新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2009/5/18- 2009/5/31 第92期

郵件伺服器 / ML 系列報導

技術淺談與應用 - 檢查郵件伺服器為何會被當垃圾郵件發送跳板

垃圾郵件一直以來都是最令人頭疼的一件事，所帶來的不便之處相信每個人都已親身體會過，由此可知垃圾郵件所造成之影響早已是遍及到網路世界的每個角落。

垃圾郵件的來源及發送方式演變至今有很多種，為了躲避種種的垃圾郵件預防機制，以達到有效將垃圾郵件送達又不被阻擋，除了不斷改變內文的格式之外，盜用外部公司與企業所架設之正當郵件伺服器來做發送之管道(跳板伺服器)也是其中一種方式。當管理人員發現郵件伺服器裡，出現一堆不認得的郵件帳號，而這些帳號之信件發送量又是非常可觀時，八九不離十的情況就是該郵件伺服器已經遭人利用當作垃圾郵件的發送跳板。

管理人員可從下列的兩種情況，來確定郵件伺服器是否遭人當做垃圾郵件或廣告信件的發送平台來用。

情況一：於郵件伺服器中發現多數不知名的帳號使用者，同時這些帳號的信件發送量都是屬於極大量的情況。

Top-N　Spam Mails　Virus Mails　Regular Mails　1/50

No.	Account	Spam Mails	Virus Mails	Regular Mails	Total Received	Outbound Mails
1	hmr	0	0	707	707	707
2	gkp	0	0	647	647	647
3	ins	0	0	551	551	551
4	glq	0	0	487	487	487
5	hlq	0	0	457	457	457
6	kpty	0	0	414	414	414
7	mrwb	0	0	410	410	410
8	kpuz	0	0	391	391	391
9	osxc	0	0	389	389	389
10	fkp	0	0	376	376	376

Time: 2009/05/03(Sun) ~ 2009/05/07(Thu)　Total:33439 Mails　Average:11146.33 Mails/Day

1/50

郵件伺服器 UI 上查閱出有大量的郵件發送，及未曾見過的帳號出現

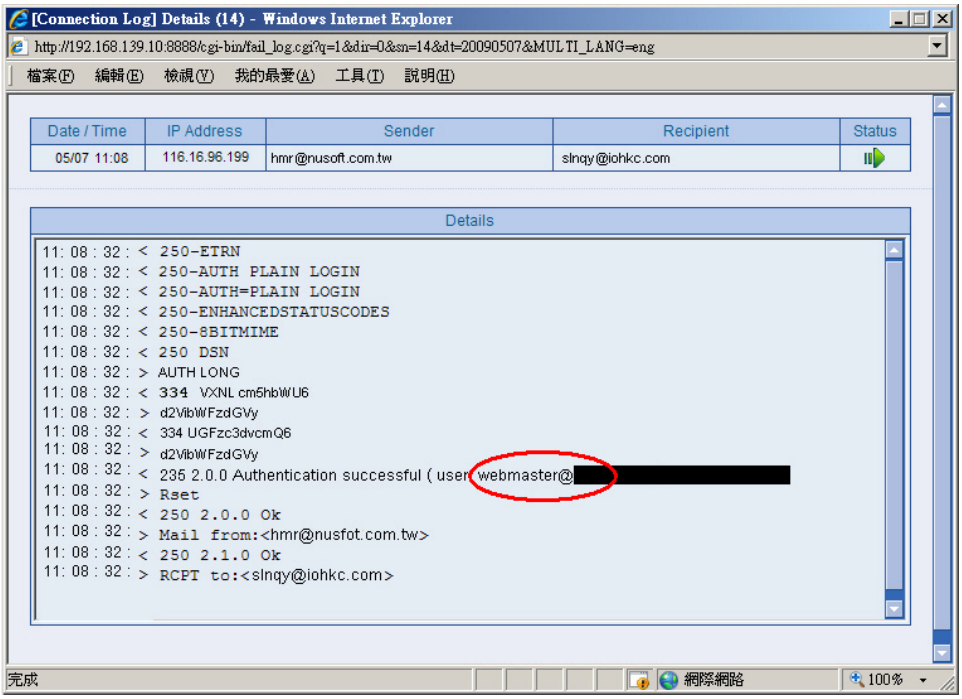
情況二：於郵件伺服器中查閱出，正常的 Outbound 記錄裡，出現不知名的帳號使用者寄出大量的垃圾信件記錄。

