2021中国企业邮箱安全性研究报告

Coremail × 奇安信
新一代网络安全领军者

2022年9月出品

中国企业邮箱安全性

研究报告

Coremail

奇安信
新一代网络安全领军者

2022 年 9 月

编写组

组长

林延中 裴智勇

主要编写人员

刘川琦

朱腾蛟 江嘉杰 练奕余

《中国企业邮箱安全性研究报告》由广东盈世科技计算机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 科技 CAC 邮件安全大数据中心、Coremail 邮件安全实验室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。

Coremail 奇安信 新一代网络安全领军者

摘　　要

- 根据 Coremail 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 2021 年，国内注册的企业邮箱独立域名约为 535 万个，相比 2020 年增加 1.5%。活跃的国内企业邮箱用户规模约为 1.8 亿，与 2020 年用户规模相比增加了 12.5%。

- 仅就正常邮件而言，统计显示，全国企业邮箱用户在 2021 年共收发正常电子邮件约 3379.7 亿封，比 2020 年增长 25.4%，平均每天发送正常电子邮件约 9.3 亿封，人均每天发送电子邮件约 5.1 封。相比 2020 年人均每天发送 4.6 封邮件，增加了 0.9 封。

- 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 31.5%，其次是交通运输行业占比 11.7%，外资机构占比 8.5%；还有互联网企业占比 7.4%，IT 信息技术占比 7.0%，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。

- 统计显示，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 73.8%；海外收发 26.2%。从服务器的所在地来看，2021 年，国内企业邮箱服务器设在北京的数量排名第一，占比为 21.7%；上海排第二，占比为 15.0%；深圳排名第三，占比 11.1%。

- 根据 Coremail 与奇安信行业安全研究中心的联合监测评估，2021 年，全国企业邮箱用户共收到各类垃圾邮件 3042.1 亿封，约占企业级用户邮件收发总量的 39.8%，是企业级用户正常邮件数量的 90.0%。这是近五年来普通垃圾邮件收发量第一次少于正常邮件。

- 根据 Coremail 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，来自美国的钓鱼邮件最多，占国内企业用户收到的钓鱼邮件的 41.0%；其次是中国，约占 11.7%；新加坡排名第三，约占 5.3%。

- 根据 Coremail 与奇安信行业安全研究中心联合监测评估，2021 年，全国企业级用户共收到约 609.5 亿封带毒邮件，相比 2020 年收到的 492.1 亿封带毒邮件相比，同比增长了 23.9%。越来越多的带毒邮件正在被发送给企业邮箱。2021 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 7.98%。平均每天约有 1.7 亿封带毒邮件被发出和接收。

关键词：企业邮箱、垃圾邮件、带毒邮件、钓鱼邮件

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者不可或缺的角色。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，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六年。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 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。

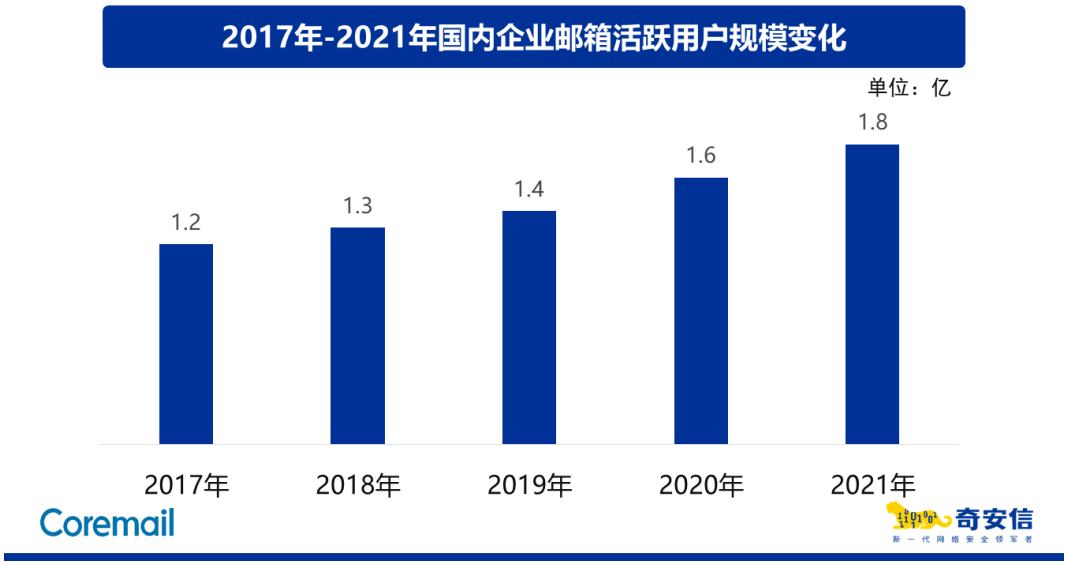
主要观点

- ✧ 邮件用户规模快速增长，以业务为基础的正常邮件收发量也在快速增长，且增速显著高于普通垃圾邮件的增速。从而使得近五年来正常邮件收发量首次超过普通垃圾邮件的收发量。
- ✧ 随着邮件识别技术的持续进步，越来越多的其他恶意邮件（如钓鱼邮件、带毒邮件等）可以被精准识别，其他恶意邮件的增长速度也在迅速增长，值得关注。
- ✧ 普通垃圾邮件发送源境内最多，占比 47.8%；钓鱼邮件与带毒邮件的发送源均为美国最多，占比分别为 41.0%与 36.8%。
- ✧ 钓鱼邮件受害者最多的三个行业及占比分别为：工业制造 26.2%、交通运输 12.0%和教育培训 7.5%。
- ✧ 僵尸网络、挖矿木马通过电子邮件进行传播的活动仍然十分猖獗，这给很多政企机构造成了巨大的困扰。以“财务补贴”、“工资补贴”为代表的针对政企机构员工的网络诈骗正处于历史高发期，甚至很多知名的互联网企业也成为了被攻击目标。针对企业财务及管理人员的“高级邮件诈骗”活动呈现出打击精准、手段多样且极具迷惑性的特点。这给很多企业造成了巨大的甚至不可挽回的损失。

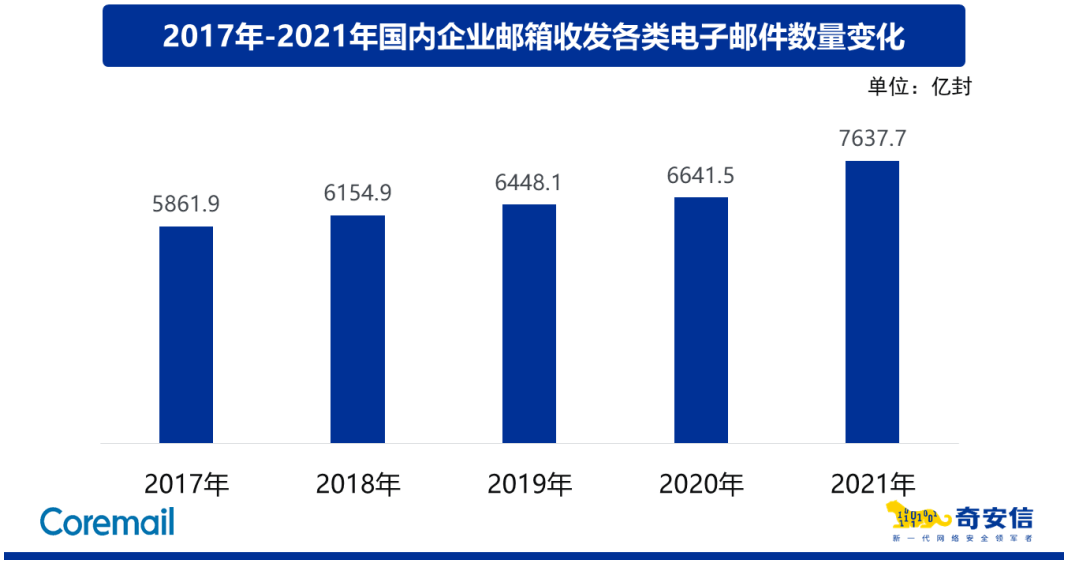
第一章　电子邮箱的使用与规模

一、　电子邮箱的使用规模

根据 Coremail 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 2021 年，国内注册的企业邮箱独立域名约为 535 万个，相比 2020 年增加 1.5%。活跃的国内企业邮箱用户规模约为 1.8 亿，与 2020 年用户规模相比增加了 12.5%。近五年国内企业级电子邮箱活跃用户规模变化如下图所示：



