2025
第一季電子郵件安全觀察

ASRC

Spam Mail
Virus Mail
Malicious Mail

May 2025 released.

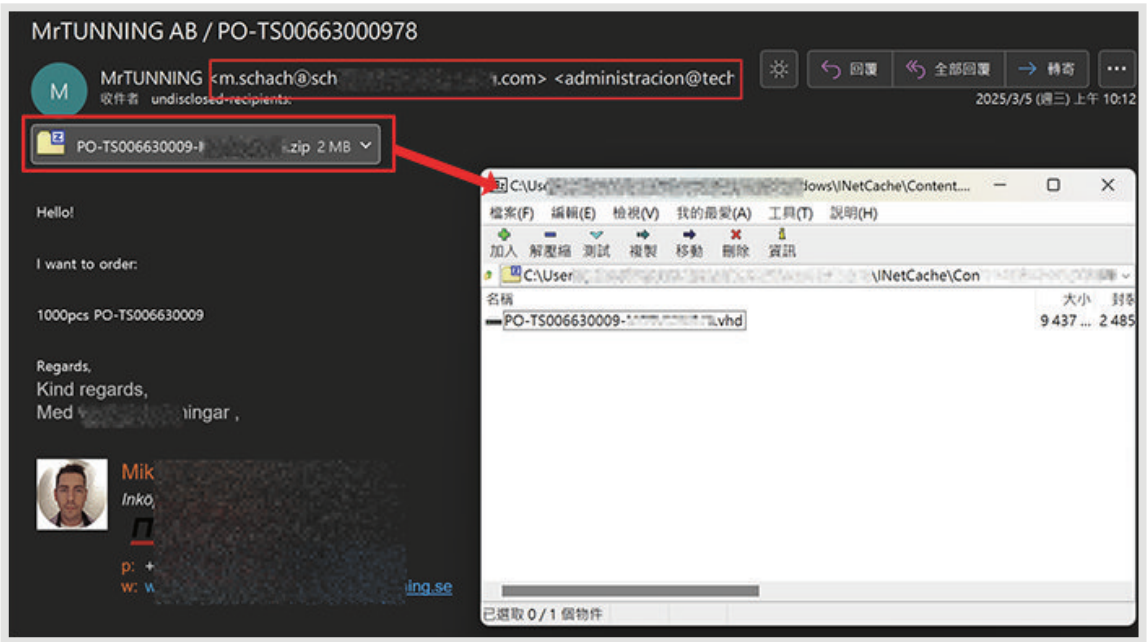
2025年，郵件安全趨勢強調更嚴格的身份驗證要求。Gmail 和 Yahoo 等主要郵件服務提供商除了持續推動 SPF、DKIM 和 DMARC 等認證協議的採用，也逐步將目標指向 DMARC 的 p=reject 的郵件政策，以防止域名被冒用。發送來源的驗證與檢測，也逐漸由 IP 信譽轉為域名信譽。一月底揭露的 7-Zip 軟體重大安全漏洞（CVE-2025-0411），已被俄羅斯網路犯罪者用於攻擊烏克蘭。透過電子郵件夾帶惡意附件，並利用該漏洞，即可繞過 Windows 系統的 MotW（Mark of the Web）安全機制，受害者可能受騙而在電腦上執行外來惡意程式，最終導致資料外洩或電腦遭控制。除須提防可疑郵件外，建議盡快將 7-Zip 更新至最新版本，以修補該漏洞。此外，CVE-2025-21298 也值得注意，這是一個影響 Microsoft Office 和 Windows 作業系統的嚴重漏洞，特別涉及 OLE（物件連結與嵌入）技術。攻擊者可以利用這個漏洞，透過精心設計的文件，在未經使用者同意的情況下執行任意程式碼；雖然目前公開資料未明確記載 CVE-2025-21298 透過電子郵件攻擊的實際案例，但根據漏洞特性與歷史攻擊模式，此漏洞極可能被用於以下攻擊場景：

