# 第5章 病毒技术


视频讲解

## 5.1 病毒的基本概念

### 5.1.1 计算机病毒的定义

计算机病毒(Computer Virus)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,病毒是指“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”。

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。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处于病毒检查,系统失去了可用性、实用性和易用性。另外,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。

病毒不是来源于突发或偶然的原因。一次突发的停电和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。而病毒是一种比较完美的、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起来的代码。病毒不会通过偶然形成,其代码本身需要有一定的长度,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,对上司的不满、好奇、报复、为了祝贺和求爱、为了得到控制口令、为了软件拿不到报酬而预留的陷阱等。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。

### 5.1.2 计算机病毒的特点

计算机病毒具有以下几个特点。

(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,其传播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,并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，在某些情况下造成被感染的计算机工作失常甚至瘫痪。与生物病毒不同的是，计算机病毒是一段人为编制的计算机程序代码，这段程序代码一旦进入计算机并得以执行，它就会搜寻其他符合其传染条件的程序或存储介质，确定目标后再将自身代码插入其中，达到自我繁殖的目的。只要一台计算机染毒，如不及时处理，那么病毒会在这台机器上迅速扩散，其中的大量文件（一般是可执行文件）会被感染。而被感染的文件又成了新的传染源，再与其他机器进行数据交换或通过网络接触，病毒会继续传染。正常的计算机程序一般是不会将自身的代码强行连接到其他程序之上的，而病毒却能使自身的代码强行传染到一切符合其传染条件的未受到传染的程序之上。计算机病毒可通过各种可能的渠道（如软盘、计算机网络）传染其他的计算机。当在一台计算机上发现了病毒，往往曾在这台计算机上用过的软盘已感染上了病毒，而与这台计算机联网的其他计算机也许也被该病毒感染了。是否具有传染性是判断一个程序是否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其中的方法达到病毒的传染和扩散。被嵌入的程序叫作宿主程序。

（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发了，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 1 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待上几天，甚至几年，一旦时机成熟，得到运行机会，就会四处繁殖、扩散，继续为害；潜伏性的第 2 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、对数据文件加密、封锁键盘和使系统死锁等。

（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，计算机内的文件被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。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。

### 5.1.3 计算机病毒的分类

根据病毒存在的媒体进行分类，病毒可以分为网络病毒、文件病毒、引导型病毒。

（1）网络病毒通过计算机网络传播感染网络中的可执行文件。

(2) 文件病毒感染计算机中的文件。

(3) 引导型病毒感染启动扇区(Boot)和硬盘的系统引导扇区(Master Boot Record,MBR)。

还有这3种病毒的混合型,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入侵系统,同时使用了加密和变形算法。

根据计算机病毒传染的方法进行分类,可分为驻留型病毒和非驻留型病毒。

(1) 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(Random Access Memory,RAM)中,这一部分程序挂接系统调用并合并到操作系统中去,它处于激活状态,一直到关机或重新启动。

(2) 非驻留型病毒在得到机会激活时并不感染计算机内存,另外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,这类病毒也被划归为非驻留型病毒。

根据病毒破坏的能力,可分为以下几种病毒。

(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、发出声音和同类音响。

(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和灾难性的破坏。由病毒引起其他程序产生的错误也会破坏文件和扇区,这些病毒也按照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360KB磁盘上很好地工作,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。

根据病毒特有的算法,病毒可以分为以下几种类型。

(1) 伴随型病毒。这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格式),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系统加载文件时,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外,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。

(4) 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。

(5) 变形病毒(又称为幽灵病毒)。这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。它们一般的做法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。

### 5.1.4 计算机病毒的发展史

**1. 计算机病毒的雏形**

1949 年，计算机之父约翰·冯·诺依曼在《复杂自动机组织》一书中提出了计算机程序能够在内存中自我复制。10 年后，在美国的贝尔实验室，程序员们利用闲暇时间编写了一种能吃掉其他程序的程序，并让其互相攻击作为消遣。例如，有一个叫“爬行者(Creeper)”的程序，每次执行都会自动生成一个副本，很快计算机中原有的资料就会被“爬行者”侵蚀；又如“侏儒(Dwarf)”程序，它可以在记忆系统中行进，每到第 5 个“地址”便把那里所储存的信息全部清除，严重损坏原本的程序；还有一个叫“小恶魔(Imp)”的程序，它只有一行移动指令——MOV 0,1，然而这条移动指令可以把程序身处地址中所载的 0 写入下一行地址当中，以致最后计算机中所有的指令都被改为 MOV 0,1，最终导致系统瘫痪。因为这些神奇的程序都在计算机的记忆磁芯中进行，因此这次实验被命名为“磁芯大战”。这些程序已经具备了一定的破坏性和传染性，成为计算机病毒的雏形。

**2. 第 1 个计算机病毒**

1987 年，巴基斯坦盗拷软件盛行一时，一对经营贩卖个人计算机的巴基斯坦兄弟巴斯特(Basit)和阿姆捷特(Amjad)为了防止他们的软件被任意盗拷，编写出了一个叫作 C-BRAIN 的程序。只要有人盗拷他们的软件，C-BRAIN 就会发作，将盗拷者的剩余硬盘空间“吃掉”。虽然在当时这个病毒并没有太大的破坏性，但许多有心的同行以此为蓝图，衍生制作出一些该病毒的“变种”，以此为契机，许多个人或团队创作的新型病毒如雨后春笋般纷纷涌现。因此，业界公认 C-BRAIN 是真正具备完整特征的计算机病毒始祖。

**3. 第 1 代计算机病毒**

习惯上，人们一般称之为 DOS 时期病毒。1987 年，计算机病毒主要是引导型病毒，具有代表性的有“小球”和“石头”病毒。当时的计算机硬件较少，功能简单，一般需要通过软盘启动后使用。引导型病毒利用软盘的启动原理工作，它们修改系统启动扇区，在计算机启动时首先取得控制权，减少系统内存，修改磁盘读写中断，影响系统工作效率，在系统存取磁盘时进行传播。1989 年，可执行文件型病毒出现，它们利用 DOS 系统加载执行文件的机制工作，代表为“耶路撒冷”和“星期天”病毒，病毒代码在系统执行文件时取得控制权，修改 DOS 中断，在系统调用时进行传染，并将自己附加在可执行文件中，使文件长度增加。1990 年发展为复合型病毒，可感染 COM 和 EXE 文件。1992 年，伴随型病毒出现，它们利用 DOS 加载文件的优先顺序进行工作，具有代表性的是“金蝉”病毒，它感染 EXE 文件时生成一个同名但扩展名为 COM 的伴随体。这样，在 DOS 加载文件时，病毒就取得控制权。1994 年，随着汇编语言的发展，实现同一功能可以用不同的方式进行完成，这些方式的组合使一段看似随机的代码产生相同的运算结果。幽灵病毒就是利用这个特点，每感染一次就产生不同的代码。例如，“一半”病毒就是产生一段有上亿种可能的解码运算程序，病毒体被隐藏在解码前的数据中，查解这类病毒就必须能对这段数据进行解码，加大了查毒的难度。

DOS 时期病毒种类相当繁杂，不断有人改写已有的病毒。到了后期甚至有人写出所谓的“双体引擎”，可以把一种病毒创造出更多元化的面貌，让人防不胜防。而病毒发作的症状更是各式各样，有的会唱歌，有的会删除文件，有的会格式化硬盘，有的还会在屏幕上显示出

各式各样的图形。不过幸运的是,这些DOS时期的病毒,由于大部分的杀毒软件都可以轻易地扫除,因此杀伤力已经大不如前了。

**4. 第2代计算机病毒**

自从互联网出现,基于网络的计算机病毒开始迅猛发展。这种新的病毒由于与传统病毒有着本质区别,因此称为第2代计算机病毒。第2代病毒与第1代病毒最大的差异就在于其传染的途径是基于浏览器的。为了方便网页设计者在网页上能制造出更精彩的动画,让网页更有空间感,几家大公司联手制定出ActiveX和Java技术。而透过这些技术,甚至能够分辨使用的软件版本,建议应该下载哪些软件来更新版本,对于大部分的一般使用者来说是颇为方便的工具。但若想让这些网页的动画能够正常执行,浏览器会自动将这些ActiveX和Java Applets的程序下载到硬盘中。在这个过程中,恶意程序的开发者也就利用同样的渠道,经由网络渗透到个人计算机之中了。这就是目前流行的"第2代病毒",也就是所谓的"网络病毒"。

而今,随着现在电子邮件被用作一个重要的企业通信工具,病毒就比以往任何时候都要扩展得快。附着在电子邮件信息中的病毒,仅仅在几分钟内就可以浸染整个企业,让公司每年在生产损失和清除病毒开销上花费数百万美元。今后任何时候病毒都不会很快地消失。根据美国国家计算机安全协会发布的统计资料,已有超过数万种病毒被辨认出来,而且每个月都在产生几百至几千种新型病毒。为了安全,可以说大部分机构必须常规性地应对病毒的突然爆发。没有一个使用多台计算机的机构是对病毒免疫的。

### 5.1.5 其他的破坏行为

计算机病毒的破坏行为体现了病毒的杀伤能力。病毒破坏行为的激烈程度取决于病毒作者的主观愿望和所具有的技术能力。数以万计不断发展扩张的病毒,其破坏行为千奇百怪,不可能穷举,而且难以做全面的描述。根据现有的病毒资料可以将病毒的破坏目标和攻击部位归纳如下。

(1) 攻击系统数据区。攻击部位包括硬盘主引导扇区、Boot扇区、FAT表、文件目录等。一般来说,攻击系统数据区的病毒是恶意病毒,受损的数据不易恢复。

(2) 攻击文件。病毒对文件的攻击方式很多,可列举如下:删除、改名、替换内容、丢失部分程序代码、内容颠倒、写入时间空白、变碎片、假冒文件、丢失文件簇、丢失数据文件等。

(3) 攻击内存。内存是计算机的重要资源,也是病毒攻击的主要目标之一,病毒额外地占用和消耗系统的内存资源,可以导致一些较大的程序难以运行。病毒攻击内存的方式如下:占用大量内存、改变内存总量、禁止分配内存、蚕食内存等。

(4) 干扰系统运行。此类型病毒会干扰系统的正常运行,以此作为自己的破坏行为。此类行为也是花样繁多,主要包括:不执行命令、干扰内部命令的执行、虚假报警、使文件打不开、使内部栈溢出、占用特殊数据区、时钟倒转、重启动、死机、强制游戏、扰乱串行口、并行口等。

(5) 速度下降。病毒激活时,其内部的时间延迟程序启动,在时钟中纳入了时间的循环计数,迫使计算机空转,计算机速度明显下降。攻击磁盘数据、不写盘、写操作变读操作、写盘时丢字节等。

(6) 扰乱屏幕显示。主要包括:字符跌落、环绕、倒置、显示前一屏、光标下跌、滚屏、抖

动、乱写、吃字符等。

(7) 键盘病毒。干扰键盘操作,已发现如下方式:响铃、封锁键盘、换字、抹掉缓存区字符、重复、输入紊乱等。

(8) 喇叭病毒。许多病毒运行时会使计算机的喇叭发出声响。有的病毒作者通过喇叭发出种种声音,有的病毒作者让病毒演奏旋律优美的世界名曲,在高雅的曲调中去劫取人们的信息财富。已发现的喇叭发声有以下方式:演奏曲子、警笛声、炸弹噪声、鸣叫、咔咔声、嘀嗒声等。

(9) 攻击 CMOS。在机器的 CMOS 区中保存着系统的重要数据,如系统时钟、磁盘类型、内存容量等。有的病毒激活时,能够对 CMOS 区进行写入动作,破坏系统 CMOS 中的数据。

### 5.1.6 计算机病毒的危害性

在计算机病毒出现的初期,说到计算机病毒的危害,往往注重病毒对信息系统的直接破坏作用,如格式化硬盘、删除文件数据等,并以此区分恶性病毒和良性病毒。其实这些只是病毒劣迹的一部分,随着计算机应用的发展,人们深刻地认识到,凡是病毒都可能对计算机信息系统造成严重的破坏。

计算机病毒的主要危害如下。

**1. 病毒激活对计算机数据信息的直接破坏作用**

大部分病毒在激活的时候直接破坏计算机的重要信息数据,所利用的手段有格式化磁盘、改写文件分配表和目录区、删除重要文件,或者用无意义的"垃圾"数据改写文件、破坏 CMOS 设置等。例如,磁盘杀手病毒(Disk Killer)内含计数器,在硬盘染毒后累计开机时间 48 小时内激活,激活时屏幕上显示"Warning!! Don't turn off power or remove diskette while Disk Killer is Processing! (警告!! Disk Killer 在工作,不要关闭电源或取出磁盘!)",改写硬盘数据。被 Disk Killer 破坏的硬盘可以用杀毒软件修复,不要轻易放弃。

**2. 占用磁盘空间和对信息的破坏**

寄生在磁盘上的病毒总要非法占用一部分磁盘空间。引导型病毒的一般侵占方式是由病毒本身占据磁盘引导扇区,而把原来的引导区转移到其他扇区,也就是引导型病毒要覆盖一个磁盘扇区。被覆盖的扇区数据永久性丢失,无法恢复。文件型病毒利用一些 DOS 功能进行传染,这些 DOS 功能能够检测出磁盘的未用空间,把病毒的传染部分写到磁盘的未用部位。所以在传染过程中一般不破坏磁盘上的原有数据,但非法侵占了磁盘空间。一些文件型病毒传染速度很快,在短时间内感染大量文件,每个文件都不同程度地加长了,这就造成磁盘空间的严重浪费。

**3. 抢占系统资源**

除少数病毒外,其他大多数病毒在动态下都是常驻内存的,这就必然会抢占一部分系统资源。病毒所占用的基本内存长度大致与病毒本身长度相当。病毒抢占内存,导致内存减少,一部分软件不能运行。除占用内存外,病毒还抢占中断,干扰系统运行。计算机操作系统的很多功能是通过中断调用技术实现的。病毒为了传染激发,总是修改一些有关的中断地址,在正常中断过程中加入病毒的"私货",从而干扰系统的正常运行。

**4. 影响计算机运行速度**

病毒进驻内存后不但干扰系统运行,还影响计算机速度,主要表现如下。

(1) 病毒为了判断传染激发条件,总要对计算机的工作状态进行监视,这相对于计算机的正常运行状态既多余又有害。

(2) 有些病毒为了保护自己,不但对磁盘上的静态病毒加密,而且进驻内存后的动态病毒也处在加密状态,CPU 每次寻址到病毒处时要运行一段解密程序把加密的病毒解密成合法的 CPU 指令再执行,而病毒运行结束时再用一段程序对病毒重新加密。这样,CPU 额外执行数千条乃至上万条指令。

(3) 病毒在进行传染时同样要插入非法的额外操作,特别是传染软盘时,不但计算机速度明显变慢,而且软盘正常的读写顺序被打乱,发出刺耳的噪声。

**5. 计算机病毒错误与不可预见的危害**

计算机病毒与其他计算机软件的最大差别是病毒的无责任性。编制一个完善的计算机软件需要耗费大量的人力、物力,经过长时间调试完善,软件才能推出。但在病毒编制者看来既没有必要这样做,也不可能这样做。很多计算机病毒都是个别人在一台计算机上匆匆编制调试后就向外抛出,反病毒专家在分析大量病毒后发现绝大部分病毒都存在不同程度的错误。错误病毒的另一个主要来源是变种病毒。有些初学计算机者尚不具备独立编制软件的能力,出于好奇或其他原因修改别人的病毒,造成错误。计算机病毒错误所产生的后果往往是不可预见的,反病毒工作者曾经详细指出“黑色星期五”病毒存在 9 处错误;“乒乓”病毒存在 5 处错误等。但是人们不可能花费大量时间去分析数万种病毒的错误所在。大量含有未知错误的病毒扩散传播,其后果是难以预料的。

**6. 计算机病毒的兼容性对系统运行的影响**

兼容性是计算机软件的一项重要指标。兼容性好的软件可以在各种计算机环境下运行;反之,兼容性差的软件则对运行条件“挑肥拣瘦”,要求机型和操作系统版本等。病毒的编制者一般不会在各种计算机环境下对病毒进行测试,因此病毒的兼容性较差,常常导致死机。