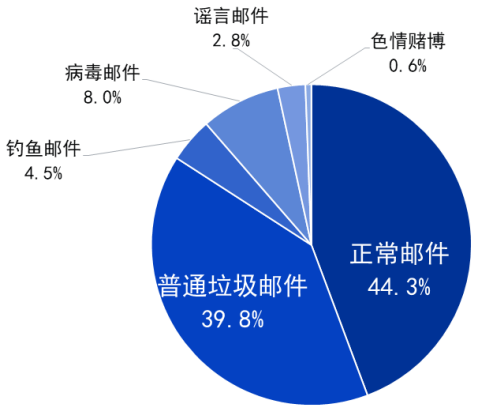
从电子邮箱的使用情况来看，2021 年，全国企业邮箱用户共收发各类电子邮件约 7637.7 亿封，相比 2020 年企业及电子邮箱用户收发邮件数量增长 15.0%。平均每天收发电子邮件约 20.9 亿封。



其中，正常邮件占比约为 44.3%，普通垃圾邮件占比为 39.8%、钓鱼邮件 4.5%、病毒

邮件 8.0%、谣言邮件 2.8%，色情、赌博等违法信息推广邮件约 0.6%。也就是说，2021 年，在邮件系统收发的邮件中，仅有 4 成左右为正常邮件，垃圾邮件及其他各类非法、恶意邮件等非正常邮件的数量，约是正常邮件数量的 1.3 倍。

2021年中国企业级电子邮箱用户收发邮件类型分布

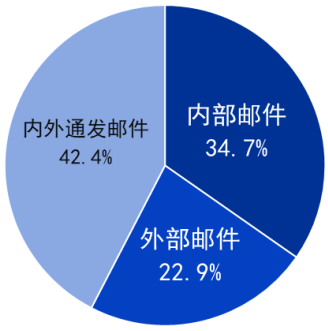


Coremail 奇安信

仅就正常邮件而言，统计显示，全国企业邮箱用户在 2021 年共收发正常电子邮件约 3379.7 亿封，比 2020 年增长 25.4%，平均每天发送正常电子邮件约 9.3 亿封，人均每天发送电子邮件约 5.1 封。相比 2020 年人均每天发送 4.6 封邮件，增加了 0.5 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，2021 年企业用户发送的电子邮件中，约 34.7%为机构内部邮件，22.9%为外部邮件，42.4%为内外通发邮件（收件人既有机构内部，也有机构外部）。

2021年中国企业级邮箱用户发送内、外部邮件比例分布



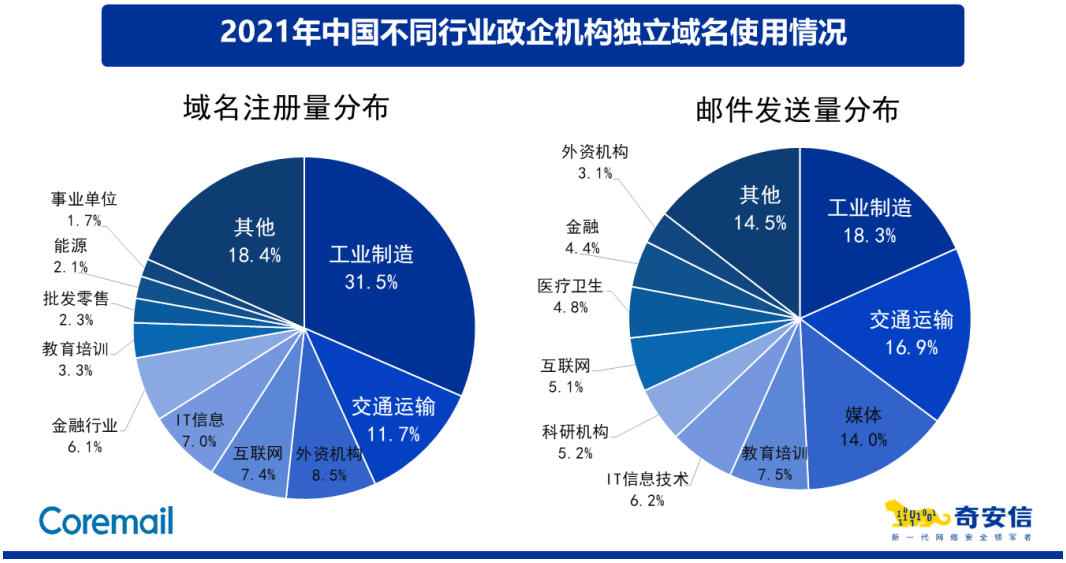
Coremail 奇安信

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 31.5%，其次是交通运输行业占比 11.7%，外资机构占比 8.5%；

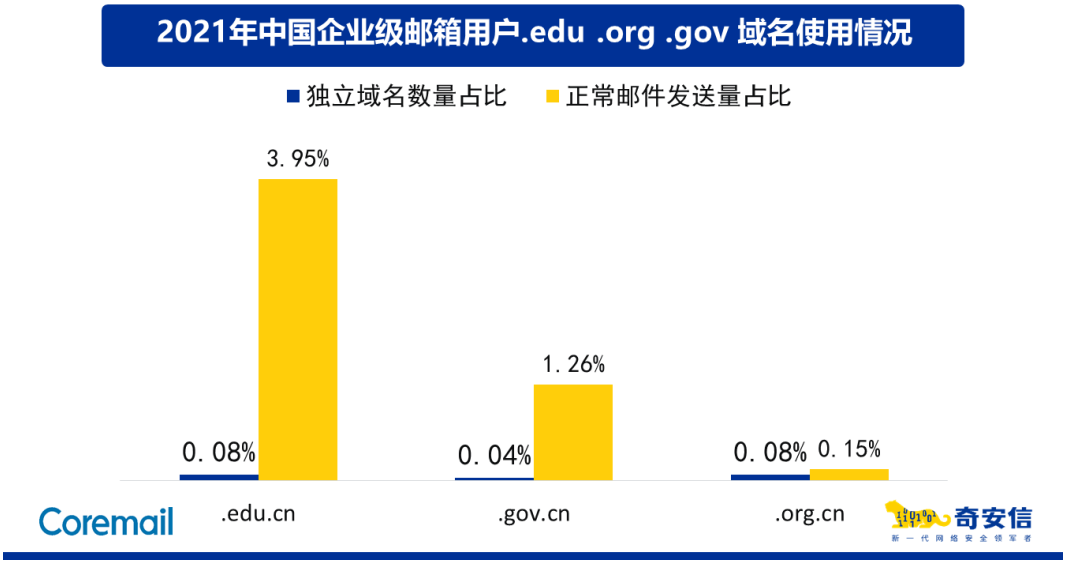
还有互联网企业占比 7.4%，IT 信息技术占比 7.0%，金融行业占比 6.1%等，这些都属于电子邮箱使用独立域名较多的行业。

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，工业制造类企业邮件正常发送量占比 18.3%，排名第一；交通运输占比 16.9%，排名第二；其次是媒体占比为 14.0%；教育培训、IT 信息技术、科研机构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，教育培训，工业制造与交通运输等行业对邮件办公的依赖度最高。

