浅析计算机病毒知识与防治

吉林工商学院　董大伟

【摘要】随着计算机应用越来越广泛，计算机病毒已经渗透到各个领域，本文主要介绍计算机病毒知识和防范措施与方法。

【关键词】计算机应用；病毒；防范

随着社会信息化的迅速发展，尤其自Internet和Internet应用发展以来，计算机病毒也日益猖獗，每年都会有几十万甚至上百万种病毒产生。一些病毒给人们日常生产生活带来了很大的困扰，甚至已经涉及到国家主权等许多重大问题。如何预防计算机病毒的感染和发作，将计算机病毒的危害降到最低，已经是迫在眉睫的事情了。

一、计算机病毒相关知识

1. 计算机病毒的定义

计算机病毒有很多种定义，从广义上讲，凡是能引起计算机故障，破坏计算机中数据的程序统称为计算机病毒。我们可以理解为：计算机病毒就是能够进行欺骗、自身复制、传染并具有破坏性的指令集合或一组程序。

在这里我们可以看出来，计算机病毒也是计算机程序，不是所有的计算机程序都是病毒，必须要满足一定条件的计算机程序才可以称为计算机病毒。

2. 计算机病毒特点

(1)寄生性：计算机病毒寄生在其他程序之中，当执行这个程序时，就会激活计算机病毒进行破坏，通常计算机病毒不易被人发现。

(2)传染性：计算机病毒不但本身具有破坏性，更有害的是具有传染性，并且传染速度非常快。

(3)潜伏性：计算机病毒一般都能潜伏在计算机程序中，当时机成熟，就会激活计算机病毒，对系统或应用程序与数据进行破坏。

(4)隐蔽性：计算机病毒具有很强的隐蔽性，有的可以通过杀毒软件检查出来，但更多的病毒是查不出来的，所以处理起来通常很困难。

3. 计算机病毒的产生

1983年11月3日美国计算机专家费雷德·科恩通过美国安全局的计算机进行实验，制造了第一例计算机病毒。从那一时刻起，计算机病毒不段发展，新病毒种类不断出现，并随计算机网络的发展而不断蔓延，给人类的生产、生活带来极大的困扰。

4. 计算机病毒迅速发展的原因

计算机病毒之所以发展如此迅速，破坏性如此之大，主要有以下几个原因：

(1)系统开放性。

(2)网络的迅速发展，1988年病毒入侵Internet。

(3)软件的防盗版。

(4)计算机专业人员或业余爱好者的恶作剧。

(5)科研变性。

(6)利益驱使。

(7)个人的报复情绪。

5. 计算机病毒的表现形式

计算机受到病毒感染后，会表现出不同的症状，出现以下症状，就要考虑机器是否中了病毒，并进行查杀。

(1)计算机不能正常启动。

(2)运行速度降低。

(3)磁盘空间迅速变小。

(4)计算机经常死机或重新启动。

(5)帐号不能登录。

(6)文件打开异常。

(7)文件容量增加等等。

6. 经典的计算机病毒

(1)1986年巴基斯坦两兄弟编写的“巴基斯坦智囊”。

(2)1987年耶路撒冷希伯莱大学的学生编写的“黑色星期五”。

(3)1998年中国台湾的陈盈豪编写的“CIH1.4”。

(4)1999年美国的史密斯编写的“美丽莎”。

(5)2004年德国的斯万-贾斯查因编写的“震荡波”。

(6)2006年中国湖北武汉的李俊编写的“熊猫烧香”等。

二、计算机病毒的防范对策和方法

病毒的繁衍方式、传播方式不断地变化，在目前的计算机系统环境下，特别是对计算机网络而言，要想完全杜绝计算机病毒的复制传染几乎是不可能的，因此，我们必须以防范为主。防范计算机病毒的侵入应该遵循一些规则，下面就对这些规则做以简单的介绍。

