Contents 目录

项目 4　恶意代码病毒环境

项目 5　高级代码演化技术和病毒生成工具

项目 6 计算机病毒的发展趋势及新进展

项目 7 计算机病毒的传播模型

项目 8　计算机病毒检测技术

项目 9　反病毒软件的编制技术

项目 10　计算机病毒防范、免疫与清除技术

项目 11 计算机病毒防治策略

项目 12 典型病毒的防范技术

项目 1 计算机病毒概述

知识目标

1. 了解计算机病毒的发展过程。
2. 理解计算机病毒的原理与分类。
3. 了解计算机感染病毒的症状。

技能目标

1. 掌握不同种类计算机病毒的感染机制。
2. 分析计算机病毒程序和一般程序的联系与区别。
3. 能够判断计算机是否感染了病毒，并采取相应策略解决问题。

知识导图

笔记

项目导入

典型的计算机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者程序代码”。计算机病毒是类似于生物病毒所具有的一些特征，它会复制自己并传播到其他宿主，并对宿主造成损害。计算机病毒中的宿主也是计算机程序。计算机病毒在传播期间一般会隐蔽自己，经过特定的条件能够触发并产生破坏。

任务 1.1 计算机病毒的产生与发展

子任务 1.1.1 计算机病毒的起源

关于计算机病毒的起源现在有几种说法，但还没有一个被人们所确认，也没有实质性的论述予以证明。下面将几种起源说简单介绍一下。

1. 科学幻想起源说

1977 年，美国科普作家托马斯·J·雷恩推出轰动一时的 *Adolescence of p-1* 一书。书中构想了一种能够自我复制，利用信息通道传播的计算机程序，并称之为计算机病毒。这是世界上第一个幻想出来的计算机病毒。人类社会有许多现行的科学技术，都在先有幻想之后才成为现实。因此，不能否认这本书的问世对计算机病毒的产生所起的作用。

2. 游戏程序起源说

在 20 世纪 70 年代，计算机在人们的生活中还没有普及，美国贝尔实验室的计算机程序员为了娱乐，在自己实验室的计算机上编制吃掉对方程序的程序，看谁先把对方的程序吃光，有人认为这是世界上第一个计算机病毒，但这也只是一个猜测。

3. 软件商保护软件起源说

计算机软件是一种知识密集型的高科技产品，由于人们对于软件资源的保护不尽合理，这就使得许多合法的软件被非法复制的现象极为普遍，从而使软件制造商的利益受到了严重的损害。因此，软件制造商为了处罚那些非法复制者，而在软件产品中加入了病毒程序并由一定条件触发感染。例如，Pakistani Brain 病毒在一定程度上就证实了这种说法。该病毒是巴基斯坦的两兄弟为了追踪非法复制其软件的用户而编制的，它只是修改磁盘卷标，把卷标改为 Brain 以便识别。也正是因为如此，当计算机病毒出现之后，有人认为这是软件制造商为了保护自己的软件不被非法复制而导致的结果。

子任务 1.1.2 计算机病毒类型及命名

1. 计算机病毒的常见类型

（1）系统病毒：前缀为 Win32、PE、Win95、W32、W95 等。共同特性：感染 Windows 操作系统的 *.exe 和 *.dll 文件，并通过这些文件进行传播。例如：CIH 病毒。

（2）蠕虫病毒：前缀为 Worm。特性：通过网络或者系统漏洞进行传播，大部分蠕虫病毒都有向外发送带毒邮件、阻塞网络的特性。例如：冲击波、小邮差病毒。

（3）木马病毒与黑客病毒：木马病毒前缀为 Trojan，黑客病毒前缀为 Hack。特性：

笔记

通过网络或系统漏洞进入用户系统并隐藏起来，然后向外界泄露用户的信息；而黑客病毒则有一个可视界面，能对用户的计算机进行远程控制。木马病毒和黑客病毒往往成对出现，木马病毒负责侵入用户计算机，黑客病毒通过木马病毒进行远程控制。两者趋于整合。

（4）脚本病毒：前缀是 Script。特性：使用脚本语言编写，通过网页进行传播。

（5）宏病毒：特殊脚本病毒，前缀是 Macro，第二前缀是 Word，Word97，Excel，Excel97 等。特性：感染 Office 文档，通过 Office 通用模板进行传播。凡是只感染 Word97 及以前版本 Word 文档的病毒采用 Word97 作为第二前缀，格式是 Macro.Word97；凡是只感染 Word97 以后版本 Word 文档的病毒都采用 Word 作为第二前缀，格式是 Macro.Word；凡是只感染 Excel97 及以前版本 Excel 文档病毒采用 Excel97 作为第二前缀，格式是 Macro.Excel97；凡是只感染 Excel97 以后版本 Excel 文档的病毒采用 Excel 作为第二前缀，格式是 Macro.Excel，以此类推。

（6）后门病毒：前缀为 Backdoor。特性：通过网络传播，给系统开后门，给用户计算机带来安全隐患。

（7）病毒种植程序：特性：运行时会释放出一个或几个新的病毒，存放在系统目录下，并由释放出来的新病毒产生破坏作用。

（8）破坏性程序病毒：前缀是 Harm。特性：本身具有好看的图标来诱惑用户点击。当用户点击时，会对计算机产生破坏。

（9）玩笑病毒：前缀是 joke，也称恶作剧病毒。特性：具有好看的图标来诱惑用户点击，当用户点击时，会呈现出各种破坏性画面来吓唬用户，并没有对计算机进行破坏。

（10）捆绑机病毒：前缀是 Binder。特性：病毒编制者使用特定的捆绑程序将病毒与一些应用程序捆绑起来。表面上看是一个正常文件，当用户运行这些捆绑了病毒的程序时，表面上运行的是正常程序，实际上隐藏地运行了捆绑在一起的病毒，从而给用户造成危害。

另外，还有一些特殊病毒，例如：DoS 病毒会针对某台主机或者服务器进行 DoS 攻击；Exploit 病毒会通过溢出系统漏洞来传播自身，或者其本身就是一个用于 Hacking 的溢出工具；HackTool 是一种黑客工具，也许它本身并不破坏用户计算机，但是会被利用，劫持用户去破坏其他人。

