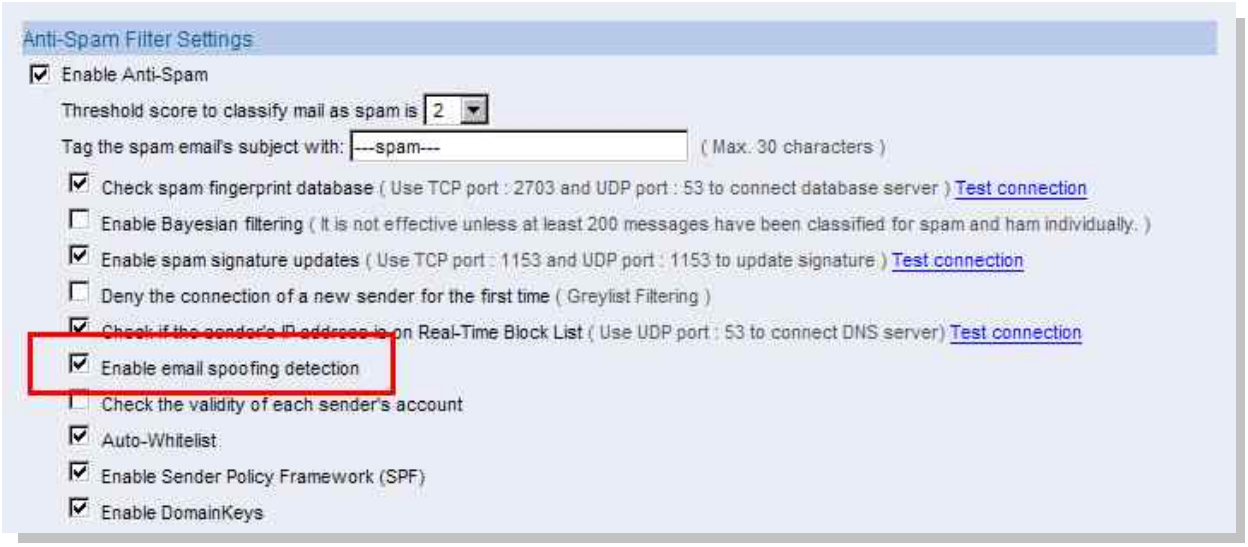
新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2009/10/5- 2009/10/18 第102期

邮件服务器 / ML系列报导

技术浅谈与应用 - 新增『寄件者伪装网域侦测』功能

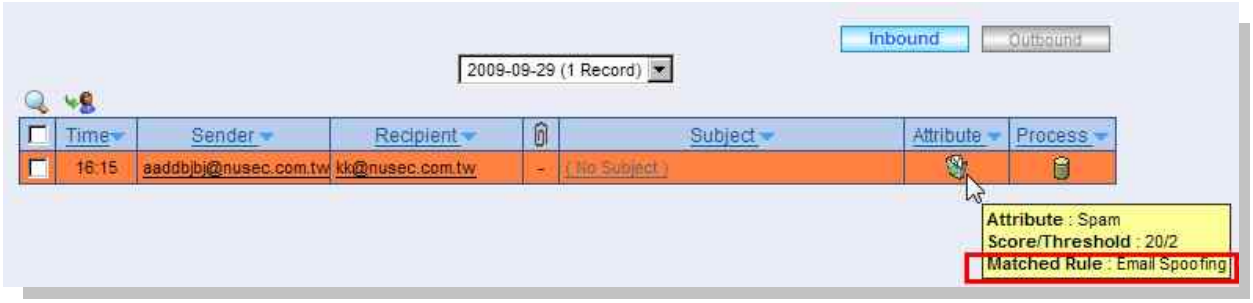
成堆的垃圾信件不只成了办公室有害物，也浪费了公司内部带宽与设备储存空间，甚至信件还与病毒同时伺机入侵企业；如此扰人的问题不但没随着科技的进步而减少，相反的还更加的变本加厉，也正因为如此，公司纷纷的导入相关的防护设备来将伤害降至最低。但垃圾邮件的散播方式也同样的不断在改变，旧有的防护机制并无法完全的阻挡不断换新花招的垃圾邮件攻势，让少数的垃圾邮件开始流入公司内部。对于如此让人头痛的问题，身为公司的网络安全管理人员又该如何去解决呢？

