新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2009/5/18- 2009/5/31 第92期

邮件服务器 / ML系列报导

技术浅谈与应用 - 检查邮件服务器为何会被当垃圾邮件发送跳板

垃圾邮件一直以来都是最令人头疼的一件事，所带来的不便之处相信每个人都已亲身体会过，由此可知垃圾邮件所造成之影响早已是遍及到网络世界的每个角落。

垃圾邮件的来源及发送方式演变至今有很多种，为了躲避种种的垃圾邮件预防机制，以达到有效将垃圾邮件送达又不被阻挡，除了不断改变内文的格式之外，盗用外部公司与企业所架设之正当邮件服务器来做发送之管道(跳板服务器)也只是其中一种方式。当管理人员发现邮件服务器里，出现一堆不认得的邮件账号，而这些账号之信件发送量又是非常可观时，八九不离十的情况就是该邮件服务器已经遭人利用当作垃圾邮件的发送跳板。

管理人员可从下列的两种情况，来确定邮件服务器是否遭人当做垃圾邮件或广告信件的发送平台来用。

情况一：于邮件服务器中发现多数不知名的账号使用者，同时这些账号的信件发送量都是属于极大量的情况。

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

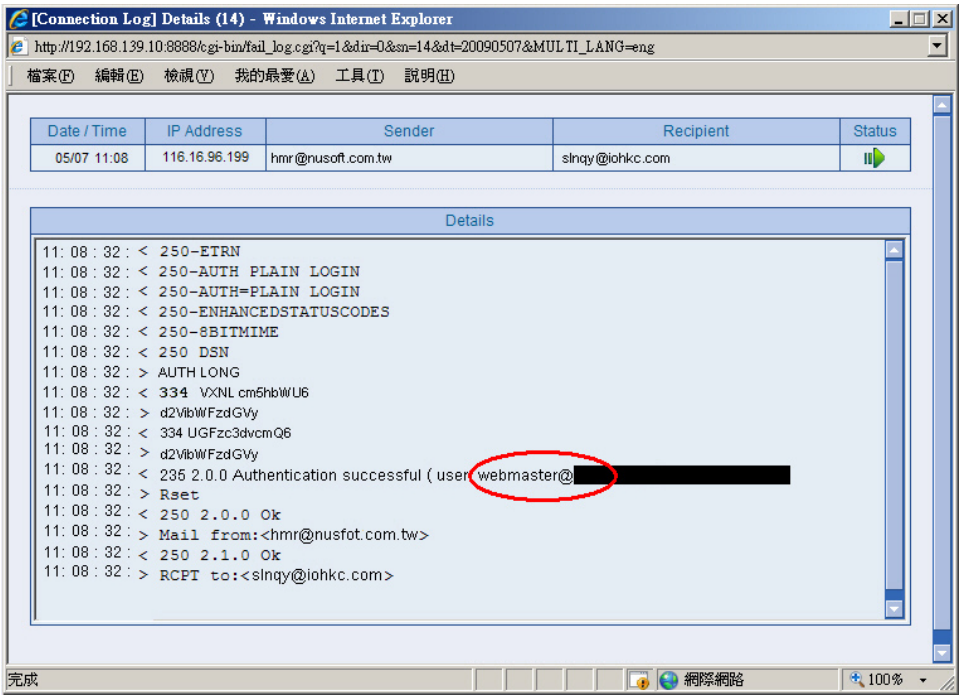
邮件伺服器 UI 上查阅出有大量的邮件发送，及未曾见过的帐号出现

情况二：于邮件服务器中查阅出，正常的 Outbound 记录里，出现不知名的账号使用者寄出大量的垃圾信件记录。

不知名的帐号，合法的从服务器来发送垃圾邮件

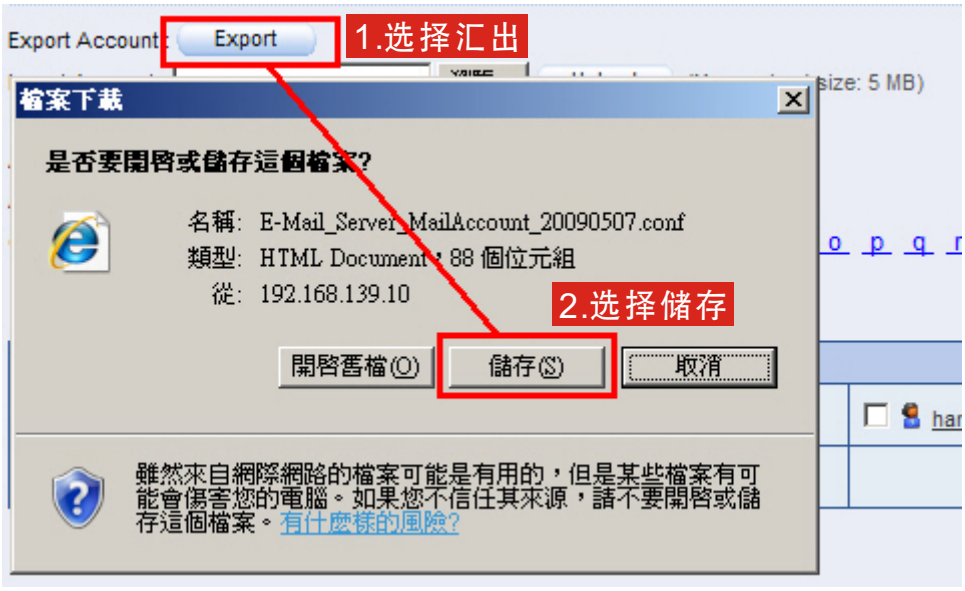
