2023
電子郵件安全趨勢回顧

ASRC

Spam Mail
Virus Mail
Malicious Mail

Feb 2024 released.

回顧 2023 年 2 月 6 日，土耳其遭受強烈地震襲擊，而地震發生不久後，我們便觀測到詐騙郵件透過冒名全球捐贈網（globalgiving.org）的募款信件伺機傳播。2024 一開年，日本石川縣能登地區也遭遇芮氏規模 7.6 的強烈地震，災害規模之大促使日本氣象廳將其命名為「令和 6 年能登半島地震」。這樣的災害是否會像過去一樣，導致各種以慈善為名的捐款詐騙郵件與網站流竄，還需要一段時間的觀察。

根據 ASRC 研究中心的觀察，2023 年相較於前一年，整體的電子郵件數量成長了 20%；可在第一時間被防毒軟體察覺的病毒郵件雖然減少了 16%，並不代表攻擊趨勢有所減緩；在帶有威脅的郵件中，含有惡意超連結的郵件增加了 35%，夾帶惡意檔案的郵件則大幅增加了 96%；以壓縮打包附件進行攻擊的格式中，.rar 為主流，其次是 .zip；419 詐騙郵件的數量相較前一年則增加了 116%。

在漏洞利用方面，2023 年 3 月份揭露的 Outlook 零時差漏洞 CVE-2023-23397，除了 2022 年底被用於攻擊烏克蘭國家移民局及一家經營軍艦與國防科技的土耳其公司外，在 2023年12月也被俄羅斯駭客 APT28 利用於存取 Exchange 伺服器上的電子郵件信箱帳號，攻擊目標為美國、歐洲、中東的政府機關、運輸業與非政府組織等。其他數量較多的漏洞利用還有：利用 Zip 檔內的唯讀屬性繞過 MotW 的 CVE-2022-41049（MotW，Mark of the Web，為Windows安全功能）；以及透過 Office 文件觸發 OLE Package Manager 的漏洞 CVE-2014-4114。

在釣魚郵件方面，我們觀察到以下的變化：

釣魚連結隱藏於 QR Code

將釣魚連結隱藏在 QR Code 的郵件，在 2023 年的第一季末開始大量出現。這種攻擊方式讓釣魚連結無法直觀的被安全設備偵測或人員辨識，需要靠手機或其他 QR Code 的解碼軟體才能解析出惡意連結。值得特別注意的是，習慣用手機掃描 QR Code 內容的受害者，曝險的設備由電腦轉向了手機，由於企業多數安全措施的保護對象是工作用電腦，因此個人的手機便成了新的風險突破口。

直至 2023 年底，在郵件內附上藏有釣魚連結的 QR Code 是常見的利用手段。而第四季開始出現**將釣魚用的 QR Code 內嵌於加密過的 Word 附件中**的案例，進一步增加了安全工事的辨識與解碼難度；但是從另一個角度來看，**這樣特殊的做法與一般正常郵件的寄送方式形成了明顯的區別，若能透過適當的資安宣導或教育訓練，便可有效避免員工落入社交工程的圈套而點擊釣魚郵件的風險**。

