第5章

计算机病毒及其防治

CHAPTER 5

随着计算机技术的普及和发展，计算机系统的安全已成为计算机用户普遍关注的问题，而计算机病毒是计算机系统的巨大威胁之一，计算机病毒一旦发作，轻则破坏文件、损害系统，重则造成网络瘫痪。因此，势必要了解计算机病毒，使计算机免受其恶意的攻击与破坏。

学习目标

- 了解计算机病毒的定义及特征。
- 熟悉计算机病毒的传播途径及其主要危害。
- 熟悉计算机病毒发作后的症状。
- 掌握CIH病毒、宏病毒、蠕虫病毒、特洛伊木马、勒索病毒的主要特征及防治对策。
- 掌握木马程序的工作原理，以及手工清除木马的常见方法。
- 掌握企业版杀毒软件的安装及配置。

5.1 计算机病毒概述

5.1.1 计算机病毒的概念

1994年2月18日,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》中进行了明确的定义:“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。”

也就是说,计算机病毒就是一段程序,但是它具有自己的特殊性。首先,计算机病毒利用计算机资源的脆弱性,破坏计算机系统;其次,计算机病毒不断地进行自我复制,在潜伏期内,通过各种途径传播到其他计算机系统并隐藏起来,当达到触发条件时被激活,将会导致系统被恶意破坏。

5.1.2 计算机病毒的发展

1. 计算机病毒的起源

20世纪60年代初,美国贝尔实验室里,三个年轻的程序员编写了一个名为“磁芯大战”的游戏,游戏中通过复制自身来摆脱对方的控制,这就是所谓“病毒”的雏形。

20世纪70年代,美国作家雷恩在其出版的《P.1的青春》一书中构思了一种能够自我复制的计算机程序,并第一次称之为“计算机病毒”。

2. 第一个病毒

1983年11月,在国际计算机安全学术研讨会上,美国学者科恩第一次明确提出“计算机病毒”的概念,并将病毒程序在VAX/750计算机上进行了演示,世界上第一个计算机病毒就这样诞生在实验室中。

20世纪80年代后期,巴基斯坦有两个以写程序为生的兄弟,他们为了打击那些盗版软件的使用者,设计出了一个名为“巴基斯坦”的病毒,该病毒只传染软盘引导区。这就是最早在世界上流行的一个真正的病毒。

3. DOS阶段

1988—1989年,我国也相继出现了能感染硬盘和软盘引导区的Stoned(石头)病毒,该病毒体代码中有明显的标志“Your PC is now Stoned!”“LEGALISE MARIJUANA!”,也称为“大麻”病毒等。该病毒感染软硬盘0面0道1扇区,并修改部分中断向量表。该病毒不隐藏也不加密自身代码,所以很容易被查出和解除。类似这种特性的还有小球、Azusa/Hong.Kong/2708、Michaelangelo,这些都是从国外传染的。而国产的有Bloody、Torch、Disk Killer等病毒,实际上它们大多数是Stoned病毒的翻版。

20世纪90年代初,感染文件的病毒有Jerusalem(黑色13号星期五)、YankeeDoole、Liberty、1575、Traveller、1465、2062,4096等,主要感染.COM和.EXE文件。这类病毒修

改了部分中断向量表，被感染的文件明显地增加了字节数，并且病毒代码主体没有加密，也容易被查出和解除。在这些病毒中，略有对抗反病毒手段的只有 Yankee Doole 病毒，当它发现你用 DEBUG 工具跟踪它时，它会自动从文件中逃走。

接着，又一些能对自身进行简单加密的病毒相继出现，有 1366(DaLian)、1824(N64)、1741(Dong)、1100 等病毒，它们加密的目的主要是防止跟踪或掩盖有关特征等。

