2026
第二季電子郵件安全觀察



ASRC

Spam Mail
Virus Mail
Malicious Mail

Jul 2026 released.

2026年第二季，電子郵件安全環境面臨顯著的威脅典範轉移。攻擊者正加速從依賴傳統的已知病毒特徵碼，轉向以規避防毒軟體靜態偵測為核心的進階威脅形式（對應 MITRE ATT&CK：Defense Evasion）。數據顯示，本季帶有惡意連結的郵件量較上一季暴增約 8 倍，並於 5 月份達到攻擊高峰。

值得警惕的是，5月份適逢多數企業執行內部社交工程演練的週期。駭客極度擅長利用此時間點發動真實攻擊，從而衍生出嚴重的管理與通報風險：

1. **警覺心偏差**
   員工在預期有「演練」的心理狀態下，可能對異常信件失去應有的警戒。
2. **警報疲勞與通報癱瘓**
   當演練信件與真實攻擊同時湧入，IT 客服（Helpdesk）與資安通報中心（SOC）的資源會瞬間被海量回報耗盡，導致應變遲緩。
3. **「計中計」效應**
   當資安團隊攔截到真實攻擊並發布全公司緊急警告（如：「請注意！目前有真實釣魚攻擊，主旨為 XXX」）時，員工容易將該警告信誤認為是演練的另一環節而置之不理，導致防護網在最關鍵的時刻失效。

本季我們攔截並分析了數個具代表性的進階威脅樣本，其共通點在於深度結合心理操縱與合法雲端服務濫用：

1. 假恐嚇真入侵：從純社交工程到實質惡意載荷的演進

過去的恐嚇郵件（Sextortion/Extortion）多半依賴暗網外洩的帳密庫，單純以話術恐嚇受害者付款，信件中通常不含惡意附件或連結。然而本季出現新型態變種：駭客在恐嚇信中附帶惡意軟體，並以「私密資料被竊取的證據」為誘餌，誘騙受害者點擊開啟。此手法結合了過去常見於網頁攻擊的「技術支援詐騙（Tech Support Scam）」的邏輯：利用恐懼感剝奪受害者的冷靜判斷力，讓真正的入侵發生在誤信攻擊者之後。一旦點開附件，設備即遭植入後門，使攻擊者從單純的詐欺犯升級為實質的入侵者，進而取得電腦的遠端控制權限。


テーマ: 商業オファー。

こんにちは、お世話になっております。

遺憾ながら、残念なお知らせがあります。
数ヶ月前から、貴方がインターネットをブラウズする際に利用しているデバイスにアクセスしており、それ以降、貴方のインターネット行動を監視しております。

アダルトサイトへの定期的な訪問に関して、責任があるのは貴方の方だと私は確信しております。
と言うのも、単純に申し上げますと、訪問されたサイトが貴方のデータを私に送信していたのです。

ウイルス対策ソフトでは検出不可能にする為、1日に数回署名を更新するトロイの木馬をドライバーベースでアップロードしました。それにより、私は貴方のカメラやマイクにもアクセスができます。
また、写真、ソーシャルメディア、チャット、連絡先を含む貴方のデータのバックアップも用意済みです。

つい最近になって、動画を1つのスクリーンで再生しながら、別のスクリーンでは貴方が射精する瞬間をとらえた動画を並べたビデオを作成するという素晴らしいアイディアを思いつきました。楽しいビデオが出来上がりましたよ！

