计算机病毒及其防治

Computer Viruses and Their Prevention and Treatment

黄　勤
(武汉七环高新技术集团)

一、席卷全球的计算机病毒

1988年11月，美国国防计算机网络INTERNET遭病毒袭击瘫痪了24小时;1989年，美国军方的一架由计算机控制的隐形机坠落，调查怀疑是病毒破坏造成的;1989年，台湾70～80%的PC机感染了病毒;自1989年上半年国内发现计算机病毒以来，病毒迅速感染了全国的大多数计算机……

大量数据丢失，机器运行速度变慢，经常死机，文件长度增加(甚至上百K字节)……

计算机病毒席卷全球。

病毒让人防不胜防，一时间人心惶惶，不少人谈毒色变。

在一般的应用领域，计算机病毒造成的后果还是有限的;但是，在工业、金融、国防等领域，每一个数据的失误都可能造成严重的危害，引起大系统的瘫痪，出现重大事故，甚至给整个人类的生命和生存带来毁灭性的打击。

无疑，计算机病毒的出现给计算机的应用带来了很多消极的影响，但是，用积极的、科学的态度去认识它，并进而治理它，计算机病毒是可以得到控制的。

二、计算机病毒是怎么回事?

计算机病毒是一种能使自身的复制品入侵到宿主程序代码中去的程序代码，被入侵后的程序代码(被感染程序代码)仍可"合法"执行。可见，计算机病毒具有下述特点:寄生性，它寄生在其它程序代码中;传染性;隐蔽性，被感染程序代码仍可"正常"执行。计算机病毒还常常具有下述特点:潜伏性，计算机病毒一般并不立即发作;表现性或破坏性，在一定的条件下通过屏幕或声响表现自己，或影响系统的正常运行，破坏文件、磁盘数据等。

计算机病毒有静态和动态两种状态。没有进入内存和没有被运行过的病毒为静态病毒，由于没有被运行，所以，静态病毒没有传染或破坏作用;一旦病毒进入内存并被运行过，在某些条件下(如通过中断调用某一读写磁盘，敲入某一键，到某一时间等)即可被激活而具有传染或破坏作用，此时的病毒为动态病毒。

计算机病毒包括引导、传染模块，一般还有表现(或破坏)模块。被感染程序代码运行时，引导模块被执行。引导模块既可以先将病毒代码驻留内存，并使病毒代码的传染模块以后能被用户的正常操作而激活(如通过更改中断向量而将病毒代码纳入中断子程序)，也可以先直接执行传染模块，然后再恢复被感染程序代码为正常代码或读入正常代码而执行之。传染模块被激活后，使病毒入侵到被感染程序代码中。引导模块、传染模块互相配合，实现了病毒的传播。

计算机的高速运算处理能力给人类带来了信息技术的新时代，掀起了新技术革命的浪潮，但是，也给对计算机进行非授权的操作带来了隐蔽性;开放的系统结构、便利的操作方式给人们带来了丰富的享受和无限的乐趣，但是，也给计算机病毒对信息系统的入侵打开了方便之门。应该说，计算机病毒的出现是必然的。

三、计算机病毒的弱点与防治策略

计算机病毒要能感染内存或磁盘(含引导扇区和文件)，它必然要进行一些非法操作，这正是计算机病毒的弱点，及时识别这些非法操作，就可采取有效措施制止病毒的传播;病毒感染内存或

磁盘及其它文件后，必然改变了内存或其它文件或磁盘，要留下一些痕迹，这同样是计算机病毒的弱点，发现这些改变就可发现计算机系统是否染毒。

病毒要能够传播，所进行的非法操作有：

1. 非法写磁盘(必然现象)；

2. 更改中断向量使病毒程序常驻内存(驻留型病毒，含引导型病毒和大部分文件型病毒)。

下述现象能帮助用户尽早发现病毒：

1. 屏幕出现非正常显示，扬声器出现非正常声响；

2. 文件长度莫名其妙地增加或减少；

3. 文件莫名其妙地消失或出现莫名其妙的文件；

4. 经常非正常读写磁盘；

5. 运行速度变慢；

6. 经常死机；

7. MAIN BOOT, BOOT被改写过。

……

计算机病毒的预防与检测正是基于病毒的这些弱点。

由于新病毒不断出现，针对已有病毒的反病毒软件局限性太大，已不可取；避开具体的病毒，依据病毒感染机器或磁盘必然存在的现象，研究通用的反病毒方法，进行系统的防治才是可行的措施。

