第 5 章

计算机安全防护软件

随着计算机硬件的发展，计算机中存储程序和数据的量越来越大，而当用户通过 Internet 上网时，会受到外部一些程序（计算机病毒）的侵害，而造成无法正常运行、内容丢失、计算机设备（部件）损坏等。目前，造成计算机上述损坏的原因主要是病毒侵蚀、人为窃取、计算机电磁辐射，以及硬件损坏等。本章将围绕计算机安全防护的相关内容，对计算机安全常识以及一些常用的安全防护软件进行介绍。

本章主要内容：

- 网络安全与杀毒软件
- 防火墙软件
- 网络监控软件

5.1 网络安全与杀毒软件

一般来说，安全的系统会利用一些专门的安全特性来控制对信息的访问，只有经过适当授权的人，或者以这些人的名义进行的进程可以读、写、创建和删除这些信息。而杀毒软件，则可以帮助用户清除计算机中的病毒，达到保护计算机数据的目的。本节将详细介绍网络安全与杀毒方面的一些基础理论和常用软件。

5.1.1 网络安全概述

计算机网络安全是指通过各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性。所以，建立网络安全保护措施的目的是确保经过网络传输和交换的数据，不会发生增加、修改、丢失和泄露等。

一般来讲，网络安全威胁有以下 8 种。

1．破坏数据完整性

破坏数据完整性表示以非法手段获取对资源的使用权限，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加、修改数据，以干扰用户的正常使用。

2．信息泄露或丢失

信息泄露或丢失是指人们有意或无意地将敏感数据对外泄露或丢失，通常包括信息在传输中泄露或丢失、信息在存储介质中泄露或丢失以及通过建立隐蔽隧道等方法窃取敏感信息等。例如，黑客可以利用电磁漏洞或搭线窃听等方式窃取机密信息，或通过对信息流向、流量、通信频度和长度等参数的分析，推测出对自己有用的信息，如用户账户、密码等。

3．拒绝服务攻击

拒绝服务攻击是指不断地向网络服务系统或计算机系统进行干扰，以改变其正常的工作流程，执行无关程序使系统响应减慢甚至瘫痪，从而影响正常用户使用，甚至导致合法用户被排斥不能进入计算机网络系统或不能得到相应的服务。

4．陷门和特洛伊木马

陷门和特洛伊木马通常表示通过替换系统的合法程序，或者在合法程序里写入恶意代码以实现非授权进程，从而达到某种特定的目的。

5．利用网络散布病毒

利用网络散布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，影响计算机使用并能够自我复制的一组计算机指令或者程序代码。目前，计算机病毒已对计算机系统和计算机网络构成了严重的威胁。

6．混合威胁攻击

混合威胁是新型的安全攻击，它主要表现为一种病毒与黑客编制的程序相结合的新型蠕虫病毒，可以借助多种途径及技术潜入企业、政府、银行等网络系统。这些蠕虫病毒利用“缓存溢出”技术对其他网络服务器进行侵害传播，具有持续发作的特点。

7．间谍软件、广告程序和垃圾邮件攻击

近年来，在全球范围内最流行的攻击方式是钓鱼式攻击。它利用间谍软件、广告程序和垃圾邮件将用户引入恶意网站。这类网站看起来与正常网站没有区别，但通常犯罪分子会以升级账户信息为理由要求用户提供机密资料，从而盗取可用信息。

8．非授权访问

非授权访问是指没有预先经过同意就使用网络或计算机资源，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。

非授权访问有假冒、身份攻击、非法用户进入网络系统进行违规操作、合法用户以未授权方式操作等形式。

5.1.2 计算机病毒概述

计算机病毒并非生物学中的病毒，而是一种在用户不知情或未批准的情况下，在计算机中运行的、具有自我复制能力的有害计算机程序。计算机病毒是一种程序，一段可执行代码，它可以像生物病毒一样，具有自我繁殖、互相传染以及激活再生等生物病毒特征。

计算机病毒往往会感染计算机中正常运行的各种软件或存储数据的文档，从而达到破坏用户数据的目的。

1．计算机病毒的历史

早在 20 世纪 60 年代，美国麻省理工学院的一些研究人员就开始在业余时间编写一些简单的游戏程序，可以消除他人计算机中的数据。这样的程序目前被某些人认定为计算机病毒的雏形。

随着 20 世纪 70 年代和 80 年代计算机在美国和西方发达国家的普及，逐渐出现了各种以恶作剧或纯恶意破坏他人计算机数据的病毒程序。由于当时互联网并不发达，因此传播计算机病毒的载体通常是各种软盘等可移动存储设备。

20 世纪 90 年代开始，互联网普及到了千家万户，在给人们带来便捷的同时也为计算机病毒的传播提供了通道。目前，互联网已成为最主要的病毒传播途径。

早期的病毒大多只能破坏用户计算机中的各种软件。1998 年 9 月被发现的 CIH 病毒被广泛认为是第一种可以破坏计算机硬件固件（一种控制硬件运行的软件，通常被固化到硬件的闪存中，如主板的 BIOS 等）的计算机病毒，因此造成了很大的破坏。

2．计算机病毒的特征

由于计算机病毒对计算机和互联网的破坏性很大，因此，我国在《中华人民共和国计算机信息系统安全保护条例》中明确给出了关于计算机病毒的法律定义，即“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’”。目前，公认的计算机病毒往往包括以下全部特征或部分特征。

- **传播性**　多数计算机病毒都会利用计算机的各种漏洞，通过局域网、互联网、可移动磁盘等方式传播，手段十分丰富，令用户防不胜防。例如，曾经流行一段时间的爱虫病毒，就是通过一封标题为“I Love You”的电子邮件传播的。
- **隐蔽性**　相比普通的软件程序，计算机病毒体积十分小，往往不超过 1KB。在病毒传播给用户之前，往往会将自己与一些正常的文件捆绑合并在一起。在感染了用户之后，病毒就会将自己隐藏到系统中一些不起眼的文件夹中，或将名称修改为类似系统文件的名称，防止用户手工将其找出。例如，曾经流行的病毒“欢乐时光”，就是将病毒代码隐藏在网页中。

- **感染性** 大部分计算机病毒都具有感染性。例如，将病毒的代码感染到本地计算机的各种可执行文件（EXE、BAT、SCR、COM 等）和网页文档（HTML、HTM）、Word（DOC、DOCX）文档等文件中。这样，一旦用户执行了这个文件，就会感染病毒。例如，几年前流行的“熊猫烧香”（又名武汉男生）病毒，就具备很强的感染性，可以向本地计算机中所有的可执行程序内添加病毒代码。
- **潜伏性** 大部分破坏力较小的病毒通常自感染以后就开始不断地破坏本地计算机的软件。而少部分破坏力比较强的病毒则是具有潜伏期的病毒，只有达到指定的条件才会爆发，大部分时间都是无害的。例如 Conficker 病毒，在不被激活的情况下只是利用电子邮件软件进行传播，只有在被激活的条件下，才会向互联网中的服务器发起攻击。
- **可激发性** 一些有潜伏性的病毒往往会在指定的日期被激发，然后开始破坏工作。例如，CIH 病毒的 1.2 和 1.3 版本，只有在 Windows 94、Windows 98、Windows ME 等操作系统下的每年 4 月 26 日爆发。
- **表现性** 一些病毒在设计方面可能有缺陷，或者病毒设计者故意将病毒运行设计为死循环。然后，当计算机被病毒感染时会表现出一定的特征，例如系统运行缓慢、CPU 占用率过高、容易使用户计算机死机或蓝屏等。这些表现性往往会破坏病毒的隐蔽性。
- **破坏性** 除了少数恶作剧式的病毒以外，大多数病毒对计算机都是有危害的，例如破坏用户的数据，删除系统文件，甚至删除磁盘分区等。

3．计算机病毒的分类

计算机病毒大体上可以根据其破坏的方式进行分类。常见的计算机病毒主要包括以下几种类型。

- **文件型病毒**

文件型病毒是互联网普及之前比较常见的病毒，也是对无网络计算机破坏性最大的病毒。其设计的根本目的就是破坏计算机中的各种数据，包括可执行程序、文档、硬件的固件等。著名的 CIH 病毒就是典型的文件型病毒。

