

## 多功能 UTM / MS 系列报导

### 技术浅谈与应用 - 病毒感染 VS 黑客攻击

近几年因特网的普及带给人们许多便利，却也潜藏着许多陷阱与危机，因特网上到处充斥着黑客的攻击与病毒的传播，不时有黑客入侵企业网络中盗取商业机密或是病毒发作造成企业损失的新闻报导，像是台湾索尼通讯网络 So-net 网站之前传出被黑客入侵，造成会员网友个人数据外泄、信用卡被盗刷，以及前阵子流行经由随身碟和 E-Mail 传播的 KAVO 病毒，占满 CPU 效能使得其它程序无法执行，造成许多使用者的困扰，这些受害案例层出不穷，因此信息安全俨然已成为企业网络中最重要的课题，在防毒防骇的前提下，认识病毒与黑客的攻击型态是首要的任务。

#### 病毒感染：

病毒通常是以被动的方式透过网络浏览、下载，E-mail 及可移动储存装置等途径传播，通常以吸引人的标题或文件名称诱惑受害者点选、下载。而某些计算机病毒类似生物病毒一样具有传染性，会感染中毒计算机里其它的执行文件，如 exe、com、bat、scr 格式的文件，或是利用网络共享的漏洞复制并传播到其它计算机，进而感染区内多台计算机的文件。然而病毒运行后，通常会有一些特征表现，如无法上网、CPU 效能达 100% 居高不下、无法显示隐藏文件、出现蓝屏... 等现象，这些明显的表现反而让使用者容易发现自己计算机中毒并对清除病毒有所帮助。

#### 黑客攻击：

黑客通常会针对特定的目标扫描，寻找出该系统的漏洞，再以各种方式入侵系统并植入木马程序，使得目标对外门户大开让黑客自由进出好窃取文件数据，而黑客也可利用一个个已被攻陷的计算机组成僵尸网络 (Botnet) 对特定目标发动大规模的分布式阻断服务攻击 (DDoS) 或 SYN 攻击，藉以把目标的系统资源耗尽并瘫痪其网络资源，若该目标是企业对外提供服务的服务器，必然会造成企业若大的损失。

	病毒感染	黑客攻击
型态	被动	主动
攻击对象	没有特定对象	针对特定目标
感染途径	恶意网页、P2P 下载、E-mail、网络芳邻、随身碟等可移动储存装置。	利用系统、程式的漏洞或以其他方式取得进入系统的帐号密码，从外部入侵进行破坏。
比喻	持有合法护照的人士携带毒品（病毒程式）入境，而海关（企业网络的 Gateway）并无察觉，于是在突破第一道关卡后，这些毒品将流入国内市面（企业网络），随时产生危害。	被限制出入境的罪犯（黑客），用假以乱真的护照蒙骗海关（企业网络的 Gateway）顺利入境国内（企业网络），锁定特定对象（企业内部的计算机）加以迫害。

为求网络安全，一般基本的防护方式就是设置防火墙并在用户的计算机安装防毒软件，想藉此方式抵挡黑客的入侵及病毒文件的感染，不过由于这几年网络发展迅速，连同黑客的攻击模式和病毒的传播方式也随之改变，日前发现黑客透过系统漏洞入侵一般网站将恶意的程序代码或带有病毒的网页嵌在正常的网页当中，使得浏览此网站的用户会自动执行黑客所设下的程序代码而下载木马病毒，然而这类的病毒通常拥有自动更新的功能，并且据说更新的速度有时甚至还比防毒软件快，由此可知使用一般的防火墙以及防毒软件作防毒防骇的资安工程已经不敷使用。

而新软系统所推出的多功能 UTM 不仅内建入侵防御侦测系统 (IDP) 可抵挡黑客的攻击，并且支持网页扫毒的功能，可补足防毒软件无法防护的项目，让企业的网络安全防护更加有保障。另外针对 UTM 与防毒软件的互补性，我们将在第 55 期「PC 防毒功能 VS UTM 防毒功能的互补性」的文章中做更多的说明。