2. 计算机病毒的命名规则

病毒名称的一般格式：＜病毒前缀＞.＜病毒名＞.＜病毒后缀＞。

病毒前缀：病毒的种类，不同种类的病毒前缀不同。例如，木马病毒的前缀 Trojan、蠕虫病毒的前缀 Worm。计算机常见的病毒前缀见表 1-1。

病毒名：病毒的家族特征。例如：CIH 病毒家族名为“CIH”、震荡波蠕虫家族名为“Sasser”。

病毒后缀：用来区别某个家族病毒的不同变种，一般用英文字母表示。例如：Worm.Sasser.b 就是指震荡波蠕虫的变种。

笔记

表 1-1　计算机常见的病毒前缀表

前缀	描述
AM	Access 宏病毒
AOL	专门针对美国在线的恶意传播代码
BAT	用 DOS 的批处理语句编写的病毒
BOOT	DOS 引导型病毒
JAVA	用 Java 编写的病毒
JS	用 JavaScript 编写的脚本病毒
PWSTEAL	盗取口令的木马病毒
TRO	一般木马病毒
VBS	Visual Basic 脚本病毒或蠕虫病毒
W32/WIN32	所有可以感染 32 位平台的 32 位病毒
W95/W98/W9X	Windows 9x 和 Windows Me 病毒
WIN/WIN16	Windows 3.x 专有病毒
WM	Word 宏病毒
W2K	Windows 2000 病毒
XF	Excel 公式病毒，利用 Excel 4.0 结构
XM	Excel 宏病毒

子任务 1.1.3 计算机病毒的性质

计算机病毒主要具有以下性质。

1. 可执行性

计算机病毒其实就是一段可执行程序，它和其他正常的计算机程序一样可以被执行，这就是计算机病毒的可执行性，计算机病毒并不是一段完整的程序，它主要寄生在存储介质的一些盲区或者是其他可执行程序中，当用户无意间执行带病毒的程序或者启动带病毒的系统时，病毒程序就有可能被激活。

2. 传染性

传染性是计算机病毒的一个最基本的特性，也是判断一个计算机程序是否是病毒的一项重要依据，正常的计算机程序是不会将其自身的程序代码强加到其他程序上的，但是病毒程序恰恰相反，它能把自身的代码强行附着在一切条例及传染性的程序中。

3. 可触发性

病毒程序都对其运行设置了一定的条件，当用户电脑满足这个条件时，病毒程序就会实施感染或者对电脑系统进行攻击，这称之为病毒程序的可触发性，病毒程序的触发条件有很多，可能是日期、时间、文件类型，某些特定的数据或者是系统启动的次数等。

4. 潜伏性

计算机病毒是设计精巧的一段计算机小程序，当其侵入到系统后并不会马上发作，可能较长时间都会隐藏在某些文件当中，等到时机成熟之后才会发作，病毒程序潜伏的时间越长，其感染的范围就可能越广。

笔记

5. 针对性

许多病毒程序都是针对特定的操作系统的，病毒程序会根据用户使用的硬件和操作系统的不同而潜伏或者是攻击。

6. 隐蔽性

随着社会的发展，黑客所编写的病毒程序在隐蔽性方面做得越来越好，这些病毒程序短小精悍，多是以隐藏的文件的形式潜伏在计算机中。

7. 破坏性

破坏性是计算机病毒的最终目的，所有病毒程序都是为了达到一定的破坏目的而编写的。当电脑中病毒后，启动系统时，除了运行一些基本的程序之外还要运行这些病毒程序，这样计算机病毒在一定程度上就会影响电脑的启动速度。

子任务 1.1.4　计算机病毒的发展历史

在病毒的发展史上，它的出现是有规律的，一般情况下一种新的病毒技术出现后迅速发展，接着反病毒技术的发展会抑制其流传。操作系统升级后，病毒也会调整为新的方式，产生新的病毒技术。计算机病毒的发展经历了以下几个阶段。

1. DOS 引导阶段

1987 年，计算机病毒主要是引导型病毒，具有代表性的是“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，引导型病毒发展为可以感染硬盘，典型的代表有“石头 2”病毒。

2. DOS 可执行阶段

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”“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。

3. 伴随、批次型阶段

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 文件时生成一个和 EXE 同名但扩展名为 COM 的伴随体；它感染文件时，改原来的 COM 文件为同名的 EXE 文件，再产生一个原名的伴随体，文件扩展名为 COM，这样，在 DOS 加载文件时，病毒就取得控制权。这类病毒的特点是不改变原来的文件内容、日期及属性，解除病毒时只要将其伴随体删除即可。在非 DOS 操作系统中，一些伴随型病毒利用操作系统的描述语言进行工作，具有典型代表的是“海盗旗”病毒，它在执行时会询问用户名称和口令，然后返回一个出错信息，将自身删除。批次型病毒是工作在 DOS 下的和“海盗旗”病毒类似的一类病毒。

4. 多形阶段

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

笔记

序，病毒体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。多形型病毒是一种综合性病毒，它既能感染引导区又能感染程序区，多数具有解码算法，一种病毒往往要两段以上的子程序方能解除。

5. 变种阶段

1995 年，在汇编语言中，一些数据的运算放在不同的通用寄存器中，可运算出同样的结果，随机地插入一些空操作和无关指令，也不影响运算的结果，这样，一段解码算法就可以由生成器生成，当生成器的生成结果为病毒时，就产生了这种复杂的“病毒生成器”，而变体机就是增加解码复杂程度的指令生成机制。这一阶段的典型代表是“病毒制造机”VCL，它可以在瞬间制造出成千上万种不同的病毒，查解时就不能使用传统的特征识别法，需要在宏观上分析指令，解码后查解病毒。

6. 网络蠕虫阶段

1995 年，随着网络的普及，病毒开始利用网络进行传播，它们只是以上几代病毒的改进。在非 DOS 操作系统中，“蠕虫”是典型的代表，它不占用除内存以外的任何资源，不修改磁盘文件，利用网络功能搜索网络地址，将自身向下一个地址进行传播，有时也在网络服务器和启动文件中存在。