随着互联网的不断发展，目前大多数新的病毒都已发展到利用操作系统的漏洞，通过互联网传播，因此文件型病毒已很少见。

- **宏病毒**

宏病毒与文件型病毒不同，其感染的目标不是可执行程序，而是用微软公司 Office 系列办公软件所制作的文档。在微软公司的 Office 系列办公软件中，允许用户使用 VBA 脚本编写一些命令，实现录制的动作，提高工作效率。宏病毒正是使用 VBA 脚本代码编写的批处理宏命令，在用户打开带有宏病毒的文件时进行传染。第一种宏病毒是 Word concept 病毒，据说诞生于 1995 年。随着 Office 系列软件的不断完善，以及用户警惕意识不断提高，目前宏病毒已经十分罕见。

- **木马/僵尸网络类病毒**

事实上，木马是一种远程监控软件，通常分为服务端和客户端两个部分。其中，服务端木马会被安装到被监控的用户的计算机中，而客户端木马则由监控者使用。

木马传播者通常会以一些欺骗性的手段诱使用户安装木马的服务端，然后，用户的计算机就成为一台“肉鸡”（类似随时会被宰杀的肉鸡）或者“僵尸”（无意识地被他人控制），完全由木马传播者控制。

现代的木马传播者往往通过互联网感染大批的“肉鸡”或“僵尸”，形成一个僵尸网络，以进行大面积的破坏，例如几年前大规模爆发的灰鸽子和熊猫烧香等。

❑ 蠕虫/拒绝服务类病毒

蠕虫病毒是利用计算机操作系统的漏洞或电子邮件等传输工具，在局域网或互联网中进行大量复制，以占用本地计算机资源或网络资源的一种病毒，其以类似于昆虫繁殖的特性而闻名。除 CIH 病毒以外，大部分全球爆发的病毒都是蠕虫病毒。蠕虫病毒也是造成经济损失最高的一种病毒。

目前，已经在全世界范围内爆发过的蠕虫病毒包括著名的莫里斯蠕虫（1988 年 11 月 2 日）、梅丽莎病毒（1999 年 3 月 26 日）、爱虫病毒（2000 年 5 月）、冲击波病毒（2003 年 8 月 12 日）、振荡波病毒（2004 年 5 月 1 日）、熊猫烧香（2007 年 1 月初）等。

4．防治计算机病毒的方法

计算机病毒作为一种破坏性的软件程序，不断地给计算机用户造成大量的损失。养成良好的计算机使用习惯，有助于避免计算机病毒感染。即使感染了计算机病毒，也可以尽量降低损失。

❑ 定时备份数据

在使用计算机进行工作和娱乐时，应该定时对操作系统中的重要数据进行备份。互联网技术的发展为人们提供了新的备份介质，包括电子邮箱、网络硬盘等。对于一些重要的数据，可以将其备份到加密的网络空间中，设置强壮的密码，以保障安全。

❑ 修补软件漏洞

目前，大多数计算机病毒都是利用操作系统或一些软件的漏洞进行传播和破坏的。因此，应定时更新操作系统以及一些重要的软件（如 Internet Explorer、FireFox 等网页浏览器、Windows Media Player、QQ 等常用的软件），防止病毒通过这些软件的漏洞进行破坏。

另外，如果使用的是 Windows 2000、Windows XP 等操作系统，还应该为操作系统设置一个强壮的密码，关闭默认共享、自动播放、远程协助和计划任务，防止病毒利用这些途径传播。

❑ 安装杀毒软件

对于大多数计算机用户而言，手动杀毒和防毒都是不现实的。在使用计算机时，应该安装有效而可靠的杀毒软件，定时查杀病毒。在挑选杀毒软件时，可以选择一些国际著名的大品牌，例如 BitDefender、卡巴斯基等。

❑ 养成良好习惯

防止计算机病毒，最根本的方式还是养成良好的使用计算机的习惯。例如，不使用盗版和来源不明的软件、在使用 QQ 或 Windows Live 时不单击来源不明的超链接，不被一些带有诱惑性的图片或超链接引诱而浏览这些网站，接收邮件时只接收文本、未杀毒前不打开附件等。

杀毒软件毕竟有其局限性，只能杀除已收录到病毒库中的病毒。对于未收录的病毒往往无能为力。有时，也会造成误杀。良好的操作习惯才是防止病毒传播、蔓延的根本解决办法。

5.1.3 恶意软件概述

恶意软件，又被称作灰色软件、流氓软件，用来泛指一些不被认为是计算机病毒，但往往违背用户意愿或者隐蔽地安装、对计算机造成负面影响的软件。恶意软件其本身可能是一种病毒、蠕虫、后门或漏洞攻击脚本，它通过动态地址改变攻击代码可以逃避入侵检测系统的特征检测。在国内，相比计算机病毒，恶意软件的流传范围更广，且更加隐蔽。

1．恶意软件的特点

由于恶意软件的危害比病毒要小一些，其危险性往往得不到用户的重视，因此造成了国内恶意软件的流行。与正常使用的软件相比，恶意软件具有如下特征。

- **强制/隐蔽安装** 指在未明确向用户提示或未经用户许可的情况下，在用户计算机上安装并且运行的行为。有些恶意软件虽然提供给用户不安装的选项，但往往将其置于极不明显的位置，使用户很难发现。这样的行为被业内称作“擦边球”。
- **难以卸载和删除** 指不提供给用户关闭、卸载和删除的方式，即使用户停止软件进程并手动删除软件的文件，软件仍然可以运行。有些恶意软件虽然提供了卸载的方式，但卸载后事实上仍然在用户计算机中存在并运行。
- **恶意捆绑** 指在软件中捆绑已被认定为恶意软件的行为。一些恶意软件往往会同时捆绑多个恶意软件。一旦安装其中一个，其他的都会一起安装。
- **浏览器劫持** 指未经用户许可，修改用户浏览器或其他相关设置（包括浏览器主页、默认搜索引擎、右键菜单等），迫使用户访问指定的网站或导致用户无法上网等的行为。
- **广告弹出** 指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和其他数字设备上的软件，弹出广告的行为。
- **恶意收集用户信息** 指未明确提示用户或未经用户许可的情况下，恶意收集用户手机号、电子邮箱等信息的行为。
- **恶意卸载** 指未明确提示用户或未经用户许可的情况下，以欺骗、诱导、误导的方式卸载用户计算机中正常软件的行为。

2．恶意软件的分类

大多数恶意软件都是以盈利为目的的，或盗取用户的隐私习惯，或强制用户浏览广告，或通过其他方式为软件开发商谋取利益。对于笼统的防病毒讨论，可以将恶意软件分为如下 3 类。

- **特洛伊木马**

特洛伊程序又称为特洛伊木马，表面看上去有用或无害，但却包含了旨在利用或损

坏运行该程序携带的隐藏代码。特洛伊木马没有复制能力，它一般伪装成一个实用工具或游戏，又或者通过没有正确说明此程序的用途和功能的电子邮件传递给用户，诱使用户进行安装进而获取计算机信息。特洛伊木马通过在其运行时传递恶意负载或任务达到此目的，例如迫使计算机速度变慢、莫名死机，或窃取用户信息，导致数据外泄等。

❑ 蠕虫

蠕虫是一种常见的计算机病毒，它利用网络进行复制和传播，其传播方式包括通过操作系统漏洞传播、通过电子邮件传播、通过网络攻击传播、通过移动设备传播以及通过即时通信等社交网络传播。

蠕虫使用自行传播的恶意代码，它可以通过网络连接自动将其自身从一台计算机分发到另外一台计算机上。蠕虫会执行有害操作，例如消耗网络或本地系统资源，这样可能会导致拒绝服务攻击。某些蠕虫无须用户干预即可执行和传播，而其他蠕虫则需用户直接执行蠕虫代码才能传播。除了复制，蠕虫也可能传递负载。

❑ 病毒

病毒是编制者在计算机程序中插入破坏计算机功能或数据的一种代码，其明确意图就是自行复制。病毒尝试将其自身附加到宿主程序，以便在计算机之间进行传播。它可能会损害硬件、软件或数据。宿主程序执行时，病毒代码也随之运行，并会感染新的宿主，有时还会传递额外负载。

3．恶意软件的安装渠道

在国内，恶意软件的流行程度不亚于病毒，而且大多数恶意软件都会影响用户对计算机的使用。大多数杀毒软件迫于法律原因，往往无法直接杀除恶意软件，因此避免安装恶意软件一直为网民所关注。恶意软件的安装渠道主要包括 3 种。

❑ 浏览器的 Active 控件

一些网站会自动将恶意软件作为网站的 Active 控件添加到网页中，一旦用户使用较老版本的网页浏览器浏览这些网页时，就会自动安装这些恶意软件。防止这些插件安装的方法是安装较新版本的网页浏览器，如 IE 8.0 等。

