2024
第二季電子郵件安全觀察

ASRC

Spam Mail
Virus Mail
Malicious Mail

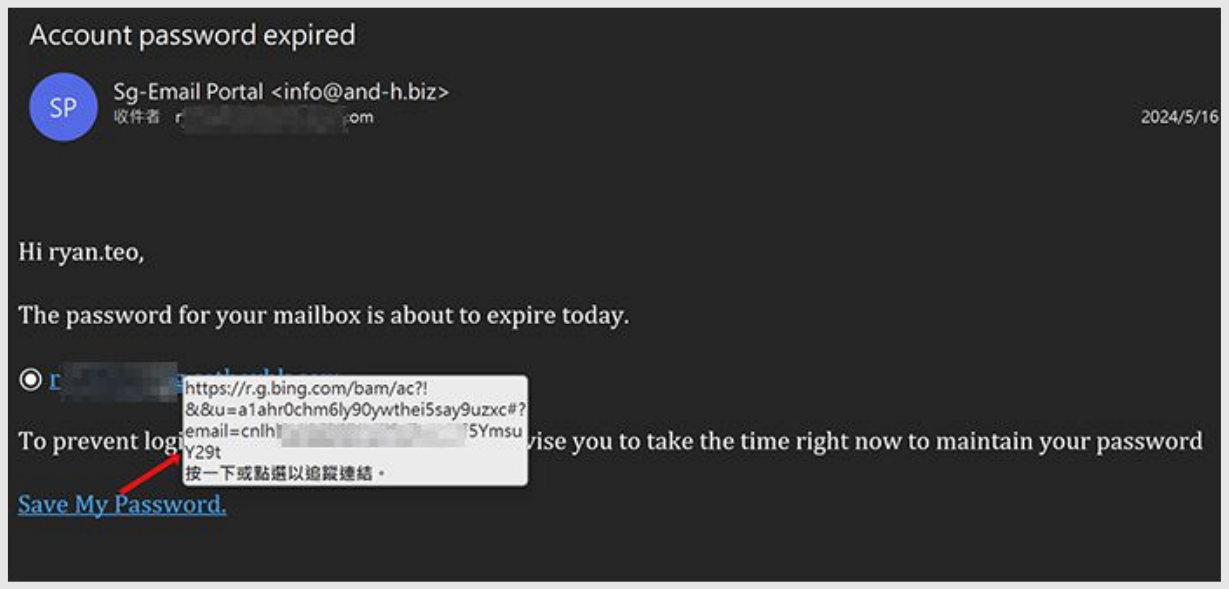
July 2024 released.

網路攻擊分工越來細緻，近期明顯區分為初始入侵與後續的橫向移動或進階攻擊兩大階段。初始入侵主要透過漏洞利用或外洩憑證為兩大入侵手段；其中，外洩憑證重要的獲取管道之一，就是透過釣魚郵件。而本季需要特別留意的便是釣魚郵件。時至年中，有許多單位集中在這個時間點進行社交工程演練，資安或資訊單位的負擔因而加重，便可能出現人為疏忽的破口，應特別留意！由上一季延伸的 QRcode 釣魚郵件攻擊未見趨緩，未來可能演變為常態性的攻擊。