1. 在计算机上安装正式版本的反病毒软件，并要经常升级

计算机上安装了反病毒软件，计算机系统的安全性相对有所提高，就算不能完全防止病毒的袭击，但对于大多数的计算机病毒都可以见之杀之，从而保证计算机系统的安全性。由于每天都有新的计算机病毒产生，对于安装的反病毒软件，要经常地更新病毒库来保证反病毒软件可以查杀最新的病毒，以最大限度地发挥出反病毒软件应有的功能。

2. 备份系统和用户的重要的数据和文件

为了保证计算机内系统和用户重要数据的安全，要养成定时备份的好习惯。即使在使用计算机的过程中受到病毒的入侵，有些重要的文件遭到破坏甚至系统瘫痪，我们也可以通过备份过的文件恢复当初。对于系统的数据和文件，备份工作有很多种，我们常用的方式就是使用ghost备份系统，可以把系统完整备份到一个独立的分区，备份完成后再把分区隐藏，或者直接通过移动硬盘拷贝出来。对于用户的数据和文件，我们可以通过移动存储设备拷贝出来，或是使用刻录机直接刻录成CD数据或DVD数据。

3. 对外来存储设备中数据的使用都应该先进行查杀计算机病毒

外来的存储设备主要包括U盘、移动硬盘和光盘，由于U盘和移动硬盘的便携性，很多人都喜欢使用U盘和移动硬盘来相互拷贝数据，在这些设备连接计算机之后不要着急打开，首先要使用杀毒软件进行查杀，确认无误之后再正常使用这些设备，并且要保持这种习惯。

4. 安全使用网络上的软件与数据

现在很多浏览器都带有检测网站安全的功能，我们在登录网络的时候应该多使用这样的浏览器，在确保网站安全之后，我们从互联网下载任何软件或数据时也应该小心注意，对于需要修改注册表的操作，请不要轻易选择确定，对于要求下载插件，也要小心操作。

5. 谨慎使用电子邮件

现在由于人们对于邮箱的使用越来越广泛，电子邮件交换数据的方式越来越普及，很多不明邮件或者广告邮件里都链接了计算机病毒，而这些病毒很隐蔽，并不容易被发现。因此我们在接收邮件时一定要仔细，不是所有的链接都可能点击的，在不确定的情况下，不要打开电子邮件，不要打开陌生人发来的电子邮件，同时也要小心处理来自于熟人的邮件附件，提防带有欺骗性质的病毒警告信息。

6. 及时修复系统软件漏洞，定期更新操作系统

我们知道很多编写计算机病毒的人更多的都是利用了系统的漏洞，漏洞永远是攻击者最喜欢使用的攻击方式，当前各种各样的安全漏洞给网络病毒开了方便之门，其中影响最大的是windows操作系统漏洞、office漏洞、SQL漏洞、IIS漏洞、IE漏洞，还有其它应用软件，如播放器、QQ、迅雷，甚至杀毒软件等。我们平时除了注意及时对系统软件和网络软件进行必要升级外，还要利用WindowsUpdate功能为操作系统的各种漏洞打上最新的补丁。

三、结束语

计算机病毒已无处不在，它通常是利用系统的弱点进行攻击，对于计算机病毒的防范不是一两个人就可以实现的，应该是一个社会性的工作，只有全社会都提高认识，从管理制度和技术两个方面进行防范，才能将计算机病毒的危害降到最低。

参考文献

[1]韩筱卿,王建锋,钟玮.计算机病毒分析与防范大全[M].电子工业出版社,2006.

[2]张仁斌,李钢,侯整风.计算机病毒与反病毒技术[M].清华大学出版社,2006.

[3]马宜兴.网络安全与病毒防范(第二版)[M].上海交通大学出版社,2005.

[4]杜彩月.网络时代的计算机病毒特征与防治[J].河南气象,2006(1).

[5]唐运平.计算机病毒的特征与防治[J].电子工程师,1995(4).