2026 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

Jul 2026 released.

2026 年第二季度，电子邮件安全环境面临典型的威胁平移。攻击者正加速从依赖传统的已知病毒特征，转向以规避防毒软件静态检测为核心的高级威胁形式（对应 MITRE ATT&CK: Defense Evasion）。数据显示，本季度带有恶意内容的邮件量较上一季暴增约 8 倍，并于今年 5 月达到峰值。

值得警惕的是，5 月恰逢多数企业开展内部演练，备战 HW 时期。极易被黑客利用此时间点发动真实攻击，从而衍生出严重的管理与通报风险：

1. **防范预期落差**
   部分员工在预知有演练的心理状态下，面对异常邮件失去应有的警惕，认为只是模拟演练，不会产生实际损失。

2. **警报疲劳与通报拥堵**
   当演练邮件与真实攻击同时涌入，it 运维（Helpdesk）与安全部门（SOC）的资源会迅速被海量反馈的钓鱼邮件信息占用，真真假假的信息可能直接影响到应急预案的响应，导致实际响应滞后。

3. **“计中计”效应**
   当安全团队拦截到真实攻击并发布给全公司紧急通知（如：【请注意！目前有真实钓鱼攻击，主题为 XXX】）时，员工容易将该通知信误认为是演练环节而置之不理，导致“人防”在最关键的时刻失效。

本季我们拦截并分析了数个具有代表性的高级威胁样本，其共通点在于深度结合社交工程与合法云端服务滥用：

1. 假恐吓真入侵：从纯社交工程到搭载恶意内容的转变

过去的恐吓邮件（Sextortion/Extortion）多半依赖暗网泄露的账密库，单纯以话术胁迫受害者付款，邮件中通常不含恶意附件或链接。然而本季出现新型变种：黑客在恐吓邮件中附带恶意软件，并以“敏感数据被盗的证据”为诱饵，诱骗受害者点击打开。

此手法结合了过去常见于网页攻击的“技术支持诈骗（Tech Support Scam）”的逻辑：利用恐惧情绪扰乱受害者的理性判断力，让真正的入侵发生在误信邮件内容之后。一旦点开附件，设备将被立即植入后门，使攻击从单纯的言语诈骗升级为实质的网络攻击，进而取得计算机的远程控制权限。

我强烈建议您查看此邮件内容 ☆

发件人：[redacted]@scn.com.cn>
时　间：2026年5月16日（星期六）下[redacted]
收件人：[redacted]

您好！
很抱歉，但我必须先说坏消息。

几个月前，我获得了您关联了操作系统的账号的访问权限，因此，我也获得了您用于浏览互联网的所有设备的访问权限。
然后，我就轻松地在您所有的设备上安装了能够追踪您每次按键和鼠标移动的特殊软件。之后，访问您的个人电子邮件（[redacted]）就不再是问题了。

我不是天才，也不是出色的黑客。造成这一情况的罪魁祸首是您对互联网安全的不屑一顾。
您似乎完全不了解什么是无痕模式、VPN、TOR，而且您还会毫不犹疑地点击电子邮件中的可疑链接。
我这封邮件的重点来了——我不仅获得了访问您浏览器历史记录和文件的权限，而且您的网络摄像头也在我的控制之下。

我不仅录制了您一边观看极具争议的内容，一边自慰的视频，而且还获得了您所有的网络聊天记录。为了避免您认为这些视频是假的，我还特意从您的好几个设备中复制了一些镜头。
您所珍视的一切——您的男友、同事，以及家人对您的看法——现在都受到了威胁。
您花了很长时间才建立起一个体面和负责任的人设。不管是你还是我，都不想通过点一下鼠标就把这一切都毁掉。
只需点击一下，您所认识的、喜爱的和尊重的所有人都会收到一部关于您的可疑视频，以及您浏览器中那"非凡"的浏览记录。