7. 视窗阶段

1996 年，随着 Windows 和 Windows95 的日益普及，利用 Windows 进行工作的病毒开始发展，它们修改（NE，PE）文件，典型的代表是 DS.3873，这类病毒的机制更为复杂，它们利用保护模式和 API 调用接口工作，解除方法也比较复杂。

8. 宏病毒阶段

1996 年，随着 Windows Word 功能的增强，使用 Word 宏语言也可以编制病毒，这种病毒使用类 Basic 语言、编写容易、感染 Word 文档等文件，在 Excel 和 AmiPro 出现的相同工作机制的病毒也归为此类，由于 Word 文档格式没有公开，这类病毒查解比较困难。

9. 互联网阶段

1997 年以后，因特网发展迅速，各种病毒也开始利用因特网进行传播，一些携带病毒的数据包和邮件越来越多，如果不小心打开了这些邮件或登录了带有病毒的网页，计算机就有可能中毒。典型代表有“尼姆达”“欢乐时光”和“欢乐谷”等病毒。

2003 年，“2003 蠕虫王”病毒在亚洲、美洲、澳大利亚等地迅速传播，造成了全球性的网络灾难。其中受害最严重的无疑是美国和韩国这两个因特网发达的国家。韩国 70% 的网络服务器处于瘫痪状态，网络连接的成功率低于 10%，整个网络速度极慢。美国不仅公众网络受到了破坏性的攻击，而且连银行网络系统也遭到了破坏，全国 1.3 万台的自动取款机处于瘫痪状态。

2004 年是“蠕虫”泛滥的一年，网络天空（Worm.Netsky）、高波（Worm.Agobot）、爱情后门（Worm.Lovgate）、震荡波（Worm.Sasser）、无极（Worm.SoBig）等病毒严重危害了互联网的使用和安全。

2006 年的“熊猫烧香”使所有程序图标变成熊猫烧香，并使它们不能应用。

2008 年“扫荡波”同冲击波和震荡波一样，也是个利用漏洞从网络入侵的程序。而且正好在黑屏事件期间，大批用户关闭自动更新以后，加剧了这个病毒的蔓延，这个病毒可以完全控制被攻击的机器。

2010 年的“鬼影”病毒成功运行后，在进程中，系统启动加载项里找不到任何异常，即使格式化重装系统，也无法将该病毒彻底清除。犹如鬼影一般阴魂不散，所以称为“鬼影”病毒。

如今，计算机病毒变得更加活跃，“木马”“蠕虫”“后门”等病毒层出不穷，自 2000 年以来，由于病毒的基本技术和原理被越来越多的人所掌握，新病毒的出现以及原有病毒的变种层出不穷，病毒的增长速度超过了以往的任何时期。

笔记

任务 1.2　计算机病毒的基本概况

子任务 1.2.1 计算机病毒的生命周期

计算机病毒的产生过程可分为：程序设计—传播—潜伏—触发—运行—实行攻击。计算机病毒拥有一个生命周期，从生成开始到完全根除结束。下面我们描述病毒生命周期的各个时期。

开发期：在几年前，制造一个病毒需要计算机编程语言的知识。但是今天，有一点计算机编程知识的人都可以制造一个病毒。通常计算机病毒是一些误入歧途的、试图传播计算机病毒和破坏计算机的个人或组织制造的。

传染期：在一个病毒制造出来后，病毒的编写者将其拷贝并确认其已被传播出去。通常的办法是感染一个流行的程序，再将其放入 BBS 站点上、校园和其他大型组织当中分发其复制物。

潜伏期：病毒是自然地复制的。一个设计良好的病毒可以在它活化前长时期里被复制。这就给了它充裕的传播时间。这时病毒的危害在于暗中占据存储空间。

发作期：带有破坏机制的病毒会在遇到某一特定条件时发作，一旦遇上某种条件，比如某个日期或出现了用户采取的某特定行为，病毒就被活化了。

发现期：当一个病毒被检测到并被隔离出来后，它被送到计算机安全协会或反病毒厂家，在那里病毒被通报和描述给反病毒研究工作者。通常发现病毒是在病毒成为社会的灾难之前完成的。这一段并非总是这样做，但通常如此。

消化期：在这一阶段，反病毒开发人员修改他们的软件使其可以检测到新发现的病毒。这段时间的长短取决于开发人员的素质和病毒的类型。

消亡期：若是用户安装了相应防范功能的软件，能够检测及控制这些计算机病毒，那么这些计算机病毒有可能被扫除。但有一些病毒在消失之前有一个很长的消亡期。

子任务 1.2.2 计算机病毒的传播途径

1. 软盘

软盘作为早期的交换媒介，在计算机应用的早期对病毒的传播发挥了巨大的作用。因那时计算机应用比较简单，可执行文件和数据文件系统都较小，许多执行文件均通过软盘相互拷贝、安装，这样病毒就能通过软盘传播文件型病毒；另外，在软盘列目录或引导机器时，引导区病毒会在软盘与硬盘引导区互相感染。因此软盘也成了计算机病毒的主要寄生的温床。

笔记

2. 光盘

光盘因为容量大，存储了大量的可执行文件，大量的病毒就有可能藏身于光盘。但是，对于只读式光盘不能进行写操作，因此光盘上的病毒不能清除。以谋利为目的非法盗版软件在制作过程中，不可能为病毒防护担负专门责任，也绝不可能会有真正可靠可行的技术保障避免病毒的传入、传染、流行和扩散。当前，盗版光盘的泛滥给病毒的传播带来了极大的便利。

3. 硬盘

由于带病毒的硬盘在本地或移到其他地方使用、维修等，将干净的硬盘传染并再扩散。

4. BBS

电子布告栏（BBS）因为上站容易、投资少，因此深受大众用户的喜爱。BBS 是由计算机爱好者自发组织的通信站点，用户可以在 BBS 上进行文件交换（包括自由软件、游戏、自编程序）。由于 BBS 一般没有严格的安全管理，亦无任何限制，这样就给一些病毒程序编写者提供了传播病毒的场所。各城市 BBS 站间通过中心站间进行传送，传播面较广。随着 BBS 在国内的普及，给病毒的传播又增加了新的介质。

