新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2007/12/10- 2007/12/16 第53期

多功能 UTM / MS 系列報導

技術淺談與應用 - 病毒感染 VS 駭客攻擊

近幾年網際網路的普及帶給人們許多便利，卻也潛藏著許多陷阱與危機，網際網路上到處充斥著駭客的攻擊與病毒的傳播，不時有駭客入侵企業網路中盜取商業機密或是病毒發作造成企業損失的新聞報導，像是台灣索尼通訊網路 So-net 網站之前傳出被駭客入侵，造成會員網友個人資料外洩、信用卡被盜刷，以及前陣子流行經由隨身碟和 E-Mail 傳播的 KAVO 病毒，佔滿 CPU 效能使得其他程式無法執行，造成許多使用者的困擾，這些受害案例層出不窮，因此資訊安全儼然已成為企業網路中最重要的課題，在防毒防駭的前提下，認識病毒與駭客的攻擊型態是首要的任務。

病毒感染：

病毒通常是以被動的方式透過網路瀏覽、下載，E-mail 及可移動儲存裝置等途徑傳播，通常以吸引人的標題或檔案名稱誘惑受害者點選、下載。而某些電腦病毒類似生物病毒一樣具有傳染性，會感染中毒電腦裡其他的執行檔，如 exe、com、bat、scr 格式的檔案，或是利用網路共享的漏洞複製並傳播到其他電腦，進而感染區網內多台電腦的檔案。然而病毒運行後，通常會有一些特徵表現，如無法上網、CPU 效能達 100% 居高不下、無法顯示隱藏檔、出現藍屏…等現象，這些明顯的表現反而讓使用者容易發現自己電腦中毒並對清除病毒有所幫助。

駭客攻擊：

駭客通常會針對特定的目標掃描，尋找出該系統的漏洞，再以各種方式入侵系統並植入木馬程式，使得目標對外門戶大開讓駭客自由進出好竊取檔案資料，而駭客也可利用一個個已被攻陷的電腦組成殭屍網路（Botnet）對特定目標發動大規模的分散式阻斷服務攻擊（DDoS）或 SYN 攻擊，藉以把目標的系統資源耗盡並癱瘓其網路資源，若該目標是企業對外提供服務的伺服器，必然會造成企業若大的損失。

	病毒感染	駭客攻擊
型態	被動	主動
攻擊對象	沒有特定對象	針對特定目標
感染途徑	惡意網頁、P2P 下載、E-mail、網路芳鄰、隨身碟等可移動儲存裝置。	利用系統、程式的漏洞或以其他方式取得進入系統的帳號密碼，從外部入侵進行破壞。
比喻	持有合法護照的人士攜帶毒品（病毒程式）入境，而海關（企業網路的Gateway）並無察覺，於是在突破第一道關卡後，這些毒品將流入國內市面（企業網路），隨時產生危害。	被限制出入境的罪犯（駭客），用假以亂真的護照蒙騙海關（企業網路的Gateway）順利入境國內（企業網路），鎖定特定對象（企業內部的電腦）加以迫害。

為求網路安全，一般基本的防護方式就是設置防火牆並在用戶的電腦安裝防毒軟體，想藉此方式抵擋駭客的入侵及病毒檔案的感染，不過由於這幾年網路發展迅速，連同駭客的攻擊模式和病毒的傳播方式也隨之改變，日前發現駭客透過系統漏洞入侵一般網站將惡意的程式碼或帶有病毒的網頁嵌在正常的網頁當中，使得瀏覽此網站的用戶會自動執行駭客所設下的程式碼而下載木馬病毒，然而這類的病毒通常擁有自動更新的功能，並且據說更新的速度有時甚至還比防毒軟體快，由此可知使用一般的防火牆以及防毒軟體作防毒防駭的資安工程已經不敷使用。

而新軟系統所推出的多功能 UTM 不僅內建入侵防禦偵測系統（IDP）可抵擋駭客的攻擊，並且支援網頁掃毒的功能，可補足防毒軟體無法防護的項目，讓企業的網路安全防護更加有保障。另外針對 UTM 與防毒軟體的互補性，我們將在第 55 期「PC 防毒功能 VS UTM 防毒功能的互補性」的文章中做更多的說明。