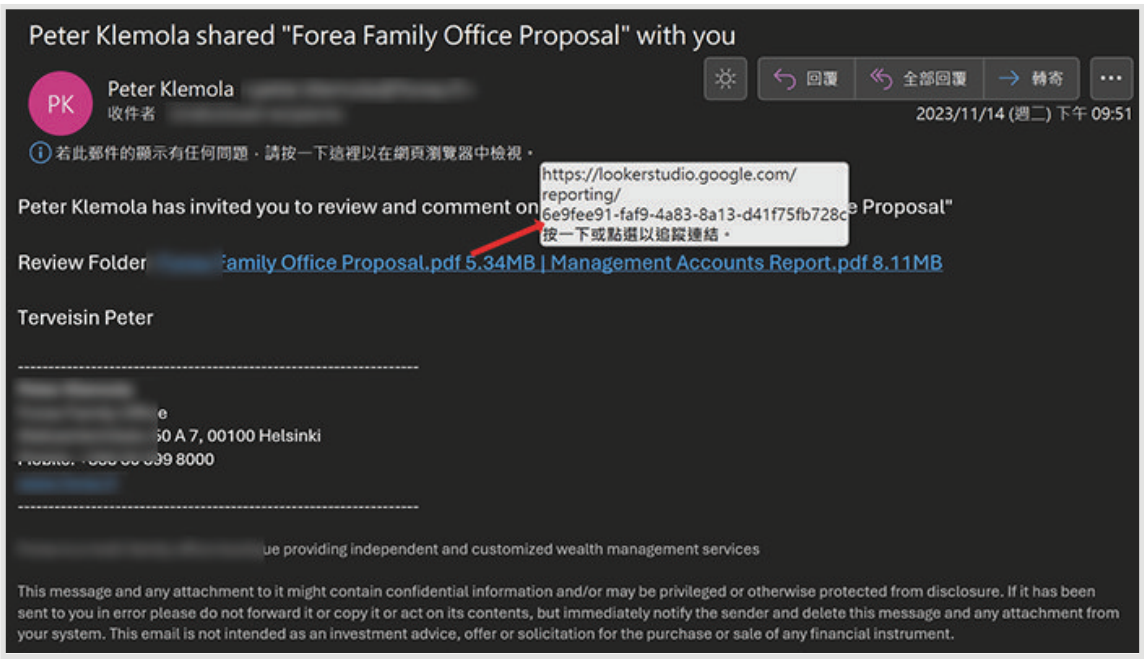
當然，管理者也可以在郵件過濾系統中設定某些條件進行預防攔截或觀察：比方，**密碼與加密檔案同時存在於郵件中，多半就是威脅或是想避開偵測的郵件**，這是否值得進一步審核？若郵件過濾機制具有 QR Code 的偵測或解碼功能，也可以對這些郵件進行審核與觀察，查看企業是否有正常使用 QR Code 的場景，排除這些場景後，其他的 QR Code 多半就是不懷好意的連結。

