账号总量的 5.37%；暴力破解是邮箱盗号最主要的手段，占到 2024 年邮箱异常登录行为检出总量的 53.7%；由被盗号的电子邮箱发出的垃圾邮件，占到国内企业邮箱收到的所有垃圾邮件总量的 26.2%。
- 黑产暴力破解最常使用的工具为 sanmao SmtpCracker.exe，占 54.9%。同时该工具应为国内黑产使用的最主要暴力破解工具。黑产暴力破解使用的 IP 国内和国外数量接近。黑产国内 IP 资源呈现明显的地区聚集性，集中于江苏、湖北、辽宁三个省份，其中江苏省达 45.8%。
- 除了生成式 AI 钓鱼内容之外，监测显示，已经有越来越多的邮件攻击者，开始采用 AI 技术进行自动化的邮件攻击，主要体现在目标人群选择、投放策略制定和口令爆破攻击等方面。

关键词：企业邮箱、垃圾邮件、钓鱼邮件、带毒邮件、暴力破解、生成式 AI、域名攻击

目　　录

研究背景

在中国当前网络空间形势下，社交网络日益发达，电子邮件发展至今已有几十年历史，但仍是最重要的现代互联网应用之一。从个人生活到工作场景的使用，邮件都在现阶段人们的生活中扮演着不可或缺的角色。近年来中国企业信息化办公程度逐年升高，更是大大促进了企业邮箱的使用，同时也使企业邮箱系统成为黑客入侵机构内部网络的首选入口。

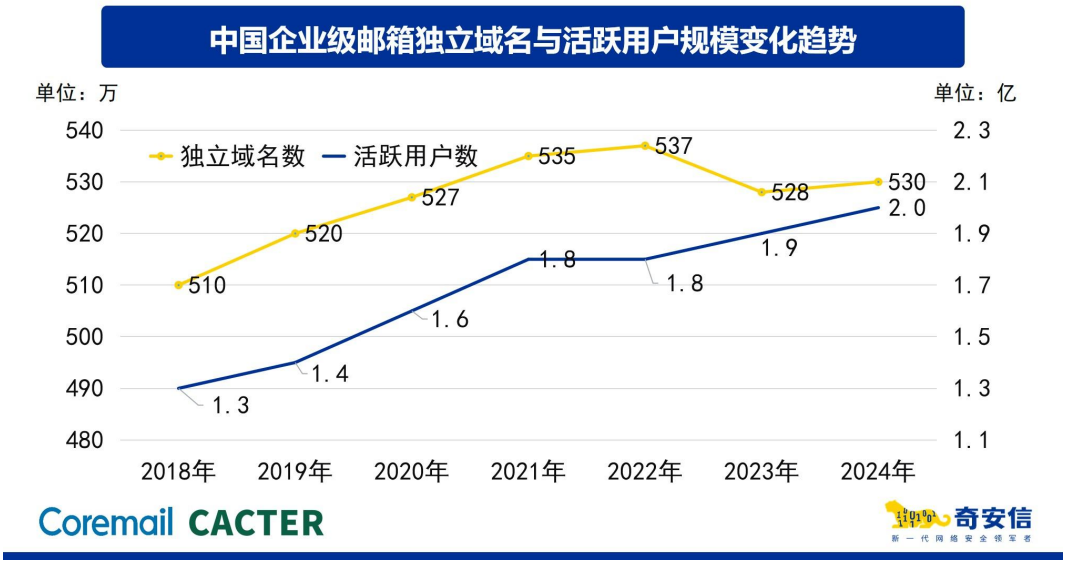
针对邮件系统在使用时存在的问题，奇安信行业安全研究中心联合 Coremail 邮件安全人工智能实验室、CACTER 邮件安全研究团队，自 2016 年起合作编撰《中国企业邮箱安全性研究报告》，截至今年已连续发布十年。报告数据主要来自 Coremail 与奇安信集团联合监测，报告内容以电子邮箱的使用、垃圾邮件、钓鱼邮件、带毒邮件为主体，从规模、发送源、受害者及典型案例等方面分析中国企业邮箱安全性。

本报告结合了 Coremail、CACTER 邮件安全与奇安信集团多年在企业邮箱领域的丰富实践经验及研究经验，相关研究成果具有很强的代表性。希望此份报告能够对各个行业、单位，开展以邮件防护为基础，增强完善整体网络安全建设，提供一定参考。

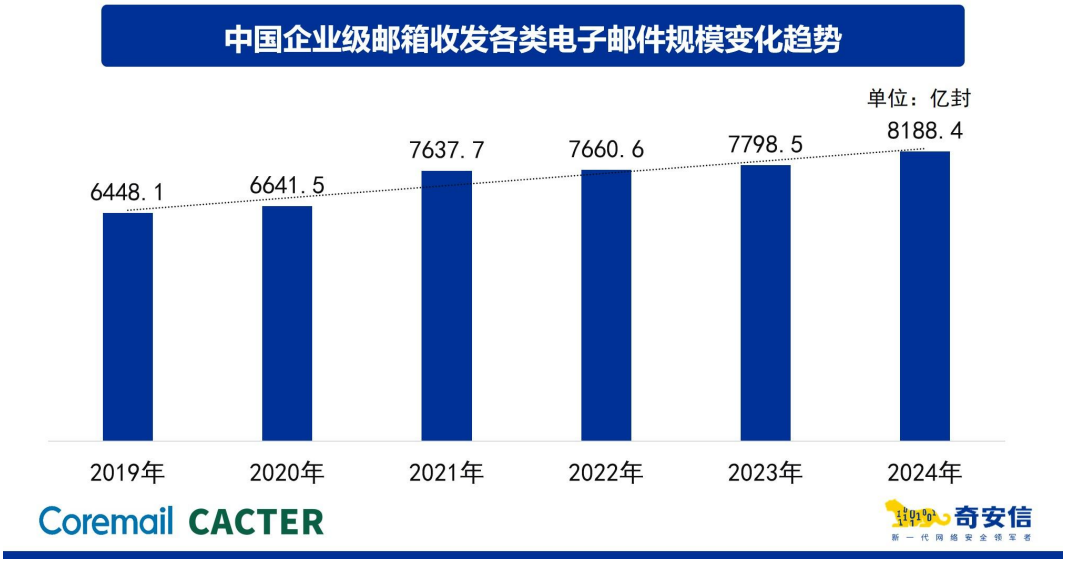
第一章 电子邮箱应用形势

一、 电子邮箱的使用规模

根据 Coremail 邮件安全人工智能实验室与奇安信行业安全研究中心的联合监测，同时综合网易、腾讯、阿里巴巴等主流企业邮箱服务提供商的公开数据进行分析评估，截止 2024 年底，国内注册的企业邮箱独立域名约为 530 万个，相比 2023 年的 528 万个增长了 0.4%。活跃的国内企业邮箱用户规模约为 2 亿，与 2023 年用户规模相比增长约 5.3%。2018 年至 2024 年国内企业级电子邮箱独立域名与活跃用户规模变化趋势如下图所示：



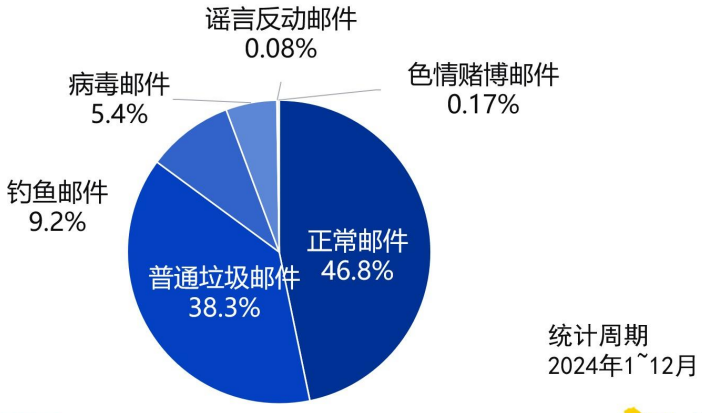
从电子邮箱的使用情况来看，2024 年，全国企业级邮箱用户共收发各类电子邮件约 8188.4 亿封，同比增长了 4.8%，日均收发电子邮件约 22.4 亿封。



其中，正常邮件占比约为 46.8%、普通垃圾邮件占比为 38.3%、钓鱼邮件 9.2%、带毒

邮件 5.4%、谣言邮件 0.08%，色情、赌博等违法信息推广邮件约 0.17%。与 2023 年相比钓鱼邮件占比增长了 1.8 个百分点；病毒邮件、谣言类邮件、色情赌博类邮件的占比均有明显下降；正常邮件和普通垃圾邮件的占比变化不大。

中国企业级电子邮箱用户收发邮件类型分布

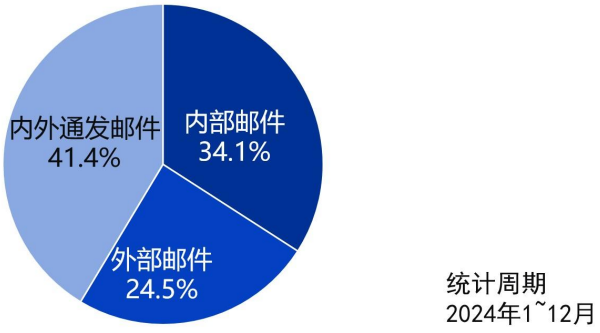


Coremail CACTER
奇安信 新一代网络安全领军者

仅就正常邮件而言，统计显示，全国企业邮箱用户在 2024 年共收发正常电子邮件约 3828.9 亿封，比 2023 年增长 7.2%，平均每天收发正常电子邮件约 10.5 亿封。

不同于个人邮箱，企业邮箱的主要用途是办公。因此，同一机构内部邮件互发往往会比较频繁。抽样统计显示，2024 年企业用户发送的电子邮件中，约 34.1%为机构内部邮件，24.5%为外部邮件，41.4%为内外通发邮件（收件人既有机构内部，也有机构外部）。

中国企业级邮箱用户发送内、外部邮件比例分布



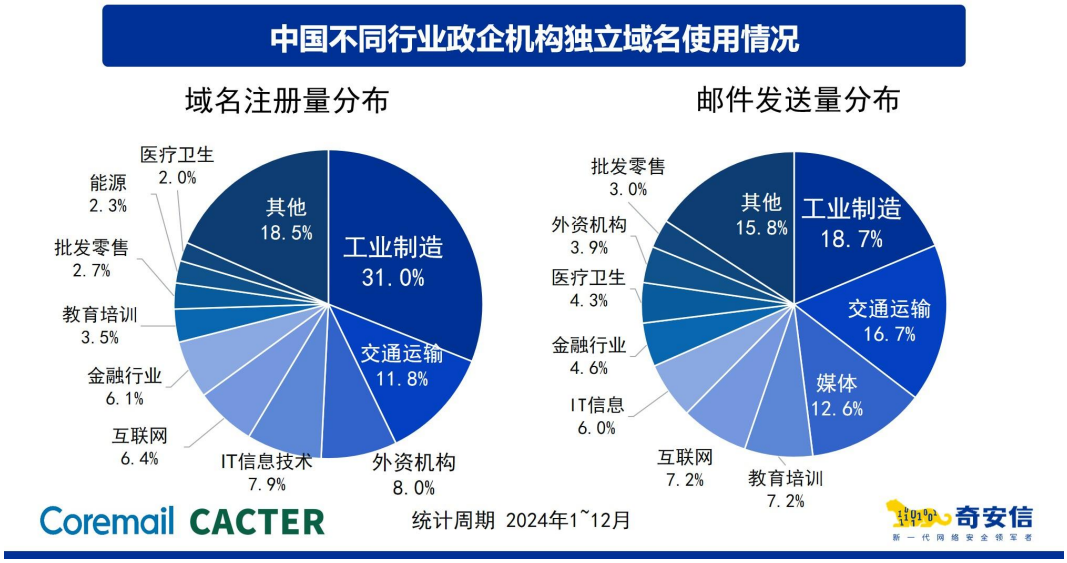
Coremail CACTER
奇安信 新一代网络安全领军者

二、 电子邮箱用户行业分布

对中国政企机构独立邮箱域名的抽样分析显示，从域名注册量来看，工业制造类企业注册的邮箱域名最多，占比为 31%，其次是交通运输行业占比 11.8%，外资机构占比 8%；还有 IT 信息技术占比 7.9%，互联网企业占比 6.4%，金融行业占比 6.1%等，这些都属于电子

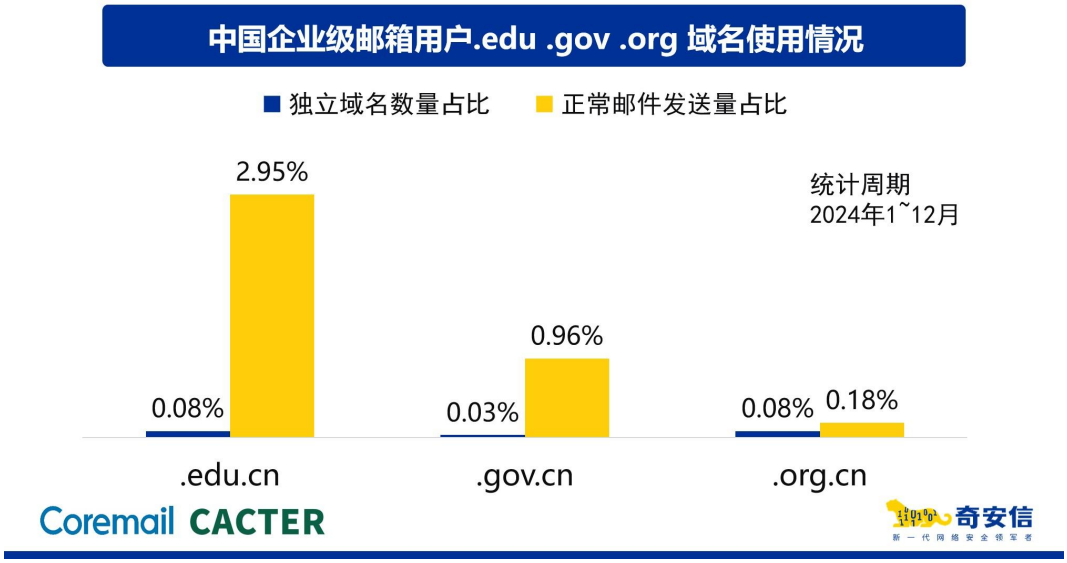
邮箱使用独立域名较多的行业。

如果从正常邮件的发送量上来看，工业制造和交通运输行业发送的邮件数量最多。工业制造类企业全年发送的邮件数量，约为全国邮件发送总量的 18.7%，排名第一；交通运输占比 16.7%，排名第二；其次是媒体占比为 12.6%；教育培训、互联网、IT 信息等也都是邮件发送量较多的行业。具体占比如下图所示：