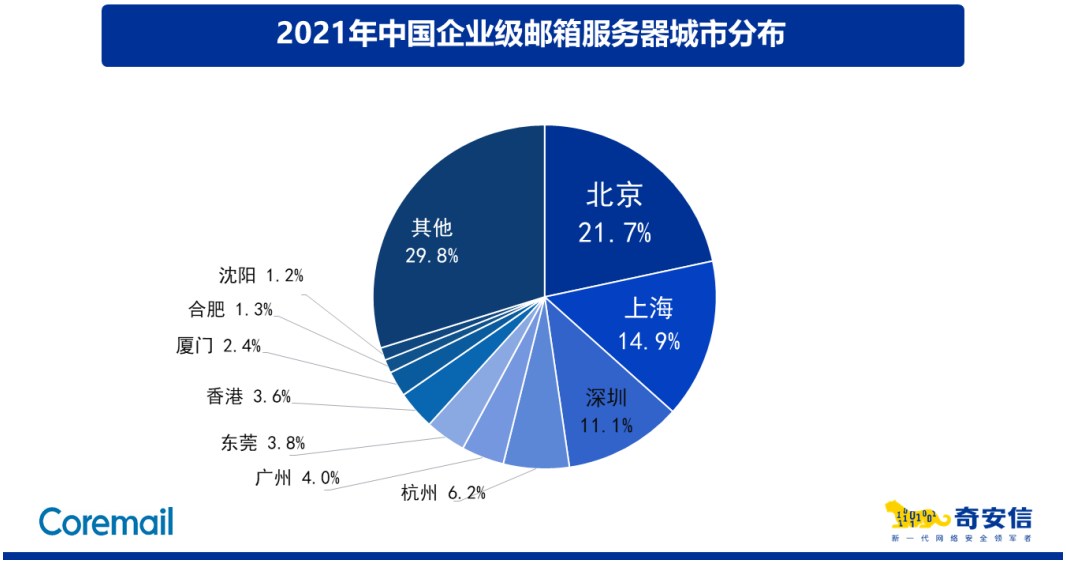
特别的，本次报告对.edu（教育）、.org（组织机构）和.gov（政府）三个域名的邮箱使用情况进行了分析。其中，.edu.cn 邮箱域名在全国占比为 0.08%，.org.cn 的邮箱域名占比约为 0.08%，.gov.cn 邮箱域名占比为 0.04%。而从正常邮件发送量上来看，.edu.cn 邮箱占 3.95%，.gov.cn 邮箱占 1.26%，.org.cn 邮箱占 0.15%。



三、 电子邮件的地域分布

统计显示，2021 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 73.8%；海外收发 26.2%。

从服务器的所在地来看，2021 年，国内企业邮箱服务器设在北京的数量排名第一，占比为 21.7%；上海排第二，占比为 15.0%；深圳排名第三，占比 11.1%。

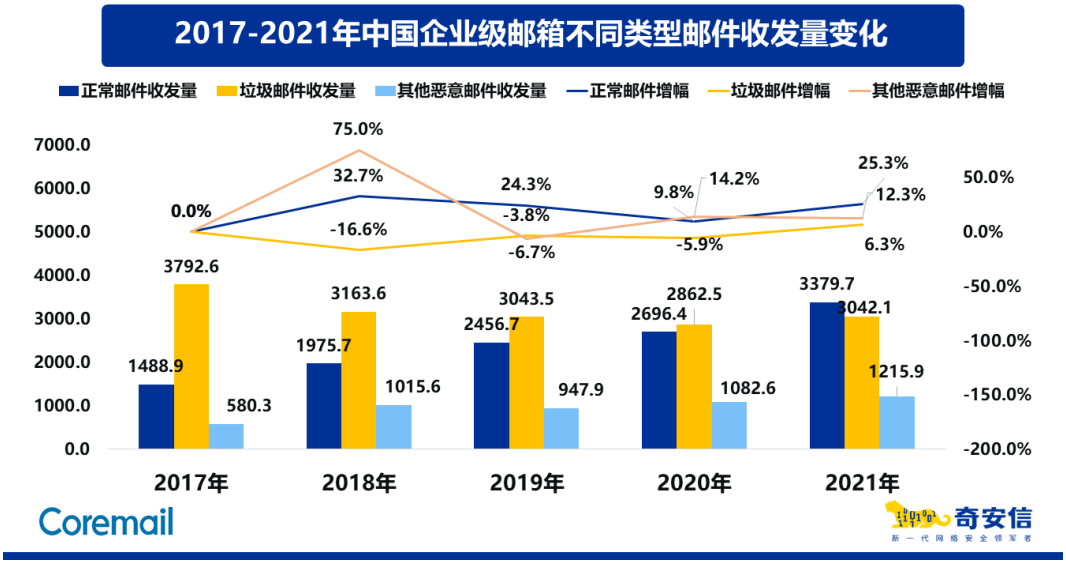


第二章　垃圾邮件

一、　垃圾邮件的规模

根据 Coremail 与奇安信行业安全研究中心的联合监测评估，2021 年，全国企业邮箱用户共收到各类垃圾邮件 3042.1 亿封，约占企业级用户邮件收发总量的 39.8%，是企业级用户正常邮件数量的 90.0%。这是近五年来普通垃圾邮件收发量第一次少于正常邮件。

从近五年情况来看，正常邮件收发量的增速高于垃圾邮件收发量的增速，同时其他恶意邮件的收发量近年来也有较快增长。具体分布如下图所示：



分析其原因有四点：第一，反垃圾邮件技术在持续进步。第二，境内机构（包括主管部门与邮件服务商）对境内垃圾邮件的源头的持续打击在相当程度上抑制了垃圾邮件的增长。第三，新增邮件用户多为企业用户，通常会配置较高的反垃圾邮件策略，从而使垃圾邮件更加难以有效的抵达目的人群。第四，邮件服务商通过持续的技术进步，将更多危害性强的恶意邮件监测并区分出来。未来此类型邮件的监测和防护也将成为邮件安全领域的主战场。

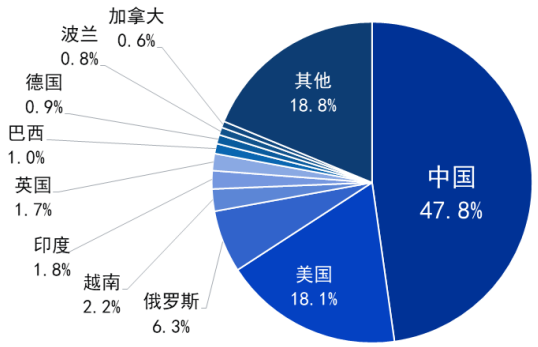
正是由于这些对垃圾邮件的抑制因素使得垃圾邮件的增长速度远不及新增用户的增长速度与正常收发邮件数量的增长速度。

二、　垃圾邮件发送源

Coremail 与奇安信行业安全研究中心对垃圾邮件的发送源头进行了分析。据统计，因盗号导致发送垃圾邮件（正常用户邮箱帐号被盗后，被黑客用来发送垃圾邮件）占所有垃圾邮件总量的 30.2%。

从发送者邮箱域名归属情况来看，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 47.8%，来自美国的垃圾邮件次之，占总量约 18.1%，第三是俄罗斯，约占 6.3%。具体占比如下图所示：