- **惡意附件攻擊：**
  攻擊者偽造電子郵件並附加特製的 .rtf 檔案，誘使用戶開啟後觸發漏洞。
- **社交工程結合漏洞利用：**
  以稅務通知、帳單等名義發送釣魚郵件，提高用戶開啟惡意文件 (可能透過 Web 下載) 的意願。

以下是本季值得留意的郵件樣本：

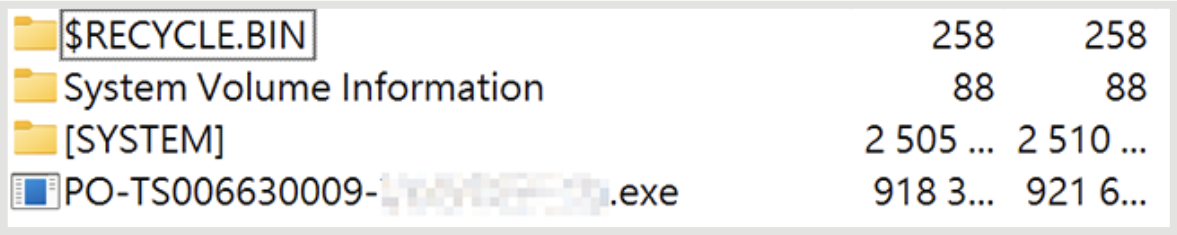
壓縮檔夾帶 .VHD 檔的攻擊

第一季，我們發現一些電子郵件攻擊，其中的附件檔以.zip 的方式包裝 .VHD 檔案。.VHD 檔案可被 Windows 作業系統視為虛擬硬碟，當收件者打開這些檔案時，系統會將其掛載為新的硬碟驅動器。在這個攻擊郵件中，寄件者的位置被填了兩次電子郵件地址，試圖讓收件者誤以為這是由第一個地址所發送的郵件，為了躲避對於寄件者位置的電子郵件檢查，攻擊者細心的將第一個地址中的 @ 改為視覺上相近的符號。



惡意郵件附件檔以 .zip 的方式，包裝了一個 .VHD 檔案

若將 .VHD 檔展開，會看到完整的虛擬硬碟結構，其中 .exe 檔即為惡意攻擊程式的本體，不會被 Windows 系統識別為 MotW（Mark of the Web）。而這個攻擊程式的圖示，刻意被換為 Excel 的圖示，藉以誘騙受害人執行。當惡意程式被執行時，便開始在系統植入後門。



.VHD 檔展開來看，會看到完整的虛擬硬碟的結構，其中 .exe 檔即為惡意攻擊程式的本體

若企業日常作業不會透過電子郵件直接傳送 .VHD 檔，建議可以直接在郵件安全掃描或過濾機制中，直接封鎖帶有此類檔案的電子郵件。同樣企業較少透過 郵件傳送但常被用來攻擊的 .ISO、.IMG 也可以考慮一併隔離。

社交工程手法誘騙

一直以來，透過社交工程手法誘騙受害者配合執行某些操作，是詐騙、釣魚慣用且成功率極高的手法。第一季，我們觀察到幾起以假亂真的惡意電子郵件，郵件本身不夾帶惡意檔案，而是以社交工程手法誘騙，要求受害者點擊並下載「加密」的惡意或後門程式。由於惡意程式經過加密，可以輕鬆躲過檔案下載的安全性稽核、瀏覽器及 Windows 針對 Web 下載檔案的 MotW 防護措施，這些惡意檔案也能躲過部分防毒軟體的檢查。同樣的社交工程手法，也可能搭配要求帳密登入確認(用以騙取帳密)；或是要求輸入信用卡相關資料做認證、支付運費、規費等動作，都需要特別留心防範！