以后又出现了引导区、文件型“双料”病毒，这类病毒既感染磁盘引导区又感染可执行文件，常见的有 Flip/Omicron(颠倒)、XqR(New Century，新世纪)、Invader(侵入者)、Plastique(塑料炸弹)、3584[郑州(狼)]、3072(秋天的水)、ALFA/3072.2、Ghost/One_Half/3544(幽灵)、Natas(幽灵王)、TPVO/3783 等，如果只解除了文件上的病毒，而没解除硬盘主引导区的病毒，系统引导时又将病毒调入内存，会重新感染文件。如果只解除了主引导区的病毒，而可执行文件上的病毒没解除，一执行带毒的文件时，就又将硬盘主引导区感染。

自 1992 年以来，DIR2.3、DIR2.6、NEW DIR2 病毒以一种全新的面貌出现，感染力极强，无任何表现，不修改中断向量表，而直接修改系统关键中断的内核，修改可执行文件的首簇数，将文件名字与文件代码主体分离。在系统有此病毒的情况下，一切就像没发生一样。而在系统无病毒时，用户用无病毒的文件去覆盖有病毒的文件，灾难就会发生，全盘所有被感染的可执行文件内容都是刚覆盖进去的文件内容。这是病毒“我死你也活不成”的罪恶伎俩。该病毒的出现使病毒又多了一种新类型。

20 世纪，绝大多数病毒是基于 DOS 系统的，有 80% 的病毒能在 Windows 中传染。TPVO/3783 病毒是“双料性”(传染引导区、文件)、“双重性”(DOS、Windows)病毒，这就是病毒随着操作系统发展而发展起来的病毒。

4. Windows 阶段

Windows 9x、Windows 2000 操作系统的发展，也使病毒种类随其变化而变化。以下例举几个典型的 Windows 病毒。

1) WIN32.CAW.1XXX 病毒

WIN32.CAW.1XXX 病毒是驻留内存的 Win32 病毒，它感染本地和网络中的 PE 格式文件。该病毒的产生是来源一种 32 位的 Windows“CAW 病毒生产机”，该“CAW 病毒生产机”是国际上一家有名的病毒编写组织开发的。

“CAW 病毒生产机”能生产出各种各样的 CAW 病毒，有加密的和不加密的，其字节数一般为 1000～2000。目前在国内流行的有 CAW.1531、CAW.1525、CAW.1457、CAW.1419、CAW.1416、CAW.1335、CAW.1226 等，在国际上流行的 CAW.1XXX 病毒种类更多。

对于 WIN32.CAW.1XXX 病毒，当病毒驻留内存时，会在每日的整点时间，如 1：00，6：00，10：00，…，病毒就会删除一些特定的文件，如.BMP、.JPG、.DOC、.WRI、.BAS、.SAV、.PDF、.RTF、.TXT、WINWORD.EXE。

当 7 月 7 日时 CAW 病毒就会发作，删除硬盘上的所有文件。

某些 CAW.1XXX 病毒有缺陷，被传染上该病毒的文件被破坏了，杀毒后文件也无法修复，只能用正常文件覆盖坏文件。病毒还有一个缺陷，即重复多层次感染文件，容易将文件写坏。

2) WIN32.FunLove.4099 病毒

WIN32.FunLove.4099 病毒感染本地和网络中的 PE.EXE 文件。

该病毒本身就是只具有".code"部分PE格式的可执行文件。

当染毒的文件被运行时,该病毒将在Windows\system目录下创建FLCSS.EXE文件,在其中只写入病毒的纯代码部分,并运行这个生成的文件。

一旦在创建FLCSS.EXE文件时发生错误,病毒将从染毒的主机文件中运行传染模块。该传染模块被作为独立的线程在后台运行,主机程序在执行时几乎没有可察觉的延时。

传染模块将扫描本地从C:to Z:的所有驱动器,然后搜索网络资源,扫描网络中的子目录树并感染具有.OCX,.SCR或者.EXE扩展名的PE文件。

这个病毒类似Bolzano病毒那样修补NTLDR和WINNT\System32\ntoskrnl.exe,被修补的文件不可以恢复只能通过备份来恢复。

3) WIN32.KRIZ.4250病毒

WIN32.KRIZ.4250病毒已大面积传播,这是一个变形病毒,变化多端,每年的12月25日像CIH病毒一样破坏硬盘数据与主板BIOS,该病毒目前也有许多字节数不同的变种。