純粹恐嚇郵件



新型態含有惡意附件的恐嚇郵件，試圖以社交工程的方式，同時騙取錢財及電腦控制的權限

2. 假加薪/中獎通知：高度混淆與 AWS 基礎設施濫用

在第二季，我們偵測到許多關於可獲得意外金錢的釣魚郵件。這些釣魚郵件內藏的釣魚連結多半都會濫用公開服務或是使用縮址來避免第一時間被偵測而失去了初始觸發攻擊的機會。



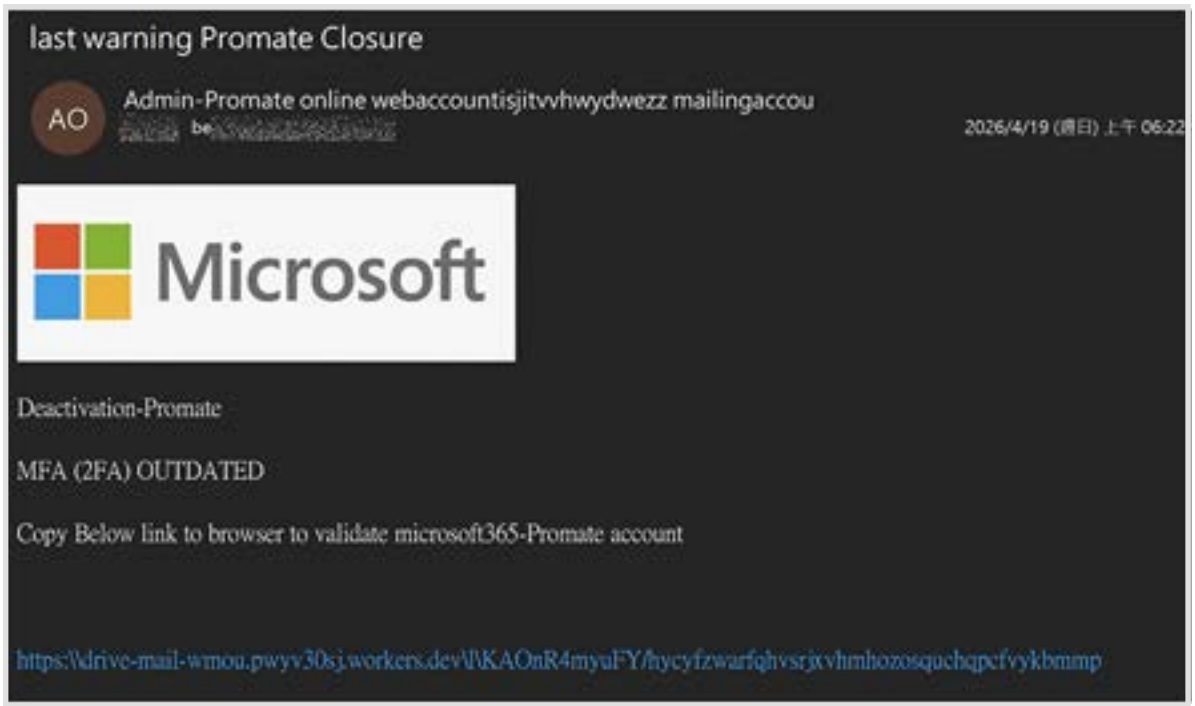
假加薪通知

以本次收到的加薪通知這個例子來看，攻擊者濫用 Amazon Web Services (AWS) 合法基礎設施來發送偽造的釣魚訊息。釣魚頁面主要的 JavaScript 攻擊程式碼，以高度混淆（Obfuscation）的方式破壞可讀性，並將變數名稱、API 網址與字串替換成陣列索引，企圖規避防毒軟體或資安人員的靜態分析。我們發現程式碼中直接寫死了 Telegram Bot 的金鑰。當使用者輸入帳號密碼並點擊送出後，程式碼會組合包含密碼的字串，並透過 AJAX 將資料傳送到駭客指定的 Telegram 聊天室。

這個攻擊主要想竊取的是合法的微軟登入憑證，而它不僅僅偷取密碼，還會收集受害者的環境資訊。程式碼中呼叫了 getVisitorIP() 函式，利用第三方服務 https://ipinfo.io/json 來抓取使用者的 IP 位址、所在城市、國家與電信商資訊。同時也會收集瀏覽器版本與語系。

3. 濫用 Cloudflare workers.dev：繞過 MFA 的設備代碼釣魚 (Device Code Phishing)

本季最精密的攻擊手法之一，是濫用 Cloudflare Serverless 服務（workers.dev）的進階釣魚。



濫用 Cloudflare Serverless 服務（workers.dev）的進階釣魚郵件

手法分析如下

1. 規避網址掃描

信件刻意將連結改寫為 https:\\，要求受害者手動複製貼上。此舉不僅避開了安全設備對惡意超連結（<a> tag）的自動解析，若收信者遵循攻擊者的指示貼至瀏覽器中，瀏覽器會將收信者導到真正的釣魚網站，而合法 Cloudflare 網域更能輕易繞過安全上網（SWG）與瀏覽器的惡意網址偵測。

2. 沙箱規避與環境隔離

惡意網頁以獨立 Scope 封裝 JavaScript 避免原網頁變數衝突，並刻意延遲 2 秒執行以規避部分動態沙箱（Sandbox）分析及等待 DOM 載入完成。

3. 剪貼簿挾持與 MFA 繞過

當受害者點擊誘餌按鈕（data-href），惡意代碼會強行寫入受害者剪貼簿，隨後導向真實的微軟登入頁面。受害者依提示貼上「設備代碼（Device Code）」並完成 MFA 驗證後，由於身分識別（Cookies/SSO）有效，駭客的遠端設備將直接獲得該帳號的 OAuth Token 完全存取權限。

4. 狀態監控

網頁在背景會攜帶特定 SID（Session ID），持續向惡意 C2 伺服器（api.duemineral.uk）輪詢攻擊狀態（captured、expired、declined），展現了高度自動化的攻擊流程。

結語與建議

攻擊者正廣泛利用開源網路情報（OSINT），從 LinkedIn 等平台自動抓取目標的姓名、職稱與組織架構。這使得高針對性的「魚叉式釣魚」已具備自動化與規模化投放的能力，心理操縱將比以往更難以肉眼辨識，企業應限制不必要的人事資訊公開；為了防止偽冒企業內部通信，在郵件閘道（Gateway）端針對外部來信的主旨或內文強制插入 [EXTERNAL] 或「外部來信」標籤，也是一種直觀能有效降低誤點率的做法。

企業針對郵件安全的防護措施，多半已導入 SPF、DKIM 與 DMARC 等識別郵件來源是否遭到偽冒的防護機制，但這並非萬靈丹，當供應鏈或外部合作夥伴的合法網域遭駭客攻陷（BEC 攻擊）時，帶有合法簽章的釣魚信仍會暢通無阻。導入基於行為分析（UEBA）或機器學習的進階防護更能強化防護能力。

最後，傳統以「釣魚信點擊率」作為 KPI 或懲罰依據的做法，可能會導致員工因恐懼而隱匿資安事件。但若採用「行為誘因（Incentives）」，建立非懲罰性政策，鼓勵員工在察覺可疑上下文（Context）時，主動通報至 phishing@ 或 abuse@ 等專屬信箱，則可將每位員工轉化為資安防禦網中，最敏銳的「人體感測器」。

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

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