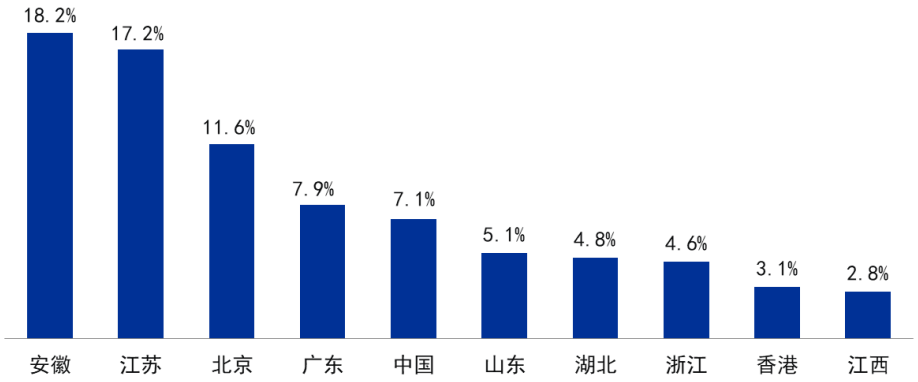
2021年垃圾邮件发送源邮箱域名归属地全球分布



Coremail
奇安信 新一代网络安全领军者

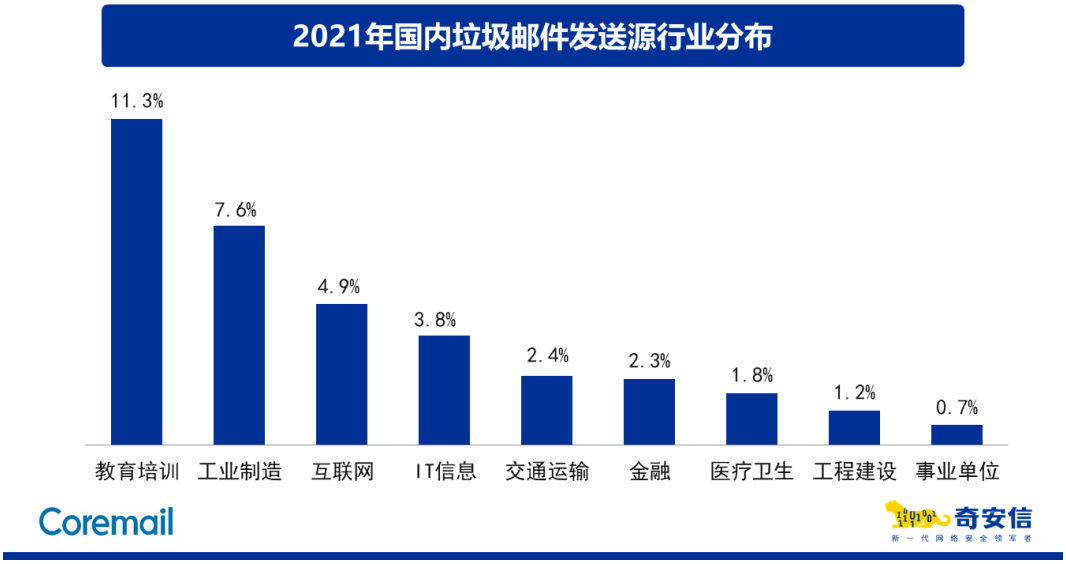
仅就国内情况来看，根据发送者的域名归属地来看，来自安徽的垃圾邮件发送者最多，占国内垃圾邮件发送总量的 18.2%，其次为江苏省，占 17.2%，北京，占 11.6%。下图给出了国内垃圾邮件发送源域名归属省份 TOP10 及其垃圾邮件发送量占比情况。

国内垃圾邮件发送源域名归属地TOP10及其垃圾邮件发送量占比



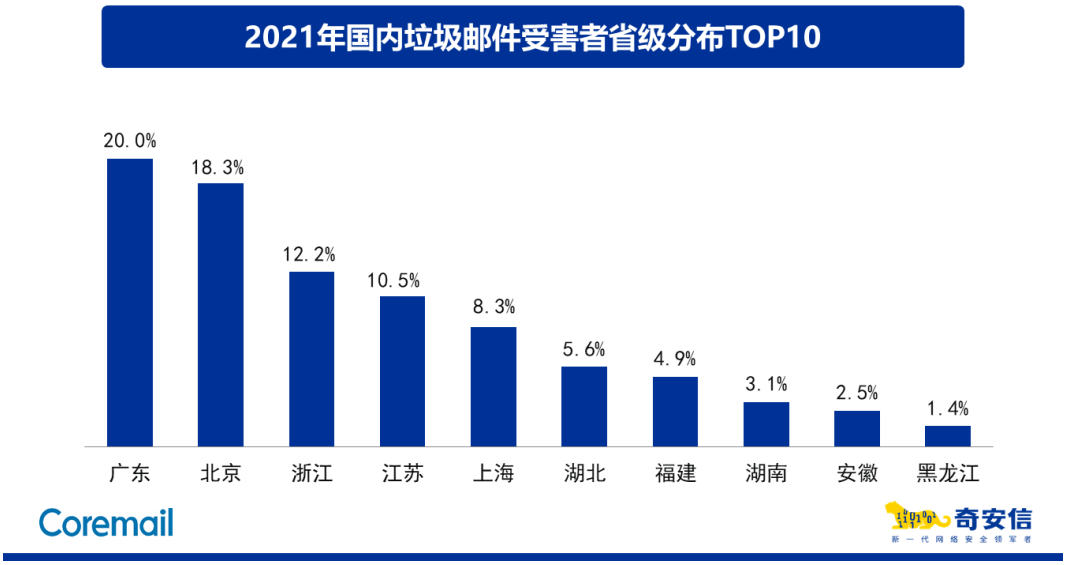
Coremail
奇安信 新一代网络安全领军者

对发送垃圾邮件的邮箱域名进行抽样行业分析显示，2021 年，国内垃圾邮件发送源中教育培训行业占比最高，为 11.3%；其次为工业制造，占比 7.6%；互联网企业排名第三，占比 4.9%。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，广东省用户收到的垃圾邮件最多，共收到了占比高达全国 20.0%的垃圾邮件；其次为北京，收到了全国 18.3%的垃圾邮件；浙江省排名第三，收到了全国 12.2%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分布 TOP10。



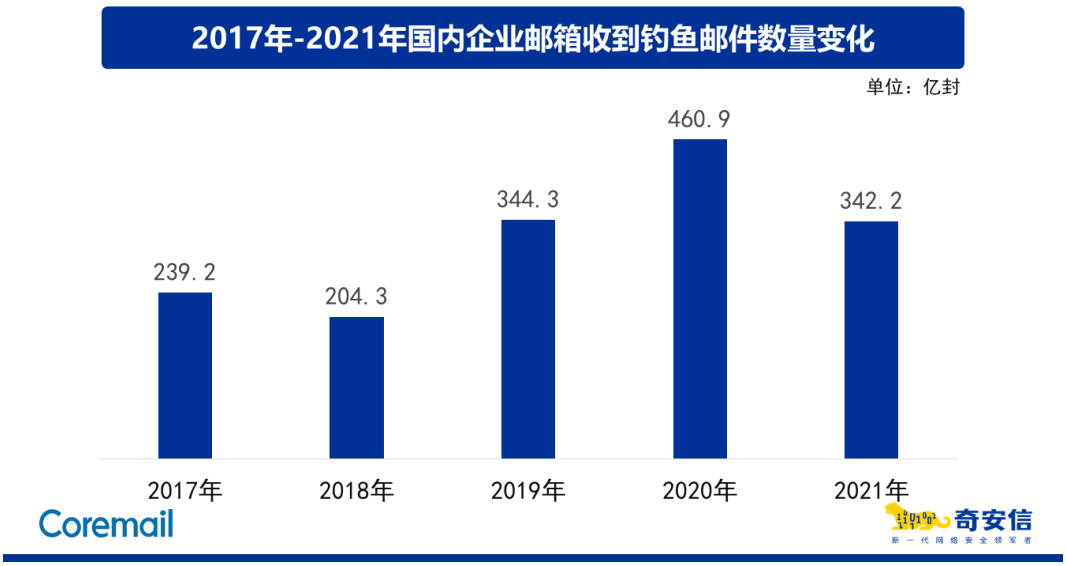
第三章　钓鱼邮件

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。在本报告中，我们将钓鲸邮件和一般的鱼叉邮件区别开来进行统计分析。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。

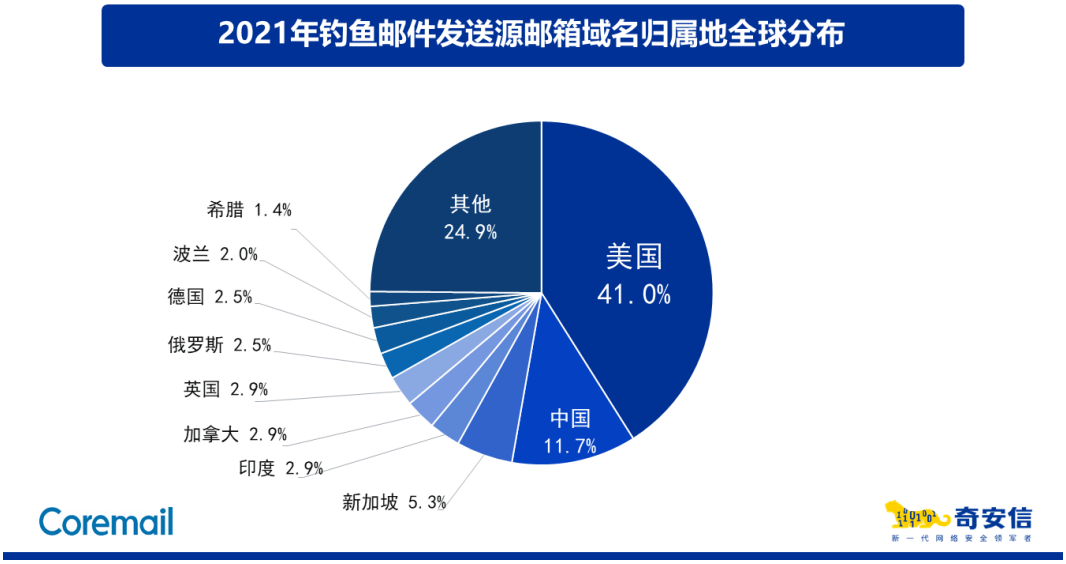
根据 Coremail 与奇安信行业安全研究中心的联合监测评估，2021 年，全国企业邮箱用户共收到各类钓鱼邮件约 342.2 亿封，相比 2020 年收到各类钓鱼邮件的 460.9 亿封减少了 25.8%。



