新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2011/6/1-2011/6/30 第128期

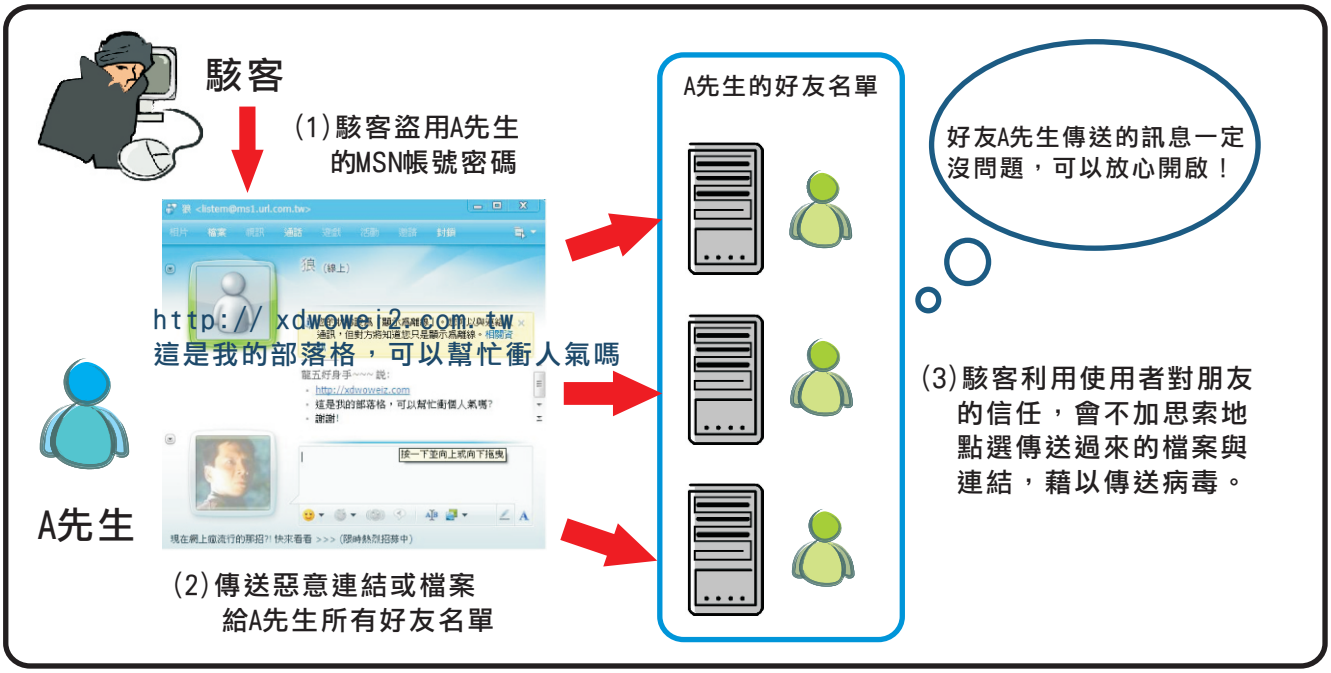
UTM / UTM系列報導

技術淺談與應用 - 新軟UTM有效預防社交工程攻擊

近年來網際網路發展迅速，使得電腦網路已成為社會發展與人們日常生活中不可或缺的重要工具，舉凡購物網站、網路銀行、社群網站等，須透過網際網路連線至這些相關商業服務的網站。因此，人們在日常生活中已與網際網路密不可分。但是，網際網路除了帶來生活的便利外，也伴隨著各種網路犯罪手法的快速成長，已對個人資料、財產、公司系統等產生極大的威脅。其中「社交工程」成為最常用且難以防範的攻擊手法。