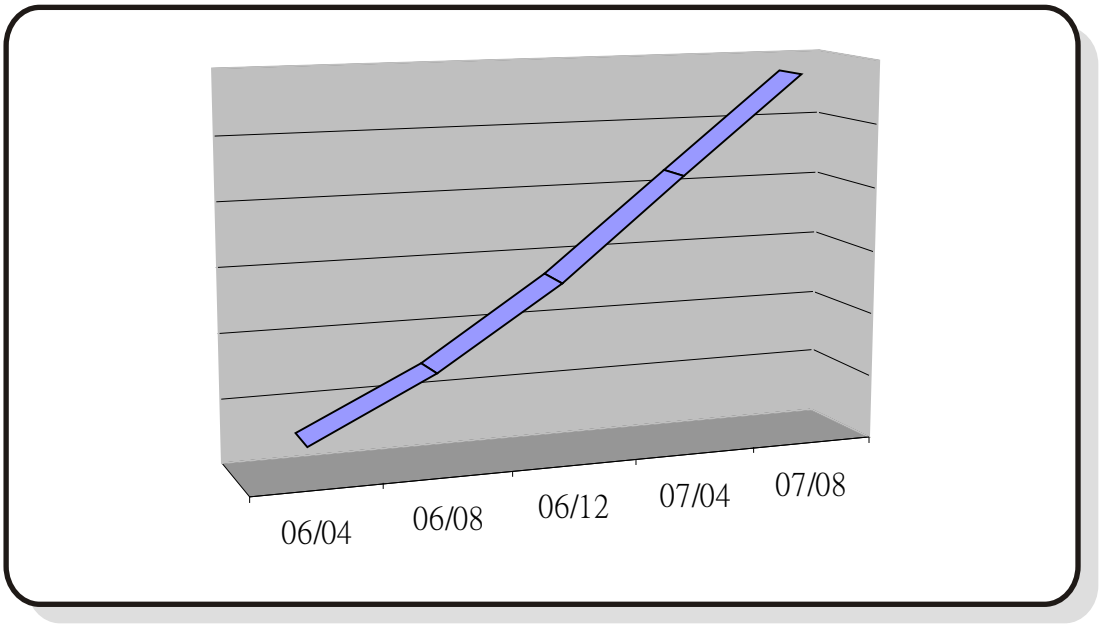
文 黃智傑 alex@nusoft.com.tw

市場行銷報導 - 如何對付氾濫成災的「惡意網頁」

在以往，「惡意程式（病毒、木馬、蠕蟲...）」的傳播以電子郵件為主；信件中夾帶「惡意程式」，再誘使收件者開啟，已達到傳撥之目的。但由於大部分的使用者已對此種傳播方式已有所了解（不會輕易去點選信件附加檔案），再加上市面上的防毒軟體對於此種郵件之防護日漸完善，使得利用電子郵件來傳播惡意程式的方式逐漸式微。取而代之的是另一種廣為大家使用的網路服務－網頁瀏覽。

駭客會將“網頁瀏覽”作為「惡意程式」的散撥管道，其原因不外乎是一般使用者最常使用的網路服務除了收發電子郵件外，就是以瀏覽網頁之使用量為最多。所以在電子郵件無法達到預期的散撥效果時，駭客們改採用網頁方式來散撥「惡意程式」。尤其在這半年內，這種散撥方式之數量快速增加，甚至已經超過所有「惡意程式」攻擊的八成之多。

也就是因為這種情況，導致網際網路上的問題網站越來越多－根據統計，其比例已經高達每 10 個網頁中，就有一個含有惡意程式。透過這些惡意程式，駭客們可以輕鬆取得使用者的各種資料、感染其他電腦、甚至是操縱使用者的電腦散撥垃圾郵件...。讓稀鬆平常的網頁瀏覽，成為敞開企業網路大門最大元兇。



圖一 全球惡意網頁數量快速成長

或許有人會想“只要小心避開駭客所架設的「惡意網站」，應該就沒有危險了”。這種想法在以前也許行的通，但是現在問題網頁反而大多數都是一般正常網站！！

正常網站怎麼會有「惡意程式」呢？其實，這些有問題之正常網站通常都有個很明顯的特徵“鮮少更新或修補其伺服器系統”。駭客們常常利用這些網站的安全弱點，入侵其網站伺服器，並在其中植入「惡意程式」。這些被竄改的網頁在外觀上完全正常，看不出有什麼不妥，而且大多為知名企業網站、政府網站、電視 / 報紙媒體網站...，所以使用者在瀏覽這些網站時通常不會有任何戒心。只要使用者瀏覽該網頁，「惡意程式」會被自動下載、安裝至使用者的電腦中。接下來，駭客要竊取使用者的資料、散發垃圾郵件...將暢通無阻。

既然瀏覽網頁會有中毒的危險，那在電腦中安裝防毒軟體來過濾「惡意程式」是不是就可以高枕無憂的瀏覽網頁呢？其實，僅用防毒軟體來預防網頁的「惡意程式」還是有風險的；防毒軟體在發現「惡意程式」之前，一些個人資料、企業機密...就可能已被「惡意程式」竊取。因此要確保電腦不會受到「惡意網頁」的威脅，最好做到以下三點：

1. 設定瀏覽器的安全權限 ——— 調整瀏覽器的自動執行權限，以防在瀏覽網頁時，瀏覽器自動執行了「惡意程式」。

2. 定期更新作業系統 ——————— 絕大部分的「惡意程式」都是利用作業系統的安全漏洞而設計。因此，定期更新作業系統才能確保不被「惡意程式」所感染。

3. 在閘道端隔離「惡意程式」—— 防堵「惡意程式」最佳方法當然就是不要讓它有任何機會進入電腦中。因此把它隔離在企業閘道外，方能避免「惡意程式」可能帶來的任何危害。

企業可以透過新軟系統－多功能 UTM 產品內建了「HTTP 防毒」機制來防護「惡意網站」之問題。使用者在瀏覽網頁時，多功能 UTM 會將網頁伺服器所回傳的資料先行過濾，確定無誤後才將這些資料傳送至使用者的電腦中。把「惡意程式」隔離在閘道端之外，使其無任何機會進入企業網路。因此，就算是使用者所瀏覽的網頁有問題時，多功能 UTM 也只是隔離「惡意程式」這一部份，不會影響到使用者的網頁瀏覽。

文 程智偉 rayearth@nusoft.com.tw