4) 宏病毒

病毒的种类、传染和攻击的手法越来越高超,在Windows环境下最为知名的就属寄存在文档或模板的宏中的宏病毒。

近几年,出现了近万种Word(Macro宏)病毒,并以迅猛的势头发展,已形成了病毒的另一大派系。由于宏病毒编写容易,不分操作系统,再加上Internet上用Word格式文件进行大量的交流,宏病毒会潜伏在这些Word文件里,被人们在Internet上传来传去。

5. Internet阶段

1997年以后,Internet发展迅速,各种病毒也开始利用Internet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。以2003年出现的"冲击波"病毒为代表,出现了以利用系统或应用程序漏洞,采用类似黑客手段进行感染的病毒。

1) 2001年——尼姆达病毒

尼姆达病毒(Nimda)是典型的蠕虫病毒,病毒由JavaScript脚本语言编写,病毒通过Email、共享网络资源、IIS服务器、网页浏览传播,修改本地驱动器上的.htm、.html和.asp文件。此病毒可以使IE和Outlook Express加载产生readme.eml病毒文件。该文件将尼姆达蠕虫作为附件,不需要拆开或运行这个附件病毒就被执行。

2) 2003年——冲击波病毒

冲击波病毒是利用在2003年7月21日公布的RPC漏洞进行传播的,该病毒于当年8月爆发。病毒运行时会不停地利用IP扫描技术寻找网络上系统为Windows 2000或XP的计算机,找到后就利用DCOM/RPC缓冲区漏洞攻击该系统,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,使系统操作异常、不停重启,甚至导致系统崩溃。另外,该病毒还会对系统升级网站进行拒绝服务攻击,导致该网站堵塞,使用户无法通过该网站升级系统。只要是有RPC服务并且没有打安全补丁的计算机都存在有RPC漏洞,具体涉及的操作系统是Windows 2000\XP\Server 2003\NT4.0。

3) 2007年——熊猫烧香病毒

熊猫烧香病毒会感染系统扩展名为.exe、.com、.src、.html、.asp等文件,并在其后追加

病毒网址，导致用户只要一打开这些扩展名的文件就会掉进不法分子的陷阱中。熊猫烧香病毒的“凶残”之处就在于：装系统对于它来说是起不到用处的。会感染镜像文件。即使用户试图采用全盘格式化的方式来摆脱熊猫烧香，但是只要用之前的镜像文件来恢复系统，病毒将依然存在于计算机中。

4）2010 年——震网病毒

震网病毒是一种典型的蠕虫病毒。它十分复杂，因此对黑客的能力要求也很高。震网病毒在 2010 年 6 月出现在人们的视野中，被称为有史以来最复杂的网络武器。作为世界上第一个网络“超级毁灭性武器”，震网病毒的威力不可小觑，它感染了全世界 45 000 多个网络。震网病毒让人不能忽视的理由——它专门破坏现实世界中的各种能源设施，例如水坝、核电站、国家电网的等重要设施。

5）2015 年——苹果 Xcode

2015 年 9 月，据报道，非官方下载的苹果开发环境 Xcode 中包含恶意代码，将编译的 App 应用里添加远程控制和盗窃用户信息的功能。此次事件波及了网易云音乐、微信、滴滴出行、高德地图、高铁管家等众多 App，许多用户也因此损失惨重。由于此病毒，个人重要信息在不知不觉间就到了不怀好意的人的手里。它的恐怖之处就在于一旦用户下载了带有恶意代码的 App 之后，一些不法分子将会神不知鬼不觉地窃取用户的信息，并利用用户信息来进行诈骗、欺诈等一系列的非法活动。

6）2016 年——DDoS 攻击

2016 年 11 月，俄罗斯 5 家主流银行遭遇长达两天的 DDoS 攻击。连续的攻击使得多家主流银行无法正常营业，其损失不可估量。不仅如此，DDoS 攻击使得同年美国一些知名网站如亚马逊、Twitter、Tumblr 等人气网站崩溃，网民一度无法使用支付系统。DDoS 攻击让人无可奈何的原因就是因为它戴上合法的面具，占用大量网络资源，以此让此网站瘫痪无法使用。