垃圾信件的寄送方式为了能躲避种种的信件检查防护机制，而其中的一种则是进而使用修改寄件者网域的方法，来欺骗大多数的邮件服务器，让该邮件服务器误认为该封信件为是内部网域或是外部所信任之网域所寄送之信件，因而放行通过。新软系统，针对不断改变的垃圾邮件攻势，同样也不断在更新新的阻挡方式，除了旧有的白名单、黑名单及多数的信件过滤机制外，近期于『邮件服务器 - ML』中的“邮件过滤”机制下，为防止伪装网域之垃圾邮件寄件方式，又新增了一项『寄件者伪装网域侦测』功能来协助公司达到更上一层的垃圾邮件保护。

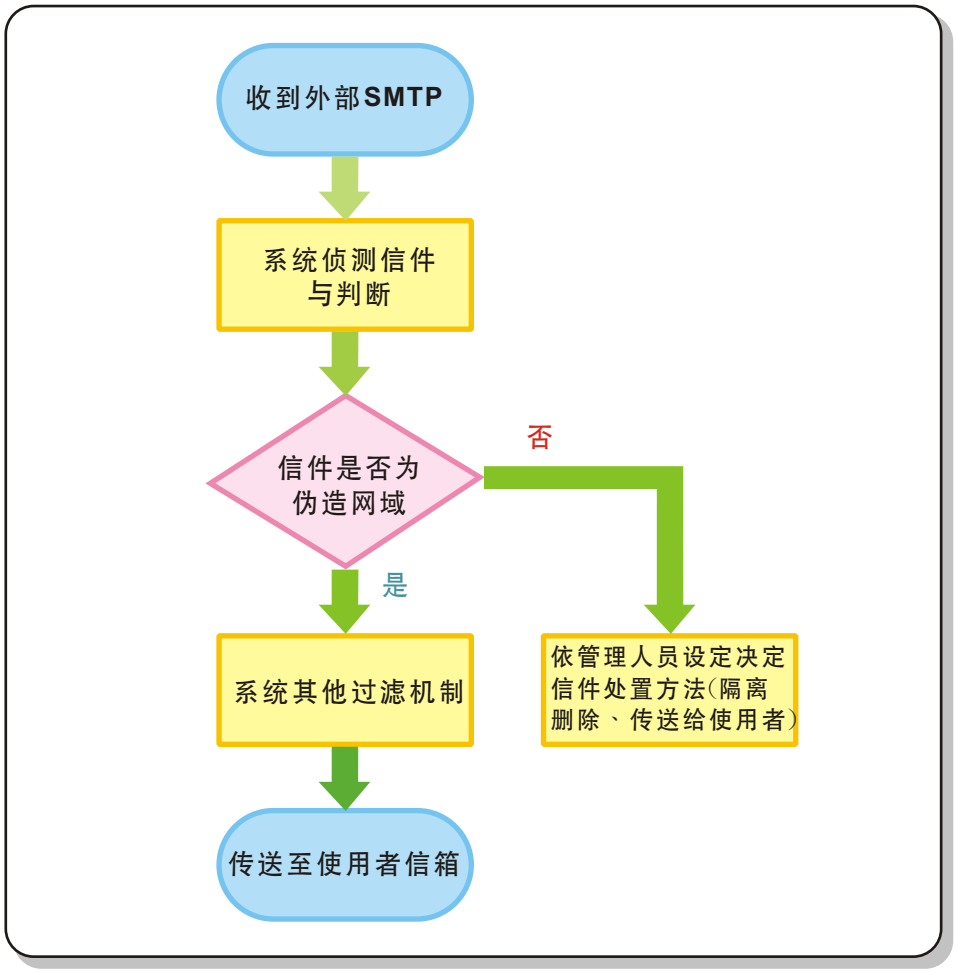


新增『寄件者伪装网域侦测』功能

而此功能所在位置为系统中『Mail Security > Anti-Spam > Settings』下，管理人员只需轻松的在 UI 中将该功能打勾即可启动，完全不需再另外键入烦杂的设定程序，该功能启动后能够在对方信件进入公司前，立即去侦测该封信件是否为所属网域寄出之信件，如此一来针对想利用伪装网域来送发垃圾信件的寄件方式，则可有效的达到阻档的效果，防止垃圾邮件篡改成与公司内部相同网域、或其它外部正当邮件网域来欺骗邮件服务器以达到成功将垃圾信件送至收件者信箱的情况发生。