从上述的两种情况可清楚的了解到，该些账号是藉由此邮件服务器来发送垃圾邮件，但想必另管理人员不解的则是，明明服务器有设定 SMTP 认证，必须要透过所认可的账号使用者才能正常的寄送邮件，为何这些盗用者能这么轻易的就利用该邮件服务器来做垃圾信件的发送平台呢？

首先管理人员可利用邮件服务器的联机追蹤功能来进行查阅，到底入侵的人是利用何组 SMTP 认证账号来进行邮件的发送动作。进入“Connection Track → Inbound SMTP”下搜寻那些发送大量垃圾信件且未曾见过的账号，并且进入查看详细的联机讯息，利用此方式来找出入侵者所使用的认证账号究竟为何。



可清楚的了解到所使用的 SMTP 认证帐号为何

当找到入侵者是利用何组 SMTP 账号来发送信件时，接下来管理人员可于“Mail Management → Account Management → Individual”下将所有使用者账号汇出检查其原因。



將帳號匯出查閱

管理人员可藉由此方式来检查账号是否出了什么问题，究竟为何会被轻易的就遭盗用。而通常管理人员会发现到原因出现在该账号和密码皆设为相同或是设置过于简单，使人易猜。因此让入侵者则可轻而易举将其密码破解后，肆无忌惮的盗用此账号来发送垃圾邮件。

被盗用者之帐号密皆设相同

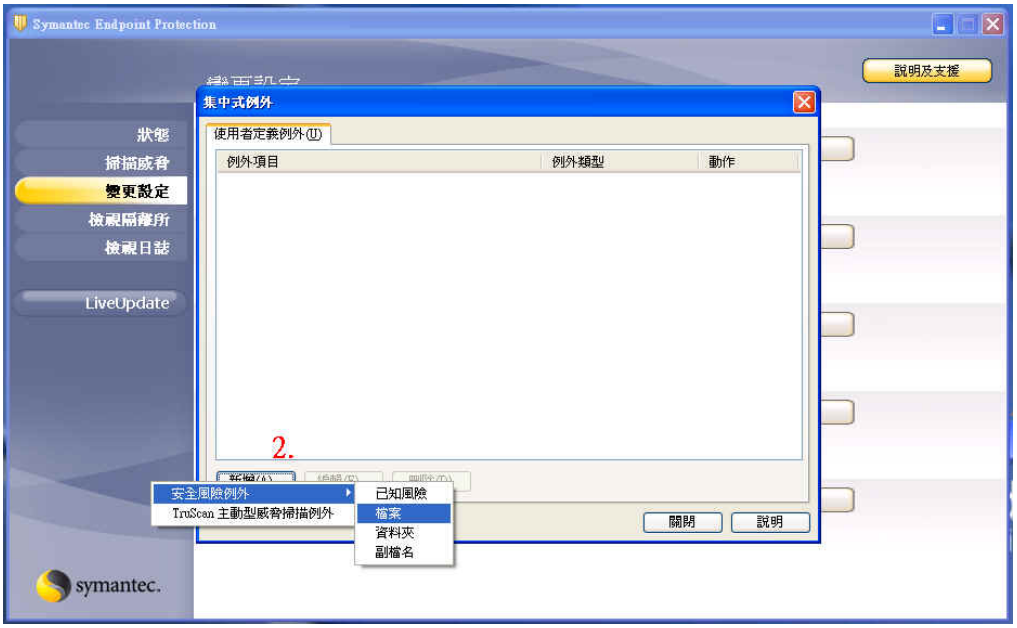
由上图可发现除了被盗用者的账号密码皆设为相同外，内部还有其它使用者也是如此，除此之外更有人使用过于容易猜测的密码。根据调查，对被盗用的密码进行分析后发现，过于简单行事是造成账号被盗用的最主要原因。新软系统提醒您，不论是何种用途，千万别将账号及密码设成相同或过于简单，以防遭到破解而进一步盗用。