5. 网络

（1）不法分子或好事之徒制作的匿名个人网页直接提供了下载大批病毒活样本的便利途径。

（2）由于学术研究的病毒样本提供机构同样可以成为别有用心的人的使用工具。

（3）专门用于病毒制作者研究讨论的学术性质的电子论文、期刊、杂志及相关的网上学术交流活动，如病毒制造协会年会等，都有可能成为国内外任何想成为新的病毒制造者学习、借鉴、盗用、抄袭的目标与对象。

（4）散列于网站上大批病毒制作工具、向导、程序等，使得无编程经验和基础的人制造新病毒成为可能。

（5）新技术、新病毒使得几乎所有人在不知情时、无意中成为病毒扩散的载体或传播者。

上面讨论了计算机病毒的传播途径，随着各种反病毒技术的发展和人们对病毒各种特性的了解，通过对各种传播途径的严格控制，来自病毒的侵扰会越来越少。

子任务 1.2.3 计算机感染上病毒的一般症状

大多数计算机病毒都是属于“恶性”计算机病毒。“恶性”计算机病毒发作后往往会带来很大的损失，以下列举了一些“恶性”计算机病毒发作后所造成的后果。

（1）硬盘无法启动，数据丢失。计算机病毒破坏了硬盘的引导扇区后，就无法从硬盘启动计算机系统了。有些计算机病毒修改了硬盘的关键内容（如文件分配表，根目录区等），使得原先保存在硬盘上的数据几乎完全丢失。

（2）系统文件丢失或被破坏。通常系统文件是不会被删除或修改的，除非对计算机操作系统进行了升级。但是某些计算机病毒发作时删除了系统文件，或者破坏了系统文件，导致无法正常启动计算机系统。通常容易受攻击的系统文件 Command.com，Emm386.exe，Win.com，Kernel.exe，User.exe 等。

笔记

（3）文件目录发生混乱。目录发生混乱有两种情况。一种就是确实将目录结构破坏，将目录扇区作为普通扇区，填写一些无意义的数据，再也无法恢复。另一种情况是将真正的目录区转移到硬盘的其他扇区中，只要内存中存在该计算机病毒，它便能够将正确的目录扇区读出，并在应用程序需要访问该目录的时候提供正确的目录项，使得从表面上看来与正常情况没有两样。但是一旦内存中没有该计算机病毒，那么通常的目录访问方式将无法访问到原先的目录扇区。这种破坏还是能够恢复的。

（4）部分文档丢失或被破坏。类似系统文件的丢失或被破坏，有些计算机病毒在发作时会删除或破坏硬盘上的文档，造成数据丢失。

（5）部分文档自动加密码。还有些计算机病毒利用加密算法，将加密密钥保存在计算机病毒程序体内或其他隐蔽的地方，而被感染的文件被加密，如果内存中驻留有这种计算机病毒，那么在系统访问被感染的文件时它自动将文档解密，使得用户察觉不到。一旦这种计算机病毒被清除，那么被加密的文档就很难恢复了。

（6）修改 Autoexec.bat 文件，增加 Format C：一项，导致计算机重新启动时格式化硬盘。 在计算机系统稳定工作后，一般很少会有用户去注意 Autoexec.bat 文件的变化，但是这个文件在每次系统重新启动的时候都会自动运行，计算机病毒修改这个文件从而达到破坏系统的目的。

（7）使部分可软件升级主板的 BIOS 程序混乱，主板被破坏。 类似 CIH 计算机病毒发作后的现象，系统主板上的 BIOS 被计算机病毒改写、破坏，使得系统主板无法正常工作，从而使计算机系统报废。

（8）网络瘫痪，无法提供正常的服务。

由上所述，我们可以了解到防杀计算机病毒软件必须要实时化，在计算机病毒进入系统时要立即报警并清除，这样才能确保系统安全，待计算机病毒发作后再去杀毒，实际上已经为时已晚。

子任务 1.2.4　计算机病毒在网络环境下表现的特征

现在，在网络环境下，计算机病毒除了以往的可传播性、破坏性、可触发性以及潜伏性等特征之外，还出现了以下几种新特征。

（1）扩散的速度特别快，传播的途径也很多。现在很多病毒都是利用局域网、系统的漏洞、邮件以及网页等方式传播，扩散起来速度也特别的快。比如说“震荡波”病毒，这种病毒利用安全漏洞进行传播，八天的时间便感染了全球一千八百万台电脑。还有蠕虫病毒三十秒之内便能够发一百封带有病毒的邮件。

（2）危害性特别大。现在计算机病毒的破坏性特别的强，并且还和其他的技术融合在了一起，比如说有些病毒具有蠕虫病毒、木马病毒、普通病毒和黑客技术的特点，有着非常明显的混合型特征。有名的“美丽杀”“爱虫”都给人们带来了很大的危害。有的甚至会导致计算机瘫痪，丢失重要的文件或者数据，还有的会出现信息被窃取的情况，甚至还有些病毒能够控制网络和计算机系统。若是病毒大规模蔓延，便很难采取有效的措施对其进行控制。

（3）病毒的变种比较多，并且速度也很快。现在很多病毒都是利用高级语言进行编写的，制作的方法比较简单。比如说“爱虫”病毒便是一种脚本语言，而“美丽杀”则是一

笔记

种宏病毒。这些病毒编写起来比较容易，并且还很容易被修改，病毒变种也特别容易，只要修改几个比较简单的指令，便能够使其变异，出现很多种计算机病毒。“爱虫”病毒在短短的十几天中，便产生了三十多种的变种。“美丽杀”也出现了好几种变种。还有很多木马的变种也非常快，比如说“灰鸽子”和“赛波”，大都能够产生 100 多种变种。

