武功極界——無影手 VS. 麥擱騙啦——有影沒

◆ 社團法人台灣 E 化資安分析管理協會、逢甲大學資訊工程系 — 李榮三主任／教授

由臺灣警政署與美國網路犯罪投訴中心（Internet Crime Complaint Center, IC3）統計的網路犯罪資訊，可發現近年來國內外的網路攻擊、詐騙等犯罪事件數量居高不下。

據臺灣警政署統計，自 2017 至 2021 年間，平均 1 年發生 1 萬 3 千例以上。雖近年來的犯罪統計稍有下降趨勢，但受害者仍成千論萬。況且，這些統計數量僅計算已通報的案件，未通報的案件更是不計其數。美國則更甚，IC3 的報告中指出每年平均有 55 萬例，且數量有顯著提升，2017 至 2021 年的通報案數量已暴增 2.8 倍。甚至網路犯罪受害者損失的金額平均每年高達 370 億美金，由此可見，網路犯罪所帶來的威脅不可估量。其中，最常見的手法即為「網路釣魚攻擊」。網路釣魚如同真實世界釣魚，釣客即為隱匿於網路背後的駭客，常見的公務通訊軟體、社群媒體等則是作為駭客的釣場，駭客透過散播魚餌誘使民眾點擊上鉤。

藝人周杰倫於 2022 年 4 月 1 日當天在 Instagram 上發文，表示自己無聊猿 NFT 被網路釣魚偷走，起初還以為是愚人節玩笑，「結果一去查看，真的沒了」。（圖片來源：周杰倫 IG，https://www.instagram.com/jaychou/；Ghost.R.C，https://flic.kr/p/qAWP1a）

參考 Medium 中 Tyler Chen 所提出的電子郵件範例與社群軟體上的詐騙實例，一旦民眾點擊其中所夾帶的鏈結、下載檔案或是開啟指定程式，便等同於上鉤，駭客成功竊取使用者個人資料、帳號密碼與信用卡號等。

個人案例與防範策略

接著，我們進行個人與企業的受害案例分析，並且說明防範策略。

一、周杰倫無聊猿 NFT 被偷損失上百萬

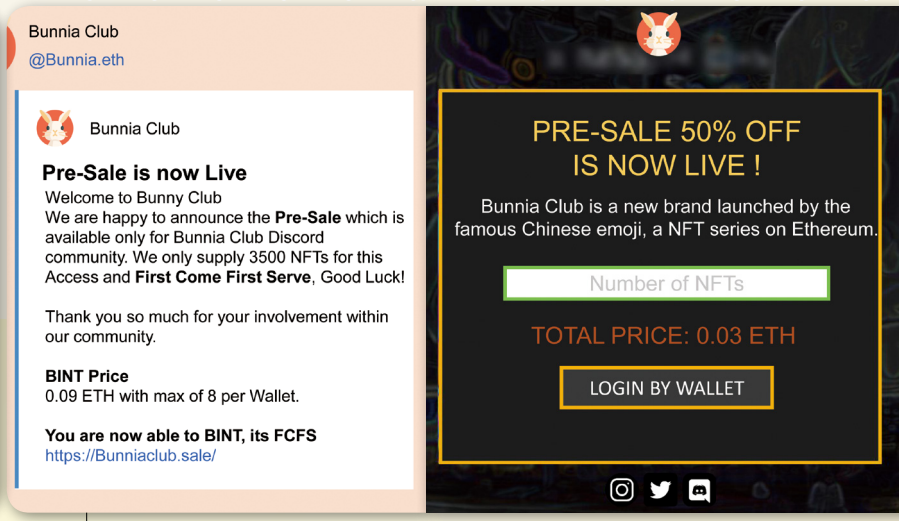
2022 年 4 月，明星周杰倫在社群網站公布其「無聊猿」非同質化代幣（Non-fungible Token, NTF）被釣魚網站偷走的消息。所謂「無聊猿」是由無聊猿遊艇俱樂部（Bored Ape Yacht Club, BAYC）推出的 1 萬隻各有獨特表情的猿猴 NFT 作品，當時每隻價格約在 100 枚以太幣（約 26 萬美金）。

