新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2010/1/11-2010/1/24 第109期

多功能 UTM / MS 系列報導

技術淺談與應用 - 異常流量的警告通知及設定所需注意之事項

網路安全一直以來都是各公司、企業首要的條件之一，隨著網路惡意攻擊事件不斷發生，公司內部也因此紛紛導入相關資訊安全設備來做為前線防護牆，藉此以減少及降低公司內部遭受波及的程度與機率。

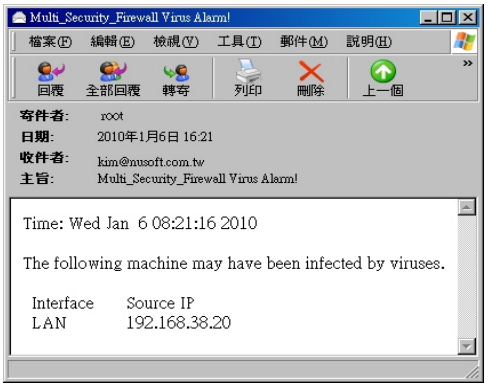
但長期以來，公司的安全防護措施，通常都有著相同情況出現，對於外來惡意攻擊有著相當的防禦能力，但卻往往無法有效阻止與防範內部機器因中毒或刻意所發出的惡意攻擊異常流量封包。以至於當情況發生時，往往無法即時將惡意攻擊杜絕，直到管理人員發現後，還必需得一台一台費時的去找尋，等找到問題源頭時早已經造成某部份嚴重損失，甚至是網路癱瘓讓公司部份作業停擺，因而使公司喪失許多商機。

新軟系統多功能 UTM - MS 所內建的『異常流量 IP』功能，就能輕鬆為公司解決如此問題。只要當 MS 收到公司內部機器所發出的大量不正常封包時，該功能會立即阻擋此類封包的傳送，即時阻斷發生問題的使用者，以避免不正常封包流量將企業網路癱瘓，並且系統會立即依照管理人員設定之通知方式來通知該使用者及管理人員，讓管理人員能在最短時間內去處理及解決相關問題，以確保公司內部網路的安全。

而『異常流量 IP』警告通知可依管理人員自行設定的方式分成“電子郵件警訊通知”、“SNMP Trap 警訊通知”、“NetBIOS 警訊通知”三種，並且在發現異常流量後會於使用者的電腦第一次透過瀏覽器上網時，於其瀏覽器上顯示警告之畫面，告知其該使用者電腦已中毒。以下將分別說明上述幾種警告方式及管理人員所需注意的事項。

一. 電子郵件警訊通知

管理人員若勾選啟動該項功能後，當系統偵測到內部有異常流量時，則會立即發送信件至管理人員的電子郵件信箱，通知管理人員相關訊息(如下圖)。

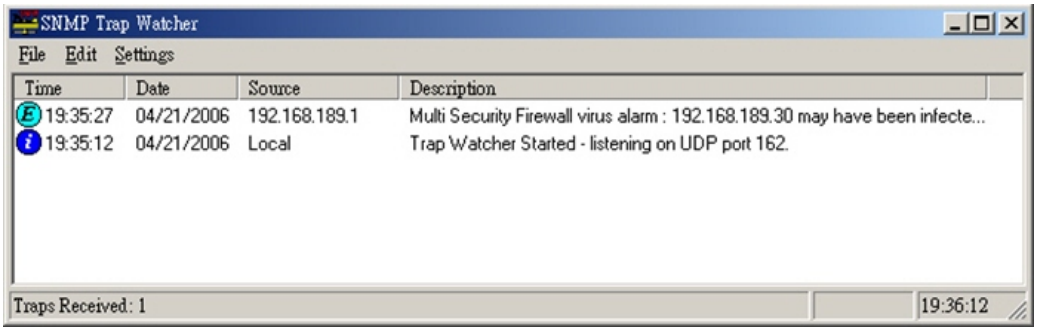


電子郵件警訊通知畫面及內容

管理人員若需開啟該項通知功能時要注意到的則是，還必須先於『系統管理 > 組態 > 系統設定』下設定管理人員郵件位置，該項通知功能才能正常啟動。也建議管理人員別單單只是開啟該項警訊通知功能而已，最好還是搭配其他通知功能，以防因一時沒留意信件而錯失處理的時間。