（4）病毒隐蔽性比较强，清除很难做到彻底。由于病毒不断地变化，现在很多病毒并不写到硬盘上，仅仅是在内存中，无法找到病毒特征和其代码，病毒启动的时候，在内存里也找不到相应的病毒体，即使病毒有相应代码，那些代码一般也都是加了密的，可以逃过搜索，隐蔽性特别强，使人很难找到病毒。并且还有的病毒善于伪装自己，伪装成一些人们比较感兴趣的东西。在网络中若是有一台工作站存在病毒，并且没有彻底地完成病毒查杀，那么网络中所有的电脑就可能重新感染，所以在网络中仅仅完成一部分工作站的病毒查杀工作，根本无法真正的解决病毒问题，所以必须整个互联网一起查杀，这种情况显然很困难。

（5）病毒的针对性和目的性要更强。以前的一些病毒都是一些编程高手为了炫耀自己的计算机技术而编写的，而现在的病毒目的往往是经济上的利益。“盗号木马”便是其中比较典型的代表。在运行的时候，没有任何的提示，用户根本不知道自己的计算机已经中毒，这些病毒会自动地记录用户的一些个人信息、各种账号的密码，并且将其传递给黑客，给大量的用户造成经济方面的损失。

子任务 1.2.5 计算机病毒的分类

1. 按照病毒的破坏情况分类

（1）良性病毒。良性病毒是不包含对计算机系统产生直接破坏作用的代码的计算机病毒。这类病毒为了表现其存在，只是不停地进行传播，并不破坏计算机系统和数据，但它会使系统资源急剧减少，可用空间越来越少，最终导致系统崩溃。如国内出现的“小球”病毒就是良性的。良性病毒又可分为无危害型病毒和无危险型病毒。

提示

良性和恶性是相比较而言的，不可轻视任何一种病毒对计算机系统造成的损害。

（2）恶性病毒。恶性病毒指在代码中包含损伤和破坏计算机系统的操作，在其传染或发作时会对系统产生直接破坏作用的计算机病毒。这类病毒很多，如米开朗基罗病毒，当其发作时，硬盘的前 17 个扇区将被彻底破坏，使整个硬盘上的数据丢失。有的病毒还会对硬盘进行格式化操作。恶性病毒又分为危险型病毒和非常危险型病毒。

2. 按照病毒攻击的系统分类

（1）DOS 病毒。这类病毒出现较早，种类及其变种极其多。尽管 DOS 技术在 1995 年以后基本上处于停滞状态，但这类病毒的数量和传播仍在发展，只是比较缓慢而已。

（2）攻击 Windows 系统的病毒。从 1995 年以后，Windows 逐渐取代 DOS 而成为微型计算机的主流操作系统，也使其成为病毒的主要攻击对象，首例破坏计算机硬件的 CIH 病毒就是一个以 VxD 为技术核心的 Windows 9x 病毒。

提示

当前，UNIX 和 Linux 应用非常广泛，并且大多数大型服务器均采用 UNIX 为主要操作系统，UNIX 病毒的出现，对信息处理是一个严重的威胁。

（3）攻击 UNIX 系统的病毒。最初，人们认为 UNIX 和 Linux 系统是免遭病毒侵袭的乐土。然而，随着病毒技术的发展，病毒的攻击目标已经开始染指 UNIX 和 Linux 系统。1997 年 2 月，出现了首例攻击 Linux 系统的病毒——Bliss（上天的赐福）病毒；2001 年 4 月，出现了首例 Windows 和 Linux 操作系统下都能传播的 Win32.Winux 病毒，它主要感染 Windows PE 和 Linux ELF 文件。

笔记

（4）攻击 OS/2 系统的病毒。第一个真正 OS/2 操作系统意义下的病毒，是在 1996 年 2 月发现的 AEP 病毒，该病毒首次将自身依附在 OS/2 系统可执行文件的后面实施感染功能，而在 AEP 病毒之前出现在 OS/2 系统上的“病毒”，要么只能使用该“病毒”文件替换原来的文件，要么只能以伴随病毒的形式出现，均不具备计算机病毒的传染性这一基本特性。第一个针对 OS/2 系统的病毒虽简单，但却是一个不好的开端。

（5）攻击 Macintosh 系统的病毒。如 Mac.simpsons 是使用 AppleScript 编写的病毒程序，它将自己发送到 Outlook Express 或 Entourage 邮件程序的用户地址。

（6）其他操作系统上的病毒。如手机病毒、PDA 病毒等。第一例手机病毒是 2000 年 6 月在西班牙发现的 VBS.Timofonica 病毒。该病毒通过运营商 Telefonica 的移动系统向该系统内的任意用户发送骂人的短消息。

3. 按照病毒的寄生部位或传染对象分类

传染性是计算机病毒的本质属性，根据寄生部位或传染对象分类，即根据计算机病毒传染方式进行分类，主要包括：磁盘引导区传染的计算机病毒、操作系统传染的计算机病毒和可执行程序传染的计算机病毒。

（1）磁盘引导区传染的计算机病毒。磁盘引导区传染的病毒主要是用病毒的全部或部分逻辑取代正常的引导记录，而将正常的引导记录隐藏在磁盘的其他地方。由于引导区是磁盘能正常使用的先决条件，因此，这种病毒在运行的一开始（如系统启动）就能获得控制权，其传染性较大。由于在磁盘的引导区内存储着需要使用的重要信息，如果对磁盘上被移走的正常引导记录不进行保护，则在运行过程中就会导致引导记录的破坏。引导区传染的计算机病毒较多，例如，“大麻”和“小球”病毒就是这类病毒。

（2）操作系统传染的计算机病毒。操作系统是一个计算机系统得以运行的支持环境，它包括 .com、.exe 等许多可执行程序及程序模块。操作系统传染的计算机病毒就是利用操作系统中所提供的一些程序及程序模块寄生并传染的。通常，这类病毒作为操作系统的一部分，只要计算机开始工作，病毒就处在随时被触发的状态。而操作系统的开放性和不绝对完善性给这类病毒出现的可能性与传染性提供了方便。操作系统传染的病毒目前已广泛存在，“黑色星期五”即为此类病毒。

（3）可执行程序传染的计算机病毒。可执行程序传染的病毒通常寄生在可执行程序中，一旦程序被执行，病毒也就被激活，病毒程序首先被执行，并将自身驻留内存，然后设置触发条件，进行传染。