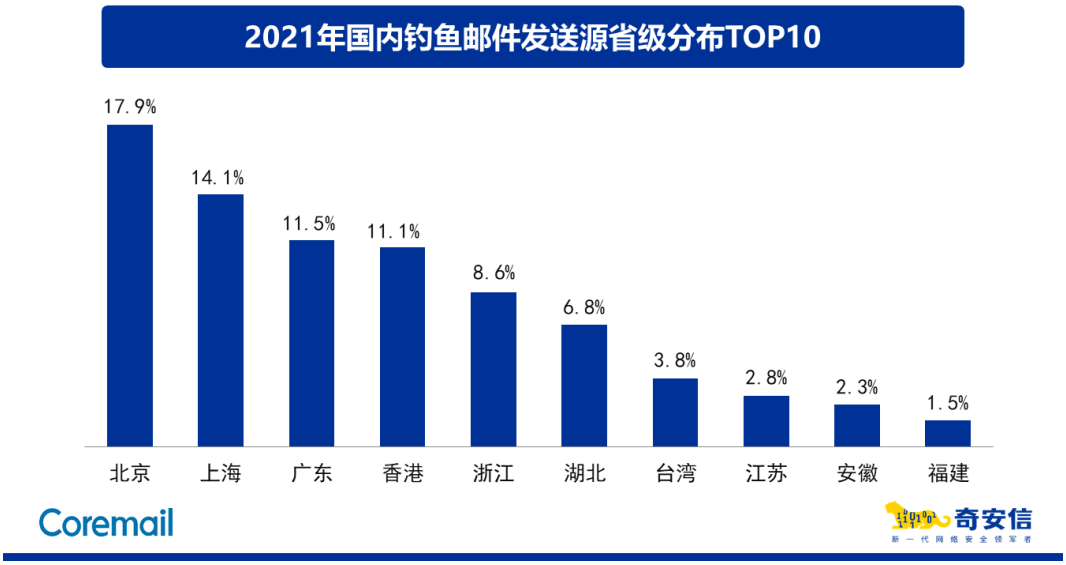
2021 年全国企业邮箱用户收到的钓鱼邮件数量约占企业级用户邮件收发总量的 4.5%，平均每天约有 0.9 亿封钓鱼邮件被发出和接收。

二、　钓鱼邮件发送源

根据 Coremail 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，来自美国的钓鱼邮件最多，占国内企业用户收到的钓鱼邮件的 41.0%；其次是中国，约占 11.7%；新加坡排名第三，约占 5.3%。针对国内企业级用户发送垃圾邮件最多的十个国家及其发送钓鱼邮件数量的占比情况如下图所示。

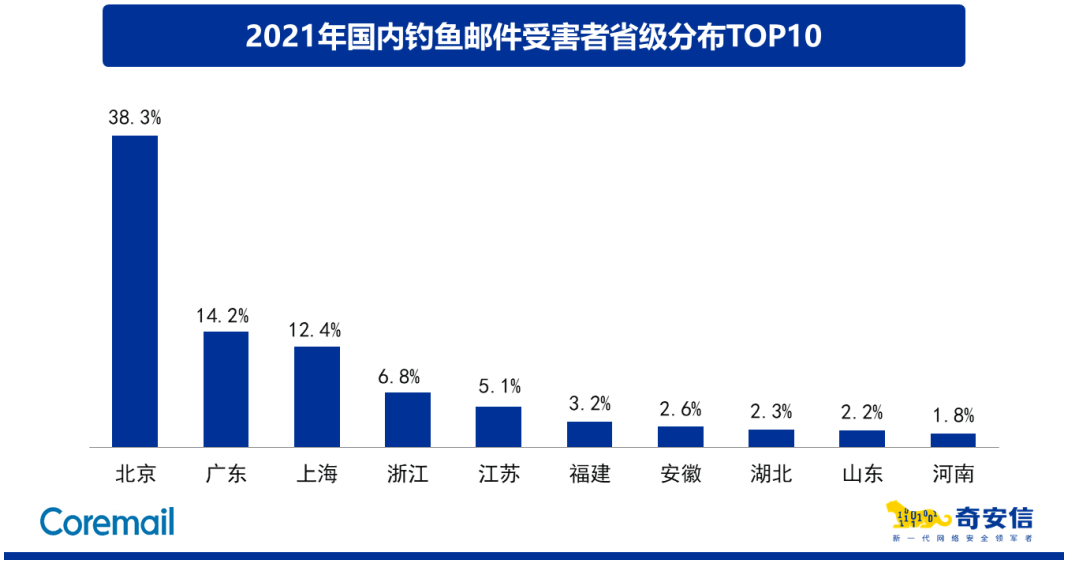


从钓鱼邮件的发送源服务器所在地来看，北京发送的钓鱼邮件最多，有 17.9%的钓鱼邮件来自北京的邮箱；另有约 14.1%的钓鱼邮件来自上海；约 11.5%的钓鱼邮件来自广东。国内钓鱼邮件发送源数量 TOP10 省级行政区分布如下图所示：

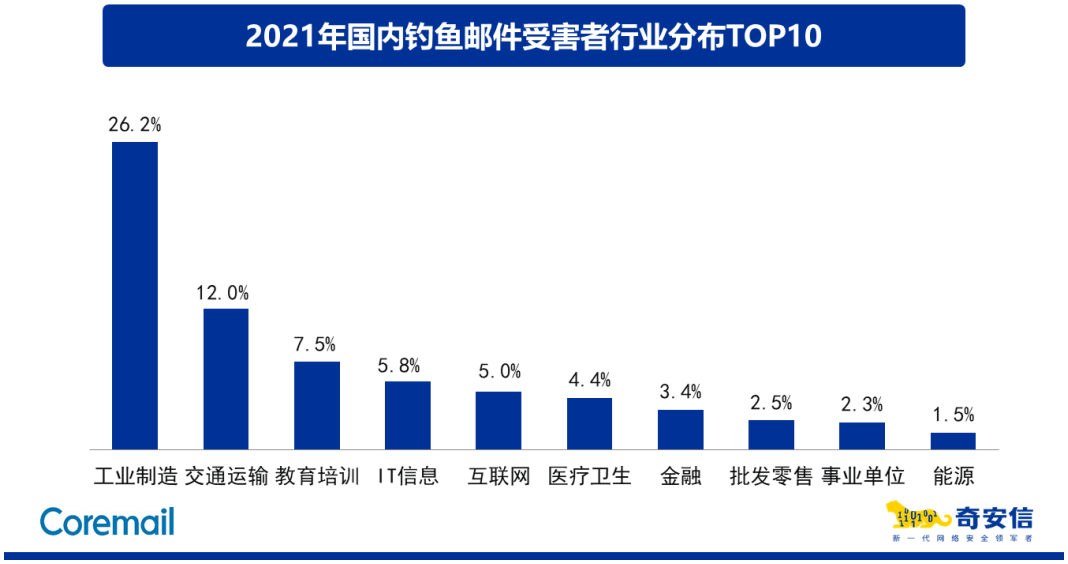


三、 钓鱼邮件受害者

从收到钓鱼邮件的受害者服务器所在地来看，北京收到的钓鱼邮件最多，有 38.3%的钓鱼邮件被发送至北京的企业邮箱用户；另有约 14.2%的钓鱼邮件被发送给广东用户；约 12.4%的钓鱼邮件被发送给上海用户。2021 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：



