第3章 病 毒 篇

3.1 引言

编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码被称为计算机病毒(Computer Virus)。病毒具有破坏性、复制性和传染性。

病毒往往会利用计算机操作系统的弱点进行传播，提高系统的安全性是防病毒的一个重要方面，但完美的系统是不存在的，过于强调提高系统的安全性将使系统多数时间用于病毒检查，系统失去了可用性、实用性和易用性，另一方面，信息保密的要求让人们在泄密和抓住病毒之间无法选择。病毒与反病毒将作为一种技术对抗长期存在，两种技术都将随计算机技术的发展而得到长期的发展。

3.2 计算机病毒的概念

计算机病毒在《中华人民共和国计算机信息系统安全保护条例》中被明确定义，病毒指“编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。与生物病毒不同的是几乎所有的计算机病毒都是人为故意制造出来的，有时一旦扩散出来后连编者自己也无法控制。它已经不是一个简单的纯计算机学术问题，而是一个严重的社会问题了。

宏病毒是一种寄存在文档或模板的宏中的计算机病毒，一旦打开这样的文档，其中的宏就会被执行，于是宏病毒就会被激活，转移到计算机上，并驻留在 Normal 模板上。从此以后，所有自动保存的文档都会“感染”上这种宏病毒，而且如果其他用户打开了感染病毒的文档，宏病毒又会转移到其他计算机上。宏病毒具有传播速度极快、制作、变种

方便、破坏可能性极大、多平台交叉感染。

3.3 计算机病毒的产生

病毒不是来源于突发或偶然的原因，一次突发的停电或偶然的错误，会在计算机的磁盘和内存中产生一些乱码和随机指令，但这些代码是无序和混乱的。病毒则是一种比较完美的、精巧严谨的代码，按照严格的秩序组织起来，与所在的系统网络环境相适应和配合。病毒不会通过偶然形成，并且需要有一定的长度，这个基本的长度从概率上来讲是不可能通过随机代码产生的。现在流行的病毒是由人为故意编写的，多数病毒可以找到作者和产地信息，从大量的统计分析来看，病毒作者的主要情况和目的是：一些天才的程序员为了表现自己和证明自己的能力，为了得到控制口令，为了防止编写软件拿不到报酬预留的陷阱等；当然也有因政治、军事、宗教、民族、专利等方面的需求而专门编写的，其中也包括一些病毒研究机构和黑客的测试病毒。

3.4 计算机病毒的传染途径

计算机病毒之所以称为病毒是因为其具有传染性的本质。传统渠道通常有以下几种：

(1) 通过 U 盘。通过使用外界被感染的软盘，例如，不同渠道来的系统盘、来历不明的软件、游戏盘等是最普遍的传染途径。

(2) 通过硬盘。通过硬盘传染也是重要的渠道，由于带有病毒的机器移到其他地方使用、维修等，将干净的软盘传染并再扩散。

(3) 通过网络。这种传染扩散极快，能在很短时间内传遍网络上的机器。

3.5 计算机病毒的特点

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，病毒就起破坏作用，而在未启动这个程序之前，它是不易被人发觉的。

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，一旦病毒被复制或产生变种，其速度之快令人难以预防。传染性是病毒的基本特征。在生物界，病毒通过传染从一个生物体扩散到另一个生物体。在适当的条件下，它可得到大量繁殖，使被感染的生物体表现出病症甚至死亡。同样，计算机病毒也会通过各种渠道从已被感染的计算机扩散到未被感染的计算机，是否具有传染性是判别一个程序为计算机病毒的最重要条件。病毒程序通过修改磁盘扇区信息或文件内容，并把自身嵌入到其中的方法达到病毒