Time	Sender	Recipient		Subject	Attribute	Process
11:11	hrm@nusoft.com.tw	julie-jung@umail.hinet....	-	--- 缺錢不找代辦,有車萬事OK		
11:10	kpty@nusoft.com.tw	crqfl@pchome.com.tw	-	--- 4月24-25日登陆深圳		
11:10	mrwb@nusoft.com.tw	stone@bhes.tnc.edu.tw	-	--- 林志玲 露點`走秀		
11:10	gkp@nusoft.com.tw	daemon@st1es.tnc.ed...	-	--- 明星走光乳暈大集合,一...		
11:10	osxc@nusoft.com.tw	vicky-mark@umail.hin...	-	--- 自拍飯店外全裸女子		
11:10	mrwb@nusoft.com.tw	ivan_ying@msn.com	-	--- [redacted]◆暗戀我叫我欣賞..		

不知名的帳號，合法的從伺服器來發送垃圾郵件

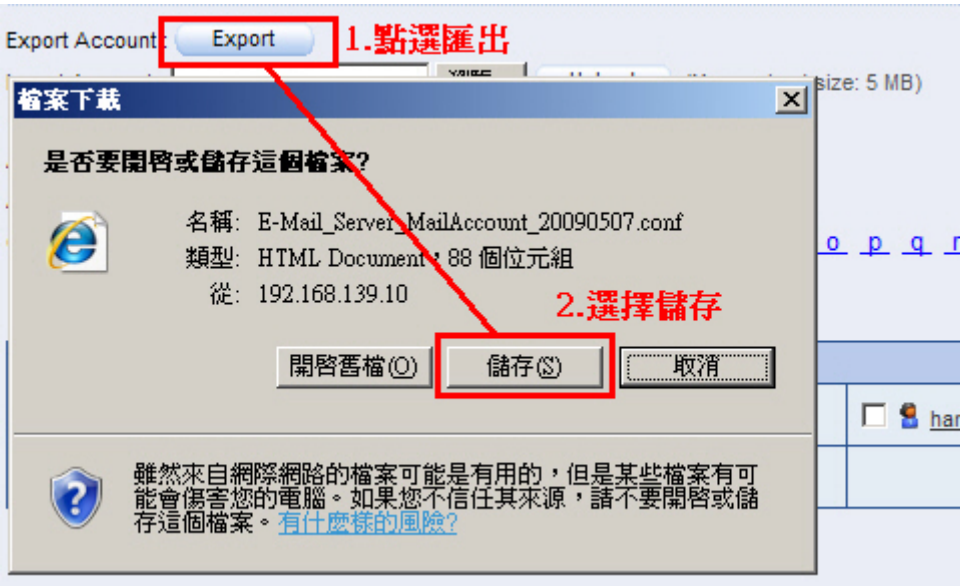
從上述的兩種情況可清楚的瞭解到，該些帳號是藉由此郵件伺服器來發送垃圾郵件，但想必另管理人員不解的則是，明明伺服器有設定 SMTP 認證，必須要透過所認可的帳號使用者才能正常的寄送郵件，為何這些盜用者能這麼輕易的就利用該郵件伺服器來做垃圾信件的發送平台呢？

