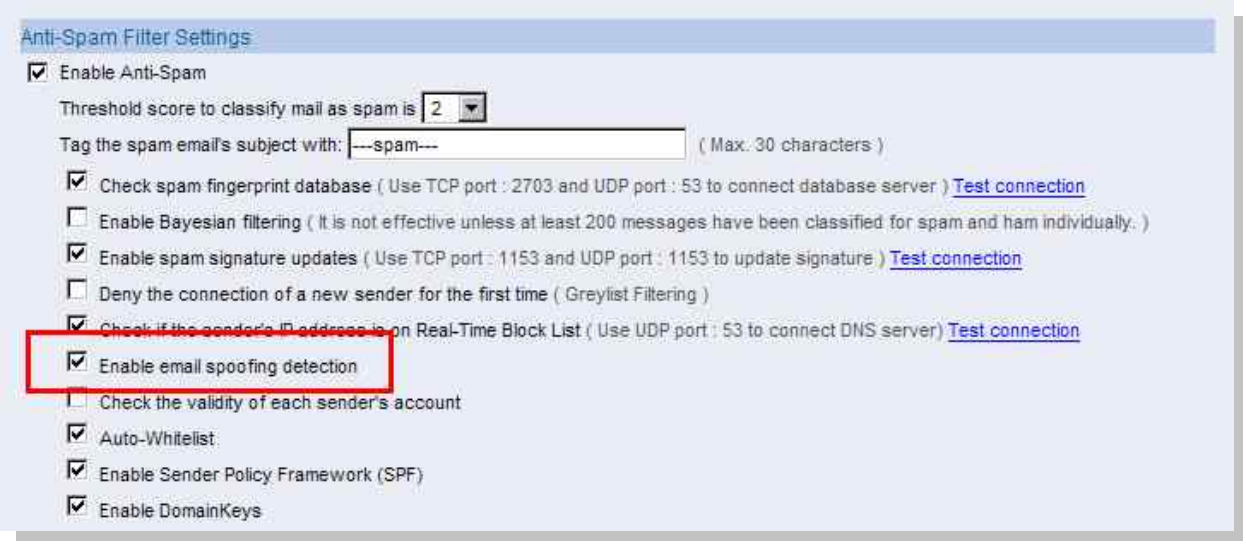
新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2009/10/5- 2009/10/18 第102期

郵件伺服器 / ML 系列報導

技術淺談與應用 - 新增『寄件者偽裝網域偵測』功能

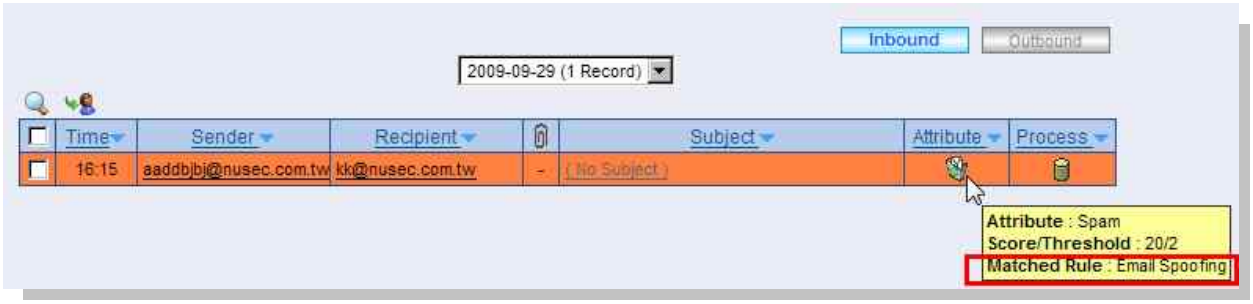
成堆的垃圾信件不只成了辦公室有害物，也浪費了公司內部頻寬與設備儲存空間，甚至信件還與病毒同時伺機入侵企業；如此擾人的問題不但沒隨著科技的進步而減少，相反的還更加的變本加厲，也正因為如此，公司紛紛的導入相關的防護設備來將傷害降至最低。但垃圾郵件的散播方式也同樣的不斷在改變，舊有的防護機制並無法完全的阻擋不斷換新花招的垃圾郵件攻勢，讓少數的垃圾郵件開始流入公司內部。對於如此讓人頭痛的問題，身為公司的網路安全管理人員又該如何去解決呢？