❑ 共享/免费软件绑定的插件

一些共享/免费软件为了收回软件开发成本，也会以绑定的方式将插件放到软件安装中。绑定分为隐性绑定和显性绑定两种。

隐性绑定往往不对用户进行提示，也不提供选择安装插件的选项，或将选项隐藏较深，很难让用户发现；显性绑定则是为用户提供选择，允许用户不安装。隐性绑定目前让用户很反感，而显性绑定则通常被认为是可以理解的行为。

目前，一些大的软件下载网站都会在软件介绍中提供软件的插件绑定情况，例如提示某软件无插件或有插件，以及可选插件等，帮助用户鉴别。

❑ 不良网站的欺骗/诱导性下载

一些不良网站往往会以欺骗性或诱导性的语言，诱使用户下载恶意软件。常见的方法包括，将用户要下载的软件隐藏在一大堆插件下载地址中，将插件的下载地址修改为某些正常的软件名称等，以及一些欺骗性的语言，例如“您的计算机已中病毒”“激情影视下载”“免费好用的网络电话”“您的浏览器版本过低”等。

5.1.4 常用网络安全软件

网络安全软件拥有查杀木马、清理插件、修复漏洞、电脑体检、保护隐私等多种功能。它依靠抢先侦测和云端鉴别，可全面、智能地拦截各类木马，保护用户的账号、隐私等重要信息。而计算机杀毒软件是用于清除计算机病毒、特洛伊木马和恶意软件的软件。多数计算机杀毒软件都具备监控识别、病毒扫描、清除和自动升级等功能。

1．金山卫士

《金山卫士》软件是当前查杀木马能力最强、检测漏洞最快、体积最小巧的免费安全软件之一。它采用双引擎技术，云引擎能查杀上亿已知木马，独有的本地 V10 引擎可全面清除感染型木马；漏洞检测针对 Windows 优化；更有实时保护、软件管理、插件清理、修复 IE、启动项管理等功能，全面保护系统安全，如图 5-1 所示。

图 5-1 【金山卫士】窗口

❑ 性能体检与网络测速

在【金山卫士】窗口中，用户可以单击右下角的【性能体检】按钮。此时，弹出一个提示框，并显示性能体检模块更新进度。性能模块更新完成后，则弹出【金山卫士性能体检】对话框，并检测计算机启动内容、网络带宽、系统文件等，如图 5-2 所示。

图 5-2 更新与体检

提　示

【金山卫士】窗口右下角的功能按钮，可以通过单击【编辑】按钮，来删除或更换功能按钮。

在体检过程中，做一些基本系统模块的检测后，将弹出一个【显卡游戏性能测试】窗口，并运行一些三维立体空间图形，如图 5-3 所示。

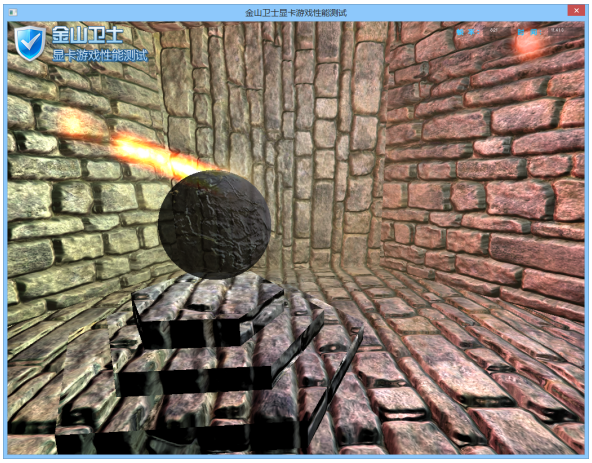

图 5-3　三维立体测试

当所有测试完成后，则弹出【金山卫士性能体检】对话框，并显示【开机性能】【系统性能】和【网络性能】的测试结果，如图 5-4 所示。

用户也可以对计算机进行单独的网络带宽测试。如在【金山卫士】窗口中，单击右下角的【网络测速】按钮，则可以在弹出的提示框中显示模块更新情况，如图 5-5 所示。

图 5-4　测试结果

图 5-5　准备测试网速

当网络测速模块更新完成后，即可弹出【金山卫士网络测速】对话框，单击【开始测速】按钮，即可检测网络带宽，如图 5-6 所示。

图 5-6　网络速度测试结果

❑ 系统优化

在【金山卫士】窗口中，系统优化包含有【一键优化】【开机时间】【开机加速】和【优化历史】等多项设置。当单击【系统优化】按钮后，该软件将自动检测系统中可以优化的软件，如图 5-7 所示。

图 5–7 系统优化

然后，单击【立即优化】按钮，即可对检测出的内容进行优化操作。优化完成后显示优化的结果，如“本次成功优化了 1 项，您的电脑变快了，立即上网体验吧”等信息，如图 5-8 所示。

图 5–8 显示优化结果

当用户选择【开机加速】选项卡时，将显示开机时一些启动项内容。而在该选项卡中，用户可以设置开机时软件、服务的【已启用】或者【已禁用】设置，如图 5-9 所示。

提　示

《金山卫士》软件除了在主窗口中所显示的常用功能外，其他的独立功能都包含于【百宝箱】功能中，包含有换肤工具、实时保护、桌面助手、硬件检测等 30 种功能。

图 5-9 设置开机软件

2. 瑞星杀毒软件

《瑞星杀毒软件》（Rising Antivirus，RAV）采用获得欧盟及我国专利的 6 项核心技术，形成全新软件内核代码。《瑞星杀毒软件》拥有国内最大的木马病毒库，采用“木马病毒强杀”技术，结合“病毒 DNA 识别”“主动防御”“恶意行为检测”等大量核心技术，可彻底查杀 70 万种木马病毒。

2011 年 3 月 18 日，国内最大的信息安全厂商瑞星公司宣布，《瑞星杀毒软件》永久免费。运行瑞星杀毒软件，将显示其主界面，如图 5-10 所示。

图 5-10 《瑞星杀毒软件》主界面

❑ 杀毒操作

在窗口中，可以单击【病毒查杀】按钮，此时，在展开的界面中，选择【快速查杀】选项，显示查杀病毒的地址、扫描对象个数、显示进度等信息，如图 5-11 所示。

图 5-11 开始查杀病毒

提 示

在查杀病毒过程中，用户还可以单击标题名称后面的【转入后台】按钮，即缩小至【任务栏】的【通知区】。

等待病毒查杀完成后，将显示查杀结果。在结果中显示共扫描对象数、所耗时间，还有在下面的【病毒】选项卡中，将显示病毒的情况，如图 5-12 所示。如果检测显示存在病毒，单击【立即处理】按钮，可处理所发现的威胁。

图 5-12 显示查杀结果

❑ 计算机防护和瑞星工具

瑞星防护提供了对文件、邮件、网页、木马等内容的监视和保护作用。例如，在【电脑防护】选项卡中，用户可以随时开启或关闭相应的监控，如图 5-13 所示。

图 5-13 开启或关闭相应的监控

激活【安全工具】选项卡，可以查看该软件所携带的一些常用工具，以及对工具所进行的设置，如图 5-14 所示。

图 5-14 《瑞星杀毒软件》中的常用工具

3. 木马克星

随着个人计算机的广泛普及和宽带网络的高速发展，越来越多的网络安全隐患出现

在用户面前。而木马以其强大的远程控制和私密信息窃取能力，逐渐受到黑客们的青睐，成为网络犯罪的主要工具。针对木马对计算机用户的威胁，高查杀率、低系统资源占用、功能强大的木马专杀软件——《木马克星》应运而生。