**7. 计算机病毒给用户造成严重的心理压力**

据有关计算机销售部门统计,计算机用户怀疑“计算机有病毒”而提出咨询约占售后服务工作量的 60%以上。经检测确实存在病毒的约占 70%,另有约 30%的情况只是用户怀疑,而实际上计算机并没有病毒。那么用户怀疑有病毒的理由是什么呢? 多半是出现诸如计算机死机、软件运行异常等现象。这些现象确实很有可能是计算机病毒造成的,但又不全是,实际上在计算机工作“异常”的时候很难要求一位普通用户去准确判断是否是病毒所为。大多数用户对病毒采取宁可信其有的态度,这对于保护计算机安全无疑是十分必要的,然而往往要付出时间、金钱等方面的代价。仅仅怀疑病毒而贸然格式化磁盘所带来的损失更是难以弥补。不仅是个人计算机用户,一些大型网络系统也难免为甄别病毒而停机。总之,计算机病毒像“幽灵”一样笼罩在广大计算机用户心头,给人们造成巨大的心理压力,极大地影响了现代计算机的使用效率,由此带来的无形损失是难以估量的。

病毒对计算机的危害是众所周知的,轻则影响机器速度,重则破坏文件或造成死机。计算机病毒不仅对计算机产生影响,而且对人也会产生一定影响。当然,计算机病毒是不会与人交叉感染的,那么它是怎样对人产生影响的呢? 其实很简单,它通过控制屏幕的输出对人

的心理进行影响。有些按破坏能力分类归为“无害”的病毒，虽然不会损坏数据，但在发作时并不只是播放一段音乐这样简单。有些病毒会进行反动宣传；有些病毒会显示一些对人身心健康不利的文字或图像。2000 年年底，人们发现了一个通过电子邮件传播的病毒——“女鬼”病毒。当打开感染了“女鬼”病毒的邮件附件时，病毒发作，在屏幕上显示一个美食家杀害妻子的恐怖故事。之后，一切恢复正常。一般人会以为这个病毒的发作只是这样而已。但是，5 分钟后，屏幕突然变黑，一具恐怖女尸的图像就会显示出来，让没有丝毫心理准备的人吓一跳。据报道，有人因此突发心脏病身亡。所以，计算机病毒的这类危害也是不可小视的。

### 5.1.7 知名计算机病毒简介

**1. CIH**

CIH 病毒是一位名叫陈盈豪的中国台湾大学生编写的，从中国台湾传入大陆，是公认的有史以来危险程度最高、破坏强度最大的病毒。全球估计损失约 5 亿美元。

CIH 感染 Windows 95/98/ME 等操作系统的可执行文件，能够驻留在计算机内存中，并据此继续感染其他可执行文件。CIH 的危险之处在于，一旦被激活，它可以覆盖主机硬盘上的数据并导致硬盘失效。它还具备覆盖主板 BIOS 芯片的能力，从而使计算机引导失败。CIH 的一些变种的触发日期恰好是切尔诺贝利核电站事故发生之日，因此它也被称为切尔诺贝利病毒。1999 年 4 月 26 日，公众开始关注 CIH，首次发作时，全球不计其数的计算机硬盘被垃圾数据覆盖，甚至 BIOS 信息被破坏，无法启动。其发作特征如下。

(1) 以 2048 个扇区为单位，从硬盘主引导区开始依次向硬盘写入垃圾数据，直到硬盘数据被全部破坏为止。最坏的情况下硬盘所有数据(含全部逻辑盘数据)均被破坏，如果重要信息没有备份，那损失更是无法想象。

(2) 某些主板上的 Flash Rom 中的 BIOS 信息将被清除。

(3) v1.4 版本每月 26 日发作，v1.3 版本每年 6 月 26 日发作，以下版本每年 4 月 26 日发作。

**2. 梅利莎**

1999 年 3 月 26 日，星期五，“梅利莎”(Melissa)病毒登上了全球各地报纸的头版。这个 Word 宏脚本病毒感染了全球 15%～20%的商用 PC。病毒传播速度之快令英特尔公司、微软公司，以及其他许多使用 Outlook 的公司措手不及，为了防止损害，被迫关闭整个电子邮件系统。“梅利莎”病毒的编写者大卫·史密斯后被判处在联邦监狱服刑 20 个月，也算得到一点惩戒。全球估计损失约 3 亿～6 亿美元。

“梅利莎”病毒通过微软公司的 Outlook 软件向用户通讯簿名单中的 50 位联系人发送邮件进行传播。该邮件包含一句话：“这就是你请求的文档，不要给别人看”，此外还包含一个 Word 文档附件。单击这个文件，就会使病毒感染主机并且重复自我复制，一旦被激活，病毒就用动画片《辛普森一家》的台词修改用户的 Word 文档。

**3. 我爱你**

“我爱你”蠕虫病毒是一个 VB 脚本，又称为情书或爱虫。2000 年 5 月 3 日，“我爱你”蠕虫病毒首次在中国香港被发现。“我爱你”蠕虫病毒通过一封标题为“我爱你(I LOVE YOU)”，附件名称为 Love-Letter-For-You. TXT. vbs 的邮件进行传输。和“梅利莎”病毒类

似,该病毒也向 Outlook 通讯簿中的联系人发送自身,还大肆复制自身覆盖音乐和图片文件。它还会在受到感染的机器上搜索用户的账号和密码,并发送给病毒作者。打开病毒邮件附件,会观察到计算机的硬盘灯狂闪,系统速度显著变慢,计算机中出现大量的扩展名为.vbs 的文件。所有快捷方式被修改为与系统目录下 wscript.exe 建立关联,进一步消耗系统资源,造成系统崩溃。由于当时菲律宾并无制裁编写病毒程序的法律,"我爱你"病毒的作者因此逃过一劫。全球估计损失超过 100 亿美元。

**4. 红色代码**

"红色代码"(Code Red)是一种蠕虫病毒,能够通过网络进行传播。2001 年 7 月 13 日,"红色代码"病毒在网络服务器上传播开来。它专门针对运行微软公司互联网信息服务软件的网络服务器进行攻击。"红色代码"还被称为 Bady,设计者蓄意进行最大程度的破坏。被它感染后,遭受攻击的主机所控制的网络站点上会显示这样的信息:"你好! 欢迎光临 www.worm.com!"。随后,病毒便会主动寻找其他易受攻击的主机进行感染。这个行为持续大约 20 天,之后它便对某些特定 IP 地址发起拒绝服务攻击。在短短不到一周的时间内,这个病毒感染了近 40 万台服务器,据估计多达 100 万台计算机受到感染。全球估计损失约 26 亿美元。

**5. SQL Slammer**

SQL Slammer 也称为"蓝宝石",2003 年 1 月 25 日首次出现。它是一个非同寻常的蠕虫病毒,给互联网的流量造成了显而易见的负面影响。它的目标并非终端计算机用户,而是服务器。它是一个单包的、长度为 376B 的蠕虫病毒,随机产生 IP 地址,并向这些 IP 地址发送自身。如果某个 IP 地址恰好是一台运行着未打补丁的微软公司 SQL 服务器桌面引擎软件的计算机,它会迅速开始向随机 IP 地址的主机发射病毒。正是运用这种效果显著的传播方式,SQL Slammer 在 10min 之内感染了 7.5 万台计算机。庞大的数据流量令全球的路由器不堪重负,导致它们一个个被关闭。全球估计损失约上百亿美元。

**6. 冲击波**

对于依赖计算机运行的商业领域而言,2003 年夏天是一个艰难的时期。一波未平,一波又起。IT 人士在此期间受到了"冲击波"(Blaster)和"霸王虫"蠕虫的双面夹击。"冲击波"首先发起攻击。病毒最早于当年 8 月 11 日被检测出来并迅速传播,两天之内就达到了攻击顶峰。病毒通过网络连接和网络流量传播,利用了 Windows 2000/XP 的一个弱点进行攻击,被激活以后,它会向计算机用户展示一个恶意对话框,提示系统将关闭,如图 5.1 所示。在病毒的可执行文件中隐藏着这些信息:"桑,我只想说爱你!""比尔·盖茨,你为什么让这种事情发生? 别再敛财了,修补你的软件吧!"。


图 5.1 "冲击波"中毒症状

病毒还包含了可于 4 月 15 日向 Windows 升级网站发起分布式 DoS 攻击的代码。但那时,"冲击波"造成的损害已经过了高峰期,基本上得到了控制。估计损失数百亿美元。

**7. 霸王虫**

"冲击波"一走,"霸王虫"(Sobig.F)蠕虫便接踵而至,对企业和家庭计算机用户而言,

2003 年 8 月可谓悲惨的一个月。最具破坏力的变种是 Sobig. F，它于 8 月 19 日开始迅速传播，在最初的 24 小时之内，自身复制了 100 万次，创下了历史纪录（后来被 MyDoom 病毒打破）。病毒伪装在文件名看似无害的邮件附件之中，被激活之后，这个蠕虫便向用户的本地文件类型中发现的电子邮件地址传播自身，最终结果是造成互联网流量激增。估计损失 50 亿～100 亿美元。

2003 年 9 月 10 日，病毒禁用了自身，从此不再成为威胁。为得到线索，找出 Sobig. F 病毒的始作俑者，微软公司宣布悬赏 25 万美元，但至今为止，这个作恶者也没有被抓到。

**8. Bagle**

Bagle 是一个经典而复杂的蠕虫病毒，2004 年 1 月 18 日首次出现。这个恶意代码采取传统的机制，电子邮件附件感染用户系统，然后彻查视窗文件，寻找到电子邮件地址发送以复制自身。

Bagle 及其 60～100 个变种的真正危险在于，蠕虫感染了一台计算机之后，便在其 TCP 端口开启一个后门，远程用户和应用程序利用这个后门得到受感染系统上的数据（包括金融和个人信息在内的任何数据）访问权限。Bagle. B 变种被设计为在 2004 年 1 月 28 日以后停止传播，但是到目前为止还有大量的其他变种继续困扰用户。估计损失 100 亿～200 亿美元。

**9. MyDoom**

2004 年 1 月 26 日，几个小时之间，MyDoom 通过电子邮件在互联网上以史无前例的速度迅速传播，顷刻之间全球都能感受到它所带来的冲击。它还有一个名称叫作 Norvarg，它传播自身的方式极为迂回曲折：把自己伪装成一封包含错误信息“邮件处理失败”的看似电子邮件错误信息邮件的附件。单击这个附件，它就被传播到了地址簿中的其他地址。MyDoom 还试图通过 P2P 软件 Kazaa 用户账户的共享文件夹进行传播。

这个复制进程相当成功，计算机安全专家估计，在受到感染的最初一小时，每 10 封电子邮件中就有一封携带 MyDoom 病毒。MyDoom 病毒程序自身设计为 2004 年 2 月 12 日以后停止传播。估计损失 385 亿美元以上。

**10. 震荡波**

“震荡波”（Sasser）病毒自 2004 年 8 月 30 日起开始传播，其破坏能力之大令法国一些新闻机构不得不关闭了卫星通信。它还导致德尔塔航空公司（Delta）取消了数个航班，全球范围内的许多公司不得不关闭系统。“震荡波”的传播并非通过电子邮件，也不需要用户的交互动作。“震荡波”病毒利用了未升级的 Windows 2000/XP 系统的一个安全漏洞，一旦成功复制，蠕虫便主动扫描其他未受保护的系统并将自身传播到那里。受感染的系统会不断发生崩溃和不稳定的情况。

“震荡波”是德国一名高中生编写的，他在 18 岁生日那天释放了这个病毒。由于编写这些代码的时候他还是一个未成年人，德国一家法庭认定他从事计算机破坏活动，因此仅被判处 21 个月监禁（缓期执行）及社区服务。估计损失 5 亿～10 亿美元。

**11. 网游大盗**

“网游大盗”出现于 2007 年，是一例专门盗取网络游戏账号和密码的病毒，其变种 wm 是典型品种。英文名为 Trojan/PSW. GamePass. jws 的“网游大盗”变种中，jws 是“网游大盗”木马家族最新变种，采用 Visual C++编写，并经过加壳处理。“网游大盗”变种 jws 运行

后会将自我复制到 Windows 目录下,自我注册为 Windows_Down 系统服务,实现开机自启。该病毒会盗取包括《魔兽世界》《完美世界》《征途》等多款网游玩家的账户和密码,并且会下载其他病毒到本地运行。玩家计算机一旦中毒,就可能导致游戏账号、装备等丢失。"网游大盗"在 2007 年轰动一时,网游玩家提心吊胆。估计损失数千万美元。

视频讲解

## 5.2 网络病毒

网络病毒通过计算机网络传播感染网络中的可执行文件(如 COM、EXE、DOC 等),主要进行游戏等账号的盗取工作、远程操控,或把受控者的计算机当作"肉鸡"使用。

具有开放性的互联网成为计算机病毒广泛传播的有利环境,而互联网本身的安全漏洞为培育新一代病毒提供了绝佳的条件。人们为了让网页更加精彩漂亮、功能更加强大而开发出 ActiveX 技术和 Java 技术,然而,病毒程序的制造者也利用同样的渠道把病毒程序由网络渗透到个人计算机中。这就是近些年崛起的第 2 代病毒,即所谓的"网络病毒"。可以说:网络是病毒的天堂。

2000 年出现的"罗密欧与朱丽叶"病毒是一个典型的网络病毒,它改写了病毒的历史。在当时,人们还以为病毒技术的发展速度不会太快,然而,"罗密欧与朱丽叶"病毒彻底击碎了人们的侥幸心理。"罗密欧与朱丽叶"病毒具有邮件病毒的所有特性,但它不再藏身于电子邮件的附件中,而是直接存在于邮件正文中,一旦计算机用户用 Outlook 打开邮件进行阅读,病毒就会立即发作,并将复制出的新病毒通过邮件发送给其他人,计算机用户几乎无法躲避。

网络病毒的出现似乎拓展了病毒制造者的思路,在随后的时间里,千奇百怪的网络病毒不断诞生。这些病毒具有更强的繁殖能力和破坏能力,它们不再局限于电子邮件之中,而是直接植入 Web 服务器的网页代码,当计算机用户浏览了带有病毒的网页之后,系统就会被感染,随即崩溃。当然,这些病毒也不会放过自己寄生的服务器,在适当的时候病毒会与服务器系统同归于尽。

国家信息中心联合瑞星公司共同发布的《2020 年中国网络安全报告》统计,2020 年瑞星"云安全"系统共截获病毒样本总量 1.48 亿个,病毒感染次数 3.52 亿次,病毒总体数量比 2019 年同期上涨 43.71%。

近年来,病毒功能越来越强大,不仅拥有蠕虫病毒的传播速度和破坏能力,还具有木马的控制计算机和盗窃重要信息的功能。2000 年以来,病毒制造者为了获得经济利益,纷纷开始制作各类木马,一时间网上木马横行。

2006 年,"熊猫烧香"这一复合型病毒的出现改变了病毒制造者的想法。利用蠕虫的传播能力和多种传播渠道,可以更快、更多地帮助木马传播,从而攫取更大的非法经济效益。因此,"熊猫烧香"病毒在几个月的时间里感染了大量机器,给被感染的用户带来重大损失。

根据病毒感染人数、变种数量和代表性综合评估,瑞星评选出 2020 年病毒 Top5:①Adware.Adpop,主要表现为流氓软件使用的弹窗模块;②Trojan.Shadow Brokers,主要表现为入侵了美国国家安全局的方程式小组,窃取了黑客工具包并免费发布,被病毒广泛使用以进行蠕虫传播;③Trojan.Vools,主要表现为"永恒之蓝"漏洞传播,攻击局域网中的计算机;④Adware.Downloader,主要表现为传播挖矿木马高速下载器,后台恶意推广流氓软件;⑤Troian.Inject,主要表现为恶意 Crypter 打包程序,常用来保护后门、木马、间谍软件,

达到逃避安全软件检测目的。

勒索软件和挖矿病毒在2020年依旧占据着重要位置，报告期内瑞星“云安全”系统共截获勒索软件样本156万个，感染次数为86万次，病毒总体数量比2019年同期下降了10.84%；挖矿病毒样本总体数量为922万个，感染次数为578万次，病毒总体数量比2019年同期上涨332.32%。瑞星通过对捕获的勒索软件样本进行分析后发现，Landcrab家族占比为67%，成为第一大类勒索软件；其次是Eris家族，占总量的13%；第三是Lockscreen家族，占总量的2%。

