

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 nostay，資安觀念 longstay。
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。

(摘錄自清流月刊 106 年 6 月號)