对比独立邮箱域名注册量和邮件发送量，可以看出，就单个政企机构而言，媒体、教育培训与医疗卫生等行业对邮件办公的依赖度最高。

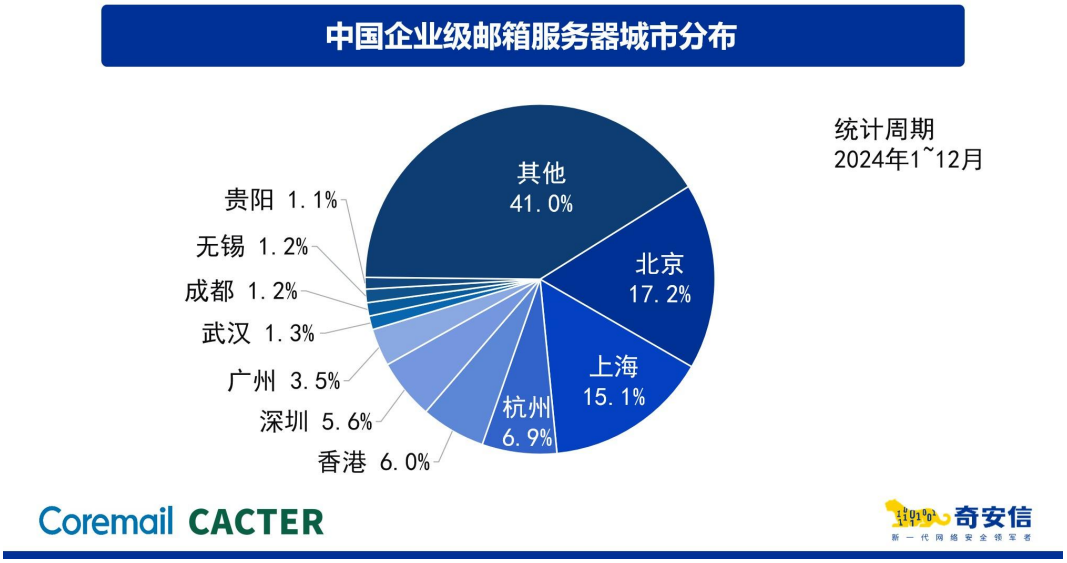
特别的，本次报告对.edu（教育）、.org（组织机构）和.gov（政府）三个域名的邮箱使用情况进行了分析。其中，.edu.cn 邮箱域名在全国占比为 0.08%，.org.cn 的邮箱域名占比约为 0.08%，.gov.cn 邮箱域名占比为 0.03%。而从正常邮件发送量上来看，.edu.cn 邮箱占 2.95%，.gov.cn 邮箱占 0.96%，.org.cn 邮箱占 0.18%。



三、 电子邮件的地域分布

统计显示，2024 年全国企业邮箱用户收发的邮件以境内收发为主。国内收发占 73%；海外收发 27%。

从服务器的所在地来看，2024 年，国内企业邮箱服务器设在北京的数量排名第一，占比为 17.2%；上海排第二，占比为 15.1%；杭州排名第三，占比 6.9%。



四、 电子邮件安全防护重要性

2024 年，全国企业邮箱日均收发量达 22.4 亿封，其中钓鱼邮件（9.2%）、带毒邮件（5.4%）等恶意内容占比近 15%，日均威胁量超 3.3 亿封。尽管病毒、谣言类邮件比例下降，但钓鱼邮件同比激增 1.8 个百分点，攻击手段持续复杂化。此类高风险邮件可能导致商业机密泄露、财务欺诈甚至关键系统瘫痪，对高度依赖邮件办公的行业（如媒体、教育、政府）冲击尤为显著。

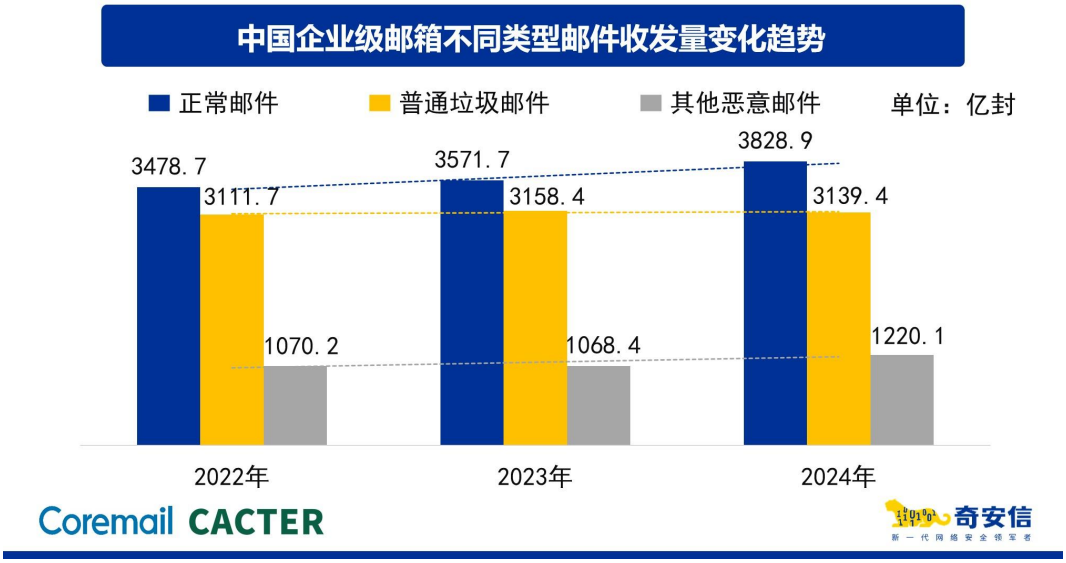
值得注意的是，.edu（教育）、.gov（政府）等敏感域名虽注册量不足 0.1%，但邮件发送量占比显著（如.edu.cn 占正常邮件 2.95%）。这类机构作为公共信息枢纽，一旦安全防线失守，不仅会引发敏感数据外泄，更可能削弱公众对数字政务、在线教育等服务的信任基础。

由此可见，强化邮件安全防护（如反钓鱼技术、内容过滤）对维护企业持续运营、保护用户信息安全、保障社会网络空间稳定愈发重要。

第二章 垃圾邮件形势分析

一、 垃圾邮件的规模

根据 Coremail 邮件安全人工智能实验室与奇安信行业安全研究中心的联合监测评估，2024 年，全国企业邮箱用户共收到各类普通垃圾邮件 3139.4 亿封，约占企业级用户邮件收发总量的 38%，是企业级用户正常邮件数量的 82%。普通垃圾邮件的收发量下降，而其他恶意邮件的收发量增多。具体分布如下图所示：



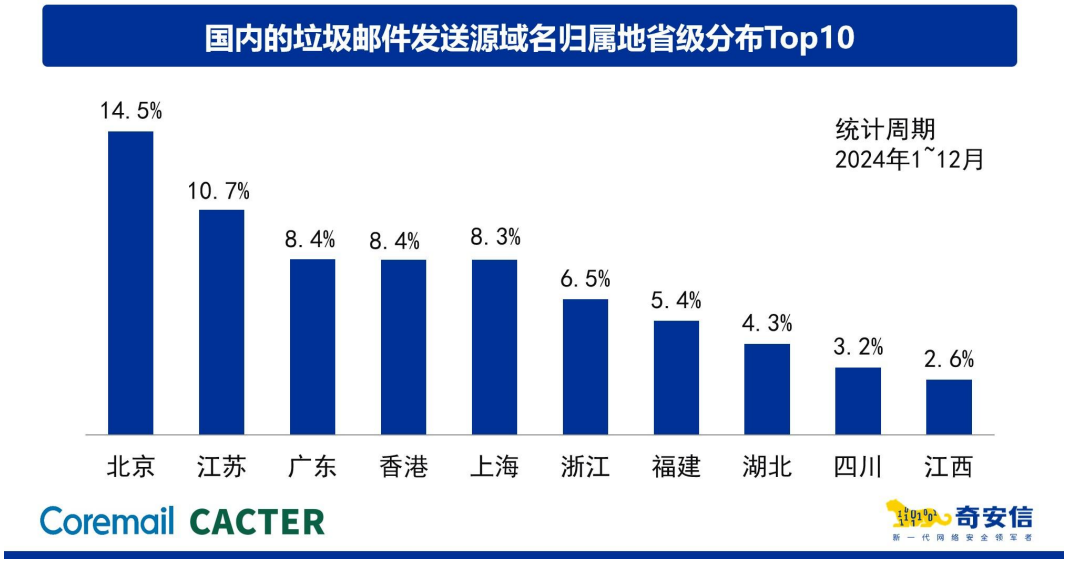
二、 垃圾邮件发送源

从发送者邮箱域名归属情况来看，2024 年，全国企业邮箱收到的垃圾邮件中，来自国内的垃圾邮件最多，占总数的 35.5%，来自美国的垃圾邮件次之，占总量约 17.7%，第三是俄罗斯，约占 5.9%。下表给出了按照垃圾邮件数量统计的，历年垃圾邮件发送源国别归属排行 Top5。整体而言，全球垃圾邮件源呈现“核心收缩、边缘扩张”的态势，中美虽仍为主导但控制力减弱，东欧、东南亚等地区逐渐形成新的次级策源地，“其他”国家合计占比从 27.1%增至 30.3%，表明除 Top5 外的中小规模垃圾邮件源国在加速扩容，反监测技术扩散趋势明显。

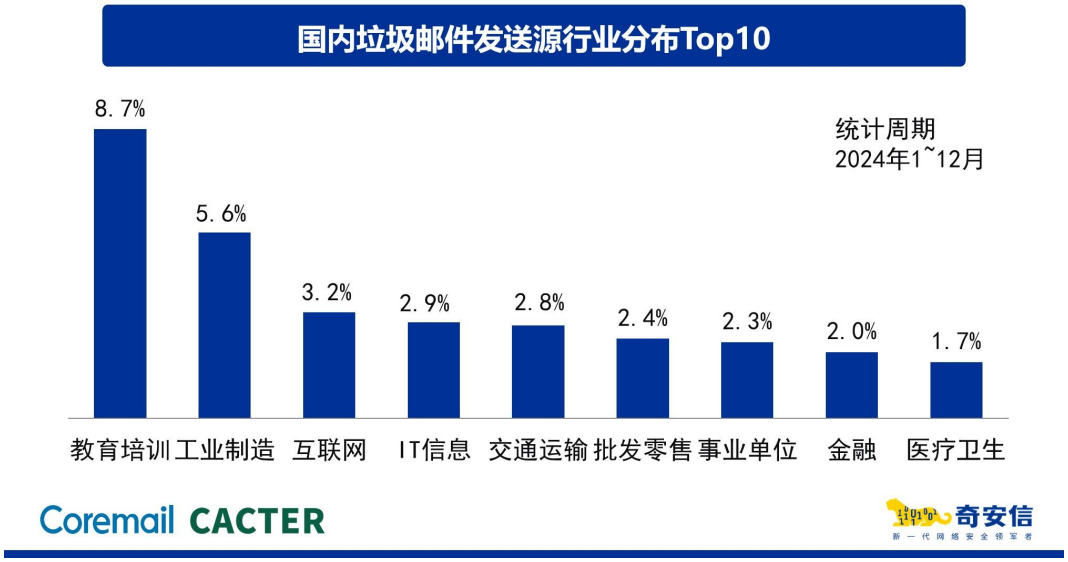
表 1 历年垃圾邮件发送源国别归属排行 Top5（按照垃圾邮件数量统计）

	2022 年		2023 年		2024 年	
排名	国家	占比	国家	占比	国家	占比
1	中国	41.9%	中国	38.6%	中国	35.5%
2	美国	19.4%	美国	20.4%	美国	17.7%
3	俄罗斯	6.7%	俄罗斯	7.2%	俄罗斯	5.9%
4	英国	1.9%	乌克兰	3.7%	乌克兰	3.0%
5	乌克兰	1.9%	英国	2.8%	英国	2.3%
	其他	28.3%	其他	27.1%	其他	30.3%

仅就国内情况来看，从发送者的域名归属地来看，来自北京的垃圾邮件发送者最多，占国内垃圾邮件发送总量的 14.5%，其次为江苏，占比 8.4%，广东排第三，占比 8.4%。下图给出了国内垃圾邮件发送源域名归属省份 Top10 及其垃圾邮件发送量占比情况：



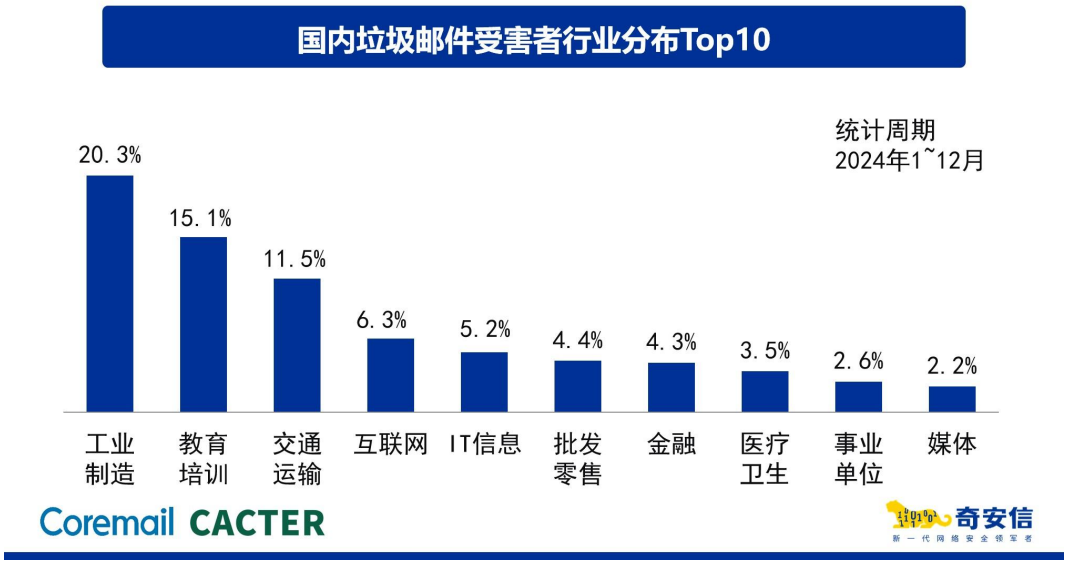
对发送垃圾邮件的邮箱域名进行抽样行业分析显示，2024 年，国内垃圾邮件发送源中教育培训占比最高，为 8.7%；其次为工业制造类企业 ，占比 5.6%；互联网企业排名第三，占比 3.2%。下图给出了国内垃圾邮件发送源行业分布：



三、 垃圾邮件受害者

从收到垃圾邮件的受害者服务器所在地来看，2024 年北京用户收到的垃圾邮件最多，共收到了占比高达全国 17.9%的垃圾邮件；其次为广东，收到了全国 14.3%的垃圾邮件；上海排名第三，收到了全国 13.1%的垃圾邮件。下图给出了国内企业邮箱用户中垃圾邮件受害者的省级行政区分布 Top10。

国内垃圾邮件受害者所在行业也比较集中，排名前十的行业收到的垃圾邮件数量，占垃圾邮件总数的 73.5%。其中，工业制造行业排名第一，约占垃圾邮件总数的 20.3%；教育培训排名第二，约占 15.1%；排名第三的行业为交通运输，占 11.5%。具体 Top10 行业排名如下图所示。