《木马克星》是一款适合网络用户的安全软件，既有面向新手的内存扫描和硬盘扫描等低端应用，也有面向高手的众多调试查看等中高端应用。下面具体介绍该工具软件。

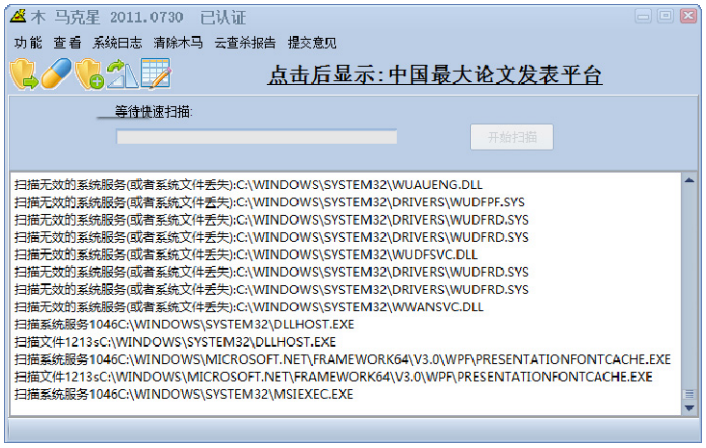

图 5-15 自动扫描内存

❑ 扫描内存

当启动《木马克星》工具软件之后，软件将自动进入内存的扫描页面，并自动查杀内存中的木马，而不需要用户手动操作，如图 5-15 所示。

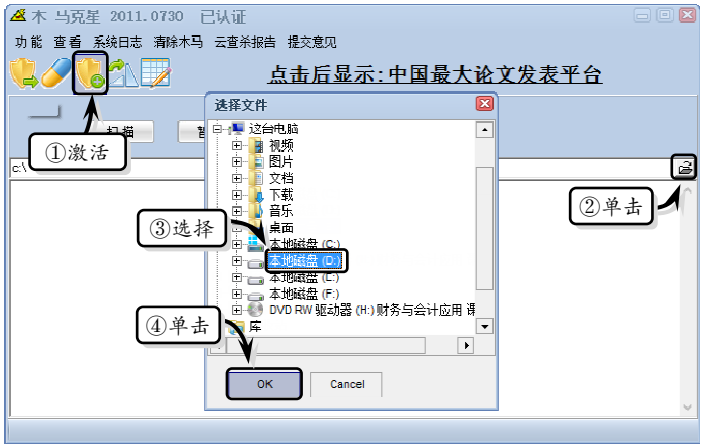

图 5-16 选择扫描位置

提　示

用户也可以单击【刷新】按钮、【扫描内存】按钮，或者单击【功能】菜单，执行【扫描内存】命令，使木马克星对系统进行再次扫描。

❑ 扫描硬盘

激活【扫描硬盘】选项卡，单击【浏览】按钮，在弹出的【选择文件】对话框中，选择要扫描的磁盘，单击 OK 按钮，如图 5-16 所示。

单击【扫描】按钮，即可开始扫描操作。当扫描完成之后，用户可以在该窗口中查看扫描结果，如图 5-17 所示。

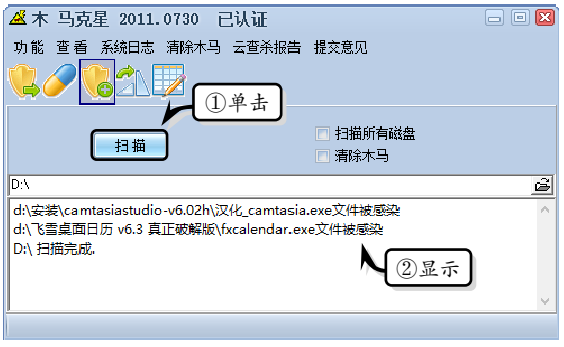

图 5-17 查看扫描结果

提　示

在【扫描硬盘】窗口中，启用【扫描所有磁盘】复选框，即可扫描计算机中所有的磁盘；若启用【清除木马】复选框，则可以在扫描过程中直接将扫描到的木马清除。

❑ 系统设置

在使用木马克星扫描木马之前，用户可以对其进行相应设置，以便用户根据需要进行不同的扫描操作。在【木马克星】窗口中，执行【功能】|【设置】命令，在弹出的对话框中，选择不同的选项卡，可以进行不同效果的设置，如图 5-18 所示。

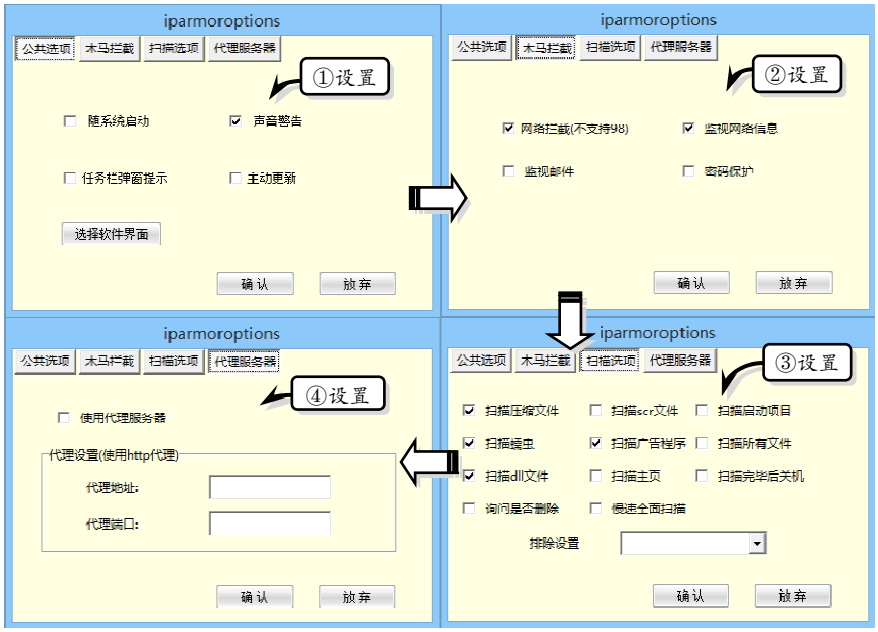

图 5-18 系统设置

❑ 更新病毒库

为了更好地查杀最新的木马程序，在使用《木马克星》软件时，用户需要及时对程序进行更新。执行【功能】|【更新病毒库】命令，在相应的窗口中单击【开始】按钮，即可开始对病毒库进行更新，如图 5-19 所示。如果当前病毒库已经是最新版本，则将弹出含有“已经是最新版本，不需要升级”的提示信息。

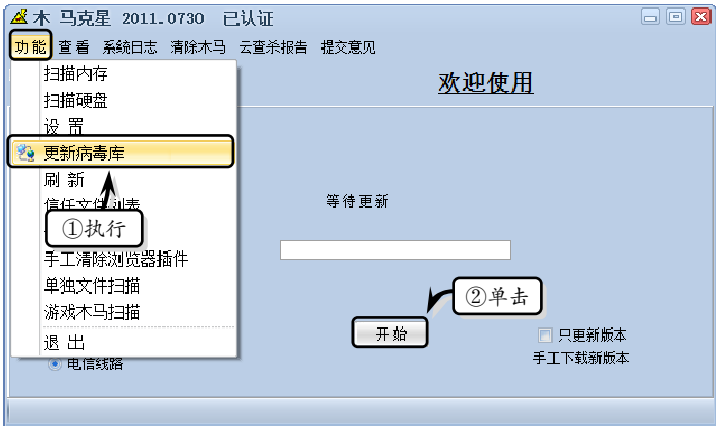

图 5-19 更新病毒库

5.1.5 练习：使用《360 安全卫士》维护计算机安全

《360 安全卫士》是当前功能最强、效果最好、最受用户欢迎的上网必备安全软件之一，具备木马查杀、恶意软件清理、漏洞补丁修复、电脑全面体检等多种功能。在本练

习中，将详细介绍使用《360 安全卫士》软件维护计算机安全的操作方法和步骤。

操作步骤：

1 查杀流行木马。运行《360 安全卫士》软件，在主界面中选择【查杀修复】选项，快速扫描木马，在弹出的对话框中，单击【立即扫描】按钮，快速扫描计算机中的木马和危险项，如图 5-20 所示。

图 5-20 快速扫描木马

2 快速扫描后，在弹出的窗口中将会显示发现的木马扫描等结果。单击【一键处理】按钮，清除所发现的木马和所有的危险项，如图 5-21 所示。

3 软件管理。在主界面中选择【软件管家】选项，弹出【360 软件管家】窗口，如图 5-22 所示。

图 5-21 清除木马

图 5-22 【360 软件管家】窗口

4 在界面左侧的列表框中选择【安全杀毒】选项，在右侧的列表框中单击【江民杀毒软件】后面的【下载】按钮，如图 5-23 所示。

5 激活【卸载】选项卡，在列表框中单击软件后面的【卸载】按钮，即可卸载该软件，如图 5-24 所示。

图 5-23 选择下载软件

图 5-24 卸载软件

6 在《360 安全卫士》软件的窗口中，激活【电脑清理】选项卡，单击【一键扫描】按钮，扫描计算机中的垃圾、痕迹、注册表和插件等，如图 5–25 所示。

图 5–25 计算机清理

7 扫描结束后，将显示扫描出来的垃圾文件。此时，单击【一键清理】按钮，即可清理计算机中的垃圾文件，如图 5–26 所示。

图 5–26 清理计算机中的垃圾文件

5.2 防火墙软件

防火墙软件又叫软件防火墙，也可以称为软防火墙。单独使用软件系统来完成防火墙功能，将软件部署在系统主机上，其安全性较硬件防火墙差，同时占用系统资源，在一定程度上影响系统性能。

