2025 守内安信息科技 & ASRC
第二季度邮件安全观察

ASRC

Spam Mail
Virus Mail
Malicious Mail

July 2025 released.

本季 ASRC 揭露了多起邮件系统相关的重大安全事件。在邮件系统漏洞方面，本季暴露出多个具有严重威胁的安全漏洞。其中，Microsoft Office Outlook 存在的「目录遍历」(path traversal) 漏洞 CVE-2025-47176 尤为值得关注。攻击者仅需凭借一般用户权限，攻击者可借由「.../...//」序列，就能轻易绕过系统的路径限制，该漏洞极大地拓展了潜在攻击面，使得大量用户的系统安全面临直接威胁。

与此同时，其他邮件系统也相继出现安全隐患，如 4 月份日本知名 Web 邮件系统 Active! Mail 被发现存在高风险的堆栈缓冲区溢出漏洞 CVE-2025-42599，该漏洞因系统未正确限制写入长度，攻击者可借此覆写堆栈内存结构，进而操控程序流程并触发远程任意程序代码执行 (RCE)；6 月份，邮件服务器 Roundcube 也被揭露存在重大漏洞 CVE-2025-49113，且在漏洞曝光短短三天内，暗网就出现了贩卖该漏洞利用方法的信息，显示出其极高的风险性。

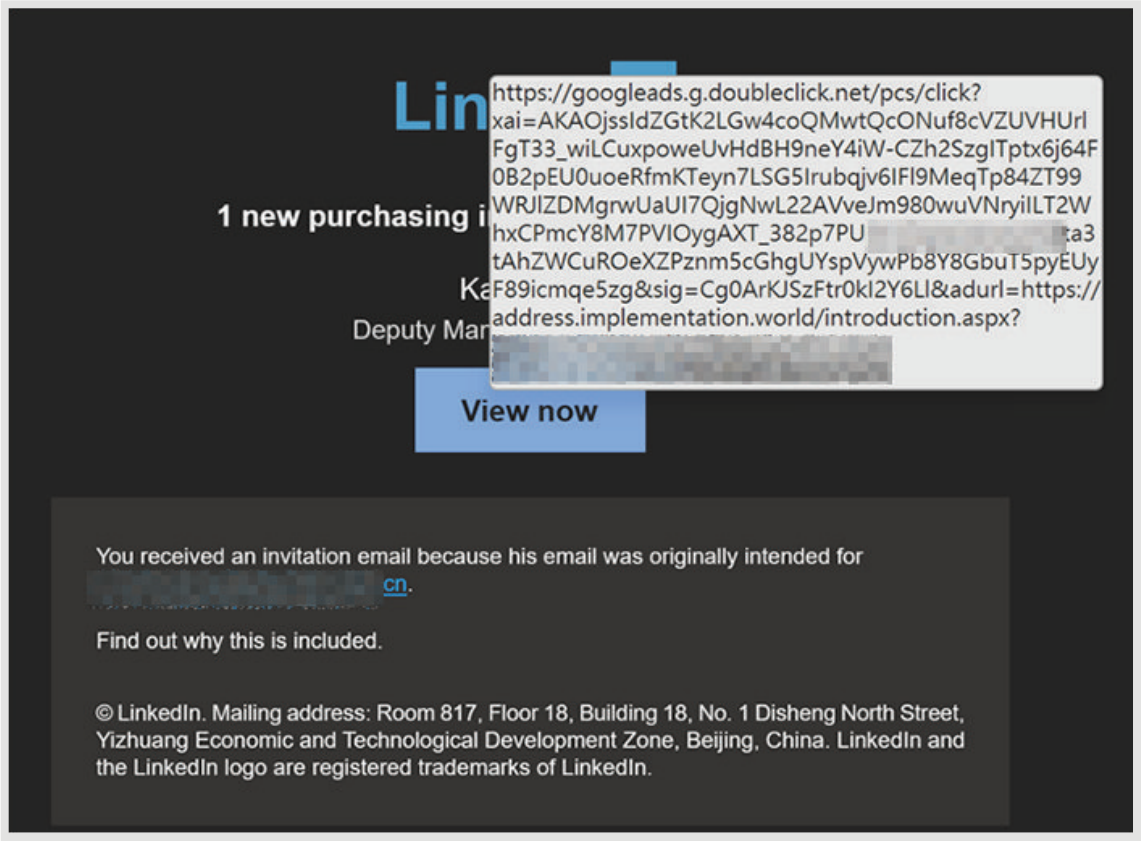
在邮件攻击活动方面，3-5月期间，滥用合法信任来源的钓鱼邮件活动呈大规模爆发态势。众多攻击者利用政府、机关组织或学校网域，通过 outlook.com 等邮件服务器发送恶意邮件。这些邮件中往往夹带 forms.clickup.com 的钓鱼链接，借助 ClickUp 的在线表单功能，伪装成正常请求，诱使收件人提交敏感数据或点击恶意链接。值得注意的是，此类钓鱼邮件大多来自遭入侵的合法账号，凭借合法身份的伪装，极大地提升了收件人的信任度，使得攻击行为更具隐蔽性和欺骗性。