我希望您已经开始意识到，我可以一瞬间就把您的生活变成羞耻和尴尬的刑场。但是，我是一个理性的人，我并不希望将痛苦强加到任何人身上，所以我们可以来谈谈条件。

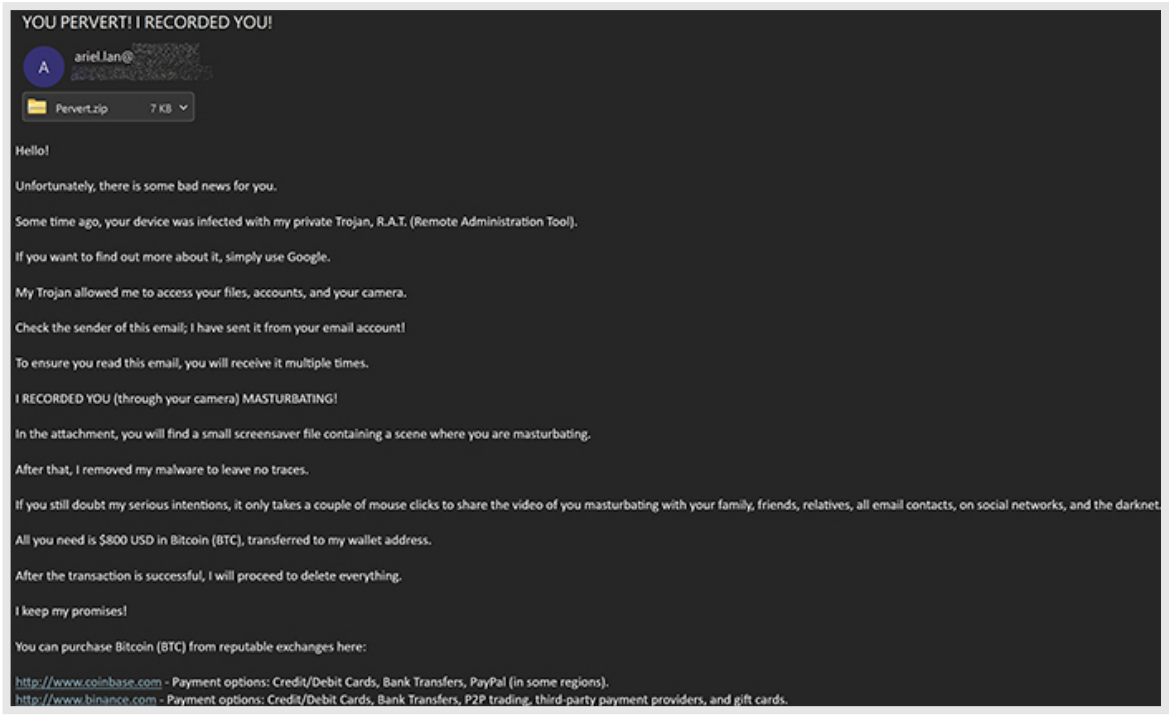
您需要将相当于1300美元的比特币转入此比特币钱包中：1Bv[redacted]zCnCZ3H

和您花了数年甚至数十年才建立起来的人设相比，这一点点钱根本不算什么。
收到付款后，我会马上将所有内容永久删除。由于我能够监控您在电脑和移动设备上的所有活动，因此我会知道您何时转账，以及何时阅读这封邮件。

从您打开此电子邮件的那一刻起，您有48小时的时间完成付款。

我是一个信守承诺的人，您可以相信我，不然我早就把这些内容公开了。让我先给您一些建议：
- 不要回复这封电子邮件。此电子邮件的发送地址是随机生成的。
- 请勿报警或联系其它执法机构。一旦我注意到您在尝试联系警方，我将会立即公开这些视频。另外，加密货币钱包都是匿名的，因此无法被追踪。
- 不要尝试重新安装系统，或重置您的设备。正如我说过的，一旦被我发现，我将立即公开这些视频。

传统恐吓邮件



YOU PERVERT! I RECORDED YOU!

A ariel.lan@[redacted]

Pervert.zip 7 KB

Hello!