### 5.2.1 木马病毒的概念

特洛伊木马(Trojan Horse，简称木马)，其名称取自希腊神话的《特洛伊木马记》。故事说的是希腊人围攻特洛伊城10年仍不能得手，于是阿伽门农受雅典娜的启发，把士兵藏匿于巨大无比的木马中，然后佯作退兵。当特洛伊人将木马作为战利品拖入城内时，高大的木马正好卡在城门间，进退两难。夜晚，木马内的士兵爬出来，与城外的部队里应外合攻下了特洛伊城。计算机世界的特洛伊木马是指隐藏在正常程序中的一段具有特殊功能的恶意代码，是具备破坏和删除文件、发送密码、记录键盘和DoS攻击等特殊功能的后门程序。它是一种基于远程控制的黑客工具，具有隐蔽性和非授权性的特点。木马病毒的产生严重危害着现代网络的安全运行。

所谓隐蔽性，是指设计者为了防止木马被发现，会采用多种手段隐藏木马，这样服务端即使发现感染了木马，由于不能确定其具体位置，往往只能望“马”兴叹。

所谓非授权性，是指一旦控制端与服务端连接后，控制端将享有服务端的大部分操作权限，包括修改文件、修改注册表、控制鼠标和键盘等，这些权限并不是服务端赋予的，而是通过木马程序窃取的。

木马和病毒都是一种人为的程序，都属于计算机病毒，为什么木马要单独提出来说？大家都知道，以前的计算机病毒其实完全就是为了破坏计算机中的资料数据。除了破坏之外，有些病毒制造者为了达到某些目的而进行的威慑和敲诈勒索行为，就是为了炫耀自己的技术。木马不一样，木马的作用是赤裸裸地偷偷监视别人和盗窃别人密码、数据等。例如，盗窃管理员密码、子网密码搞破坏；或者出于好玩，偷窃上网密码用于他用；窃取游戏账号、股票账号、网上银行账户等，达到偷窥别人隐私和得到经济利益的目的。所以木马比早期的计算机病毒更加有害，更能够直接达到使用者的目的，导致许多别有用心的程序开发者大量编写这类带有偷窃和监视别人计算机的侵入性程序，这就是目前网上大量木马泛滥成灾的原因。鉴于木马的这些巨大危害性和它与早期病毒的作用性质不一样，因此木马虽然属于病毒中的一类，但是要单独地从病毒类型中间剥离出来，称为“木马”程序。

“木马”程序是指通过一段特定的程序控制另一台计算机。木马通常有两个可执行程序：一个是客户端，即控制端；另一个是服务端，即被控制端。植入被控制计算机的是“服务器”部分，而所谓的“黑客”正是利用“控制器”进入运行了“服务器”的计算机。运行了木马程序的“服务器”以后，被植入的计算机就会有一个或几个端口被打开，使黑客可以利用这些打开的端口进入计算机系统，安全和个人隐私也就全无保障了。木马的设计者为了防止木马被发现而采用多种手段隐藏木马。木马的服务一旦运行并被控制端连接，其控制端将享有服务端的大部分操作权限，如给计算机增加口令，浏览、移动、复制、删除文件，修改注册

表,更改计算机配置等。随着病毒编写技术的发展,木马程序对用户的威胁越来越大,尤其是一些木马程序采用了极其狡猾的手段隐蔽自己,使普通用户在中毒后很难发觉。

木马的发展可以分为以下几个阶段。

**1. 第1代木马:伪装型病毒**

这种病毒通过伪装成一个合法性程序诱骗用户上当。世界上第1个计算机木马是出现在1986年的PC-Write木马。它伪装成共享软件PC-Write的2.72版本(事实上,编写PC-Write的Quicksoft公司从未发行过2.72版本),一旦用户信以为真,运行该木马程序,那么下场就是硬盘被格式化。有人用BASIC做了一个登录界面木马程序,当用户把他的用户ID、密码输入一个和正常的登录界面一模一样的伪登录界面后,木马程序一边保存用户的ID和密码,一边提示用户密码错误让用户重新输入,当用户第2次登录时,就已成了木马的牺牲品。此时的第1代木马还不具备传染特征。

**2. 第2代木马:AIDS木马**

继PC-Write之后,1989年出现了AIDS木马。由于当时很少有人使用电子邮件,因此AIDS木马的作者就利用现实生活中的邮件进行散播:给其他人寄去一封封含有木马程序软盘的邮件。之所以叫这个名称是因为软盘中包含AIDS疾病的药品、价格、预防措施等相关信息。软盘中的木马程序在运行后,虽然不会破坏数据,但是它将硬盘加密锁死,然后提示受感染用户花钱消灾。可以说第2代木马已具备了传播特征(尽管通过传统的邮递方式)。

**3. 第3代木马:网络传播型木马**

随着Internet的普及,这一代木马兼备伪装和传播两种特征并结合TCP/IP网络技术四处泛滥。同时,它还添加了新的特征——"后门"功能。所谓后门,就是一种可以为计算机系统秘密开启访问入口的程序。一旦被安装,这些程序就能够使攻击者绕过安全程序进入系统。该功能的目的就是收集系统中的重要信息,如财务报告、口令和信用卡号。此外,攻击者还可以利用后门控制系统,使之成为攻击其他计算机的帮凶。由于后门是隐藏在系统背后运行的,因此很难被检测到。它们不像病毒和蠕虫那样通过消耗内存而引起注意。图5.2所示为QQ软件中木马病毒时的现象。

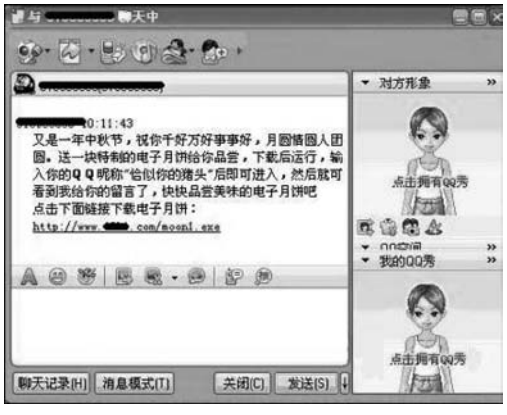


图5.2 QQ软件中木马病毒时的现象

第3代木马添加了击键记录功能。从名称上就可以知道,该功能主要是记录用户所有的击键内容,然后形成击键记录的日志文件发送给恶意用户。恶意用户可以从中找到用户名、口令和信用卡号等用户信息。这一代木马中比较有名的有国外的BO2000和国内的"冰河"木马。它们有以下共同特点:基于网络的客户端/服务器应用程序,具有搜集信息、执行系统命令、重新设置机器、重新定向等功能。当木马程序攻击得手后,计算机就完全成为黑客控制的傀儡主机,黑客成了超级用户,用户的所有计算机操作不但没有任何秘密而言,而且黑客可以远程控制傀儡主机对别的主机发动攻击,这时候被俘获的傀儡主机成了黑客进行进一步攻击的挡箭牌和跳板。

**4. 网页挂马**

网页挂马指的是把一个木马程序上传到一个网站上，然后用木马生成器生成一个木马，上传到网站空间里面，再添加代码使木马在打开网页时运行。

网页挂马常见方式主要有以下几种。

(1) 将木马伪装为页面元素，木马则会被浏览器自动下载到本地。

(2) 利用脚本运行的漏洞下载木马。

(3) 利用脚本运行的漏洞释放隐含在网页脚本中的木马。

(4) 将木马伪装为缺失的组件，或和缺失的组件捆绑在一起(如 Flash 播放插件)。这样既达到了下载的目的，下载的组件又会被浏览器自动执行。

(5) 通过脚本运行调用某些 COM 组件，利用其漏洞下载木马。

(6) 在渲染页面内容的过程中利用格式溢出释放木马(如 ANI 格式溢出漏洞)。

(7) 在渲染页面内容的过程中利用格式溢出下载木马(如 Flash 9.0.115 的播放漏洞)。

虽然木马程序手段越来越隐蔽，只要加强个人安全防范意识，还是可以大大降低“中招”的概率。对此有如下建议：安装个人防病毒软件、个人防火墙软件；及时安装系统补丁；对不明来历的电子邮件和插件不予理睬；经常去安全网站转一转，以便及时了解一些新木马的底细，做到知己知彼，百战不殆。

## 5.2.2 木马的种类

**1. 网游木马**

随着网络在线游戏的普及和升温，中国拥有规模庞大的网游玩家。网络游戏中的金币、装备等虚拟财富与现实财富之间的界限越来越模糊。与此同时，以盗取网游账号、密码为目的的网游木马病毒也随之发展泛滥起来。网游木马通常采用记录用户键盘输入、截获(Hook)游戏进程 API 函数等方法获取用户的密码和账号。窃取到的信息一般通过电子邮件或向远程脚本程序提交的方式发送给木马作者。

网游木马的种类和数量在国产木马病毒中都首屈一指。流行的网络游戏无一不受网游木马的威胁。一款新游戏正式发布后，往往在一到两个星期内就会有相应的木马程序被制作出来。大量的木马生成器和黑客网站的公开销售也是网游木马泛滥的原因之一。

**2. 网银木马**

网银木马是针对网上交易系统编写的木马病毒，其目的是盗取用户的卡号、密码，甚至安全证书。此类木马种类数量虽然比不上网游木马，但它的危害更加直接，受害用户的损失更加惨重。

网银木马通常针对性较强，木马作者首先对某银行的网上交易系统进行仔细分析，然后针对安全薄弱环节编写病毒程序。2013 年，安全软件计算机管家截获网银木马最新变种“弼马温”，它能够毫无痕迹地修改支付界面，使用户根本无法察觉。木马通过不良网站提供假 Qvod 下载地址进行广泛传播，当用户下载这一挂马播放器安装后就会中木马，该病毒运行后即开始监视用户网络交易，屏蔽余额支付和快捷支付，强制用户使用网银，并借机篡改订单，盗取财产。随着我国网上交易的普及，受到外来网银木马威胁的用户也在不断增加。

**3. 下载器木马**

这种木马程序的体积一般很小，其功能是从网络上下载其他病毒程序或安装广告软件。

由于体积很小,下载器木马更容易传播,传播速度也更快。通常功能强大、体积也很大的后门类病毒,如“灰鸽子”“黑洞”等,传播时都单独编写一个小巧的下载器木马,用户中毒后会把后门主程序下载到本机运行。

**4. 代理类木马**

用户感染此类木马程序后,会在本机开启 HTTP、SOCKS 等代理服务功能。黑客将受感染计算机作为跳板,以被感染用户的身份进行黑客活动,达到隐藏自己的目的。

**5. FTP 木马**

FTP 木马打开被控制计算机的 21 号端口(FTP 所使用的默认端口),使每个人不用密码就可以将 FTP 客户端程序连接到受控制端计算机,并且可以进行最高权限的上传和下载,窃取受害者的机密文件。新 FTP 木马还加上了密码功能,这样,只有攻击者本人才知道正确的密码,从而进入对方计算机。

**6. 通信软件类木马**

此类木马可以感染即时通信软件。国内即时通信软件百花齐放,网上聊天用户群十分庞大。常见的通信软件类木马一般有以下 3 种。

1) 发送消息型

通过即时通信软件自动发送含有恶意网址的消息,目的在于让收到消息的用户点击网址中毒,用户中毒后又会向更多好友发送病毒消息。此类病毒的常用技术是搜索聊天窗口,进而控制该窗口自动发送文本内容。发送消息型木马常常充当网游木马的广告,如“武汉男生 2005”木马,可以通过 MSN、QQ、UC 等多种聊天软件发送带毒网址,其主要功能是盗取《传奇》游戏的账号和密码。

2) 盗号型

此类木马的主要目标为即时通信软件的登录账号和密码,工作原理和网游木马类似。病毒作者盗得他人账号后,可能偷窥聊天记录等隐私内容,在各种通信软件内向好友发送不良信息、广告推销等,或将账号卖掉赚取利润。

3) 传播自身型

2005 年年初,“MSN 性感鸡”等通过 MSN 传播的蠕虫泛滥了一阵之后,MSN 推出新版本,禁止用户传送可执行文件。2005 年上半年,“QQ 龟”和“QQ 爱虫”这两个国产病毒通过 QQ 聊天软件发送自身进行传播,感染用户数量极大,在江民公司统计的 2005 年上半年十大病毒排行榜上分列第 1 名和第 4 名。从技术角度分析,发送文件类的 QQ 蠕虫是以前发送消息类 QQ 木马的进化,采用的基本技术都是搜寻到聊天窗口后,对聊天窗口进行控制以达到发送文件或消息的目的,只不过发送文件的操作比发送消息复杂很多。

**7. 网页点击类木马**

此类木马会恶意模拟用户点击广告等动作,在短时间内可以产生数以万计的点击量。病毒作者的编写目的一般是赚取高额的广告推广费用。此类木马的技术简单,一般只是向服务器发送 HTTP GET 请求。

### 5.2.3 木马病毒案例

木马病毒在互联网时代让无数网民深受其害。无论是网购、网银还是网游的账户和密码,只要与钱有关的网络交易都是当下木马攻击的重灾区,用户稍有不慎极有可能遭受重大

钱财损失甚至隐私被窃。下面列举一些比较典型的案例。

**1. “支付大盗”花钱上百度首页**

2012 年 12 月 6 日，一个名为“支付大盗”的新型网购木马被发现。木马网站利用百度排名机制伪装为“阿里旺旺官网”，诱骗网友下载运行木马，再暗中劫持受害者网上支付资金，把付款对象篡改为黑客账户。

**2. “新鬼影”借《江南 Style》疯传**

火遍全球的《江南 Style》很不幸被一个名为“新鬼影”的木马盯上了。只要下载打开《江南 Style》相关视频文件，浏览器主页就被篡改为陌生网址导航。此木马主要寄生在硬盘 MBR（主引导扇区）中，如果用户计算机没有开启安全软件防护，中招后无论是重装系统还是格式化硬盘，都无法将其彻底清除干净。

**3. “图片大盗”最爱私密照**

绝大多数网民都有一个困惑，为什么自己计算机中的私密照会莫名其妙地出现在网上。“图片大盗”木马运行后会全盘扫描搜集 JPG、PNG 格式图片，并筛选大小为 100KB～2MB 的文件，将其暗中发送到黑客服务器上，对受害者隐私造成严重危害。

**4. “浮云”木马震惊全国**

盗取网民钱财高达千万元的“浮云”成为 2012 年度震惊全国的木马。首先诱骗网民支付一笔小额假订单，却在后台执行另外一个高额订单，用户确认后，高额转账资金就会进入黑客的账户。该木马可以对 20 多家银行的网上交易系统实施盗窃。

**5. “黏虫”木马专盗 QQ**

“QQ 黏虫”在 2011 年度就被业界评为十大高危木马之一，2012 年该木马变种卷土重来，伪装成 QQ 登录框窃取用户 QQ 账号及密码。值得警惕的是，不法分子盗窃 QQ 后，除了窃取账号关联的虚拟财产外，还有可能假冒身份向被害者的亲友借钱。

**6. Loapi 木马**

2017 年，安全工作者发现了 Trojan. AndroidOS. Loapi 木马，该木马结构复杂，与之前的木马病毒相比，它可以做非常多的恶意活动，可谓“全能”，如订阅付费服务、持续发送广告、挖矿、DDoS 攻击等。Loapi 恶意家族样本被放置到广告重定向的网页中，当用户点击之后就会进行下载，恶意网页大多为主流的反病毒软件。在用户成功安装之后，会循环向用户发送请求直到获取到 Administrator 权限，然后隐藏图标或伪装成其他的应用。此木马同时查看用户有没有被 Root 过，虽然没有使用 Root 权限，但是很显然 Root 权限在将来的某些模块中会用到。Loapi 使用了一种防止被移除的技术，安装成功之后会调用手机的管理权限，当用户不想继续授权时，Loapi 会将用户手机锁屏并关闭设备管理器设定的窗口。

**7. Kemoge 木马病毒**

Kemoge 同其他手机木马病毒一样，通过伪装成正常的软件进行病毒的传播。Loapi 木马会检测用户手机有没有被 Root 过，但当时并不会直接使用此权限；Kemoge 病毒软件安装成功之后，会直接获取用户手机 Root 权限，并使用此权限进行恶意操作，如自主下载安装无用的软件，删除 360 安全卫士、手机管家等安全检测软件等，同时会不停地给用户发送广告。

Kemoge 会时刻监听用户手机，一旦手机解锁并处于网络连接状态，就会启动。判断用户手机是否已经被 Root 过，如果没有，则解密资源文件 info. mp4，以获取 Root 权限开展后

续操作。为了保证病毒能获取 Root 权限,info.mp4 中包含了 8 个 Root 工具。病毒获取权限之后,会将安装包安装到系统目录下,并重命名,使用户难以察觉,因此,即使用户将手机重置,依旧无法删除该病毒。

