淺談駭客攻擊

◎魯明德

科技部於今（103）年3月初才成立，就驚爆網頁遭到入侵。小潘看到這則新聞後，想到以前念過的資訊安全，好像都在講資訊的加解密；駭客到底是如何入侵網站？帶著滿肚子的疑問，小潘立刻針對駭客問題向司馬特老師請教，司馬特老師娓娓道來，其實網際網路是個非常不安全的平臺，它在確保資訊安全的能力上，本來就是先天不足、後天失調，才造成今天的駭客橫行。

網際網路在設計初始，其目的是為了提供美軍做為資訊交換之用，並沒有想到有今日的用途，所以網路架構設計係採用 TCP/IP 的協定，主要著眼在快速、正確地傳達訊息，因此在安全性的考量上著墨較少，這是它先天不足的地方。

當柯林頓政府把網際網路開放做為商業用途至今，網際網路快速擴張，輔以微軟作業系統的普及，幾乎大部分的電腦都採用微軟的 windows 作業系統，透過 TCP/IP 的通訊協定連上網際網路。然而，問題就在於微軟的作業系統其實也有許多安全漏洞，加上使用者眾，遂成為駭客覬覦的目標，這是它後天失調之處。

小潘聽完司馬特老師的說明，終於了解網際網路常被入侵的原因。但是，什麼是駭客呢？司馬特老師繼續說明，我們一般都把那些惡意入侵他人電腦、破壞或竊取資料的人稱為駭客，其實英文上，對於入侵他人電腦的人，又可分為 Hacker 及 Cracker 二類；其中 Hacker 原來是指那些具有電腦程式能力，喜歡寫程式或挑出系統問題，並予以補強的程式設計師，他們通常是針對系統中存在的弱點處入侵，但不會故意破壞系統；Cracker 則是指那些比較惡意，未經他人允許就進入系統搞破壞的人，不過現在大家也都把他們稱為駭客。

駭客在入侵前，一定會根據入侵的目的，先確定要攻擊的目標。攻擊的目的可能有：商業目的、報復目的、單純練功等；確定攻擊目標後，駭客就會開始大量蒐集目標資訊，其中包括：主機的數量、使用的作業系統、使用何種郵件系統、網路伺服器、防火牆、系統漏洞等。當這些資訊都蒐集完畢後，駭客們就會使用他們的攻擊方法，運用各種技巧入侵目標系統。

小潘聽完後頻頻點頭，原來駭客的攻擊是有戰略的，但是它的戰術又有哪些呢？司馬特老師接著說下去，駭客的攻擊通常分為4個階段：感染、持續、通訊、操作。駭客入侵電腦的過程，類似人們感冒般，感冒前會先受到病毒的感染。同樣地，駭客在入侵前，也會透過釣魚郵件、軟體漏洞、

下載惡意程式等方式，讓目標電腦先遭到感染。由於電腦技術的進步，駭客可能藉由一個暗藏攻擊的網址，就能讓電腦的門戶大開，所以大家常用的社群網站或通訊軟體，便是很好的攻擊載具。

當惡意程式順利進入目標後，必須要讓它能夠持續存活，不致因系統重新開機而陣亡，因此惡意程式要能夠修改開機順序，比作業系統更早載入，才能確保常駐被感染的電腦。為了避免被防毒軟體或防火牆發現，惡意程式也會偽裝，本身沒有寫入攻擊指令，在常駐後再向外界的伺服器溝通。因此，駭客會透過遠端遙控的方式，操縱惡意程式，進行各種破壞或竊取工作。為避免傳遞指令被電腦使用者發現，通常會利用加密的方式傳遞，或利用 proxy 代理伺服器做為跳板，或是直接取代 DNS 伺服器。當受感染的電腦接到指令後，就會尋找電腦內特定的資訊，或是記錄使用者操作電腦的指令，或是再去感染其他的電腦，尤其在今日社群網站普及的時代，很多感染都是透過社群網站做為媒介。

聽完駭客攻擊的方式後，小潘又想到：該如何避免惡意程式的攻擊呢？司馬特老師接著說，為避免電腦遭到惡意程式攻擊，首先要做應用程式的控管，不明來源的程式不要安裝在電腦中，如果真的要使用，也應先進行掃描後再行安裝。其次，要進行使用者的控管，現實生活中常是１臺電腦有多位使用者，此時應儘量將使用者設定成不同的使用者帳號，權限也應越低越好，最好每位使用者的儲存空間或應用程式完全分開，避免交互感染。最後是網路管理，千萬不要為了資料交換的方便，而開啟無帳號密碼的資料分享空間，以避免惡意程式感染公用資料夾中的檔案，造成大量感染。

小潘對於駭客有更進一步的認識，同時也深刻體會到任何科技如果無使用者的自制與管理制度，終究是無法有效控制。

（文摘自法務部調查局清流月刊 103 年 5 月號）

嘉義區監理所 關心您