浅谈计算机网络病毒的防治措施

作者：西安外事学院　商娟叶

［摘要］　防治计算机网络病毒应该从基于工作站的防治技术和基于服务器的防治技术两个部分实施，一是软件防治；二是插防病毒卡；三是在网络接口卡上安装防病毒芯片。但是，计算机网络病毒的防治，单纯依靠技术手段是不可能十分有效地杜绝和防止其蔓延的，只有把技术手段和管理机制紧密结合起来，提高人们的防范意识，才有可能从根本上保护网络系统的安全运行。

［关键词］　网络；计算机病毒；程序；　防治

随着计算机在社会生活各个领域的广泛运用，计算机病毒攻击与防范技术也在不断拓展。据报道，世界各国遭受计算机病毒感染和攻击的事件屡屡发生，严重地干扰了正常的人类社会生活，给计算机网络和系统带来了巨大的潜在威胁和破坏。最近几年，出现了许多危害极大的邮件型病毒，如“LOVEYOU”病毒、“库尔尼科娃”病毒、“Homepage”病毒以及“求职信”病毒等，这些病毒主要是利用电子邮件作为传播途径，而且一般都是选择 Microsoft Outlook 侵入，利用 Outlook 的可编程特性完成发作和破坏。因此，防范计算机病毒已经越来越受到世界各国的高度重视。

计算机病毒是人为编制的具有破坏性的计算机程序软件，它能自我复制并破坏其它软件的指令，从而扰乱、改变或销毁用户存贮在计算机中的信息，造成无法挽回的损失。通过采取技术上和管理上的措施，计算机病毒是完全可以防范的。只要在思想上有反病毒的警惕性，依靠使用反病毒技术和管理措施，新病毒就无法逾越计算机安全保护屏障，从而不能广泛传播。

计算机网络中最主要的软硬件实体就是服务器和工作站，所以防治计算机网络病毒应该首先考虑这两个部分，另外加强综合治理也很重要。下面就从三个方面谈谈计算机病毒的防范措施：

一、基于工作站的防治技术

工作站就像是计算机网络的大门。只有把好这道大门，才能有效防止病毒的侵入。工作站防治病毒的方法有三种：一是软件防治，即定期不定期地用反病毒软件检测工作站的病毒感染情况。软件防治可以不断提高防治能力，但需人为地经常去启动软盘防病毒软件，因而不仅给工作人员增加了负担，而且很有可能在病毒发作后才能检测到。二是在工作站上插防病毒卡。防病毒卡可以达到实时检测的目的，但防病毒卡的升级不方便，从实际应用的效果看，对工作站的运行速度有一定的影响。三是在网络接口卡上安装防病毒芯片。它将工作站存取控制与病毒防护合二为一，可以更加实时有效地保护工作站及通向服务器的桥梁。但这种方法同样也存在芯片上的软件版本升级不便的问题，而且对网络的传输速度也会产生一定的影响。

下载防病毒软件要到知名度高、信誉良好的站点，通常这些站点软件比较安全。不要过于相信和随便运行别人给的软件。要经常检查自己的系统文件，注册

表、端口等,多注意安全方面的信息,再者就是改掉 Windows 关于隐藏文件扩展名的默认设置,这样可以让我们看清楚文件真正的扩展名。当前许多反病毒软件都具有查杀“木马”或“后门”程序的功能,但仍需更新和采用先进的防病毒软件。如果突然发现自己的计算机硬盘莫名其妙的工作,或者在没有打开任何连接的情况下 Modem 还在“眨眼睛”就立刻断开网络连接,进行木马的搜索。

二、基于服务器的防治技术

网络服务器是计算机网络的中心，是网络的支柱。网络瘫痪的一个重要标志就是网络服务器瘫痪。网络服务器一旦被击垮，造成的损失是灾难性的、难以挽回和无法估量。目前基于服务器的防治病毒的方法大都采用防病毒可装载模块(NLM)，以提供实时扫描病毒的能力。有时也结合利用在服务器上的插防毒卡等技术，目的在于保护服务器不受病毒的攻击，从而切断病毒进一步传播的途径。

邮件病毒主要是通过电子邮件进行传染的,而且大多通过附件夹带,了解了这一点,对于该类病毒的防范就比较明确和容易:

第一， 不要轻易打开陌生人来信中的附件,尤其是一些 EXE 类的可执行文件。

第二，对于比较熟悉的朋友发来的邮件,如果其信中带有附件却未在正文中说明,也不要轻易打开附件,因为它的系统也许已经染毒。

第三，不要盲目转发邮件。给别人发送程序文件甚至电子贺卡时,可先在自己的电脑中试一试,确认没有问题后再发,以免无意中成为病毒的传播者。

第四，如果收到主题为“I LOVE YOU”的邮件后立即删除,更不要打开附件。

第五，随时注意反病毒警报,及时更新杀毒软件的病毒代码库。从技术手段上,可安装具有监测邮件系统的反病毒实时监控程序,随时监测系统行为,如使用最新版本的杀毒实时软件来查杀该附件中的文件。

三、加强计算机网络的管理

计算机网络病毒的防治，单纯依靠技术手段是不可能十分有效地杜绝和防止其蔓延的，只有把技术手段和管理机制紧密结合起来，提高人们的防范意识，才有可能从根本上保护网络系统的安全运行。目前在网络病毒防治技术方面，基本处于被动防御的地位，但管理上应该积极主动。应从硬件设备及软件系统的使用、维护、管理、服务等各个环节制定出严格的规章制度、对网络系统的管理员及用户加强法制教育和职业道德教育，规范工作程序和操作规程，严惩从事非法活动的集体和个人。尽可能采用行之有效的新技术、新手段，建立”防杀结合、以防为主、以杀为辅、软硬互补、标本兼治”的最佳网络病毒安全模式。必须采取有效的管理措施和技术手段,防止病毒的感染和破坏,力争将损失降到最小。

计算机病毒在形式上越来越难以辨别，造成的危害也日益严重，这就要求网络防毒产品在技术上更先进，功能上更全面。从目前病毒的演化趋势来看，网络防病毒产品的发展趋势主要体现在以下几个方面。

一是反黑与杀毒相结合;二是从入口拦截病毒;三是提供全面解决方案;四是客户化定制模式;五是防病毒产品技术由区域化向国际化转变。

随着计算机网络、数字技术及互联网技术的发展，计算机病毒的危害更是与日俱增。因此，加强计算机病毒的防治、确保计算机信息安全是当前计算机应用过程中的一项重要、迫切的研究课题。我们一方面要掌握对现在的计算机病毒的防范措施，切实抓好病毒防治工作；另一方面要加强对未来病毒发展趋势的研究，探讨新时期科学防治计算机病毒的新策略，真正做到防患于未然。

[参考文献]

[1]陈立新. 计算机：病毒防治百事通[M]. 北京：清华大学出版社，2001
[2]电脑报. 2003 合订本. 北京：电子工业出版社，2003