的传染和扩散。被嵌入的程序称为宿主程序。

3. 潜伏性

有些病毒像定时炸弹一样，让它什么时间发作是预先设计好的。例如，黑色星期五病毒，不到预定时间一点都觉察不出来，等到条件具备的时候一下子就爆炸开来，对系统进行破坏。一个编制精巧的计算机病毒程序，进入系统之后一般不会马上发作，可以在几周或者几个月内甚至几年内隐藏在合法文件中，对其他系统进行传染，而不被人发现，潜伏性越好，其在系统中的存在时间就会越长，病毒的传染范围就会越大。潜伏性的第一种表现是指病毒程序不用专用检测程序是检查不出来的，因此病毒可以静静地躲在磁盘或磁带里呆上几天，甚至几年，一旦时机成熟，得到运行机会，就要四处繁殖、扩散，继续为害。潜伏性的第二种表现是指计算机病毒的内部往往有一种触发机制，不满足触发条件时，计算机病毒除了传染外不做什么破坏。触发条件一旦得到满足，有的在屏幕上显示信息、图形或特殊标识，有的则执行破坏系统的操作，如格式化磁盘、删除磁盘文件、对数据文件做加密、封锁键盘以及使系统死锁等。

4. 隐蔽性

计算机病毒具有很强的隐蔽性，有的可以通过病毒软件检查出来，有的根本就查不出来，有的时隐时现、变化无常，这类病毒处理起来通常很困难。

5. 破坏性

计算机中毒后，可能会导致正常的程序无法运行，把计算机内的文件删除或受到不同程度的损坏。

6. 可触发性

病毒因某个事件或数值的出现，诱使病毒实施感染或进行攻击的特性称为可触发性。为了隐蔽自己，病毒必须潜伏，少做动作。如果完全不动，一直潜伏的话，病毒既不能感染也不能进行破坏，便失去了杀伤力。病毒既要隐蔽又要维持杀伤力，它必须具有可触发性。病毒的触发机制就是用来控制感染和破坏动作的频率的。病毒具有预定的触发条件，这些条件可能是时间、日期、文件类型或某些特定数据等。病毒运行时，触发机制检查预定条件是否满足，如果满足，启动感染或破坏动作，使病毒进行感染或攻击；如果不满足，使病毒继续潜伏。

3.6　计算机病毒的分类

根据对计算机病毒的研究，按照科学的、系统的、严密的方法，计算机病毒可以根据以下的属性进行分类。

1. 按照计算机病毒存在的媒体进行分类

根据病毒存在的媒体，病毒可以划分为网络病毒、文件病毒和引导型病毒。网络病毒通过计算机网络传播感染网络中的可执行文件，文件病毒感染计算机中的文件（如

COM、EXE、DOC 等),引导型病毒感染启动扇区(Boot)和硬盘的系统引导扇区(MBR)。还有这三种情况的混合型,例如:多型病毒(文件和引导型)感染文件和引导扇区两种目标,这样的病毒通常都具有复杂的算法,它们使用非常规的办法侵入系统,同时使用了加密和变形算法。

2. 按照计算机病毒传染的方法进行分类

根据病毒传染的方法可分为驻留型病毒和非驻留型病毒。驻留型病毒感染计算机后,把自身的内存驻留部分放在内存(RAM)中,这一部分程序挂接系统调用并合并到操作系统中,它处于激活状态,一直到关机或重新启动。非驻留型病毒在得到机会激活时并不感染计算机内存,一些病毒在内存中留有小部分,但是并不通过这一部分进行传染,这类病毒也被划分为非驻留型病毒。

3. 按照病毒破坏能力划分

根据病毒破坏能力可分为无害型、无危险型、危险型和非常危险型病毒。

(1) 无害型:除了传染时减少磁盘的可用空间外,对系统没有其他影响。

(2) 无危险型:这类病毒仅仅是减少内存、显示图像、发出声音及同类音响。

(3) 危险型:这类病毒在计算机系统操作中造成严重的错误。

(4) 非常危险型:这类病毒删除程序、破坏数据、清除系统内存区和操作系统中重要的信息。

这些病毒对系统造成的危害,并不是本身的算法中存在危险的调用,而是当它们传染时会引起无法预料的、灾难性的破坏。由病毒引起其他的程序产生的错误也会破坏文件和扇区,这些病毒也按照它们引起的破坏能力划分。一些现在的无害型病毒也可能会对新版的 DOS、Windows 和其他操作系统造成破坏。例如,在早期的病毒中,有一个“Denzuk”病毒在 360K 磁盘上很好的工作,不会造成任何破坏,但是在后来的高密度软盘上却能引起大量的数据丢失。

