计算机病毒工作机理分析及检测预防

刘仲义,朱江东

(西昌学院　信息技术系,四川　西昌　615013)

【摘　要】本文从计算机病毒起源和日益增多的原因分析及其危害入手,分析阐述了病毒的工作机理、常用的病毒检测方法与预防措施。

【关键词】病毒编写原因;危害;工作机理;检测技术;预防措施

【中图分类号】TP309.5　　【文献标识码】A　　【文章编号】1673-1891(2007)03-0068-05

一 病毒的起源

计算机技术发展的历史几乎就是病毒发展的历史,美国是计算机病毒的起源地。早在 1949 年,计算机之父冯·诺依曼在《复杂自动机组织论》中便提出了计算机病毒的概念——即是一种"能够实际复制自身的自动机"。1960 年,美国的约翰·康维在编写"生命游戏"程序时首先实现了程序自我复制技术。80 年代初贝尔实验室的三位年轻程序员也受到冯·诺依曼理论的启发,编写了"磁心大战"游戏,游戏双方编制许多能自身复制,并可保存在磁心存储器中的程序,双方的程序在指令控制下就会竭力去消灭对方的程序,这种有趣的游戏很快就传播到其它计算机中心。由此我们可以看到计算机病毒最初起源于一些攻击性的游戏。1983 年 11 月 3 日在计算机安全学术讨论会上弗莱德·科恩(Fred Cohen)提出计算机病毒(Computer Viruses)的概念,与会专家在运行 UNIX 的 VAX11/750 机型上实验成功第一个病毒,一周后演示了另外 5 个病毒。

二 现今病毒日益增多的原因分析及其危害

现今计算机病毒编写的原因由早期的开玩笑、恶作剧、表现高智商、炫耀技术能力、报复等因素发展成为商业经济利益趋动下的恶意攻击性武器,以非法牟利为目的的病毒产业链正逐步形成。开发工具由早期晦涩复杂的汇编程序语言发展到简单易用的高级语言编写(如用 VB、VBscript、JAVA、VC、DELPHI 等,2006 年的病毒魁首"熊猫烧香"木马病毒就采用 DELPHI 编写),并采用 Activex 等当前最新的编程技术以及各种功能强大的"病毒生产机"等软件自动生产出大批量的同族变种新病毒,例如威金病毒最多一天竟然有 292 个不同的变种。病毒制造人员也由早期的精通计算机工作原理的专业程序设计师退变成通晓一门高级语言并学习了病毒开发方法的软件工人,网络上病毒开发案例教程比比皆是,有一定编程基础的非计算机专业人员也不难学会。开发过程变得如此简单快捷,开发人员素质要求不是太高,高经济利润的追求,相关法律制约发展滞后,用户使用的操作系统等软件自身的缺陷以及电脑用户防范意识不强、消防技术有限,杀毒软件的更新速度以及清除病毒的复杂性永远落后于病毒更新的超前性和多样性,病毒网络传播的迅捷性最终导致电脑病毒的感染率呈爆炸式增长,网络经济犯罪率不断增加。

据江民科技 1 月 10 日发布的 2006 年计算机病毒疫情报告显示,2006 年江民反病毒中心共截获新病毒 60383 种,较 2005 年增长 56%。据江民病毒预警中心统计的数据,2006 年全国共有 19319658 台计算机感染了病毒,感染计算机病毒种类为 66606 种。计算机病毒可造成电脑用户计算机资源浪费,破坏用户的数据资料,删除文件,非法格式化用户磁盘,使用户电脑内存减少,运行效率降低,频繁死机,机器瘫痪,盗取用户信息和网络财富,攻击网上银行,甚至有些病毒直接破坏电脑硬件,严重地影响到