垃圾信件的寄送方式為了能躲避種種的信件檢查防護機制，而其中的一種則是進而使用修改寄件者網域的方法，來欺騙大多數的郵件伺服器，讓該郵件伺服器誤認為該封信件為是內部網域或是外部所信任之網域所寄送之信件，因而放行通過。新軟系統，針對不斷改變的垃圾郵件攻勢，同樣也不斷在更新新的阻擋方式，除了舊有的白名單、黑名單及多數的信件過濾機制外，近期於『郵件伺服器 - ML』中的“郵件過濾”機制下，為防止偽裝網域之垃圾郵件寄件方式，又新增了一項『寄件者偽裝網域偵測』功能來協助公司達到更上一層的垃圾郵件保護。

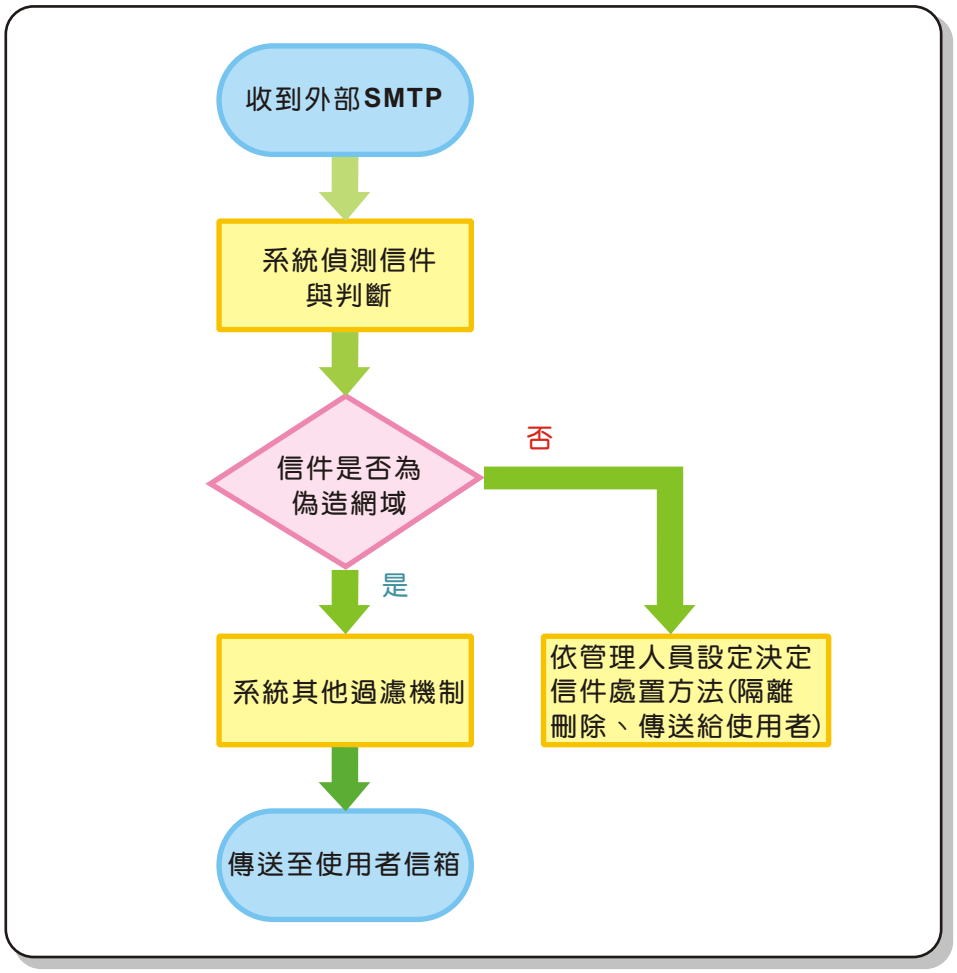


新增『寄件者偽裝網域偵測』功能

而此功能所在位置為系統中『Mail Security > Anti-Spam > Settings』下，管理人員只需輕鬆的在 UI 中將該功能打勾即可啟動，完全不需再另外鍵入煩雜的設定程序，該功能啟動後能夠在對方信件進入公司前，立即去偵測該封信件是否為所屬網域寄出之信件，如此一來針對想利用偽裝網域來送發垃圾信件的寄件方式，則可有效的達到阻檔的效果，防止垃圾郵件篡改成與公司內部相同網域、或其他外部正當郵件網域來欺騙郵件伺服器以達到成功將垃圾信件送至收件者信箱的情況發生。