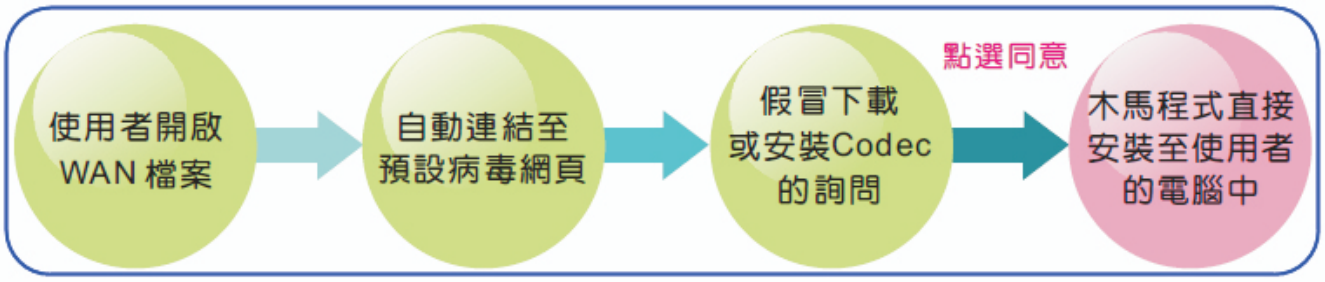
何謂「社交工程」(Social Engineering)？是一種「非全面」技術性的資訊安全攻擊方式，藉由人性的弱點進行詐騙。如惡意人士利用電話、電子郵件或假扮身分，取得他人信任進行欺騙。這些手法的特性是攻擊者並不需具備頂尖的電腦專業技術或攻擊工具，僅利用人缺乏警覺性或好奇心的弱點，就可輕鬆騙取個人資料、系統帳號密碼等重要資料。以下是常見的社交工程型態：

1. 各種即時通訊軟體(IM)：
即時通訊軟體病毒必須仰賴使用者之間互相傳遞。因此，駭客藉由入侵電腦，竊取電腦使用者的IM軟體帳號(如MSN、Yahoo…等)，並傳送惡意檔案或URL連結等方法，利用假冒使用者的身分誘騙使用者好友點擊傳送的連結。



