2025 守内安信息科技 & ASRC
第一季度邮件安全观察

ASRC

Spam Mail
Virus Mail
Malicious Mail

May 2025 released.

2025 年，邮件安全趋势强调更严格的身份验证要求。Gmail 和 Yahoo 等主要邮件服务提供商除了持续推动 SPF、DKIM 和 DMARC 等认证协议的采用，还逐步将目标指向 DMARC 的 p=reject 邮件策略，以防止域名被冒用。发送来源的验证与检测也逐渐从 IP 信誉转向域名信誉。一月底披露的 7-Zip 软件重大安全漏洞（CVE-2025-0411）已被俄罗斯网络犯罪分子用于攻击乌克兰。攻击者通过邮件携带恶意附件，并利用该漏洞绕过 Windows 系统的 MotW（Mark of the Web）安全机制，诱骗受害者在计算机上执行恶意软件，最终导致数据泄露或设备被控制。除了需警惕可疑邮件外，建议尽快将 7-Zip 更新至最新版本以修复该漏洞。

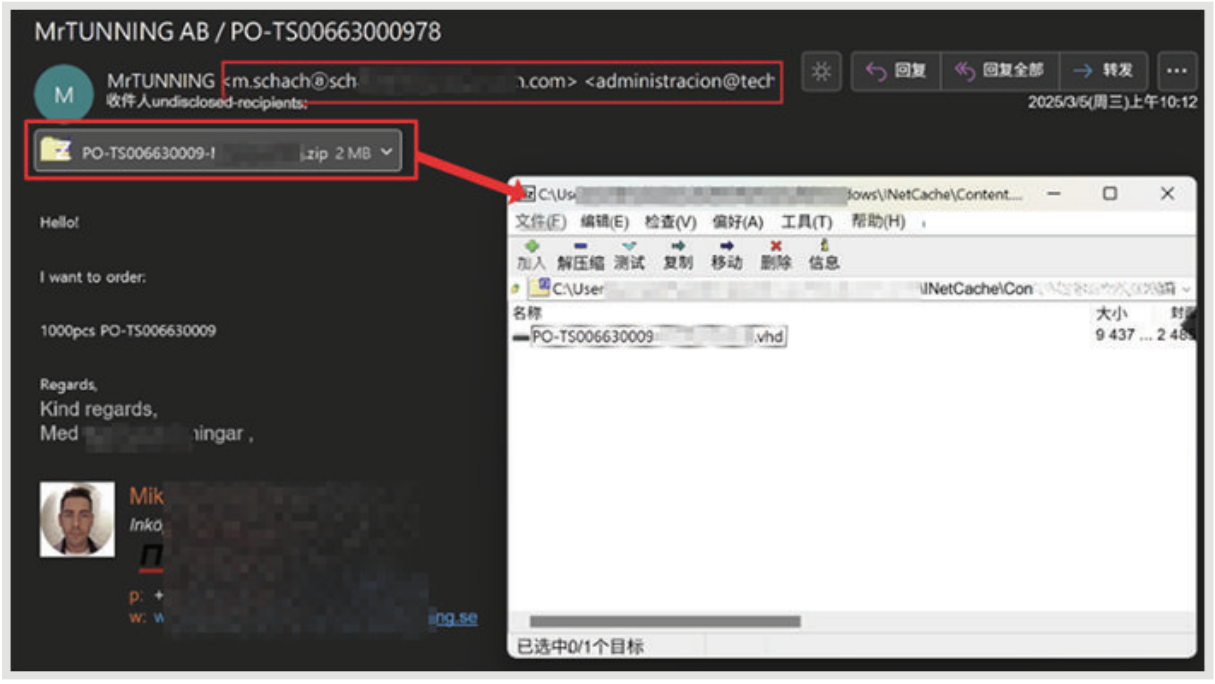
此外，CVE-2025-21298 也值得关注。这是一个影响 Microsoft Office 和 Windows 操作系统的严重漏洞，涉及 OLE（对象链接与嵌入）技术。攻击者可利用精心设计的文件，在未经用户允许的情况下执行任意代码。尽管目前公开数据中尚未明确记录该漏洞通过电子邮件攻击的实际案例，但根据漏洞特性及历史攻击模式，此漏洞极可能被用于以下场景：

- **恶意附件攻击：**
  攻击者伪造电子邮件并附加特制的.rtf 文件，诱使用户打开后触发漏洞。
- **社交工程结合漏洞利用：**
  以税务通知、账单等名义发送钓鱼邮件，诱导用户下载并打开恶意文件（可能通过网页下载）。