有效偵測及阻擋篡改網域的垃圾郵件

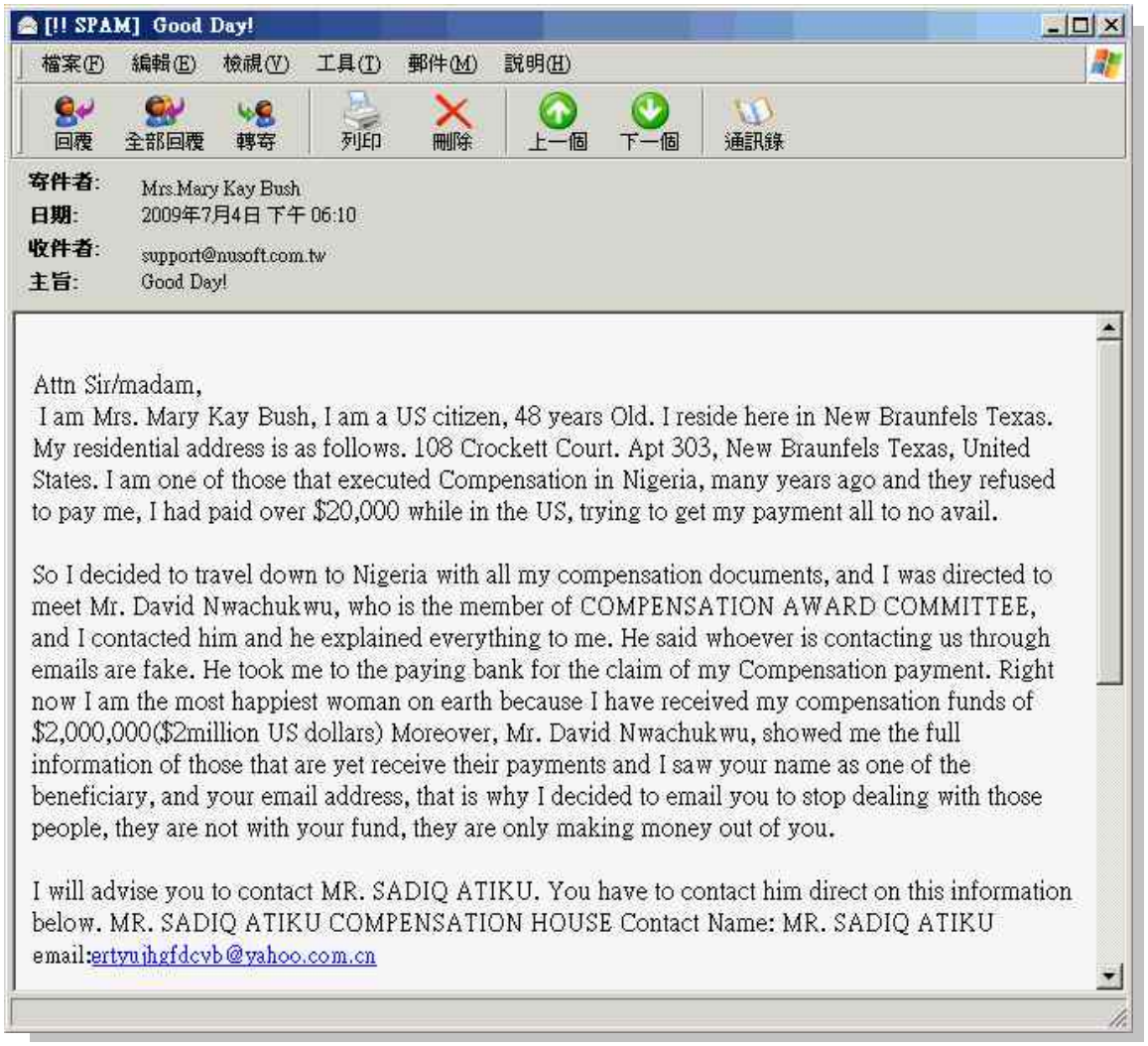


新功能簡易流程圖

文 陳殿鴻 kim@nusoft.com.tw

市場行銷報導 - 垃圾郵件流行「裝熟」釣肥羊，新軟郵件伺服器給您更嚴謹的過濾機制

近期以來網路上出現許多垃圾郵件，常常以『Hey』、『Hi』、『Hello』、『Good Day』等一般且輕鬆性的口吻為標題，讓受害者在第一時間誤以為此封信件為熟人或朋友所寄送來之信件，甚至是假冒郵件傳遞失敗通知信、訂貨通知信等，藉以企圖躲過層層的垃圾郵件過濾功能，蒙騙受害者上當開啟信件，點選信件內的超連結下載不法檔案或登錄其釣魚網站。



近期網路上有許多以輕鬆語氣為標題的垃圾郵件，四處流竄引誘受害者上當。

新軟系統一向秉持著「不斷進步」的精神，嚴格地自我要求；針對目前網路上不斷翻新手法的垃圾郵件問題提出相對解決之道，力求以「兵來將擋、水來土淹」的模式來全面防止垃圾郵件的攻擊。因此目前除了原本在新軟郵件伺服器（ML1000G、ML2500）中的七大垃圾郵件過濾機制以外，另外新增了三道垃圾郵件過濾機制，藉以讓垃圾郵件過濾能力能更為強大、完整。三道新增垃圾郵件過濾機制如下：