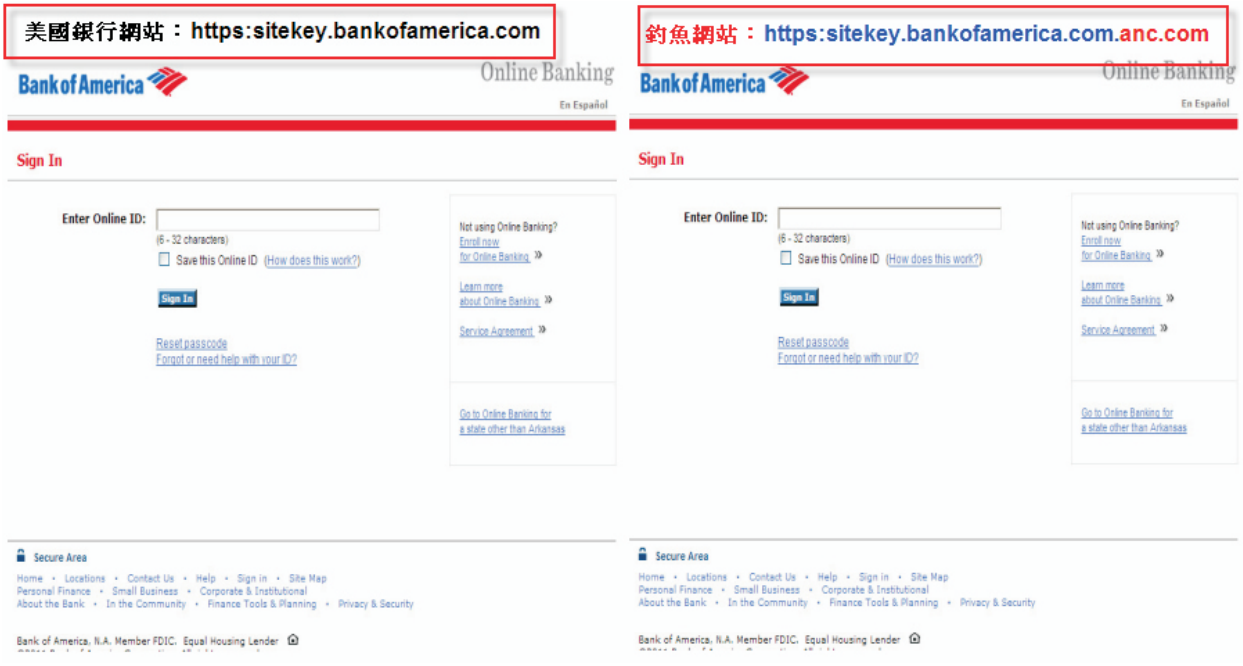
圖一

2. 多媒體影音中的惡意程式：
是針對影音播放程式攻擊的木馬，將多媒體檔案嵌入惡意程式，使用者一旦用影音播放程式打開受感染的多媒體檔案，電腦就會被連上惡意程式。



圖二

3. 網路釣魚：
網路釣魚所用的誘餌千奇擺怪，包括偽裝知名銀行或機關單位通知收件人資料過期、無效需要更新，或登入某網址輸入個人資料等詐騙方式。取得個人帳戶、信用卡或公司機密…等資料，造成公司資料外洩或個人帳號密碼被盜用等嚴重後果。



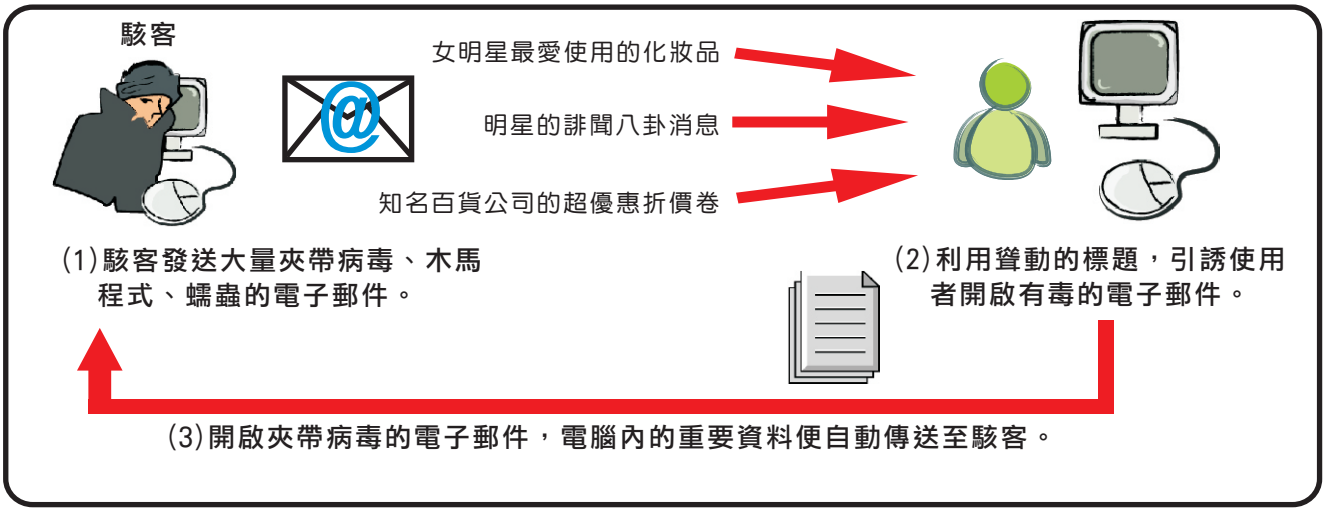
圖三

4. 偽裝修補程式：
偽裝系統廠商或防毒軟體業者，寄送假的修補程式或更新程式的電子郵件，引誘使用者下載安裝。此種手法不但不會修補作業系統的任何漏洞，還可能被安裝了遠端竊取資料的木馬程式。