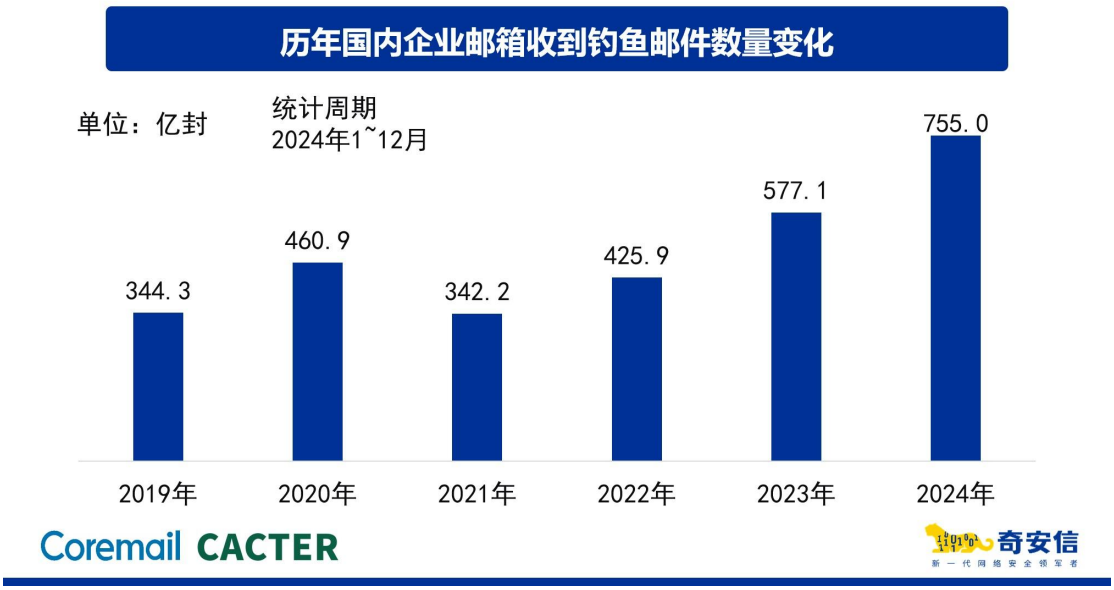
第三章 钓鱼邮件形势分析

一、 钓鱼邮件的规模

在本章内容中，钓鱼邮件是指含有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。

其中，鱼叉邮件是指针对特定目标投递特定主题及内容的欺诈电子邮件。相比一般的钓鱼邮件，鱼叉邮件往往更具迷惑性，同时也可能具有更加隐秘的攻击目的。而钓鲸邮件则是指那些专门针对企业高管或重要部门进行的鱼叉邮件攻击。而 CEO 仿冒邮件则是指冒充企业高管对公司员工或某些部门进行的鱼叉邮件攻击。

根据 Coremail 邮件安全人工智能实验室与奇安信行业安全研究中心的联合监测评估，2024 年，全国企业邮箱用户共收到各类钓鱼邮件约 755.0 亿封，相比 2023 年收到各类钓鱼邮件的 577.1 亿封增加了 30.8%。网络钓鱼攻击事件逐年增加，钓鱼邮件数量在 2021 年短暂抑制后，持续迅猛增长。



钓鱼邮件作为网络攻击最常用的手段，可以说是自电子邮件诞生以来一直存在的安全威胁。2024 年全国企业邮箱用户收到的钓鱼邮件数量约占企业级用户邮件收发总量的 9.2%，平均每天约有 2.1 亿封钓鱼邮件被发出和接收。换种说法，即平均每个企业邮箱用户每月会收到约 31 封钓鱼邮件。

二、 钓鱼邮件发送源

根据 Coremail 邮件安全人工智能实验室与奇安信行业安全研究中心联合监测，钓鱼邮件的发送者遍布全球，其中，来自中国的钓鱼邮件最多，占国内企业用户收到钓鱼邮件总量的 42.9%；其次是美国，约占 13.9%；俄罗斯排名第三，约占 8.4%。下表给出了按照钓鱼邮件数量统计的，历年钓鱼邮件发送源国别归属排行 Top5。

表 2 历年钓鱼邮件发送源国别归属排行 Top5（按照钓鱼邮件数量统计）

	2022 年		2023 年		2024 年	
排名	国家	占比	国家	占比	国家	占比
1	美国	31.50%	中国	48.40%	中国	42.90%
2	中国	18.40%	美国	12.40%	美国	13.90%
3	俄罗斯	3.30%	俄罗斯	7.90%	俄罗斯	8.40%
4	英国	3.10%	乌克兰	2.70%	荷兰	2.60%
5	罗马尼亚	2.90%	西班牙	1.80%	新加坡	2.50%
	其他	40.80%	其他	26.80%	其他	29.70%

可以看出，2024 年，来自国内发送源的钓鱼邮件数量占比虽小幅下降至 42.9%，但仍稳居第一。具体来看，以下几个因素是导致这一情况出现的主要原因：

1. 新的中文邮件黑产团伙出现。自 2023 年第三季度开始，有大量专门针对中文用户的钓鱼邮件黑产团伙开始变得活跃，一直持续到 2024 年，从而导致来自国内的钓鱼邮件数量占比快速增长。

2. 新的攻击节点被利用。2024 年出现了大量通过我国香港地区服务器发送的钓鱼邮件，黑产团伙通过香港地区作为新的攻击节点，发动了大规模的钓鱼攻击，严重威胁到企业用户的信息安全。

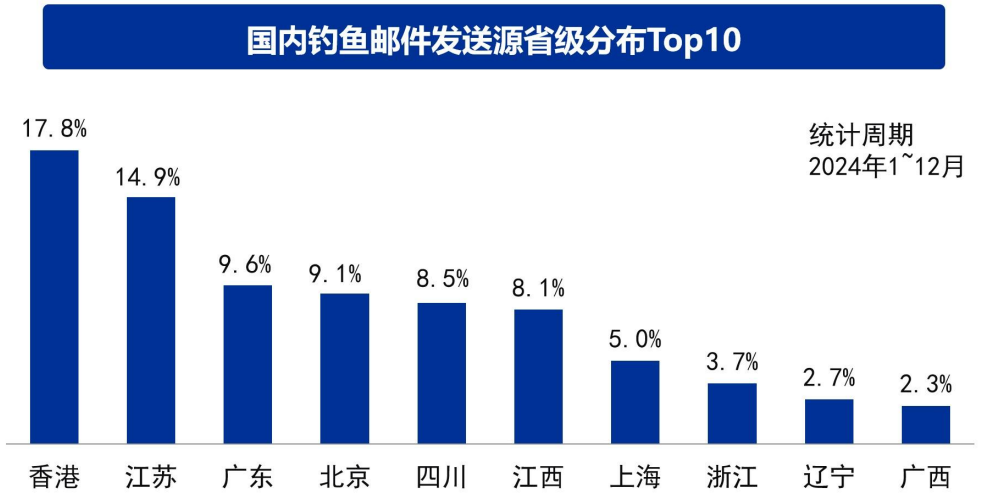
3. 生成式 AI 加剧钓鱼邮件威胁。快速发展的生成式人工智能显著提升了钓鱼攻击的复杂度与隐蔽性，攻击者通过 AI 自动化生成发送高度拟人化的钓鱼邮件，精准模仿企业/个人语言风格，实现低成本而高成功率的攻击链。这种动态演进的威胁模式对传统防御策略提出了更高的挑战，推动企业与安全厂商加速研发 AI 驱动的防御工具以应对持续升级的威胁。

4. 云服务平台滥用问题依旧。虽然有部分云服务平台在用户的持续举报中加强了安全监管，但仍有不少漏洞被黑产团伙钻了空子，导致钓鱼邮件泛滥。

5. 盗号问题依旧严峻。大量被入侵的境内设备（如物联网设备、个人电脑等）被用作钓鱼邮件发送节点。

上述多种因素，最终也导致 2024 全年钓鱼邮件数量有一个明显的增长。

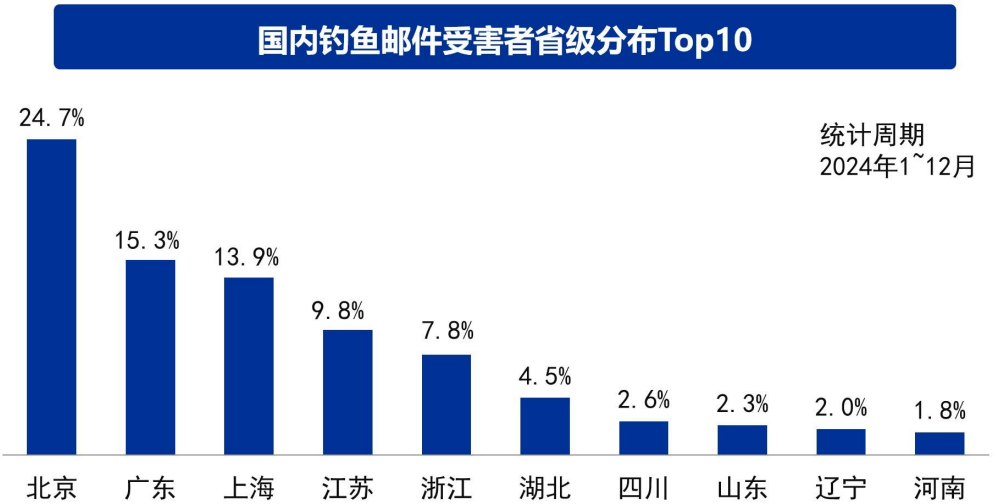
从国内钓鱼邮件发送源的服务器所在地来看，香港特别行政区超越了江苏省成为国内发送钓鱼邮件最多的省级行政区，有 17.8%的钓鱼邮件来自香港的邮箱；江苏的钓鱼邮件活动依旧活跃，有约 14.9%的钓鱼邮件来自江苏；另有约 9.6%的钓鱼邮件来自广东。国内钓鱼邮件发送源发送钓鱼邮件数量 Top10 省级行政区分布如下图所示：



Coremail CACTER
奇安信 新一代网络安全领军者

三、 钓鱼邮件受害者

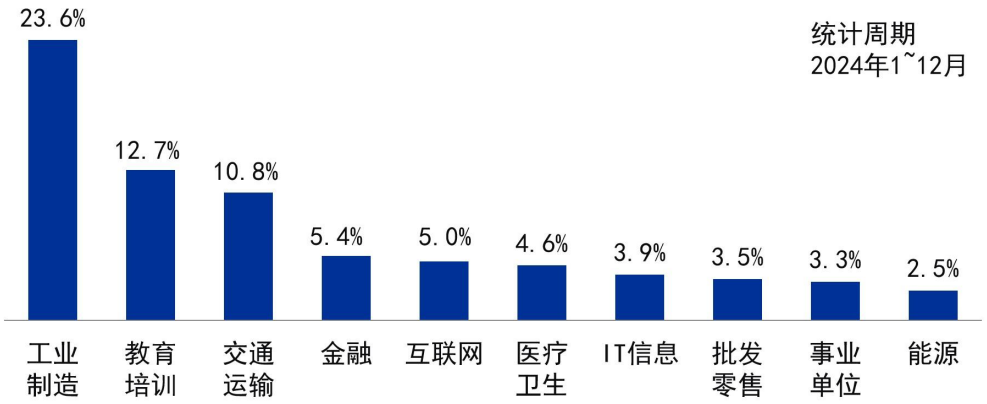
从收到钓鱼邮件的受害者服务器所在地来看，北京用户收到的钓鱼邮件最多，有 24.7%的钓鱼邮件被发送至北京的企业邮箱用户；另有约 15.3%的钓鱼邮件被发送给广东用户；约 13.9%的钓鱼邮件被发送给上海用户。2024 年国内钓鱼邮件受害者数量 Top10 省级行政区分布如下图所示：



Coremail CACTER
奇安信 新一代网络安全领军者

国内钓鱼邮件受害者所在行业也比较集中，排名前十的行业收到的钓鱼邮件数量，占钓鱼邮件总数的 75.3%。其中，工业制造行业排名第一，约占钓鱼邮件总数的 23.6%；教育培训排名第二，约占 12.7%；排名第三的行业为交通运输，占 10.8%。具体 Top10 行业排名如下图所示。

国内钓鱼邮件受害者行业分布Top10



Coremail CACTER
奇安信 新一代网络安全领军者

四、 钓鱼邮件年度主题榜

从主题分布榜单分析，当前钓鱼邮件攻击呈现两个显著特征：一是以系统通知类主题为主导诱骗方式，通过模仿正规邮件系统的服务提醒实施定向欺诈；二是日文语言类钓鱼邮件数量呈现爆发式增长，显示攻击者正针对特定语言群体进行精准化渗透。

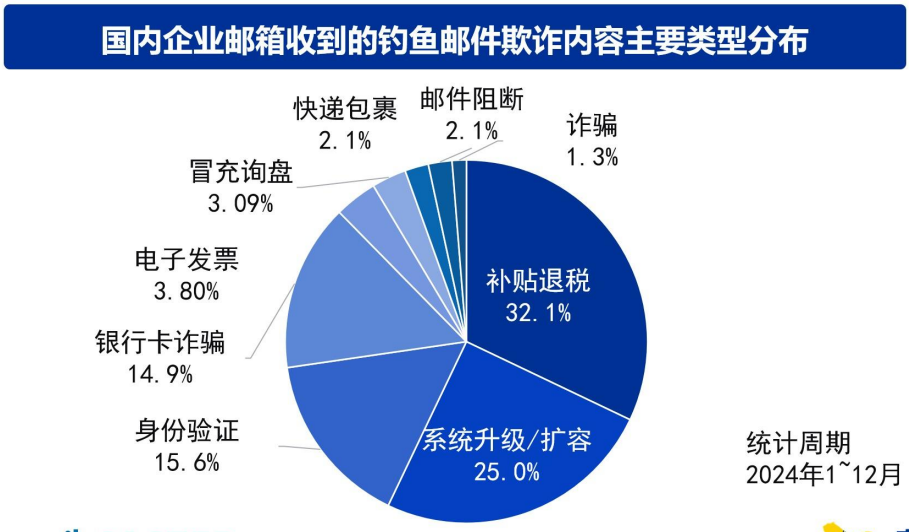
2024年热门钓鱼邮件主题榜TOP15

序号	主题	主题（中文翻译）	邮件数
1	OA迁移升级	OA迁移升级	606.9万
2	关于邮件系统的通知	关于邮件系统的通知	393.4万
3	关于电子邮件系统升级的通知	关于电子邮件系统升级的通知	355.1万
4	【アイフル株式会社】回答をお願いいたします。	[Aiful Corporation]请告诉我们您的答案。	318.7万
5	关于电子邮件系统升级的通知	关于电子邮件系统升级的通知	272.2万
6	邮件管理系统通知	邮件管理系统通知	222.9万
7	OA迁移升级	OA迁移升级	215.1万
8	カードご利用内容の確認のお願い	请求确认卡使用详情	213.3万
9	异常提醒	异常提醒	197.3万
10	10月ご請求額のお知らせ	10 月份账单金额通知	194.1万
11	安全通知	安全通知	192.9万
12	邮箱异常登录提醒	邮箱异常登录提醒	184.6万
13	公司内部通知	公司内部通知	175.7万
14	【ORICO CARD】お取引のご確認	[ORICO CARD] 确认您的交易	162.0万
15	お支払い日のご案内	付款日期信息	160.4万

Coremail CACTER
奇安信 新一代网络安全领军者

五、 钓鱼邮件的类型

从具体内容来看，2024 年流行的钓鱼邮件主要有 8 种类型，分别是：补贴/退税、升级/扩容、身份验证/备案、银行卡信息诈骗、虚假发票、冒充询盘、虚假快递、系统退信。其中，补贴/退税类钓鱼邮件数量最多，占比约为 32.1%；其次是升级/扩容类钓鱼邮件，占比约为 25.0%；身份验证/备案类钓鱼邮件排第三，占比约为 15.6%。Top3 之和占到了所有钓鱼邮件总量的 72.7%。具体分布，详见下图。



Coremail CACTER
奇安信 新一代网络安全领军者

下面将对 2024 年流行的钓鱼邮件类型做详细说明并举例。

1. 补贴/退税

这是一类专门冒充国家有关部门或公司人力资源部门，打着给员工发放补贴、办理退税等借口，诱骗企业员工登录钓鱼网站，以骗取受害人个人信息的钓鱼邮件。下面几图是此类钓鱼邮件的真实案例。