**8. CTB-Locker 木马病毒**

CTB-Locker 又名比特币敲诈者,该病毒通过远程加密用户计算机文件,从而向用户勒索赎金。由于病毒作者要求的赎金并非美元,而是比特币,因此获得了比特币敲诈者的名号。据悉,该病毒首先通过邮件发送病毒样本,之后在大量垃圾指令的掩护下,动态解密自身并将自身复制到 Temp 目录,实现自启。待网友打开 Office 等文件时,便会自动被加密,无法打开。值得一提的是,CTB-Locker 的作者是俄罗斯知名黑客艾维盖尼耶·米哈伊洛维奇·波格契夫,在 FBI 通缉 10 大黑客名单中排名第 2。在 CTB-Locker 病毒大范围传播后,FBI 也对该病毒束手无策,只得将波格契夫的悬赏金调高至 300 万美元。这也是 FBI 在网络犯罪案件中所提供的最高悬赏金。

**9. "大灰狼"远控木马**

360 安全团队披露 BT 天堂网站挂马事件,该网站被利用 IE 神洞 CVE-2014-6332 挂马,如果用户没有给应用软件打补丁或开启安全软件防护,计算机会自动下载执行"大灰狼"远控木马程序。"大灰狼"远控木马由于长期被杀毒软件追杀,所以大量使用动态调用系统 API 躲避查杀,所有的文件相关操作都采用了动态调用的方式,并且几乎所有的样本都需要动态的解码才能获取到相关的函数调用。木马进入计算机后会强制安装大量软件赚取推广费,同时计算机还会被植入 Gh0st 远程控制木马,木马作者能够窃取任意文件或监视键盘操作,甚至开启摄像头偷窥。

**10. Xcode Ghost 手机木马病毒**

该木马病毒主要通过非官方下载的 Xcode 传播,能够在开发过程中通过 CoreService 库文件进行感染,使编译出的 App 被注入第三方的代码,向指定网站上传用户数据。也就是说,当应用开发者使用带毒的 Xcode 工作时,编译出的 App 都将被注入病毒代码,从而产生众多带毒 App,并且苹果应用商店 AppStore 无法检测出这种病毒,因为商店审核只能确定 App 调用了哪些系统 API,于是带毒应用顺利进入 AppStore,而广大用户则通过 AppStore 下载到了病毒应用。

### 5.2.4 木马病毒的防治

**1. 防范木马攻击的主要措施**

(1) 运行反木马实时监控程序。

我们在上网时必须运行反木马实时监控程序,实时监控程序可即时显示当前所有运行程序并配有相关的详细描述信息。另外,也可以采用一些专业的最新杀毒软件、个人防火墙进行监控。

(2) 不要执行任何来历不明的软件。

对于网上下载的软件在安装、使用前一定要用反病毒软件进行检查,最好是专门查杀木马程序的软件,确定没有木马程序后再执行、使用。

(3) 不要轻易打开不熟悉的邮件。

现在,很多木马程序附加在邮件的附件之中,收邮件者一旦点击附件,它就会立即运行。

所以，千万不要打开那些不熟悉的邮件，特别是标题有点乱的邮件，这些邮件往往就是木马携带者。

(4) 不要轻信他人。

不要因为是我们的好朋友发来的软件就运行，因为不能确保他的计算机上就不会有木马程序。当然，好朋友故意欺骗你的可能性不大，但也许他中了木马自己还不知道呢。况且今天的互联网到处充满了危机，也不能保证这一定是好朋友发给我们的，也许是别人冒名给我们发的文件，或者就是木马程序本身发来的。例如，最常见的“QQ 尾巴”病毒，经常会冒充主人给好友发来附件。

(5) 不要随意下载软件。

不要随便在网上下载一些盗版软件，特别是从一些不可靠的 FTP 站点、公众新闻组、论坛或 BBS，因为这些正是新木马发布的首选之地。

(6) 将 Windows 资源管理器配置成始终显示扩展名。

一些扩展名为 VBS、SHS、PIF 的文件多为木马程序的特征文件，一经发现，要立即删除，千万不要打开。

(7) 尽量少用共享文件夹。

如果计算机连接在互联网或局域网上，要少用、尽量不用共享文件夹。如果因工作等其他原因必须设置成共享，则最好单独开一个共享文件夹，把所有需共享的文件都放在这个共享文件夹中。注意，千万不能把系统目录设置成共享。

(8) 隐藏 IP 地址。

这一点非常重要。在上网时，最好用一些工具软件隐藏自己计算机的 IP 地址。

前面讲了防范木马程序攻击的 8 个方法，似乎已经很安全了。但是，我们知道的方法，木马程序设计者自然也会知道，他们会想尽一切办法，尽量避免被我们预防到。

**2. 木马病毒的检测**

如果怀疑自己的计算机上被别人安装了木马，或者是中了病毒，就要进行相应的检测与查杀了，可以按照以下步骤进行。

(1) 检测网络连接。

可以使用 Windows 自带的网络命令查看谁在连接你的计算机。

具体的命令格式为 netstat -an，这个命令能看到所有和本地计算机建立连接的 IP，它包含 4 部分：Proto(连接方式)、Local Address(本地连接地址)、Foreign Address(和本地建立连接的地址)和 State(当前端口状态)。通过这个命令执行结果的详细信息，就可以完全监控计算机上的连接，从而达到控制计算机的目的。

(2) 禁用不明服务。

如果在某天系统重新启动后发现计算机速度变慢了，不管怎么优化都慢，用杀毒软件也查不出问题，这个时候很可能是别人通过入侵你的计算机后开放了某种特别的服务，如 IIS 信息服务等，这样杀毒软件是查不出来的。但是可以查看系统中究竟有什么服务被开启，如果发现了不是自己开启的服务，就可以有针对性地禁用这个服务。方法就是在命令行窗口中直接输入 net start 查看服务，再用 net stop server 命令禁止服务。

(3) 轻松检查账户。

很长一段时间，恶意攻击者非常喜欢使用复制账号的方法控制计算机。采用的方法就

是激活一个系统中的默认账户,但这个账户是不经常用的,然后使用工具把这个账户提升到管理员权限,从表面上来看这个账户还是和原来一样,但是这个复制的账户却是系统中最大的安全隐患。恶意攻击者可以通过这个账户任意地控制计算机。

为了避免这种情况,可以对账户进行检测。首先在命令行输入 net user,查看计算机上有些什么用户,然后再使用"net user 用户名"命令查看这个用户属于什么权限。一般除了 Administrator 是 administrators 组的以外,其他都不是,如果发现一个系统内置的用户是属于 administrators 组的,那几乎肯定被入侵了,而且别人在计算机上复制了账户。可以使用"net user 用户名/del"命令删掉这个账户。

对于没有联网的客户端,当其联网之后也会在第一时间内收到更新信息将病毒特征库更新到最新版本,不仅省去了用户手动更新的烦琐过程,也使用户的计算机时刻处于最佳的保护环境之下。

(4) 对比系统服务项。

首先执行"开始"→"运行"命令,在打开的对话框中输入 msconfig.exe 后按 Enter 键,打开系统配置实用程序,然后在"服务"选项卡中勾选"隐藏所有 Microsoft 服务"复选框,这时列表中显示的服务项都是非系统程序。

再执行"开始"→"运行"命令,在打开的对话框中输入 Services.msc 后按 Enter 键,打开系统服务管理,对比两张表,在该"服务列表"中可以逐一找出刚才显示的非系统服务项。

然后在"系统服务"管理界面中找到那些服务后双击打开,在"常规"选项卡中的可执行文件路径中可以看到服务的可执行文件位置,一般正常安装的程序,如杀毒软件、MSN、防火墙等都会建立自己的系统服务,不在系统目录下,如果有第三方服务指向的路径是在系统目录,那么它就是木马。选中它,选择表中的"禁止",重新启动计算机即可。

**3. 木马病毒的查杀**

木马病毒的查杀可以采用手动和自动两种方式。最简单的方式是安装杀毒软件,当今国内很多杀毒软件(如 360、瑞星、金山毒霸等)都能删除网络中最猖獗的木马。使用杀毒软件的步骤如下。

(1) 升级杀毒软件到最新版本,保证病毒库是最新的。

(2) 对于局域网内部用户,在杀毒之前请断开网络。

(3) 重启计算机,开机后按 F8 键,再按 Enter 键,进入"安全模式"进行杀毒。在 Windows 下杀毒会有些不放心,因为它们极有可能会交叉感染。而一些杀毒程序又无法在 DOS 下运行,这时可以把系统启动至安全模式,使 Windows 只加载最基本的驱动程序,这样杀毒就更彻底、更干净了。

(4) 杀毒之前确认扫描选项中的"杀毒前备份染毒文件""在杀毒前先扫描内存中的病毒"被选中,不要选中"染毒文件清除失败后删除此文件"选项。因为经验证明,很多病毒都是内存驻留型,备份染毒文件是因为没有哪个杀毒软件能保证杀过毒之后的文件 100%能够正常使用。

(5) 碰到病毒已经清除,但系统重新启动又出现中毒情况的,请确认所在网络无毒,然后制作 USB 启动盘在 Windows PE 环境下查杀。如果网络中毒,请联系网络管理员,断网杀毒(Windows PE 是在 Windows 内核上构建的具有有限服务的最小 Win32 子系统,可以方便地从网络文件服务器上复制磁盘映像并启动 Windows 安装程序)。

(6) 如果经过以上步骤后还能发现木马病毒，就需要到网上查找是否有相关病毒的专用杀毒工具了。专用杀毒工具杀毒精确性相对较高，因此推荐在条件许可的情况下使用专用杀毒工具。

**4. 木马病毒的手工查杀**

用杀毒软件相对简单方便，但杀毒软件的升级通常慢于新木马的出现，因此学会手工查杀很有必要。常用方法如下。

(1) 检查注册表。从“开始”菜单运行 regedit，打开注册表编辑器，注意在检查注册表之前要先备份注册表。检查 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run 和 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runserveice，查看键值中有没有自己不熟悉的自启动文件，它的扩展名一般为 EXE，然后记住木马程序的文件名，再在整个注册表中搜索，凡是看到相同的文件名的键值就删除，接着到计算机中找到木马文件的藏身地将其彻底删除。

(2) 检查 HKEY_LOCAL_MACHINE 和 HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main 中的几项(如 Local Page)，如果发现键值被修改了，只要根据判断改回去即可。恶意代码(如“万花谷”)就经常修改这几项。

(3) 检查 HKEY_CLASSES_ROOT\inifile\shell\open\command 和 HKEY_CLASSES_ROOT\txtfile\shell\open\command 等几个常用文件类型的默认打开程序是否被更改，若有更改一定要改回来，很多病毒就是通过修改 TXT 和 INI 等文件类型的默认打开程序而清除不了。

(4) 检查系统配置文件。从“开始”菜单运行 msconfig，打开系统配置实用程序。检查 win.ini 文件(在 C:\windows 下)，在[WINDOWS]选项下面如果有 run=和 load=参数，是加载木马程序的一种途径。一般情况下，在它们的等号后面什么都没有，如果发现后面跟着不熟悉的启动程序，那个程序就是木马程序。

(5) 检查 system.ini 文件(在 C:\windows 下)，在 BOOT 下面有一个“shell=文件名”。正确的文件名应该是 explorer.exe，如果是“shell=explorer.exe 程序名”，那么后面跟着的那个程序也是木马程序。不管出现以上哪种情况，先将程序名删除，然后再在硬盘上找到这个程序进行删除。

## 5.2.5 蠕虫病毒的概念

“蠕虫”这个生物学名词于 1982 年由 Xerox PARC 的 John F. Shoeh 等最早引入计算机领域，并给出了计算机蠕虫的两个最基本的特征：“可以从一台计算机移动到另一台计算机”和“可以自我复制”。最初，他们编写蠕虫的目的是做分布式计算的模型实验。1988 年 Morris 蠕虫爆发后，Eugene H. Spafford 为了区分蠕虫和病毒，给出了蠕虫的技术角度的定义：“计算机蠕虫可以独立运行，并能把自身的一个包含所有功能的版本传播到另外的计算机上”。计算机蠕虫和计算机病毒都具有传染性和复制功能，这两个主要特性上的一致导致二者之间是非常难区分的。近年来，越来越多的病毒采取了蠕虫技术达到其在网络上迅速感染的目的。因而，蠕虫本身只是计算机病毒利用的一种技术手段。

蠕虫病毒的传染机理是利用网络进行复制和传播，传染途径是通过网络、电子邮件以及 U 盘、移动硬盘等移动存储设备。例如，2006 年年底的“熊猫烧香”病毒就是蠕虫病毒的一

种。蠕虫程序主要利用系统漏洞进行传播。它通过网络、电子邮件和其他的传播方式,像生物蠕虫一样从一台计算机传染到另一台计算机。因为蠕虫使用多种方式进行传播,所以蠕虫程序的传播速度是非常快的。

蠕虫病毒侵入一台计算机后,首先获取其他计算机的IP地址,然后将自身副本发送给这些计算机。蠕虫病毒也使用存储在染毒计算机上的邮件客户端地址簿中的地址传播程序。虽然有的蠕虫程序也在被感染的计算机中生成文件,但一般情况下,蠕虫程序只占用内存资源而不占用其他资源。

蠕虫也是一种病毒,因此具有病毒的共同特征。一般的病毒是需要寄生的,它可以通过自己指令的执行,将自己的指令代码写到其他程序的体内,被感染的文件称为"宿主"。例如,Windows下可执行文件的格式为PE格式,需要感染PE文件时,首先在宿主程序中建立一个新段,将病毒代码写到新段中,修改程序入口点等,这样,宿主程序执行的时候就可以先执行病毒程序,病毒程序运行完之后,再把控制权交给宿主原来的程序指令。可见,病毒主要是感染文件,当然也有像DIRII这种链接型病毒,还有引导区病毒。引导区病毒是感染磁盘的引导区,如果是软盘、U盘、移动硬盘等被感染,其受感染的盘在其他机器上使用后,同样也会感染其他机器,所以传播媒介也可以是移动存储设备。

蠕虫一般不采取利用PE格式插入文件的方法,而是复制自身在互联网环境下进行传播,病毒的传染能力主要是针对计算机内的文件系统而言,而蠕虫病毒的传染目标是互联网中的所有计算机。局域网条件下的共享文件夹、电子邮件、网络中的恶意网页、大量存在着漏洞的服务器等都成为蠕虫传播的良好途径。网络的发展也使蠕虫病毒可以在几个小时内蔓延全球,而且蠕虫的主动攻击性和突然爆发性将令人们手足无措。

**1. 蠕虫病毒的组成**

蠕虫病毒由两部分组成:一个主程序和一个引导程序。主程序一旦在计算机上建立就会去收集与当前计算机联网的其他计算机的信息。它能通过读取公共配置文件并运行显示当前网上联机状态信息的系统实用程序而做到这一点。随后,它尝试利用前面所描述的那些缺陷在这些远程计算机上建立其引导程序。

蠕虫病毒程序常驻于一台或多台计算机中,并有自动重新定位的能力。如果它检测到网络中的某台计算机未被占用,它就把自身的一个备份(一个程序段)发送给那台计算机。每个程序段都能把自身的备份重新定位于另一台计算机中,并且能识别它占用的那台计算机。

**2. 蠕虫病毒的特征**

蠕虫病毒的一般特征如下。

(1) 独立个体,单独运行。

(2) 大部分利用操作系统和应用程序的漏洞主动进行攻击。

(3) 传播方式多样。

(4) 造成网络拥塞,消耗系统资源。

(5) 制作技术与传统的病毒不同,与黑客技术相结合。

蠕虫病毒的行为特征主要包括主动攻击、行踪隐蔽、利用系统和网络应用服务漏洞、造成网络拥塞、降低系统性能、产生安全隐患、反复性、破坏性等。

**3. 蠕虫病毒的分类**

根据攻击对象不同可分为两类:一类是面向企业用户和局域网的,这类蠕虫病毒利用

系统漏洞主动进行攻击，可以使整个网络瘫痪，以“红色代码”和“SQL 蠕虫王”为代表；另一类是针对个人用户的通过网络迅速传播的蠕虫病毒，以“爱虫”病毒和“求职信”病毒为代表。