首先管理人員可利用郵件伺服器的連線追蹤功能來進行查閱，到底入侵的人是利用何組 SMTP 認證帳號來進行郵件的發送動作。進入 “Connection Track → Inbound SMTP” 下搜尋那些發送大量垃圾信件且未曾見過的帳號，並且進入查看詳細的連線訊息，利用此方式來找出入侵者所使用的認證帳號究竟為何。



可清楚的瞭解到所使用的 SMTP 認證帳號為何

當找到入侵者是利用何組 SMTP 帳號來發送信件時，接下來管理人員可於 “Mail Management → Account Management → Individual” 下將所有使用者帳號匯出檢查其原因。



將帳號匯出查閱

管理人員可藉由此方式來檢查帳號是否出了什麼問題，究竟為何會被輕易的就遭盜用。而通常管理人員會發現到原因出現在該帳號和密碼皆設為相同或是設置過於簡單，使人易猜。因此讓入侵者則可輕而易舉將其密碼破解後，肆無忌憚的盜用此帳號來發送垃圾郵件。

被盜用者之帳號密皆設相同

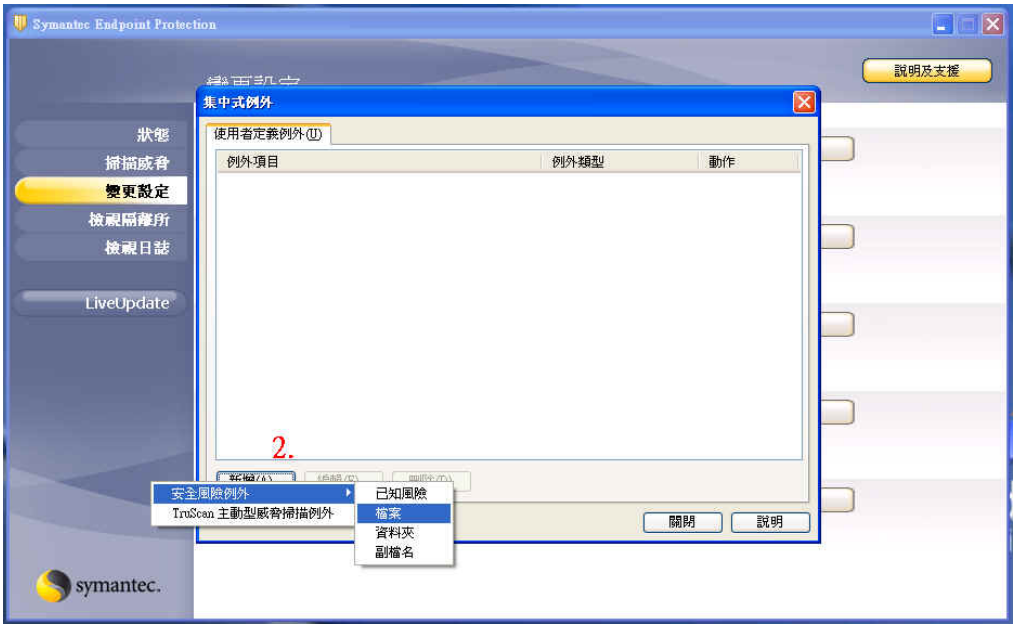
由上圖可發現除了被盜用者的帳號密碼皆設為相同外，內部還有其他使用者也是如此，除此之外更有人使用過於容易猜測的密碼。根據調查，對被盜用的密碼進行分析後發現，過於簡單行事是造成帳號被盜用的最主要原因。新軟系統提醒您，不論是何種用途，千萬別將帳號及密碼設成相同或過於簡單，以防遭到破解而進一步盜用。