二. SNMP Trap 警訊通知

管理人員若勾選啟動該項功能後，當系統偵測到內部有異常流量時，MS 會將警告訊息即時顯示於管理端電腦所安裝之 SNMP Trap 用戶端軟體上(如下圖)。

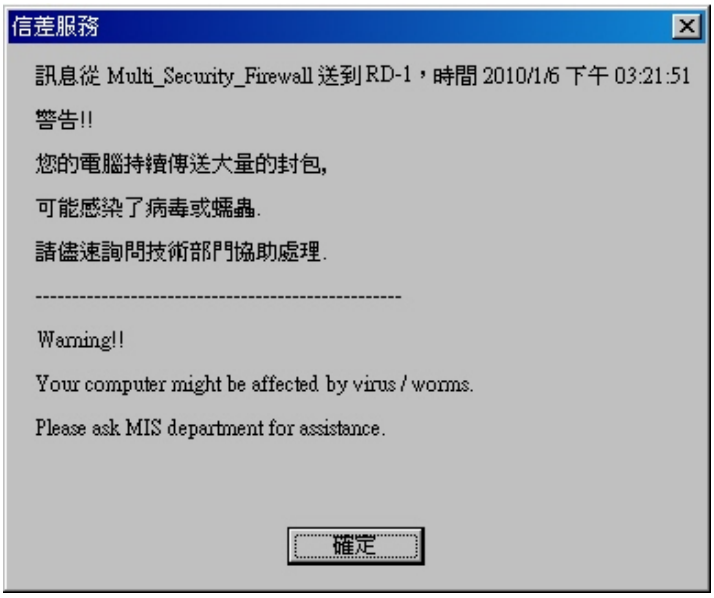


SNMP Trap 用戶端軟體所接收到之病毒警示

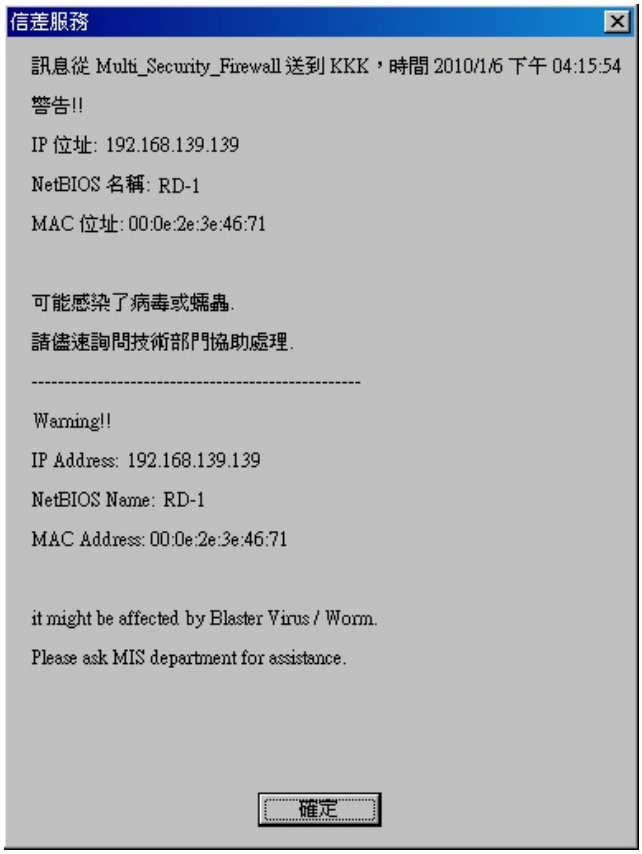
若需開啟該項通知功能時要注意到的則是，還必須先於『系統管理 > 組態 > SNMP』下做設定，該項通知功能才能正常啟動。然而較為不便之處則是還必須安裝 SNMP Trap 相關軟件才能正常接收通知，但對於已有使用該項軟體的使用者而言，該項通知功能也肯定是非常有效的通知管道之一。