2. 升级/扩容

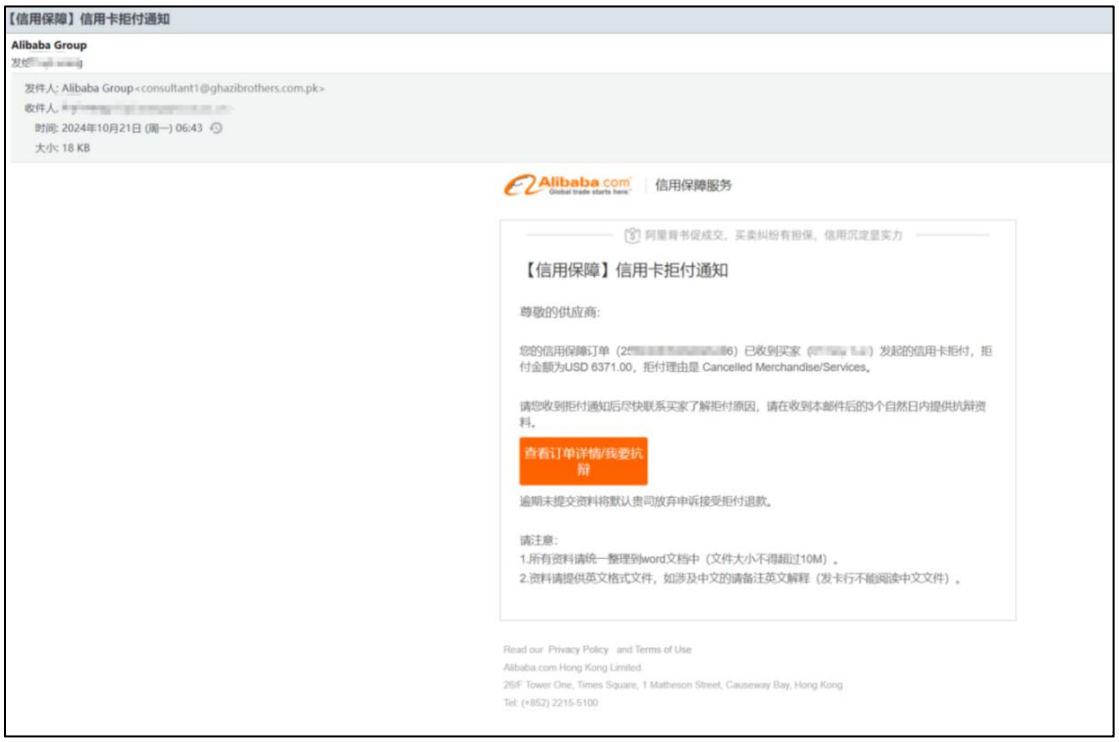
这是一类专门以系统升级或系统扩容等理由，诱骗受害者在钓鱼网站上登录，从而盗取受害者账号、口令等信息的钓鱼邮件。下面几图是此类钓鱼邮件的真实案例。

3. 身份验证/备案

这是一类专门诱骗受害者在虚假的钓鱼网站上，进行身份验证或身份备案的钓鱼邮件，目的是盗取受害者的账号、口令和个人信息。此类邮件诱骗受害者的理由多种多样，最为常见的是以保护邮件系统安全性为由要求用户进行身份验证/备案，具体理由包括但不限于离职员工邮箱管理、账号密码重置、异常登录通知等。下面几图是此类钓鱼邮件的真实案例。

4. 银行卡信息诈骗

这是一类冒充银行或者支付平台，以银行卡信息需要验证、支付功能故障、信用卡到期等为借口，诱导收件用户进入钓鱼链接，以骗取受害人个人信息及钱财的钓鱼邮件。下面几图是此类钓鱼邮件的真实案例。



5. 虚假发票

这是一类专门通过发送虚假发票信息，诱骗受害者下载电子发票，从而盗取受害者个人信息和公司财务信息的钓鱼邮件。其中，还有部分此类邮件诱导受害下载的所谓电子发票，实际上是木马、病毒等恶意程序。

需要说明的是，由于电子发票目前在生活、工作中的应用非常广泛，所以不论是单位或个人，收到电子发票相关的邮件，一般都不会感到意外，下载发票或点开附件都是常事。但如果总是习惯性地忽视正常发票邮件中可能夹杂的钓鱼邮件，就有可能给个人或企业造成重大的损失。下面几图是此类钓鱼邮件的真实案例。

陈海涛9FyaaZ8c
鄞州区EYFp <ccknvrtvcx@outlook.com> 2024-01-04 17:23:19
发送至 [redacted]；

发件人 鄞州区EYFp <ccknvrtvcx@outlook.com>
收件人 "ya[redacted]" <y[redacted]>；
时 间 2024-01-04 17:23:19
大 小 24.7 KB

[redacted]责任公司 纳税识别号：913[redacted]4Y6K

企业漏申报个税：

税务通知企业漏申报个税，详情点击以下链接预览和下载：

《复制链接到浏览器打开》

https://pan.tencent.com/web/[redacted]4113

企业开票地址：[redacted]1

2024/01/02

您的电子发票（发票号码：4738837620470）已开具
百旺云 <lucas7407@bmroc.com> 2024-04-12 13:15:26
发送至 fs3d；

发件人 百旺云 <lucas7407@bmroc.com>
收件人 [redacted]；
时 间 2024-04-12 13:15:26
大 小 19.4 KB

百旺金穗云
财税服务平台

尊敬的，

[redacted]团有限公司给您开具了电子发票，请查收。

发票信息

开票日期：2024-4-12
销方名称：亿天产业投资集团有限公司
购方名称：
金额合计：3520.00 元
发票代码：044002200411
发票号码：92605996
为了避免发票丢失,请在30天内领取 请 （点击下载）

百旺金穗云
企业一站式财税服务平台
为您提供综合性智能票财税服务

财税代理
提供代理记账、代理申报、代理开票服务

票财税云服务
提供云开票、云财务、预申报接入一体化服务

财务共享
提供税务共享、费控管理解决方案，
数字化、集中式解决财税问题

6. 虚假快递

这是一类专门冒充快递公司，以结算、包裹等名义发出的钓鱼邮件。此类邮件或者是夹带恶意附件，或者是通过钓鱼网站链接盗取受害者个人信息。

下图是此类钓鱼邮件的真实案例。

7. 其他诈骗邮件

除了上述最为典型的 6 种钓鱼邮件外，2024 年，还有其他很多不同类型的诈骗邮件出现。不过由于整体数量不大，这里不再做详细分类，只是把一些典型案例做个举例。

下图是声称你侵权需要你在线申诉的钓鱼邮件。


【重要】涉嫌盗用图片【超时未响应】

alibabanotice 代表 ALIBABA NOTICE

发件人: alibabanotice<alibabanotice@sentry.nash.io> 代表 ALIBABA NOTICE<ALIBABA NOTICE>

收件人

时间: 2024年11月21日 (周四) 05:39

大小: 15 KB

尊敬的

HY收到商家投诉您涉嫌盗用图片构成不当侵权，投诉时间：2024-11-18，投诉编号为：457 447。

由于您在接到我司通知未在有效时间内及时进行申诉，故已经确认删除此被投诉信息，并根据阿里巴巴国际站盗图规则：[https://rule.alibaba.com/rule/detail/7768.htm?spm=a381m.8038972.0078789909.4.788e880bFZDEE] 对您做出相应处理。

具体请点击 申诉页面 登录账号进行查看并申诉。

申诉时间限制：第一次：3个工作日（阿里发送投诉通知起3个工作日内）。第二次：7个工作日（第一次申诉失败后7个工作日内）。第三次：7个工作日（第二次申诉失败后7个工作日内）。
注：若客户没有在规定时限内发起申诉，则等同于申诉失败。

此信由系统自动发出，请勿直接回复。

感谢您的及时关注。

阿里巴巴国际站

下图是一封冒充绩效报告诱导点击的钓鱼邮件。


每月员工绩效报告 - 2024 年 01 月

人力资源部 <info@g > 2024-01-17 15:20:37

发送至 hr；

发件人 人力资源部 <info@g >

收件人 "hr" ;

时 间 2024-01-17 15:20:37

大 小 3.6 KB

先生们好，

请找到以下链接，查看上个月的员工绩效报告（24 年 01 月）：

记录/职员.1 n/记录/2023- 报告/文件编号6703765197

注：所有以红色突出显示的姓名均表示将被解雇的员工。

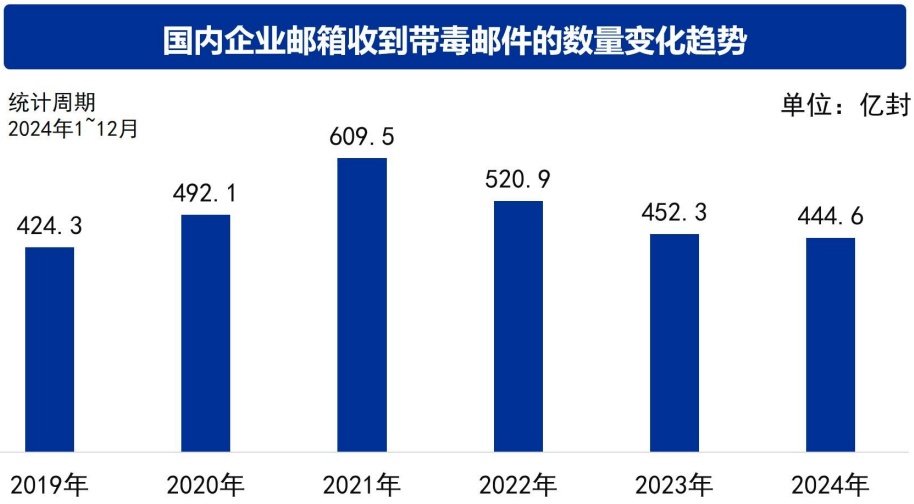
此致，
人力资源总监
人力资源部
cn |总部
1

下图是冒充律师事务所，发送虚假律师函件的钓鱼邮件。

第四章 带毒邮件形势分析

一、 带毒邮件的规模

根据 Coremail 邮件安全人工智能实验室与奇安信行业安全研究中心联合监测评估，2024 年，全国企业级用户共收到约 444.6 亿封带毒邮件，相比 2023 年收到的 452.3 亿封带毒邮件相比，同比减少了 1.7 %。2024 年企业级用户收到的带毒邮件量约占用户收发邮件总量的 5.4%。平均每天约有 1.2 亿封带毒邮件被发出和接收。



二、 带毒邮件发送源

Coremail 邮件安全人工智能实验室与奇安信行业安全研究中心对带毒邮件的发送源头进行了分析。据统计，带毒邮件的发送者多集中于北美洲与欧亚。其中，来自美国的带毒邮件最多占全球带毒邮件的 28.2%；荷兰排名第二，占 18%；保加利亚排名第三，占 6.1%。最近三年针对国内企业级用户发送带毒邮件的发送源全球分布及占比情况如下表所示。

表 3 历年带毒邮件发送源国别归属排行 Top5（按照带毒邮件数量统计）

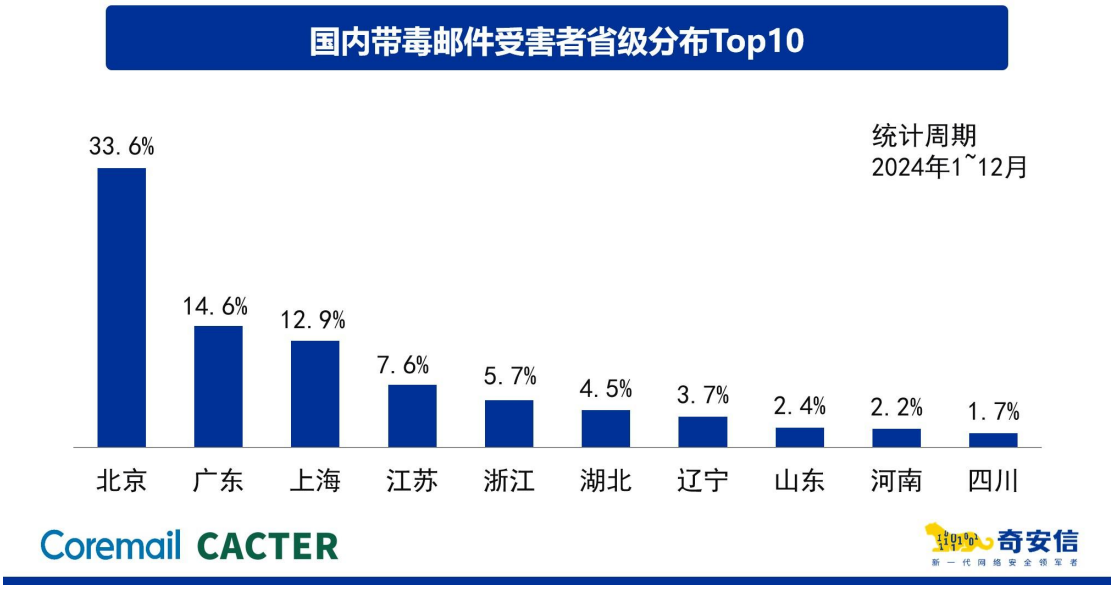
	2022 年		2023 年		2024 年	
排名	国家	占比	国家	占比	国家	占比
1	美国	22.40%	美国	23.70%	美国	28.20%
2	保加利亚	10.90%	匈牙利	18.50%	荷兰	18.00%
3	中国	9.30%	俄罗斯	7.00%	保加利亚	6.10%
4	匈牙利	3.80%	德国	3.70%	英国	4.80%
5	俄罗斯	3.20%	中国	3.10%	土耳其	2.90%
	其他	50.40%	其他	44.00%	其他	40.10%

对比过去三年的情况可以发现，美国始终是全球最大的带毒邮件发源地。而中国服务商

对于带毒邮件的治理则有显著成效，带毒邮件发送量从 2021 年的占比 20.8%，连续数年大幅下降至 2024 年的 2.6%，排名下降至第七。这也表明，在邮件反病毒领域，国内各大邮件服务商已取得重大进展。

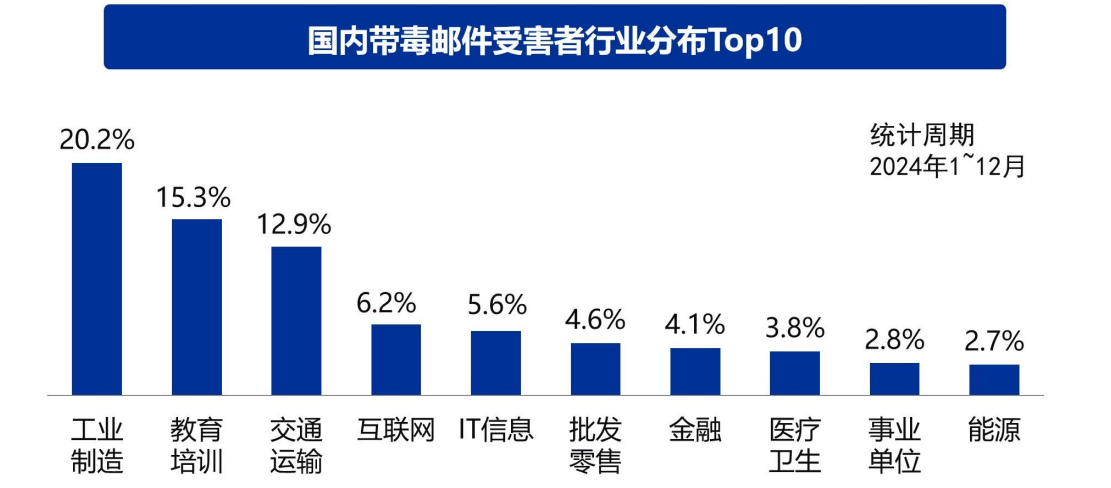
三、 带毒邮件受害者

从收到带毒邮件的受害者服务器所在地来看，2024 年北京用户收到的带毒邮件最多，全国占比高达 33.6%的带毒邮件；其次为广东，全国占比 14.6%；上海排名第三，全国占比 12.9%。下图给出了国内企业邮箱用户中带毒邮件受害者的省级行政区分布 Top10。