5.2.1 防火墙概述

防火墙又称防护墙，是指设置在不同网络（如可信任的企业内部网和不可信的公共网）或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的唯一出入口，能根据企业的安全政策控制（允许、拒绝、监测）出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务，实现网络和信息安全的基础设施。

在逻辑上，防火墙是一个分离器，一个限制器，也是一个分析器，可有效地监控内部网和 Internet 之间的任何活动，保证内部网络的安全。

1．防火墙的类型

古代的人们在房屋之间修建一道墙，这道墙可以防止火灾发生的时候蔓延到别的房屋，因此被称为“防火墙”。而现在，人们将防火墙应用于网络，其含意为“隔离在内部网络与外部网络之间的一道防御系统”。现代防火墙的主要类型可分为网络层防火墙、应用层防火墙、数据库防火墙等。

❑ 网络层防火墙

网络层防火墙可以被看成一种 IP 封包过滤器，它运作在底层的 TCP/IP 堆栈上。用户可以通过一些规则设置，只允许符合特定规则的封包通过，其余的一概禁止穿越防火墙（病毒除外，防火墙不能防止病毒侵入）。另外，操作系统及网络设备大多已内置防火墙功能，可以另一种较宽松的角度来制定防火墙规则，只要封包不符合任何一项“否定规则”就予以放行。

较新的防火墙能利用封包的来源 IP 地址、来源端口号、目的 IP 地址或端口号、服务类型（如 HTTP 或是 FTP）等多样属性进行过滤，也能经由通信协议、TTL 值、来源的网域名称或网段等属性进行过滤。

❑ 应用层防火墙

应用层防火墙是在 TCP/IP 堆栈的“应用层”上运作。通常，用户使用浏览器时所产生的数据流或是使用 FTP 时的数据流都属于这一层。应用层防火墙可以拦截进出某应用程序的所有封包，并且封锁其他的封包。理论上，这一类防火墙可以完全阻绝外部的数据流进到受保护的计算机中。

❑ 数据库防火墙

数据库防火墙是一款基于数据库协议分析与控制技术的数据库安全防护系统，通过 SQL 协议分析，根据预定义的禁止和许可策略让合法的 SQL 操作通过，阻断非法违规操作，形成数据库的外围防御圈，实现 SQL 危险操作的主动预防、实时审计。另外，数据库防火墙面对来自外部的入侵行为，提供 SQL 注入禁止和数据库虚拟补丁包功能。

2．防火墙的优点

应该说，在互联网上防火墙是一种非常有效的网络安全模型，通过它可以隔离风险

区域（即 Internet 或有一定风险的网络）与安全区域（局域网）的连接，同时不会妨碍人们对风险区域的访问。防火墙的作用是防止未授权的通信进出被保护的网络，使单位强化自己的网络安全政策。

防火墙是加强网络安全的一种有效手段。它具有以下优点。

- **强化安全策略** 因为 Internet 上每天都有上百万人在那里收集信息、交换信息，不可避免地会出现个别非法用户。防火墙是为了防止不良现象发生的“交通警察”，执行站点的安全策略，仅允许合法用户或者符合规则的请求通过。
- **有效地记录 Internet 上的活动** 因为所有进出信息都必须通过防火墙，所以非常适用收集关于系统和网络使用与误用的信息。防火墙像门卫一样，记录外部网络进入内部网络，或者内部网络访问外部网络的信息。
- **限制暴露用户** 防火墙能够用来隔开网络中的一个网段与另一个网段。这样，能够防止影响一个网段的问题通过整个网络传播。
- **核准合法信息** 所有进出内部网络的信息都必须通过防火墙，所以防火墙便成为安全问题的检查点，使可疑的访问被拒绝于门外。

5.2.2 常用防火墙软件

对于一些保存了重要资料的计算机来讲，防火墙软件是必装的工具软件之一。通过防火墙软件，不仅可以有效地监控内部网和 Internet 之间的任何活动，而且还可以保证内部网络的安全。在本节中，将详细介绍一些常用的防火墙软件，如 COMODO 防火墙、360 网络防火墙、天网防火墙等。

1．COMODO 防火墙

COMODO Firewall 是一款功能强大的、高效的且易于操作的软件。它提供了针对网络和个人用户的最高级别的保护，从而阻挡黑客侵入计算机，避免造成资料泄露；提供程序访问网络权限的控制能力，抵制网络窃取，实时监控数据流量，可以在发生网络窃取或者攻击时迅速做出反应。

运行 COMODO Firewall，进入主界面窗口，在该窗口中分别包含防火墙内容、自动沙盒、入侵设置等内容，如图 5-27 所示。

图 5-27 COMODO Firewall 主界面

❑ 设置防火墙

初次安装COMODO Firewall后，系统会自动扫描计算机。当扫描计算机并处理相关危险之后，该软件会自动显示默认的防护模式。例如，防火墙为默认的“安全模式”，而自动沙盒则为默认的“禁止”模式。此时，用户可以通过单击【防火墙】选项右侧的【安全模式】选项，在其列表框中选择相应的模式，即可更改防火墙的使用模式，如图 5-28 所示。

图 5-28 设置防火墙模式

提 示

在主界面中，默认整体模式为【安全的】模式，可通过单击【游戏模式】按钮，来切换软件的整体模式。

除此之外，还可以在界面中直接选择【防火墙】选项，在弹出的【高级设置】对话框中，设置防火墙的基本设置，包括开启流量过滤、警告设置及一些防火墙的高级设置，如图 5-29 所示。

图 5-29 设置防火墙设置

提 示

在【高级设置】对话框中的【防火墙】选项卡中，除了可以设置防火墙设置之外，还可以设置应用程序规则、端口、全局规则、网络区域等。

❑ 扫描计算机

当计算机运行一段时间之后，需要运用该软件扫描计算机中的危险项。此时，可单击主界面底部的【扫描】按钮，在弹出的对话框中对计算机进行全面的评价扫描。在该对话框中，可通过单击【行为】后的下拉按钮，在其下拉列表中设置扫描后的操作行为，如图 5-30 所示。

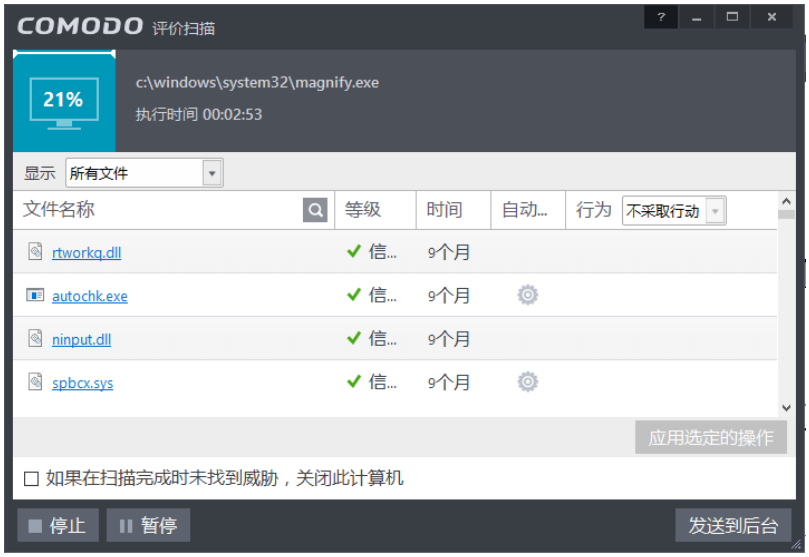

图 5-30 扫描计算机

扫描结束后，会在界面的最上方显示扫描结果，包括受信任的文件、无法识别的文件、恶意文件、正在运行的文件、自动运行的文件等内容，如图 5-31 所示。

图 5-31 显示扫描结果

❑ 查看日志

在主界面中，单击【任务】图标，在展开的列表中选择【常规任务】选项卡。同时，选择【查看日志】选项，在弹出的对话框中，查看防护日志，如图 5-32 所示。

提　示

用户还可以选择【高级任务】选项卡，在其列表中通过选择相应的选项，进行创建应急磁盘、清理系统、观察活动等高级任务的操作。

❑ 设置网络控制规则

在主界面中选择【防火墙】选项，在弹出的【高级设置】对话框中，选择【全局规则】选项。在该选项卡中用户可以查看当前的一些防护规则，单击底部的展开按钮，可以选择某项规则，对其进行编辑、移除、上移或下移等操作，如图 5-33 所示。