有效侦测及阻挡篡改网域的垃圾邮件

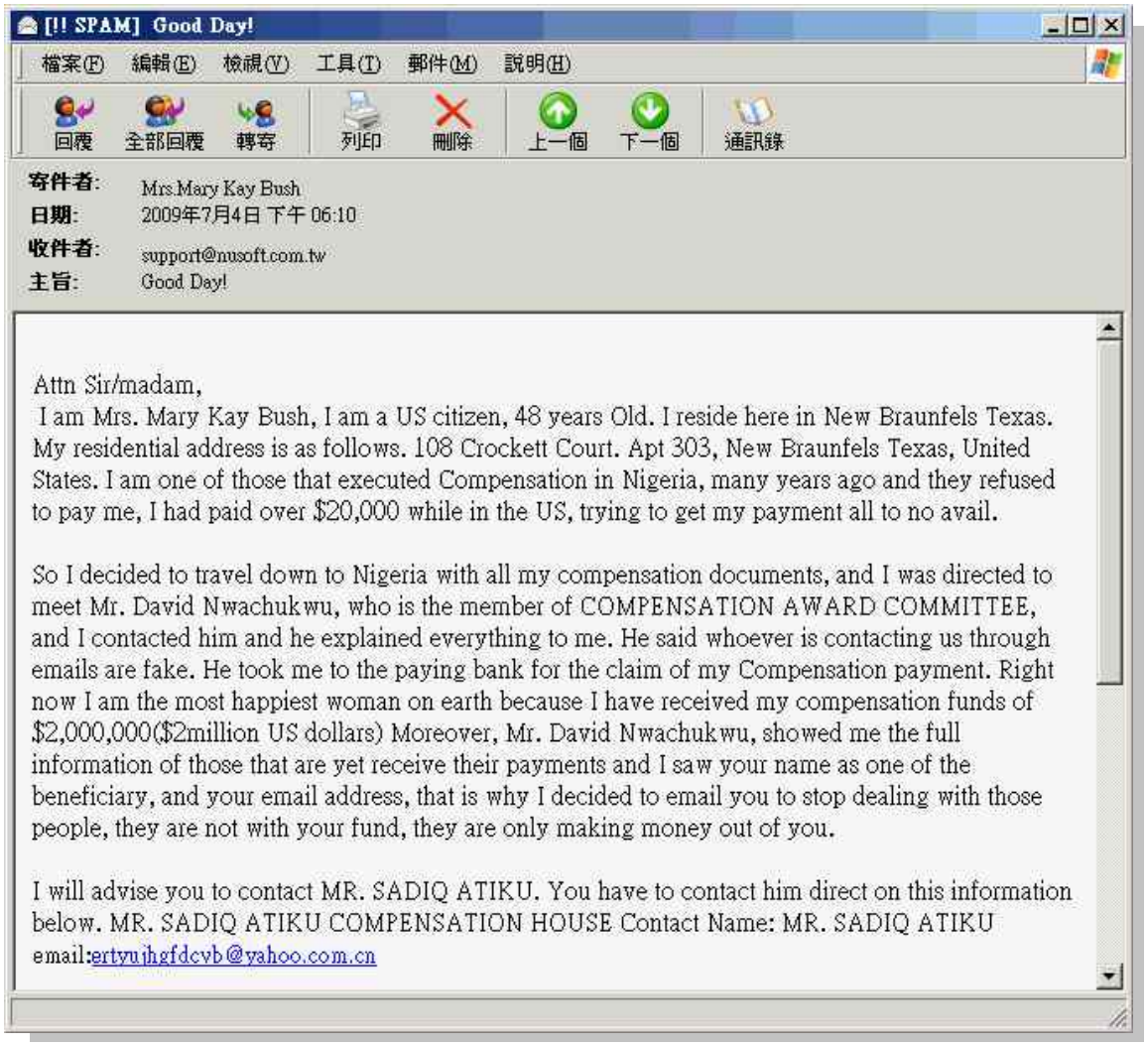


新功能简易流程图

文 陈殿鸿 kim@nusoft.com.tw

市场行销报导 - 垃圾邮件流行「装熟」钓肥羊，新软邮件服务器给您更严谨的过滤机制

近期以来网络上出现许多垃圾邮件，常常以『Hey』、『Hi』、『Hello』、『Good Day』等一般且轻松性的口吻为标题，让受害者在第一时间误以为此封信件为熟人或朋友所寄送来之信件，甚至是假冒邮件传递失败通知信、订货通知信等，藉以企图躲过层层的垃圾邮件过滤功能，蒙骗受害者上当开启信件，点选信件内的超级链接下载不法文件或登录其钓鱼网站。



近期网络上有许多以轻松语气为标题的垃圾邮件，四处流窜引诱受害者上当。

新软系统一向秉持着『不断进步』的精神，严格地自我要求；针对目前网络上不断翻新手法的垃圾邮件问题提出相对解决之道，力求以『兵来将挡、水来土淹』的模式来全面防止垃圾邮件的攻击。因此目前除了原本在新软邮件服务器(ML1000G、ML2500) 中的七大垃圾邮件过滤机制以外，另外新增了三道垃圾邮件过滤机制，藉以让垃圾邮件过滤能力能更为强大、完整。三道新增垃圾邮件过滤机制如下：

