資安木馬屠城記

論社交工程與APT駭客攻擊手法

■ 法務部調查局資通安全處　張文忠

社交工程（Social Engineering）與進階持續性滲透攻擊（Advanced Persistent Threat）是目前十分常見的駭客攻擊手法。攻擊的第一步是誘騙使用者打開含有惡意程式的檔案或電子郵件，猶如上演木馬屠城記，使用者自願開啟後門後，讓駭客輕而易舉地入侵使用者電腦，再透過長時間地潛伏尋找最佳時間出手竊密或進行破壞。比起直接攻破網路閘道器的外部攻擊，電子郵件詐騙是屬於最常見的社交攻擊手法之一，因採取社交攻擊成本最低、效果最好，這種針對資訊系統中最弱的一環「人性」發動攻擊的手法，也成為駭客最愛利用的方式。

進階持續性滲透攻擊又稱為「APT攻擊」：A（Advanced）指精心策劃進階攻擊手法、P（Persistent）則指長期且持續性地潛伏、T（Threat）可理解為威脅或攻擊，指人為參與策劃的攻擊。APT 攻擊通常是針對特定的目標，經過隱匿而持久的電腦入侵過程，最常見的是出於商業或政治動機，針對特定組織或國家，在長時間內保持高隱蔽性，特色在於低調且緩慢，利用各種複雜的工具與手法，相當有耐心地逐步掌握目標的人、事、物，不動聲色地引誘受害者上當，進而竊取機密資料；而與社交工程密不可分的原因在於，通常駭客利用特製的社交程式或電子郵件當作攻擊的釣餌，所以社交工程可以稱作是 APT 攻擊的蜜糖蛋糕。除了常見的 EXE 檔、COM 檔及 BAT 檔等執行檔能夠藏病毒外，開啟 PDF 檔、Word 檔等文件檔案都有可能中社交工程的招。

在 APT 攻擊還未廣泛被駭客運用之前，境外敵對勢力早已發動過這類的攻擊，目標常鎖定在我國的政府機關。目前境外網軍也已大規模發動 APT 攻擊，因此我政府機關時常遭到社交工程及 APT 攻擊，本（法務部調查）局亦是最常受到攻擊的目標之一。

攻擊實例

本局為討論兩岸交流及統戰因應防處作為等議題，於 105 年 7 月舉辦國安研討會，邀請國內各情治單位中堅幹部參訓。承辦科Ｏ科長於 5 月初即著手邀請研討會來賓等事宜，為求研討會盡善盡美，Ｏ科長上網搜尋了相關領域的專家並得到了 A 君之公務郵件信箱，隨後以電子郵件詢問 A 君是否能夠蒞會指導。經多次電子郵件往來後，A 君因「520」政府交接後擔任要職分身乏術，只能婉拒參加本次的國安研討會。

數日後，Ｏ科長的信箱收到新政府另一位官員 B 君的來信，信件內容涉及本次國安研討會討論之機密事項，且為Ｏ科長十分重視急需之資料，惟此時Ｏ科長腦中冒出了幾個問號，觸動了雷達警報：

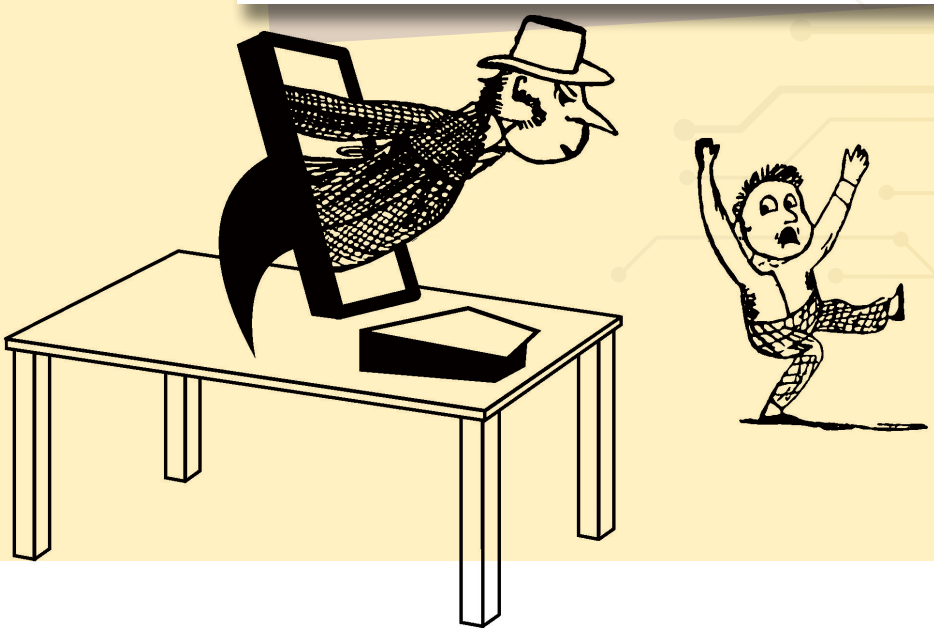
1. 平日未使用之公務信箱，為何在寄信給 A 君後，就收到 B 君的回信？
2. Ｏ科長與 B 君素昧平生，不相識且未曾聯繫，B 君如何得知本次國安研討會之資訊？