对于以上三种病毒的分类，实际上可以归纳为两大类：一类是引导区型传染的计算机病毒；另一类是可执行文件型传染的计算机病毒。

4. 按照计算机病毒的攻击机型分类

（1）微型计算机的病毒。这是最为庞大的病毒家族。例如，攻击 Commodore 公司生产的微型计算机的 Amiga 病毒，攻击 Apple 公司生产的微型计算机的 MacMag 病毒，攻击 IBM 和其他公司生产的微型计算机及其兼容机的病毒，如巴基斯坦病毒。

（2）工作站的病毒。计算机硬件的飞速发展，使工作站的能力大大加强，并且应用范围也有了较大的发展，所以不难想象，攻击工作站的病毒是对信息系统的一大威胁。

（3）小型计算机的病毒。小型计算机的应用极为广泛，既可以作为网络中的节点机，又可以作为网络主机。1988 年，因特网受到了莫里斯蠕虫病毒攻击，改变了病毒只攻击

笔记

微型机的传统观念。如 WANK.com 和 HL.com 通过 VAX 型号的计算机传播。

（4）中、大型计算机的病毒。相对于攻击其他机型的病毒而言，攻击中、大型计算机的病毒很少。20 世纪 60 年代末，大型机 Univax 1108 系统上发现了一种可将自身链接于其他程序之后的病毒 Pervading Animal（流浪的野兽）病毒。

5. 按照计算机病毒的链接方式分类

（1）源码型病毒。该类病毒攻击用高级语言（如 C、Fortran、PASCAL 等）编写的程序。在编译用高级语言编写的程序之前，将病毒代码插入到源程序中，经编译成为合法程序的一部分。这类病毒一般存在于语言处理程序或链接（Link）程序中。第一例感染 C 语言和 PASCAL 语言源代码的病毒是 Srevir 病毒。

（2）嵌入型病毒，也称入侵型病毒。该类病毒将自身嵌入到已有程序中，把计算机病毒的主体程序与其攻击对象以插入方式链接，并代替其中部分不常用到的功能模块或堆栈区。

（3）外壳型计算机病毒。外壳型计算机病毒将自身包围在主程序的四周，对原来的程序不做修改。这种计算机病毒最为常见，易于编写，也易于发现，一般测试文件的大小即可知。

（4）操作系统型计算机病毒。这种计算机病毒用它自己的程序意图加入或取代部分操作系统进行工作，具有很强的破坏力，可以导致整个系统的瘫痪。“圆点”计算机病毒和“大麻”计算机病毒就是典型的操作系统型计算机病毒。

6. 按照计算机病毒激活的时间分类

按照计算机病毒激活的时间可分为定时的和随机的。定时病毒仅在某一特定时间才发作，而随机病毒一般不是由时钟来激活的。

7. 按照计算机病毒的传播媒介分类

按照计算机病毒的传播媒介来分类，可分为单机病毒和网络病毒。

（1）单机病毒 。单机病毒的载体是磁盘、光盘和 U 盘等可移动存储介质，常见的是病毒从 U 盘、光盘等传入硬盘，感染系统及已安装的软件或程序，然后再传染其他存储介质，继而传染其他系统。

（2）网络病毒。网络病毒的传播媒介不再是移动式载体，而是网络通道，这种病毒的传染能力更强，破坏力更大。

8. 按照计算机病毒特有的算法分类

（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，伴随体被优先执行，再由伴随体加载执行原来的 .EXE 文件。

（2）“蠕虫”型病毒。该型病毒把计算机网络地址作为感染目标，利用网络从一台计算机的内存传播到其他计算机的内存，将自身通过网络发送。病毒通过计算机网络传播，不改变文件和资料信息，除了内存，一般不占用其他资源。

（3）寄生型病毒。除了伴随型和“蠕虫”型，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）练习型病毒。病毒自身包含错误，不能进行很好的传播，例如，一些在调试阶段

的病毒。

（5）诡秘型病毒。诡秘型病毒一般不直接修改中断和扇区数据，而是通过设备技术或文件缓冲区等操作系统内部修改，不易看到资源，利用操作系统空闲的数据区进行工作。

（6）变形病毒，又称幽灵病毒。这一类病毒使用一种复杂的算法，一般由一段混有无关指令的解码算法和变化过的病毒体组成，使自己传播的每一份都具有不同的内容和长度。每一个中毒的文件中所含的病毒码都不一样，更有甚者，几乎无法找到相同的病毒特征码。对于扫描固定病毒特征码的防毒软件来说，无疑是一个严峻的考验。

笔记

9. 按照计算机病毒的破坏行为分类

计算机病毒的破坏行为体现了计算机病毒的杀伤能力。计算机病毒破坏行为的激烈程度取决于计算机病毒编制者的主观愿望和他所具有的技术。根据现有的计算机病毒资料可以把计算机病毒的破坏目标和攻击部位归纳如下。

（1）攻击系统数据区。计算机病毒的攻击部位包括硬盘主引导扇区、Boot 扇区、FAT 表和文件目录。一般来说，攻击系统数据区的计算机病毒是恶性计算机病毒，被它们攻击过的数据不易恢复。

（2）攻击文件。计算机病毒对文件的攻击方式很多，主要包括：丢失数据文件、替换内容、改名、删除、丢失部分程序代码、写入时间空白、变碎片、内容颠倒、假冒文件、丢失文件簇等。

（3）攻击内存。内存是计算机的重要资源，也是计算机病毒的攻击目标。计算机病毒攻击内存的方式主要有：占用大量内存、蚕食内存、禁止分配内存和改变内存总量等。

（4）干扰系统运行。计算机病毒会干扰系统的正常运行，以此作为自己的破坏行为。主要的破坏行为有：不执行命令、死机、打不开文件、干扰内部命令的执行、虚假报警、强制游戏、内部栈溢出、时钟倒转、换当前盘、重启动、占用特殊数据区和扰乱串并行口等。