**4. 传播过程**

（1）扫描。由蠕虫的扫描功能模块负责探测存在漏洞的主机。

（2）攻击。攻击模块按漏洞攻击步骤自动攻击找到的对象，取得该主机的权限（一般为管理员权限），获得一个 Shell。

（3）现场处理。进入被感染的系统后，要做现场处理工作，现场处理部分工作主要包括隐藏、信息搜集等。

（4）复制。复制模块通过原主机和新主机的交互将蠕虫程序复制到新主机并启动。

## 5.2.6 蠕虫病毒案例

**1. “熊猫烧香”病毒**

“熊猫烧香”是一个由 Delphi 工具编写的蠕虫，终止大量的反病毒软件和防火墙软件进程。病毒会删除扩展名为 GHO 的文件，使用户无法使用 Ghost 软件恢复操作系统。“熊猫烧香”感染系统的 EXE，COM，PIF，SRC，HTML，ASP 文件，添加病毒网址，导致用户一打开这些网页文件，浏览器就会自动连接到指定的病毒网址中下载病毒。在硬盘各个分区下生成文件 autorun.inf 和 setup.exe，可以通过 U 盘和移动硬盘等方式进行传播，并且利用 Windows 系统的自动播放功能运行，搜索硬盘中的 EXE 可执行文件并感染，感染后的文件图标变成“熊猫烧香”图案，如图 5.3 所示。“熊猫烧香”病毒还可以通过共享文件夹、系统弱口令等多种方式进行传播。

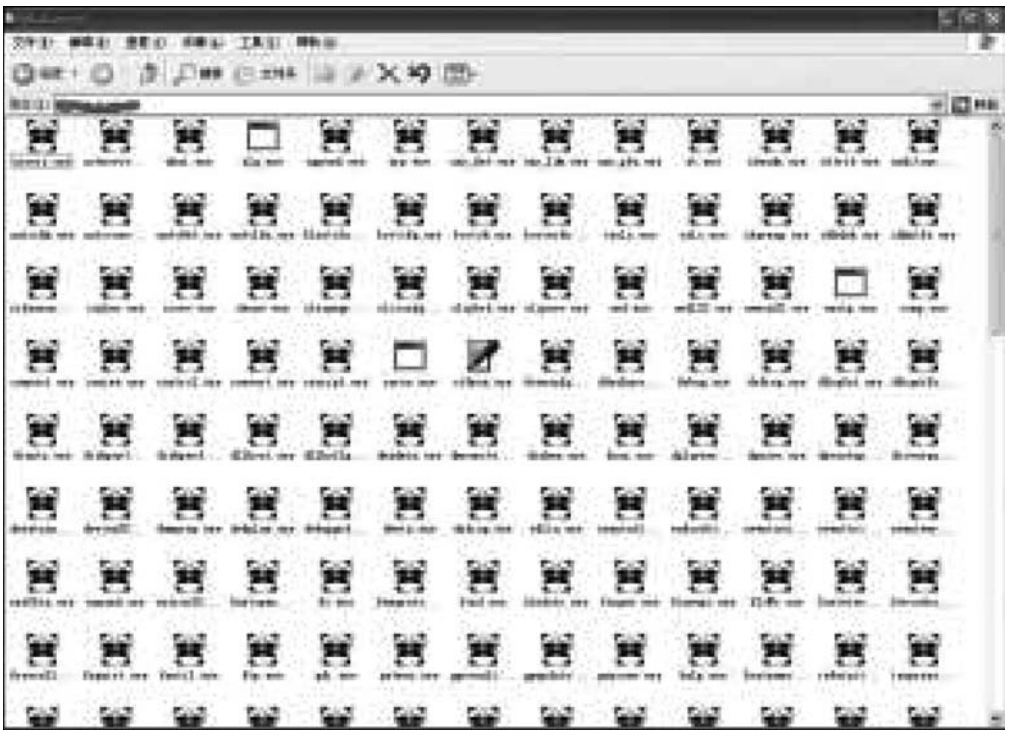

图 5.3 感染“熊猫烧香”病毒现象

据瑞星反病毒专家介绍,“熊猫烧香”其实是“尼姆亚”病毒的新变种,最早出现在2006年11月,由于它一直在不停地进行变种,而且该病毒会将中毒计算机中所有的网页文件尾部添加病毒代码,因此,一旦一些网站编辑人员的计算机被该病毒感染,网站编辑在上传网页到网站后,就会导致所有浏览该网页的计算机用户也感染上该病毒。

同时,金山毒霸反病毒中心表示,“熊猫烧香”除了通过网站带毒感染用户之外,还会通过QQ最新漏洞传播,通过网络文件共享、默认共享、系统弱口令、U盘和移动硬盘等多种途径传播。局域网中只要有一台计算机感染,就可以瞬间传遍整个网络,甚至在极短时间之内就可以感染几千台计算机,严重时可以导致网络瘫痪。中毒症状表现为计算机中所有EXE可执行文件图标都变成了“熊猫烧香”图案,继而系统蓝屏、频繁重启、硬盘数据被破坏等,严重时整个公司局域网内所有计算机全部中毒。

对此,江民公司的反病毒专家分析认为:目前存在三大原因导致病毒快速传播。一是大量的企业用户使用国外杀毒软件,而国外杀毒软件对于此类国产病毒响应速度特别慢。二是由于被种植“熊猫烧香”病毒网站的点击量的全球排名均在前300名之列,而一部分网站编辑本身计算机感染了病毒,当他们把受感染文件上传到服务器后,访问者点击此类受感染网页即中毒,因此该病毒才得以迅速传播。三是病毒具有极强的变种能力,仅从2006年11月至2006年年底短短一个多月的时间,该病毒就变种30余次,因此在许多用户疏于防范而没有更新杀毒软件时,该病毒即可借机迅速传播。

下面简单叙述一下“熊猫烧香”的案件过程。李俊于2006年10月开始制作计算机病毒“熊猫烧香”,并请雷磊对该病毒提修改建议。雷磊认为,该病毒会修改被感染文件的图标,且没有隐藏病毒进程,容易被发现,建议李俊从这两个方面对该病毒进行修改。李俊按照雷磊的建议修改了“熊猫烧香”病毒,由于其技术方面的原因而使修改后的病毒虽然能不改变别人的图标,但会使图标变花、变模糊,隐藏病毒进程问题也没有解决。2007年1月,雷磊亲自对该病毒进行修改,也未能解决上述两个问题。2006年11月中旬,李俊在互联网叫卖该病毒,同时也请王磊及其他网友帮助出售该病毒。随着病毒的出售和赠送给网友,“熊猫烧香”病毒迅速在互联网上传播,由此导致自动链接李俊个人网站www.krvkr.com的流量大幅上升。王磊得知此情形后,主动提出为李俊卖“流量”,并联系被告人张顺购买李俊网站的“流量”,所得收入由王磊和李俊平分。为了提高访问李俊网站的速度,减少网络拥堵,王磊和李俊商量后,由王磊化名董磊为李俊的网站在南昌锋讯网络科技有限公司租用了一个2GB内存、百兆独享线路的服务器,租金由李俊、王磊每月各负担800元。张顺购买李俊网站的流量后,先后将9个游戏木马挂在李俊的网站上,盗取自动链接李俊网站游戏玩家的“游戏信封”,并将盗取的“游戏信封”进行拆封、转卖,从而获取利益。从2006年12月至2007年2月,李俊获利145 149元,王磊获利80 000元,张顺获利12 000元。“熊猫烧香”病毒的传播造成北京、上海、天津、山西、河北、辽宁、广东、湖北等省市众多单位和个人的计算机受到病毒感染,不能正常运行,同时也使众多游戏玩家的游戏装备、游戏币被盗。2007年2月2日,李俊将其网站关闭,之后再未开启该网站。被告人李俊归案后,向公安机关提供线索抓获了其他同案人。案发后,被告人李俊、王磊、张顺退回了所得全部赃款。被告人李俊交出“熊猫烧香”病毒专杀工具。

法院认为:4被告均构成破坏计算机信息系统罪。根据《刑法》第286条规定:违法国家规定,对计算机信息系统功能进行删除、修改、增加、干扰,造成计算机信息系统不能正常

运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑；故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的依照第一款的规定处罚。

- 被告人李俊犯破坏计算机信息系统罪，判处有期徒刑四年；
- 被告人王磊犯破坏计算机信息系统罪，判处有期徒刑两年六个月；
- 被告人张顺犯破坏计算机信息系统罪，判处有期徒刑两年；
- 被告人雷磊犯破坏计算机信息系统罪，判处有期徒刑一年。

被告人李俊的违法所得人民币 145 149 元，被告人王磊的违法所得人民币 80 000 元，被告人张顺的违法所得人民币 12 000 元，予以没收，上缴国库。

预防“熊猫烧香”这类病毒的措施如下。

(1) 立即检查本机 administrators 组成员口令，一定要放弃简单口令甚至空口令，安全的口令是字母、数字、特殊字符的组合，自己记得住，别让病毒猜到就行。

修改方法：右击“我的电脑”图标，从弹出的快捷菜单中选择“管理”，在打开的“计算机管理”窗口中选择“本地用户和组”节点，在右侧的窗格中选择具备管理员权限的用户名右击，从弹出的快捷菜单中选择“设置密码”，输入新密码即可，如图 5.4 所示。


图 5.4　设置用户密码

(2) 利用组策略，关闭所有驱动器的自动播放功能。

修改方法：执行“开始”→“运行”命令，在打开的对话框中输入 gpedit. msc，打开“组策略”窗口，展开“计算机配置”→“管理模板”→“系统”节点，在右侧的窗格中双击“关闭自动播放”，该配置默认是未配置。在弹出对话框中的下拉列表框中选择“所有驱动器”，再选中“已启用”单选按钮，单击“确定”按钮后关闭。最后，执行“开始”→“运行”命令，在打开的对话框中输入 gpupdate，单击“确定”按钮后该策略就生效了。

(3) 修改文件夹选项，以查看不明文件的真实属性，避免无意双击骗子程序中毒。

修改方法：打开资源管理器(按 Windows 徽标键＋E 组合键)，执行“工具”→“文件夹选项”菜单命令，再选择“查看”选项卡，在“高级设置”列表框中选择查看所有文件，取消对

“隐藏受保护的操作系统文件”和“隐藏已知文件类型的扩展名”复选框的勾选。

(4) 时刻保持操作系统获得最新的安全更新,不要随意访问来源不明的网站,特别是微软公司的 MS06-014 漏洞,应立即打好该漏洞补丁。同时,QQ、MSN 的漏洞也可以被该病毒利用,因此,用户应该去官方网站打好最新补丁。此外,由于该病毒会利用 IE 浏览器的漏洞进行攻击,因此用户还应该给 IE 打好所有的补丁。如果必要的话,用户可以暂时改用 Firefox,Opera 等比较安全的浏览器。

(5) 启用 Windows 防火墙保护本地计算机。局域网用户尽量避免创建可写的共享目录,已经创建共享目录的应立即停止共享。

此外,对于未感染的用户,病毒专家建议不要登录不良网站,及时下载微软公司公布的最新补丁避免病毒利用漏洞袭击用户的计算机,同时上网时应采用“杀毒软件+防火墙”的立体防御体系。

**2. “U 盘寄生虫”病毒**

金山反病毒中心将该病毒统称为“AV 终结者”,瑞星反病毒中心将该病毒称为“帕虫”,江民反病毒中心将该病毒称为“U 盘寄生虫”。

“U 盘寄生虫”是一款利用 U 盘等移动存储设备传播的蠕虫病毒,通过网络大规模自动传播,传播方式包括电子邮件、网络共享、系统漏洞、即时通信软件等。“U 盘寄生虫”会利用 U 盘、MP3、移动硬盘等设备中的自动播放文件发作,大量占用系统资源,使计算机运行缓慢、无法上网,甚至导致系统瘫痪。此外,受到攻击的局域网还可能出现网络堵塞、瘫痪等严重症状。

“U 盘寄生虫”是蠕虫家族的重要成员之一,采用 Delphi 语言编写,并经过加壳处理。“U 盘寄生虫”运行后自我复制到系统盘根目录下,文件名为 test.exe,将文件属性设置为“隐藏”,并在相同目录下创建 autorun.inf 文件,达到双击盘符就可启动“U 盘寄生虫”病毒的目的。普通用户一旦感染该病毒,从病毒进入计算机到实施破坏,4 步就可导致用户计算机彻底崩溃。第 1 步,禁用所有杀毒软件及相关安全工具,让计算机失去安全保障;第 2 步,破坏安全模式,致使用户根本无法进入安全模式清除病毒;第 3 步,强行关闭带有病毒字样的网页,只要在网页中输入“病毒”相关字样,网页遂被强行关闭,即使是一些安全论坛也无法登录,用户无法通过网络寻求解决办法;第 4 步,格式化系统盘重装后很容易被再次感染。

用户格式化后,只要双击其他盘符,病毒将再次运行。此外,用户计算机的安全防御体系被彻底摧毁,安全性几乎为零,而“AV 终结者”自动连接到拥有病毒的网站,并下载数百种木马病毒,各类盗号木马、广告木马、风险程序在用户计算机毫无抵抗力的情况下鱼贯而入,用户的网银、网游、QQ 账号密码及机密文件都处于极度危险之中。因此,提醒计算机用户目前使用计算机需慎之又慎。

据瑞星反病毒中心表示:“该病毒采用了多种技术手段保护自身不被清除,例如它会终结几十种常用的杀毒软件,如果用户使用 Google、百度等搜索引擎搜索‘病毒’,浏览器也会被病毒强制关闭,使用户无法取得相关信息。尤为恶劣的是,该病毒还采用了 IFEO(Image File Execution Options)劫持(Windows 文件映像劫持)技术,修改注册表,使 QQ 医生、360 安全卫士等几十种常用软件无法正常运行,从而使用户很难手动清除该病毒。”

此外,据反病毒专家介绍:“该病毒通过映像劫持技术将大量杀毒软件‘绑架’,使其无

法正常应用，而用户在双击相关安全软件后，实际上已经运行了病毒文件，实现病毒的‘先劫持后调包’计划。该病毒不但可以劫持大量杀毒软件和安全工具，还可以禁止 Windows 的自动更新和系统自带的防火墙，大大降低了用户系统的安全性，这也是近几年来对用户的系统安全破坏程度最大的一个病毒之一。而且该病毒还会在每个磁盘分区上建立自动运行文件（包括 U 盘），从而使其通过 U 盘传播的概率大大增加。同时，由于每个分区上都有病毒留下的文件，普通用户即使格式化 C 盘重装系统，也无法彻底清除该病毒。”

病毒专家建议，计算机用户应及时升级杀毒软件，开启杀毒软件“实时监控”和“系统监测”功能，防范已知和未知病毒。针对越来越多的病毒通过 U 盘传播的特征，专家建议用户在使用 U 盘前务必先使用杀毒软件进行扫描，确认无毒后再打开。此外，用户应养成良好的安全习惯，不随意点击不明链接和运行不明文件，及时为操作系统打好补丁，关闭系统共享以及为系统设置复杂的口令都可有效减少病毒侵害。

**3. Mydoom 邮件病毒**

Novarg/Mydoom.a 蠕虫是 2004 年 1 月 28 日开始传入我国的一个通过邮件传播的蠕虫，在全球造成的直接经济损失至少达 400 亿美元，是 2004 年 1 月十大病毒之首。该蠕虫利用欺骗性的邮件主题和内容诱使用户打开邮件中的附件。拒绝服务的方式是向网站的 Web 服务发送大量 GET 请求，在传播和攻击过程中会占用大量系统资源，导致系统运行变慢。蠕虫还会在系统留下后门，通过该后门，入侵者可以完全控制被感染的主机。

该蠕虫没有使用特别的技术和系统漏洞，之所以能造成如此大的危害，主要还是由于人们防范意识的薄弱和蠕虫本身传播速度较快的原因。该蠕虫主要通过电子邮件进行传播，它的邮件主题、正文和所带附件的文件名都是随机的，另外它还会利用 Kazaa 的共享网络进行传播。病毒文件的图标和 Windows 系统的记事本（Notepad.exe）图标非常相似，运行后会打开记事本程序，显示一些乱码信息，其实病毒已经开始运行了。病毒会创建名为 SwebSipcSmtxSO 的排斥体判断系统是否已经被感染。

蠕虫在系统中寻找所有可能包含邮件地址的文件，包括地址簿文件、各种网页文件等，从中提取邮件地址作为发送的目标。病毒会避免包含以下信息的域名：gov，mil，borlan，bsd，example 等；避免包含以下信息的电子邮件账户：accoun，ca，certific，icrosoft，info，linux 等。当病毒检测到邮件地址中含有上述域名或账户时则忽略该地址，不将其加入发送地址链表中。