Unfortunately, there is some bad news for you.

Some time ago, your device was infected with my private Trojan, R.A.T. (Remote Administration Tool).

If you want to find out more about it, simply use Google.

My Trojan allowed me to access your files, accounts, and your camera.

Check the sender of this email; I have sent it from your email account!

To ensure you read this email, you will receive it multiple times.

I RECORDED YOU (through your camera) MASTURBATING!

In the attachment, you will find a small screensaver file containing a scene where you are masturbating.

After that, I removed my malware to leave no traces.

If you still doubt my serious intentions, it only takes a couple of mouse clicks to share the video of you masturbating with your family, friends, relatives, all email contacts, on social networks, and the darknet.

All you need is $800 USD in Bitcoin (BTC), transferred to my wallet address.

After the transaction is successful, I will proceed to delete everything.

I keep my promises!

You can purchase Bitcoin (BTC) from reputable exchanges here:

http://www.coinbase.com - Payment options: Credit/Debit Cards, Bank Transfers, PayPal (in some regions).
http://www.binance.com - Payment options: Credit/Debit Cards, Bank Transfers, P2P trading, third-party payment providers, and gift cards.

含恶意附件的恐吓邮件，试图同时骗取财物及电脑控制权限

2. 假加薪/中奖通知：仿真欺骗与 AWS 基础设施滥用

在第二季度，我们检测到许多关于“天降横财”的钓鱼邮件。这些钓鱼邮件内藏的钓鱼链接多半都会滥用公共服务或是使用短链接来避免第一时间被检测拦截。

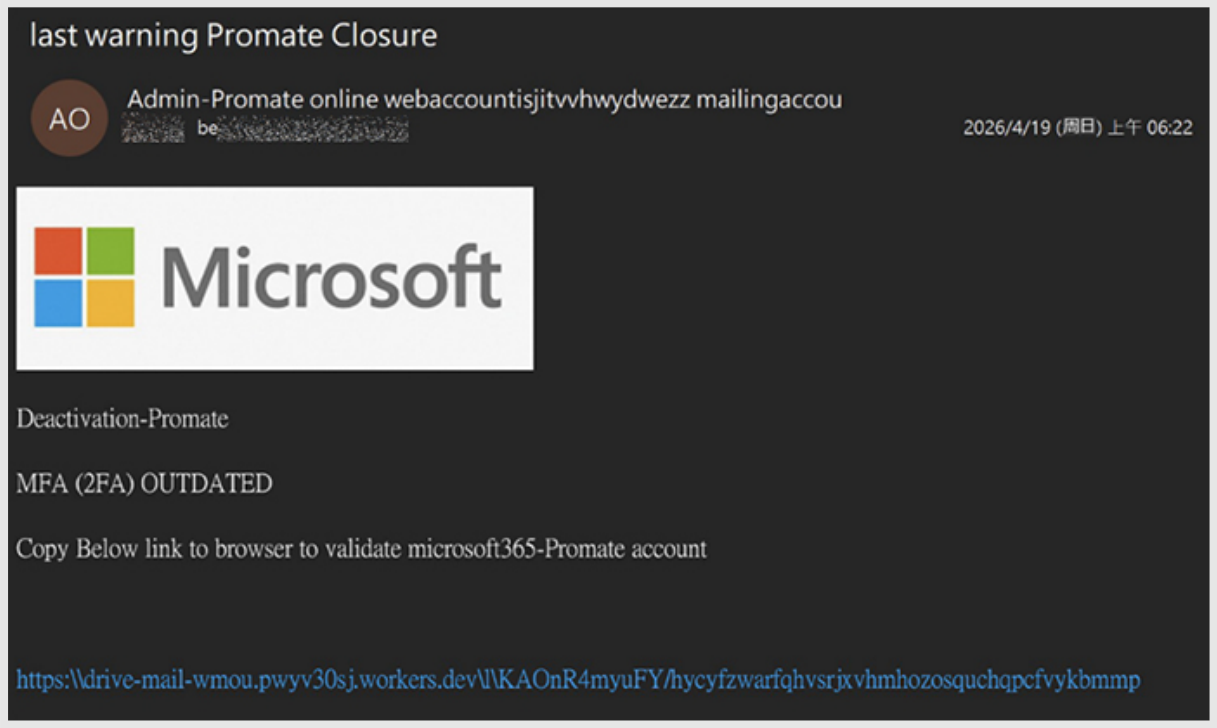
假加薪通知

从以上收到的涨薪邮件来看，攻击者滥用 Amazon Web Services (AWS) 合法基础设施来发送伪造的钓鱼信息。钓鱼页面主要的 JavaScript 攻击程序代码，以高度混淆（Obfuscation）的方式破坏可读性，并将变量名称、API 网址与字符串替换成数组索引，企图规避防毒软件或安全人员的静态分析。我们发现程序代码中直接写死了 Telegram Bot 的密钥。

当用户输入账号密码并点击发送后，程序代码会组合包含密码的字符串，并通过 AJAX 将数据传送到黑客指定的 Telegram 聊天室。这个攻击主要想窃取的是合法的微软登录凭证，而它不仅仅偷取密码，还会收集受害人的环境信息。代码中包含请求 getVisitorIP() 函式，利用第三方服务 https://ipinfo.io/json 来抓取用户的 IP 地址、所在城市、国家与电信运营商信息。同时也会收集浏览器版本与语言配置信息。

3. 滥用 Cloudflare workers.dev：绕过多因素认证（MFA）的设备代码钓鱼（Device Code Phishing）

本季最精密的攻击手法之一，是滥用 Cloudflare Serverless 服务（workers.dev）的进阶钓鱼。



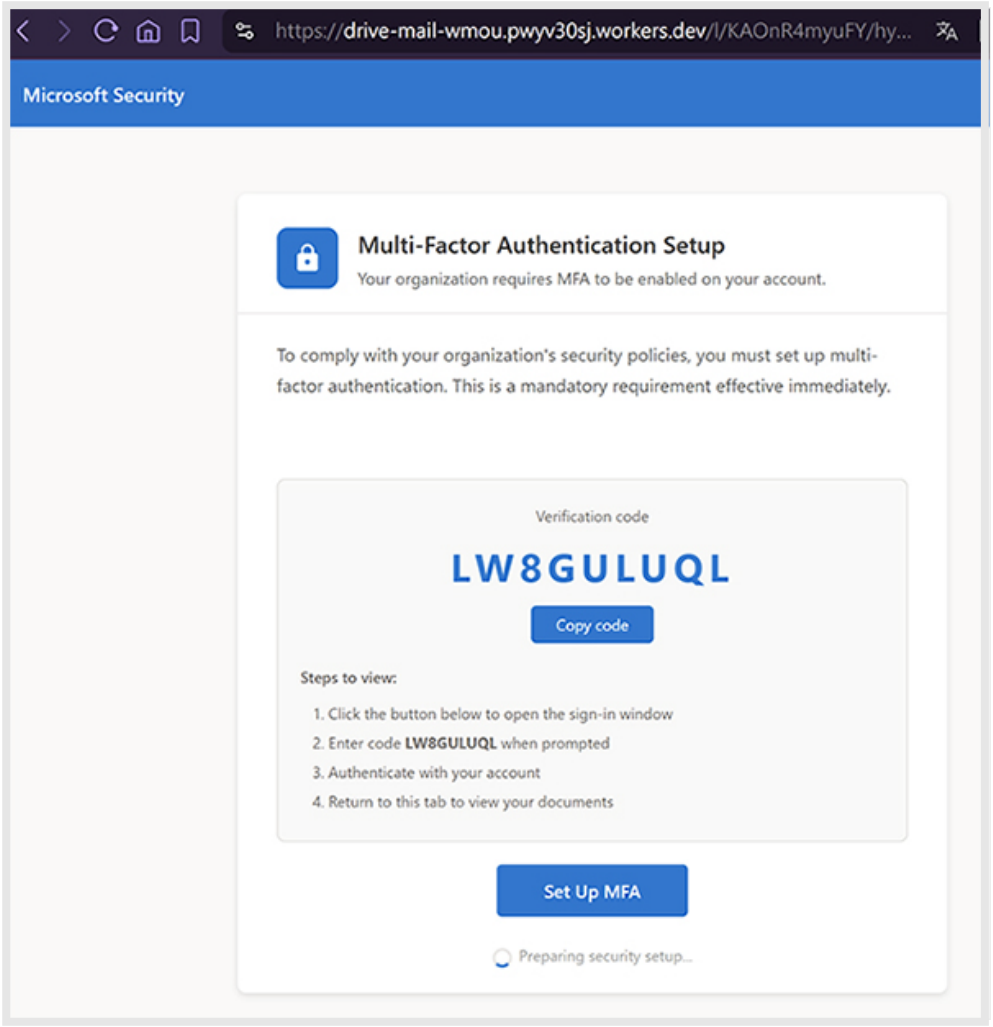
滥用 Cloudflare Serverless 服务（workers.dev）的进阶钓鱼邮件

