2025
第二季電子郵件安全觀察

ASRC

Spam Mail
Virus Mail
Malicious Mail

July 2025 released.

郵件系統重大安全事件陸續曝光

多起郵件系統相關的重大安全事件在這一季被揭露。4 月份，日本知名的 Web 郵件系統 Active! Mail 爆出高風險漏洞 CVE-2025-42599。該漏洞屬於堆疊緩衝區溢位問題，因系統未正確限制寫入長度，導致攻擊者可覆寫堆疊記憶體結構，進一步操控程式流程並觸發遠端任意程式碼執行（RCE）。

緊接著在 6 月份，郵件伺服器 Roundcube 也被揭露存在幾近滿分的重大漏洞 CVE-2025-49113。僅僅三天內，暗網即出現販售該漏洞利用方法的訊息，顯示其風險極高。

同月，還爆出 Microsoft Office Outlook 存在「目錄遍歷」（path traversal）漏洞 CVE-2025-47176，攻擊者可藉由「.../...//」序列繞過路徑限制。此漏洞一般使用者權限即可觸發，無需管理員或更高權限，擴大了潛在攻擊面。

來自合法來源的釣魚郵件，規避傳統安全檢測機制

除了上述漏洞外，3 至 5 月間亦觀察到大量濫用合法信任來源的釣魚郵件活動。許多釣魚郵件運用政府、機關組織或學校網域，透過 outlook.com 或其他被濫用的郵件伺服器發送，信件中夾帶 forms.clickup.com 的釣魚連結。這些攻擊行為是利用 ClickUp 的線上表單功能，發送看似正常的請求，引誘收件者提交敏感資料或點擊惡意連結。

這類郵件可能來自遭入侵的合法帳號，因此具有較高的信任度，較不易被收件者識破。透過 forms.clickup.com 所嵌入的表單，攻擊者引導目標至偽造的登入頁面，竊取 Microsoft 365 或其他雲端服務的登入憑證。這種利用合法域名與平台進行繞過式偽裝的釣魚手法，能有效規避許多傳統的安全檢測機制，需特別留意。

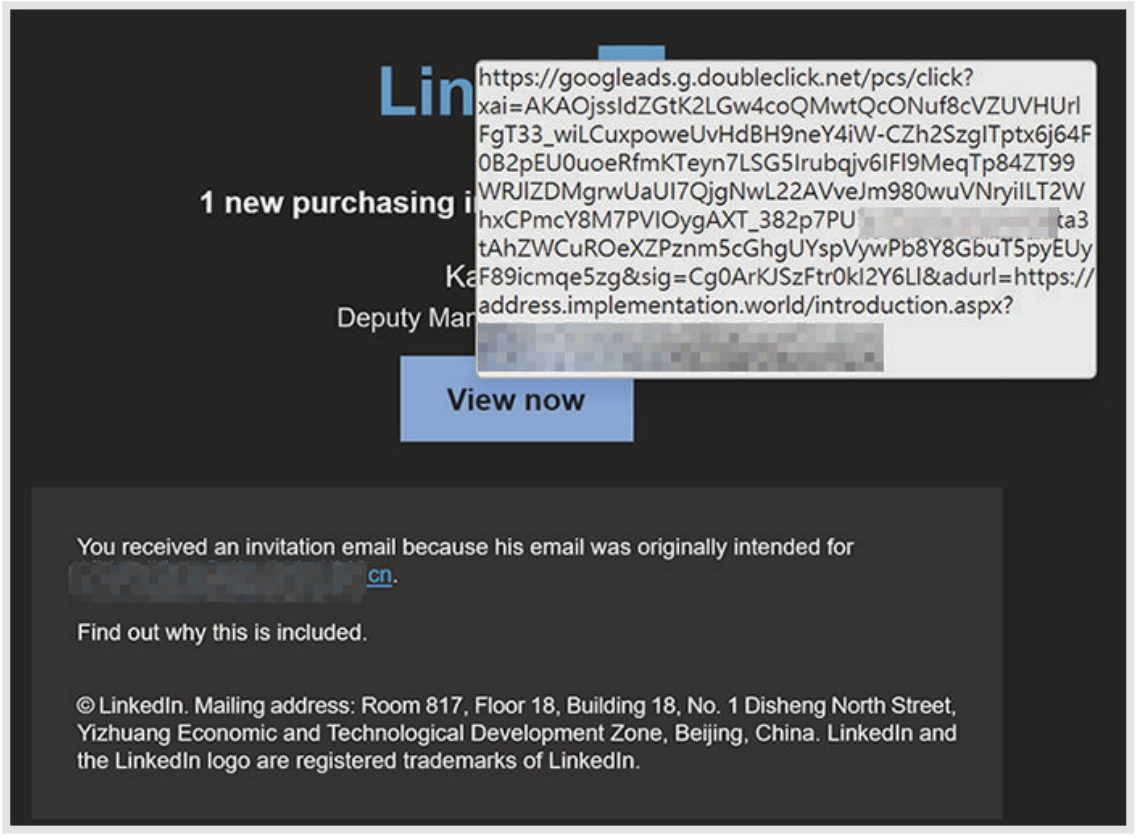
forms.clickup.com 表單，被用來收集 Microsoft 365 用戶的敏感資料