4. 按照病毒特有的算法划分

根据病毒特有的算法可分为伴随型病毒、“蠕虫”型病毒和寄生型病毒。

(1) 伴随型病毒:这一类病毒并不改变文件本身,它们根据算法产生 EXE 文件的伴随体,具有同样的名字和不同的扩展名(COM),例如,XCOPY. EXE 的伴随体是 XCOPY. COM。病毒把自身写入 COM 文件并不改变 EXE 文件,当 DOS 加载文件时,伴随体优先被执行再由伴随体加载执行原来的 EXE 文件。

(2) “蠕虫”型病毒:通过计算机网络传播,不改变文件和资料信息,利用网络从一台机器的内存传播到其他机器的内存,计算网络地址,将自身的病毒通过网络发送。有时它们在系统中存在,一般除了内存不占用其他资源。

(3) 寄生型病毒:除了伴随型和“蠕虫”型病毒,其他病毒均可称为寄生型病毒,它们依附在系统的引导扇区或文件中,通过系统的功能进行传播,按其算法不同又可分为练习型病毒、诡秘型病毒和变型病毒。

练习型病毒:病毒自身包含错误,不能进行很好地传播,例如,一些病毒在调试阶段。

诡秘型病毒：它们一般不直接修改 DOS 中断和扇区数据，而是通过设备技术和文件缓冲区等 DOS 内部修改，不易看到资源，使用比较高级的技术。利用 DOS 空闲的数据区进行工作。

变型病毒（又称幽灵病毒）：这一类病毒使用一个复杂的算法，使自己每传播一份都具有不同的内容和长度。它们一般是由一段混有无关指令的解码算法和被变化过的病毒体组成。

5. 计算机病毒的危害性

计算机资源的损失和破坏，不但会造成资源和财富的巨大浪费，而且有可能造成社会性的灾难，随着信息化社会的发展，计算机病毒的威胁日益严重，反病毒的任务也更加艰巨了。1988 年 11 月 2 日下午 5 时 1 分 59 秒，美国康奈尔大学的计算机科学系研究生，23 岁的莫里斯（Morris）将其编写的蠕虫程序输入计算机网络，致使这个拥有数万台计算机的网络被堵塞。这件事就像是计算机界的一次大地震，引起了巨大反响，震惊全世界，引起了人们对计算机病毒的恐慌，也使更多的计算机专家重视和致力于计算机病毒研究。1988 年下半年，我国在统计局系统首次发现了“小球”病毒，它对统计局系统影响极大，此后由计算机病毒发作而引起的“病毒事件”接连不断，之后发现的 CIH、美丽杀等病毒更是给社会造成了很大损失。

3.7　中毒的诊断

（1）按 Ctrl＋Shift＋Esc 键，调出 Windows 任务管理器查看系统运行的进程，找出不熟悉的进程并记下其名称（这需要经验），如果这些进程是病毒的话，以便于后面的清除。暂时不要结束这些进程，因为有的病毒或非法的进程可能在此没法结束。单击性能查看 CPU 和内存的当前状态，如果 CPU 的利用率接近 100％或内存的占用值居高不下，此时计算机中毒的可能性是 95％。

（2）查看 Windows 当前启动的服务项，执行“开始”→“控制面板”→“管理工具”→“服务”命令，在打开的“服务”窗口中查看右栏状态为“启动”、启动类别为“自动”项的行。一般而言，正常的 Windows 服务，基本上是有描述内容的（少数被黑客或蠕虫病毒伪造的除外），此时双击打开认为有问题的服务项查看其属性中的可执行文件的路径和名称，假如其名称和路径为 C:\winnt\system32\explored.exe，计算机中毒。另一种情况是“控制面板”打不开或者是所有里面的图标跑到左边，中间有一纵向的滚动条，而右边为空白，再双击添加/删除程序或管理工具，窗体内是空的，这是病毒文件 winhlpp32.exe 发作的特性。