收稿日期:2007-05-12

作者简介:刘仲义(1970-　),男,计算机实验师,主要从事计算机应用技术研究与教学。

电脑用户的工作、学习和生活，对社会造成巨大的经济损失。1999 年 4 月 26 日爆发的 CIH 计算机病毒，对全球造成 10 亿美元的损失。2000 年 5 月 4 日，“爱虫”计算机病毒在世界各地迅速蔓延，更大规模地发作，造成全世界空前的计算机系统被破坏，损失高达 100 亿美元。2006 年 12 月大规模爆发的感染型蠕虫病毒“熊猫烧香”，造成的危害堪称严重。据统计，仅国内就有上百万台电脑遭受感染，数以千计的企业受到侵害，对网络世界的影响，不逊色于恐怖分子对美国的袭击进而对全球经济造成的影响。因此逐步走向信息化、网络化的今天，了解计算机病毒工作机理、提高防毒意识、掌握检测与防治的常用方法已成为每一位电脑用户的必修课。

三 病毒的工作机理

病毒按破坏性可分为良性病毒和恶性病毒；按传染方式分为引导型病毒、文件型病毒、系统引导与文件复合型病毒；按链接方式分为源码病毒、入侵病毒、操作系统病毒和外壳病毒。病毒短小精干，具有隐蔽性、传染性、潜伏性、可激发性、破坏性、针对性、主动攻击等特性。尽管计算机病毒种类繁多层出不穷，机理和组成千奇百怪，但病毒主要部分是相同的，工作逻辑也大同小异。计算机病毒程序主要由引导模块、传染模块和表现模块组成。传染模块有传染条件判断段和传染段两个程序段；表现模块有表现条件判断段和表现段两个程序段。计算机病毒的工作逻辑大致可划分为四个过程：引导过程、执行过程、表现（或破坏）过程和传染过程。

（一）病毒程序的引导过程

任何计算机病毒都是一个可执行的程序。它们平时存放在外存上，病毒的引导过程即是病毒程序从外存装入内存的过程。一个病毒如果没有引导过程就无法执行，更不能继续传染和破坏计算机系统，从而丧失生命力，因此病毒利用自身隐蔽性依附在系统文件或用户程序和文件中，随着这些程序一起装入内存，并窃取系统的控制权，窃取部分内存并驻留内存，监视整个系统运行，当激发条件满足时实施传染或破坏。病毒的隐蔽性主要表现在其本身为机器码，与正常程序耦合在一起。特别是有些病毒对自身采用自加密技术，并且具有反跟踪的功能，以躲避杀毒软件的查杀和实时监控程序的跟踪；有些病毒能够关闭一些安全软件的进程，由于可以关闭安全软件，从而使自我保护不好的杀毒软件自身也受到攻击。

（二）病毒程序的执行过程

病毒引导装入内存后，首先窃取系统控制权，病毒运行后，完成对系统的修改等非授权性操作，然后才把控制权交给宿主程序，再执行用户所要求的操作。

（三）病毒程序的表现过程

病毒驻留内存后，当有程序装入内存执行或有读写磁盘操作时，它时刻判断是否满足表现（破坏）条件，一旦满足即启动其表现（破坏）模块，进行破坏活动。

（四）病毒程序的传染过程

病毒在程序运行、文件操作、网络操作等过程中首先运行传染条件判断段代码判断传染条件是否满足，如果满足则执行传染段代码进行传播行为，从而使得病毒能不断繁衍和传播。

四 常用病毒检测技术

（一）直接检测法

计算机病毒入侵计算机系统后将使其系统内部发生某些变化，并在一定条件下表现出来，因而可通过直观现象判断系统是否感染病毒。以下是一些病毒感染时的可疑症状或肯定症状，需确定时，可对计算机系统作进一步检测。

1. 计算机启动速度明显变慢，系统引导时间比平时明显增长。

2. 计算机运行速度明显变慢，运行软件（如 Word）的速度比平时明显要慢，就连打开文件夹也可能很慢。

3. 计算机开机自检能通过并出现自检结果画面，但系统不认识磁盘，硬盘不引导系统或引导时出现死机现象。

4. 频繁出现内存不够或虚拟内存不足提示，而察看虚拟内存设置空间又足够。

5. 系统频繁死机。

6. 磁盘上出现了不正常的坏簇，坏簇莫名其妙地增多。这有可能是病毒为了保护自己而对保存病毒程序的扇区做出的标志，故可在 DOS 方式下用 winnt \ system32 \ chkdsk 命令查看坏扇区和校验文件、索引等情况。