三. NetBIOS 警訊通知

該項功能啟用後，當系統偵測到內部有異常流量時，會立即發出警訊給中毒及管理員的 PC(如下圖)。

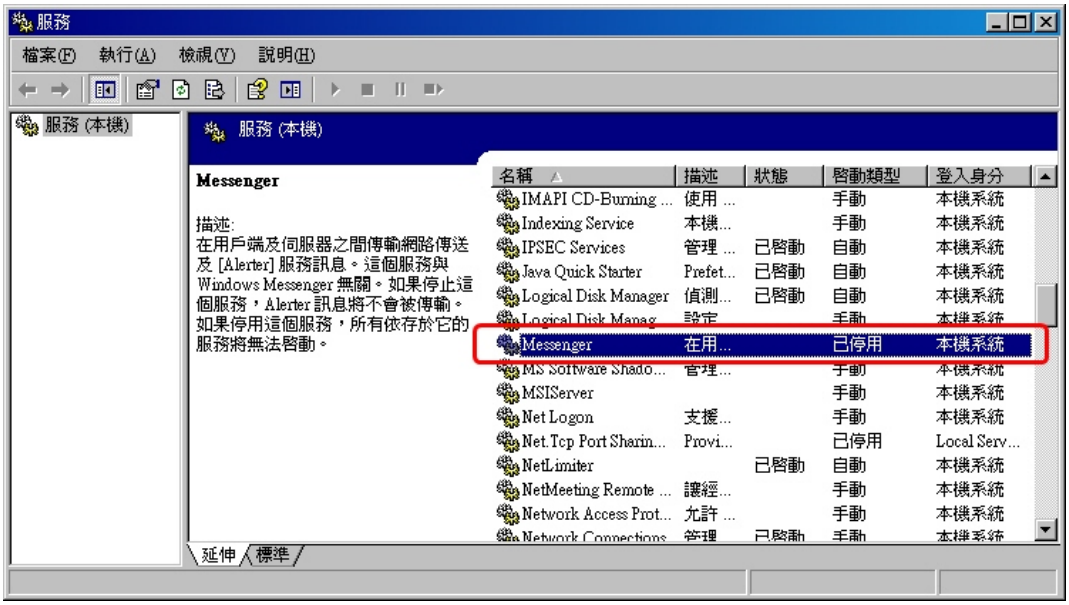


中毒使用者 PC 所接收到的 NetBIOS 警訊通知

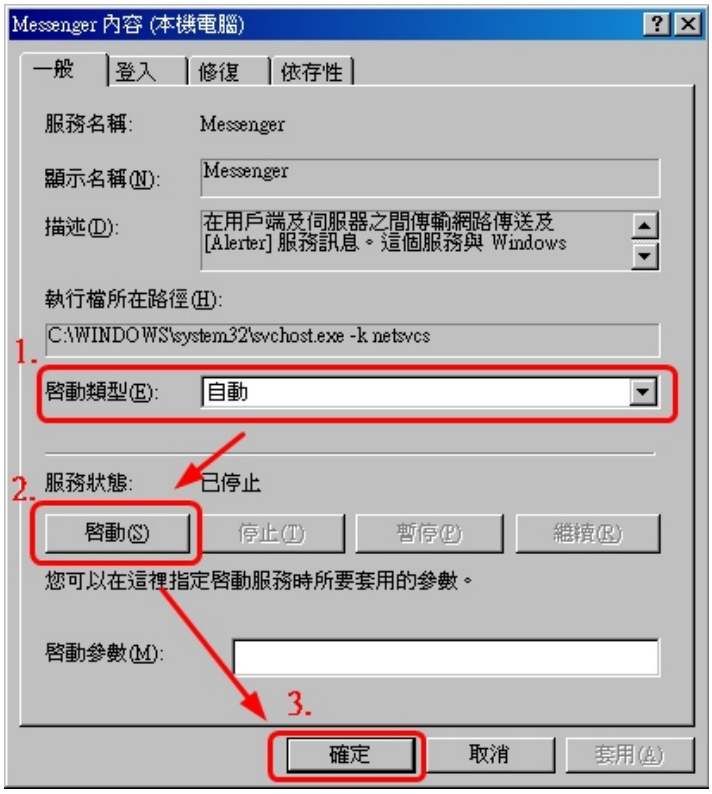


管理員 PC 所接收到的 NetBIOS 警訊通知

此項通知功能是最不容易被忽略的，因為系統會立即於 PC 上跳出通知訊息，但還須注意到的是電腦作業系統中的 “Messenger” 是否有正常啟動，否則將無法正確接受到 “NetBIOS 警訊通知” 功能所發出的通知訊息。而管理人員可於『控制台 → 系統管理工具 → 服務』中設定啟動。



於『控制台 → 系統管理工具 → 服務』中選擇 “Messenger”



將啟動類型設定為“自動”，於服務狀態點擊“啟動”，完成後並按下“確定”

