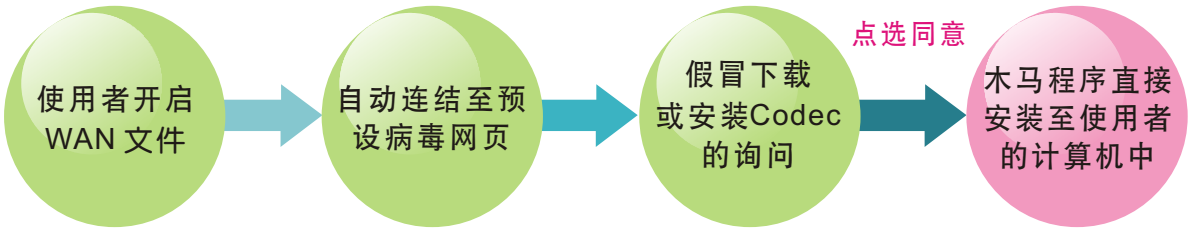
新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2008/11/10- 2008/11/23 第80期

多功能 UTM / MS 系列报导

技术浅谈与应用 - MS 该如何防范新型木马利用 WMA 格式入侵

在网络病毒层出不穷的环境下，为了达到能入侵使用者的计算机，病毒的入侵管道及方式也同样的不断在变，然而某知名防毒厂商近期也发现了新的木马入侵方式。这次则是利用 WMA 影音文件来当作感染途径的新型蠕虫程序，可在使用者计算机安装木马病毒，以做为网络罪犯控制。

新品种的蠕虫会隐藏在 Windows Media Audio（WMA) 格式的文件中，并增入连结至受感染的网页。一旦使用者开启文件，并且连到该网页，就会开启一个下载或安装 Codec 的询问。如果使用者同意安装这个文件，木马程序将直接安装至使用者的计算机中，进而成为网络罪犯控制的殭尸计算机。



木马入侵流程图

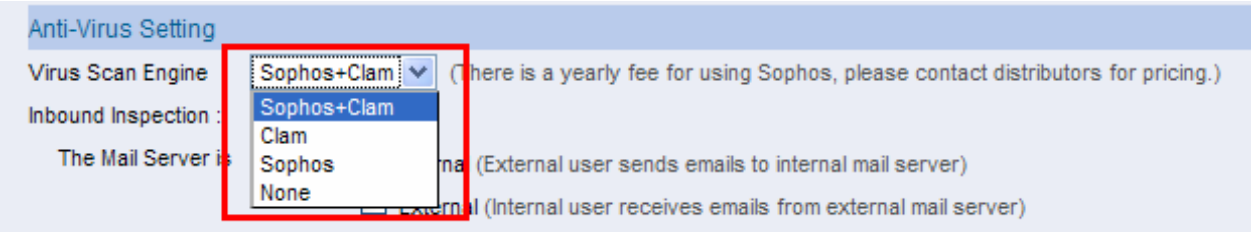
根据知名防毒厂商分析，到目前为止这是第一个属于感染影音文件的蠕虫，也正因为如此，大部分的使用者不认为这些影音文件可能受到感染，也不曾因此类型文件而受感染，以致于造成攻击成功机率不断的增加。

倘若公司一不小心被此类木马所入侵，重要文件及机密数据被外泄的机率也就相对的大为增加，为了预防此类新品种病毒、木马，一般人处理的手法即是立刻更新计算机中所安装的防毒软件来做预防，当然不可否认这也是必须的处理动作之一，但往往却也忽略了此类型属于新种的病毒，在往后的日子里也有变种型态出现的极大可能性，而公司何时会被入侵也因此变成了未知数。

员工所使用的是公司内部的计算机而非一般家用计算机，一但出了问题，所连带造成的损失是无法相比拟的，若是像一般家用计算机只以更新病毒码来作预防处理的动作，往后所需面临的风险也相对较高。为了能够彻底的保护公司网络信息的安全，“新软多功能 UTM-MS”则能够轻松的满足资安人员的需求。利用多功能 UTM-MS 中管制条例里的“Download”功能来做针对 WMA 格式的管制。如此的设定，一方面可管制公司内部因下载 WMA 影音文件而占用带宽的问题，另一方面则可让员工减少偷懒摸鱼的时间，同时也让公司大为减少病毒入侵的机率。

功能画面截图

而文件的来源当然绝对不会只是单单经由下载的管道而来，市面上多数的应用程序也都可能成为感染的途径，为了能够达到更完善的防护，管理人员同时还可搭配 MS 中“Application Blocking”的功能，再视公司情况而作最适当的控管及辅助，可有效的降低病毒来源的管道及公司内部不必要的带宽浪费，并且同时配合利用 MS 所内建防毒机制（双扫毒引擎 ClamAV、Sophos）在线更新病毒码，还可针对 SMTP、POP3、HTTP、FTP 的扫瞄，如此一来即可多方面的防护，使公司内部拥有干净的网络环境。