攻击者通过 forms.clickup.com 嵌入的伪造表单，引导目标用户访问精心设计的虚假登入页面，从而窃取 Microsoft 365 或其他云端服务的登入凭证。当前，这种利用合法域名与平台进行绕过式伪装的银狐木马钓鱼手法正处于高发期，能够有效规避众多传统安全检测机制，对 Microsoft 365 用户的账户安全构成了严重威胁。

forms.clickup.com 表单，被用来收集 Microsoft 365 用户的敏感资料

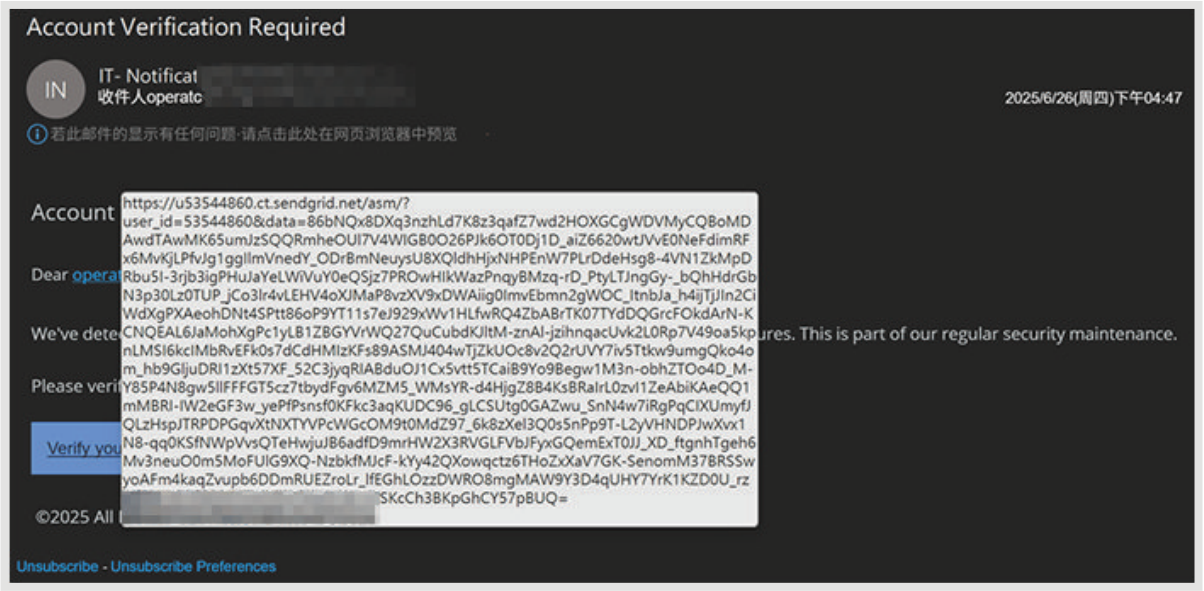
此外，开放重定向（Open Redirect）机制也逐渐成为攻击者实施钓鱼攻击的重要工具。该机制原本用于提升用户体验或进行使用分析，但在缺乏有效验证机制的情况下，被攻击者恶意利用。大量来自知名网站或大型平台，如云端服务供应商、政府或教育机构网站、企业入口页等的开放重定向漏洞，由于其域名本身具有较高的信任度，成为了钓鱼网站的“保护伞”。

攻击者将钓鱼网址巧妙包装在可信网域的跳转参数中，轻松骗过收件人、安全扫描机制，甚至能够绕过浏览器的安全警告或封锁措施。令人担忧的是，部分服务的开放重定向漏洞已被长期滥用却仍未得到有效修复，这凸显出业界在信任机制与网域声誉管理方面存在的严重不足。



来自知名的域名或服务，但被用于导向钓鱼网站，有机会骗过收件人、信息安全检测机制或浏览器的安全检查

在邮件传播渠道方面，钓鱼邮件常常滥用合法的 EDM（电子邮件营销）发送平台。攻击者利用这些信誉良好、广泛使用的平台，将钓鱼邮件伪装成正常的促销信或服务通知，以此欺骗用户和安全系统。由于 EDM 平台设计侧重于邮件投递的效率与送达率，难以实时识别和阻止个别账号的滥用行为，即便部分平台引入了内容扫描与异常行为侦测功能，也难以抵御针对性强、伪装精细的钓鱼邮件攻击。因此，传统的“信任平台即信任邮件”的信任模型已难以适应如今的安全形势。为提升邮件安全，应将 EDM 的信任基础从“企业单位”下沉至“个人层级”，用户仅对主动订阅并确认过的寄件来源建立信任，同时定期管理自己的订阅名单；系统层面则需强化对 EDM 类邮件的验证与过滤策略，降低因盲目信任平台而带来的安全风险。



常见的合法 EDM 发送机制遭到滥用以发送钓鱼邮件

综合本季观察，邮件攻击呈现出五大显著趋势：

- 滥用合法资源，攻击者偏好利用已建立信任的云端服务、知名邮件平台以及遭入侵的机构账号，通过“信任转嫁”绕过传统安全侦测
- 漏洞快速武器化，尤其是低权限即可触发的漏洞，攻击者无需管理员权限便能渗透系统，攻击效率大幅提升
- 信任链渗透，攻击者从平台服务及其漏洞入手，将合法资源转化为攻击跳板
- 低权限即可入侵，降低了攻击门槛，扩大了攻击范围
- 多层混合式攻击手法，结合社交工程、假登入页、跨平台整合等多种技术，使得攻击手段更加复杂隐蔽

面对日益复杂隐蔽的邮件攻击态势，单纯依靠企业自身的单点防御措施已无法有效抵御攻击链的侵袭。构建有效的邮件安全防护体系，需要跨单位、跨平台的紧密协作，整合威胁情报，共享信任评级，才能及时发现并切断复合型攻击的传播路径，切实保障邮件系统及用户信息的安全。

关于 ASRC 威胁邮件研究中心

ASRC 威胁邮件研究中心 (AsiaSpam-message ResearchCenter)，与守内安长期合作，致力于全球垃圾邮件、威胁邮件、钓鱼邮件、网络攻击等相关研究，运用相关数据统计、调查、趋势分析、学术研究、跨界交流、研讨活动等方式，与学术，行业及政府共同推动净化电子邮件使用环境。