最後當內部使用者的電腦中毒且發生異常流量後，第一次透過瀏覽器上網時，MS會於其瀏覽器上顯示警告畫面，告知其使用者電腦已中毒(如下圖)。

中毒後使用者第一次使用瀏覽器出現之警告訊息

須注意到的是使用者若是不能排除本身中毒之情況，往後皆會受到 MS 限制，導致上網變慢，並且不會再有警告訊息顯示於瀏覽器。

文 陳殿鴻 kim@nusoft.com.tw

市場行銷報導 - 員工利用「無界、自由門」上網“開心”，新軟多功能 UTM 替企業嚴格把關

網際網路蓬勃發展，帶動人類生活 e 化，至今許多人生活模式都離不開網路。去年最為火紅之例子莫過於著名的社交網站 - Facebook，其以活潑之網路互動方式讓使用者趨之若鶩，其中“開心農場”便是其成功風靡群眾裡最典型的工具之一。

然而，使用者愛好玩諸如“開心農場”此類互動型網路遊戲，卻經常不分公私時間地玩；身受其害最為嚴重的企業界最為了解。在公司企業裡，重視奉行的法則莫過於「提高公司生產效力、降低公司營運成本」，但是底下企業員工若於上班時間利用公司網路偷上 Facebook 的話：

1.員工無心於自己工作本務上，反而沉迷於 Facebook 裡，因而降低生產效率。
2.員工上 Facebook 時所讀取之 Flash 網頁物件會消耗大量的網路頻寬，間接造成公司其他同仁的使用網路頻寬遭到擠壓，進而延誤掌握商機之第一時間。

因此現今很多企業為了「防範員工混水摸魚以及提高生產效率」的問題，而花費添購相關網路行為管理設備。可是“道高一尺、魔高一丈”，雖然起初此類產品能對企業網路底下的用戶產生簡單之管制效果；不過現在網路科技發達，卻已有人研發出能突破網路行為管理功能的軟體，如：無界(Ultra-Surf)、自由門(FreeGate)、熱點盾牌(Hotspot Shield)、Tor…等等。此類軟體俗稱“穿牆軟體”，其原理是以特殊加密機制來包裝所有進出之網路封包，讓一般網路行為管理設備誤判為正常封包，導致間接在網路管理設備及前端防火牆內形成一條通道進出自如，讓不肖員工可以在一般網路行為管理設備無法管制的情況下為所欲為地使用公司網路資源來上網，除此之外，也因為使用此軟體後彷彿在防火牆裡開了一條通道，因此可能造成於上網時讓網路上之病毒透過此通道滲透至內部網路裡，造成不可想像的損害。

於此，新軟系統多功能 UTM 以強大之應用程式管制機制來打擊摸魚上網的不肖員工，有別於市面上其他網路管理設備以「阻擋 Server IP、關閉通訊埠號」等毫無效率可言之管制方式；新軟系統多功能 UTM 以獨家分析方式正確過濾所有的網路封包，即使底下不肖員工欲使用“穿牆軟體”來突破管制，但是在新軟系統多功能 UTM 的獨家過濾機制下，所有的網路封包都將無所遁形，便可以完整的管制底下的不肖員工，另外新軟系統多功能 UTM 成功管制“穿牆軟體”後，將會隨之產生相關資料報表(使用 IP、使用時間、使用軟體)，因此可以透過記錄報表得知有哪些員工企圖使用“穿牆軟體”來混水摸魚。如此一來，就可以達到完善的管制效果，企業也可以達到「提供公司生產效率、降低企業營運成本」的營運目標。

	新軟多功能 UTM	一般網路行為管理設備
管制方式	以獨家分析方式正確過濾所有的網路封包，即使底下不肖員工欲使用“穿牆軟體”來突破管制，但是在新軟系統多功能 UTM 的獨家過濾機制下，都將無所遁形。	採用「阻擋 Server IP、關閉通訊埠」等治標不治本的管制方式。
管制效率	高 不管 Server IP 或通訊 Port 如何變更，單純針對進出封包進行分析過濾，藉此達到準確的判斷及管制。	低 當 Server IP 或通訊 Port 變更時，就容易發生無法管制的窘境。
目前能提供管制機制的對象軟體： VNN Client、無界瀏覽(Ultra-Surf)、Tor、Hamachi、自由門(FreeGate)、熱點盾牌(Hotspot Shield)		

文 黃政銘 ming@nusoft.com.tw