2026 守内安信息科技 & ASRC
第三季度邮件安全观察



ASRC

Spam Mail
Virus Mail
Malicious Mail

Oct 2026 released.

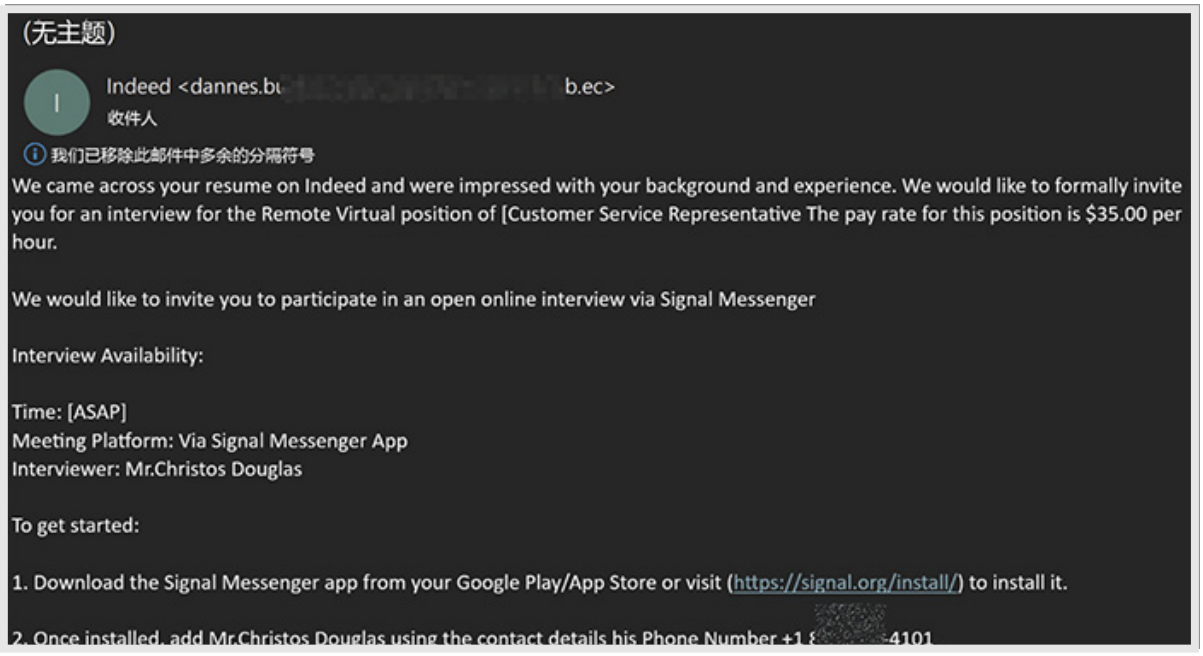
2026 年第三季度，邮件安全威胁呈现显著的攻击手段升级。自第二季末起，针对邮件服务器的 DoS 攻击大幅增加，持续消耗企业邮件系统资源。同时，社会工程学与升级的规避技术结合成为主流。攻击者大量转向云原生就地利用（Living off the Cloud, LotC,）策略，并滥用 VHDX 虚拟硬盘格式等新兴威胁载体（Threat Vector）进行恶意软件派发。这些演化预示黑客正在积极尝试能够绕过传统端点防护与静态网址扫描的高级防御规避（Defense Evasion）技术，企业需重新评估现有的邮件安全边界。

2026 Q3 关键攻击样本与手法剖析

留意求职诈骗

攻击者持续锁定求职网站，利用履历上的联络方式发送待遇优厚的招聘邮件，并以急迫语气要求通过加密通讯软件进行远程面试。此手法利用求职者急于谋职的心理，设法骗取个人信息、汇款手续费、假支票诈骗或是植入后门，欺骗性较强。实际操作上，攻击者常在攻击准备阶段，利用公开社交媒体信息与求职平台开展目标试探与情报搜集等前置作业。

与真实求职信相比，此类诈骗邮件通常不揭露具体公司信息，缺乏详细职务说明，对目标背景描述模糊，且多使用非正式联络渠道。为躲避过滤系统，攻击者亦可能伪造合法发件人身份，或利用已遭入侵的邮件系统发送邮件。这类邮件排版通常较不正式，不采用企业标准面试模板文案，而是私下诱导目标使用私人加密软件进行面试或联络。若担心错失真实面试机会，应通过亲自查证过的官方联络渠道核实信息，切勿直接回复邮件或点击邮件中的私下联络链接。


(无主题)

I Indeed <dannes.b[redacted]b.ec>
收件人

我们已移除此邮件中多余的分隔符号

We came across your resume on Indeed and were impressed with your background and experience. We would like to formally invite you for an interview for the Remote Virtual position of [Customer Service Representative The pay rate for this position is $35.00 per hour.