更重要的是，因平日的社交工程演練，讓本局同仁皆有資安防護的危機意識，Ｏ科長首先利用了防毒軟體掃毒，B 君來信安全通過掃毒軟體的檢驗。為求謹慎，Ｏ科長再透過管道聯繫 B 君，不料 B 君表示未曾發過此封郵件，顯見此封信件應是冒名傳送的社交工程郵件；Ｏ科長隨後致電資通安全處的電腦偵辦科請求協助，經過電腦偵辦科的鑑識後才發現，這正是一個不折不扣的社交工程郵件，只要一開啟文件，就會開啟電腦的後門，拱手歡迎敵對勢力進入內部網路恣意瀏覽機密。從這個例子中可以發現，即使自己的電腦再安全，駭客仍可以利用入侵 A 君電腦，抑或是在網路上中途攔截封包，藉以進行社交工程及 APT 攻擊，面對這種針對「人性」弱點的攻擊手法，千萬不可掉以輕心，時時都須將資安意識放在心裡。

資訊安全的大原則是：「整體資安水平取決於全體最低的水準」，機關內的資安設備再先進，人員訓練再優良，只要有 1 位同仁輕忽資安的重要性，讓駭客有機可乘，整體的資安防護也隨之瓦解。每個人都應隨時保持資安意識，不要成為機關內部的「老鼠屎」了！

社交工程與 APT 攻擊所造成的資安事件未來只會層出不窮，釣魚攻擊手法必定時時翻新，身處危機當中的我們應當小心防範，以下的資安宣導短語請大家銘記在心：

1. 電腦漏洞常更新，防患駭攻才安心。
2. 防毒軟體常啟動，阻擋病毒沒漏洞。
3. 資訊安全心中放，個人資料有保障。
4. 來路不明軟體不安裝，電腦防毒做好最健康。
5. 電子郵件不亂收，慎點連結防陰謀。
6. 電腦防駭、心情才 HIGH。
7. 不明網站 no stay，資安觀念 long stay。
8. 資料上雲端，駭你好簡單。
9. 社交工程無警覺，勒索軟體緊跟隨。
10. 網路使用便利多，資安觀念要囉嗦。
11. 電子郵件若亂開，電腦病毒跟著來。
12. 網路謠言多，查證莫放過。



不只是X戰警

—從好萊塢電影的駭客觀談資通安全

■資訊工業策進會資安科技研究所技術服務中心資安工程師　陳彥銘

您是否有特別注意？電腦駭客其實是好萊塢電影裡相當重要的角色元素，這個角色雖是不惹人注目的配角，卻必須提供高度的技術性支援，負責解決一切跟資訊系統或機電設施有關的疑難雜症，這樣的設定尤其容易出現在特務團隊的電影裡，「不可能的任務」系列電影就是最典型的例子。

駭客角色之設定

在「不可能的任務」情報局（IMF）這個特務團隊中，由阿湯哥飾演的特務—伊森韓特必須冒死與反派搏鬥，必要時還需要入侵高度機密組織竊取有價值資產或資料，而背後支持他的電腦高手—班吉，則肩負為主角排除一切障礙的重要工作；駭入攝影監控及機電系統以躲避警衛的察覺只是家常便飯，入侵俄國衛星系統以取得飛機艙門的控制權更是小菜一碟，更常見的任務則是入侵嚴密保護的政府網站，如CIA 或軍情局來取得高度機敏的資料。