這類事件的起因就是駭客在官方社群網站放上釣魚網址來誘騙被害人。使用者在社群媒體上看見 NFT 的預購訊息，以為可以用較便宜的方式來購買新的 NFT；誘使使用者點擊鏈結後會進入釣魚網站，便可選擇金額開始進行交易手續。然而釣魚網站的交易內容並非預購 NFT 作品，實際上是受害者被鏈結的文章所吸引，毫無警覺內容的真偽，導致駭客成功騙取授權交易。

二、FB Messenger 點擊網址詐騙達高峰

亦有受害者 2020 年在 Messenger 收到名為「我不敢相信是你」的假 YouTube 影片鏈結，想觀看者必須先輸入 Facebook 帳號密碼，一旦使用者於假網站中登入，駭客便成功盜用使用者帳號密碼，隨後再將

無聊猿遊艇俱樂部推出 1 萬隻各有獨特表情的猿猴 NFT 作品。（Photo Credit: Bored Ape Yacht Club, https://boredapeyachtclub.com/#/gallery）



駭客透過官方推特私訊被害人（左），放上釣魚網址誘騙被害人點選購買商品（右）。（圖片來源：作者提供）

鏈結散播給該帳號的好友，讓被害人淪為散播惡意鏈結的工具。根據國外資安廠商 Pixm 發布的最新研究報告，**推估全球臉書至少有數百萬位用戶遭誘騙導致個資外洩**。

三、個人防範策略

在網路資訊發達的年代，駭客偽裝成一般使用者來散播惡意鏈結進行釣魚已是常態，因此資安意識對於民眾而言已是必修課題之一。防範作為有：

（一）提升潛在威脅警覺性：當收到陌生訊息、開啟未知網址、下載非官方軟體時，人們其實難以辨別其中是否夾帶惡意行為或攻擊，應提高警覺性，避免落入駭客陷阱。

（二）陌生訊息：當使用者瀏覽社群媒體上陌生人所發布的訊息時，應時刻保持懷疑的態度，在進入網址前要先查證訊息的正確性。如 NFT 遭盜取事件中，在社群網站看到 NFT 鏈結時，**應先去向官方求證**，而不是相信社群網站的訊息。只要使用者對內容產生懷疑並查證，就可以有效避免釣魚事件發生。

FB Messenger 曾遭駭客利用傳送假訊息，誘騙使用者登入釣魚網站，藉此竊取個資。（圖片來源：作者提供）

圖 1　一般使用者遇到的網路釣魚情況

（三）未知網址：收到朋友傳遞的未知網址時，使用者**應先確定該消息為本人傳遞，才點擊鏈結**。如案例 FB Messenger 點擊網址詐騙中，使用者在收到可疑鏈結後，可透過打電話的方式來確認朋友身分的真偽，避免朋友的個人帳號遭到駭客利用而不自知。

（四）使用威脅檢測軟體：使用檢測軟體可以有效偵測惡意鏈結和惡意程式，大幅降低使用者被釣魚的風險。當使用者遇到必須點擊陌生鏈結或執行來歷不明檔案的情況時，可以利用 Virustotal 檢測軟體，使用者將鏈結或檔案上傳後，該軟體會自動偵測其是否被資安廠商認證為惡意鏈結或檔案，並產出相應的報告。使用者可自行評估該檔案所伴隨的風險。基於安全考量，倘若有任一廠商對該鏈結報有疑慮，建議使用者不要點擊。

企業事件與防範策略

有別於個人案例，駭客對於企業的攻擊更具威脅性，其會針對企業的特色、員工的素質、工作內容進行釣魚郵件的客製化，進而達成各種攻擊目的。這種持續針對特定組織發起的網路攻擊我們稱之為進階持續性滲透攻擊（Advanced Persistent Threat, APT），以下為 APT 案例發生的過程。