7. 磁盘上发现有特殊标记或引导扇区、卷标等

信息被修改，用分区软件查看分区总容量和超过100%。

8. 文件莫名其妙地丢失或被篡改。如‘熊猫烧香’病毒会删除扩展名为GHO的系统备份文件。

9. 平时能够正常运行或打开的文件在运行时出现死机或根本无法正常运行或打开。

10. 文件无法执行正常写盘操作，如正在编辑的word文档无法存盘。

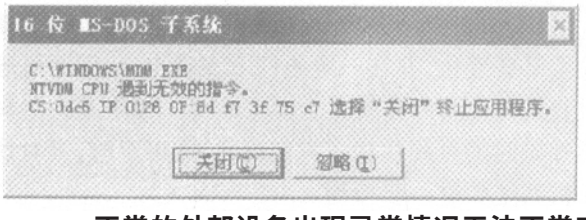
11. 磁盘可用空间无法使用。剩余空间有几个G但总提示剩余空间不足无法保存文件。

12. 系统自动生成一些特殊文件。如‘熊猫烧香’病毒感染后在磁盘根目录出现autorun自运行文件，可执行文件图标被改成熊猫烧香图样。双击桌面word快捷方式图标结果桌面又出现一个word.exe新图标。每打开一个文件夹就有新文件产生等。

13. 可执行文件长度、文件属性、日期、时间等属性发生变化。

14. 蜂鸣器发出异常的声音和音乐。

15. 屏幕有规律地出现一些无意义不正常的画面或信息，这往往是一些病毒的表现症状。例如下图所示信息。



16. 正常的外部设备出现异常情况无法正常工作。如打印机只打印奇怪字符或无法连通。

17. 异常的外部设备访问。程序没有使用外部设备时，系统却非法使用外部设备。

18. 异常的磁盘访问。如用word写文稿时，软驱中无软盘但软驱灯不时闪亮并听见电机转动声音。光盘已正常退出，屏幕始终提示光驱未准备好。未进行格式化操作硬盘就自动格式化等。

19. 直接用debug调试可疑文件，查找病毒特征码。

(二)检测内存空间法

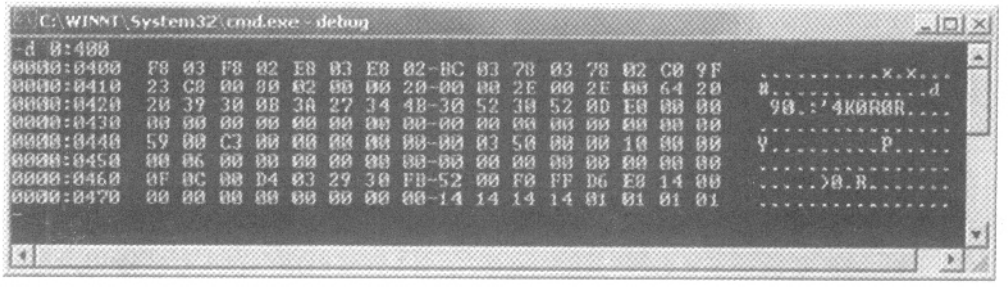
当计算机染毒后，由于病毒具有传染性，因而在引导或执行病毒程序时要申请一定的内存空间，然后常驻内存，监测系统运行，待机进行传染、攻击或发作。为避免用户程序或数据把在内存中的病毒程序覆盖掉，病毒程序一般把自己放入内存高端，然后使系统可用内存减少，使用户程序和数据无法使用到病毒所占用的内存区，从而起到保护自身的作用。因此我们可以通过检测内存变化的方法来检测计算机系统是否染毒。以下是几种检测内存的方法：

