新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2010/1/11-2010/1/24 第109期

多功能UTM / MS系列报导

技术浅谈与应用 - 异常流量的警告通知及设定所需注意之事项

网络安全一直以来都是各公司、企业首要的条件之一，随着网络恶意攻击事件不断发生，公司内部也因此纷纷导入相关信息安全设备来做为前线防护墙，藉此以减少及降低公司内部遭受波及的程度与机率。

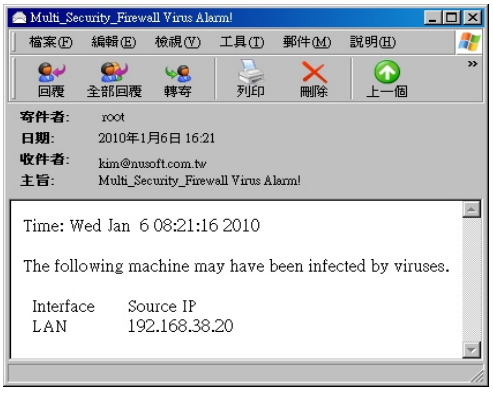
但长期以来，公司的安全防护措施，通常都有着相同情况出现，对于外来恶意攻击有着相当的防御能力，但却往往无法有效阻止与防范内部机器因中毒或刻意所发出的恶意攻击异常流量封包。以至于当情况发生时，往往无法实时将恶意攻击杜绝，直到管理人员发现后，还必需得一台一台费时的去找寻，等找到问题源头时早已经造成某部份严重损失，甚至是网络瘫痪让公司部份作业停摆，因而使公司丧失许多商机。

新软系统多功能UTM - MS所内建的『异常流量IP』功能，就能轻松为公司解决如此问题。只要当MS收到公司内部机器所发出大量不正常封包时，该功能会立即阻挡此类封包的传送，实时阻断发生问题的使用者，以避免不正常封包流量将企业网络瘫痪，并且系统会立即依照管理人员设定之通知方式来通知该使用者及管理人员，让管理人员能在最短时间内去处理及解决相关问题，以确保公司内部网络的安全。

而『异常流量IP』警告通知可依管理人员自行设定的方式分成“电子邮件警讯通知”、“SNMP Trap警讯通知”、“NetBIOS警讯通知”三种，并且在发现异常流量后会于使用者的计算机第一次透过浏览器上网时，于其浏览器上显示警告之画面，告知其该使用者计算机已中毒。以下将分别说明上述几种警告方式及管理人员所需注意的事项。

一. 电子邮件警讯通知

管理人员若勾选启动该项功能后，当系统侦测到内部有异常流量时，则会立即发送信件至管理人员的电子邮件信箱，通知管理人员相关讯息(如下图)。

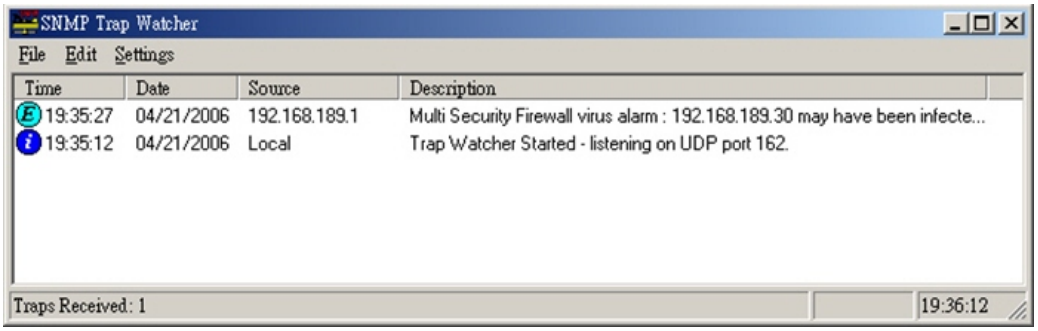


电子邮件警讯通知画面及内容

管理人员若需开启该项通知功能时要注意到的则是，还必须先于『系统管理 > 组态 > 系统设定』下设定管理人员邮件位置，该项通知功能才能正常启动。也建议管理人员别单单只是开启该项警讯通知功能而已，最好还是搭配其它通知功能，以防因一时没留意信件而错失处理的时间。