图 5-32 查看防护日志

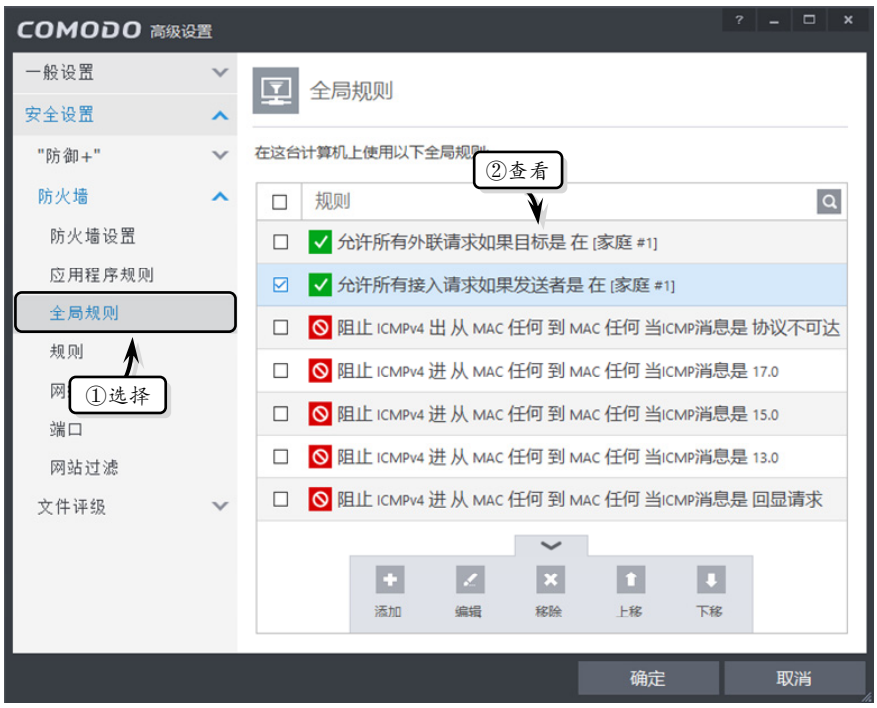

图 5-33 查看全局规则

除此之外，还可以单击底部的【添加】按钮，在弹出的【防火墙规则】对话框中，添加新的规则，如图 5-34 所示。

图 5-34 添加防火墙规则

在【防火墙规则】对话框中，用户可以设置参数的内容，如表 5-1 所示。

表 5-1 网络控制规则参数设置

操作名称	参　数
行为	在该下拉列表中，可以设置允许/阻止操作，启用【如果触发了规则将在防火墙日志中记录】复选框，表示如添加并使用了该规则后将被记录到防火墙日志中
协议	在该下拉列表中，包含有 TCP、UDP、TCP 或 UDP、ICMP 和 IP
方向	用户可以选择协议的方向，包括【出】【入】和【入或出】
源地址	在该选项卡中，可以设置排除任意地址、主机名、物理地址、网络区域、IPv4 地址范围、IPv4、单个地址、IPv4 子网掩码、IPv6 单个地址、IPv6 子网掩码中的任意一项
目的地址	在该选项卡中，可以设置排除任意地址、主机名、物理地址、网络区域、IPv4 地址范围、IPv4、单个地址、IPv4 子网掩码、IPv6 单个地址、IPv6 子网掩码中的任意一项
源端口	在该选项卡中，可以设置排除为任何、端口范围、一系列端口、单个端口中的任意一项
目的端口	在该选项卡中，可以设置排除为任何、端口范围、一系列端口、单个端口中的任意一项

2．瑞星防火墙

《瑞星防火墙软件》是一款永久免费的防火墙软件，具有保护网络安全、免受黑客攻击、有效拦截恶意钓鱼网站、保护个人隐私信息、网上银行账号密码和网络支付账号密码安全等功能，为用户提供智能化的上网安全保护策略。

运行该软件，在【首页】选项卡中，将自动显示检测后本地计算机的安全级别。用户只需单击【立即修复】按钮，在弹出的【安全检查-修复】对话框中，单击【立即修复】按钮，即可快速修复软件所检测到的危险项目，如图 5-35 所示。

提　示

在【安全检查-修复】对话框中，单击【立即修复】按钮之后，瑞星防火墙会自动在后面运行修复操作，并显示运行结果或重启计算机来重置修复选项。

图 5-35 立即修复

激活【网络安全】选项卡，在该选项卡中显示了安全上网防护和严防黑客等各项有效措施，用户只需单击各措施后面的【已开启】或【已关闭】按钮，即可禁用或启用该项措施，如图 5-36 所示。

图 5-36 设置网络安全措施

激活【家长控制】选项卡，单击【已关闭】按钮，开启家长控制措施。然后，分别设置策略名称、生效时段和上网策略等选项，并单击【保存】按钮，如图 5-37 所示。

图 5-37 设置家长控制

提　示

保存家长控制策略之后，新制定的策略将显示在左侧的列表框中，单击【添加策略】按钮，将清除前一次设置的家长控制策略。

激活【防火墙规则】选项卡，在该选项卡中将显示【联网程序规则】和【IP 规则】两部分内容。对于不同部分中的内容，用户只需启用或禁用规则前面的复选框，单击【修改】按钮，即可修改防火墙规则，如图 5-38 所示。另外，用户也可以选择某个规则，单击【删除】按钮，来删除所选规则；或者单击【清理无效规则】按钮，来清理无效的防火墙规则。

图 5-38 防火墙规则

5.2.3 练习：使用 Outpost Firewall Pro 防护计算机

Agnitum Outpost Firewall 是一款短小精悍的网络防火墙软件，它不仅能够预防来自 Cookies、广告、电子邮件病毒、后门、窃密软件、解密高手、广告软件和其他 Internet 危险的威胁，而且还具有广告和图片过滤、内容过滤、DNS 缓存等功能。Agnitum Outpost Firewall 是市场上第一个支持插件的防火墙，资源占用小，无须配置便可使用，深受广大用户的青睐。

操作步骤：

1 安装 Agnitum Outpost Firewall 并设置向导之后，软件会自动保护用户计算机，并显示产品状态，如图 5-39 所示。

图 5-39 显示产品状态

2 在左侧列表中激活【防火墙】选项卡，将会显示防火墙所拦截的程序，如图 5-40 所示。

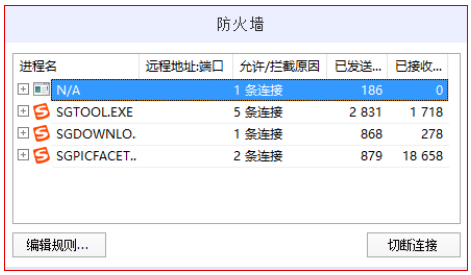

图 5-40 查看拦截进程

提 示

选择类别中的某个进程，单击【切断连接】按钮，可切断联网。

3 在左侧列表中激活【设置】选项卡，查看防火墙的基本设置情况，单击【攻击检测】右侧的【已禁用】选项，启用该功能，如图 5-41 所示。

图 5-41 设置基本设置

4 在【防火墙】选项卡中，选择底部的【高级设置】选项，在弹出的【设置】对话框中，设置防火墙的常规和一些高级设置，如图 5-42 所示。

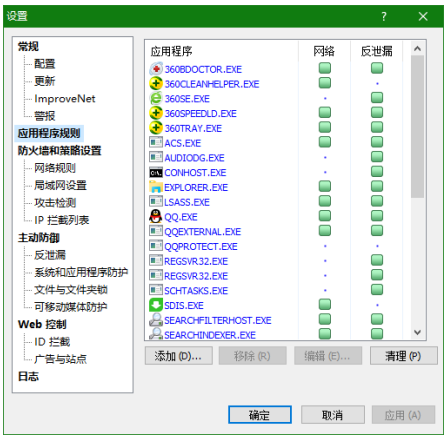

图 5-42 设置高级设置

5 在左侧列表中激活【工具】选项卡，同时在类别中选择【文件和注册表活动】选项，如图 5–43 所示。

图 5–43 【工具】选项卡

6 在弹出的【文件和注册表活动】对话框中，查看文件和注册表的活动情况。同时，选择某个进程，单击【启动监控】按钮，对其进行监控，如图 5–44 所示。

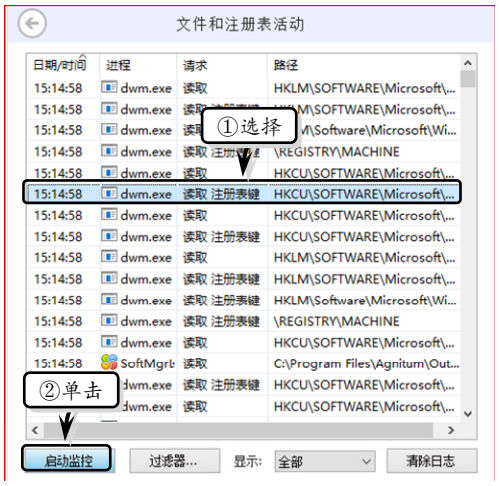

图 5–44 监控文件和注册表活动

5.3 网络监控软件

网络监控软件一般能够监控 QQ 软件、MSN 软件等一些聊天工具，并且可以在不安装客户端的情况下，轻松封堵屏蔽这些聊天软件的使用。当然，网络监控软件还可以监控到每台计算机实时的上行流量、下行流量等内容。