寄件者偽裝網域偵測

由新軟郵件伺服器發送檢查封包，檢查在 HELO / EHLO SMTP 命令中所提交的寄件者地址，並與其將信件中所填入的寄件者地址之網域名稱進行符合性比對，若完全符合便屬於正常信件；若不符合便直接判斷為垃圾郵件，並進行垃圾郵件過濾阻擋。

檢查寄件者帳號是否存在

一般垃圾郵件的寄件者帳號皆為偽造帳號，利用由新軟郵件伺服器所發出檢測封包到寄件者帳號所在的郵件伺服器進行查詢，利用所回覆的封包可得知此封信的寄件者帳號是否存在；若否，則以判為垃圾郵件處理之。

自動化白名單

當寄件者寄出一封信時，自動化白名單機制會計算這封信的評等，分數越高，代表該信的內容越符合垃圾郵件的定義。其原理是將信件來源與寄件者帳號依係數設定做權重分析，經常信件往返者便會將自動加入至白名單。

網路上的各類垃圾郵件威脅興起，不斷翻新之手法是所有垃圾郵件共同的特徵。因此若只靠少數幾種過濾機制來防範是不夠的；而新軟系統便是以自家研發團隊為強力後盾，在多變的網路潮流裡不斷尋找過濾垃圾郵件的解決之道，因而讓新軟郵件伺服器能以強大的郵件過濾能力來滿足眾多用戶防範垃圾信件攻擊的需求。

文 黃政銘 ming@nusoft.com.tw