# 你被駭客害了嗎？

看似平靜無波的網路世界，實則波濤洶湧，充滿難以預料的數位危機。隱匿在網路背後，可能是單純的數位資料使用者，也可能是居心叵測的駭客。由於電腦的軟硬體防護條件、網路使用者的電腦技能參差不齊，使得駭客可利用特定的網路技術，不知不覺地入侵防護力較弱的電腦，竊取、竄改各種電磁資料，進而癱瘓電腦設備，甚至當成網路攻擊的中繼跳板，造成無法有效控管的資訊危機。

透過網際網路攻擊連網電腦的駭客，可能是個人或具特定立場的組織，也可能是各國的網軍。駭客攻擊的動機則可歸納為以下幾點：掌握各國政府機密、破壞重要設施、獲取商業利益、炫耀電腦技術、彰顯特定政治立場。駭客的攻擊流程通常如下表：

## 一、駭客常用的攻擊手法

### （一）特洛伊木馬程式（Trojan horse）

駭客透過 e-mail 附件及偽裝成有用程式等方式，將特洛伊木馬程式傳送到被害主機，並誘使用戶安裝。電腦被植入特洛伊木馬程式後，會自動安裝後門程式。當本機使用者開機連網後，程式會自動向駭客報告本機的 IP 及預設的連接埠，駭客再利用惡意程式，取得本機的完全主控權，甚至以此為網路攻擊跳板。有些駭客會把木馬程式與合法檔案加以捆綁，以欺騙本機的管理者。木馬程式的攻擊型態，可再細分為：遠端訪問型、密碼發送型、鍵盤記錄型、系統毀滅型、FTP 控制型。

### （二）阻斷服務式攻擊（Dos/Denial of service）

本攻擊通常是利用 TCP/IP 協定的某些弱點或系統中的安全漏洞，對目標主機發動大規模的攻擊，使目標主機無法對合法用戶提供正常

服務。Dos 攻擊又可細分為：電子郵件攻擊、畸形訊息攻擊、SYN 攻擊、Smurf 攻擊、路由攻擊、分散式阻斷攻擊、DNS 攻擊、UDP 攻擊、Land 攻擊、死亡之 Ping 等。

（三）Web 欺騙模式

Web網頁的URL若被駭客篡改過，假的URL會掩蓋真正的URL。當瀏覽者點選目標網頁後，假的 URL 會將瀏覽者導引到駭客所架設的伺服器，並利用假網頁騙取使用者的帳號、密碼及金融交易資料等。

（四）Web 攻擊

Web 攻擊主要可分為 XSS 攻擊及 SQL Injection 攻擊。XSS 攻擊主要是在可信任的網站上，插入一段惡意程式碼。駭客可以偷取使用者的 cookie，利用 cookie 竊取帳號，並登入系統。SQL Injection 攻擊發生在程式未檢驗使用者的輸入內容，攻擊者可利用此漏洞，攻擊後端的資料庫，甚至是奪取資料庫的控制權。Injection 攻擊容易發起，在短暫時間可達到大量的網站攻擊。

（五）網路監聽（Sniffer）

根據 Ethetnet 協議，在同一條物理傳輸通道上的主機，可以接收到本網段的所有訊息。當網路監聽者將網卡設定為混雜模式（Promiscuous），就可以進行網路監聽，並記錄符合監視條件的封包。本網段傳輸資料只要沒有加密，當某一主機使用網路監聽工具，就可以監視網路狀態、數據流量、傳輸資訊等。

（六）緩衝區溢出（Buffer Overflow）攻擊

本攻擊乃針對通往緩衝區的程式，編寫超過緩衝區長度的內容，造成緩衝區的溢出，可能出現的結果有二：1.破壞程式的堆棧，使程

式轉而執行任意指令，甚至可以取得系統 root 特級權限；2.以過長的字串覆蓋相鄰的儲存單元，引起程式執行失敗，甚至導致系統崩潰。此類型攻擊，因傳輸的數據分組並無異常特徵，所以防火牆無法發揮阻擋功用。

（七）系統植入病毒的破壞性攻擊

駭客利用普通檔案或圖片作為病毒傳遞的載體，輕則破壞檔案資料，重則將硬碟格式化，造成主機的極大災難。

## 二、偵測駭客攻擊的徵兆

駭客入侵電腦系統時，會隱藏自己的真實 IP；入侵目標電腦後，會抹除日誌檔中的入侵操作紀錄，並安裝後門程式，以便日後可以隨時入侵本機。一發現主機可能有被入侵的跡象，使用者可以透過以下的方式，進行初步檢測：檢查電腦用戶名單、目前的網路連線、遠端服務、事件檢視器、Web 日誌文件紀錄、新增的可疑檔案、監控異常的數據流量及其特徵、主動檢查檔案或資料夾是否被強制隱藏。

## 三、防制駭客攻擊十八要

（一）重要主機要有獨立的網段

為防範網路監聽，要將網路進行合理分段，並在網路中設置交換器、動態集線器、橋接器，對數據流量進行限制。作為 FTP、Telnet 用途的主機，應具有獨立的網段，避免同一網段的某一臺主機被入侵後，駭客利用網路監聽技術，截取本網段的所有通信資料。重要主機可以考慮裝設在交換機上，避免駭客利用 Sniffer 監聽密碼。