在資安產業中，駭客可分為「黑帽駭客」、「白帽駭客」與「灰帽駭客」三種。所謂黑帽駭客指的就是資訊犯罪分子，例如之前轟動一時的一銀盜領案，利用惡意程式不法取得金錢；白帽駭客是所謂的道德駭客，由政府企業聘雇，在業主許可下為組織所維護的資訊系統進行探測入侵行為，藉以發掘安全漏洞；灰帽駭客則是遊走於白帽與黑帽之間，一方面從事資訊安全任務，另一方面也會從事未經授權的入侵行為。好萊塢電影的官方設定基本上以灰帽及黑帽駭客較為常見。

駭客手法之描述

電影為了彰顯駭客高竿的功力，最廉價的方式是在對白裡描述該角色的豐功偉業（通常是驚人的資訊犯罪紀錄），但口

（圖片來源：作者提供）

說無憑怕觀眾不會買帳，故有時也需要一些畫面來加深說服力。常見的方式之一，是在電腦螢幕上呈現指令操作紀錄或程式碼，通常會選擇進階一點的讓觀眾有看沒有懂，例如文字形操作指令或是較低階的組合語言，但若要同時兼顧技術性與娛樂性著實不容易。電影「劍魚」裡，由休傑克曼（曾飾演「X 戰警」電影中的金鋼狼）所飾演的頂尖駭客，被僱來建構超級電腦進行破密分析，以入侵美國最高機密的劍魚系統，但必須先通過雇主約翰屈伏塔的殘酷考核，在腦門被槍口指著的情況下，被要求於一分鐘內入侵美國國防部資料庫網站。此時導演以鍵盤打字速度來彰顯其電腦功力，若內行人看來，必定認為其專業性不足；但若以一般民眾觀影角度來說，堪稱娛樂性十足，畢竟若要花時間向觀眾解釋何謂資料隱碼攻擊（SQL Injection）或跨網站指令碼（Cross Site Scripting, XSS）等攻擊手法，稍顯強人所難。

脆弱的資訊安全

電影裡呈現的駭客攻擊手法也讓觀眾了解資訊安全原來可以如此脆弱。影片「迫切的危機」，由哈里遜福特所飾演的 CIA 副主任，委託局內的資訊高手破解帳戶密碼，他只用了帳戶本人及相關家屬的出生年月日的排列組合就輕易解開密碼，速度快到甚至連哈里遜福特都還未踏出資訊室就已完成，可以想像有多少觀眾在電影散場後立即去修改自身的帳戶密碼。

布魯斯威利所擔綱演出的終極警探系列電影裡，也常出現駭客的角色，尤其是「終極警探 4.0」，此部就是以駭客為電影主軸，駭客試圖掌控網路系統，包含交通、

金融、民生相關資訊系統都難逃魔掌，甚至核電廠也受害，讓觀眾驚覺關鍵基礎設施資訊安全防護的重要性，更與目前政府喊出「資安即國安」的觀念相呼應。

社交工程攻擊

近期最貼近真實駭客手法的電影，非克里斯漢斯沃領銜主演的「黑帽駭客」莫屬，雖然以一部娛樂商業片而言，觀眾的接受度不是挺好，票房口碑也不如預期，但若以資安專家的角度來看，這部電影細膩刻劃出駭客的真實行為，可說是專業度十足。其特別之處在於：精心呈現了典型的社交工程攻擊手法。為了取得特定使用者的密碼，克里斯漢斯沃所飾演的駭客首先偽冒 E-mail 寄件者，信件主旨為要求收件者立即更改密碼以提升資訊安全，但其實 E-mail 內夾帶了惡意的鍵盤側錄程式，故收件者開啟信件附檔的同時，此惡意程式就被植入主機，後續所輸入的新密碼立即被側錄，接著透過隱匿的網路連線傳送至駭客手中。試想，若這不是一部商業大片而是由多名當紅演員所擔綱的資通安全教育電影，其實已相當值回票價。

結語

我國政府為推廣全民的資安意識及加強校園學生的資訊安全技術能力，每年也會定期舉辦資安系列競賽，包含微電影、動畫金像獎等；除此之外，我國主管機關或可加入與國內影視業者之合作，透過置入式行銷的手法宣導資通安全教育。資安題材於電影中的出現，某種程度來說，讓民眾於日常休閒娛樂的同時，更可深植維護資訊安全應該有的具體作為。下次走出電影院時，除了討論精采緊湊的情節、帥氣動人的男女主角外，我們更應該謹記，密碼設定不應簡單的取自自身或家人的生日年月、收到可疑郵件時更應再三確認；換個角度，從資訊安全的層面來觀影，相信能帶來更豐富的省思。