防止各种病毒被引导、激活和感染其它程序是第一道防线，感染病毒后及时发现并处理是第二道防线，只要任一道防线有效，一般说来，计算机系统是安全的。

四、计算机病毒的预防

病毒可分为引导型(可在系统启动时感染系统，寄生于MAIN BOOT、BOOT)和文件型(寄生于文件中)两类，一个病毒也可同时为引导型和文件型。

无论何种病毒，都是可执行代码。因此，只要不用带毒盘启动，就不会带引导型病毒；只要不运行带毒文件，就不会带文件型病毒。这样也就可避免病毒进入内存或传播。

必须指出，不敢对病毒盘进行任何操作的病毒恐惧症是毫无根据的。

预防病毒要注意：

1. 不用来历不可靠的盘启动系统，不运行来历不可靠的文件，最好只用硬盘启动；

2. 带引导型病毒的盘应及时从A驱动器中抽出，以防热启动或机器掉电后的来电引起用带毒A盘误启动系统；

3. 作好文件的备份工作，特别是重要文件，如系统软件，自开发软件等，备份盘加写保护；

4. 经常检查，发现异常及时处理。

对已知的病毒使用相应的反病毒软件有可能在其进入系统(内存)时发现并清除，但对某些未知的病毒则只能在其引导完成后或进行传染时甚至传染后才能发现它。

可以监视中断向量表。大多数病毒在执行引导时会修改中断向量表，及时发现这些修改就可发现这些病毒，并还可以从内存中消除之。但，许多正常程序也会修改中断向量表，如CCDOS，DEBUG等。这要求用户对系统很熟悉，有很强的判断力。一般用户难以做到这一点。又，智能病毒可不修改中断向量表，而直接修改相应的中断调用子程序，也可达到同样的功能。故其局限性是明显的。

这里介绍一种防止病毒感染磁盘的方法。它对BIOS、DOS作了改进，对驱动器进行严格的管理，拦截所有写操作(任何企图避开监视的用户自编的写操作程序也被拦截)，一但发现有试图写BOOT、MAIN BOOT、可执行文件(COM, EXE,OVL,SYS等型)、目录(改写可执行文件目录基项)、FAT等企图即报警，正常写才被允许进行下去。此法理论上可杜绝任何病毒的新感染，或在可能的感染后立即报警(病毒可能混入正常的文件写操作中，先直接改可执行文件的相应扇区，再改目录、FAT等)。但实施中仍可能有漏洞。比如，设想有一种只在正常的COPY操作中感染文件的病毒，或仅在编译系统生成可执行文件的同时感染生成文件的病毒，本法就无法识别。另，本法并不能阻止病毒的引导，只是在病毒传染时加以识别。对本法可以有各种基于硬件与软件的改进措施。

五、计算机病毒的检测

引导型病毒在系统启动时进入内存，为能进行传播，它一定要更改中断向量使病毒常驻内存。由于此时DOS尚未装入，为使病毒程序不被覆盖，病毒只能更改BIOS数据区中的RAM容量，将病毒常驻内存高端。这些特点可作为发现各种引导型病毒是否进入内存的主要方法。

文件型病毒可分为外壳型、入侵型、源码型等类。外壳型病毒将病毒寄生于宿主程序的外围，因此，文件长度不同，特别是这种病毒：它将宿主程序换名，病毒程序换为宿主程序名，长度补齐，病毒程序调用宿主程序，但该病毒太粗糙，很易被发现。入侵型病毒将病毒寄生于宿主程序的内部，这种病毒难写，有较强的针对性，因而少见，但对程

序代码进行和校验，异或校验或按一定的间隔对代码采样检验就可发现。源码型病毒在源程序编译时插入到源程序中，这种病毒难写，针对性强，传染性差，少见，发现也难，但如果某种病毒总是在某种编译系统下生成的可执行文件上出现，就可怀疑这种病毒了。文件型病毒针对的目标是可执行的文件。

可用下述方法发现引导型病毒:

1. 用PCTOOLS查看内存

在PCTOOLS下进入F3(磁盘服务)方式，可查看机器信息，如DOS报告的内存比PCTOOLS报告的内存小，亦异于下面的内存报告，则表示有毒。

2. 染毒测试(ANTIVIR2.COM, ANTIVIR3.COM程序)

这是笔者开发的系列反病毒软件之一。其功能是(1)测试内存，将计算机实际内存与DOS报告的内存比较，不同则报警;(2)测试BOOT, MAIN BOOT，与原始测试记录比较，不同则报警;(3)测试IBMBIO,IBMDOS,COMMAND三个COM文件，比较长度，按长度的1/64采样并比较代码，与原始测试记录不同则报警。

由于提取了BOOT,MAIN BOOT，所以，只要将原无毒的BOOT, MAIN BOOT写回磁盘，就可对任何引导型病毒解毒。

3. 用PCTOOLS查看BOOT，用DEBUG查看BOOT, MAIN BOOT

对系统比较熟悉时，可查看BOOT, MAIN BOOT，有异常则可认为带毒。

4. 用SCAN或其它软件扫描病毒

这些软件在被扫描对象中寻找已知病毒的特征字节、比较部分代码，以判断是否有某种病毒。因此，只能发现已有的种类有限的病毒。

前二种方法最有效，可发现任何引导型病毒。方法2可置于AUTOEXEC.BAT中自检。

文件型病毒入侵COM,EXE,OVL,SYS等型可执行文件，可用下述方法发现:

1. 文件运行时的染毒报警(ANTIVIR1.EXE,ANTIVIR1.DAT程序)

这是笔者开发的系列反病毒软件之一。它将COM型文件(其它型方法类似)进行加工，运行时自动比较文件加工前的长度与当前长度，不同则报警。经加工后几乎所有病毒的新感染均可正确识别。最好软件商提供的软件已经经过本软件加工。

2. 检测的染毒报警

本软件对一个目录下的文件进行程序的完整性检验，如和校验，异或校验，代码采样检验和文件长度校验。每有新文件加入，就将新文件的这些信息记录下来，以后经常使用本软件进行检验，有不同则报警。本软件在作这些工作以前还自检，看自己是否带毒。文件检验范围也可仅限于文件的第一扇区以提高速度。这些检验可由软件开发商置于程序内部，在运行时自动进行。提取检验信息后的任何病毒感染均可识别。方法1和2不能识别仅编译才进入文件的病毒。

3. 用SCAN软件或其它软件扫描病毒

它们能发现已有的病毒。

病毒的预防与检测常常需要互相配合使用。

国外反病毒软件有上百种，列举一、二:

□Bomb squad: 对ROM BIOS写、格式化等危险操作发出报警。

□Disk Watcher: 检测病毒，防止非法写。

□Novir U2: 监视中断向量。

国内也有一些反病毒软件、防病毒卡，如M6403防病毒汉卡等。

六、计算机病毒的消除

病毒的消除包括病毒本身的消除(恢复无毒的BOOT、MAIN BOOT、可执行文件)和被病毒破坏的其它类型文件的恢复。

病毒本身的消除最简单的方法是将备份的无毒的BOOT、MAIN BOOT、可执行文件重写到磁盘上。另外，还有下述方法可用:

1. 专用解毒软件的应用。但是，这类软件的针对性很强，依赖于软件商的开发成果。很可能解毒后的磁盘不能用(系统型病毒)或文件不能运行(文件型病毒)。

2. SYS命令恢复BOOT、IBMBIO.COM、IBMDOS.COM。

但它不能恢复MAIN BOOT。

3. DEBUG下恢复MAIN BOOT, BOOT。

只要硬盘分区信息表能找到，则用无毒盘上的MAIN BOOT与此分区信息表组合就能恢复MAIN BOOT。

有了MAIN BOOT，就可用无毒盘上的BOOT，及本盘的BPB参数恢复BOOT。

4. DEBUG下恢复可执行文件。

病毒程序一般都要恢复原可执行文件以正常运行，用DEBUG得当地跟踪一般可恢复原可执行文件。但，这也要很高的技巧，因为，很可能死机或原文件仍带毒。

5. COM型文件的一种通用解毒方法。

可执行文件在执行完后，一般说都要返回DOS，所以，我们只要拦截INT20(结束进程)或INT27(结束进程但驻留)，就可在染毒文件执行完返回DOS前将无毒的文件(此时病毒已对染毒