5.3.1 网络监控软件概述

网络监控软件是指针对局域网内的计算机进行监视和控制；针对内部的计算机上互联网，以及内部行为与资产等过程管理；包含了上网监控（上网行为监视和控制、上网行为安全审计）和内网监控（内网行为监视、控制、软硬件资产管理、数据与信息安全）。

网络监控软件一般能够监控 QQ 软件、MSN 软件，可以在不安装客户端的情况下轻松封堵屏蔽这些聊天软件的使用。网络监控软件一般包含以下 4 种工作模式。

1. 网关模式

把本机作为其他计算机的网关（设置被监视计算机的默认网关指向本机），分别可以作为单网卡方式和双网卡甚至多网卡方式。

目前，常用的是 NAT 存储转发的方式。简单说有点像路由器工作的方式，因此控制力极强；但由于存储转发的方式，性能多少有点损失，不过效率已经比较好了；缺陷是假如网关死了，全网就瘫痪了。

2．网桥模式

双网卡做成透明桥，而桥是工作在第 2 层（OSI 网络体系结构）的，所以可以简单理解为桥是一条网线，并且性能较好。

因为桥是透明的，可以看成网线，所以桥坏了就可以理解为网线坏了，换一条而已；支持多 VLAN、无线、千兆万兆以及 VPN、多出口等几乎所有的网络情况。

3．旁路模式

使用 ARP（地址解析协议）技术建立虚拟网关，只能适合于小型的网络，并且环境中不能有限制旁路模式。

例如，路由或防火墙的限制，被监视安装 ARP 防火墙都会导致无法旁路成功。同时，如果网内同时存在多个旁路将会导致混乱而中断网络。

4．旁听模式

旁听模式即旁路监听模式，是通过交换机的镜像功能来实现监控。该模式需要采用共享式交换机镜像。如果采用镜像模式，一方面需要支持双向的镜像交换机设备，另一方面需要专业的人设置镜像交换机。

该模式的优点是部署方便灵活，只要在交换机上面配置镜像端口即可，不需要改变现有的网络结构；而且即使旁路监控设备停止工作，也不会影响网络的正常运行。

缺点在于，旁听模式通过发送 RST 包只能断开 TCP 连接，不能控制 UDP 通信，如果要禁止 UDP 方式通信的软件，需要在路由器上面做相关设置进行配合。

5.3.2 常用网络监控软件

在实际工作或生活中，为了保护计算机内容和网络速度，还需要使用网络监控软件，来有效地监控文件和注册表，以及测量、显示并控制计算机中的数据流量。下面，将详细向用户介绍一些常用的网络监控软件，以帮助用户熟悉并完全掌握多种网络监控软件的使用。

1．超级巡警

超级巡警可以用来自动解决利用 RootKit 功能隐藏进程、隐藏文件和隐藏端口的各种木马，包括 HACKDEF、NTRootKit、灰鸽子、PCSHARE、FU RootKit、AFXRootKit 等。

超级巡警弥补传统杀毒软件的不足，提供非常有效的文件监控和注册表监控，使用户对系统的变化了如指掌。它也提供了多种专业级的工具，使用户可以自己手动分析，100%地查杀未知木马。

运行该软件后，即可在窗口的上方看到【病毒查杀】【实时防护】【工具大全】等选项卡，如图 5-45 所示。

图 5-45 超级巡警窗口

❑ 扫描检测

在窗口中的【病毒查杀】选项卡中，可以用快速扫描、全面扫描、目录扫描等方式查找计算机病毒。

用户需要对计算机操作系统的重要文件，或者以最快的速度完成计算机系统的查杀病毒操作时，可以单击【全面扫描】按钮，如图 5-46 所示。在查杀病毒过程中，查找到可疑文件时，则在显示器屏幕的右下角弹出提示信息。

图 5-46 扫描计算机系统

❑ 实时防护

为了保护计算机上网的安全性，可以激活【实时防护】选项卡，并在该选项卡中进行相关的设置，如图 5-47 所示。在【实时防护】选项卡中，包含有进程防护、系统防护、

上网防护、下载防护、U 盘防护和漏洞防护等。

图 5-47 系统实时防护

用户可以在不同的防护项后面，单击【已开启】或【已关闭】按钮，对该防护内容进行启用或禁用操作，如图 5-48 所示。

图 5-48 关闭进程防护

用户也可以单击后面的【详细设计】链接，在弹出的【超级巡警杀毒软件-设置】对话框中，对防护内容进行详细的设置，如图 5-49 所示。

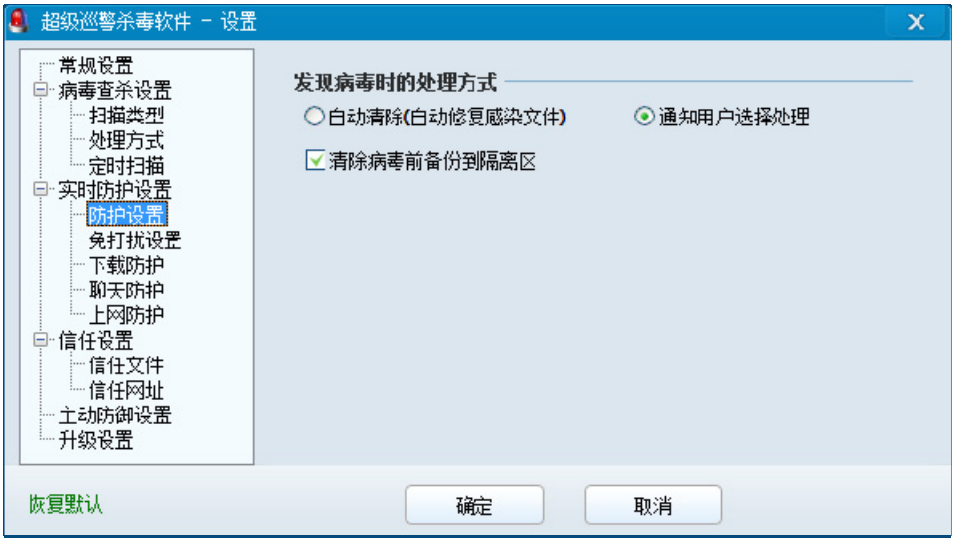

图 5-49 详细设计

在该对话框中，用户可以选择不同的选项，对主要内容进行简单的设置，如病毒查杀设置、实时防护设置、信任设置，以及主动防御设置和升级设置等，如表 5-2 所示。

表 5-2 超级巡警的设置内容

选项名称	参 数 内 容	说　　明
常规设置	常规设置	主要对开机自动启动、退出提示、发现病毒播放声音、退出时密码保护等设置项进行设置
	附加选项	参与体验计划、自动发送错误报告、加入智能云计划等
	高级选项	开机自我保护设置
病毒查杀设置	扫描类型	主要用来设置扫描文件的类型，如 EXE、DLL、VBS 等。另外，还可以设置使用什么样的启发引擎
	处理方式	主要是对发现病毒处理，以及隔离设置等
	定时扫描	设置定时内容，并指定扫描的周期时间
实时防护设置	防护设置	设置发现病毒处理方式，以及清理病毒前备份等
	免打扰设置	在运行游戏或者全屏程序时，设置进行免打扰模式，即发现病毒，软件自行处理，并不做提示
	下载防护	自动扫描下载的文件，并嵌入下载工具
	聊天防护	即时扫描聊天工具传输的文件
	上网防护	检测网页木马病毒以及钓鱼诈骗网站，保护上网首页
信任设置	信任文件	添加信任文件目录
	信任网址	添加可以浏览的信任网址
主动防御设置	启用主动防御，并设置云端分析高危程序，以及弹窗设置	
升级设置	主要包含自动升级、手动升级，以及代理服务器设置等	