（二）專門用途的主機只打開專用功能

具有專門用途（如網管、資料庫、電子郵件、WWW、DNS 等）的主機，不安裝任何開發工具，只執行與用途相關的應用程式，並關閉遠端協助的功能，使主機減少被駭客攻擊的機會。

（三）關閉不用的連接埠

電腦與網路連結要透過連接埠，對我們無用的連接埠，對駭客可能是有用的攻擊路徑。因此將主機不必要的連接埠（如 NETBIOS）關掉，可以減少駭客入侵的風險。

（四）網管原則

為維護網路安全，網管人員的網管原則：將網路用戶的權限最小化、監控各用戶異常的封包傳輸量、不用電子郵件寄送密碼、加強密碼強度以提高駭客入侵主機的難度。

（五）單次性密碼技術

單次性密碼技術並非在網路上傳遞密碼，而是在使用端與伺服器端進行字元串匹配。使用端從伺服器端得到 Challenge，與自身的密碼演算出一組新的字元串，並傳回伺服器端，經過驗證匹配後，即允許建立連線。所有的 Challenge 與字元串只使用一次，具有極高的安全性。

（六）下載作業系統及應用程式的安全修補程式

作業系統廠商會不定時發布安全漏洞修補程式，使用者要將電腦的安全性更新設定為「自動更新」，那麼只要電腦開機連網，便能自動更新系統漏洞，提升電腦環境的安全性。

（七）重要資料備份

當電腦網路受到駭客入侵，系統、資料被破壞時，平時定期備份的重要資料就可將損害降到最低。重要資料要異地備份儲存，並要定時掃瞄檢查，以確保其可用性。

（八）資料加密

將傳送到網路上的封包予以加密，可以保障資訊的完整性、真實性、保密性，如此也能防止駭客網路監聽。加密時可以對數據封包中的重要訊息加密，也可只對應用層加密；加密方式取決於資料的安全等級。

（九）過濾封包

配置路由器可以拒絕網路外部與本網段具有相同IP的連接請求。當外來封包的 IP 不在本網段內時，路由器不應發送本機的封包。但路由器僅能過濾聲稱來自內部網路的外來封包，而無法防止駭客冒用外部可信任的主機，進行 IP 欺騙。因此可以在路由器前端進行 TCP 攔截，只有完成三次 TCP 交握程序的封包才能進入本網段。

（十）取消檔案及列印共用功能

電腦系統中的「檔案及列印共用」功能，是駭客入侵的漏洞之一。因此除可將對話框的「檔案及列印共用」功能取消外，還可從註冊表中修改：首先執行 regedit 指令，進入 HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Policies，接著在「Policies」按滑鼠右鍵，新增 DWORD 值，數值名稱鍵入「NoFileSharing-Control」，數值設為「１」，以防他人更改。

（十一）禁用 GUEST 帳號

透過 GUEST 帳號，可以有限制地訪問主機，卻也為駭客打開入侵之門，進而獲得系統管理者的密碼及權限。因此最好禁用 GUEST 帳號：控制臺/使用者帳戶/關閉 GUEST 帳戶。

（十二）禁止空連接

在系統默認的狀況下，任何用戶皆可透過空連接方式連上伺服器，猜測帳號及密碼。使用者可透過註冊表關閉空連接功能：執行 regedit 指令，進入 HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/Lsa，按滑鼠右鍵兩下，在「restrictanonymous」中，數值設為「１」。

（十三）隱藏本機 IP

在本機與網站伺服器間加入代理伺服器，可以保護本機的 IP。當本機向網站伺服器提出服務需求時，代理伺服器先截取本機的請求，再由代理伺服器轉發本機的請求給網站伺服器。如此則駭客只能探測到代理伺服器的 IP，而非本機的 IP，便達到隱藏自己 IP 的目的。

（十四）謹慎使用 e-mail

e-mail 是駭客入侵的重要管道之一，用以實施垃圾郵件的阻斷式攻擊，進行郵件詐騙，騙取主機用戶的帳戶、密碼等；或將木馬程式附檔佯裝成有用的程式或更新，要讓使用者誤開而被入侵。以下為注意原則：1.不要開啟來路不明的郵件及其附檔；2.過濾較大的郵件；3.取消郵件預覽功能；4.下載附檔後，要先掃瞄檔案是否為病毒的偽裝。

（十五）避免下載來路不明的檔案

駭客常在熱門的程式、影片、音樂、圖片、電玩遊戲中植入惡意程式。使用者下載來路不明的檔案，要先用掃毒軟體澈底掃毒，確定沒有木馬病毒後再執行。

（十六）調整 SYN 的設定

網管人員必須在本網段的路由器上，對 SYN 半開封包的數量及流量進行配置上的調整，並在系統中設定與 SYN 數據段相對應的內核參數，讓系統對於超時的 SYN 請求封包強制復位，防制 SYN 阻斷攻擊。

（十七）調整防火牆設定

為防止駭客通過網路攻擊本機，使用者可以關閉防火牆的廣播位址特性，並在防火牆的進階設定中，設定丟棄該類型 ICMP 封包。

（十八）禁用瀏覽器的 JavaScript 功能

JavaScript 可對網路連接狀態進行改寫，因此駭客可以將他改寫過的 URL 恢復為改寫前的狀態，亦即用假的 URL 掩蓋真正的 URL。因此禁用瀏覽