We would like to invite you to participate in an open online interview via Signal Messenger

Interview Availability:

Time: [ASAP]
Meeting Platform: Via Signal Messenger App
Interviewer: Mr.Christos Douglas

To get started:

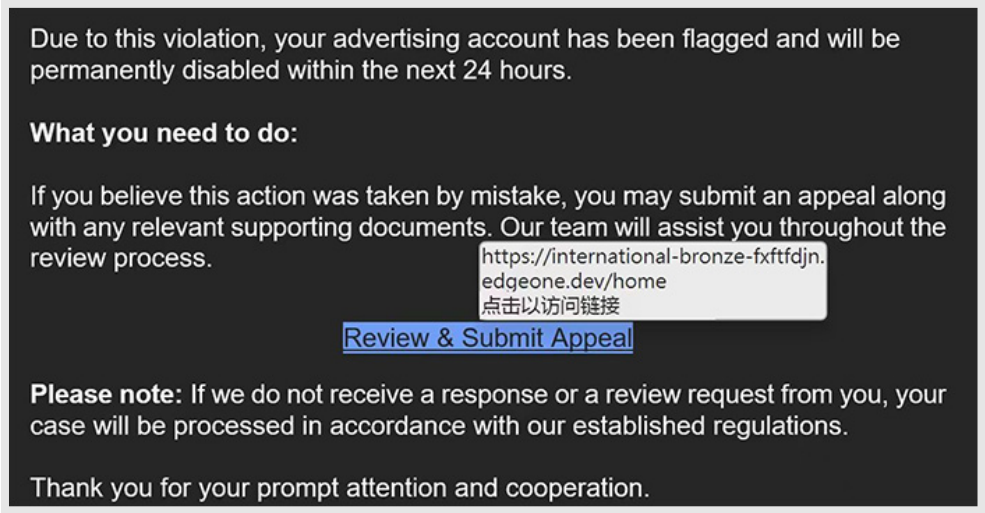
1. Download the Signal Messenger app from your Google Play/App Store or visit (https://signal.org/install/) to install it.

2. Once installed, add Mr.Christos Douglas using the contact details his Phone Number +1 [redacted]4101

求职诈骗邮件，要求私下以加密通讯软件进行远程面试

云原生就地利用（LotC）攻击

本季度，我们观测到大量钓鱼邮件链接滥用合法的云端服务，该类攻击技术包含云原生就地利用（Living off the Cloud, LotC）以及可信站点就地利用攻击（Living off Trusted Sites, LOTS）。由于传统钓鱼网站容易被 AI 或安全浏览器侦测拦截，黑客正大规模转向使用合法云端平台实施攻击，目前约有近 50% 的钓鱼网站滥用合法云端服务来规避过滤系统。许多「钓鱼即服务（PhaaS）」套件也已预设支持将恶意页面部署在这类平台之上。



云原生就地利用（LotC）攻击示例

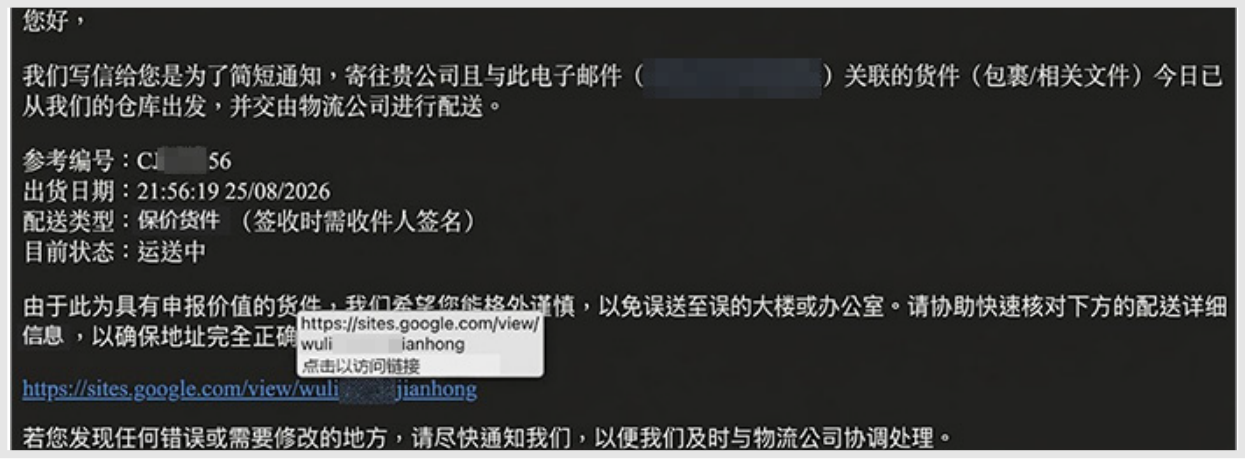
攻击者借助云端平台，可以极低的成本获得被浏览器信任的合法网站身份，还可利用服务自带的 CAPTCHA 人机验证机制，阻挡网络安全系统的自动化扫描。此外，攻击者会利用手机版 Google App 或 Chrome 浏览器的「分享（Share）」功能，将恶意网址自动转换为以 https://share.google/ 开头的随机混淆链接。这种经由合法分享机制完成的恶意改造，可以有效规避多数针对网址的静态扫描检测。