附录：

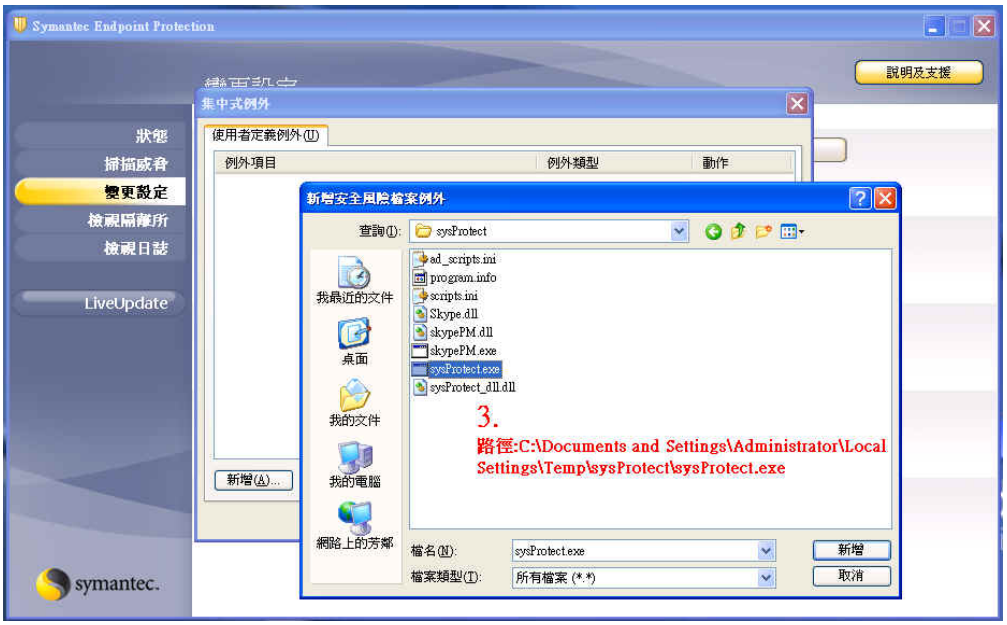
针对 IR-Plugin 安装后，在 Symantec 防毒软件下该如何避免被误侦测为问题程序？