以下是本季度值得关注的邮件样本：

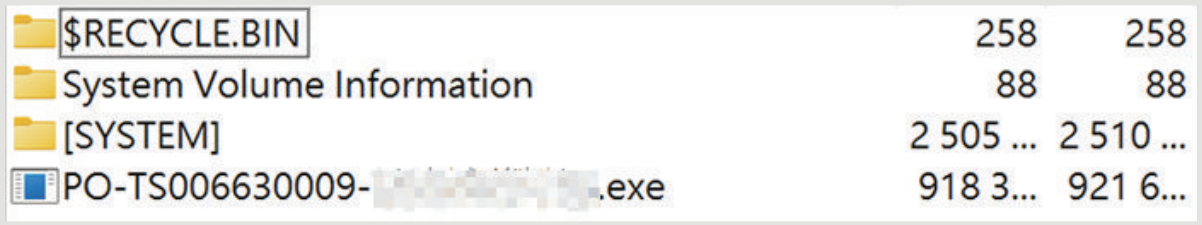
压缩文件夹携带 .VHD 的攻击

本季度我们发现部分攻击邮件通过 .zip 压缩包携带 .VHD 文件。.VHD 文件可被 Windows 系统识别为虚拟硬盘，当用户打开时，系统会将其挂载为新驱动器。在此类攻击邮件中，发件人字段被填入两个电子邮件地址，试图让收件人误以为邮件由第一个地址发送。为规避发件人检查，攻击者还将第一个地址中的“@”替换为视觉相似的符号。



恶意附件以 .zip 的方式，包装了一个 .VHD 文件

若展开 .VHD 文件，会看到完整的虚拟硬盘结构，其中 .exe 文件为恶意程序本体，且不会被Windows 系统标记为 MotW。攻击者还将该程序图标伪装成 Excel 文件，诱骗用户执行。一旦运行，恶意软件便会植入后门。



.VHD 文件解压后 .exe 文件即为恶意攻击程序的本体

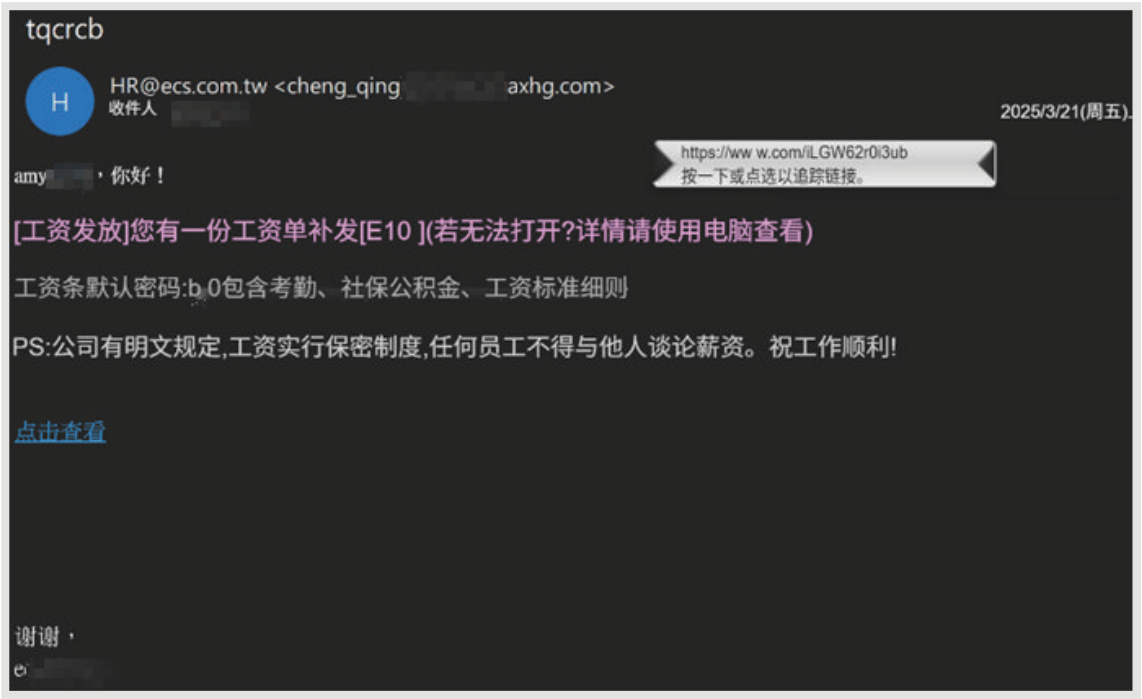
若企业日常业务无需通过邮件传输 .VHD 文件，建议直接在邮件安全扫描或过滤机制中拦截此类附件。类似少用但常被攻击的 .ISO、.IMG 文件也可考虑一并隔离。