附錄：

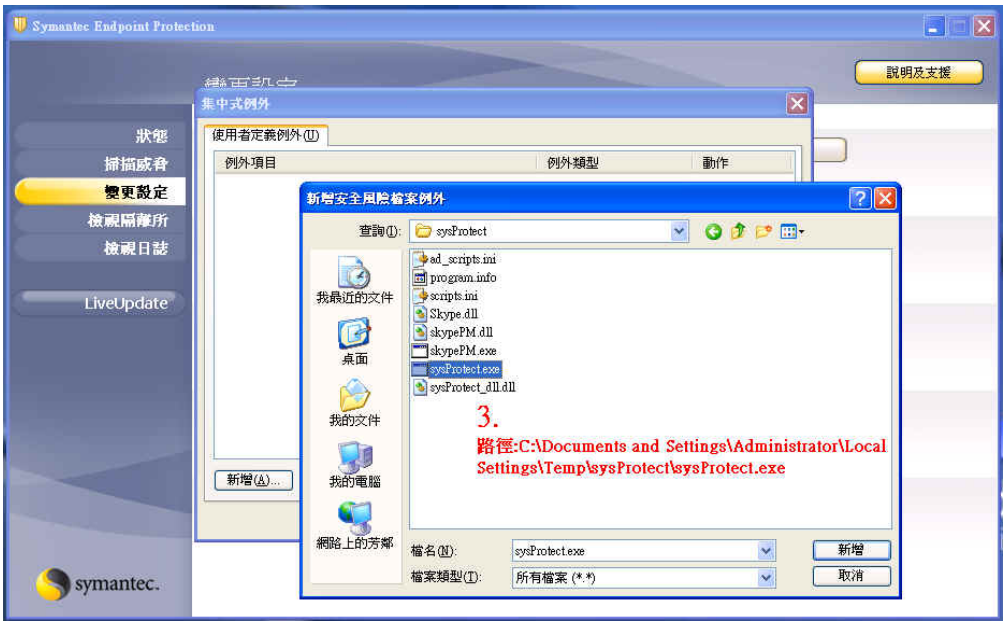
針對 IR-Plugin 安裝後，在 Symantec 防毒軟體下該如何避免被誤偵測為問題程式？