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 70.6%。其中，工业制造行业排名第一，约占钓鱼邮件总数的 26.2%；交通运输排名第二，约占 12.0%；排名第三的行业为教育培训，占 7.5%。具体 TOP10 行业排名如下所示。



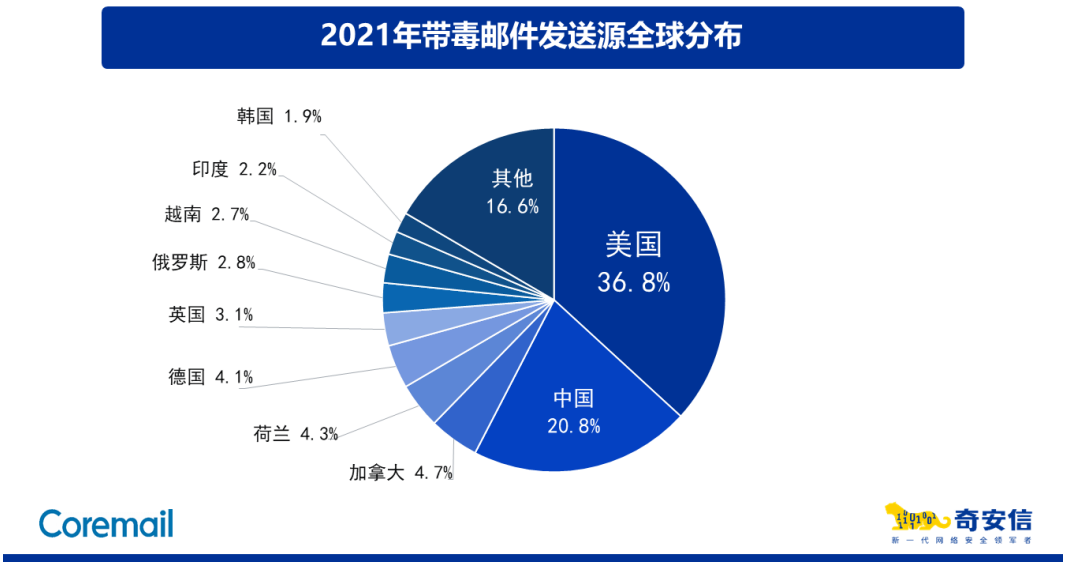
第四章　带毒邮件

一、　带毒邮件的规模

根据 Coremail 与奇安信行业安全研究中心联合监测评估，2021 年，全国企业级用户共收到约 609.5 亿封带毒邮件，相比 2020 年收到的 492.1 亿封带毒邮件相比，同比增长了 23.9%。越来越多的带毒邮件正在被发送给企业邮箱。2021 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 7.98%。平均每天约有 1.7 亿封带毒邮件被发出和接收。

二、　带毒邮件发送源

Coremail 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洲。其中，来自美国的带毒邮件最多占全球带毒邮件的 36.8%；中国排名第二，占 20.8%；加拿大排名第三，占 4.7%。针对国内企业级用户发送带毒邮件全球分布及占比情况如下图所示。



第五章　邮件安全应急响应案例

一、下载破解软件，导致内网终端自动发送恶意邮件

（一）事件概述

2021 年 3 月，奇安信安服应急响应团队接到制造业某企业应急响应请求，其内网中多个终端出现自动发送恶意邮件行为，希望对该事件进行分析排查处理。

应急人员抵达现场后对邮件样本进行分析，判断该病毒为“永恒之蓝下载器木马”家族的最新变种。分析邮件日志发现，第一封恶意邮件于事发当天 15:32 由员工 A 邮箱发出。对员工 A 主机进行分析发现，该主机中天擎存在多个“永恒之蓝下载器木马”恶意文件拦截记录。继续对其系统日志及计划任务分析发现，事发当天员工 A 主机曾成功执行永恒之蓝下载器木马恶意计划任务。

应急人员与员工 A 沟通了解到，他半年前曾通过第三方渠道下载某破解版软件，从安装该软件之后，天擎就曾有相关拦截提示。事发当天，因误操作，对天擎弹出的拦截提示点了“允许请求”。

经过最终分析研判确定，因员工 A 安全意识不足，安装了携带木马的破解版软件，导致个人主机感染“永恒之蓝下载器木马”病毒，后又因误操作对天擎弹出的告警点击了“允许请求”，导致病毒下载执行了挖矿模块和邮件攻击模块，并以员工 A 主机为源头，通过读取邮箱通讯录，向其联系人发送恶意邮件导致了内网大范围传播。

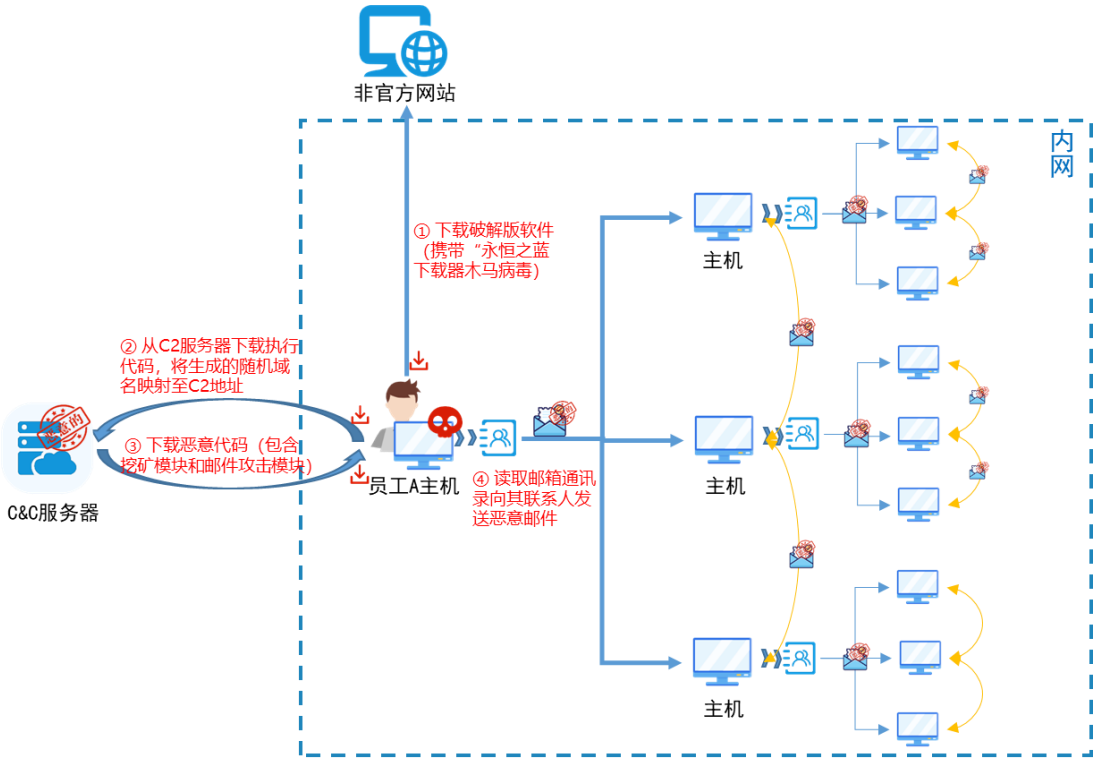


图 2-7：攻击路径图

（二）防护建议

1) 禁止或限制个人 PC 接入内网，如业务需要，增加访问控制 ACL 策略，采用白名单机制只允许对个人 PC 开放特定的业务必要端口，其他端口一律禁止访问；

2) 禁止通过非官方渠道下载应用软件，不随意点击来历不明的链接，加强内部人员安全意识；

3) 浏览网页或启动客户端时注意 CPU/GPU 的使用率，出现异常时，及时排查异常进程，找到挖矿程序并清除；

4) 加强日常安全巡检制度，定期对系统配置、系统漏洞、安全日志以及安全策略落实情况进行检查，及时修复漏洞、安装补丁，将信息安全工作常态化。

二、APT 组织利用钓鱼邮件进行攻击

（一）事件概述

2021 年 6 月，奇安信安服团队接到制造业某企业应急响应求助，该企业反馈办公网疑似被 APT 组织攻击，要求协助进行排查并溯源。

应急人员抵达现场后，删除恶意计划任务、恶意进程、木马文件，对失陷主机进行全盘查杀，并溯源攻击路径发现：攻击者为蔓灵花 APT 团伙。蔓灵花 APT 团队使用 songxxx@mfa.xx.cn 邮箱账号向该单位内网发送钓鱼邮件，受害主机（x.x.x.103）使用者下载并运行了钓鱼邮件中的木马文件。木马文件落地后在主机中创建恶意计划任务 DefenderUpdater 及恶意进程 msicexec.exe，使受害主机每隔 15 分钟向 APT 恶意域名 webmailcgwip.com/xingsu/asp.php 发送下载恶意程序请求，同时将发起请求的主机名和用户名信息上传。