5. 互動式社群網站攻擊：
是一種通過社群網站傳播的蠕蟲，可以在推特、facebook、噗浪等知名網站散佈；一旦受害，電腦會被啟動後門程式，私密個資可能不保，同時還會發送有害連結給線上朋友。

圖四

6. 電子郵件：
駭客利用電子郵件夾帶病毒、木馬等惡意程式，郵件標題再藉由熱門時事、養生保健或情色相關等聳動標題，引誘收件者開啟郵件所附帶的惡意程式。甚至假冒收件人好友，騙取收件人的信任，進而開啟郵件，造成資料外洩。



圖五

在瞭解社交工程的攻擊手法後，有效防範社交工程企業應著手於三大方向：一是內部資安政策，另一網路防護的軟硬體，最後員工須有正確的資安觀念。此三大方向是相輔相成，缺一不可，小則造成個人用戶使用的不便，大則造成網路的癱瘓、重要機密資料被竊、存檔資料遺失…。因此，新軟系統UTM系列產品，提供「郵件安全機制」、「入侵偵測防禦」、「應用程式管制」、「網站管制」等幾種方式，且搭配公司的資安政策，有效防止公司成為社交工程攻擊的對象。

1. 郵件安全機制：
由於電子郵件的便利，卻帶來垃圾郵件與病毒郵件的危害。因此，新軟系統「MLS」、「MAF」與「UTM」系列是擁有郵件安全防護性質的產品，皆提供「多重垃圾郵件過濾機制」與「病毒防護」(內建ClamAV與Sophos雙掃毒引擎)功能結合，除了直接將垃圾、病毒郵件阻擋在公司網路之外；亦可將阻擋釣魚郵件。而且公司資安政策中應規定內部員工須確認信件來源，不要開啟來路不的電子郵件（如過於聳動的主旨、陌生人或少往來對象來信、要求輸入機密資料等）及可疑的附件檔案(如exe、dll、scr、bat等)；也避免開啟與公務無關的電子郵件。

2. 應用程式管制：
繼電子郵件之後，各種應用程式軟體成為現代人或公司員工所廣泛使用的通訊及娛樂的橋梁，如即時通訊軟體(MSN、QQ、Yahoo、Web IM…)已成為與客戶商業往來的重要溝通工具。由於即時通訊軟體的便利，進而使駭客利用IM傳送惡意連結或木馬程式等攻擊，來竊取個人或公司內部相關重要資料。而且公司網管人員可依據各部門業務的需求給予開放或限制使用即時通訊軟體的權限，且透過新軟系統「UTM」「IDR」系列產品之內建「應用程式管制」功能作IM管制。此功能採用獨有的「應用程式特徵碼」阻擋機制，針對目前一些主流的IM或Web IM所特別設計，不論這些應用程式的 Port 號再怎麼改變、版本再如何異動，只要符合IM「應用程式特徵碼」的封包一律皆阻擋下來。並且新軟UTM「應用程式特徵碼」提供永久免費線上更新，讓應用程式特徵碼保持最新狀態。另外，給予開放使用即時通訊軟體的員工，新軟UTM提供了詳細的即時通訊訊息記錄，藉此防止員工洩漏公司資料。

3. 網站管制：
若針對FaceBook、網路銀行…等網站，容易成為偽裝平台，須作為有效管制。
新軟「UTM」、「IDR」系列皆提供「網站管制」機制。公司網管人員利用「網站白、黑名單」功能，針對特定網站做開放或限制進入的制訂，同時亦可對FTP或HTTP上傳檔案之副檔名做阻擋，以免造成員工洩漏公司重要資料；且「UTM」內建的「網站類別資料庫」(此為付費功能，內含65型網站分類包括：釣魚&詐騙網站、社交網站…等等)來判別目前使用者所欲瀏覽的網站是否為「釣魚網站」且將釣魚網站自動屏蔽掉，讓使用者無法順利連結，藉此告知使用者所瀏覽的網頁為釣魚網站；而且雲端的「網站類別資料庫」保持在最新狀態。所以網管人員依公司網路政策管制員工所不能瀏覽之網站類別(社群網站、非官Web IM網站…等)，及員工不慎開啟惡意連結或附件檔案並加以阻擋。