Coremail CACTER
奇安信 新一代网络安全领军者

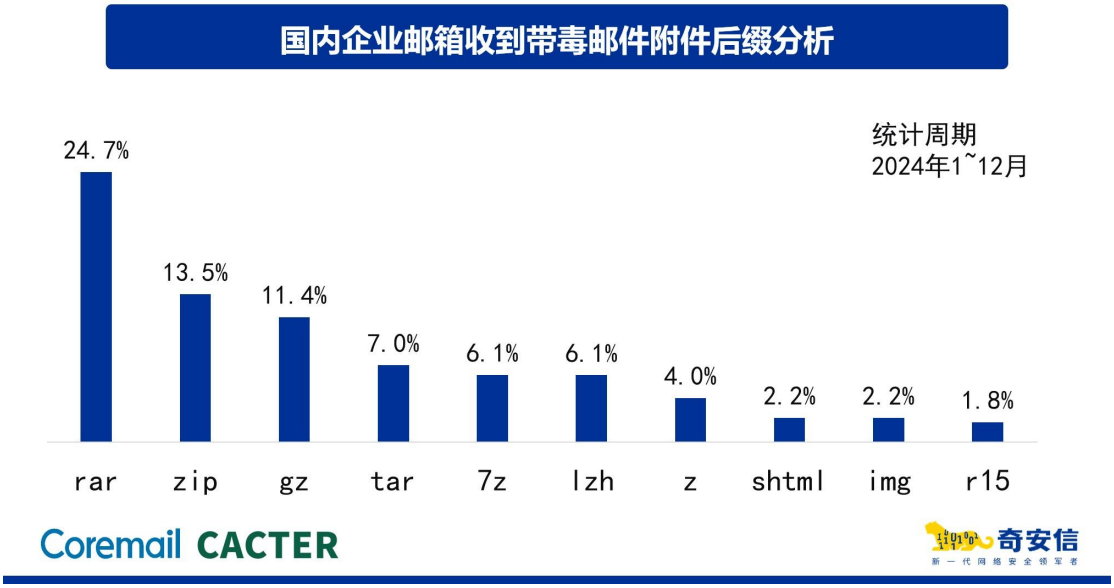
国内带毒邮件受害者所在行业也比较集中，排名前十的行业收到的带毒邮件数量，占带毒邮件总数的 78.2%。其中，工业制造行业排名第一，约占带毒邮件总数的 20.2%；教育培训排名第二，约占 15.3%；排名第三的行业为交通运输，占 12.9%。具体 Top10 行业排名如下图所示。



Coremail CACTER
奇安信 新一代网络安全领军者

四、 带毒邮件的类型

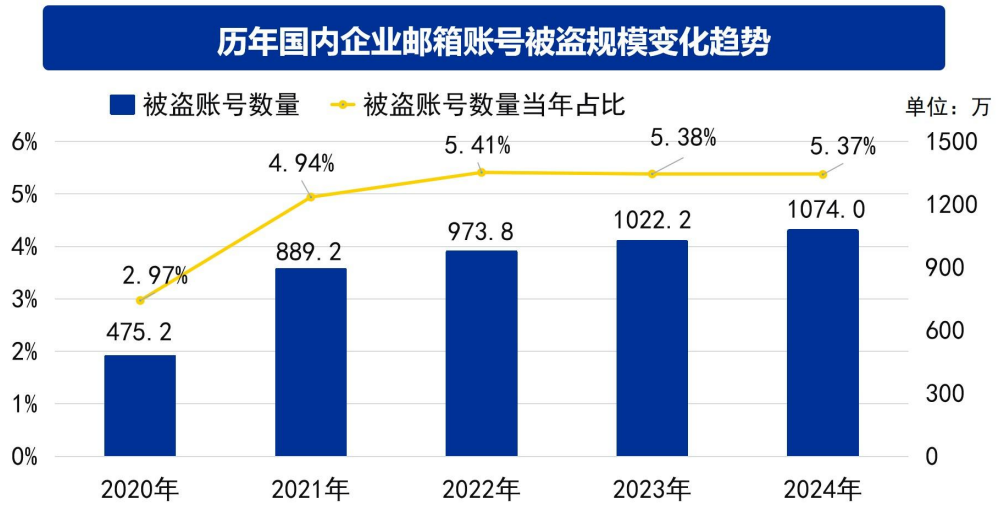
通过对带毒邮件附件文件的后缀分析发现，.rar 和.zip 两种压缩格式最为常见，占比分别为 24.7%和 13.5%。.gz、.tar 和.7z 分列第三到第五位。在排名 Top5 的后缀名中，4 个都是压缩文件格式。由此可见，压缩包是邮件攻击者最喜欢使用的病毒隐藏方式。不过，随着邮件反病毒技术的日益成熟，一般的压缩技术已经不能阻碍邮件反病毒引擎的查杀。



第五章 电子邮箱账号安全

一、 邮箱盗号的规模

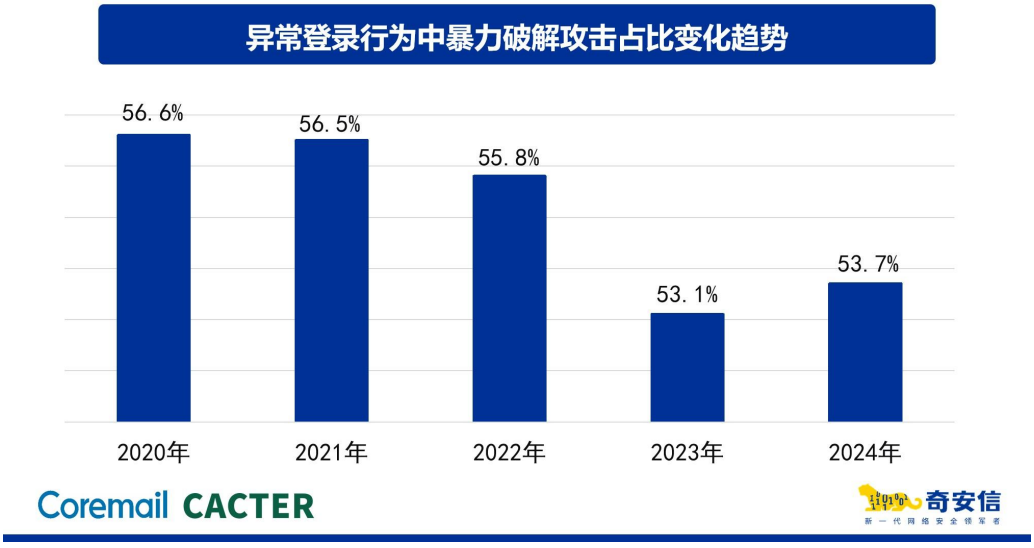
盗号，是电子邮箱账号安全的主要问题。根据 Coremail 邮件安全人工智能实验室与奇安信行业安全研究中心的联合监测显示：2024 年，国内电子邮箱账号被盗规模高达 1074 万个，占全年活跃邮箱账号总量的 5.37%。从过去几年的总体情况来看，邮箱盗号问题仍在持续加剧：2024 年国内企业邮箱账号被盗总量是 2020 年的近 2.3 倍；被盗账号数量在当年活跃邮箱账号中的占比也从 2.97%猛增到 5.37%。邮箱账号安全管理问题亟待加强。



Coremail CACTER
奇安信 新一代网络安全领军者

二、 暴力破解的形势

暴力破解是邮箱盗号最主要的手段，占到 2024 年邮箱异常登录行为检出总量的 53.7%。

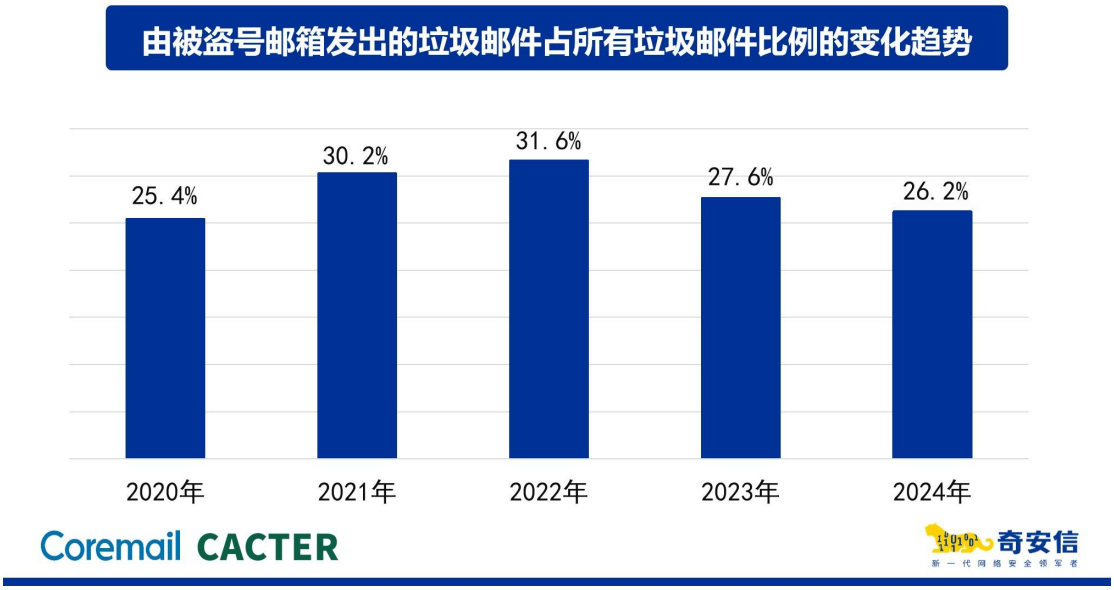


Coremail CACTER
奇安信 新一代网络安全领军者

从历年趋势来看，尽管暴力破解活动在所有异常登录行为中的占比逐年下降，从 2020 年的 56.6%逐步下降至 2023 年的 53.1%，在 2024 年又小幅增长到 53.7%，过去 5 年的占比始终保持在 50%以上。这也就意味着：“防爆破”目前仍然是电子邮箱账号安全的最大威胁。严格禁止弱口令，采取有效的防爆破措施，对于电子邮件系统来说非常重要。

三、 邮箱盗号的影响

邮箱盗号问题带来的一个直接影响，就是垃圾邮件、钓鱼邮件、带毒邮件数量的增加。统计显示，自 2020 年以来，利用被盗号的邮箱发送垃圾邮件的活动就一直非常活跃。2022 年高峰时期，由被盗号的电子邮箱发出的垃圾邮件，曾一度占到国内企业邮箱收到的所有垃圾邮件的 31.6%。2024 年虽然比例有所下降，但占比也高达 26.2%，共计约 822.5 亿封。

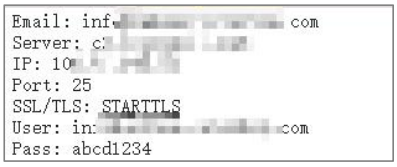


除此之外，邮箱账号被盗，还会引发商业机密泄露、商业邮件诈骗等风险发生。2024 年最新相关案例将在“第六章 邮件攻击典型案例”中进行介绍。

四、 基于盗号测试信的黑产攻击分析

2024 年邮箱盗号攻击频发，为此 Coremail 对黑产盗号行为进行了专项研究。

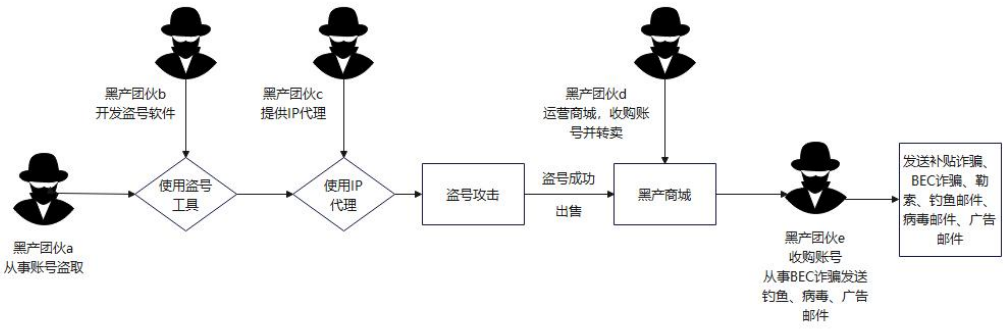
盗号测试信是黑产在盗取邮箱账号后发送的测试性邮件，一些黑产在使用脚本爆破账号成功后，会发送一封测试信到自己的邮箱，测试信通常会带有用户名、密码、登录地址等。其目的，一是测试邮箱能否对外发信，二是在大规模账号破解时便于收集账号信息。一个典型的盗号测试信内容如下：



2024 年 Q4，Coremail 邮件安全人工智能实验室共监测到盗号测试信 12833 封，涉及受害邮箱账号 3746 个，受害域名 1048 个，攻击者使用的邮箱 933 个，黑产使用的 IP 6524 个。

（一）黑产盗号攻击综述

Coremail 邮件安全人工智能实验室经过长期在邮件安全领域与黑产攻防对抗发现，目前邮箱账号盗取已形成了专门的黑色产业，从事邮箱盗号的黑产团伙已经掌握了专业工具和大量的 IP 资源池，同时分工合作形成了产业链。



（二）黑产盗号使用的口令

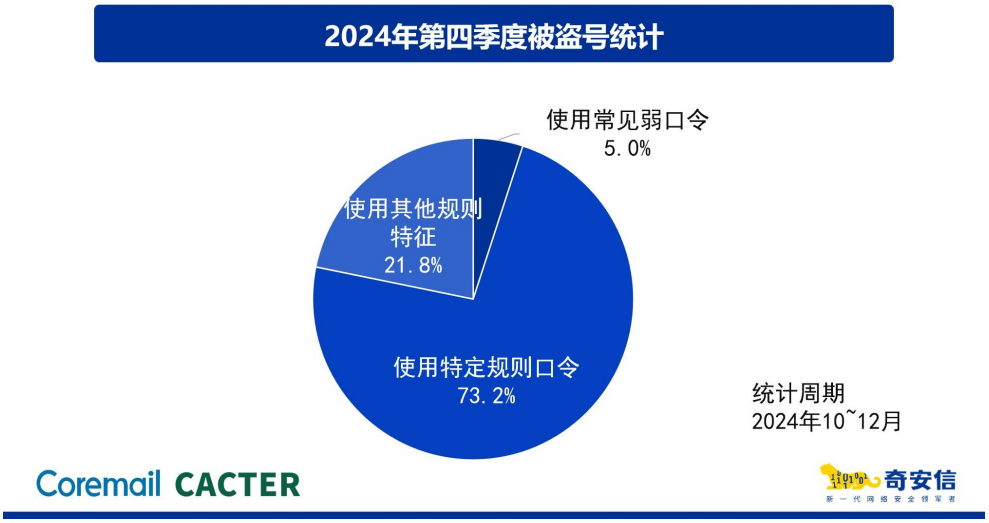
2024 年 Q4 监测到盗号测试信涉及的被盗邮箱账号共 3746 个，针对包含口令信息的 3156 个样本，我们分析了被盗账号使用的口令特征。

被盗账号使用的口令主要分为以下三类：

1. 常见口令：最常见的弱口令字典，例如：123456、abc123、abcd1234、Aa123456、123456a、qwer@1234、asd123。常见弱口令导致被盗的账号占比已经非常小。

2. 使用用户名根据特定规则构造（重要）：此类口令并非常见的弱口令，甚至可能符合强口令复杂度要求，但是这类口令具有特定特征，攻击者很容易构造出此类口令。例如：姓名缩写@123456、姓名全拼 2024、企业英文名称 888。