（二）防护建议

1) 定期进行内部人员安全意识培训，禁止点击来源不明邮件附件，禁止将敏感信息私自暴露至公网等；

2) 安装杀毒软件并定期更新病毒库，开启杀毒软件对邮件附件的扫描功能，有效识别恶意附件；

3) 禁止或限制个人 PC 接入内网，如有业务需要，加强访问控制 ACL 策略，采用白名单机制只允许对个人 PC 开放特定的业务必要端口，其他端口一律禁止访问；

4) 部署高级威胁监测设备，及时发现恶意网络流量，同时可进一步加强追踪溯源能力，对安全事件发生时可提供可靠的追溯依据；

5) 加强日常安全巡检制度，定期对系统配置、系统漏洞、安全日志以及安全策略落实情况进行检查，及时修复漏洞、安装补丁，将信息安全工作常态化。

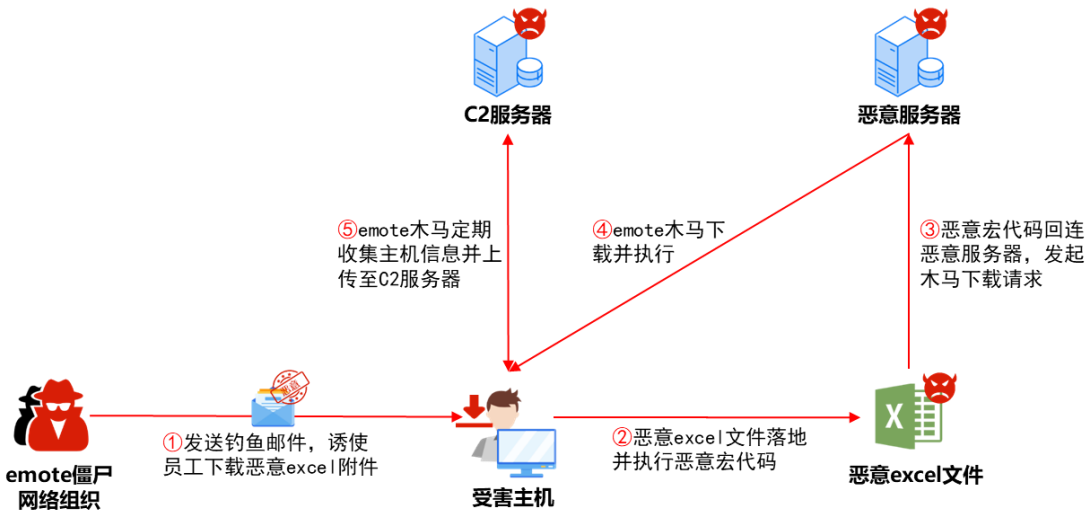
三、能源行业某客户内网收到钓鱼邮件应急事件处置

（一）事件概述

2021 年 12 月，奇安信安服团队接到能源行业某客户应急响应求助，公司内部收到数千封钓鱼邮件，客户期望对钓鱼邮件内容进行分析并排查疑似感染终端情况。

应急人员抵达现场后，对钓鱼邮件内容进行查看发现，邮件所带附件是一个压缩包，应急人员将其下载至沙箱并解压，发现压缩包内为多个带有恶意宏代码的 excel 文件，打开后会诱导用户启动宏功能，为自身恶意宏代码创造执行条件。恶意宏代码运行后，会调用 powershell 回连恶意服务器将 Emotett 木马病毒下载至本地并执行。Emotet 木马会定期收集主机信息并将数据加密上传至 C2 服务器，使服务器沦为 Emotet 僵尸网络中的一员。

根据客户反馈，应急人员对疑似点击了钓鱼邮件的 3 台员工电脑进行病毒查杀及特征排查，均未发现其它异常。至此，应急人员确认，本次攻击并非针对单一用户的定向攻击，是 Emotet 僵尸网络在全网范围的钓鱼邮件投递。投递的钓鱼邮件附件内包含带有恶意 excel 4.0 宏代码的 excel 文档，功能为下载并执行 Emotet 木马，进而控制受害终端。



（二）防护建议

1) 加强人员安全意识培养，不要点击来源不明的邮件附件，不要从不明网站下载软件。对来源不明的文件包括邮件附件、上传文件等要先杀毒处理；

2) 部署邮件安全检测设备，对外部邮件进行安全检测，提高垃圾邮件、恶意邮件识别及过滤能力；

3) 建议安装防病毒软件，及时拦截病毒落地，并且定期进行全面扫描，加强服务器病毒预防、抑制及清除能力；

4) 部署高级威胁监测设备，及时发现恶意网络流量，同时可进一步加强追踪溯源能力，在安全事件发生时可提供可靠的追溯依据；

5) 加强日常安全巡检制度，定期对系统配置、系统漏洞、安全日志以及安全策略落实情况进行检查，及时修复漏洞、安装补丁，将信息安全工作常态化。

四、【补贴】主题钓鱼邮件泛滥

（一）事件概述

某企业部分员工遭遇工资补助诈骗的新闻成为热门话题。据悉，该公司员工 18 日早收到一封自称是 “财务部”发来的《5 月员工工资补助通知》邮件，大量员工按照附件要求扫码，并填写了银行账号等隐私信息。结果不仅没领到补助，反而损失了银行卡余额。同样操作手法的诈骗案多次出现，已有多个互联网公司中招

Coremail 进行主动追溯后发现，该类诈骗钓鱼邮件正文内容为国家下发工资补贴通知，并在正文中放置了一张二维码图片，诱导受害者扫描正文中二维码。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。

该主题的钓鱼邮件从 2021 年 12 月持续泛滥至 2022 年 6 月，攻击手法逐渐转变为先盗号，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。

主题也逐渐发展为【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】。

2022,Q1 工资诈骗类钓鱼邮件

2022,Q2 工资诈骗类钓鱼邮件

Coremail 已对拦截策略进行优化，同时将此类邮件的相关特征更新到云端特征库。目前 CAC 中心已实现对相似特征的有效拦截。

在全行业的围剿下，黑产团伙狡猾地转变了钓鱼思路，钓鱼邮件类型从正文展现变为附件型钓鱼，将诈骗内容变为将内容存放至 pdf、word、txt 或其他加密附件中，以逃避企业邮箱厂商的反垃圾检查或邮件网关拦截。

（二）防护建议

1) 使用 CACTER 邮件安全网关拦截钓鱼诈骗邮件攻击

2) 提高邮箱密码策略要求，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) 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。

