Computer Virus Prevention from the Perspective of Quality Management

Leilei Zhao[1, a], Tiejun Ci[1, b] and Yingxue Li[2, c]

[1]School of Energy Power and Mechanical Engineering, North China Electric Power University, Baoding, China, 071003

[2]School of Environmental Science and Engineering Department, North China Electric Power University, Baoding, China, 071003

[a]2773754282@qq.com,[b]cjt920@126.com, [c]602497168@qq.com

Keywords: Computer virus; Precaution; Quality management; Relationship graph

Abstract. With the deepening degree of information technology, network technology and the rapid development of computer virus outbreaks it provides an effective way to spread. From time to time by the computer virus attacks, seriously affect the normal operation of the computer. Computer viruses have the unique ability to replicate and destructive computer viruses and constantly updated virus variants emerging. Only technically complete protection against viruses is not realistic. From the current situation of computer virus infection, the use of quality management and technical controls a combination of methods to explore prevent computer viruses.

基于质量管理的计算机病毒预防

赵蕾蕾[1,a]，慈铁军[1,b]，李颖雪[2,c]

1. 华北电力大学(保定) 能源动力与机械工程学院 机械工程系，河北省保定市 071003

2. 华北电力大学(保定) 环境科学与工程学院 河北省保定市 071003

[a]2773754282@qq.com, [b]cjt920@126.com, [c]602497168@qq.com

摘要：随着信息化程度不断加深，网络技术迅速发展为计算机病毒的大规模爆发提供了有效的传播途径，电脑时不时地受到病毒的侵袭，严重影响电脑的正常运行。计算机病毒有独特的复制能力与破坏性，并且计算机病毒库在不断更新，病毒变种不断出现，单从技术上彻底防御病毒是不太现实的。本文从电脑侵染病毒的现状，运用质量管理和技术控制相结合的方法探讨计算机病毒的预防。

关键词：计算机病毒；预防措施；质量管理；关联图

1. 前言

计算机病毒是指编制者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组恶意计算机指令或者程序代码。随着网络的出现，病毒传播媒介从移动式载体转移到以网络为主，病毒也从单机病毒发展到网络病毒。随着网络的迅速发展，计算机病毒及其病毒变种越来越多，而且因为网络的开放性．所以计算机病毒的传染能力更强，破坏力更大。单从技术上彻底防御病毒是不太现实的。本文将以电脑侵染病毒的现状为出发点，运用质量管理和技术控制相结合的方法探讨计算机病毒的预防。

2. 计算机侵染病毒现状调查

为了弄清电脑侵染病毒的现状，我们通过网络发放问卷，调查对象主要集中在各大高校的大学生群体，以及一些企事业单位的工作人员。经过一个月的调查，一共收回调查表 1912 份，其中有效调查表共收回 1986 份，并按照项目分类进行统计见表 1。

表 1 电脑侵染病毒方式统计表

侵染方式	频数	频率
硬盘之间的数据复制	3	0.06%
使用盗版光盘上的软件和游戏	493	9.86%
点入电子邮件中携带病毒的链接	43	0.86%
浏览网页时点入危险链接	1331	26.63%
不小心向光盘上刻录带毒文件	2	0.04%
下载的软件、网络游戏里携带病毒	1103	22.07%
使用即时通讯软件时侵染（QQ、P2P 等）	529	10.58%
玩网络游戏时侵染	151	3.02%
使用移动硬盘、U 盘等移动设备时侵染	1217	24.34%
使用公共无线局域网时侵染	127	2.54%
合计	4999	100%

3. 使用分层法按照传播途径进行分类

经过调查发现，在实际计算机使用过程中影响其中病毒的因素有很多，而且很多影响因素的概率都很相近，如果不把这些因素区别开来就难以看出变化的规律，不利于以后的分析与措施的制定。通过分析研究发现病毒主要通过不可移动的计算机硬件设备、移动存储设备、计算机网络、点对点通信系统和无线传播等传播方式侵染计算机。所以将使用分层法，将这些影响因素按照其传播途径进行分层。如下：

表 2 综合分层的电脑侵染病毒统计表

传播途径	侵染方式	频数	累计频数	频率	累计频率
利用计算机网络进行传播	点入电子邮件中携带病毒的链接	3157	3157	63.16%	63.16%
	浏览网页时点入危险链接				
	下载的软件、网络游戏里携带病毒				
	使用即时通讯软件时侵染（QQ、P2P 等）				
	玩网络游戏时侵染				
通过移动存储设备来传播	使用盗版光盘上的软件和游戏	1710	4867	34.2%	97.36%
	使用移动硬盘、U 盘等移动设备时侵染				
点对点通信系统和无线传播	使用公共无线局域网时侵染	127	4994	2.54%	99.90%
不可移动的计算机硬件设备进行传播	硬盘之间的数据复制	5	4999	0.10%	100%
	不小心向光盘上刻录带毒文件				
	合计	4999	4999	100%	100%