Mydoom 蠕虫病毒除了造成网络资源的浪费，阻塞网络，被攻击网站不能提供正常服务外，最大的危险在于安装了后门程序。该后门即 shimgapi.dll，通过修改注册表，使自身随着浏览器的启动而运行，将自己加载到资源管理器的进程空间中。后门监听 3127 端口，如果该端口被占用，则递增端口号，但不大于 3198。后门提供了以下两个功能。

（1）作为端口转发代理。

（2）作为后门接收上传程序并执行。

当 3127 端口收到连接之后，如果接收的第 1 个字符是 x04，转入端口转发流程。若第 2 个字符是 0x01，则取第 3 和第 4 个字符作为目标端口，取第 5～8 这 4 个字节作为目标 IP 地址，进行连接并和当前 Socket 数据转发。如果接收的第 1 个字符是 x85，则转入执行命令流程。先接收 4B，转成主机字节序后验证是否是 x133c9ea2，验证通过则创建临时文件接收数据，接收完毕运行该文件。也就是说，只要把任意一个可执行文件的头部加上 5 个字符

x85133c9ea2作为数据发送到感染了Mydoom.a蠕虫计算机的3127端口,这个文件就会在系统上被执行,从而对被感染系统的安全造成极大的威胁。

**4. Nimda蠕虫病毒**

在Nimda蠕虫病毒出现以前,蠕虫技术一直是独立发展的。Nimda病毒首次将蠕虫技术和计算机病毒技术结合起来。从Nimda的攻击方式来看,Nimda蠕虫病毒只攻击微软公司的Windows系列操作系统。Nimda蠕虫病毒在技术实现上与许多蠕虫病毒都有一些共性的特点,主要有以下几方面。

(1) 被利用的系统漏洞。它通过电子邮件、网络临近共享文件、微软公司IE异常处理MIME头漏洞、Microsoft IIS UniCode解码目录遍历漏洞、Microsoft IIS CGI文件名错误解码漏洞、Code Red II和Sadmind/IIS蠕虫留下的后门程序共6种方式进行传播,其中前3种方式是病毒传播方式。

(2) 传播方式。邮件传播、IIS Web服务器传播、文件共享传播、通过网页进行传播、通过修改EXE文件进行传播、通过Word文档进行传播、感染病毒文件并修改System.ini配置、后门安装技术。

**5. 冲击波病毒**

冲击波病毒的行为特征如下。

(1) 病毒运行时会将自身复制为%systemdir%\msblast.exe。%systemdir%是一个变量,它指的是操作系统安装目录中的系统目录,默认为c:\windows\system或c:\Winnt\system32。

(2) 病毒运行时会在系统中建立一个名为BILLY的互斥量,目的是病毒保证在内存中只有一份病毒体,避免用户发现。

(3) 病毒运行时会在内存中建立一个名为msblast.exe的进程,该进程就是活的病毒体。

(4) 病毒会修改注册表,在HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run中添加键值"windows auto update"="msblast.exe",以便每次启动系统时病毒都会运行。

(5) 病毒体内隐藏有一段文本信息:I just want to say LOVE YOU SAN!! Billy gates why do you make this possible? Stop making money and you're your software!!。

(6) 病毒会每20s检测一次网络状态,当网络可用时,病毒会在本地的UDP/69端口上建立一个简单文件传输协议(Trivial File Transfer Protocol,TFTP)服务器,并启动一个攻击传播线程,不断地随机生成攻击地址进行攻击。另外,该病毒攻击时会首先搜索子网的IP地址,以便就近攻击。

(7) 当病毒扫描到计算机后,就会向目标计算机的TCP/135端口发送数据。

(8) 当病毒攻击成功后,目标计算机便会将监听的TCP/4444端口作为后门,并绑定cmd.exe。然后蠕虫会连接到这个端口,发送TFTP下载信息,目标主机通过TFTP下载病毒并运行病毒。

(9) 当病毒攻击失败时,可能会造成没有打补丁的Windows系统的远程文件复制(Remote File Copy,RFC)服务崩溃,Window XP系统可能会自动重启计算机。

(10) 病毒检测到当前系统月份是8月之后或为当月日期的15日之后,就会向微软公

司的更新站点 windowsupdate.com 发动拒绝服务攻击，使微软公司网站的更新站点无法为用户提供服务。

从上述冲击波病毒的行为特征可以看出，冲击波病毒与其他两个病毒的不同点在于其传播方式。冲击波病毒利用了 Windows 系统的 DCOM RPC 缓冲区漏洞攻击系统，一旦攻击成功，病毒体将会被传送到对方计算机中进行感染，不需要用户的参与，而其他两种病毒是通过邮件附件的方式引诱用户点击执行。破坏性方面，因病毒而异；病毒的执行、自启动方面，3 种病毒都相似。

RPC 是运用于 Windows 操作系统上的一种协议。RPC 提供相互处理通信机制，允许运行该程序的计算机在一个远程系统上执行代码。RPC 协议本身源于 OSF（Open Software Foundation）RPC 协议，后来又另外增加了一些微软专用扩展功能。RPC 中处理 TCP/IP 信息交换的模块由于错误地处理畸形信息，导致存在缓冲区溢出漏洞，远程攻击者可利用此缺陷以本地系统权限在系统上执行任意指令，如安装程序、查看或更改、删除数据或建立系统管理员权限的账户。

据 CERT 安全小组称，操作系统中超过 50％的安全漏洞都是由内存溢出引起的，其中大多数与微软公司技术有关，这些与内存溢出相关的安全漏洞正在被越来越多的蠕虫病毒所利用。缓冲区溢出是指当计算机程序向缓冲区内填充的数据位数超过缓冲区本身的容量时，溢出的数据就会覆盖在合法数据上，这些数据可能是数值、下一条指令的指针，或者是其他程序的输出内容。一般情况下，覆盖其他数据区的数据是没有意义的，最多造成应用程序错误。但是，如果输入的数据是经过“黑客”或病毒精心设计的，覆盖缓冲区的数据恰恰是“黑客”或病毒的入侵程序代码，一旦多余字节被编译执行，“黑客”或病毒就有可能为所欲为，获取系统的控制权。

溢出根源在于编程：缓冲区溢出是由编程错误引起的。如果缓冲区被写满，而程序没有检查缓冲区边界，也没有停止接收数据，这时缓冲区溢出就会发生。因此，防止利用缓冲区溢出发起的攻击，关键在于程序开发者在开发程序时仔细检查溢出情况，不允许数据溢出缓冲区。此外，用户需要经常登录操作系统和应用程序提供商的网站，跟踪公布的系统漏洞，及时下载补丁程序，弥补系统漏洞。

### 5.2.7 蠕虫病毒的防治

蠕虫病毒的一般防治方法是使用具有实时监控功能的杀毒软件，防范邮件蠕虫的最好办法就是提高自己的安全意识，不要轻易打开带有附件的电子邮件。另外，可以启用杀毒软件的“邮件发送监控”和“邮件接收监控”功能，也可以提高对病毒邮件的防护能力。

**1. 一般防治措施**

因为目前的蠕虫病毒越来越表现出 3 种传播趋势：邮件附件、无口令或弱口令共享、利用操作系统或应用系统漏洞传播病毒，所以防治蠕虫也应从这 3 方面入手。

（1）针对通过邮件附件传播的病毒。

在邮件服务器上安装杀毒软件，对附件进行杀毒。在客户端（主要是 Outlook）限制访问附件中的特定扩展名的文件，如 PIF，VBS，JS，EXE 等；用户不打开可疑邮件携带的附件。

（2）针对弱口令共享传播的病毒。

严格来说，通过共享和弱口令传播的蠕虫大多也利用了系统漏洞。这类病毒会搜索网

络上的开放共享并复制病毒文件,更进一步的蠕虫还自带口令猜测的字典破解薄弱用户口令,尤其是薄弱管理员口令。对于此类病毒,在安全策略上需要增加口令的强度策略,保证必要的长度和复杂度;通过网络上的其他主机定期扫描开放共享和对登录口令进行破解尝试,发现问题及时整改。

(3) 针对通过系统漏洞传播的病毒。

配置 Windows Update 自动升级功能,使主机能够及时安装系统补丁,防患于未然;定期通过漏洞扫描产品查找主机存在的漏洞,发现漏洞,及时升级;关注系统提供商、安全厂商的安全警告,如有问题则采取相应措施。

(4) 重命名或删除命令解释器。

例如,Windows 系统下的 WScript.exe,通过防火墙禁止除服务端口外的其他端口,切断蠕虫的传播通道和通信通道。

**2. 个人用户对蠕虫病毒的防范措施**

通过上述分析和介绍可以知道,病毒并不可怕,网络蠕虫病毒对个人用户的攻击主要还是通过社会工程学,而不是利用系统漏洞,所以防范此类病毒需要注意以下几点。

(1) 选用合适的杀毒软件。网络蠕虫病毒的发展已经使传统的杀毒软件的"文件级实时监控系统"落伍,杀毒软件必须向内存实时监控和邮件实时监控发展。另外,面对防不胜防的网页病毒,也使用户对杀毒软件的要求越来越高。

(2) 经常升级病毒库。杀毒软件对病毒的查杀是以病毒的特征码为依据的,而病毒每天都层出不穷,尤其是在网络时代,蠕虫病毒的传播速度快、变种多,所以必须随时更新病毒库,以便能够查杀最新的病毒。

(3) 提高防范杀毒意识。不要轻易访问陌生的站点,有可能里面就含有恶意代码。当运行 IE 时,执行"工具"→"Internet 选项"命令,在打开的"Internet 属性"对话框中选择"安全"选项卡,在"该区域的安全级别"区域将安全级别由"中"改为"高"。因为这类网页主要是含有恶意代码的 ActiveX,Applet 或 JavaScript 的网页文件,所以在 IE 设置中将 ActiveX 插件和控件、Java 脚本等全部禁止,就可以大大降低被网页恶意代码感染的概率。具体操作是在 IE 窗口中执行"工具"→"Internet 选项"命令,在弹出的"Internet 属性"对话框中选择"安全"选项卡,单击"自定义级别"按钮,如图 5.5 所示。在弹出的"安全设置"对话框中,将所有 ActiveX 控件和插件和与 Java 相关的全部选项"禁用"。但是,这样做在以后的网页浏览过程中有可能会使一些正常应用 ActiveX 的网站无法浏览。


图 5.5 定义安全级别

(4) 不随意查看陌生邮件,尤其是带有附件的邮件。由于有的病毒邮件能够利用 IE 和 Outlook 的漏洞自动执行,因此计算机用户需要升级 IE 和 Outlook 程序,以及其他常用的应用程序。

(5) 打好相应的系统补丁。可以应用瑞星杀毒软件的“漏洞扫描”功能或 360 安全卫士等工具,这些工具可以引导用户打好补丁并进行相应的安全设置,杜绝病毒的感染。

(6) 警惕聊天软件发来的信息。从 2004 年起,MSN、QQ 等聊天软件开始成为蠕虫病毒传播的途径之一。“性感烤鸡”病毒就通过 MSN 传播,在很短时间内席卷全球,一度造成中国大陆地区部分网络运行异常。对于普通用户,防范聊天蠕虫的主要措施之一就是提高安全防范意识,对于通过聊天软件发送的任何文件和信息,都要经过好友确认后再运行,不要随意单击聊天软件发送的网络链接。

**3. 蠕虫技术发展的趋势**

(1) 与病毒技术的结合。很早的病毒编写者就提出过这样的思路,现在已经变成了现实。越来越多的蠕虫开始结合病毒技术,在攻击计算机系统之后继续攻击文件系统,从而导致传播机制的多样化。

(2) 动态功能升级技术。提出动态调整蠕虫程序的思路顺理成章,这样的蠕虫可以升级上文提到的功能模型中除控制模块外的所有功能模块,从而获得更强的生存能力和攻击能力。

(3) 通信技术。蠕虫之间、编写者与蠕虫之间传递信息和指令的功能将成为未来蠕虫编写的重点趋势。

(4) 隐身技术。操作系统内核一级的黑客攻防技术将进一步纳入蠕虫的功能中以隐藏蠕虫的踪迹。

(5) 巨型蠕虫。蠕虫程序包含多操作系统的运行程序版本,包含丰富的漏洞库,从而具有更强大的传染能力。

(6) 分布式蠕虫。数据部分同运行代码分布在不同的计算机之间,运行代码在攻击时从数据存放地获取攻击信息。同时,攻击代码用一定的算法在多台计算机上寻找、复制数据的存放地。不同功能模块分布在不同的计算机之间,协调工作,产生更强的隐蔽性和攻击能力。

## 5.2.8 病毒、木马、蠕虫的比较

通过网络传播的病毒不是网络病毒,只有蠕虫等一些威胁可以算作网络病毒。蠕虫病毒也不是普通病毒所能比拟的,网络的发展使蠕虫可以在短短的时间内蔓延整个网络,造成网络瘫痪。表 5.1 列出了病毒、木马、蠕虫各自的特点和区别,便于理解。

**表 5.1 病毒、木马、蠕虫的比较**

| 比较项目 | 病　毒 | 木　马 | 蠕　虫 |
|---|---|---|---|
| 感染其他文件 | 会 | 不会 | 不会 |
| 被动散播自己 | 是 | 是 | 不是 |
| 主动散播自己 | 不是 | 不是 | 是 |
| 造成程序增加数目 | 计算机使用率越高,文件受感染的数目越多 | 不会增加 | 取决于网络连接情况,范围越广,散布的数目越多 |
| 破坏力 | 取决于病毒作者 | 取决于病毒作者 | 无 |
| 对企业的影响 | 中 | 低 | 高 |

网络用户所受网络攻击类型统计如图 5.6 所示,病毒、蠕虫和木马造成的安全事件占发生安全事件总数的 79%;拒绝服务、端口扫描和篡改网页等网络攻击事件占 43%;大规模

垃圾邮件传播造成的安全事件占36%；54%的被调查单位网络安全事件造成的损失比较轻微；损失严重和非常严重的占发生安全事件总数的10%。

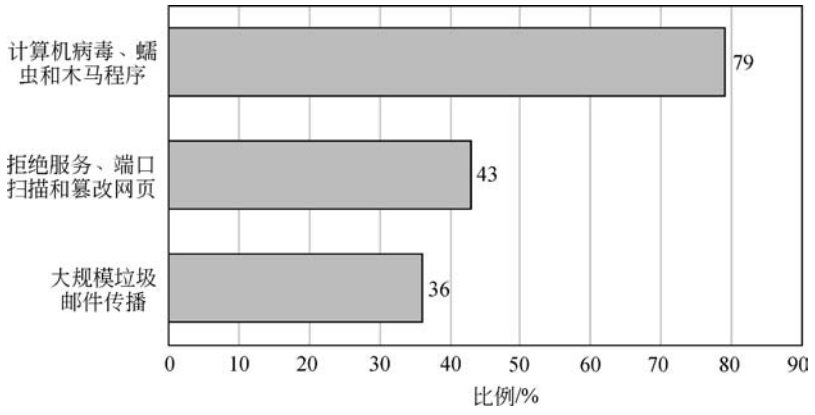


图5.6　网络用户所受网络攻击类型统计

### 5.2.9　网络病毒的发展趋势

随着网络的发展，网络病毒呈现出一些新的发展趋势，主要有以下几点。

(1) 传播介质与攻击对象多元化，传播速度更快，覆盖面更广。网络病毒的传播不仅可利用磁介质，更多的是通过各种通信端口、网络和邮件等迅速传播。攻击对象由单一的个人计算机变为所有具备通信功能的工作站、服务器甚至移动通信工具。

(2) 破坏性更强。网络病毒的破坏性日益增强，它们可以造成网络拥塞进而瘫痪，重要数据丢失，机密信息失窃，甚至通过病毒完全控制计算机信息系统和网络。

(3) 难以控制和根治。在网络中，只要有一台计算机感染病毒，就可通过内部机制进行传播，很快使整个网络受到影响甚至拥塞或瘫痪。

(4) 病毒携带形式多样化。在网络环境下，可执行程序、脚本文件、HTML网页、电子邮件、网上贺卡甚至卡通图片等都有可能携带计算机病毒。

(5) 编写方式多样化，病毒变种多。网络环境下除了传统的汇编语言、C语言等，以JavaScript和VBScript为首的脚本语言已成为最流行的病毒语言。利用新的编程语言与编程技术实现的病毒更易于修改以产生新的变种，从而逃避反病毒软件的检查。另外，已经出现了专门生产病毒的病毒生产机程序，使新病毒出现的频率大大提高。