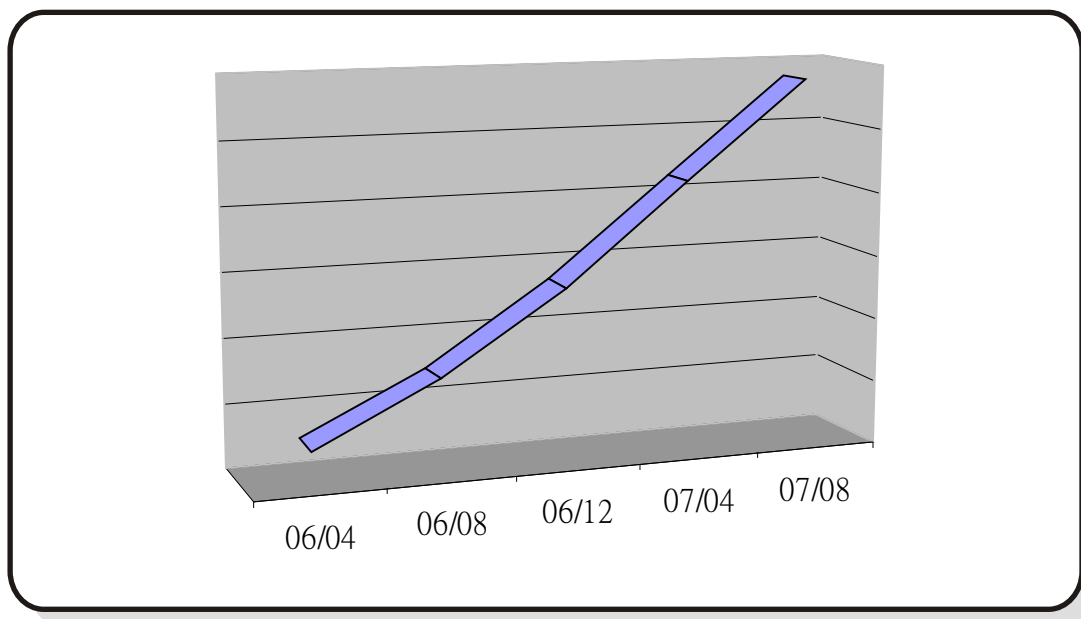
文  黄智杰 alex@nusoft.com.tw

## 市场营销报导 - 如何对付泛滥成灾的「恶意网页」

在以往，「恶意程序（病毒、木马、蠕虫...）」的传播以电子邮件为主；信件中夹带「恶意程序」，再诱使收件者开启，已达到传拨之目的。但由于大部分的使用者已对此种传播方式已有所了解（不会轻易去点选信件附加文件），再加上市面上的防毒软件对于此种邮件之防护日渐完善，使得利用电子邮件来传播恶意程序的方式逐渐式微。取而代之的是另一种广为大家使用的网络服务—网页浏览。

黑客会将“网页浏览”作为「恶意程序」的散拨管道，其原因不外乎是一般使用者最常使用的网络服务除了收发电子邮件外，就是以浏览网页之使用量为最多。所以在电子邮件无法达到预期的散拨效果时，黑客们改采用网页方式来散拨「恶意程序」。尤其在这半年内，这种散拨方式之数量快速增加，甚至已经超过所有「恶意程序」攻击的八成之多。

也就是因为这种情况，导致因特网上的问题网站越来越多—根据统计，其比例已经高达每 10 个网页中，就有一个含有恶意程序。透过这些恶意程序，黑客们可以轻松取得使用者的各种数据、感染其它计算机、甚至是操纵使用者的计算机散拨垃圾邮件...。让稀松平常的网页浏览，成为敞开企业网络大门最大元凶。



图一 全球恶意网页数量快速成长


或许有人会想“只要小心避开黑客所架设的「恶意网站」，应该就没有危险了”。这种想法在以前也许行的通，但是现在问题网页反而大多数都是一般正常网站！！

正常网站怎么会有「恶意程序」呢？其实，这些有问题之正常网站通常都有个很明显的特征“鲜少更新或修补其服务器系统”。黑客们常常利用这些网站的安全弱点，入侵其网站服务器，并在其中植入「恶意程序」。这些被窜改的网页在外观上完全正常，看不出有什么不妥，而且大多为知名企业网站、政府网站、电视 / 报纸媒体网站...，所以使用者在浏览这些网站时通常不会有任何戒心。只要使用者浏览该网页，「恶意程序」会被自动下载、安装至使用者的计算机中。接下来，黑客要窃取使用者的数据、散发垃圾邮件...将畅通无阻。

既然浏览网页会有中毒的危险，那在计算机中安装防毒软件来过滤「恶意程序」是不是就可以高枕无忧的浏览网页呢？其实，仅用防毒软件来预防网页的「恶意程序」还是有风险的；防毒软件在发现「恶意程序」之前，一些个人数据、企业机密...就可能已被「恶意程序」窃取。因此要确保计算机不会受到「恶意网页」的威胁，最好做到以下三点：

1. 设定浏览器的安全权限 —— 调整浏览器的自动执行权限，以防在浏览网页时，浏览器自动执行了「恶意程序」。
2. 定期更新操作系统 —— 绝大部分的「恶意程序」都是利用操作系统的安全漏洞而设计。因此，定期更新操作系统才能确保不被「恶意程序」所感染。
3. 在网关端隔离「恶意程序」—— 防堵「恶意程序」最佳方法当然就是不要让它有任何机会进入计算机中。因此把它隔离在企业网关外，方能避免「恶意程序」可能带来的任何危害。

企业可以透过新软系统—多功能 UTM 产品内建了「HTTP 防毒」机制来防护「恶意网站」之问题。使用者在浏览网页时，多功能 UTM 会将网页服务器所回传的数据先行过滤，确定无误后才将这些数据传送至使用者的计算机中。把「恶意程序」隔离在网关端之外，使其无任何机会进入企业网络。因此，就算是使用者所浏览的网页有问题时，多功能 UTM 也只是隔离「恶意程序」这一部份，不会影响到使用者的网页浏览。

文  程智伟 rayearth@nusoft.com.tw