透过合法的“分享”功能对恶意超链接进行隐蔽的攻击

VHDX「虚拟硬盘」挂载攻击

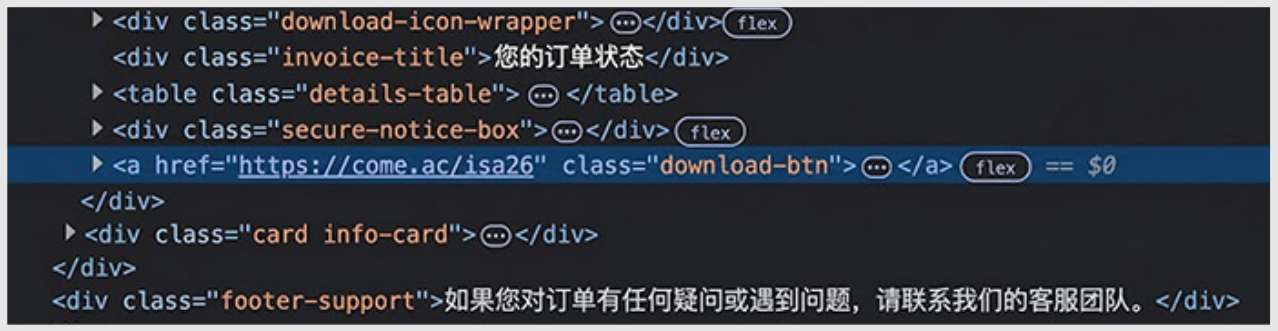
本季度也观测到多起利用 VHDX（Virtual Hard Disk v2，第二代虚拟硬盘）文件格式实施的恶意攻击样本。攻击者先通过 Google Sites 搭建看似合法的静态网页，诱骗受害者点击短链接，下载一份标称订单数据、实际大小达 164MB 的虚拟硬盘文件。该攻击利用体积异常庞大的 VHDX 文件，内部嵌套封装.img 磁盘镜像，以此绕过防病毒软件针对文件容量与格式的检测限制。当受害者被诱导将文件挂载为虚拟磁盘后，内藏的恶意 JavaScript 载荷才会暴露；载荷一旦执行，计算机极有可能被植入后门。此攻击链结合社会工程学与高级防御规避能力，反映威胁载体已经从传统恶意宏文档，演进为利用操作系统内置挂载功能的虚拟磁盘镜像文件。



伪造物流通知邮件



利用 Google Sites 搭建的仿冒静态页面



导向短链接，诱导下载约 164MB 的恶意虚拟硬盘文件

结论与建议

纵观本季度攻击手法，攻击者大量采用合法载体掩护恶意行为的攻击思路。无论是云原生就地利用（LotC），还是滥用操作系统原生挂载文件格式（VHDX、IMG），其核心均为防御规避。针对以上威胁趋势，建议落实以下防范措施：

- **落实电子邮件身份验证**
  企业应全面配置并严格执行 SPF、DKIM 与 DMARC 等电子邮件安全协议，防范域名伪造与商业电子邮件劫持诈骗（BEC），完成外部发件人身份校验。
- **升级动态检测与沙盒分析能力**
  针对 VHDX 或 ISO 等可挂载的镜像格式，传统防病毒软件常会因为文件体积过大而跳过扫描。企业可在邮件网关侧拦截非业务必要的虚拟硬盘扩展名；配置规则，将异常文件强制送入沙盒开展深层拆解分析，不可以单纯依据文件大小决定扫描深度。同时评估通过组策略（GPO），限制普通用户自动挂载磁盘镜像或可移动存储介质的权限。
- **遵循零信任架构，实施网页隔离防护**
  鉴于合法云端服务被大量用于 LOTS 攻击，仅依靠域名信誉评级的静态黑名单防护已经不足以抵御威胁。建议引入远程浏览器隔离技术（RBI），强化网页内容过滤；配套企业邮件安全策略，将来源不明、非业务用途的云端分享链接视为不可信流量进行拦截。
- **网络安全意识培训**
  面对邮件中要求脱离企业正规流程（例如使用私人通讯软件开展面试）、或是带有强烈急迫口吻的讯息，培养人员“默认存疑、多方核验”的习惯，切断社会工程攻击链。

关于守内安

守内安信息科技（上海）有限公司，是上海市政府及国家奖励支持的自主研发高科技创新的“双软认定企业”和“高新技术企业”，钻研邮件风险管理和信息安全内控管理。以电子邮件安全管理为核心，研发了一系列“电邮安全与合规”为中心的核心产品线，衍生到威胁防御与联合防御体系。守内安 20 年来秉承“以客为尊”的服务理念，树立了“服务・品质・值得信赖”的品牌理念，目前已拥有 7000+ 家全球性企业级用户，终端用户达 80,000,000+ 人次。



© 2026 Asia Spam-message Research Center. All Rights Reserved.