功能画面截图

项目	内容	备注
扫毒引擎	ClamAV Sophos	目前已可侦测超过四万种以上的病毒、蠕虫以及木马程序，并 24 小时随时在线自动更新病毒码。ClamAV 可永久免费更新病毒码，而且并无使用人数限制。这可让病毒防护功能，能以最少的成本，永远保持在最新的状态。免受病毒、木马、恶意网页程序、间谍软件、网络钓鱼...危害。
支持防护方面	SMTP POP3 HTTP FTP	

病毒侦测功能

文 陈殿鸿 kim@nusoft.com.tw

市场行销报导 - 让公司不再有计算机「毒患」的身影

根据统计，台湾上网人口早已经超过一千五百万人，不过到底有多少人的计算机因为病毒入侵而中毒呢？若以一般的中小企业的情况来统计，一台计算机一年平均要中毒八十六次，相对的公司也必须得要花上高额的维修防护费用，而家庭用户则是每一百台计算机中，就有三十八台曾经感染计算机病毒，加上木马、病毒不断的推陈出新在眼前，台湾有超过七成五的人都在使用病毒计算机。

病毒在网络世界里，无所不在，而发出计算机病毒网址的来源，百分之三十四点二出自美国，百分之三十点一出自中国大陆，而病毒程序中，百分之三十是在中国写的，其中又以特洛依木马型病毒占大多数，甚至有些病毒还会自我更新，让人防不胜防，这些病毒几乎都是利用使用者爱贪小便宜的心态及耸动人心的标题来使用户踏入陷阱，像是在非法网站下载音乐和影片、浏览不明的情色网站、开启不明的网址和信件…等，这些都极容易让计算机中毒的使用行为。

在公司里，有着众多的部门，部门里又有不少的员工，而每个员工所使用网络的行为及习惯也都大不相同，面对处于危机四伏的网络环境下，为了避免公司内部计算机因种种的使用行为而导致中毒，管理人员又该如何去一一防范、一一限制内部员工的网络使用行为呢？

对于无法一一去限制公司内员工的网络使用行为，一般处理的手法大多会选择于前端采购、架设防火墙来做为公司最前线的防护，但倘若单单只使用防火墙的话能力却也有限，在现阶段的网络世界里，依然是无法阻挡各地蜂拥而来的病毒。而若是于每台计算机上再加装防毒软件，每一期所需支付的软件费用则必然让老板大叹吃不消。为了能有效的将公司里的计算机做到完善的防护，必须额外采购的安全设备到底需要多少台才够？

这些让人头痛且烦人的问题就交给新软系统，新软系统所推出的“多功能 UTM-MS”系列产品将众多强大的功能整合为一体，公司只需架设一台就可抵多台使用，不需要再为了不同的防护机制而多浪费额外的采购成本，同时产品所内建之重量级防毒机制－双扫毒引擎 ClamAV、Sophos，可针对 SMTP、POP3、HTTP、FTP 加以防护，并且随时自动在线更新病毒码，让防毒的效能永远保持在最佳的状态，不用担心会错过任何更新病毒码的时机。

此外 MS 还拥有“应用程序管制”功能，不必担心员工不当的滥用公司网络，管理人员只要利用管制功能，不但可以轻松又准确的限制公司内部员工的网络使用行为，最为重要的是可降低病毒利用各种管道入侵的风险，也能有效的为公司带宽上减少不必要的浪费。加上 MS 还备有邮件上的各种安全机制及入侵防御的侦测功能，与内部异常流量的警示功能，以全方面的方式为公司内部打造一个最优质的网络环境，让公司可省下大量而且不必要的额外开销。

	新软多功能UTM	一般市售网络安全设备
采购成本	较低 （功能合一，一台抵多台）	较高 （必须适需求而分项购入多台）
额外支出(电费、维护费用)	低 （只需一台，节能又环保）	高 （多台机器较费电，相对的维护费用自然多）
设备整合相容性	完美整合 （完美整合成一台，完全不用考虑兼容性问题）	问题较多 （多台式的架设，兼容性较容易有影响）
操作、设定难易度	低 （使用单一接口，操控简单）	高 （多种接口，不易控制处理）
防毒效能	高 （采用双扫毒引擎，24 小时随时在线自动更新病毒码）	低 （单扫毒引擎，能力有限）

公司采购基本顾虑比较表

	新软多功能UTM	一般防火墙 及各式安全设备	每台计算机 安装防毒软件
架购成本	低(只需一台)	中	高
架设难易度	低	高	高
支持病毒更新	○	×	○
日後维护成本	低	高	高(需不断的支付使用费用)
控管使用者上网行为	○	×	×
全方面的病毒防护	○	×	×
内部异常流量警示	○	×（需管理人员主动查阅）	×
广告垃圾及病毒邮件的过滤与阻挡	○	需依功能购入相关防火墙设备	×（过於阳春，不敷使用）

防护功能比较表

除此之外 MS 还有更多的相关机制功能，让公司在不论是在防护、管理、使用方面都能无往不利，更可以轻松的处理内部网络所有大大小小的事，若欲了解更多、更详细的功能及规格欢迎请至：http://www. nusoft.com.tw/

文 陈殿鸿 kim@nusoft.com.tw