（3）运行注册表编辑器，命令为 regedit 或 regedt32，查看都有哪些程序与 Windows 操作系统一起启动。主要查看 Hkey_Local_Machine\Software\microsoft\Windows\CurrentVersion\Run 和后面几个 RunOnce 等，查看窗体右侧的项值，查看是否有非法的启动项。Windows XP 运行 msconfig 也起相同的作用。随着经验的积累，可以轻易地判

断病毒的启动项。

(4) 用浏览器上网判断。以前发作的 Gaobot 病毒,可以上 yahoo.com、sony.com 等网站,但是不能访问诸如 www.symantec.com、www.ca.com 这样著名的安全厂商的网站,安装的杀毒软件不能上网升级。

(5) 取消隐藏属性,查看系统文件夹 winnt(windows)\system32,如果打开后文件夹为空,表明计算机已经中毒;打开 system32 后,可以对图标按类型排序,查看有没有流行病毒的执行文件存在。顺便查一下文件夹 Tasks、wins、drivers。有的病毒执行文件就藏身于此;drivers\etc 下的文件 hosts 是病毒喜欢篡改的对象,它本来只有 700B 左右,被篡改后就成了 1KB 以上,这是造成一般网站能访问而安全厂商网站不能访问、著名杀毒软件不能升级的原因所在。

(6) 由杀毒软件判断是否中毒,如果中毒,杀毒软件会被病毒程序自动终止,并且手动升级失败。

3.8 病毒预防

要预防计算机网络病毒,首先是不要随便从小的个人网站上下载软件。下载软件要到知名度高、信誉良好的站点,通常这些站点软件比较安全。其次不要过于相信和随便运行别人给的软件。要经常检查自己的系统文件,注册表、端口等,多注意安全方面的信息,再次就是修改 Windows 关于隐藏文件扩展名的默认设置,这样可以看清楚文件真正的扩展名。当前许多反病毒软件都具有查杀“木马”或“后门”程序的功能,但仍需更新和采用先进的防病毒软件。最后要提醒的是:如果突然发现自己的计算机硬盘莫名其妙的工作,或者在没有打开任何连接的情况下 Modem 还在“眨眼睛”就立刻断开网络连接,进行木马的搜索。邮件病毒主要通过电子邮件进行传染的,而且大多通过附件夹带,了解了这一点,对于该类病毒的防范就比较明确和容易,要想预防计算机网络病毒,还要做到以下几点。

(1) 不要轻易打开陌生人来信中的附件,尤其是一些.EXE 类的可执行文件。

(2) 对于比较熟悉的朋友发来的邮件,如果其信中带有附件却未在正文中说明,也不要轻易打开附件,因为它的系统也许已经感染病毒。

(3) 不要盲目转发邮件。给别人发送程序文件甚至电子贺卡时,可先在自己的计算机中试一试,确认没有问题后再发,以免无意中成为病毒的传播者。

(4) 如果收到主题为“I LOVE YOU”的邮件后立即删除,更不要打开附件。

(5) 随时注意反病毒警报,及时更新杀毒软件的病毒代码库。从技术手段上,可安装具有监测邮件系统的反病毒实时监控程序,随时监测系统行为,如使用最新版本的杀毒实时软件来查杀该附件中的文件。切记要注意一点,预防与消除病毒是一项长期的工作任务,不是一劳永逸的,应坚持不懈。

3.9　计算机病毒的清除

计算机病毒的清除，最常用的是杀毒软件。国产杀毒软件主要有瑞星、江民、金山毒霸等；国外杀毒软件有 Kaspersky、PC-Cillion、Norton、McAfee 等。至于哪种杀毒软件最好，或者说更好，众说纷纭。但是，不管选择哪种杀毒软件，一定要使用正版的杀毒软件，切记不要使用盗版杀毒软件。如果计算机有疑似感染病毒的症状时，可以采取如下应急措施。