低調卻高風險，Open Redirect 成為釣魚網站庇護傘

此外，大量的開放重新導向（Open Redirect）機制正被攻擊者廣泛利用，成為釣魚網站的「庇護傘」。這類漏洞允許使用者透過合法網站的連結，自動跳轉至任意指定的外部網址，原本設計用途多為用戶體驗或流量分析所需，但一旦缺乏驗證機制，即成為攻擊者進行欺騙的工具。

令人憂心的是，這些被濫用的 Open Redirect 通常來自知名網站或大型平台，例如雲端服務供應商、政府或教育機構網站、企業入口頁等，其域名本身具有高度信任度。一旦攻擊者將釣魚網址包裝在這些可信網域的跳轉參數中，就容易騙過收件者、資安掃描機制，甚至繞過瀏覽器的安全警告或封鎖措施。

實務上，我們觀察到部分服務的開放重新導向漏洞已被濫用多年，但仍持續存在、未被修補，顯示出業界對此類低調卻高風險漏洞的關注仍有所不足。這不僅為釣魚攻擊提供穩定的跳板，也凸顯了在信任機制與網域聲譽管理上仍有加強空間。



來自知名的網域或服務，但被用於導向釣魚網站，有機會騙過收件者、資安檢測機制或瀏覽器的安全檢查

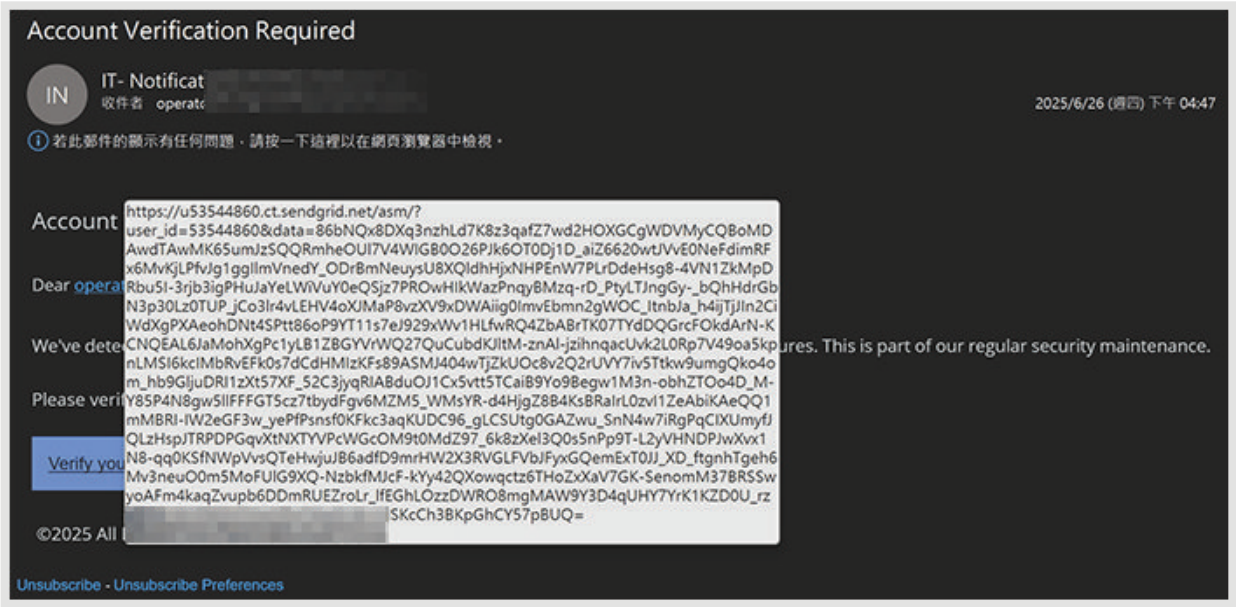
釣魚郵件濫用合法 Edm 發送平台，仍難以根除

除了釣魚網站經常藏身於各種「庇護傘」之下，釣魚郵件本身也經常濫用合法的 EDM（電子郵件行銷）發送平台作為傳遞工具。攻擊者利用這些廣泛使用、信譽良好的發信機制，讓釣魚郵件表面上看起來就像一般正常的促銷信或服務通知，更容易騙過使用者與安全系統的判斷。這種情況已經持續存在多年，至今仍難以根除。

主要原因在於 EDM 平台本身的設計目的就是為了協助企業大規模寄送郵件，因此在機制上往往偏重效率與送達率，較難即時察覺個別帳號是否被濫用或出現異常行為。即便部分平台導入內容掃描與異常行為偵測，也往往無法阻擋針對性強、包裝精緻的釣魚郵件。

在這樣的風險環境下，我們應重新思考對 EDM 發送機制的信任模型。過去多數使用者傾向「信任平台即信任郵件」的思維，特別是來自知名企業或第三方發信商的郵件，往往自動被視為安全。但實際上，這類信任機制已無法抵擋針對性濫用行為的滲透。