1. 於變更設定中選『取集中式例外』的『架構設定』選項

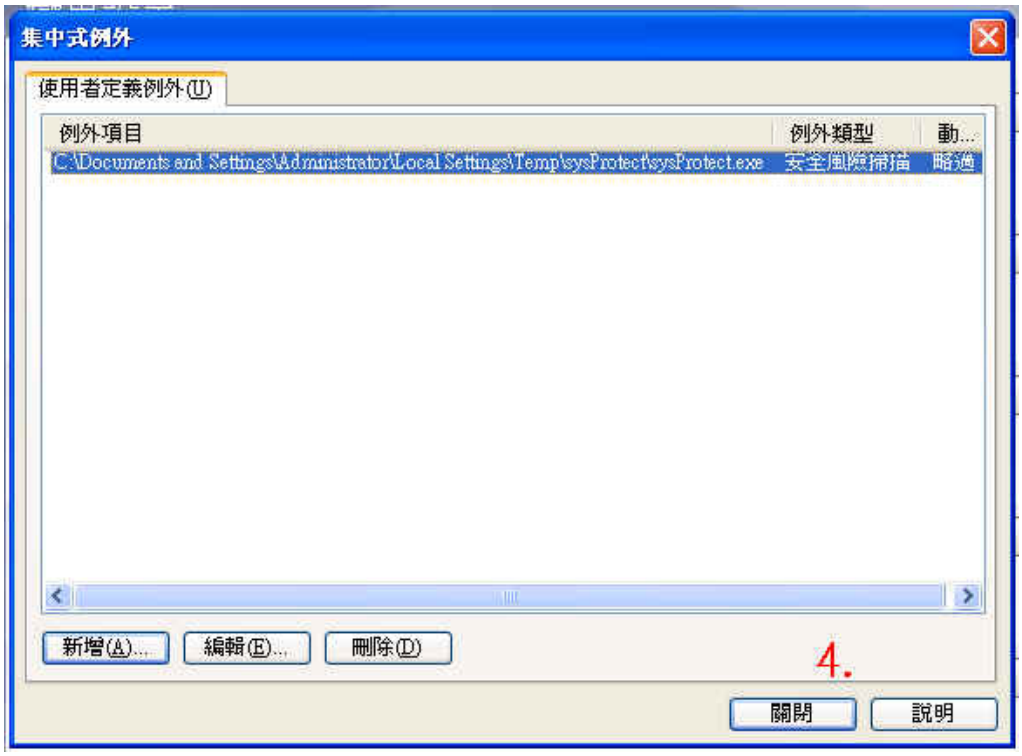
2. 新增『安全風險例外』→『檔案』



3. 並將其“sysProtect. exe”程式新增



4. 確定後點選關閉離開



文 陳殿鴻 kim@nusoft.com.tw

市場行銷報導 - 利用「AD server帳號整合」功能，輕鬆管理郵件伺服器帳號

隨著時代變遷及科技進步，在現今 e 化的社會中幾乎人人都會使用電腦，而隨之普及的便是人與人之間互相溝通之工具—電子郵件。如今電子郵件已是人與人互相聯絡的重要管道，也是現在企業與企業之間生意上相互溝通的重要橋樑，更是商業往來中不可或缺的重要武器。

然而，現今的企業為了能使公司營運分工更有效率，在公司內通常會配給每個員工一人一個電子郵件帳號。藉此，上司可以透過電子郵件將公司的營運方向、業績目標甚至其他交辦事宜，更完整清楚地交辦給底下的員工，員工就可以在第一時間清楚了解到「此刻工作目標為何？」、「該如何去做？」、「做到何種程度？」…等等一些業務上的工作指示。

但是有時候可能因應公司營運政策之關係會產生一些人事上的異動，因此會有人需要配給新郵件帳號、有人需要撤銷帳號之狀況發生。雖然目前很多公司企業內部都有架設統一集中管理帳號密碼之 LDAP 伺服器，但是由於目前一般市售的郵件伺服器並無法與 LDAP 伺服器做帳號整合，因而讓 LDAP 伺服器無用武之地。所以假使現在公司臨時需要新增或變更大量之郵件帳號的話，那就得由網管人員自行至郵件伺服器上以傳統的手動鍵入方式逐一將帳號建立或刪除，這樣的鍵入方式一來既費工又費時、二來又有可能鍵入錯誤之可能性發生，因此該如何以最有效率之做法來完成公司內所有的郵件帳號變動呢？

例如：公司網路內部裡有架設統一集中管理帳號之 LDAP 伺服器，假使今天公司有部門擴編需要新增數十個新郵件帳號或者有員工離職需要將其郵件帳號刪除，此時該如何以最輕鬆簡單之方式完成所有的帳號變動呢？

為了因應目前科技講求「快速」、「輕鬆」之理念，新軟系統也將這樣的理念實現於郵件伺服器- ML 系列產品上，設計出「AD server 帳號整合」之功能，藉此讓網管人員能以最輕鬆容易之方法來完成所有郵件帳號的新增及變動。對於類似這樣的帳號變動需求，由於郵件伺服器 - ML 系列產品有「AD server 帳號整合」功能的關係，利用其帳號學習整合功能之特性和 LDAP 伺服器做即時帳號整合，讓郵件伺服器自行去向公司內部統一管理帳號密碼之 LDAP 伺服器學習其所有之帳號密碼（如圖 1）。如此一來，只要網管人員在 LDAP 伺服器上有做帳號之任何變動的話，那麼在 ML 系列郵件伺服器上也會自動新增或變更帳號（如圖 2）達到帳號即時整合。甚至公司內還有架設新軟系統之 IR 或 MS 系列產品，一樣可以使用「AD server 帳號整合」之功能與 LDAP 伺服器上之帳號密碼來做相互對映，達到即時帳號整合。