QR Code 編碼的釣魚連結圖片，內嵌於加密的 Word 檔案中

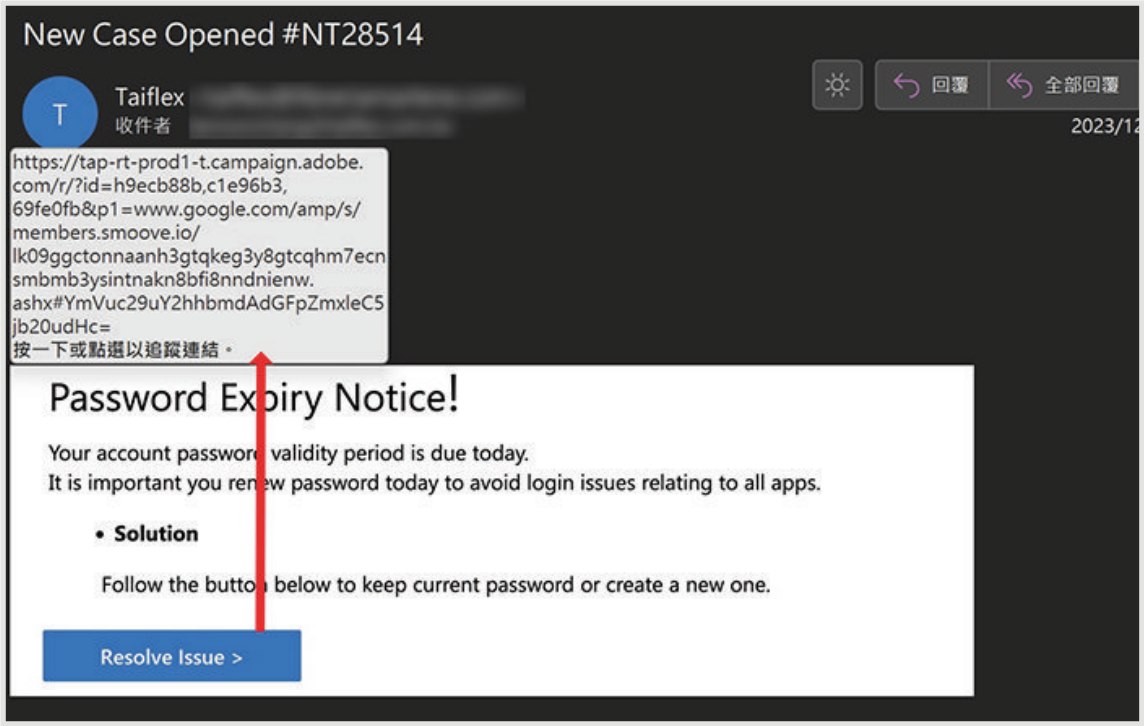
惡意連結的變化

釣魚郵件連結為了避免被資安設備發現，同時又要能對目標發動攻擊，有很多不同的作法，例如，轉址、濫用公開服務...等。然而，大多數轉址服務的網域名稱並不那麼值得信賴，因此，若能使用值得信賴的廠商所提供的服務，不僅能躲避偵測，還能使被攻擊的對象信以為真。

在 2023 年第四季，我們發現 Google 及 Adobe 的服務被用來導向釣魚網站的案例。



Google Looker Studio 服務被利用



Adobe 服務被利用

此外，也有攻擊使用 Unicode 字元替換域名中的部分字元。攻擊者能對郵件內惡意連結中的域名做一些細微的變動，例如：將小寫字母切換為大寫字母，或塞入不可見字元...等，藉此繞過資料庫的比對判斷，而這種域名帶有特殊字元的惡意網址對於瀏覽器與收信軟體來說，仍能將其解析為可被收件者點擊的網址。

星際檔案系統 (InterPlanetary File System，縮寫為IPFS) 的利用

三年前，由 ISP、域名管理公司、雲端服務商及其他基礎架構管理單位與資安公司通力合作，大約 1/3 的釣魚網站出現不到一天，便會遭到檢舉、關閉。而自 2022 年開始，越來越多的釣魚郵件開始搭配使用星際檔案系統 (InterPlanetary File System，縮寫為 IPFS) 的釣魚網站。IPFS 是一個對等的分散式檔案系統，捨棄了傳統的集中式架構，改用遍布全球的點對點 (P2P) 數據網絡，無需第三方或中央機構管理，因此，IPFS 網絡釣魚內容可以很容易地分發、更難以檢測、具有持久性，且釣魚網站只能由建立者自行刪除。

礙於星際檔案系統的發展之初有其合理的應用範圍，因此利用 IPFS 產生壽命更長的釣魚網站將會形成一種新的趨勢。

2024 年可能帶來的變化與防禦工事

2023 年 3 月微軟發布的 Microsoft Security Copilot 可顯著提高企業資安團隊的覆蓋範圍、速度和效率；但道高一尺，魔高一丈，生成式 AI 帶來的效益若被用於攻擊，則可預見的，也能提高攻擊者的效率。儘管目前尚未看到較具體的攻擊應用，但生成式AI確實能在短時間內產生較以往更令人信服的文字、流暢的翻譯和以假亂真的畫面。加上 2023 年許多的研究都指出，利用 AI 辨識 AI 生成內容的準確性過低。因此，社交工程攻擊將會是未來的一大隱憂，而跨語系的社交工程攻擊因為 AI 的關係將變得更加流暢！

因應攻擊的升級，防禦工事的部署或資安概念也必須跟著升級。面對來自電子郵件的威脅，「人」是最大的目標，運用防禦設備使人避免接觸威脅郵件是最基本的措施。更進一步，應該利用設備的紀錄、分析、調查等能力，找出企業較易遭受到攻擊的惡意郵件類型與人員，並透過動態調整，才能更及時的因應多變的攻擊手段。

在人員教育訓練方面，應著重在不屬於自己的郵件就應該抱持懷疑的核心概念，教育內部員工在發現可疑郵件時，不點擊、不回應、不轉傳、通報內部資安窗口，以利早期發現攻擊徵兆，提升整體資安防護，應對不斷演進的威脅。

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