3. 其他规则口令：此类口令无特定规律，攻击者无法通过邮箱账号等要素来构造。因此判断用户被钓鱼泄露，或者口令在社工库中泄露。



使用特定规则的口令已经成为账号被黑产盗取的主要原因，其占比高达 73.2%。

黑产根据邮箱账号进行变形，构造暴力破解的口令字典。口令构造基本结构有三种：“账号名变形”+“常用数字组合”、“账号名变形”+“@”+“常用数字组合”、“账号名变形”+“常用数字组合”+“！”

1.账号名变形：包括邮箱账号名、姓名缩写、姓名缩写大写、姓名缩写首字母大写、邮箱域名。

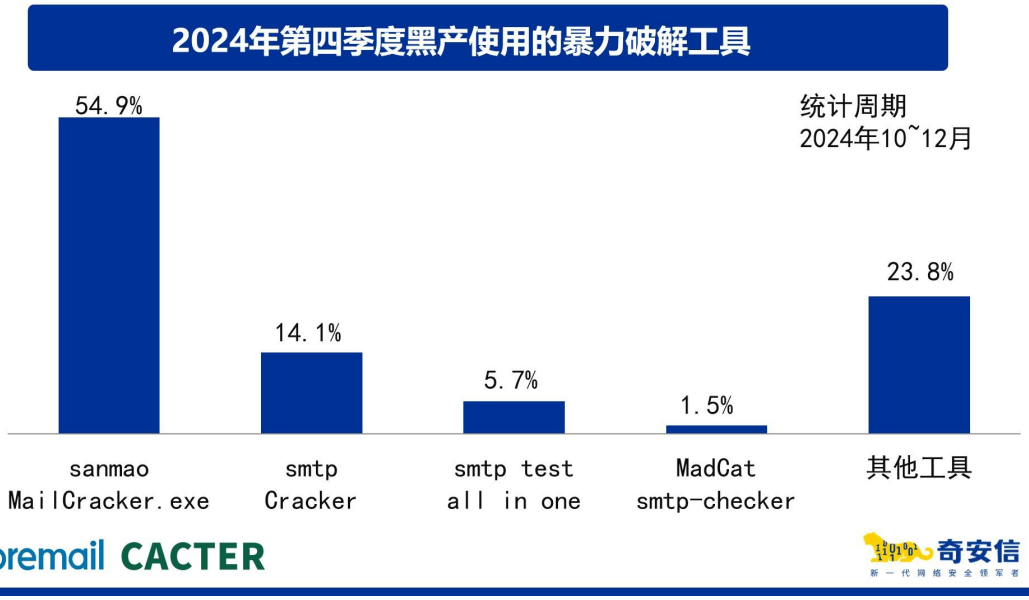
2.特殊字符：@通常在中间，！通常在结尾。

3.常用数字组合：包括常见数字串 12345、123、123456 和年份 2025、2024 等。

假设爆破目标账号为 lihua@coremail.com，则根据黑产常用规则，将构造口令字典如下：lihua@123、lihua@123456、lihua@2024、lh@123、Lh1234、coremail123456、Lh1234!等。如果用户规避掉上述口令构造方式，可以大幅提升账号安全性。

（三）黑产盗取账号使用的工具

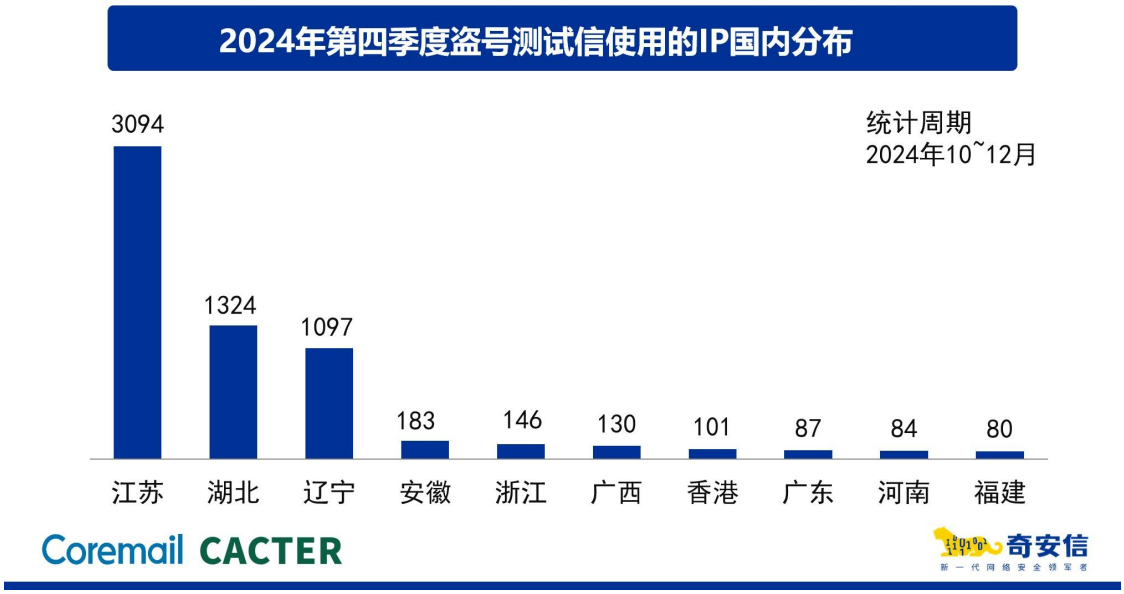
本次监测到的黑产使用的暴力破解工具主要包括“smtp cracker”“SMTP Cracker”“MadCat smtp-Checker”等开源工具，非开源工具主要包括“sanmao MailCracker.exe”“SMTP TESTER ALL IN ONE”。

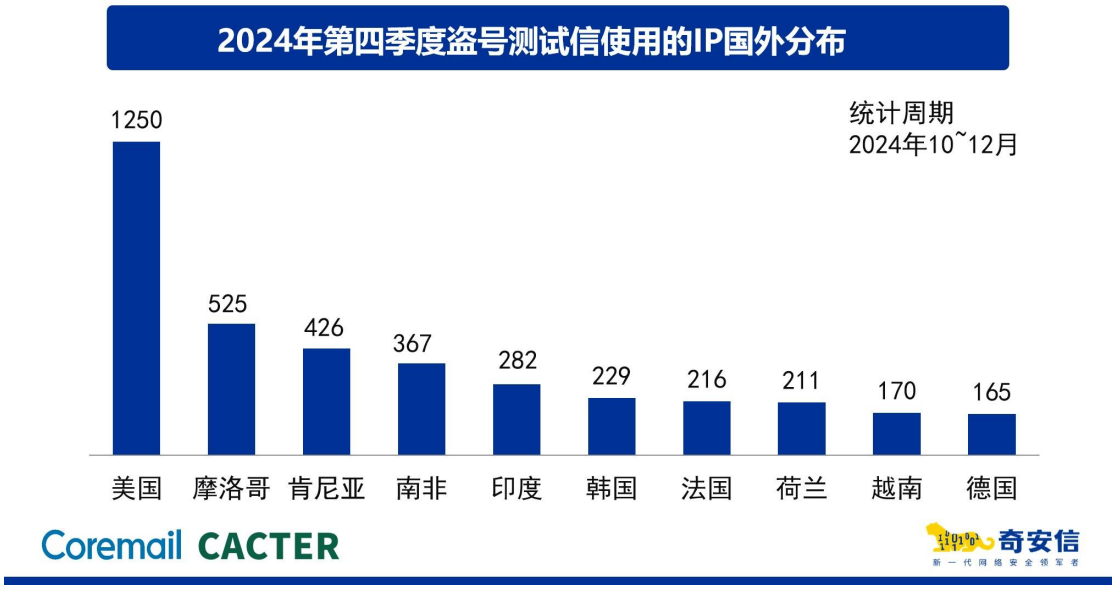


黑产使用最多的 smtp 暴力破解工具是 sanmao MailCracker，占比高达 54.9%。使用该工具的黑产团伙通常使用国内代理 IP 和国内收信域名，代理 IP 集中于江苏、湖北、辽宁三个省。推测该工具极可能是国内邮件盗号黑产最主要的暴力破解工具。

（四）黑产盗取账号使用的 IP 分布

针对 2024 年 Q4 盗号测试信使用的 IP 分布进行分析。其中 6749 次攻击记录来自国内，6084 次攻击记录来自国外。





攻击 IP 共分布在多达 2950 个 C 段，在整个 Q4 平均每个 C 段用于发送盗号测试信仅 4.35 次！这说明黑产已经掌握了大量的 IP 池资源。同时，针对 IP 和 C 段的封禁策略针对当前的黑产资源规模已经难以奏效。

（五）结论

通过对 2024 年 Q4 黑产盗号测试信的研究得出以下关键结论：

1. 目前邮箱账号盗取已形成了专门的黑色产业，盗号测试信是黑产盗取账号成功的重要标志；

2. 黑产暴力破解使用的口令字典，大部分通过目标邮箱账号名变形生成，其他占比达到 73.2%。黑产构造口令常用的规则为：“账号名变形”+“常用数字组合”、“账号名变形”+“@”+“常用数字组合”、“账号名变形”+“常用数字组合”+“！”，用户如果规避掉这种口令规则可以大幅降低账号被暴力破解的风险。

3.黑产暴力破解最常使用的工具为 sanmao SmtpCracker.exe，占 54.9%，同时该工具应为国内黑产使用的最主要暴力破解工具。

4.黑产暴力破解使用的 IP 国内和国外数量接近。黑产国内 IP 资源呈现明显的地区聚集性，集中于江苏、湖北辽宁三个省份，其中江苏省达 45.8%。

第六章 邮件攻击典型案例

本章主要介绍 2024 年，各种流行的邮件攻击典型案例，并结合案例实际情况，给出鉴别相关邮件真伪的方法及安全建议。

一、 变化多端的二维码补贴诈骗类邮件

2024 年 11 月某企业员工小李收到了一封关于“五险一金补贴资格认证”的邮件。邮件的附件是一张图片，内容看起来是非常正式的政府通知。看到国家人社部的标题和备案信息，小李没有再怀疑，非常高兴地扫描二维码。


关于《五险一金补贴资格认证》的提醒

人力资源部 <[redacted]n.cn> 2024-11-22 12:38:15

发送至 [redacted]

隐藏信息

发件人 人力资源部 [redacted]vhn.cn>

收件人 [redacted];

时 间 2024-11-22 12:38:15

大 小 104.3 KB

GIF 关于五险一金资格认证！.gif 72.5 KB

各位同事领导:

你好!

根据人力资源行政部通知！您符合本年度“五险一金补贴”申请认证的资格！符合条件的人员将在认证信息提交后三个工作日内（法定节假日除外）收到五险一金补贴，金额将直接转入您申请绑定的银行卡，为了顺利领取补贴，逾期未完成认证的将无法享受本年度“五险一金补贴”敬请注意。

祝工作顺利!

此致


中华人民共和国人力资源和社会保障部
Ministry of Human Resources and Social Security of the People's Republic of China

关于五险一金补贴资格认证的提醒

尊敬的领导/同事

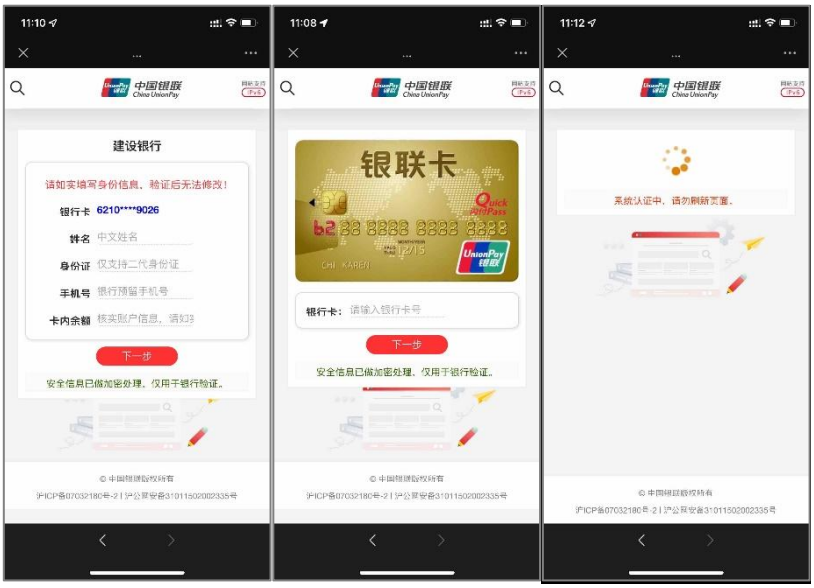
根据人力资源行政部通知！您符合本年度“五险一金补贴”申请认证的资格！根据财政部补贴政策，符合条件的人员将在认证信息提交成功后的三个工作日内（法定节假日除外）收到五险一金补贴，为了顺利领取发放，请您务必在【2024 年 12 月 31 日】之前完成信息认证。逾期未完成认证将无法享受本年度补贴，敬请注意。

使用微信扫一扫进入认证

主办单位：财政部办公厅 运行维护单位：中国政府网运行中心

京 ICP 备 05070218 号 京公网安备 11010202000001 号

扫码后，小李根据指引，填入了自己收款的银行卡信息、姓名、身份证号、手机号、支付密码，并且根据指引进行短信验证码的认证。



完成一系列操作后， 小李非常开心地等待着收款。然而很快，他却收到通知，发现自己银行卡的余额居然被转走了！小李这才意识到原来这是一封诈骗邮件，他追悔莫及。原来小李在扫码后进入了钓鱼网站，已经将自己在银行预留的全部验证信息都泄露给了骗子，甚至帮助骗子完成了短信认证！

2024 年以补贴、报税、年终奖等主题的二维码诈骗类邮件依然大行其道。这种攻击手法自 2021 年起就一直处于持续流行状态。2024 年，此类钓鱼邮件已经成为数量最多危害最大的钓鱼邮件。此类邮件大多打着人力资源部或财政部的名义发放“补贴”，只不过扫码之后的钓鱼网站大多都会套取身份信息和银行卡信息。骗子们在获得关键信息后，就会开始盗刷网银，并诱骗受害者在钓鱼页面上填写验证码，从而完成盗刷转账活动。

2024 年此诈骗邮件出现了非常多的变种，一些诈骗邮件采用了加密，并将密码标注在了标题中，解密后才能看到通知内容；一些诈骗邮件将“补贴通知”包含在图片中；还有一些邮件中附带超链接，点击超链接进入的网站有“补贴通知”和二维码。由于这些变种对通知正文进行了各种隐藏，因此没有专业的邮件安全网关设备的情况下很难有效对其进行识别和拦截。以下是一些此类诈骗邮件的变种。


津贴补发！查看码Aa1234

财务部 com> 2024-11-04 09:01:09

隐藏信息

发件人 财务部 com>

时 间 2024-11-04 09:01:09

大 小 38.4 KB

解密密码: 解密

这是一封由 "财务部" <[redacted]:om> 发出的加密邮件，需要解密才能阅读。 (您可以通过电话、短信或者其他方式向发件人索取密码)

关于2024薪酬认证通知

行政管理部 <[redacted].com> 2024-11-22 09:28:49

发送至 [redacted]

隐藏信息

发件人 行政管理部 [redacted]com>

收件人 [redacted];

时 间 2024-11-22 09:28:49

大 小 279.3 KB

DOCX 2024.docx 201.0 KB

各位领导/同事:

根据人力资源保障部通告！自2024年10月起进行部分人事薪酬职位个税补贴汇算预约申办领取通知！具体补贴标准与申办流程已下达，收到邮件通知请查收附件申请，依据《关于2024薪酬认证通知》逾期申请视为放弃，逾期申请特殊情况请向财务部提交相应说明

注：附件已加密查看码《2588》

实施通知

[redacted] 2024-12-20 07:43:29

发送至 [redacted]

隐藏信息

发件人 [redacted]>

收件人 [redacted]>;