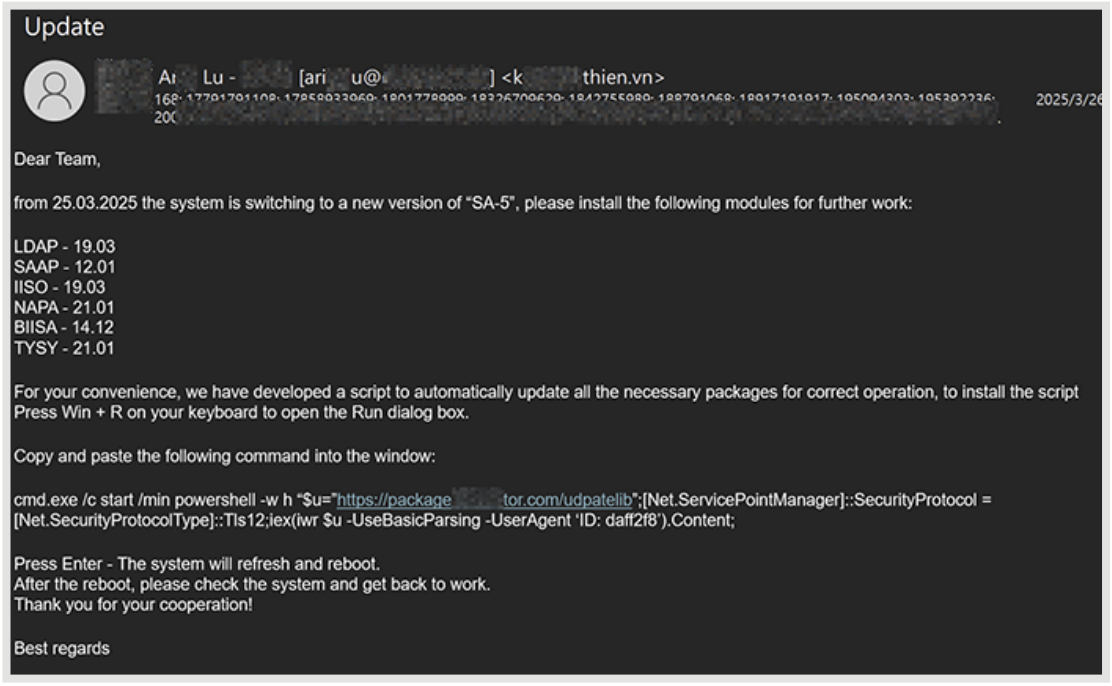
冒充法令修訂公告，仔細留心還是能發現是透過免費信箱寄達，且連結網址非政府域名

要求下載加密的壓縮後門程式並執行

以工資補發單為名，誘騙受害者下載加密惡意程式並點擊

技術支援攻擊

我們觀察到特殊的社交工程攻擊正在流竄。收件者收到一份系統更新或升級的操作通知，其中詳載系統更新升級的方法及操作步驟。事實上，這並非來自技術部門的升級通知，而是攻擊者以社交工程手段，誘騙收件者下載檔名為 netscanner.exe 的後門並執行的攻擊郵件，主要目的用於竊資。值得留意的是，netscanner.exe 在截稿時，無法被一般主流的防毒軟體識別出風險。



攻擊者以社交工程手段，誘騙收件者下載並執行檔名為 netscanner.exe 的後門程式

這類攻擊早期常見於網頁瀏覽。在瀏覽網頁的過程中，突然彈出系統故障的警示，接著要求受害人與「技術支援專員」通話並接受指導；或是彈出「Click Fix」的下載修復連結與詳細的操作步驟，以社交工程的手法，誘導使用者一步步在電腦中埋入後門。現在這類手法也開始透過電子郵件散播！

結論

資安攻擊時時變化，資安政策以及資安意識訓練也應與時俱進。資安部署原則中的「最小權限原則」概念，也可以應用在郵件寄送附件類型或對象的審核：合理使用的附件檔才允許寄送，對於特殊的附件檔案，應預設為暫時封鎖並搭配人工審核，再根據實際情況適時調整防禦策略；對於收件者也應仔細考量，可發送給內部群組信箱的對象應合理限縮，以減少暴露在風險中的機會。

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

© 2025 Asia Spam-message Research Center. All Rights Reserved.