1. 于变更设定中选『取集中式例外』的『架构设定』选项

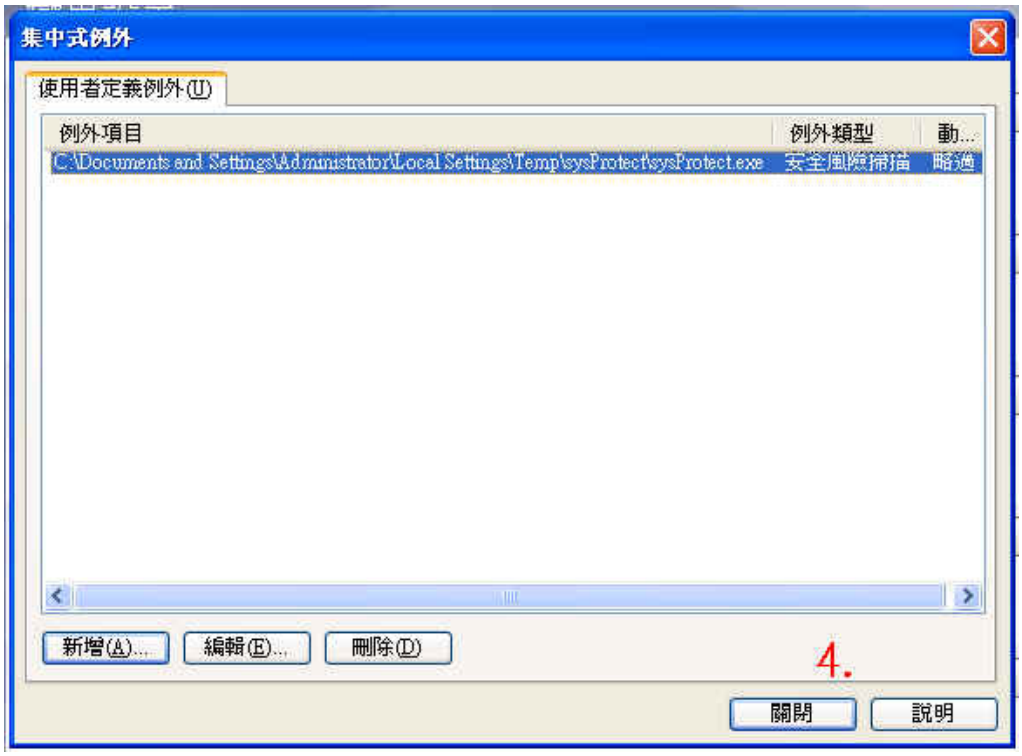
2. 新增『安全风险例外』→『文件』



3. 并将其“sysProtect. exe”程序新增



4. 确定后点选关闭离开



文 陈殿鸿 kim@nusoft.com.tw

市场营销报导 - 利用「AD server帐号整合」功能，轻松管理邮件服务器帐号

随着时代变迁及科技进步，在现今e化的社会中几乎人人都会使用计算机，而随之普及的便是人与人之间互相沟通之工具—电子邮件。如今电子邮件已是人与人互相联络的重要管道，也是现在企业与企业之间生意上相互沟通的重要桥梁，更是商业往来中不可或缺的重要武器。

然而，现今的企业为了能使公司营运分工更有效率，在公司内通常会配给每个员工一人一个电子邮件账号。藉此，上司可以透过电子邮件将公司的营运方向、业绩目标甚至其它交办事宜，更完整清楚地交办给底下的员工，员工就可以在第一时间清楚了解到「此刻工作目标为何？」、「该如何去做？」、「做到何种程度？」…等等一些业务上的工作指示。

但是有时候可能因应公司营运政策之关系会产生一些人事上的异动，因此会有人需要配给新邮件账号、有人需要撤销账号之状况发生。虽然目前很多公司企业内部都有架设统一集中管理账号密码之LDAP服务器，但是由于目前一般市售的邮件服务器并无法与LDAP服务器做账号整合，因而让LDAP服务器无用武之地。所以假使现在公司临时需要新增或变更大量之邮件账号的话，那就得由网管人员自行至邮件服务器上以传统的手动键入方式逐一将账号建立或删除，这样的键入方式一来既费工又费时、二来又有可能键入错误之可能性发生，因此该如何以最有效率之做法来完成公司内所有的邮件账号变动呢？

例如：公司网络内部里有架设统一集中管理账号之LDAP服务器，假使今天公司有部门扩编需要新增数十个新邮件账号或者有员工离职需要将其邮件账号删除，此时该如何以最轻松简单之方式完成所有的账号变动呢？

为了因应目前科技讲求「快速」、「轻松」之理念，新软系统也将这样的理念实现于邮件服务器 — ML系列产品上，设计出「AD server账号整合」之功能，藉此让网管人员能以最轻松容易之方法来完成所有邮件账号的新增及变动。对于类似这样的账号变动需求，由于邮件服务器 — ML系列产品有「AD server账号整合」功能的关系，利用其账号学习整合功能之特性和LDAP服务器做实时账号整合，让邮件服务器自行去向公司内部统一管理账号密码之LDAP服务器学习其所有之账号密码（如图1)。如此一来，只要网管人员在LDAP服务器上有做账号之任何变动的话，那么在ML系列邮件服务器上也会自动新增或变更账号(如图2）达到账号实时整合。甚至公司内还有架设新软系统之IR或MS系列产品，一样可以使用「AD server账号整合」之功能与LDAP服务器上之账号密码来做相互对映，达到实时账号整合。