7）2017 年——勒索病毒 WannaCry

WannaCry 是一种计算机软件敲诈病毒。该恶意软件进行端口扫描，找到漏洞之后即刻进行攻击，并以蠕虫式方式传播。感染了该病毒的计算机文件将被加密，而后攻击主机以支付等额 300 美元比特币的形式向用户勒索赎金。2017 年 5 月，WannaCry 勒索病毒袭击了 99 多个国家，包括英国、美国、中国、俄罗斯、西班牙和意大利。勒索病毒 WannaCry 利用用户以图省事关闭防火墙的坏习惯进行攻击，之后对用户文件进行加密，最后展现出自己要勒索的真面目。但是，当用户支付完黑客想要的酬金之后，会得到黑客更加猖狂的攻击。

5.2　计算机病毒的特征及传播途径

5.2.1　计算机病毒的特征

1. 非授权可执行性

用户通常调用执行一个程序时，把系统控制权交给这个程序，并分配给它相应系统资

源,如内存,从而使之能够运行完成用户的需求,因此程序执行的过程对用户是透明的。而计算机病毒是非法程序,正常用户不会明知它是病毒程序,而故意调用执行的。但计算机病毒具有正常程序的一切特性:可存储性和可执行性。它隐藏在合法的程序或数据中,当用户运行正常程序时,病毒伺机窃取到系统的控制权,得以抢先运行,而此时用户还认为在执行正常程序。

2. 隐蔽性

计算机病毒是一种具有很高编程技巧、短小精悍的可执行程序。它通常黏附在正常程序之中或磁盘引导区中,或者磁盘上标为坏簇的扇区中,以及一些空闲概率较大的扇区中,这是它的非法可存储性。病毒想方设法隐藏自身,就是为了防止用户察觉。

3. 传染性

传染性是计算机病毒最重要的特征,是判断一段程序代码是否为计算机病毒的依据。病毒程序一旦侵入计算机系统就开始搜索可以传染的程序或者磁介质,然后通过自我复制迅速传播。由于目前计算机网络日益发达,计算机病毒可以在极短的时间内通过 Internet 传遍世界。

4. 潜伏性

计算机病毒具有依附于其他媒体而寄生的能力,这种媒体称为计算机病毒的宿主。依靠病毒的寄生能力,病毒传染合法的程序和系统后,不立即发作,而是悄悄隐藏起来,然后在用户不察觉的情况下进行传染。这样,病毒的潜伏性越好,它在系统中存在的时间也就越长,病毒传染的范围也越广,其危害性也越大。

5. 表现性或破坏性

无论何种病毒程序一旦侵入系统都会对操作系统的运行造成不同程度的影响。即使不直接产生破坏作用的病毒程序也要占用系统资源(如占用内存空间、占用磁盘存储空间以及系统运行时间等)。而绝大多数病毒程序要显示一些文字或图像,影响系统的正常运行,还有一些病毒程序删除文件,加密磁盘中的数据,甚至摧毁整个系统和数据,使之无法恢复,造成不可挽回的损失。因此,病毒程序的副作用轻者降低系统工作效率,重者导致系统崩溃、数据丢失。病毒程序的表现性或破坏性体现了病毒设计者的真正意图。

6. 可触发性

计算机病毒一般都有一个或者几个触发条件。一旦满足其触发条件或者激活病毒的传染机制,就会使之进行传染,或者激活病毒的表现部分或破坏部分。触发的实质是一种条件的控制,病毒程序可以依据设计者的要求,在一定条件下实施攻击。这个条件可以是输入特定字符、使用特定文件、某个特定日期或特定时刻,或者是病毒内置的计数器达到一定次数等。