二. SNMP Trap 警讯通知

管理人员若勾选启动该项功能后，当系统侦测到内部有异常流量时，MS 会将警告讯息实时显示于管理端计算机所安装之 SNMP Trap 客户端软件上（如下图）。

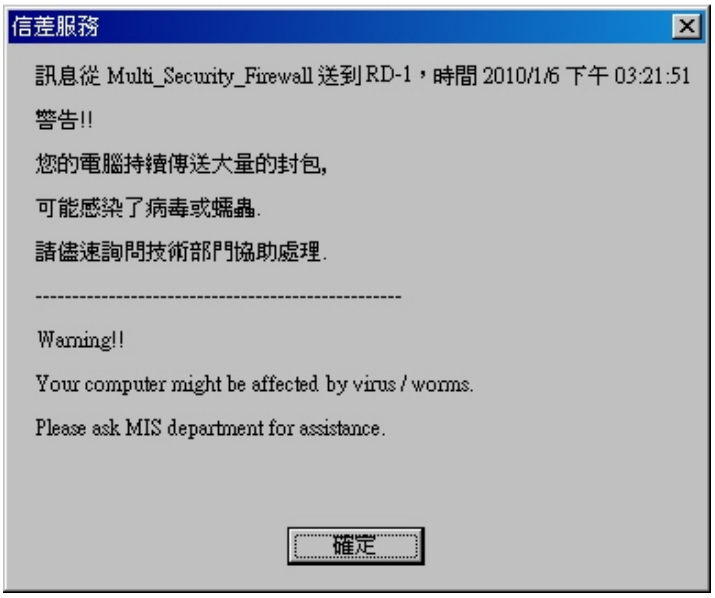


SNMP Trap 用户端软件所接收到之病毒警示

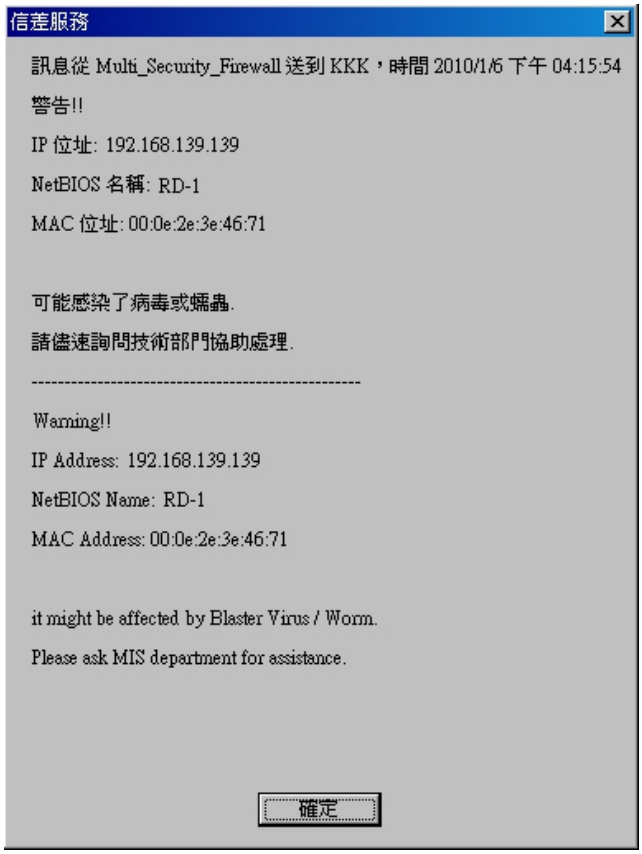
若需开启该项通知功能时要注意到的则是，还必须先于『系统管理 > 组态 > SNMP』下做设定，该项通知功能才能正常启动。然而较为不便之处则是还必须安装 SNMP Trap 相关软件才能正常接收通知，但对于已有使用该项软件的使用者而言，该项通知功能也肯定是非常有效的通知管道之一。