因此，更安全且可控的方式，應是將 EDM 的信任基礎由「企業單位」下放到「個人層級」：僅對使用者本人主動訂閱且確認過的寄件來源建立信任，並鼓勵使用者定期檢視、管理自己的訂閱名單。系統層面則應強化對 EDM 類郵件的驗證與過濾策略，降低僅因信任平台就放行所有郵件的風險。



常見的合法 EDM 發送機制遭到濫用

本季郵件攻擊趨勢可歸納為五個方向

1. 濫用合法資源：

攻擊者利用知名的雲端服務、郵件平台，甚至是遭入侵的政府或學術機構帳號。除了大幅降低成本，還能藉由「信任轉嫁」繞過傳統的安全偵測機制。相較之下，購買專用的惡意資源不僅價格昂貴，還可能在取得過程中暴露身份資訊，一旦遭列為惡意資源，便會立即遭封鎖或失效。

2. 信任鏈滲透：

透過合法的發信來源發送釣魚郵件，並將惡意網站寄生於可信的第三方平台下，不僅難以察覺也更具迷惑性與高成功率。這類攻擊先從平台服務本身或其漏洞著手，將合法資源轉為攻擊跳板，進一步對真正的目標發動攻擊，讓原本處於信任關係中的節點也成為潛在風險源。

3. 漏洞快速武器化：

漏洞一被發現，尤其是 CVSS 評分高及遠端任意執行代碼的漏洞，發現漏洞的攻擊者除了可能自行利用外，也會在很短的時間內將漏洞武器化並兜售，極短的時間就可獲得實際收益。

4. 低權限即可入侵：

攻擊者無需取得管理員權限，就能透過簡單手法滲透系統、橫向移動甚至植入惡意程式，有效提升攻擊效率並擴大影響範圍。

5. 多層混合式攻擊：

社交工程、假登入頁、跨平台整合等多種技術的組合應用，使得釣魚與入侵手法呈現多層混合、難以單一手段應對。

因此，面對日益複雜與隱蔽的攻擊樣態，僅靠單點式的防禦措施（如僅靠企業建置的防禦機制）已難以有效阻擋整體攻擊鏈。真正有效的防護策略，需仰賴跨單位、跨平台的協作，整合威脅情資、共享信任評級，才能及時發現並阻斷這類複合型攻擊的傳播路徑。

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