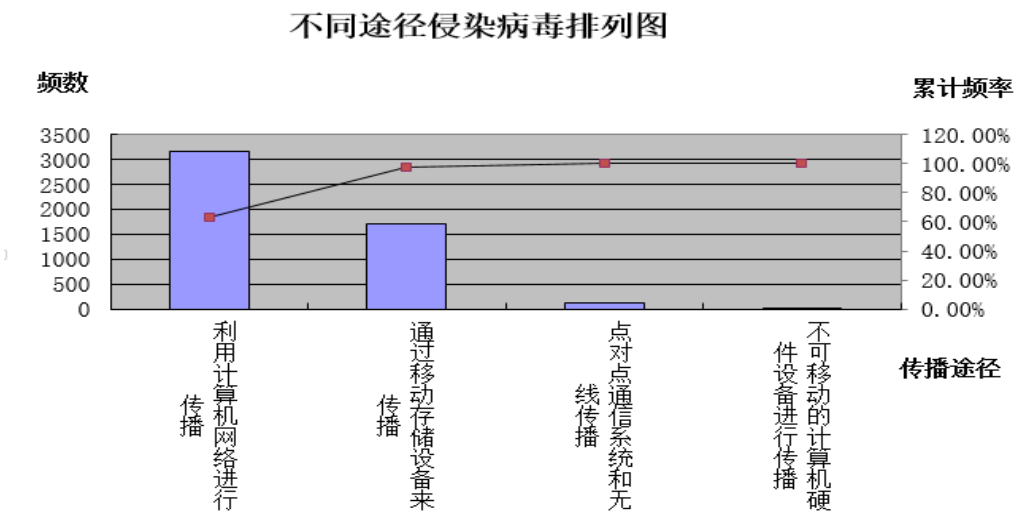

图 1 不同途径侵染病毒排列图

病毒主要通过计算机网络和移动设备进行传播，所以从这两个方面采取具体措施，预防计算机病毒的侵染。

4. 利用关联图进行原因分析

关联图是表示事物依存或因果关系的连线图。把与事物有关的各环节按相互制约的关系连成整体，从中找出解决问题因从何处入手。用于搞清各种复杂因素相互缠绕、相互牵连等问题，寻找发现内在的因果关系，用箭头逻辑性的连接起来，综合地掌握全貌，找出解决问题的措施。

针对病毒通过计算机网络以及移动存储设备传播这两方面的原因利用关联图做如下分析：

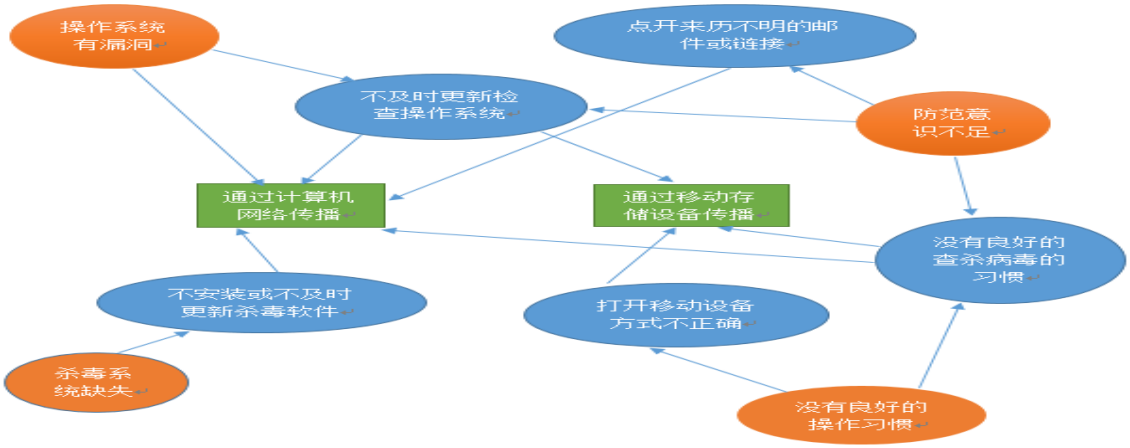

图 2 因素关联图

根据箭头只进不出是问题，只出不进是主要因素，有进有出是中间因素，出多于进的中间因素是关键中间因素的判断原则，发现影响所研究问题的主要因素是： 防范意识不足、杀毒系统缺失、操作系统有漏洞、没有良好的操作习惯。

5. 根据主要因素制定对策

5.1. 针对防范意识不足采取措施

（1）不打开来历不明的邮件

不要打开一些来历不明的邮件，最主要的是不要下载其附件并运行。正确的步骤是：点击邮件标题，看看邮件附件的类型。如果附件是可执行文件(文件后缀名为 exe，vbs 等)，很可能是病毒，要做的唯一操作就是直接删除。

（2）不要因为好奇点开不明链接

不要上一些不太了解的网站。更不要因为好奇点击一些奇怪有风险的链接。

（3）小心使用公共局域网，公共场合上网不要留下个人信息

局域网是由相互连接的一组计算机组成的，这是数据共享和相互协作的需要。组成网络的每一台计算机都能连接到其他计算机，数据也能从一台计算机发送到其他计算机上。如果发送的数据感染了计算机病毒，接收方的计算机将自动被感染，因此，有可能在很短的时间内感染整个网络中的计算机。利用他人的电脑或者在公共场合上网，不要让系统记下个人信息，或者在完成以后要删掉这些个人信息。