三. NetBIOS 警讯通知

该项功能启用后，当系统侦测到内部有异常流量时，会立即发出警讯给中毒及管理员的 PC（如下图）。

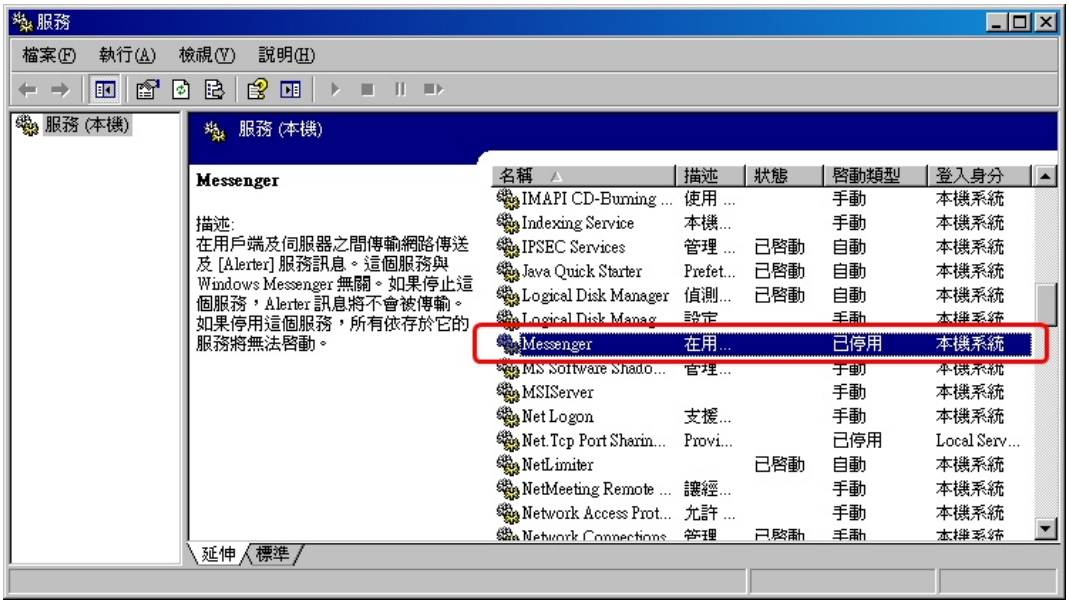


中毒使用者 PC 所接收到的 NetBIOS 警讯通知

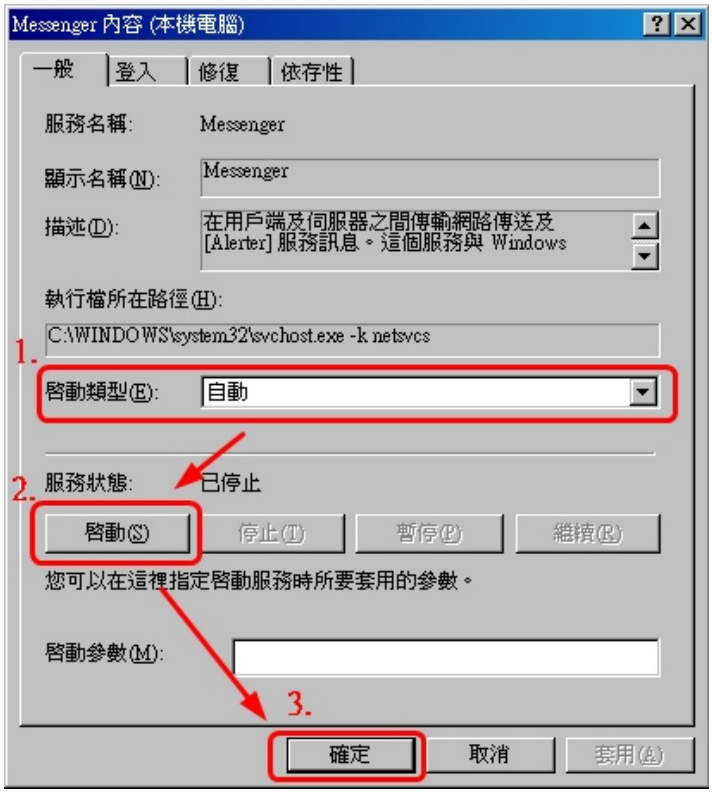


管理员 PC 所接收到的 NetBIOS 警讯通知

此项通知功能是最不容易被忽略的，因为系统会立即于 PC 上跳出通知讯息，但还须注意到的是计算机操作系统中的“Messenger”是否有正常启动，否则将无法正确接受到“NetBIOS 警讯通知”功能所发出的通知讯息。而管理人员可于『控制台 → 系统管理工具 → 服务』中设定启动。

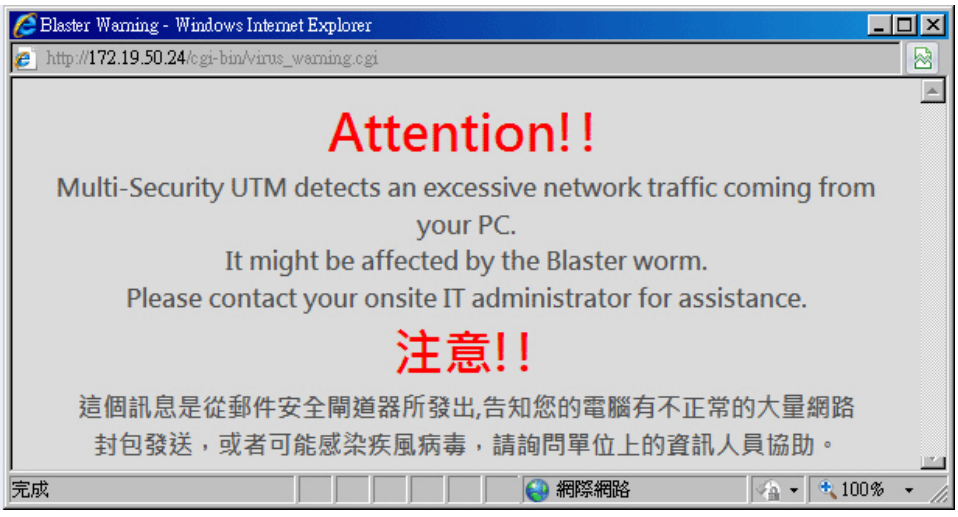


於『控制台 → 系统管理工具 → 服务』中选择“Messenger”