(1) 将杀毒软件升级至最新版，进行全盘杀毒。最好使用自动升级功能在线升级，如果不能自动升级，也可以下载最新的升级包，进行离线升级。

(2) 如果杀毒软件不能清除病毒，或者重新启动计算机后病毒再次出现。则应该进入安全模式进行查杀。进入安全模式的方法是：在计算机启动自检时按 F8 键，会出现各种启动模式的选择菜单，选择“安全模式”选项即可。

(3) 有些病毒造成杀毒软件无法启动，则需要根据现象，判断病毒的种类，使用相应的专杀工具进行查杀。因为这类病毒虽然能自动关闭杀毒软件，但一般不会关闭专杀工具。使用专杀工具查杀后，升级或重装杀毒软件，再按上面所述的方法进行杀毒。

(4) 如果病毒非常顽固，使用多种方法都不能彻底查杀，则最好格式化并重装操作系统。但是在重装操作系统后，切记不能直接打开除 C 盘外的其他盘，否则病毒又会被激活。必须先做好防护措施，安装杀毒软件，并升级至最新版，对所有硬盘进行杀毒。在确保没有病毒的情况下再打开其他盘。

(5) 有个别病毒在重装操作系统后仍无法彻底清除，则只好对硬盘进行重新分区或进行格式化处理。

实验 5　病毒清除

一、实验目的

了解什么是病毒危害性，了解病毒破坏系统方式，学会简单的清除病毒。

二、实验原理

计算机病毒是一种恶意计算机代码，可以破坏系统程序，占用空间，盗取账号和密码。严重可以导致网络、系统瘫痪。

清除方法：使用安全的杀毒软件清除或了解其原理通过手工清除。

通过 Windows 任务管理器等各种系统自带程序进行疑点排查，逐一清除病毒。

找出病毒真实路径，进行查杀。

三、实验内容

1. 实验环境

(1) 硬件设备：计算机两台 PC-A、PC-B。

(2) 软件工具：冰河木马控制端；文件夹 EXE 病毒。

2. 实验角色

单人操作或双人合作。

3. 实验步骤

1) 冰河木马

本实验将终端 PC-A 作为远程控制攻击端，PC-B 作为受控端进行试验。

(1) 在终端 PC-B 上，打开 Windows 任务管理器，结果如图 3.1 所示。

图 3.1 Windows 任务管理器的初始状态

(2) 在 PC-B 上运行 G_server.exe，再次打开 Windows 任务管理器，结果如图 3.2 所示。