文件解毒)写回磁盘。本软件可以常驻于内存，以随时激活。

被病毒破坏的其它文件的恢复有下述方法:

1. 若MAIN BOOT, BOOT, FAT已恢复，则CHKDSK/F可恢复所有文件，只是文件名，长度需人工恢复。

2. 用DEBUG＋PCTOOLS恢复FAT被破坏的盘上的部分数据文件

方法是:待恢复的文件有一些特征字符串，在PCTOOLS的磁盘服务方式下，用F功能全盘找这些字符串，若找到则可能恢复文件的部分或全部。因为，很可能该文件在一段连续的扇区。在PCTOOLS下记下这些扇区，在DEBUG下将其联接成文件即可恢复原文件。

七、计算机病毒对抗与软件保护

一种病毒，即使制造时是“良性”的，也很容易在传播过程中被有不良动机者或恶作剧者利用，改成有破坏作用的“恶性”病毒。这种情况将后患无穷，特别是一旦产生各种变体病毒，将给病毒的防治增加极大的困难。

美国军方悬赏研制摧毁敌方电子系统的计算机病毒。必须看到，一旦病毒失控的潜在危险性比生物武器还大，这种作为已经引起一些学者的不安。

计算机病毒可以成为军事系统电子对抗的一种新的进攻性武器，可以保护软件，但也可以是一种新的恐怖手段。所以，无论出自何种目的和动机，从效果看，制造和传播病毒均是一种危险的游戏，从人类的利益出发，应该停止研制各种病毒!

八、计算机病毒与反病毒之战

有一种病毒，就可以有一种相应的反病毒软件，同样，对任何纯软件的反病毒方法，有一种反病毒软件，也可以有一种相应的病毒对抗它。而无论使用硬件或软件手段，对病毒的抵抗力越强，要增加的开销也越大，对系统的开放性、使用的灵活性、计算机系统的使用效率的影响也越大。

在目前的系统结构下，一种能抵抗任何病毒的一劳永逸的反病毒方法几乎是不可能实现的。要想根本不感染病毒，必须把机器隔离起来，这是不现实的。

病毒种类越来越多，变体也大量产生，计算机病毒防治的工作量越来越大。计算机病毒总是试图避开反病毒系统的监视和摧毁反病毒系统的功能，反病毒系统则总是试图识别病毒、希望摧毁病毒的入侵，计算机病毒与反病毒之战将愈演愈烈。

人工智能、专家系统具有知识库，有自学习、推理、判断能力，在这场高技术战争中，越来越受到人们的重视。我们看到，智能型病毒的代码长度将增加，被发现的可能性也增加，因此，反病毒领域的前景是乐观的。

附带指出，定时炸弹——特洛伊木马，除不具传染性外，与病毒无异，同样有破坏作用。由于其无传染性，特洛伊木马长期处于潜伏状态，隐蔽性更强，其对数据的破坏还可在正常的数据修改与更新时进行，因而更难识别，对安全性、可靠性要求高的重要场合，其危险性比病毒更大，应予特别的重视。

九、计算机病毒防治:一项社会系统工程

在技术上，对前述各种防治病毒的方法要灵活应用，要善于判断、推理。但是，计算机病毒防治不仅仅是一个技术课题，它同时还是一项社会系统工程。

要不断完善有关法律，病毒防治部门作为专门机构，要做好管理、协调工作，要加强技术开发、交流、咨询、培训等工作。

制造病毒、在软件中暗藏病毒、公布病毒程序、有意传播病毒等行为均是危害社会的犯罪行为，全社会应该有此共识。

十、预警:切不可掉以轻心

信息系统的安全仍面临着挑战。

信息系统的脆弱，过去计算机病毒猖獗的历史，已经给了人们一个难忘的警告和教训;而未来仍预示着潜在的巨大的危险。计算机病毒与反病毒之战将是一场持久、艰苦的智力竞赛。随着科学技术的进步和社会经济的发展，计算机技术这一人类智慧的结晶必将大量普及，进入社会生活的每一个角落。因此，计算机病毒的防治、信息系统的安全问题必须引起计算机研制者、计算机用户、决策者及社会各界的高度重视，切不可掉以轻心!

(责任编辑　宋义荣)