（4）使用正版软件

使用正版软件，不要从一些小型的网站上下载软件，那样的网站中的软件经常携带病毒，当软件安装运行时，病毒将会执行，导致电脑中毒。我们要尽量购买官方的正版杀毒软件，因为盗版软件粗制滥造，甚至本身就带有病毒。盗版杀毒软件不能正常升级，不能及时的更改病毒库，不能掌握最新的杀毒信息。

5.2. 针对杀毒系统缺失采取措施

（1）安装杀毒软件进行实时监控

杀毒软件安装成功并启用后，就会自动进行查毒和杀毒。它会对病毒实时监控，任何程序或文件在被调用之前，都先被过滤一遍。一旦有病毒侵入，反病毒就报警，并自动杀毒，将病毒拒之门外。

（2）及时更新杀毒软件

因为电脑病毒为人工编写的程序，所以新的病毒已经病毒的变种经常出现，我们要经常对杀毒软件进行升级，及时地更新病毒库，掌握最新的杀毒信息。

（3）设置病毒过滤器

病毒过滤器通常又称防毒卡。病毒过滤器是将软件的思想用硬件来实现，利用硬件设备在系统运行的过程中来防止电脑病毒入侵系统。

5.3. 针对操作系统有漏洞采取措施

（1）对系统进行必要的检查

对新来的电脑应先对操作系统内部进行病毒检查，防止病毒潜伏，以后被激活，造成损失。对正常使用的电脑，也要定期检查操作系统。

(包括软件系统)要定期进行病毒检测

（2）正确安装操作系统

正确安装计算机操作系统，是做好计算机安全防范的基础。安装使用较新的正版系统软件，在安装的过程中要断开网络，避免在安装过程中感染病毒;还要设置好超级用户的密码并且再设置一个口常使用的用户帐号。操作系统安装完后，可以马上设置网络连接，然后通过互联网更新最新的系统补丁，因为最新的系统补丁通常可以弥补系统中被发现的安全漏洞。

（3）及时升级更新操作系统

系统补丁是系统生产商等根据系统在运行的过程中发现的漏洞而设计的修复程序，及时安装系统补丁能够有效地避免黑客利用系统漏洞而对系统进行的攻击，从而保障计算机系统以及网络信息的安全。

5.4. 针对没有良好的操作习惯采取措施

（1）对移动设备经常性杀毒

移动存储设备携带方便，使用广泛、移动频繁，因此成了计算机病毒寄生“温床”。所以要经常性对 U 盘等移动存储设备进行杀毒。

（2）不插入有风险的电脑

对于有未知风险的电脑不要随意插入移动存储设备。

（3）应用资源管理器的方式打开

不要直接双击打开移动存储设备，而应选择住盘符，单击右键，在弹出的菜单中选“打开”或“资源管理器”，打开移动存储设备。

6. 总结

计算机病毒在不断的更新，预防计算机病毒是一项长期而又艰巨的任务。将质量工程中的方法运用到计算机病毒预防中，从纵向上规范预防病毒侵染过程与措施，一定程度上完善了预防计算机病毒的理论体系，可以保证计算机病毒防御工作规范开展。基于全面质量管理的基本理念和着眼于解决当前计算机防御实际中存在的问题。将质量管理原理理念运用于计算机病毒防御系统也是管理科学与计算机技术有机统一的体现。

参考文献

[1] 刘永新. 电脑病毒的特征及预防[A], 河南科技, 2013.NO.06

[2] 钱林红.个人计算机信息安全的防护方法[A], 信息技术, DOI10.13751/j.cnki. kjyqy.2013.17.270

[3] 冯建成. 高校多媒体教室移动存储设备病毒防治[A], 赤峰学院学报(自然科学版), Vo.27 No. 6 Jun. 2011

[4] 陈岭.计算机网络信息安全及防护技术[A], 技术探讨, 第 5 卷 第 20 期 2015 年 7 月

[5] 张磊.初探计算机病毒及其预防和处理措施[A], 电脑知识与技术, Vo1.9. No.26, Setptember 2013

References

[1] Yongxin Liu. Characteristics and prevention of computer viruses [A]. Journal of Henan Science and Technology. 2013.NO.06

[2] Linhong Qian. Personal computer information security protection methods [A]. Information Technology. DOI10.13751/j.cnki. kjyqy.2013.17.270

[3] Jiancheng Feng. College Multimedia Classroom virus control removable storage devices [A].

[4] Journal of Chifeng University (Natural Science Editior). Vo .27 No. 6 Jun. 2011

[5] Ling Chen. Computer network information security and protection technology [A]. Technology Discussion. Volume 5, 20 July 2015

[6] Lei Zhang. Of computer viruses and their prevention and treatment measures [A]. Computer Knowledge and Technology. Vo1.9,No.26,Setptember 2013