图 3.2 运行 G_server.exe 后 Windows 任务管理器的状态

提示：

实际环境中可以通过邮件、链接等方式将被控制端木马注入到被控制端。这个程序需要在被控制端引诱运行。通常是做成美丽的图片作为伪装，或是通过 QQ 发送，使其运行等。

(3) 在安装 G_server. exe 之前，查看 PC-B 中的资源管理器的进程和性能的运行情况。

(4) 在 PC-A，打开控制端程序：G_CLIENT. EXE，如图 3.3 所示。

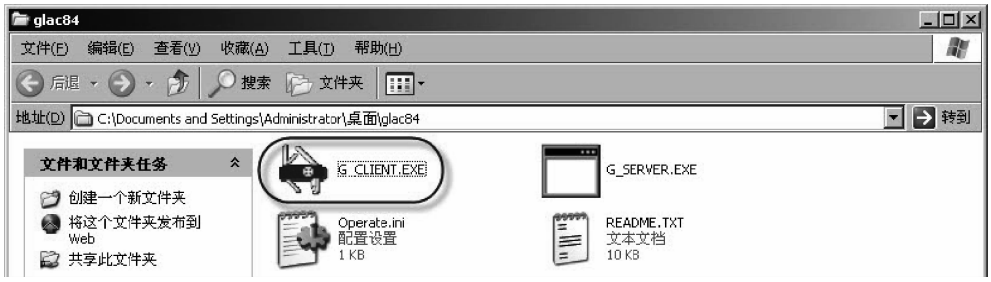

图 3.3　运行 G_CLIENT. EXE

(5) 在冰河主窗口下，单击“添加计算机”图标，如图 3.4 所示。

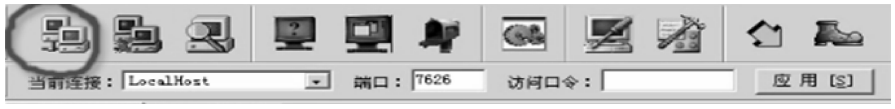

图 3.4　添加计算机

(6) 在显示名称中输入 PC-B 的 IP 地址(本实验中为 192. 168. 1. 20)。

提示：

一般地如果网内有多台设备被植入程序，可以用扫描工具扩大扫描范围，以获取所有的被控主机。

(7) 单击终端 PC-A 冰河主窗口下的“冰河信使”图标，输入任何内容(本实验中为冰河测试)，单击“发送”按钮，如图 3. 5 所示，在 PC-B 端，弹出“冰河信使”窗口。这样在 PC-B 和 PC-A 间就建立起了通信。

(8) 在 PC-B 上，将看到接收到的“冰河信使”窗口。

(9) 现在回到被攻击方——机架服务器 Windows 系统，打开 Windows 任务管理器，找到 kernel32. exe 进程，关闭该进程。这个进程就是受控的守护程序，通过它的隐藏，使系统常常被黑客随意联入控制。

(10) 回到控制端，重新扫描，发现已经无法扫描成功，完成破解攻击，如图 3.6 所示。

2) 蠕虫病毒

(1) 插入 U 盘，格式化，并在根目录下新建 3～4 个空文件夹，并退出 U 盘。

(2) 解压桌面上的病毒样本(Recycled. rar)，并运行。

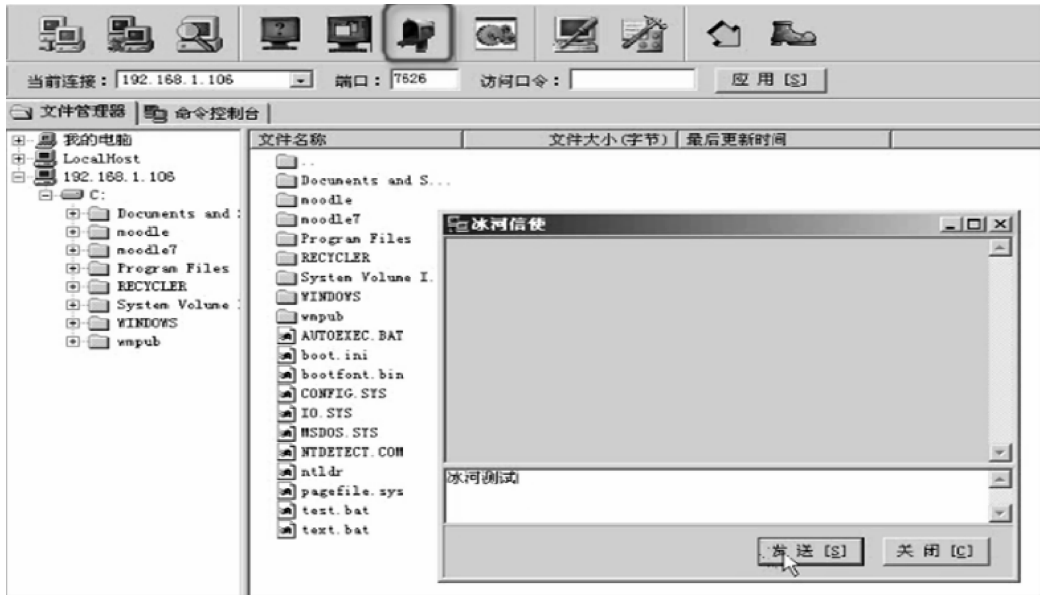

图 3.5　启动冰河信使

图 3.6　扫描失败