时 间 2024-12-20 07:43:29

大 小 3.6 KB

符合条件的员工可申请五险一金补贴，务必按时认证信息，点击查看详情！

虽然此类诈骗手法狡猾多变，但也是有明显的特征的，只要掌握识别方法，还是可以通过“肉眼”轻松识破的。以下几点可以参考。

鉴别方法

1. 任何国家部委机关都不可能直接给普通的个人邮箱发送邮件。所以，来自任何国家机关的“广告式”邮件一定都是诈骗。

2. 人社部从未通过邮件发放过任何补贴，任何以人社部、财务部为名义的涉及补贴的

邮件都是诈骗。

3. 任何政府通知、人力资源部通知都不会使用加密的方式发送。

4. 需要同时输入银行卡号、银行卡密码、短信验证码的除网上银行以外的页面都是诈骗网站。

二、 最为常见的系统升级/扩容钓鱼邮件

2024 年 11 月某知名制造业公司员工小王在垃圾邮件箱中发现了一封“备案升级通知”。为了确保邮箱正常使用，他立即点击链接，输入了账号和密码进行“备案”。

第二天邮件管理员通知小王，他的邮箱在异常地点登录，并且对外发送了大量的垃圾邮件。管理员已经将他的邮箱锁定。

鉴别方法

以系统升级、扩容、备案为话题的钓鱼邮件是最为常见的类型。对于此类邮件可以使用以下方法鉴别：

1. 系统通知邮件认清发信人域名

在收到各类“系统通知”时，注意认清发信人域名，办公系统和管理员不可能使用外部域名发送通知。

2. 备案、升级等都是钓鱼话术

但凡使用邮箱备案、安全升级、邮箱搬家、幽灵账号（长期无人使用的账号）清理等借口，要求用户通过指定链接进行登录的，全部都是钓鱼邮件。正常情况下，IT 部门或网络安全部门只会要求员工正常登录自己的邮箱系统后再进行安全操作或升级操作。

3. 垃圾邮件箱中邮件的处理应格外谨慎

2024 年有多起案例是由于员工查看垃圾箱中的钓鱼邮件导致。对于垃圾箱邮件的处理一定要格外小心，不要点击其中的任何链接，不要下载其中的任何附件。

三、 贼喊捉贼的身份验证钓鱼邮件

2024 年 12 月某知名 IT 企业员工小张突然收到一封“邮件异常登录提醒”，邮件显示他的邮箱几天前在一个加拿大的 IP 被异常登录。小张心中一惊，难道自己的账号被盗了？于是他立即点击链接，对账号进行了“安全认证”。

然而第二天小张发现自己的邮箱已经无法登录，于是联系了邮箱管理员。管理员排查日志，发现他的账号在前一天晚上被异常登录并修改了口令。原来所谓的“安全认证”才是口令泄露的罪魁祸首。

鉴别方法

企业防范邮箱盗号最好的方法还是部署双因子认证。不过，对于撒网式钓鱼邮件，也还是可以通过一些安全意识提升来进行防范的。

1. 系统通知、安全提醒类邮件认清发信人域名

在收到各类“系统通知”时，注意认清发信人域名，办公系统和管理员不可能使用外部域名发送通知。

2. 认证不可能在外部网站进行

任何系统的安全认证不可能在外部网站进行，识别所谓“安全网站”的域名可以规避大部分钓鱼网站。

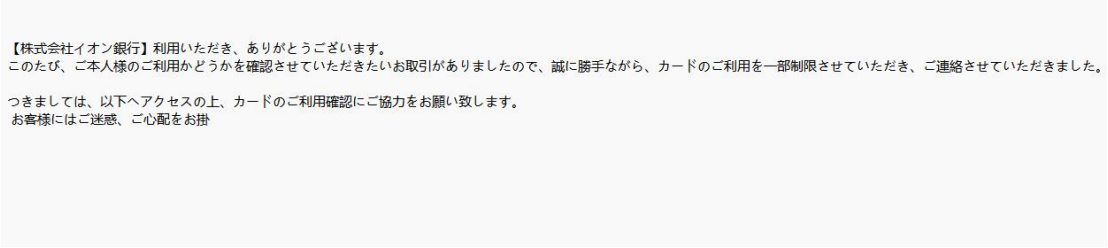
3. 系统安全机制只会要求重置口令而不会要求“认证”

邮箱系统对于异常登录的账号，要么会直接进行锁定，要么会要求重置口令，但不会要求用户输入口令进行“认证”。因此以账号异常登录需要认证为主题的邮件都是钓鱼邮件。

四、 突然爆发的日语银行卡诈骗邮件

2024 年日文的银行卡诈骗邮件数量激增，在各种钓鱼邮件分类中高居第四位。此类型邮件通常仿冒日本知名银行，以银行卡交易确认、银行卡将被冻结为话术，引导用户进入钓鱼网站泄露银行卡信息。攻击目标中，高校邮箱占据了较大比重。

以下是一封日语银行卡诈骗邮件的案例。


【株式会社イオン銀行】利用いただき、ありがとうございます。
このたび、ご本人様のご利用かどうかを確認させていただきたいお取引がありましたので、誠に勝手ながら、カードのご利用を一部制限させていただき、ご連絡させていただきました。

つきましては、以下へアクセスの上、カードのご利用確認にご協力をお願い致します。
お客様にはご迷惑、ご心配をお掛

翻译为中文后内容是：

感谢您使用 AEON 银行。

我们需要确认是否为您本人进行的交易，因此我们暂时限制了您的部分卡片使用，并与您联系进行确认。

请通过以下链接进行访问，并协助我们确认卡片的使用情况。对于给您带来的不便和担忧，我们深感抱歉。

鉴别方法

没有办理过日本银行卡业务的用户自然不会收到此类钓鱼邮件威胁，但是由于钓鱼邮件数量庞大，部分真的有办理日本银行卡业务的用户可以用以下方法鉴别：

1. 认清发信人域名

所有银行都只会用官方域名的邮箱联系自己的用户。非官方域名发送的“银行邮件”一定是钓鱼邮件；

2. 认清链接的域名

银行都在官网以外的网站要求用户进行账户安全认证，因此仔细辨别链接的域名是否为银行官方网站即可识别是否是钓鱼。

第七章 邮件风险趋势分析

章将主要对 2024 年邮件安全风险形势中的一些新特点，以及未来的发展变化趋势展开分析。

一、 域名劫持技术被大范围应用于邮件攻击

2024 年 2 月底，Guardio Labs 的安全研究人员披露了一个名为“SubdoMailing”的恶意邮件攻击组织发动的大规模广告欺诈活动。该组织使用 8000 多个“合法”的互联网域名、1.3 万个子域名和 2.2 万个独立 IP，大量发送垃圾邮件，平均每天发送量高达 500 万封，用于诈骗和恶意广告盈利。该组织的攻击活动自 2022 年开始，一直持续至今。

所谓域名，是指互联网上用于标识和定位网站的唯一名称，通常由一串用点分隔的字符组成。很多大型机构和大型企业，都会注册几十个乃至上百个网站域名用于经营活动或域名储备。一般来说，每个域名都需要定期进行重新注册，并缴纳一定的费用。如果域名持有者放弃连续注册，域名就会被释放出来，可以被其他用户重新注册。

而攻击组织 SubdoMailing 就是利用了这一机制，对于知名品牌企业曾经使用，但不再持续注册的域名进行恶意抢注，之后再以这些域名作为邮箱后缀名，注册邮箱地址，绑定恶意服务器 IP，对外发送垃圾邮件或欺诈邮件。由于很多邮件防火墙或邮件防护系统都会将一些知名大品牌企业的邮箱后缀名（域名）加入白名单，因此，以攻击者恶意抢注域名做后缀的邮箱系统发出的邮件，就很有可能被邮件防火墙或邮件防护系统无条件放行。

根据 Guardio Labs 发布的研究报告显示，域名遭到 SubdoMailing 组织劫持的企业中包括大量知名品牌，例如 MSN、VMware、McAfee、经济学人、康奈尔大学、哥伦比亚广播公司、NYC.gov、普华永道、培生、联合国儿童基金会、美国公民自由联盟、赛门铁克、Java.net、Marvel 和易趣等。

域名劫持技术也被广泛应用于钓鱼网站攻击。从 SubdoMailing 组织的活动来看，域名劫持对于恶意邮件投放也十分有效。预计未来几年内，此类攻击还有可能愈演愈烈。企业想要减少此类攻击造成的损害，应当在邮件防护系统中谨慎设置邮箱域名的白名单。

二、 邮件系统成为 APT 攻击活动的重要目标

以往，邮件系统在 APT 组织活动中的作用主要是被攻击者用来发送鱼叉邮件，即通过定向发送带有恶意内容、恶意链接或恶意附件的邮件，实现对目标人邮箱的盗号或对目标人终端设备的控制。而 2024 年发生的多起 APT 攻击事件则表明，越来越多的 APT 组织开始将邮件系统本身作为攻击目标，批量盗取邮件系统中的数据资料，并通过对供应链企业邮件服务系统的控制，间接入侵目标机构。

最为典型的案例是 2024 年 8 月发生的英国内政部遭网络攻击事件。据媒体报道，被认为是来自俄罗斯 APT 组织，侵入了英国内政部系统，盗取了内部电子邮件和个人数据。此前，同一攻击组织突入了微软公司的邮件系统，并利用微软邮件系统中的某些特殊权限，进一步入侵和破坏了微软的多个客户系统。由于微软公司也在为英国内政部提供企业系统，所以，安全专家分析认为，英国内政部遭遇的攻击事件很可能与微软邮件系统遭攻击事件存在内在

关联。

无独有偶，2024 年卡巴斯基披露了疑似 The Mask 组织针对拉丁美洲的攻击行动。攻击者首先获取了对目标组织 MDaemon 邮件服务器的访问权限，并向 MDaemon 服务器 WorldClient 组件添加恶意扩展 DLL 文件，实现在目标网络中的持久化，并进一步向目标系统植入 FakeHMP 木马，从而实现文件检索、键盘记录、截屏以及部署更多有效载荷的攻击目的。

此外，2024 年，奇安信威胁情报中心在日常的威胁监控中，也发现多起攻击者利用国内某些邮箱系统的 0day 漏洞，针对国内重点单位，窃取目标单位的核心数据的攻击事件。

三、 邮件成为通往巨额商业诈骗的高速公路

2024 年，两起从邮件攻击开始的巨额商业诈骗事件引起了业界的高度关注。在这两起事件中，一家印度公司被骗 5.2 亿卢比（约合人民币 4500 万元），一家中国香港的跨国公司被骗 2 亿港币。恶意邮件正在成为通往巨额商业诈骗的高速公路。

2024 年初，印度制药巨头阿尔肯实验室（Alkem Laboratories）被证实发生一起网络欺诈事件，导致其旗下一家子公司向欺诈分子转账 5.2 亿卢比（约合人民币 4500 万元）。据阿尔肯实验室透露，欺诈分子入侵了其子公司部分员工的业务电子邮箱账号，并最终导致欺诈事件的发生。不过，阿尔肯实验室坚称，欺诈行为与当事人、董事或员工的任何内部不当行为无关。

同样是在 2024 年初，中国香港一家跨国公司也发生了一起令人瞠目结舌的商业诈骗事件。该公司某员工先是收到了一封仿冒英国总部 CFO 的邮件，称总部正在计划一个秘密交易，需要将公司资金转到几个香港本地账户中。该员工一开始认为这是钓鱼邮件，未予理会。但是骗子反复发邮件强调项目重要性，使该员工的想法发生了动摇。随后，骗子给该员工拨打了一个视频电话。

在视频电话中，这位员工看到了公司的 CFO 和他认识的几位同事。骗子还要求该员工进行自我介绍会。然后，视频会议中的英国领导要求他赶快转账，之后就突然中断了视频。于是，信以为真的员工分 15 次向 5 个香港本地账户陆续汇款 2 亿港币。直到事发 5 天后该员工向领导核实此事，才发现被骗，如梦初醒。

尽管在这起事件中，使用 AI 生成换脸仿冒视频起到了至关重要的作用，但前期以内部邮件形式发出的虚假的项目说明，也起到了很大的迷惑和铺垫作用。由邮件安全事件带来的商业风险正在显著提升。

四、 生成式 AI 成钓鱼邮件内容重要生产者

以 DeepSeek 为代表的新一代大模型技术加速了生成式 AI 的普及，却也被恶意分子利用成为“新型武器”，成为各类恶意邮件的重要生产者，生成式 AI 正以每分钟数万封 AI 生成的恶意邮件突破传统邮件防御体系。

首先，越来越多的攻击者正在使用生成式 AI，更加快速地制作更有针对性的恶意邮件文案内容。尽管目前还没有实际案例表明 AI 编写的恶意邮件比诈骗分子人工编写的恶意邮件更具欺骗性，但由 AI 生成文案的速度，显然要比人工快得多，且平均质量有所保证，从

而可以大大提升攻击者的攻击效率。

第二，某些带毒邮件的恶意附件，疑似是使用生成式 AI 编写而成的。部分恶意样本还具有明显的快速变异和免杀能力，这些都符合生成式 AI 编写恶意程序的一些特征，这也给带毒邮件的识别和检测带来了巨大的挑战。

除了生成内容之外，监测显示，已经有越来越多的邮件攻击者，开始采用 AI 技术进行自动化的邮件攻击，主要体现在目标人群选择、投放策略制定和口令爆破攻击等方面。

附件 1　CACTER 邮件安全品牌

CACTER 邮件安全是由 Coremail 孵化的独立品牌，隶属于广东盈世计算机科技有限公司。凭借 26 年的反垃圾反钓鱼技术沉淀，CACTER 致力于提供一站式邮件安全解决方案。产品涵盖 CACTER 邮件安全网关 V7.0、大模型邮件安全网关 V7.0、CAC2.0 反钓鱼防盗号、安全海外中继、邮件数据防泄露 EDLP、安全管理中心 SMC2、Email Webrisk API、重保服务、反钓鱼演练等。

CACTER 的核心技术依托自研国产反垃圾引擎和国内头部企业级邮件安全大数据中心，拥有多项发明专利与软件著作权，与中国科学院成立邮件安全 AI 实验室，并与清华大学、奇安信、网易等国内权威机构持续开展前沿研究与合作，为客户提供从建立安全意识到数据保护的多层次邮件安全防护，为各领域提供更加安全、高效、自主可控的邮件安全解决方案。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、华润集团等。

CACTER 邮件安全产品组合概览（部分）

- **CACTER 邮件安全网关：**基于神经网络平台 NERVE 2.0 恶意邮件检测能力，对垃圾邮件、钓鱼邮件、病毒邮件、BEC 诈骗邮件等恶意邮件进行全方位检测拦截；反垃圾邮件过滤准确率高达 99.8%，误判率低于 0.02%。
- **安全海外中继：**依托全球优质中继服务器，智能选择最优质通道进行投递和接收，融合反垃圾网关技术，保障海外交流安全通畅。
- **邮件数据防泄露系统 EDLP：**基于深度内容识别技术，对敏感数据通过邮件系统外发的行为，提供事后审计和提醒，以及事中审批和拦截，保障企业数据安全。
- **安全管理中心 SMC2：**邮件系统专属安全管家，支持监测失陷账号、网络攻击、主机威胁，拥有邮件审计、用户行为审计、用户威胁行为分析等能力，并提供账号锁定、IP 加黑、邮件召回、告警等处置手段。