4. 入侵偵測防禦(Intrusion Detection Prevention)：
如上述之「應用程式管制」和「網站管制」二項功能，搭配新軟UTM「入侵偵測防禦」機制，增強防禦社交工程攻擊。由於駭客藉由即時通訊登入/傳檔、電子郵件及網頁等攻擊方式，竊取公司重要資料。網管人員利用可針對公司網路實際需求，自訂所要的特徵加以阻擋或通行；並且內建的「IDP特徵資料庫」會每兩小時自動上線檢查是否有新的特徵擋下載，以維持資料庫在最新的狀態。另外，網管人員藉由「異常偵測」設定，可針對各種網路攻擊模式防禦；當網路連線符合攻擊模式時，新軟UTM會將它視為網路攻擊，並依管理人員所訂定的處理方式處理該連線。

隨著資訊科技日新月異，社交工程手法也不斷翻新。因此企業除了投資各種網路防護的軟硬體外，須建立正確防範社交工程的觀念(包括員工教育訓練與平常的宣導)，且企業應擬定內部資安政策，即使有違法員工也會受到該有的處置。儘管不斷研發出新技術加強資訊防護，但整個資訊系統環節中，最脆弱的部分仍然是「電腦使用者」，因為只要有「人」，就會有弱點。所以電腦使用者須有正確資安觀念與良好的電腦使用習慣，也隨時具備危機意識及警覺心，才能減少社交工程攻擊傷害。