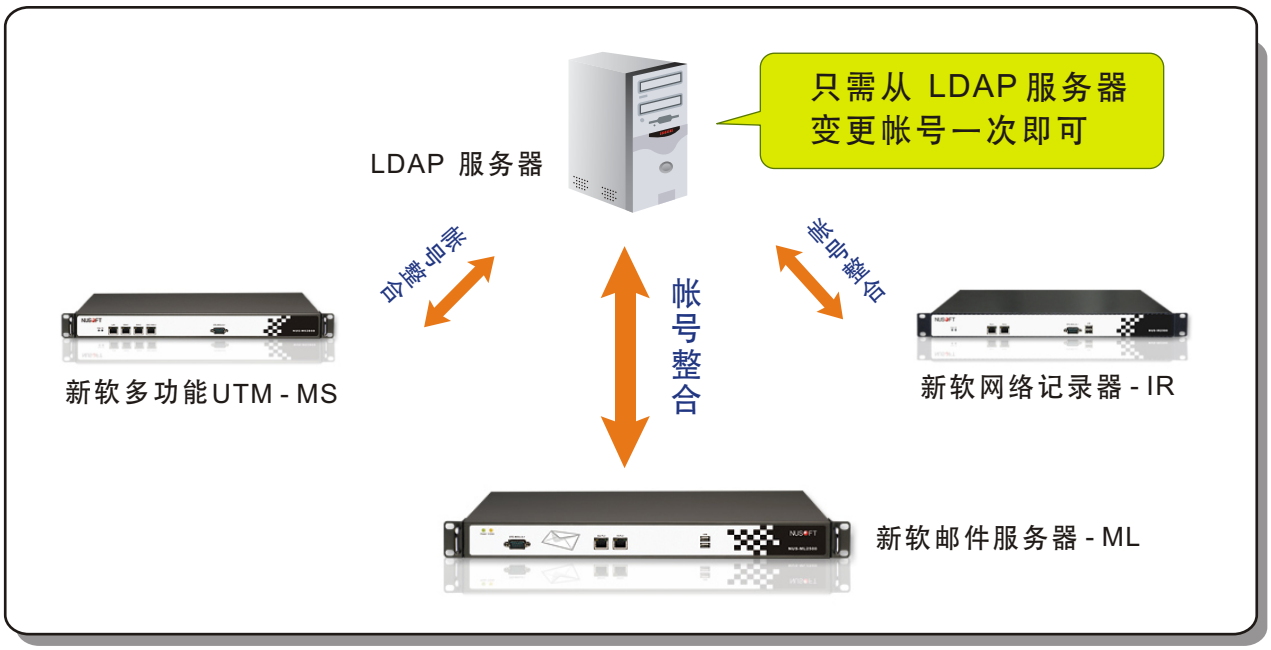


图 1 只需在 LDAP 服务器上轻松变更帐号即可，底下之新软邮件服务器会自动整合帐号。

图 2 使用「AD server 帐号整合」功能，即使 LDAP 服务器有帐号新增，ML 邮件服务器也会随之新增。

	新软邮件服务器(ML系列)	一般市售网邮件伺服器
新增/变更帐号方式	使用「AD server帐号整合」功能，由系统自行与LDAP服务器上之数据做即时帐号整合。	需由网管人员以手动方式至邮件服务器上逐一新增或变更帐号。
新增/变更帐号方式效率	优 若需新增或变更帐号，只需在LDAP服务器上修改即可，ML 邮件服务器会即时帐号整合。若公司内还架设有新软系统IR或MS系列产品，一样会同时有即时帐号整合之效果。	差 只能手动键入方式，既费工又费时，虚耗人力於该业务上，加上会有键入错误的可能性发生。

表 新软邮件服务器「AD server 帐号整合」与一般市售邮件服务器帐号结合方式差异。

文 黄政铭 ming@nusoft.com.tw