1. 用mem命令查看内存

在Windows的MS-DOS方式下，运行mem命令查看内存容量，基本内存如不是655360B(即640KB)则肯定有病毒(注意个别品牌电脑因开辟硬盘数据区等原因而占用1KB或2KB空间，因此未染毒时就应清楚所用电脑的基本属性)

2. 用DEBUG进行检测

在Windows的MS-DOS方式下，运行debug调试命令，用D命令显示0:0413H和0:0414H两字节的内容，内存系统检测的结果如下图所示



图中0:0413H和0:0414H字节中显示的内容分别为80和02，即为十六进制数的0280H，换算成十进制即是640KB。如果比正常系统内存数减少，则减少内存被病毒所占用。

3. 用磁盘工具软件来查看内存使用情况(如用Norton等工具软件)

(三)检测硬盘主引导扇区法

系统的启动一般都是先把硬盘主引导扇区内容读入内存并执行，一些引导型病毒就利用它来感染计算机系统。因此可通过检测硬盘主引导扇区的内容或功能有无变化，来判断该硬盘是否染有主引导型病毒。可用debug动态调试命令或用NU等工具软件读出主引导扇区内容并和原未染毒情况下的备份相比较，如有不同则染毒。

(四)查看BOOT区(引导记录)

正常引导区最后约128字节大都是引导出错时

的英文提示信息,而感染病毒的引导区该部分内容很多是一些乱七八糟的字符,这样就可以得到确诊。

DEBUG

－L 100 2 0 1

－D 100 2FF　屏幕显示引导区内容

(五)检测硬盘分区法

一些病毒是通过感染硬盘的分区,把病毒程序写入分区或对分区程序作部份修改,来达到传染和破坏的目的。因此,可通过查看分区和引导扇区的内容有无变化来判断是否感染引导型病毒。可用 debug 或用 NU 等工具软件读出引导扇区内容并和原未染毒情况下的备份相比较,如有不同则染毒。

(六)检测内存数据区法

ROM BIOS 用内存 0040:0000H 到 0040:00FFH 的 256 字节作为键盘、显示器、硬盘、打印机和通讯等程序的数据区。这些数据在加电后由 ROM BIOS 初始化。因此可通过 debug 检测该数据区有无变化来判断计算机系统是否染毒。

(七)文件比较法

在 Windows 的 MS－DOS 方式下,用 winnt\system32\fc.exe 比较命令,将可疑执行文件和其原备份比较,如有不同则染毒。

(八)杀毒软件检测法

这是高效快捷的方法,被普通用户广泛采用。杀毒软件使用很简单,最好用两款不同的知名杀毒软件并升级到最高版本后在系统安全模式下查杀。但由于病毒的超前性、未知性和复杂性等因素,杀毒的结果不可全信,在有多种病毒交叉感染和交叉重复感染情况下病毒清除后往往会破坏原程序,因此很多用户发现杀毒后系统运行速度不但没有提升反而变得更慢,甚至有的发现系统无法使用了。因此杀毒前一定要做好有用文件的备份工作。

五 预防措施

计算机病毒防治时主要以预防为主清除为辅,预防是积极的清除是被动的,可采取以下措施来积极预防:

1. 首先确保安装系统用盘无毒,有经验的维护人员不会轻易使用他人的光盘以确保系统无毒安装和所安装系统的稳定性。

2. 我校采用局域网方式上网,因此安装系统时应断开网线以避免网内病毒传染。

3. 清除主引导记录　最简单的方法是用 fdisk/mbr 命令即可)

4. 安装操作系统后应立即安装性能优异的杀毒软件并打开病毒监控程序和安装防火墙再将其升级到最新版。要经常升级病毒库和定期查杀硬盘。所谓性能优异的杀毒软件,是指除了能够彻底预防、彻底杀除已知病毒外,还具有实时监视技术、自动解压缩技术、全平台反病毒等主要技术,即使在没有病毒特征码情况下,也能够给出提示让用户阻止未知病毒的行为,从而避免病毒发作时杀毒软件先遭破坏。在安装时不要给超级用户设置过于简单的密码。