（5）速度下降。计算机病毒激活时，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等。

（6）攻击磁盘。计算机病毒攻击磁盘包括攻击磁盘数据、不写盘、写操作变读操作和写盘时丢字节等。

（7）扰乱屏幕显示。计算机病毒扰乱屏幕显示的方式很多，主要包括：显示前一屏、环绕、倒置、字符跌落、吃字符、滚屏、抖动、乱写和光标下跌等。

（8）键盘。计算机病毒干扰键盘操作，主要的方式有：输入紊乱、抹掉缓存区字符、换字、封锁键盘、重复和响铃等。

（9）喇叭。很多计算机病毒在运行时，会使计算机的喇叭发出响声。有的计算机病毒编制者让计算机病毒演奏旋律优美的世界名曲，在高雅的曲调中去“杀戮”人们的信息财富。有的计算机病毒编制者则通过喇叭发出种种声音，用过的方式主要有：演奏曲子、警笛声、炸弹噪声、鸣叫、咔咔声和嘀嗒声等。

（10）攻击 CMOS。在计算机的 CMOS 区中，保存着系统的重要数据，例如，系统时钟、磁盘类型、内存容量等。有的计算机病毒激活时，能够对 CMOS 区进行写入动作，破坏系统 CMOS 中的数据，从而使计算机感染病毒。

（11）干扰打印机。这种类型一般有：假报警、间断性打印和更换字符等。

笔记

10. 按照计算机病毒的“作案”方式分类

计算机病毒的“作案”方式五花八门，按照危害程度的不同，可分为以下几种类型。

（1）暗藏型病毒：该病毒进入计算机后能够潜伏下来，到预定时间或特定事件发生时，再出来为非作歹。

（2）杀手型病毒：也叫暗杀型病毒，钻入机器后，专门用来篡改和毁伤某一个或某一组特定的文件、数据，不留任何痕迹。

（3）霸道型病毒：该病毒能够中断整个计算机的工作，迫使信息系统瘫痪。

（4）超载型病毒：该病毒进入计算机后能大量复制和繁殖，抢占内存和硬盘空间，使机器因超载而无法工作。

（5）间谍型病毒：该病毒能从计算机中寻找特定信息和数据，并将其发送到指定地点，借此窃取情报。

（6）强制隔离型病毒：该病毒主要用来破坏电脑网络系统的整体功能，使各个子系统与控制中心以及各子系统间相互隔离，进而造成整个系统肢解瘫痪。

（7）欺骗型病毒：该病毒能打入系统内部，对系统程序进行删改或给敌方系统注入假情报，造成其决策失误。

（8）干扰型病毒：该病毒通过对计算机系统或工作环境进行干扰和破坏，达到消耗系统资源、降低处理速度、干扰系统运行、破坏计算机各种文件和数据的目的，从而使其不能正常工作。

任务 1.3 病毒载荷

子任务 1.3.1 没有载荷

在计算机中存在这样一种病毒，它们不具有破坏性，不会破坏用户数据，也不会重新格式化硬盘，它们只有传播功能，比如 WM/Concept。这样的病毒可能携带一条永远也不会显示的信息，却把这条信息留给了那些渴望发现病毒的人（比如病毒研究人员）。最让反病毒工作者头痛的计算机病毒就是除了传播代码外，不包含任何其他信息的病毒。病毒研究者把这类病毒称为无载荷病毒（no payload）。虽然它们不具有破坏性，但是病毒的复制过程也会带来很多副作用。如果计算机病毒的代码中包含能够造成计算机崩溃的 bug，在某些情况下，他们也能造成数据丢失或者是用相关数据重写硬盘的某个区域。

子任务 1.3.2 偶然破坏型载荷

有些计算机病毒，比如 Stoned，在复制过程中可能会造成数据丢失。在病毒保存原启动扇区信息的时候，可能会重写一些重要的数据。比如，如果磁盘上有很多目录信息，Stoned 病毒就可能会重写其中的一部分，因为该病毒把原引导扇区保存在根目录（root directory）的尾部。如果用 DIR 命令列文件名，就会显示些垃圾数据而不是文件名。虽然磁盘上丢失的数据可以用磁盘编辑器来恢复，但对于多数用户来说，经历这样的事情以后，他们的数据就永远丢失了。病毒研究者称这类病毒为偶然破坏型载荷。

子任务 1.3.3 非破坏型载荷

笔记

非破坏型载荷可以在屏幕上显示动画或者消息，还可以用扬声器播放音乐，甚至可以说话。病毒中携带动画，最著名的应该是法国的病毒编制者 Spanka，病毒 IDEA 就是他的佳作。这个病毒可以显示好几个动画。

还有些蠕虫病毒会写诗，比如西班牙病毒编制者 sandman 编写的病毒 W95/Haiku。它在攻击过程中能连接到 206.132.185.167，并利用 get 命令下载一个 Windows Wav 文件。把这个文件存储为 C:\haiku.wav，然后播放这个文件。病毒 Haiku 证明了现在的复制代码不需要自己携带载荷，这样可以让病毒代码更短小一些。

子任务 1.3.4 低破坏型载荷

顾名思义，此类病毒的破坏性比较低。比如，病毒 W95/HPS 在初始化的时候检查日期，如果这一天是星期天就激活病毒程序，如果系统打开一个没有压缩的 bitmap 文件，病毒就把这个图像水平翻转。

病毒 W95/HPS 在它翻转过的图片的 ID 上做了标记，它在 bitmap 头的尾部加上 DEADBABEh，这样就可以避免再次翻转该图片，病毒就不会恢复图片原来的样子。有些 DOS 病毒能够临时翻转屏幕上显示的字符，与这些 DOS 病毒相比，病毒 W95/HPS 的破坏性要大一些。因为 Windows 系统中经常使用没有压缩的 bitmap 文件，病毒 HPS 能制造很多诡异的效果，你只有从镜子中观察这些图片才知道计算机在干些什么。

子任务 1.3.5 强破坏型载荷

强破坏型载荷的计算机病毒会故意破坏计算机上的数据，甚至破坏计算机硬件系统。它包括数据重写型病毒，数据欺骗，加密数据的病毒和破坏硬件。

（1）数据重写型病毒，它直接格式化硬盘驱动器或者重写硬盘上的数据。比如 Michelangelo 病毒。它并不重写整个磁盘的数据，而只是重写系统启动部分，因此，被这个病毒攻击后，系统中的数据还是可以恢复的。