(6) 触发条件增多，感染与发作的概率增大。

(7) 智能化，隐蔽化。目前网络病毒常常用到隐形技术、反跟踪技术、加密技术、自变异技术、自我保护技术、针对某种反病毒技术的反措施技术和突破计算机网络防护措施的技术等，这使网络环境下的病毒更加智能化、隐蔽化。

(8) 攻击目的明确化。一些高级病毒出于某种经济或政治上的目的，被研制出来扰乱或破坏社会信息、政治、经济秩序，甚至是作为一种信息战略武器。

### 5.2.10　计算机防毒杀毒的常见误区

**1. 有了杀毒软件就可以什么毒都不怕**

真的有了杀毒软件就什么毒都不怕吗？答案肯定是不。不断有新的病毒出现，而且它

的出现往往无法预料，杀毒软件也要不断更新，要不断升级才能应对新出现的病毒。即使这样，有很多时候杀毒软件升级到最新也不能杀掉全部的病毒，升级到最新只是能让计算机拒绝更多的病毒，让计算机处于更安全的状态，并不意味着就可以忽略计算机安全，平时还是要注意共享安全。不要下载不明程序，不要打开不明网页。

**2. 安装杀毒软件越多越好**

真的安装杀毒软件越多越好吗？其实不同厂商开发的杀毒软件很容易引起冲突。不少杀毒软件厂商为了避免这种情况的发生，在安装的时候就检测计算机中是否安装有其他杀毒软件，目的就是避免两个杀毒软件同时使用的时候发生冲突。而且，对于大部分的病毒，一般一个杀毒软件就可以杀掉，对付特殊病毒也有不少专杀工具。安装的杀毒软件越多，除了可能发生冲突以外，还会消耗更多的系统资源，减慢计算机运行速度。多装几个杀毒软件，得益没多少，效能却损失很大。所以，并不是杀毒软件越多越好。

**3. 杀毒软件能杀毒就行了**

杀毒软件能杀毒就行？是不是等到病毒入侵然后才来杀毒？有些人关闭了杀毒软件，想减小系统资源的消耗，当病毒入侵的时候才用杀毒软件杀毒。这种意识是不对的，现在病毒肆虐，无孔不入，一不小心就会“中毒”，况且现在硬盘之大，令很多杀毒软件杀毒时间都很长。而且假如病毒入侵的时候才杀毒，那么可能系统早已崩溃，数据早已丢失，为时已晚，到时候损失就大了。因此，杀毒不是重点，防毒才是最重要的。与其说是杀毒软件，不如说是防毒软件更好。

**4. 只要我不上网就不会有病毒**

有些人的计算机连接到 Internet，以为只要不上网就不会感染病毒，所以不运行杀毒软件防毒。其实，虽然不少病毒是通过网页传播的，但是也有不少病毒不等打开网页就早已入侵到计算机中，这个是必须防范的。冲击波、蠕虫病毒等都会在不知不觉中进入计算机。而且，U 盘、移动硬盘也会存在病毒。因此，只要计算机开着，最好就防着。

**5. 文件设置为只读就可以避免病毒**

设置只读只是调用系统几个命令而已，而病毒也可以调用系统命令。因此，病毒可以修改文件属性，严重的可以删掉重要文件，格式化硬盘，让系统崩溃。设置只读并不能有效防毒，不过对于局域网中为了共享安全，防止误删除，设置只读属性还是比较有用的。

**6. 病毒不感染数据文件**

有人觉得病毒是一段程序，而数据文件，如 TXT、PCX 等文件一般不会包含程序，因此不会感染病毒。殊不知像 Word、Excel 等数据文件由于包含了可执行代码却会被病毒感染，而且有些病毒可以让硬盘中的文件全部格式化，因此不能忽视数据文件的备份。

上面只介绍了常见的防毒杀毒误区，还有一些其他误区，在我们使用计算机的时候都有可能慢慢碰到。在使用计算机的时候，最重要的还是防毒，而要做好防毒，那就需要不断更新杀毒软件，同时注意对系统进行升级。

视频讲解

## 5.3 流氓软件

“流氓软件”是介于病毒和正规软件之间的软件。通俗地讲，是指在使用计算机上网时，不断弹出的窗口让鼠标无所适从；有时计算机浏览器被莫名修改增加了许多工作条，当用

户打开网页时却变成不相干的奇怪画面,甚至是黄色广告。有些流氓软件只是为了达到某种目的,如广告宣传,这些流氓软件虽然不会影响用户计算机的正常使用,但在启动浏览器的时候会多弹出一个网页,从而达到宣传的目的。

"流氓软件"起源于 Badware 一词,对 Badware 的定义为:是一种跟踪你上网行为并将你的个人信息反馈给"躲在阴暗处的"市场利益集团的软件,并且可以通过该软件向你弹出广告。Badware 又可分为间谍软件(Spyware)、恶意软件(Malware)和欺骗性广告软件(Deceptive Adware)。

国内互联网业界人士一般将这类软件称为流氓软件,并分为间谍软件、行为记录软件、浏览器劫持软件、搜索引擎劫持软件、广告软件、自动拨号软件、盗窃密码软件等。

### 5.3.1 流氓软件的定义

流氓软件的定义为"在未明确提示用户或未经用户许可的情况下,在用户计算机或其他终端上强行安装运行,侵犯用户合法权益的软件,但已被我国法律法规规定的计算机病毒除外"。它具有以下特点。

**1. 强制安装**

在未明确提示用户或未经用户许可的情况下,在用户计算机或其他终端上强行安装软件。强制安装时不能结束它的进程,不能选择它的安装路径,带有大量色情广告甚至计算机病毒。

**2. 难以卸载**

未提供通用的卸载方式,或在不受其他软件影响、人为破坏的情况下,卸载后仍活动或残存程序。

**3. 浏览器劫持**

未经用户许可,修改用户浏览器或其他相关设置,迫使用户访问特定网站或导致用户无法正常上网。

**4. 广告弹出**

未明确提示用户或未经用户许可的情况下,利用安装在用户计算机或其他终端上的软件弹出色情广告等页面。

**5. 恶意收集用户信息**

未明确提示用户或未经用户许可,恶意收集用户信息。

**6. 恶意卸载**

未明确提示用户、未经用户许可,或误导、欺骗用户卸载非恶意软件。

**7. 恶意捆绑**

在软件中捆绑已被认定为恶意软件。

**8. 恶意安装**

未经许可的情况下,强制在用户计算机中安装其他非附带的独立软件。

**9. 其他**

强制安装到系统盘的软件或侵犯用户知情权、选择权的恶意行为的软件也称为流氓软件。

### 5.3.2 流氓软件的分类

根据不同的特征和危害，困扰广大计算机用户的流氓软件主要有以下几类。

**1. 广告软件**

定义：广告软件(Adware)是指未经用户允许，下载并安装在用户计算机上；或与其他软件捆绑，通过弹出式广告等形式牟取商业利益的程序。

危害：此类软件往往会强制安装并无法卸载；在后台收集用户信息牟利，危及用户隐私；频繁弹出广告，消耗系统资源，使其运行变慢等。

例如，用户安装了某下载软件后，会一直弹出带有广告内容的窗口，干扰正常使用。还有一些软件安装后，会在 IE 浏览器的工具栏位置添加与其功能不相干的广告图标，普通用户很难清除。

**2. 间谍软件**

定义：间谍软件(Spyware)是一种能够在用户不知情的情况下，在其计算机上安装后门、收集用户信息的软件。

危害：用户的隐私数据和重要信息会被“后门程序”捕获，并被发送给黑客、商业公司等。这些“后门程序”甚至能使用户的计算机被远程操纵，组成庞大的“僵尸网络”，这是网络安全的重要隐患之一。

例如，某些软件会获取用户的软硬件配置，并发送出去用于商业目的。

**3. 浏览器劫持**

定义：浏览器劫持是一种恶意程序，通过浏览器插件、浏览器辅助对象(Browser Helper Object，BHO)、Winsock LSP 等形式对用户的浏览器进行篡改，使用户的浏览器配置不正常，被强行引导到商业网站。

危害：用户在浏览网站时会被强行安装此类插件，普通用户根本无法将其卸载，被劫持后，用户只要上网就会被强行引导到其指定的网站，严重影响正常上网浏览。

例如，一些不良站点会频繁弹出安装窗口，迫使用户安装某浏览器插件，甚至根本不征求用户意见，利用系统漏洞在后台强制安装到用户计算机中。这种插件还采用了不规范的软件编写技术(此技术通常被病毒使用)逃避用户卸载，往往会造成浏览器错误、系统异常重启等。

**4. 行为记录软件**

定义：行为记录软件(Track Ware)是指未经用户许可，窃取并分析用户隐私数据，记录用户计算机使用习惯、网络浏览习惯等个人行为的软件。

危害：危及用户隐私，可能被黑客利用进行网络诈骗。

例如，一些软件会在后台记录用户访问过的网站并加以分析，有的甚至会发送给专门的商业公司或机构，此类机构会据此窥测用户的爱好，并进行相应的广告推广或商业活动。

**5. 恶意共享软件**

定义：恶意共享软件(Malicious Shareware)是指某些共享软件为了获取利益，采用诱骗手段、试用陷阱等方式强迫用户注册，或在软件体内捆绑各类恶意插件，未经允许即将其安装到用户计算机中。

危害：使用“试用陷阱”强迫用户进行注册，否则可能会丢失个人资料等数据。软件集

成的插件可能会造成用户浏览器被劫持、隐私被窃取等。

例如,用户安装某款媒体播放软件后,会被强迫安装与播放功能毫不相干的软件(搜索插件、下载软件)而不给出明确提示,并且用户卸载播放器软件时不会自动卸载这些附加安装的软件。又如某加密软件,试用期过后所有被加密的资料都会丢失,只有交费购买该软件才能找回丢失的数据。

**6. 其他**

随着网络的发展,"流氓软件"的分类也越来越细,一些新种类的流氓软件在不断出现,分类标准必然会随之调整。

### 5.3.3 流氓软件的防治

流氓软件实在是令人憎恶,但是流氓软件都能很好地隐藏自己,因此相对而言,杀毒软件及时杀除流氓软件的可能性就大大降低了,这就要求用户要有一定的流氓软件的防护能力,才能使上网更加安全。

**1. 要有安全的上网意识**

不要轻易登录不了解的网站,因为这样很可能遇到网页脚本病毒的袭击,从而使系统感染上流氓软件。不要随便下载不熟悉的软件。安装软件时应仔细阅读软件附带的用户协议及使用说明,有些软件在安装的过程中会以不引起用户注意的方式提示用户安装流氓软件,这时如果用户不认真看提示信息就会安装上流氓软件。在安装操作系统后,应该先上网给系统打补丁,堵住一些已知漏洞,这样能够避免利用已知漏洞的流氓软件驻留。如果用户使用 IE 浏览器上网,则应该将浏览器的安全级别调到中高级别,或者将 Active X 控件、脚本程序都禁止执行,这样能够防止一些隐藏在网页中的流氓软件入侵。

**2. 判断流氓软件**

判断自己是否已经安装了流氓软件,要根据流氓软件的中招症状来看。一般地,浏览器首页被无故修改、总是弹出广告窗口、CPU 的资源被大量占用、系统变得很慢、浏览器经常崩溃或出现找不到某个库文件的提示框,这些都是安装了流氓软件最常见的现象,就要采取相应的措施。

流氓软件无论多么复杂,它们的传播流程几乎是一样的,都是会通过软件捆绑或网页下载先进入计算机的一个临时目录,一般是系统的根目录或系统默认的临时目录,然后将自己激活,这时流氓软件进入内存中正常运行。为了下一次能够自动运行,它们往往会修改注册表的自启动项,从而达到自动启动的目的。然后流氓软件会将自己复制到系统目录隐藏起来,并将临时的安装文件删除,最后监听系统端口,进行各种各样的"流氓"行为。

如果用户喜欢下载安装一些小的工具软件,或者去一些小的网站上浏览网页,也极有可能感染流氓软件,这时也应该关注一下计算机,看是否真正中招,可以按照流氓软件的这个传播链去一一排查。

首先,利用一些第三方的内存查看工具查看内存中是否有一些可疑的进程或线程,这需要用户对系统中的进程或一些常用软件的进程有所了解,这样才有可能看出问题。其次,用户在查看进程的过程中应该看看这些进程的路径,如果有一些进程的路径不是正常的安装目录,而是系统的临时目录,那有可能是流氓软件。另外,用户还要看看注册表中(执行"开始"→"运行"命令,在弹出的对话框中输入 regedit)的自启动项(HKEY_LOCAL_

MACHINE\SOFTWARE\ Microsoft\ Windows\CurrentVersion\Run)中是否有一些用户不认识的程序键值,这些很可能就是流氓软件建立的。

**3. 清理流氓软件**

确认自己中了流氓软件,清除就相对比较简单了。对于已知的流氓软件,建议用户用专门的清除工具进行清除,目前这些工具都是免费的,用户很轻松就能够在网站上下载。很多流氓软件在进入系统之前就对系统进行了修改和关联,当用户擅自删除流氓软件文件时,系统无法恢复到最初状态,从而导致流氓软件虽然清除了,但系统也总是出现各种错误。而专业的清除工具往往已经考虑到这一点,能够帮助用户完全恢复系统。如果在一些特殊场合用户需要手动清除流氓软件,则按照流氓软件的传播链条,按照"先删除内存的进程,再删除注册表中的键值,最后删除流氓软件,将系统配置修改为默认属性"这样一个过程进行处理。

## 5.4 计算机病毒发展趋势

视频讲解

近年来,我国计算机病毒感染率呈现了连续下降的趋势,我国联网计算机用户的病毒防范意识明显增强,并且随着防病毒产品的普及,尤其是个人安全产品的免费化时代的到来,大多数计算机都安装了一些基本的安全软件。一向被视为难以入侵的 Mac 操作系统经历了大规模感染事件,还发生了多起大规模的信息泄露事件,用户的私密信息受到严重的威胁和侵害,同时拥有大量用户的门户网站、社交网络、金融系统、大型企业的系统等成为不法分子攻击的主要目标,通过攻击可从中攫取大量有价值的商业机密和个人用户的私密信息。Java 漏洞成为黑客的新宠。微信、二维码等新型应用在给用户带来良好体验的同时,也给移动终端的安全带来了新的问题和隐患。Android 系统的移动终端病毒呈现爆炸式增长,移动终端安全形势不容乐观。云服务在面临大量市场需求的同时,随之而来的是难以回避的安全问题,海量数据的存储必定成为不法分子新的攻击目标。网络支付的交易规模大幅度增长,支付安全受到普遍关注。

**1. 计算机病毒传播的主要途径**

受经济利益的驱动,网上银行、网络支付等仍然是病毒的主攻目标,在盗取钱财的同时,不法分子还会窃取用户的私密信息。微博也成为新的关注点。针对大型企业、重点行业的病毒传播和攻击增多调查显示,通过网络下载或浏览传播病毒的比例占 75%,操作系统、浏览器和应用软件中存在的大量未修补的漏洞是联网用户的重大安全隐患,也是不法分子用来传播病毒、挂马和发动攻击的最主要途径。下载应用软件中含有的病毒、木马等恶意程序仍然是威胁用户安全的主要因素,尤其各类游戏网站和低俗网站更是病毒、木马散布的温床。通过移动存储介质和电子邮件传播也是其主要传播方式。

**2. 计算机病毒造成的主要危害**

目前计算机病毒主要造成密码和账号被盗、受到远程控制、系统(网络)无法使用、浏览器配置被修改等破坏后果。整体形势不容乐观,虽然大多数用户安装使用了防病毒软件和防火墙,但用户对安全软件的依赖性过高,认为有了安全软件就可以高枕无忧,但安全软件也有其局限性。如何保护用户的私密信息,应对和解决频频爆发的大规模信息泄露事件,已经成为信息安全领域的焦点问题。

**3. 移动终端病毒逐渐增多**

调查显示,移动终端的病毒感染比例每年都在30%以上。但在受感染用户中,多次感染的比例在半数以上,目前出现了利用手机操作系统的僵尸程序,利用微信、微博的钓鱼和欺诈迅猛增长,钓鱼欺诈仿冒技术不断推陈出新,反钓鱼技术的自动化、智能化水平提高。移动终端的安全问题仍然是安全领域的重点和难点。