以下為本季特殊的攻擊樣本介紹：

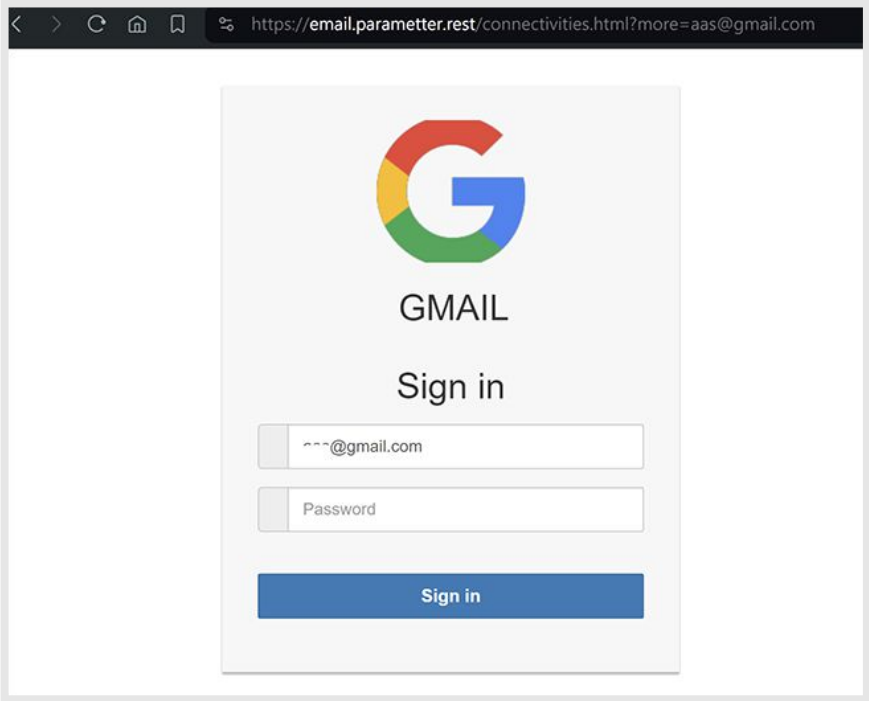
Bing 服務遭到釣魚郵件利用

合法服務一直是釣魚郵件覬覦的對象，畢竟釣魚郵件的組成，最關鍵、也是破綻所在，就是釣魚郵件中的超連結。本季，我們發現 Bing 的服務被利用於釣魚郵件的超連結轉址。



Bing 的服務被利用於釣魚郵件的超連結轉址

透過 Bing 的連結，會先將受害者導至惡意網址中繼，然後再轉至真正的惡意頁面。這個惡意頁面會直接顯示受害者的電子郵件信箱，並仿造為 Gmail 的登入頁面，主要是為了騙取郵件登入的帳號及密碼！比較有趣的是，輸入第一次密碼送出，頁面會更新一次，讓受害者以為沒有輸入成功；第二次在輸入時就會直接轉址至 Gmail 入口，這個手段可能是用來提高密碼獲取的正確性。



頁面直接顯示受害者的電子郵件信箱，並仿造為 Gmail 登入畫面

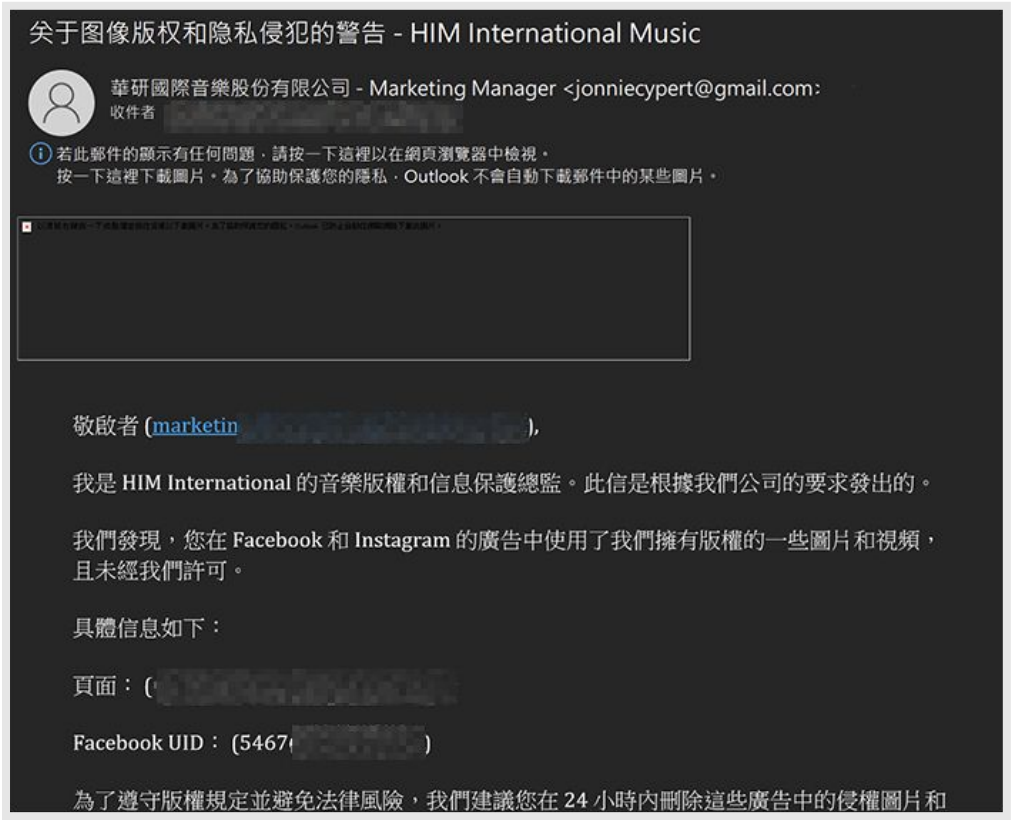
以假亂真的釣魚郵件

有些釣魚郵件，是拿真實通知郵件來改造，甚至還帶有提防詐騙的宣導連結，整封郵件的超連結幾乎都指向真正的網站；只有一個關鍵的超連結，會被導向真正的釣魚網站！這對於受害者或掃描機制而言，都有一定的欺騙效果。

