

网络中计算机病毒传播的途径分析

作者：陕西教育学院 杨竞

[摘要] 网络计算机病毒传播途径有：电子邮件病毒传播途径；、网页病毒传播途径；利用系统漏洞，破解密码字典，攻击系统；木马病毒通过 MSN、QQ 等即时通信软件或电子邮件传播等。

[关键词] 网络；计算机病毒；传播途径

随着因特网技术的发展，计算机病毒的定义也在进一步扩大化，一些带有恶意性质的特洛伊木马程序，黑客程序和蠕虫程序等从广义角度也被归入计算机病毒的范畴。据国外统计，计算机病毒以 10 种/周的速度递增，另据我国公安部统计，国内以 4 至 6 种/月的速度递增。但是在与计算机病毒斗争的过程中，防范病毒的工具始终落后于计算机病毒的快速传播，不能自动防范未知病毒，也不能自动查杀未知病毒及正确自动恢复被这些新病毒感染的文件。所以当信息系统遭到病毒攻击时，科学地识别、防治计算机病毒，是我们从事这项工作要思考解决的问题。

一、计算机病毒起源和在网络中的传播

病毒不是偶然因素形成的，需要有一定的长度，病毒是人为的特制程序。1949 年，计算机之父约翰·冯·诺依曼在他的《复杂自动机组织》一书中提出了计算机程序能够在内存中自我复制，到 1983 年 11 月 3 日，美国计算机安全学科恩博士研制出一种在运行过程中可以复制自身的破坏性程序，伦·艾·德勒曼将它正式命名为 computervirus。1986 年初，在巴基斯坦的拉合尔，巴锡特和阿姆杰德两兄弟编写了 Pakistan 病毒，此病毒在一年内流传到世界各地。这是世界上第一例传播的病毒。此后，互联网出现，在增加人们信息交流的同时，也为病毒传播提供了便捷、快速的通道。据统计，1989 年 1 月，病毒种类不超过 100 种，而到了 2004 年 5 月其病毒的总数已超过 8 万种，而且有快速增长的趋势。病毒传播是一种动态行为，目前人们提出基于免疫防御的模型，还仅仅考虑了静态的免疫行为，很难使病毒传播之前将网络中一小部分计算机进行预先免疫。所以目前降低计算机病毒传播速度和阻止病毒的爆发处于被动地位。

二、网络计算机病毒的本质

病毒是一种可以通过修改某些程序以达到感染该程序目的的程序。修改操作可能包括复制病毒程序，之后去感染其他程序。典型的网络病毒通过用户打开网页进入系统之后将驻留其中，感染病毒后的计算机和其信息系统进行交互时，病毒的副本就会进入新系统，网络计算机病毒就这样通过网络传播开来，由于网络环境下访问其他计算机时，可能会盗取用户计算机上的重要信息如帐号、密码等。

1、网络中的良性计算机病毒

良性病毒是不包含有立即对计算机系统产生直接破坏作用的代码。这类病毒只是不停地进行扩散，通过网络从一台计算机传染到另一台，并不破坏计算机内的数据。有时系统内还会出现几种病毒交叉感染的现象，一个文件不停地反复被



几种病毒所感染，整个计算机系统也由于多种病毒寄生于其中而无法正常工作。因此也不能轻视所谓良性病毒对计算机系统造成的损害。网络中良性病毒发作为：自动打开网页，显示特殊文字和图像；可用磁盘空间变小，上网速度缓慢；病毒程序迫使 CPU 执行无用的大量垃圾程序，使得系统始终处于忙碌状态，打不开 IE，进程显示 CPU 使用 100%；QQ 信息显示异常，或者出现异地登陆。

2、网络中的恶性计算机病毒

网络中恶性病毒的破坏性较严重，通常恶性病毒通过使用用户打开网页，攻击计算机系统，会导致管理员重做系统。恶性病毒是在其代码中包含有损伤和破坏计算机系统的操作，在其传染或发作时会对系统产生直接的破坏作用。这类病毒是很多的，硬盘的扇区将被彻底破坏，使整个硬盘上的数据无法被恢复，造成的损失是无法挽回的。网络中恶性病毒发作现象：上网后再次开机操作系统无法正常启动，开机后是黑屏；陌生人发来的电子函件，例如求职信，这种病毒传播速度是一小时内全世界可以造成该病毒爆发；普通邮件病毒的传播速度是一天内爆发；自动链接到一些陌生的网站；启动杀毒软件，不能查找出病毒。

三、网络病毒传播途径

1、电子邮件病毒传播途径。恶意软件的一个发展是电子邮件病毒出现，第一个广泛传播的电子邮件病毒 **Melissa** 病毒。该病毒使用了 **Microsoft Word** 宏，并嵌在电子邮件病毒中。如果邮件接收者打开了该附件，**Word** 宏就被激活，之后电子邮件病毒搜寻用户通信簿的邮件列表，并把自身发送到邮件列表中的每一个地址；病毒进行一些对本地有危害性的操作。常见的电子邮件病毒有合作单位或个人通过 **E-mail** 上报、**FTP** 上传、**Web** 提交都会导致网络病毒传播。

2、利用系统漏洞，破解密码字典，攻击系统。有些大型、中型系统使用的的每台计算机设置相同密码，或者相似密码，对于帐号选用较为相同的口令。那么这就容易造成这些计算机密码容易集体遭遇破坏，许多网络就是通过空密码或者弱密码来攻击用户机器的，也就是通过破解密码字典猜测用户机器管理员密码的方式攻击系统，因此使用较为复杂的密码，能有效降低计算机的病毒感染率。

3、木马病毒通过 **MSN**、**QQ** 等即时通信软件或电子邮件传播。有时候频繁的打开即时通讯工具传来的网址、来历不明的邮件及附件、到不安全的网站下载可执行程序等，就会导致网络病毒进入计算机。现在很多木马病毒可以通过 **MSN**、**QQ** 等即时通信软件或电子邮件传播，一旦你的在线好友感染病毒，那么所有好友将会遭到病毒的入侵。

4、网页病毒传播途径。网页病毒主要是利用软件或系统操作平台等的安全漏洞，通过执行嵌入在网页 **HTML** 超文本标记语言内的 **Java Applet** 小应用程序，**JavaScript** 脚本语言程序，**ActiveX** 软件部件网络交互技术支持可自动执行的代码程序，以强行修改用户操作系统的注册表设置及系统实用配置程序，或非法控制系统资源盗取用户文件，或恶意删除硬盘文件、格式化硬盘为行为目标的非法恶意程序。这种非法恶意程序能够得以被自动执行，在于它完全不受用户的控制。一旦浏览含有该病毒的网页，在用户不知不觉的情况下，给用户的系统带来一般性的、轻度性的、恶性等不同程度的破坏。网页病毒的激发条件是浏览网页，网页的浏览量直接影响病毒传播的速度，网页的浏览量宏观上是随着时间的增加而增加的。

以上通过对网络中计算机病毒的起源、历史、类型以及发展趋势的全面分析，对网络中计算机病毒简要的描述，其目的是帮助人们对网络计算机病毒有一个了解和认识，从而为计算机病毒的防范提供理论依据。

[参考文献]

[1]计算机病毒的种类!清除方法及防治策略,纪勇,中国媒介生物学及控制杂志[J],2005(6)



[2]计算机病毒数据库及其信息管理平台的设计与实现, 张引, 计算机工程与应用[J], 2005 (7)

[3]高效电子阅览室计算机病毒防治, 杨竞, 兰台世界[J], 2008 (9)

[作者简介]

杨竞, 女, 1981年生, 硕士, 助理工程师。