将启动类型设定为“自动”，於服务状态点击“启动”，完成後并按下“确定”

最后当内部使用者的计算机中毒且发出异常流量后，第一次透过浏览器上网时，MS 会于其浏览器上显示警告画面，告知其使用者计算机已中毒(如下图)。



中毒后使用者第一次使用浏览器出现之警告讯息

须注意到的是使用者若是不能排除本身中毒之情况，往后皆会受到 MS 限制，导致上网变慢，并且不会再有警告讯息显示于浏览器。

文 陈殿鸿 kim@nusoft.com.tw

市场营销报导 - 员工利用「无界、自由门」上网“开心”，新软多功能 UTM 替企业严格把关

因特网蓬勃发展，带动人类生活 e 化，至今许多人生活模式都离不开网络。去年最为火红之例子莫过于著名的社交网站 - Facebook，其以活泼之网络互动方式让使用者趋之若鹜，其中“开心农场”便是其成功风靡群众里最典型的工具之一。

然而，使用者爱好玩诸如“开心农场”此类互动型网络游戏，却经常不分公私时间地玩；身受其害最为严重的企业界最为了解。在公司企业里，重视奉行的法则莫过于「提高公司生产效力、降低公司营运成本」，但是底下企业员工若于上班时间利用公司网络偷上 Facebook 的话：

1. 员工无心于自己工作本务上，反而沉迷于 Facebook 里，因而降低生产效率。
2. 员工上 Facebook 时所读取之 Flash 网页对象会消耗大量的网络带宽，间接造成公司其它同仁的使用网络带宽遭到挤压，进而延误掌握商机之第一时间。

因此现今很多企业为了「防范员工混水摸鱼以及提高生产效率」的问题，而花费添购相关网络行为管理设备。可是“道高一尺、魔高一丈”，虽然起初此类产品能对企业网络底下的用户产生简单之管制效果；不过现在网络科技发达，却已有人研发出能突破网络行为管理功能的软件，如：无界(Ultra-Surf)、自由门(FreeGate)、热点盾牌(Hotspot Shield)、Tor...等等。此类软件俗称“穿墙软件”，其原理是以特殊加密机制来包装所有进出之网络封包，让一般网络行为管理设备误判为正常封包，导致间接在网络管理设备及前端防火墙内形成一条通道进出自如，让不肖员工可以在一般网络行为管理设备无法管制的情况下为所欲为地使用公司网络资源来上网，除此之外，也因为使用此软件后彷佛在防火墙里开了一条通道，因此可能造成于上网时让网络上之病毒透过此信道渗透至内部网络里，造成不可想象的损害。

于此，新软系统多功能 UTM 以强大之应用程序管制机制来打击摸鱼上网的不肖员工，有别于市面上其它网络管理设备以「阻挡 Server IP、关闭通讯端口」等毫无效率可言之管制方式；新软系统多功能 UTM 以独家分析方式正确过滤所有的网络封包，即使底下不肖员工欲使用“穿墙软件”来突破管制，但是在新软系统多功能 UTM 的独家过滤机制下，所有的网络封包都将无所遁形，便可以完整的管制底下的不肖员工，另外新软系统多功能 UTM 成功管制“穿墙软件”后，将会随之产生相关数据报表(使用 IP、使用时间、使用软件)，因此可以透过记录报表得知有哪些员工企图使用“穿墙软件”来混水摸鱼。如此一来，就可以达到完善的管制效果，企业也可以达到「提供公司生产效率、降低企业营运成本」的营运目标。

	新软多功能 UTM	一般网络行为管理设备
管制方式	以独家分析方式正确过滤所有的网络封包，即使底下不肖员工欲使用“穿墙软件”来突破管制，但是在新软系统多功能 UTM 的独家过滤机制下，都将无所遁形。	采用「阻挡 Server IP、关闭通讯端口」等治标不治本的管制方式。
管制效率	高 不管 Server IP 或通讯 Port 如何变更，单纯针对进出封包进行分析过滤，藉此达到准确的判断及管制。	低 当 Server IP 或通讯 Port 变更时，就容易发生无法管制的窘境。
目前能提供管制机制的对象软件： VNN Client、无界浏览(Ultra-Surf)、Tor、Hamachi、自由门(FreeGate)、 热点盾牌(Hotspot Shield)		

文 黄政铭 ming@nusoft.com.tw