联系我们

官方网站：www.cacter.com
服务热线：400-000-8664、400-000-1631
微信公众号：CACTER 邮件安全

附件 2　CACTER 邮件安全网关

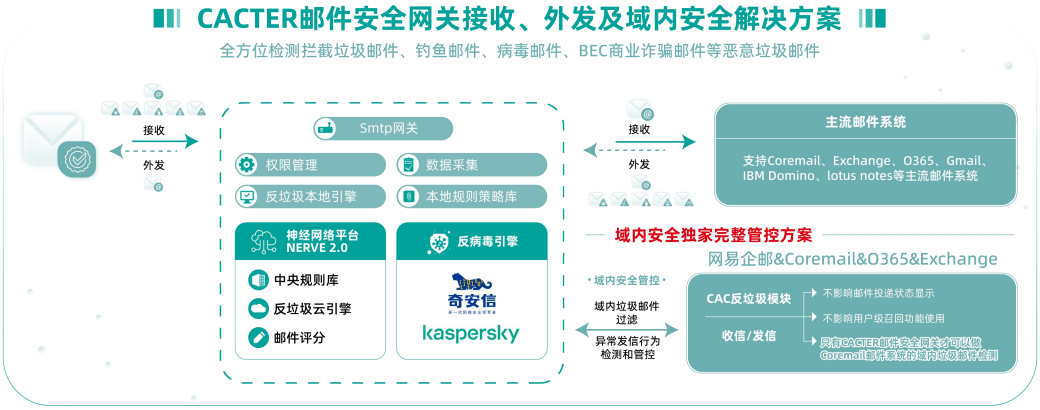
CACTER 邮件安全网关 V7.0 介绍

CACTER 邮件安全网关 V7.0 基于自主研发神经网络平台 Nerve2.0 恶意邮件检测能力，实时拦截垃圾广告、钓鱼邮件、病毒邮件、BEC 诈骗邮件等，反垃圾准确率高达 99.8%，支持几乎所有邮箱系统包含 Exchange、Microsoft 365、网易企业邮箱、Coremail，Eyou，安宁，139，Winmail 等，为企业邮件通信保驾护航。

产品优势

- **独家域内安全解决方案**

针对用户账号被盗后、“域内互发”垃圾钓鱼邮件等场景，独家域内安全解决方案支持域内垃圾邮件过滤检测、域内发信行为管控和告警，确保钓鱼邮件、病毒邮件、垃圾邮件精准拦截，异常发信行为及时发现，以保障邮件系统不受恶意邮件威胁。



- **检测能力 实时更新**

拥有国内头部的企业级邮件安全数据中心，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技术和能力。

- **恶意链接安全防护**

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。

✧ 基于“URL 情报”的静态检测以及“远程浏览器隔离”技术实时动态检测

✧ 首次过滤+二次检测防护，事前拦截、事中提醒、事后追溯结合。

- **附件全方位查杀**

与 Coremail 与顶尖反病毒厂商合作，提供邮件附件的多级防护

✧ 支持病毒库的自动更新和实时升级、解密加密附件，对文档型附件拆解及深入检测；
✧ 采用附件全方位查杀云沙箱技术，在隔离环境中自动化检测附件中的恶意代码和可执行文件，有效识别并隔离高级威胁。

- **高级威胁邮件事后处置方案**

与 Coremail 邮件系统深度联动，当新型高级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，CACTER 邮件安全网关可基于 Coremail 邮件安全大数据中心的恶意威胁情报，对投递到邮件系统的高级恶意威胁邮件自动召回，提高高级恶意威胁邮件处置时效性，守护邮箱系统安全最后一道防线。

CACTER 大模型邮件安全网关介绍

2025 年，CACTER 大模型邮件安全网关基于大模型技术突破传统网关局限，精准拦截高级恶意威胁。创新推出三大核心模块：高管保护方案（定向防御核心人员的恶意攻击）、大模型 URL 沙箱（智能检测新型恶意链接）、AI 统计报告（深度解析邮件恶意数据，提出邮件防控策略）。在提升反垃圾/反钓鱼/反病毒能力的同时，降低运维成本，适配企业多样化安全需求。

产品优势

- **新增能力模块－高管保护**

AI 深度语义威胁识别，及时拦截针对企业核心人员发起的新型恶意攻击：

✧ 检测混淆文本类恶意邮件、罕见恶意后缀附件检测；
✧ 基于意图理解的高级威胁二次筛查（从垃圾邮件中捕获新型攻击）；
✧ 多语种支持：提升小语种恶意邮件检出率；
✧ 数据可视化统计：全局统计防护高管用户的异常邮件总量；个体追踪单高管用户异常邮件明细分析。

- **新增大模型 URL 沙箱**

实现 AI 赋能的动态防御，通过 AI 驱动意图级行为追踪、多模态分析验证识破伪装，提升新型恶意 URL 检出率，让伪装的钓鱼链接无处遁形。

- **新增 AI 智能报告模块**

支持 AI 数据分析，“自定义制作统计报告”和“定时推送统计报告”场景

✧ 邮件过滤数据深度挖掘和可视化解读；
✧ 智能生成邮件安全防护策略；

附件 3　CACTER 邮件数据防泄露 EDLP

CACTER EDLP，是独立的网关类产品，垂直于邮件数据防泄露，是 Coremail 基于深度内容识别技术，根据不同安全级别采用不同算法和策略，支持多种响应规则，对敏感数据通过邮件系统外发的行为，提供事后审计和提醒，以及事中审批和拦截，预防并阻止有意或无意的邮件数据泄露行为，保障企业数据安全。

- **多维度涉敏感检测：**

CACTER-EDLP 采用深度内容识别技术，包括关键字检测、正则表达式检测、数据标识符检测、非结构化数据指纹检测等技术对出站邮件和站内邮件进行涉敏感检测。

- **多模态内容识别：**

CACTER-EDLP 支持办公文档、图片、压缩包等 1000 余种常见文件的解析辨别，并对递归压缩、文件嵌套、篡改类型等伪装手段具备强大的检测能力

- **多层级、定制化防护策略**

CACTER EDLP 支持邮件审批、自动补全抄送、自动密送等组合式邮件管控措施，并且提供“自动生成审批流”、“标准对接第三方系统审批”、“事件完整留痕”等管理增效功能

- **模糊指纹、智能模型、字典词库等技术强强联合，构建动态防护体系**

智能模糊指纹引擎：CACTER-EDLP 能根据精准的自定义规则进行检测，且支持模糊指纹，支持管理者通过喂给样本作为敏感检测依据

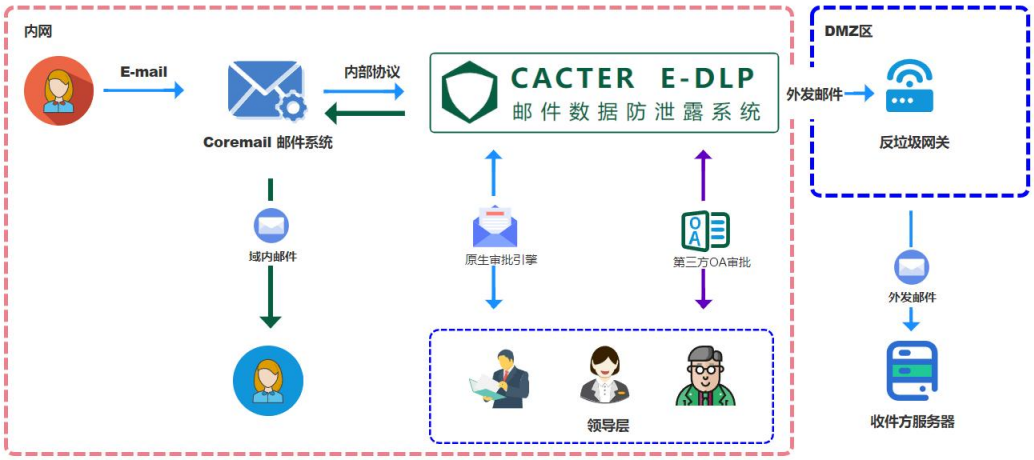
全栈式智能检测矩阵：CACTER-EDLP 原厂内置多样化智能模型，以及百余种字典词库，打造立体防护网

- **多种部署方式，支持软件、硬件、信创等**

全面兼容：CACTER-EDLP 支持 Exchange、Microsoft 365 等多种邮件系统及市面所有

邮件网关品牌，部署方式多样，能够适应不同企业的 IT 环境。

私有云托管：针对企业邮件数据防泄露（DLP）过渡阶段的核心需求，CACTER-EDLP 提供安全可控的专属云托管服务，通过本地化+私有云托管混合部署，在保障敏感数据零泄露的同时，确保业务连续性与运维敏捷性，助力企业平稳完成数字化转型过渡



附件 4　奇安信网神邮件威胁检测系统

奇安信网神邮件威胁检测系统是奇安信集团面向政府、企业、金融、军队等大型企事业单位推出的针对邮件场景的高级威胁检测及处置的解决方案。邮件威胁检测系统采用多种的病毒检测引擎，结合威胁情报以及 URL 信誉库对邮件中的 URL 和附件进行恶意判定，并使用动态沙箱技术、邮件行为检测模型、机器学习模型发现高级威胁及定向攻击邮件。通过对海量数据建模、多维场景化对海量的邮件进行关联分析，对未知的高级威胁进行及时侦测。强大的侦测技术和全面的处置手段，对电子邮件系统进行全面的安全防御。

用户价值

为客户提供更高级的邮件安全防护

- 通过定制化沙箱分析，发现传统邮件安全产品无法侦测的附件高级威胁。
- 通过专业的机器学习模型，发现更隐蔽的钓鱼邮件等社交工程邮件。

提供更灵活的安装和部署方式

- 提供多种部署方式，可适应不同的用户场景和需求。
- 可以和现有的邮件安全解决方案无缝协同工作，建造完整的应用、防护于一体的综合邮件办公系统。
- 与现有天眼高级威胁检测方案联动，实现更全面的威胁检测和分析。

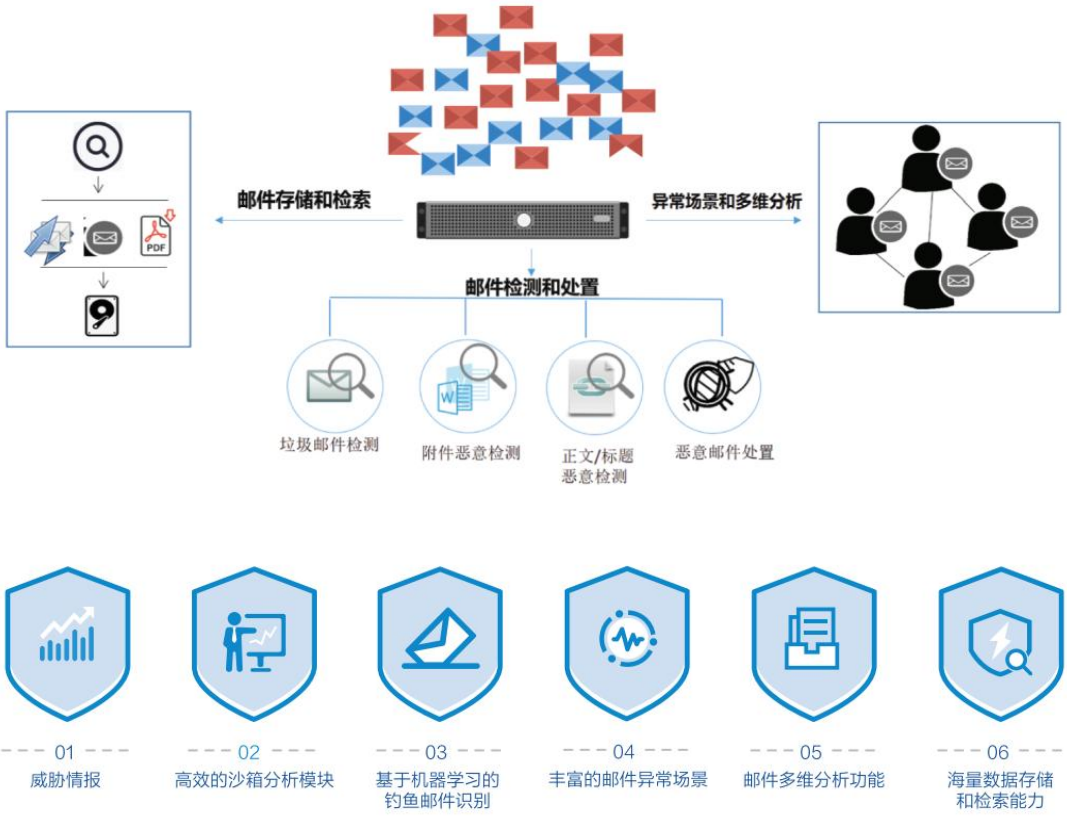
看得见的投入产出比

- 阻止社交工程邮件，避免昂贵的事后补救措施。
- 通过阻止、隔离、移除威胁、通知收件人等方式减少恶意邮件威胁。

更炫酷的展示效果

- 产品支持将邮件外部攻击态势在 4K 的屏幕上投屏展示，满足日常巡检需求。

产品介绍



威胁情报

邮件威胁检测系统结合了奇安信强大的威胁情报数据，使产品对邮件威胁的检测能力如虎添翼。

高效的沙箱分析模块

邮件威胁检测系统沙箱模块可针对文件进行深度检测，采用静态检测、漏洞利用检测、行为检测多层次手法，构建基于沙箱技术的文件深度检测分析能力。静态检测模块通过多种检测引擎互为补充增强静态检测能力。动态检测模块以硬件模拟器作为动态沙箱环境，分析过程中所有的数据获取和数据分析工作都在虚拟硬件层实现，全面分析恶意代码恶意行为，细粒度检测漏洞利用和恶意行为。

基于机器学习的钓鱼邮件识别

机器学习引擎基于云端海量邮件数据进行训练，通过自适应学习引擎、综合检测引擎及 URL 增强判定引擎进行综合检测，能够在不同的企业环境下自适应学习，保持低误报的同时，准确高效地检出钓鱼 URL。

丰富的邮件异常场景

能够通过大量邮件数据进行分析，深入挖掘潜在的威胁行为与线索。

包括发件异常、收件异常、暴力破解、单个 IP 登录多个邮箱、异地登录等异常场景，支持全面分析仿冒邮件场景，并可根据需求自定义异常场景的检测条件。

邮件多维分析功能

产品提供基于联系人之间的收发关系的多维分析模块以及基于恶意文件/URL 的传输路径的多维分析模块。通过关键信息的检索生成的邮件数据之间的多维关系网，使错综复杂的数据展现一目了然。

海量数据存储和检索能力

奇安信网神邮件威胁检测能够快速检索匹配邮件主题或者正文中的关键字，结合统计学相关理论，达到快速精准内容过滤和关键字分析，配套了大量的检索和分析软件以对数据做到高效分析。

联系我们

官方网站： https://www.qianxin.com/product/detail/pid/406

服务热线：95015

微信咨询：奇安信集团

附录 5　奇安信观星实验室

观星实验室是奇安信核心攻防技术研究团队，致力于互联网、各行业领域、政企以及关键信息基础设施的攻防技术研究。实验室不仅精通实网攻防、漏洞挖掘、应急响应与攻击溯源等传统领域，还积极开拓新的研究方向，如数据安全和云安全，旨在全面掌握网络安全的各个环节。

在安全漏洞挖掘方面，观星实验室汇聚了业界顶尖的专家团队，专注于对全球范围内主流的应用软件、中间件、网络设备和 IoT 设备进行深入的漏洞分析，为实网攻击防御提供强有力的技术支持。同时，实验室也积极拓展数据安全与云安全的研究领域，运用先进的技术手段，深入挖掘云环境中的数据泄露风险，确保企业云上安全。

在实网攻防演习方面，以观星实验室为核心的奇安信攻击团队，在近 3 年的时间里，参与了超过 1000 场攻防演习，攻击目标超过 5000 家，其中前三名占比达到了 80%以上。