（2）数据欺骗，这类病毒慢慢地修改数据，不会突然删除数据。这种类型的破坏是非常危险的，因为人们在发现病毒之前，已经把被破坏的数据写到备份系统中了。具有代表性的病毒有 Dark_Avenger.1800.A，即 Eddie，Eddie 这个名字的来源并不是存储在病毒体内的字符串，而是在磁盘各处随机写下的一些文本，但是避开了 FAT 表，这样就导致系统慢慢地死掉了。病毒故意不破坏 FAT 表，这样感染病毒的系统就不会那么快地崩溃，而且病毒就有更多的机会感染其他系统。病毒在随机选择的磁盘扇区上写入“Eddie lives...somewhere in time”。后来，可以通过检测到这样的文本来发现病毒，但是为时已晚，因为已经有太多的文件（包括数据库系统）中包含这样的文本了。

另一个数据欺骗型病毒的例子是 Ripper（它是由于 Jack 的 Ripper 得名的）。Ripper 随机选择一些磁盘扇区，交换该扇区上的两个单词，再把交换结果写回到磁盘。这是一种严重的破坏活动，少数情况下，这样的数据交换实际有助于计算机病毒的变异（因为病毒修改了自己的代码），尽管大多数情况下，二进制病毒会被这种随机的数据修改操作破坏，

笔记

但是理论上这样的破坏可能会产生一个新的病毒变种，而且反病毒软件用检测原来病毒的规则可能检测不到这个新的变种。

（3）加密数据的病毒，磁盘杀手（Disk Killer）病毒是第一个用加密方法攻击数据的病毒。它是引导区病毒，于 1989 年 6 月第一次在美国被发现。之后的几个月内，该病毒在欧洲广为流传。该病毒感染的系统启动 48 小时后，调用它的载荷显示一条信息，并用简单的 XOR 操作搅乱了硬盘上的数据内容，加密过程从分区表开始。结果，病毒导致系统不能启动。下面是被攻击系统的屏幕上显示的内容。

```
Disk Killer-Version 1.00 by COMPUTER OGRE 04/01/1989
Warning!!
Don’t turn off the power or remove the diskette while Disk Killer is Processing!
PROCESSING
```

在病毒完成加密操作后，它显示下面的信息。

```
Now you can turn off the power
I wish you luck!
```

该病毒加密的级别很低，用特殊的解密工具就能恢复磁盘上的数据。但是，该病毒的加密程序中存在一些错误，某种情况下，这些错误加大系统恢复的难度。

（4）破坏硬件，这其中最著名的应该是 20 世纪 90 年代的 W95/CIH 病毒，该病毒在内核模式下用 I/O 端口命令访问 Flash BIOS，这种端口操作命令在用户模式下也可以执行，但是这样做使人们比较容易采取保护措施阻止病毒的激活例程。

任务 1.4 病毒常见攻击行为

子任务 1.4.1 DoS 攻击

过去，有很多成功的 DoS（拒绝服务）攻击案例，有些攻击是由计算机蠕虫发起的，大部分攻击并不是针对某个特定组织的。然而，计算机蠕虫自我复制的数据就像洪水一样填满了整个网络，这种繁殖的副作用就发展成了 DoS 攻击。蠕虫 W32/Slammer 就是进行这种攻击。蠕虫本身并不大，但是它在网络上自动繁殖的行为非常具有攻击性和破坏性。在蠕虫爆发期间，像路由器这样的网络设备严重超载，结果导致互联网的通信状况严重恶化，在某些地域，网络丢包率高达 90%。在蠕虫爆发期间发一封电子邮件都很困难，因为全世界的网络系统都变得很慢。

Linux 系统上最有名的蠕虫可能是 Linux/Slapper。Slapper 构建了一个 P2P 的网络系统来执行 DDoS（分布式拒绝服务攻击）。它允许攻击者连接到一个被蠕虫感染的节点，然后通过一直发送命令控制所有受到感染并连接到该节点的“僵尸”系统（Zombie system）。每一个蠕虫的拷贝都携带了命令接口，攻击者可以通过这个接口执行各种拒绝服务攻击。最大的僵尸系统可能包含 20000 台计算机，它们时刻等待攻击者的攻击命令。

蠕虫还发展出很多其他类型的 DoS 攻击。比如针对 911 电话系统（911 是美国紧急服

务电话的号码）的攻击，通常都是由蠕虫的攻击程序发起的。工作在微软 WebTV 系统上的蠕虫 Neat，就能够发起这种攻击，该蠕虫简单地重新配置 WebTV 系统，让它拨打电话 911 而不是默认 ISP 的电话号码。

笔记

子任务 1.4.2 窃取数据：用病毒牟利

现在的攻击者开始利用计算机病毒牟利了。虽然专业的攻击者可以在入侵个人计算机系统后偷窃用户信用卡账号和其他有用的信息，但是，计算机蠕虫攻击可以在更短的时间内攻击更多的目标，从而获取更大的利益，同时又降低了被追踪到的可能性。

（1）网络钓鱼攻击，这种攻击方法等待用户自己暴露自己的信用卡号和密码。网络钓鱼攻击通常使用欺骗性的邮件和伪造的站点来欺骗收件人，使他们泄露自己的个人信息。W32/Mimail.I@mm 就是用于网络钓鱼攻击的例子，是一种相对有效的攻击。

（2）后门，计算机蠕虫常常携带后门。此类蠕虫中最有名的是 W32/HLLW.Qaz.A。该蠕虫最早于 2000 年 7 月在中国发现。QAZ 是一个伴生病毒，但它本身也在网上传播。此外，该病毒携带了一个后门，该后门允许远程用户通过 7597 端口连接并控制受害的计算机。QAZ 通过枚举保护措施很弱的 NetBIOS 共享区来企图发现要感染的计算机，在感染了远程计算机之后，用电子邮件将被感染计算机 IP 地址发送给攻击者。蠕虫中的后门程序等待攻击者的连接，这就允许黑客连接并控制受感染的计算机。根据对几个版本的源代码的分析，QAZ 很有可能成功进入了 Microsoft 的网络，攻破了一个不安全的家用计算机，通过该计算机进入公司内部的站点，并窃取大量有用信息。