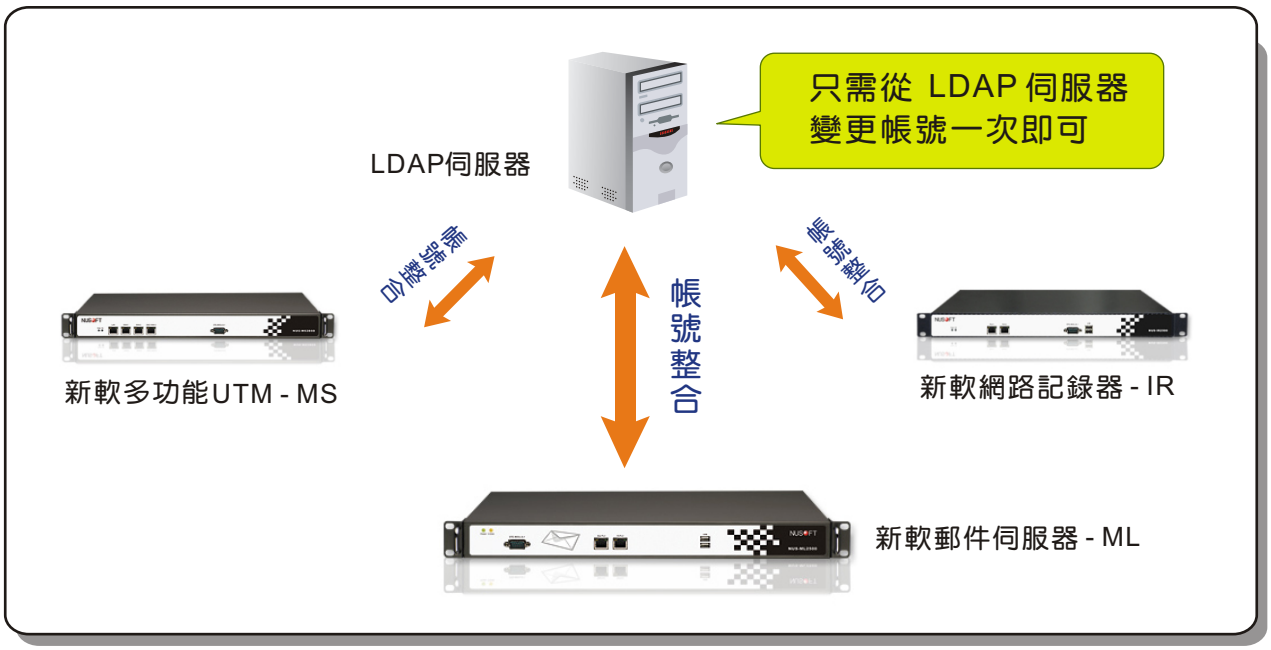


圖 1 只需在 LDAP 伺服器上輕鬆變更帳號即可，底下之新軟郵件伺服器會自動整合帳號。

圖 2 使用「AD server 帳號整合」功能，即使 LDAP 伺服器有帳號新增，ML郵件伺服器也會隨之新增。

	新軟郵件伺服器(ML 系列)	一般市售網郵件伺服器
新增/變更帳號方式	使用「AD server帳號整合」功能，由系統自行與 LDAP 伺服器上之資料做即時帳號整合。	需由網管人員以手動方式至郵件伺服器上逐一新增或變更帳號。
新增/變更帳號方式效率	優 若需新增或變更帳號，只需在 LDAP 伺服器上修改即可，ML 郵件伺服器會即時帳號整合。若公司內還架設有新軟系統 IR 或 MS 系列產品，一樣會同時有即時帳號整合之效果。	差 只能手動鍵入方式，既費工又費時，虛耗人力於該業務上，加上會有鍵入錯誤的可能性發生。

表 新軟郵件伺服器「AD server 帳號整合」與一般市售郵件伺服器帳號結合方式差異。

文 黃政銘 ming@nusoft.com.tw