手法分析如下

- **规避网址扫描**
  邮件刻意将链接改写为https:\\，诱导收件人手动复制粘贴。此举不仅避开了安全设备对恶意超链接（tag）的自动解析，一旦收件人按照黑客的指引粘贴至浏览器地址栏，浏览器页面会直接跳转至真实的钓鱼网站，而如 Cloudflare 这样的合法域名更能轻易绕过安全网关（SWG）与浏览器内置的恶意网址检测。

- **沙箱规避与环境隔离**
  恶意网页通过独立作用域封装 JavaScript 代码，防止与原始页面变量产生冲突；同时代码刻意延迟 2 秒执行，一方面规避部分动态沙箱检测机制，另一方面等待页面文档对象模型（DOM）加载完毕。

- **剪贴板挟持与多因素（MFA）绕过**
  当受害人点击诱饵按钮（data-href），恶意代码会强制篡改受害人剪贴板内容，随后跳转至真正的微软登录页面。若受害人按页面提示粘贴设备代码并完成多因素认证，凭借有效的身份凭证（Cookie / 单点登录凭证），攻击者远端设备可直接获取该账号的完整 OAuth 访问令牌，实现账号全权限接管。



滥用 Cloudflare Serverless 服务（workers.dev）的进阶钓鱼邮件

- **状态监控**

  该网页会在后台携带专属会话标识（SID，Session ID），持续向恶意命令控制服务器（域名：api.duemineral.uk）轮询攻击执行状态，返回状态包含捕获成功、会话失效、请求拒绝三类，整套攻击流程自动化程度极高。

结论与建议

攻击者正广泛利用开源网络情报（OSINT），从 LinkedIn 等平台自动抓取目标的姓名、岗位与组织架构信息。这使得高针对性的鱼叉式钓鱼已具备自动化与规模化投放的能力，社交工程将比以往更难分辨，企业应限制不必要的人事信息公开；为了防止假冒企业内部邮件，在邮件网关（Gateway）端针对外来邮件的主题或邮件正文强制插入“内部”或“外部”标签，也是一种直观能有效降低误点率的做法。

企业针对邮件安全的防护措施，多半已采用SPF、DKIM 与 DMARC等识别邮件来源是否遭到假冒的防护机制，但这并不能高枕无忧，当供应链或外部合作伙伴的合法网域遭黑客攻陷（BEC 攻击）时，带有合法签章的钓鱼邮件仍会畅通无阻。导入基于行为分析（UEBA）或升级智能体来进一步强化防护能力

最后，建议采用正向鼓励的方式，建立非惩罚性政策，鼓励员工在察觉可疑上下文（Context）时，主动反馈给相关安全部门或管理员，以达到“人防+技防”的安全目的。

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。