寄件者伪装网域侦测

由新软邮件服务器发送检查封包，检查在 HELO / EHLO SMTP 命令中所提交的寄件者地址，并与其将信件中所填入的寄件者地址之网域名称进行符合性比对，若完全符合便属于正常信件；若不符合便直接判断为垃圾邮件，并进行垃圾邮件过滤阻挡。

检查寄件者帐号是否存在

一般垃圾邮件的寄件者账号皆为伪造账号，利用由新软邮件服务器所发出检测封包到寄件者账号所在的邮件服务器进行查询，利用所回复的封包可得知此封信的寄件者账号是否存在；若否，则以判为垃圾邮件处理之。

自动化白名单

当寄件者寄出一封信时，自动化白名单机制会计算这封信的评等，分数越高，代表该信的内容越符合垃圾邮件的定义。其原理是将信件来源与寄件者账号依系数设定做权重分析，经常信件往返者便会将自动加入至白名单。

网络上的各类垃圾邮件威胁兴起，不断翻新之手法是所有垃圾邮件共同的特征。因此若只靠少数几种过滤机制来防范是不够的；而新软系统便是以自家研发团队为强力后盾，在多变的网络潮流里不断寻找过滤垃圾邮件的解决之道，因而让新软邮件服务器能以强大的邮件过滤能力来满足众多用户防范垃圾信件攻击的需求。

文 黄政铭 ming@nusoft.com.tw