5. 给操作系统安装最新 service pack 程序和系统漏洞补丁程序。

6. 所有应用软件确信无毒后再安装并安装应用软件补丁程序。

7. 可在策略编辑器中关闭系统“自动运行”功能以避免诸如‘熊猫烧香’等病毒在打开磁盘时自动运行。

8. 备份系统分区表、引导记录、注册表等关键数据。

9. 用 Ghost 克隆软件给系统分区做一个镜像备份文件,将其扩展名更名并加上只读属性还可将其放入隐藏分区中。也可使用“一键还原”或‘还原精灵’等软件来保护系统。XP 的用户可用系统自带的还原系统。一旦系统需要恢复时,在几分钟内即可将系统恢复到新安装时状态。为了避免恢复系统分区时‘我的文档’中的文件丢失,系统安完后可在‘我的文档”属性中用‘移动”按钮将其移动到其它逻辑盘中。

10. 在 CMOS 设置中把 BIOS FEATURES SETUP 项的 Virus Warning 设为 Enabled。

11. 外来文件查毒后再使用,不轻易打开不熟悉和来历不明的邮件、附件,不浏览不安全的网站,不上网时即时断开网络。

12. 网上资源帐户密码要经常更改。有用文件即时多备份。

六 结束语

由于计算机病毒发展速度迅猛、技术超前,防治水平永远滞后,因此我们要提高安全防范意识和病毒防治技术,降低病毒造成损失的最好办法就是备份、备份再备份。

致谢:本文在写作过程中得到了朱盛科教授的悉心指导,在此深表谢意!

参考文献:

[1]杨立. 微型计算机原理与接口技术. 北京:中国铁道出版社,2004.
[2]郑学坚. 微型计算机原理及应用. 北京:清华大学出版社,2000.
[3]梁和. 微机组装与维修. 北京:清华大学出版社,2002.
[4]赵育新. 计算机病毒的发展趋势与防治. 辽宁警专学报,2006(1):45-47.
[5]胡坚强. 几类流行计算机病毒的分析与处理. 华南金融金脑,2006(11):68-70.
[6]实例解析蠕虫病毒的原理[EB/OL]. http://www.anqn.com/article/g 2006 09 08.
[7]手工发现和清除木马的方法[EB/OL]. http://it.rising.com.cn/channels/Anti-Virus 2005 02 01.

An Analysis of the Working Mechanism of Computer Virus and the Methods of Detection and Prevention

LIU Zhong-yi, ZHU Jiang-dong

(Department of Information Technology, Xichang College, Xichang, Sichuan 615013)

Abstract: This article starts with the origin of computer virues, the reasons of its proliferation and its harm. It expounds the working mechanism of computer virus and gives the common methods of detection and prevention.

Key words: Reasons of computer virus program; Harm; Working mechanism; Detection technology; Preventive measures

(责任编辑:张荣萍)

(上接67页)

参考文献:

[1]李美超,马淳安,吴庆,甘永平. 电解制备离子水的研究[J]. 化学世界,2002(8):0406-0412.
[2]皖文. 离子水生成器[J]. 家用电器,2000(8):24-25.
[3]赵锡斌. 离子水生产技术[J]. 天津化工,1999(6):18-19.

The Design and Implementation of Ion Water Generator for Agricultural Use Based on Computer Controlling Technology

SHI Zhi-xiong, TENG Xiao-long, ZHOU Ming-guang

(Department of Information Technology, Xichang college, Xichang, Sichuan 615013)

Abstract: Based on the technology of computer controlling, transducer and modern membrane technology, we designed and made a new type of low-cost inowater sterilizer for agriculture use. This papor provides some related technical datas as follows: a functional block diagram, a schematic circuit diagram and some major primary codes in the control program.

Key words: Computer controlling; Transducer; Membrane technology; Ion water

(责任编辑:张荣萍)