❑ 工具大全

几乎在所有安全软件中，都包含有工具类的内容。而工具类内容中主要包含了一些针对性的工具应用，在该软件中也不例外。

激活【工具大全】选项卡，可以非常清楚地看到【Arp 防火墙】【漏洞修复】【系统工具箱】【暴力删除】和【U 盘巡警】等一些常用的工具，如图 5-50 所示。

图 5-50 工具软件

2．360 流量防火墙

360 流量防火墙是从 360 安全卫士中分离出来的一个独立程序，集管理网速、保护网速、防蹭网和无线路由器管理等多个功能于一体的网络监控软件。

运行 360 安全卫士，在主界面的右下方，选择【更多】选项。然后，在展开的列表中选择【流量防火墙】选项，如图 5-51 所示。

图 5-51 360 安全卫士软件

❑ 管理网速

在【360 流量防火墙】界面中，激活【管理网速】选项卡，在其列表框中将显示目前需要访问网络或曾经访问过网络的程序，以及建立连接数等信息。用户只需单击程序后面的【管理】按钮，执行【禁止访问网络】命令，即可禁止该程序的访问功能，如图 5-52 所示。

提　示

禁止程序访问网络之后，同样单击【管理】按钮，执行【允许访问网络】命令，即可启用该程序访问网络的功能。

除了限制访问网络之外，用户还可以单击【管理】按钮，执行【限制下载速度】命令。然后在【限制下载】文本框中输入下载数值即可，如图 5-53 所示。

图 5-52 禁止访问网络

图 5-53 限制下载速度

❑ 测网速

在【360 流量防火墙】界面中，激活【测网速】选项卡，会自动弹出【360 宽带测速器】对话框，测试当前网速速度，如图 5-54 所示。

网速测试结束之后，将自动显示检测结果。在检测结果中，包括宽带接入速度、长途网络速度、网页打开速度、网速排行榜和测速说明等内容，如图 5-55 所示。

图 5-54 测网速

图 5-55 显示测试结果

提　示

在【360 流量防火墙】对话框中，除了上述所介绍的功能之外，还可以激活【保护网速】选项卡，来设置需要保护网速的程序，以确保主要程序连接网络的流畅性。

5.4 思考与练习

一、填空题

1. _____是指计算机资产安全，即计算机信息系统资源和信息资源不受自然和人为有害因素的威胁和危害。

2. 20 世纪 80 年代，_____首次公开发表的论文《计算机病毒：原理和实验》提出了计算机病毒的概念：_____。

3. _____是指设置在不同网络（如可信任的企业内部网和不可信的公共网）或网络安全域之间的一系列部件的组合。

4. _____是多种类似软件的集合名词，是指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安装运行，侵害用户合法权益的软件，但不包含我国法律法规规定的计算机病毒。

5. 计算机杀毒软件，又称为_____。

6. _____也是应用软件中的一种，它的作用是为了对付病毒，保护系统的稳健工作，保护用户私密信息安全。

二、选择题

1. 现今的企业网络及个人信息安全存在的威胁，下面_____描述不正确。

A. 非授权访问

B. 冒充合法用户

C. 破坏数据的完整性

D. 无干扰系统正常运行

2. 在国内，最初引起人们注意的病毒是 20 世纪 80 年代末出现的病毒，而下列不属于该年代的病毒是_____。

A. 黑色星期五

B. 米氏病毒

C. 熊猫烧香

D. 小球病毒

3. 用户通过下列一些现象，不能判断是否

感染计算机病毒的是_____。

A．机器不能正常启动（加电后机器根本不能启动，或者启动时间变长了。有时会突然出现黑屏现象）

B．运行速度降低（发现在运行某个程序时，读取数据的时间比原来长，存文件或调文件的时间较长）

C．磁盘空间迅速变小（内存空间变小甚至变为“0”，用户什么信息也进不去）

D．文件内容和长度有所改变（一个文件存入磁盘后，有时文件内容无法显示或显示后又消失了）

4．一般的防火墙都可以保护计算机安全功能，下列描述不正确的是_____。

A．可以限制他人进入内部网络，过滤掉不安全服务和非法用户

B．防止入侵者接近防御设施

C．不限定用户访问特殊站点

D．为监视 Internet 安全提供方便

5．具有一些特征的软件可以被认为是恶意软件，那么下列描述不正确的是_____。

A．指没有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，卸载后仍然有活动程序的行为

B．指没有经过用户许可，修改浏览器参数或其他相关设置，迫使用户访问特定网站或导致用户无法正常上网的行为

C．在用户计算机或其他终端上安装软件的行为

D．指未明确提示用户或者未经用户许可，将被认定为恶意软件的软件捆绑到其他软件的行为

6．在“超级巡警”软件中包含有多个扫描方式，下列_____不属于该软件的扫描方式。

A．文件扫描

B．内存扫描

C．快速扫描

D．全面扫描

三、问答题

1．描述防火墙的优点。

2．什么是恶意软件？

3．网络监控软件包括哪几种模式？

四、上机练习

1．禁用 Windows 10 防火墙

Windows 10 在安全性上面已有大大提高，但是好多人还不知道如何设置 Windows 7 的防火墙。下面就对 Windows 10 防火墙做一些简单的了解。打开 Windows 10 防火墙的方法比较简单，右击【开始】图标，执行【控制面板】命令，打开【控制面板】窗口，如图 5-56 所示。

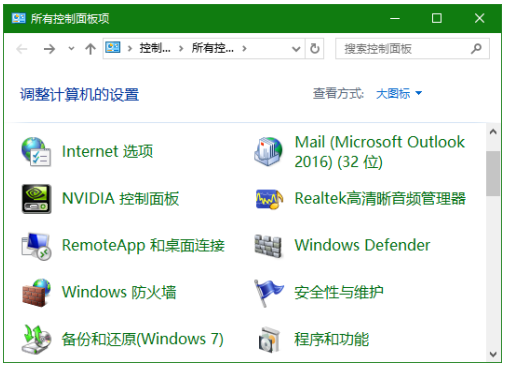

图 5-56 【控制面板】窗口

在【控制面板】窗口中，单击【Windows 防火墙】链接，即可打开【Windows 防火墙】窗口，如图 5-57 所示。

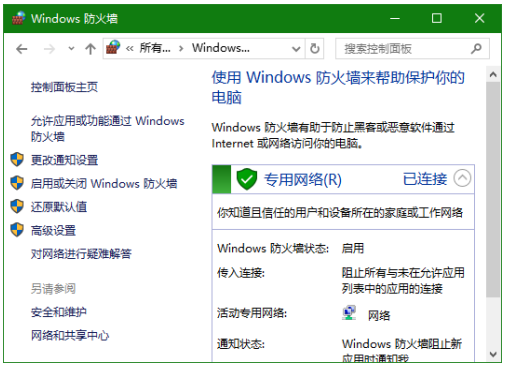

图 5-57 【Windows 防火墙】窗口

然后，单击左侧的【启用或关闭 Windows 防火墙】链接。此时，在打开的窗口中，可以启用或者关闭防火墙，如图 5-58 所示。

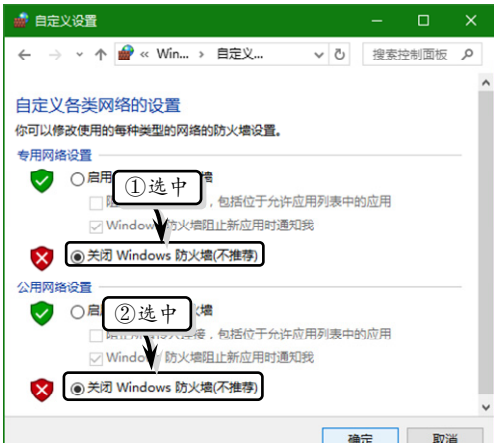

图 5-58 启用 Windows 防火墙

2．停止金山卫士

当用户安装【金山卫士】软件后，则重新启动计算机后将自动启动该卫士。如果用户需要停止金山卫士对计算机保护功能，则可以单击任务栏中的【显示隐藏的图标】按钮，并右击金山安全卫士图标，执行【退出】命令，如图 5-59 所示。然后，在弹出的提示对话框中，单击【确定】按钮即可。

图 5-59 执行【退出】命令