一、SolarWinds 網路監控軟體公司遭駭客入侵

SolarWinds 開發的軟體 Orion 主要是幫企業進行網路監控及管理。**2020 年 12 月傳出 Orion 遭到駭客入侵的消息，其嚴重性不只影響 SolarWinds 本身，連透過該軟體進行網路管理的企業都深受其害。比較知名的包括美國國務院、國防部、司法部及 NVIDIA、Microsoft 與 Intel 等國際企業皆傳出災情**。只要使用該軟體，駭客就能一舉獲得該組織的網路架構，並且遠端執行惡意程式碼進行攻擊。

圖 2　SolarWinds 軟體遭駭散布流程

這次事件 SolarWinds 企業本身並不是駭客的主要目標，而是與其合作的相關企業。駭客首先透過社交工程手段入侵 SolarWinds 後，並沒有急於進行攻擊，而是持續蒐集資料，第二階段目標就是將惡意程式混入 Orion 軟體中且不被發現，在最終階段經由各企業下載，將帶有惡意程式的軟體散布出去。

根據上述實例可發現，駭客主要是透過釣魚郵件來進行攻擊，因現今企業仍然以電子郵件為主流的通訊方式，其不限時間地點的特性便於員工使用。然而企業中每天需要處理的郵件數量非常多且種類繁雜，一不小心便讓駭客有機可乘，其中最常見的郵件設計內容為商業電郵詐騙（Business Email Compromise, BEC）。

二、BEC 釣魚郵件實例

根據 2022 年臺灣資安公司對 BEC 郵件進行的分析，得出一些常見案例，駭客經常使用像“office”、“president”、“chief”、“director”等高階職務名稱作為電子郵件帳號，透過偽造身分，來向員工索要機密檔案。或是會偽造一個與被冒充人非常相似的地址，包括將某些英文字母和數字互換以達到混淆的目的，像是英文 l（小寫 L）與數字 1（數字一）、英文

圖 3　真實與混淆的郵件地址

o 與數字 0 等，讓受害者難以在第一時間辨認出真偽。因此，使用者收到信件時，應多留意信件的來源地址是否正常，若有異常之處即可通報或忽略該信件。

三、現今企業的防範措施

整體來說，釣魚郵件的設計類型千變萬化，只要謹慎檢查寄件方的電子郵件與檔案就可以有效避免。當你在郵件中看到檔案，可以先確認是否為圖片偽裝、檢查寄件人電子郵件地址是否完全正確等等，千萬不要忽略這些重要步驟。

但企業中每天需要處理的郵件數量極多，單靠員工本身的資安意識來抵擋所有的釣魚郵件有點不切實際，倘若能實現沙盒測試與零信任架構，必定能有效抵抗威脅。因此以下分別介紹沙盒測試及零信任架構這兩種現今企業可用的防範措施。

（一）沙盒測試：BEC 商業詐騙之所以難以抵擋，是因為很難斷定該郵件檔案是好是壞，依目前技術來說，最有效的方式就是進行沙盒測試。通過將環境徹底隔離，模擬檔案執行的情況，並觀察這些程式會做哪些動作？連到哪些網站？安裝哪些程式？做一個詳細完整的分析紀錄並上傳至監控中心。雖然執行過程要一段時間，但只要取得該惡意程式