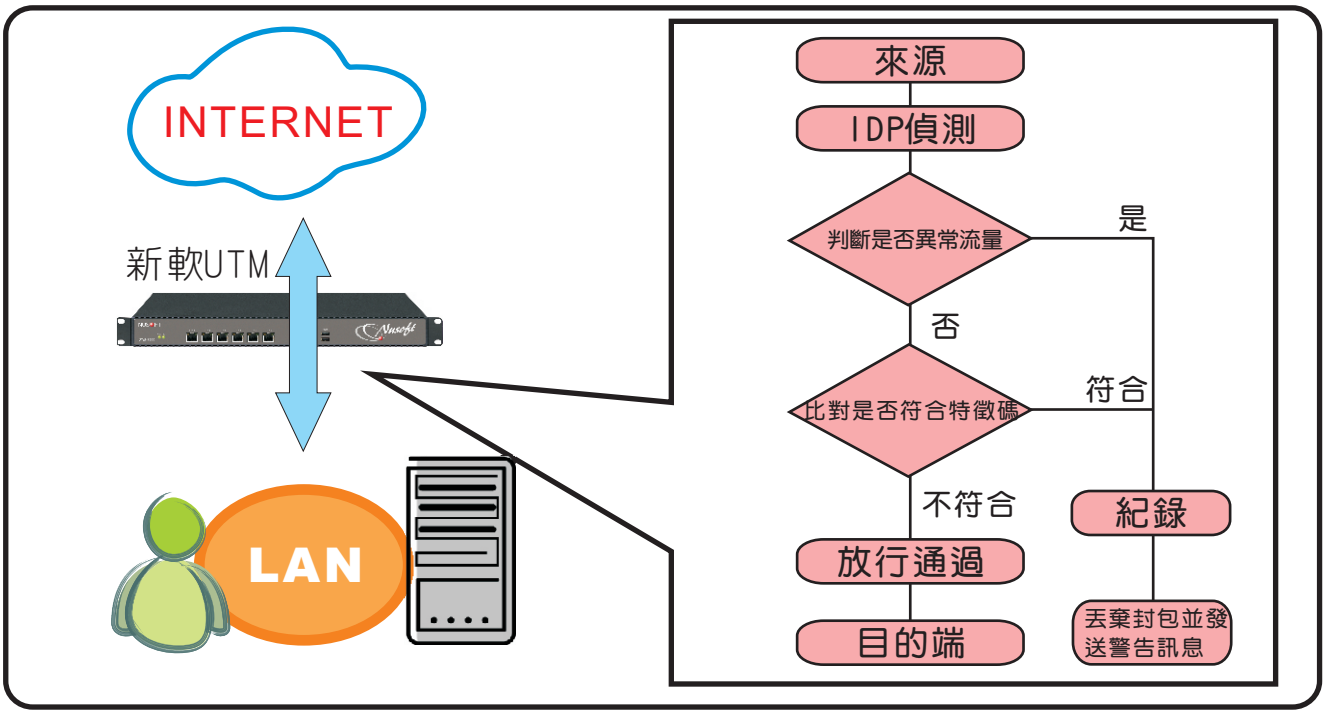
文 余光明 kongmeng@nusoft.com.tw

市場行銷報導 - 新軟UTM幫企業做好防護措施，不怕駭客入侵

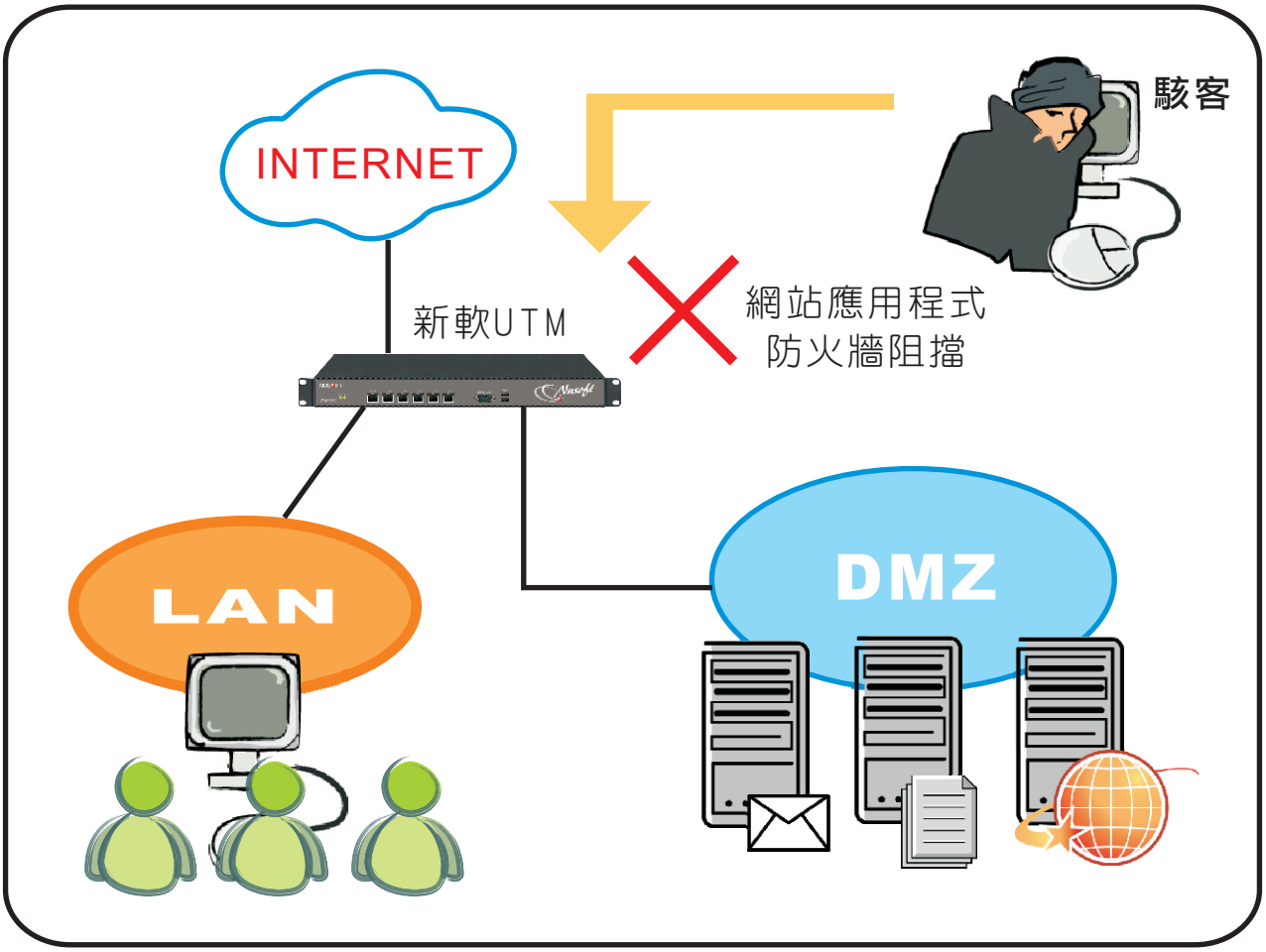
網路生活的普及化，卻也潛藏著許多陷阱與危機，網路上到處充斥著駭客的攻擊，不時有駭客入侵企業網路中盜取機密資料造成企業損失的負面新聞報導，如Sony旗下遊戲平台PlayStation Network在近期數日遭駭客入侵、被竊取1億筆用戶的個人資料，甚至連資安大神HBGary Federal也踢到鐵板，該網站遭駭客入侵，被竊取主管電子郵件約6萬封，而且1TB以上的備份資料被銷毀，這些受害案例層出不窮，如何防止駭客入侵已成為資安重要的課題。