社交工程诱骗

通过社交工程手段诱导用户执行特定操作，一直是诈骗和钓鱼攻击的高效手法。本季度我们观察到多起高度仿真的恶意邮件，其本身不携带恶意附件，而是诱导用户点击链接下载“加密”的恶意程序。由于文件经过加密，可绕过下载安全审核、浏览器及 Windows 的 MotW 防护，甚至部分杀毒软件的检测。此类攻击还可能要求用户登录验证（窃取账号密码）或输入信用卡信息（如支付运费、手续费等），需格外警惕！

登录验证类钓鱼邮件

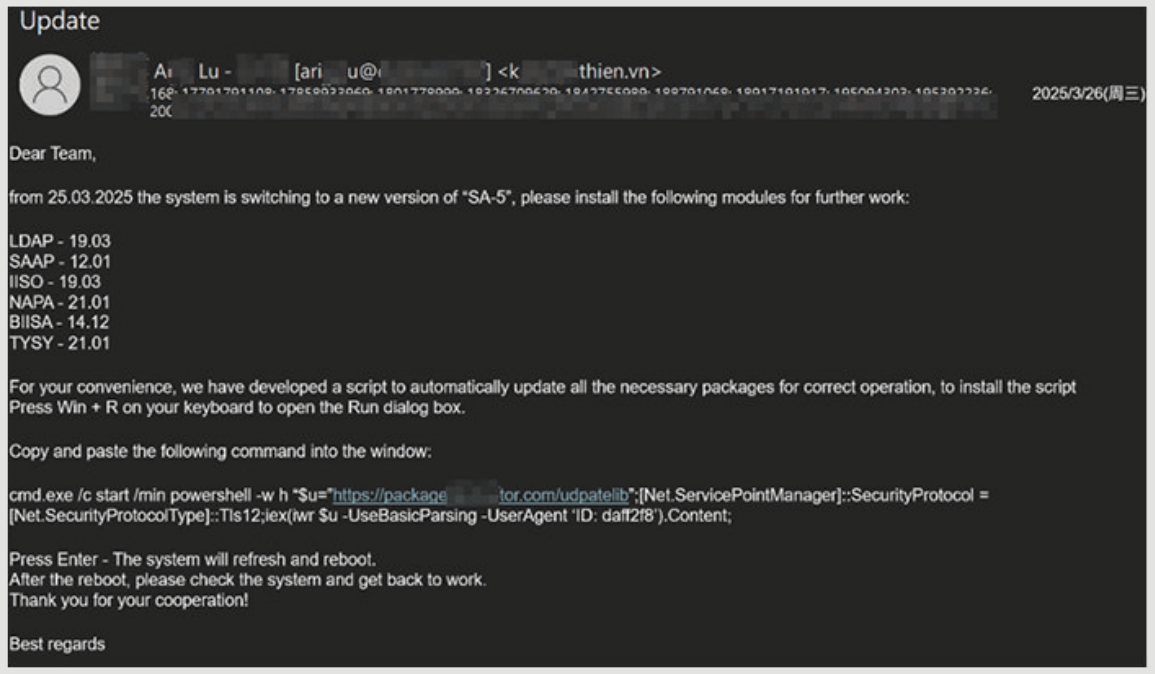
诱骗点击下载并执行恶意软件



以工资单为名，诱骗受害人点击并下载恶意软件

技术支持攻击

我们监测到一种特殊的社交工程攻击。收件人会收到一份系统更新或升级的操作通知，其中详细列出操作步骤。实际上，这是攻击者伪造的技术支持邮件，诱骗用户下载名为 netscanner.exe 的后门程序并执行，目的是窃取数据。值得注意的是，截至发稿时，主流杀毒软件仍无法识别该文件的风险。



黑客诱骗收件人下载并执行文件名为 netscanner.exe 的后门程序

此类攻击早期多见于网页浏览场景，例如页面突然弹出系统故障警告，要求用户联系“技术支持专员”或下载“Click Fix”修复工具并指导“修复”步骤，通过社交工程的手段，诱导用户一步步在计算机中埋入后门。如今，攻击者开始通过邮件传播此类手法！

结论

网络安全威胁不断演变，安全策略和意识培训也需同步更新。邮件安全部署可参考“最小权限原则”：仅允许发送合理使用的附件类型，对特殊附件默认拦截并人工审核，再根据实际情况调整策略；同时限制内部群组邮件的收件范围，减少暴露风险。

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。