圖 4　沙盒測試示意圖

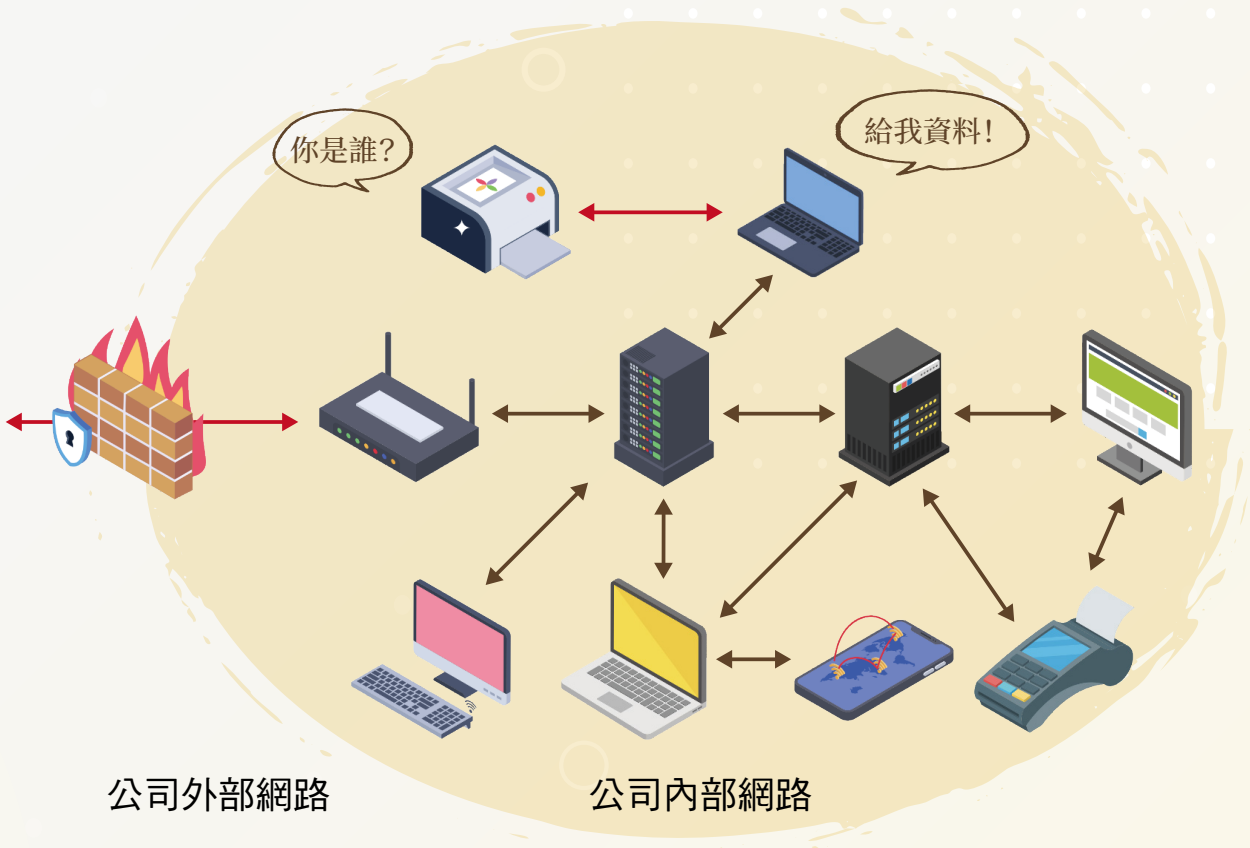


圖 5　零信任架構示意圖

的特徵後，之後檔案只要進行比對就可以確認是否為惡意程式，不必再模擬一次。透過這種方式，可以很好且有效率的分辨出惡意檔案。

（二）零信任架構：於此架構下，不論進行任何操作都需要進行身分驗證，以抵擋駭客入侵後所造成的威脅。基於對各種流量頻繁的驗證，儘管駭客入侵員工的電腦，也難以繞過員工的身分驗證系統進行進一步的攻擊，因此零信任架構是近幾年資安持續推動的方向。例如美國聯邦政府在頻繁遭受攻擊後，於 2021 年 9 月 7 日公布《聯邦零信任戰略草案》（Federal Zero Trust Strategy），目標是讓企業組織的網路安全架構，都是基於零信任原則而成。

結語

無論是一般民眾或是政府企業，都會收到來自駭客的釣魚攻擊，手法層出不窮且越加高明。除了依靠系統提供的自動防禦偵測機制外，全民應提升對於釣魚訊息的警覺性以及基本認知，才能計出萬全，去危就安。

社團法人台灣 E 化資安分析管理協會（ESAM）