駭客入侵企業網路，通常利用系統的應用程式漏洞，再以資料隱碼攻擊(SQL Injection)或跨網站腳本攻擊(Cross-Site Scripting)等攻擊方式入侵系統植入木馬程式，以便駭客自由進出該系統竊取檔案資料，甚至駭客利用殭屍網路(Botnet)中的受害電腦對特定目標發動大規模的分散式阻斷服務(DDoS)或阻斷服務(DoS)等其他攻擊手法，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。

因此，新軟系統推薦UTM作為企業網路與網際網路間的大門守衛，新軟UTM內建「入侵偵測防禦系統」(Intrusion Detection and Prevention；IDP)，能依照各種網路服務的漏洞做防護，無論駭客想透過系統的應用程式漏洞入侵企業網路，還是利用殭屍網路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防火牆的功能可在預設情況下拒絕所有對外的服務，只要符合已建立的規則，封包就能通過防火牆進入內部網域；並且透過NAT位址轉址的功能讓內部電腦不易成為駭客攻擊的目標，在新軟UTM層層的保護之下，駭客想入侵企業網路是難上加難。



此外新軟UTM還擁有「網頁應用程式防火牆」(Web Applicaltion Firewall；WAF)功能，加強對企業內部的網站安全與防護，而且有別於其他「軟體式」的網站安全佈署模式，新軟UTM所內建的「網頁應用程式防火牆」完全不需要再另外安裝內部網站主機上，也沒有煩雜的設定程序，讓管理人員只需針對欲使用的特徵碼做簡單的勾選動作，即可讓企業網站享有專業級的防護能力。



為因應多變的網路攻擊環境，新軟UTM除了會不斷自動線上更新「入侵偵測防禦特徵碼」和「網頁應用程式特徵碼」之外，管理人員亦可針對企業網路實際需求，自訂所要的特徵碼，讓新軟UTM的IDP和WAF防護更具彈性。另外，新軟UTM之「異常流量IP」功能，當內部電腦中毒時，導致區域內網中產生大量且不明的對外連線，新軟UTM偵測出異常流量並將相關資訊記錄於設備中，且即時阻斷發生問題的使用者，以確保網路安全。在發生異常流量的同時，新軟UTM根據管理人員所設定的警訊通知形式發出警訊(如：E-Mail、SNMP Trap、NetBIOS)，通知該使用者及管理人員協助處理，使資安事件的發生達到即時且有效的控管，以避免異常流量對於企業網路造成危害。

文 余光明 kongmeng@nusoft.com.tw