移动终端病毒感染的途径中,排名第1的是网站浏览,其次是计算机连接和网络聊天,存储介质和电子邮件也占有较高比例。用户感染移动终端病毒后造成的后果主要有影响手机正常运行、信息泄露、恶意扣费、远程受控等。感染后影响手机正常运行成为在感染移动终端病毒后造成的最主要危害,在感染移动终端病毒后产生恶意扣费、发生信息泄露等也占有较高比例。

**4. 隐藏技术越来越强**

隐藏是计算机病毒的一个重要技术。病毒得以有效和广泛传播,被发现的时间长短是关键。隐藏技术的进步是利用数码水印技术隐藏病毒;可通过操作系统或网络层面实现隐藏的网络,如使用编码技术(红色代码);心理学也将被用来隐藏,如利用人类的好奇心或知名品牌的信任(如假冒知名病毒软件应用程序);主动防御技术势必成为病毒的重要隐蔽手段,甚至可能形成专杀防病毒软件和反病毒软件的病毒。

**5. 混合攻击手段更加多样化**

所谓的混合攻击,一方面是指同样的攻击,都含有病毒、黑客攻击,也包括隐蔽通道攻击、拒绝服务攻击,并且可能包含密码攻击、中间人攻击等多种攻击路线;另一方面是指来自不同的地方,或从系统的不同部分,如服务器、客户端、网关等混合式攻击更多的计算机以传播病毒,造成更大的伤害和更快的攻击。混合攻击的主要攻击目标为微软公司的IIS服务器、IE浏览器等市场占有率较高的系统和软件。混合病毒攻击的复杂性将会越来越高,黑客技术和计算机病毒技术日益紧密结合。越来越多的病毒能够在未来的攻击中采用各种组合,从而提高病毒的生存能力和传播能力。

**6. 发生和传播的速度越来越快**

病毒利用系统漏洞的速度和传播速度会越来越快。目前新的计算机系统漏洞不断地被发现。有些漏洞从发现到针对漏洞产生的病毒爆发时间比较短,所以很多用户还来不及修补系统。随着互联网带来的快捷,病毒传播的速度也在迅速发展,只要漏洞是已知的,黑客用于开发新的病毒造成系统崩溃的时间就会更短。一些软件厂商停止对其旧版本的软件进行升级维护,也会造成漏洞不能及时修补,这样也会使用户更加容易受到病毒的攻击。

**7. 跨平台病毒越来越多**

自从1995年开放式语言Java诞生,跨平台便渐成热点,它实现了很多人"一次编译,跨平台运行"的设计理想,Java语言短时间内风靡全球。目前Java和ActiveX Web技术正逐渐被广泛应用于Internet,从而使跨平台病毒的设计更容易。例如,国外研究人员发现了一种只在Linux和Mac OS X上存在的木马,当计算机被入侵之后,该木马会在计算机上安装Wirenet-1键盘记录软件,捕获用户输入的密码和敏感信息,包括Opera,Firefox,Chrome浏览器提交的信息,一些App存储的信息,以及E-mail、Web组件和聊天应用程序的密码。

还出现了通过互联网浏览病毒作者所设计的网站以感染在 Linux 或 Windows 系统的病毒，该病毒会在感染用户的计算机上运行 Java 控件和 Java 虚拟机。跨平台病毒的出现必将对计算机系统造成更大的伤害。

## 5.5 病毒检测技术


视频讲解

随着计算机病毒技术的不断发展，检测和查杀计算机病毒的技术也在不断地更新并趋于复杂化和智能化。为了选取有效的病毒检测技术，本节首先将对传统的病毒诊断技术进行分析和对比，其次对基于网络的病毒检测技术进行分析。

### 5.5.1 传统的病毒检测技术

**1. 程序和数据完整性检测技术**

完整性病毒检测技术是一种相当古老的病毒检测方法。它的基本原理是对每个程序或代码根据某种算法生成校验码(提取签名)，一旦程序发生变化，所产生的校验码必然与原来生成的校验码不同，这时可以初步判断该程序已经被病毒感染。这种技术具有很多弱点，以至于现在几乎不被采用了。其中，病毒检测软件需要建立一个统一的校验码库，不能对经常发生变化的数据文件进行检测和保护。有时，程序被改动并不是病毒感染造成的，从而造成检测的误报率相当高。这种检测方法不能明确地判定病毒的具体类型，而且如果程序在生成校验码前已经被病毒感染，则会逃脱以后的完整性检测。

**2. 病毒特征码检测技术**

病毒特征码检测技术是目前被广泛使用的一种病毒检测技术。它的基本原理是通过对病毒源程序的分析，提取出能够唯一代表该病毒的一串病毒代码，该串代码经过测试是其他程序所没有的。这种病毒检测的方法非常高效，如果病毒特征码提取质量高，病毒的检测率会相当高，而误报率会非常小。这种病毒检测方法能够唯一确定病毒的种类和名称，为下一步的杀毒提供依据。这种检测技术的弱点是它仅仅能够检测已知病毒，而对于未知病毒往往需要经过人工分析，提取特征码后才能进行。随着病毒技术的不断发展，特别是变形病毒的出现，每次传染后病毒代码本身都会加密而各次代码都不相同。这时就不存在一个单一的病毒特征码了，所以病毒特征码检测技术对于变形病毒可以说是无能为力。

**3. 启发式规则(或广谱特征码)病毒检测技术**

启发式规则病毒检测是一种专门针对未知病毒的病毒检测技术。基本原理是通过对一系列病毒代码的分析，提取一种广谱特征码，即代表病毒的某种行为特征的特殊程序代码。当然，仅仅是一段特征码还不能确定一定是某种病毒，通过多种广谱特征码，也就是启发式规则的判断，综合考虑各种因素，确定到底是否是病毒，是哪一种病毒。这种病毒检测方法的优点就是针对未知病毒，而缺点在于它的诊断正确率(包括检测率和误报率)和规则的选取有密切的关系。往往是某些规则对某种病毒很有效，却影响其他类型的病毒检测。规则选取的困难和相互矛盾决定了这种方法只能是一种辅助的检测手段。

**4. 基于操作系统的监视和检测技术**

较早的操作系统监视和检测技术是从中断向量监视开始的，病毒诊断软件通过监视系统的中断向量表判定是否有病毒入侵。此外，内存检测也是操作系统检测技术的手段之一。

随着技术的不断发展,现在的一些杀毒产品采用的是嵌入操作系统内核的检测,它不仅检测中断向量表等一些关键数据结构,还要监视系统的一些关键调用、系统的运行状况、文件系统的访问状况等多个指标,从而判定系统是否工作正常,程序是否被病毒感染。这种监视和检测技术的实现难度很大,需要操作系统厂商的配合。而且,这种方法同样无法确定究竟是何种病毒,误报率很高。

**5. 传统虚拟机病毒检测技术**

虚拟机病毒检测技术是一种最新的病毒检测技术。它的基本原理是为可能的病毒程序构建一个虚拟的运行环境,诱使病毒程序进行感染和破坏活动。虚拟机病毒检测技术的最大优点是能够很高效率地检测出病毒,特别是特征码技术很难解决的变形病毒技术。早期的虚拟机并不是真正意义上的虚拟机,它们仅仅是利用 Windows 操作系统的一些特殊功能构造一个伪虚拟机,但是聪明的病毒程序往往可以破坏虚拟机本身。而且虚拟机的运行需要相当的系统资源,可能会影响正常程序的运行。

通过对以上技术的比较可以看出,无论哪一种技术都不能说是十全十美的。就目前计算机病毒的诊断技术而言,无论哪种诊断软件都不可能只采用某一种诊断方法。最新的病毒诊断技术往往把多种技术融合在一起,发挥各种技术的长处,达到最好的效果。

## 5.5.2 基于网络的病毒检测技术

从本质上讲,基于网络的病毒检测技术并没有在传统的病毒检测技术上做出本质性的更新,新的技术往往是针对网络病毒的特点,对传统的病毒监测技术进行优化并应用在网络环境中。

**1. 实时网络流量检测**

从原理上,实时网络流量检测继承了病毒特征码检测技术,但是网络病毒检测有其独到之处。网络病毒的实时检测将实时地截取网络文件传输的信息流,从传播途径上对病毒进行及时的检测,并能够实时做出反馈行为。网络病毒实时检测的目标是已知的病毒。其优点在于它能实时监测网络流量,发现绝大多数已知病毒;缺点在于随着网络流量呈几何级增长,对巨大的流量进行实时地监测往往需要占用大量的系统资源,同时这种方法对未知病毒完全无能为力。在系统中也使用了实时的网络流量监测,并针对它存在的缺陷进行了改进和完善。

**2. 异常流量分析**

网络流量异常的种类较多,从不同的角度分析有不同的分类结果。从产生异常流量的原因分析可以将其分成 3 个广义的异常类:网络操作异常、闪现拥挤异常和网络滥用异常。网络操作异常是指网络设备的停机、配置改变等导致的网络行为的显著变化,以及流量达到环境极限引起的台阶行为。闪现拥挤异常出现的原因通常是软件版本的问题,或者是国家公开带来的 Web 站点的外部利益问题。特定类型流量的快速增长(如 FTP 流),或者知名 IP 地址的流量随着时间渐渐降低都是闪现拥挤的显著表现。网络滥用异常主要是由以 DoS 洪泛攻击和端口扫描为代表的各种网络攻击导致的,这种网络异常也是网络病毒检测系统所感兴趣的。

基于网络滥用异常的流量分析可以看作对启发式规则病毒检测技术的一种衍生,这种技术的优势是能发现未知的网络病毒,同时可以通过流量信息直接定位可能感染了病毒的计算机,对于一些蠕虫的变种和新的网络病毒有较好的发现效果。

**3. 蜜罐系统**

蜜罐系统可以看作传统的虚拟机病毒检测技术在网络环境中的一种新的应用。蜜罐定义为一种安全资源，它并没有任何业务上的用途，它的价值就是吸引攻击者对它进行非法使用。蜜罐技术本质上是一种对攻击者进行欺骗的技术，通过布置一些作为诱饵的主机、网络服务和信息诱使攻击者对其进行攻击，减少对实际系统所造成的安全威胁。更重要的是，蜜罐技术可以对攻击行为进行监控和分析，了解攻击者所使用的攻击工具和攻击方法，推测攻击者的意图和动机，在此基础上尽可能地追踪攻击者的来源，对其攻击行为进行审计和取证，从而能够让防御者清晰地了解他们所面对的安全威胁，并通过法律手段去追究攻击者的责任，或者通过技术和管理手段增强对实际系统的安全防护能力。蜜罐技术最大的应用目标是提供一个高度可控的环境对互联网上的各种安全威胁（包括黑客攻击、恶意软件传播、垃圾邮件、僵尸网络和网络钓鱼等）进行深入的了解与分析，从而为安全防御提供知识和经验支持。

## 课 后 习 题

**一、选择题**

1. 下列不属于计算机病毒防治策略的是（　　）。

A. 确认手头常备一张真正“干净”的引导盘

B. 及时、可靠升级反病毒产品

C. 新购置的计算机软件也要进行病毒检测

D. 整理磁盘

2. 计算机病毒的特征之一是（　　）。

A. 非授权不可执行性　　B. 非授权可执行性

C. 授权不可执行性　　D. 授权可执行性

3. 计算机病毒最重要的特征是（　　）。

A. 隐蔽性　　B. 传染性　　C. 潜伏性　　D. 破坏性

4. 计算机病毒（　　）。

A. 不影响计算机的运算速度　　B. 可能会造成计算机器件的永久失效

C. 不影响计算机的运算结果　　D. 不影响程序执行，破坏数据与程序

5. CIH 病毒破坏计算机的 BIOS，使计算机无法启动。它是由时间条件来触发的，其发作的时间是每月的 26 日，这主要说明病毒具有（　　）。

A. 可传染性　　B. 可触发性　　C. 破坏性　　D. 免疫性

6. 计算机病毒最本质的特性是（　　）。

A. 寄生性　　B. 潜伏性　　C. 破坏性　　D. 攻击性

7. 针对操作系统安全漏洞的蠕虫病毒根治的技术措施是（　　）。

A. 防火墙隔离　　B. 安装安全补丁程序

C. 专用病毒查杀工具　　D. 部署网络入侵检测系统

8. 下列不属于网络蠕虫病毒的是（　　）。

A. 冲击波　　B. SQL Slammer

C. CIH　　D. 震荡波

9. 传统的文件型病毒以计算机操作系统作为攻击对象,而现在越来越多的网络蠕虫病毒将攻击范围扩大到了(　　)等重要网络资源。

A. 网络带宽　　B. 数据包　　C. 防火墙　　D. Linux

10. (　　)不是计算机病毒所具有的特点。

A. 传染性　　B. 破坏性　　C. 潜伏性　　D. 可预见性

11. 下列不属于计算机病毒特征的是(　　)。

A. 潜伏性　　B. 传染性　　C. 免疫性　　D. 破坏性

12. 在目前的信息网络中,(　　)病毒是最主要的病毒类型。

A. 引导型　　B. 文件型　　C. 网络蠕虫　　D. 木马型

13. 编制或在计算机程序中插入的破坏计算机功能或毁坏数据,影响计算机使用,并能自我复制的一组计算机指令或程序代码是(　　)。

A. 计算机病毒　　B. 计算机系统　　C. 计算机游戏　　D. 计算机程序

14. 要实现有效的计算机和网络病毒防治,(　　)应承担责任。

A. 高级管理层　　B. 部门经理

C. 系统管理员　　D. 所有计算机用户

15. (　　)不属于在局域网中计算机病毒的防范策略。

A. 仅保护工作站　　B. 完全保护工作站和服务器

C. 保护打印机　　D. 仅保护服务器

16. 现代病毒木马融合了(　　)新技术。

A. 进程注入　　B. 注册表隐藏　　C. 漏洞扫描　　D. 以上都是

17. 当收到认识的人发来的电子邮件并发现其中有附件,应该(　　)。

A. 打开附件,然后将它保存到硬盘

B. 打开附件,但是如果它有病毒,立即关闭它

C. 用防病毒软件扫描以后再打开附件

D. 直接删除该邮件

18. 下列不能防止计算机感染病毒的措施是(　　)。

A. 定时备份重要文件

B. 经常更新操作系统

C. 除非确切知道附件内容,否则不要打开电子邮件附件

D. 重要部门的计算机尽量专机专用,与外界隔绝

**二、填空题**

1. 网络病毒主要进行游戏等_____的盗取工作,远程操控,或把你的计算机当作_____使用。

2. 特洛伊木马简称木马,它是一种基于_____的黑客工具,具有_____和_____的特点。

3. 木马通常有两个可执行程序:一个是_____;另一个是_____。

4. 蠕虫程序主要利用_____进行传播。

5. 蠕虫病毒采取的传播方式一般为_____和_____。

6. _____可以阻挡90%的黑客、蠕虫病毒及消除系统漏洞引起的安全性问题。

7. 网络流量异常的种类较多，从产生异常流量的原因分析可以将其分为 3 个广义的异常类：_____、_____和网络滥用异常。

8. 受经济利益的驱动，_____、_____等仍然是病毒的主攻目标。

9. 通过_____和_____是病毒的主要传播方式。

10. 移动终端病毒感染的途径中，排名第 1 的是_____，其次是计算机连接和_____。

11. 流氓软件定义为“在_____或_____未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上强行安装运行，侵犯用户合法权益的软件，但已被我国法律法规规定的计算机病毒除外”。

12. 网络蠕虫病毒越来越多地借助网络作为传播途径，主要包括互联网浏览、文件下载、_____、_____、局域网文件共享等。

**三、简答题**

1. 什么是计算机病毒？
2. 计算机病毒的特点有哪些？
3. 计算机病毒的破坏行为有哪些？
4. 计算机病毒的主要危害有哪些？
5. 什么是木马？
6. 网页挂马常见方式主要有哪几种？
7. 木马的种类有哪些？
8. 防范木马攻击的主要措施有哪些？
9. 木马病毒的检测步骤有哪些？
10. 木马病毒的查杀步骤有哪些？
11. 什么是蠕虫？
12. 蠕虫病毒的特征有哪些？
13. 蠕虫病毒的防治措施有哪些？
14. 蠕虫技术发展的趋势有哪些？
15. 网络病毒的发展趋势有哪些？
16. 计算机防毒杀毒的常见误区有哪些？
17. 流氓软件有哪些特点？
18. 流氓软件分为哪些类型？
19. 计算机病毒的发展趋势有哪几点？
20. 病毒检测技术主要有哪些种类？