以假亂真的釣魚郵件

假冒侵權警告的攻擊郵件

本季，我們觀察到冒名侵權警告的攻擊郵件。攻擊郵件製作十分精細，對於侵權的內容也舉證歷歷，看來煞有其事！但這封攻擊郵件來自Gmail，通常正式的商業往來或重大通知不會從免費信箱發送，若收到此類攻擊郵件只要冷靜判斷，便能從中察覺異常。像這樣涉及金錢、法律等重大事件的郵件，一定要從官方揭露的合法管道求證；絕對不能因為一時心急，順著郵件內容附帶的聯絡方式或超連結與對方進行接觸，或貿然下載相關文件。



釣魚郵件製作十分精細

這封郵件主要希望受害者能下載他們整理好的侵權證據文件檔案，但攻擊者並不希望自動化檢查機制介入檢查檔案的內容，因此，在正式下載檔案之前需要先驗證是否為人類，成功通過驗證後，才會開始下載壓縮檔案。

確定為人類後，就會自動下載壓縮檔案

在這份壓縮檔內，共有三個檔案，最主要的是可執行的 PE 檔，這個 PE 檔的圖示已被置換為 PDF 圖示，用以誘騙被害者打開 PDF 文件；.dll 檔則是 Remcos 後門；而另一個 .inf 檔在解壓縮之後會變得十分巨大，可能用於干擾掃描與檢查機制。Remcos 常見的部署方式為嵌入在偽裝成 PDF 的惡意 ZIP 檔案中，聲稱包含發票或訂單；而本身的後門能力包括了躲避防毒檢查、權限提升以及資料收集。

過往常見的部署方式為嵌入在偽裝成 PDF 的惡意 ZIP 檔案中，聲稱包含發票或訂單

冒充 LINE 的付款釣魚

目前台灣最常使用的通訊軟體為「LINE」，使用率高達 99%，且 LinePay 在台灣已有 1200 萬用戶，因此，LINE 成為釣魚郵件的假冒對象並不意外。在本季我們發現一封假冒 LINE 的釣魚郵件，聲稱付款有問題，要受害者點擊惡意連結更新帳戶資訊。

惡意連結表面是連往 LINE 的官方網站，實際連結卻是連往惡意中繼網址；這個中繼網址會先進行一次 CAPTCHA 人類驗證，確定不是沙箱或自動化爬蟲檢查機制後，才會將受害者帶往釣魚網站。

假冒 LINE 的釣魚郵件，聲稱付款有問題，要受害者點擊惡意連結更新帳戶資訊

這個釣魚網站仿造 LINE 的頁面，要求受害者填妥身分資料，但只要稍加留意瀏覽器上方顯示的網址，便能發現這是一個與 LINE 完全無關的網頁。

要求受害者填寫身分資料

這個釣魚郵件真正的目標是釣取信用卡資料，可能是為了後續盜刷或賣入黑市。若將資料輸入並送出，頁面會馬上轉到 LINE 真正的官方頁面，讓受害者不易發現破綻。

這個釣魚郵件真正的目標是釣取信用卡資料

結語

有調查指出，寄發試探性質的社交工程演練郵件，可能讓員工提心吊膽增加壓力，對於識別真正的釣魚或攻擊郵件未必有幫助；反而是樣本示例的教育性質訓練有助於資安意識與識別能力的提升！釣魚或詐騙郵件都是以社交工程為基礎的攻擊手段，因此，這類攻擊很容易利用受害者好奇、害怕、時間或其他壓力的心理操作，讓受害者疏忽。

面對詭譎多變的釣魚郵件，光從郵件上的識別，有時真的難辨真假！但釣魚或詐騙郵件的通則，都是希望受害者遵循郵件提供的「管道」確認或執行某一個動作，若遇到郵件要求這樣的動作，務必從官方網站，或自行查詢官方電話進行確認或聯繫，不要直接透過郵件提供的「管道」確認，將可避開許多釣魚風險！

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