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

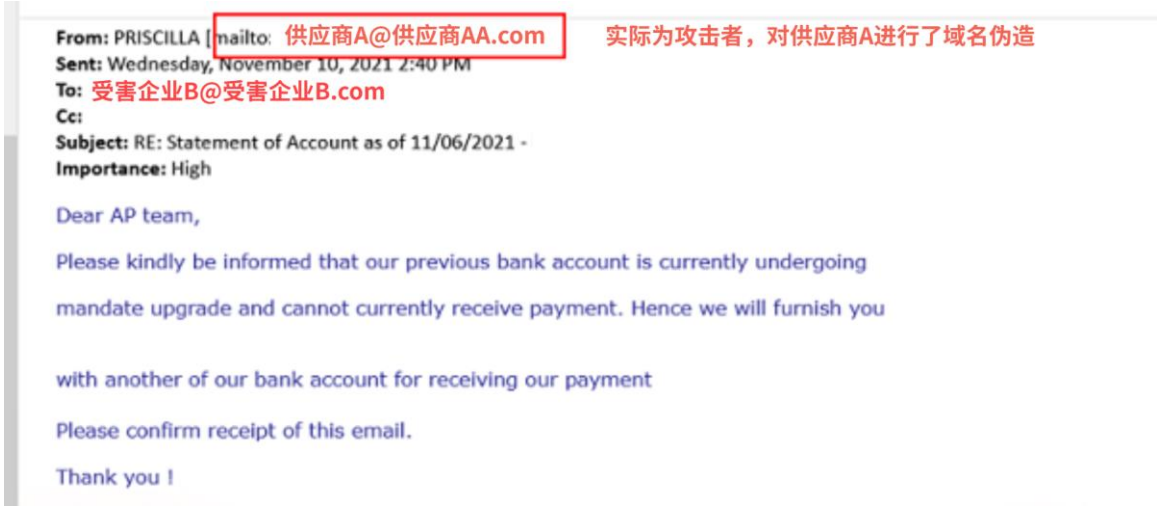
6) 如遇可疑情况，可拨打 96110 咨询求助；或下载国家反诈中心 APP，关注国家反诈服务公众号，学习防骗知识，防诈反诈。

五、BEC（Business Email Compromise）商业邮件诈骗

（一）事件概述

2021 年 11 月，Coremail 收到客户求助，称其在汇款时发现遭到诈骗。调查发现，诈骗团伙冒充企业原有供应商，多次与企业往来邮件，获取信任后要求更换汇款银行账号。经排查该诈骗团伙使用仿冒域名【@供应商 AA.com】发送邮件。此仿冒域名与实际域名【供应商 A.com】高度相似，因此可以绕过 SPF 初查防护。

进一步排查供应商邮件系统发现，此邮件并非由实际供应商 A 域名发出，且实际供应商 A 域名旗下邮箱账号并未被盗，推测为诈骗团伙通过盗取受害企业内部邮箱账号，获得企业通讯录及邮件内容，而后假冒供应商发起商业诈骗。



要求业务汇款的 BEC 诈骗邮件

此类案例通常被称为 BEC（Business Email Compromise）商业邮件诈骗。通常 BEC 攻击可以被分为九种类型，主要是根据攻击者采用的欺诈请求方式进行分类。例如冒充供应商，员工或客户进行发信钓鱼，BEC 通常伴随着多种攻击手法混合，包括域名伪造，接管被盗帐户等。

在 BEC 诈骗前期，犯罪分子通过鱼叉式钓鱼、社会工程学、恶意软件等方式盗取客户邮箱账密，并通过被盗账号了解目标公司的业务流程，高管邮箱，业务内容等，再通过仿冒目标公司域名的账号接入邮件会话中，并发起转账诈骗需求或偷偷替换银行账户等行动。

在这套攻击流程下，攻击者可以把 BEC 编造得天衣无缝、真实可信，使得受害者往往在遭受大量金钱损失后方才察觉。

除域名伪造外，攻击者常用的攻击方式还包含以下 2 种特征。

特征 A：抄送来自被冒充供应商的多个角色

为了提升 BEC 的可信度，攻击者在最初阶段会同时将邮件抄送五个同伙（一般是冒充供应商员工的犯罪分子），同伙常常扮演真实供应商的财务或行政员工。

特征 B：初始请求风险极低

通常，攻击者的初始请求只是简单地要求对方确认一份转账表单，不含任何敏感信息。然而，一旦目标公司员工进行了回复，就会与攻击者之间建立起信任链，随着交流的加深，攻击者与其他员工的互动将会逐渐可信。

对应的防御手法还包括：域名仿冒检测、域名信息分析、邮件内容分析。

然而，由于 BEC 往往不携带可检测的 URL 或恶意附件等钓鱼特征，因而能轻易地避开大多数成熟的安全防护技术，逃避邮箱系统的反垃圾反钓鱼检查，员工受骗后，最终给企业带来不可挽回的巨大损失。

（二）防护建议

1) 使用CACTER邮件安全网关对邮件进行域名仿冒检测、域名信息分析、邮件内容分析，拦截BEC诈骗邮件。

2) 提高警惕，业务审批层层确认，涉及款项往来务必多方核实。

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

4) 如遇可疑情况，可拨打 96110 咨询求助；或下载国家反诈中心APP，关注国家反诈服务公众号，学习防骗知识，防诈反诈。

附件 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、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。

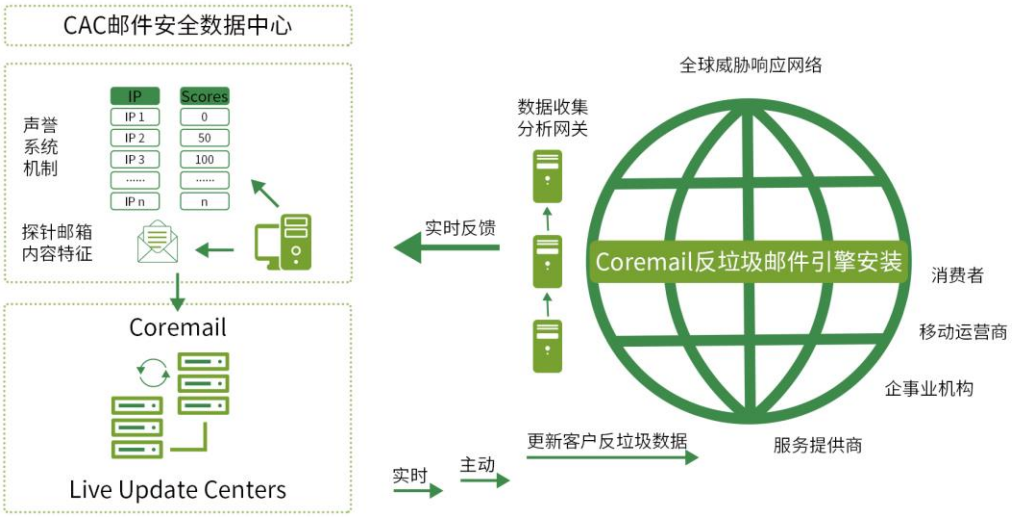
产品优势

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。

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。



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。

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。

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——NEVER1.0、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。

联系我们

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

附件 2　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。

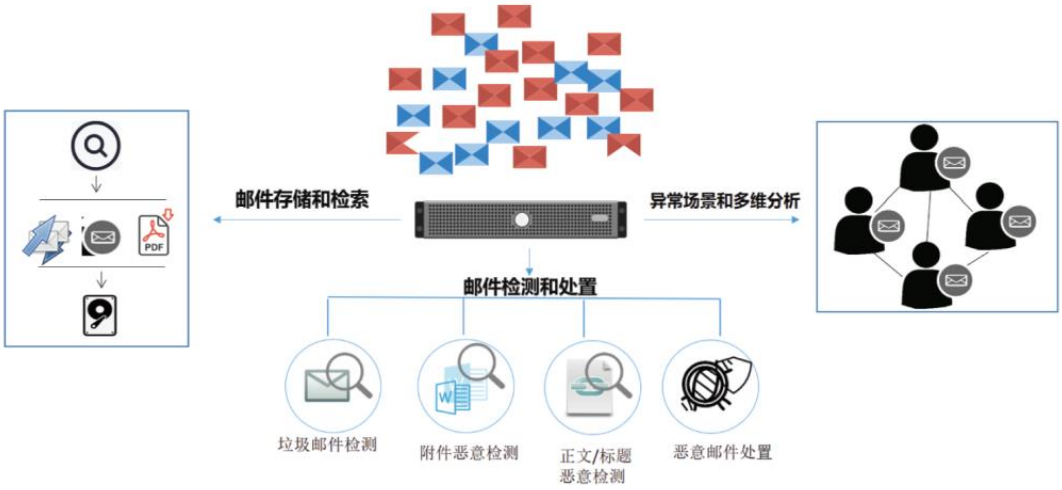
看得见的投入产出比

- 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，准确高效的检出钓鱼 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/skyeye_MTDS
服务热线：4008-136-360
微信咨询：奇安信集团