5.2.2　计算机病毒的传播途径

传染性是计算机病毒最重要的特征，计算机病毒从已被感染的计算机感染到未被感染的计算机，就必须要通过某些方式来进行传播，最常见的就是以下两种方式。

第一种：通过移动存储设备来进行传播，包括软盘、光盘、移动硬盘和 U 盘等。

在计算机应用早期，计算机应用较简单，许多文件都是通过软盘来进行相互复制、安装，这时，软盘也就是最好的计算机病毒的传播途径。光盘容量大、存储内容多，所以大量的病毒就有可能藏匿在其中，对于只读光盘，不能进行写操作，光盘上的病毒更加不能查杀。曾经盗版光盘泛滥，这样给病毒的传染带来了极大的便利。又曾广泛使用移动硬盘和 U 盘来交换数据，这些存储设备也就成了计算机病毒的主要寄生的“温床”。

第二种：通过网络来进行传播。

毫无疑问，网络是现在计算机病毒传播的重要途径。我们平时浏览网页、下载文件、收发电子邮件，访问 BBS 等，都可能会使计算机病毒从一台计算机传播到网络上其他的计算机上。

5.3　计算机病毒的分类

计算机病毒的种类有很多，按照计算机病毒的特征来分类可以将计算机病毒分为以下几类。

1. 按寄生方式分

按寄生方式分可分为引导型病毒、文件型病毒和复合型病毒。

引导型病毒是指寄生在磁盘引导区或主引导区的计算机病毒。此种病毒利用系统引导时，不对主引导区的内容正确与否进行判别的缺点，在引导型系统的过程中侵入系统，驻留内存，监视系统运行，待机传染和破坏。按照引导型病毒在硬盘上的寄生位置又可细分为主引导记录病毒和分区引导记录病毒。主引导记录病毒感染硬盘的主引导区，如大麻病毒、2708 病毒、火炬病毒等；分区引导记录病毒感染硬盘的活动分区引导记录，如小球病毒、Girl 病毒等。

文件型病毒是指能够寄生在文件中的计算机病毒。这类病毒程序感染可执行文件或数据文件。如 1575/1591 病毒、848 病毒感染.COM 和.EXE 等可执行文件，Macro/Concept、Macro/Atoms 等宏病毒感染.DOC 文件。

复合型病毒是指具有引导型病毒和文件型病毒寄生方式的计算机病毒。这种病毒扩大了病毒程序的传染途径，它既感染磁盘的引导记录，又感染可执行文件。当染有此种病毒的磁盘用于引导系统或调用执行染毒文件时，病毒就会被激活。因此在检测、清除复合型病毒时，必须全面彻底地根治，如果只发现该病毒的一个特性，把它只当作引导型或文件型病毒进行清除，虽然好像是清除了，但还留有隐患，这种经过消毒后的“洁净”系统更赋有攻击性。这种类型的病毒常见的有：Flip 病毒、新世纪病毒、One. half 病毒等。

2. 按破坏性分

按破坏性分可分为良性病毒和恶性病毒。

良性病毒是指那些只是为了表现自身,并不彻底破坏系统和数据,但会大量占用CPU时间、增加系统开销、降低系统工作效率的一类计算机病毒。这种病毒多数是恶作剧者的产物,他们的目的不是破坏系统和数据,而是让使用染有病毒的计算机用户了解病毒设计者的编程技术。这类病毒常见的有小球病毒、1575/1591病毒、救护车病毒、扬基病毒、Dabi病毒等。还有一些人利用病毒的这些特点宣传自己的政治观点和主张。也有一些病毒设计者在其编制的病毒发作时进行人身攻击。

恶性病毒是指那些一旦发作后,就会破坏系统或数据,造成计算机系统瘫痪的一类计算机病毒。这类病毒常见的有黑色星期五病毒、火炬病毒、米开朗·基罗病毒等。这种病毒危害性极大,有些病毒发作后可以给用户造成不可挽回的损失。

5.4 计算机病毒的破坏行为及防御

5.4.1 计算机病毒的破坏行为

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他所具有的技术能量。数以万计、不断发展扩张的病毒,其破坏行为千奇百怪。根据常见的病毒特征,可以把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。一般来说,攻击系统数据区的病毒是恶性病毒,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,一般包括删除文件、修改文件名、替换文件内容、丢失部分程序代码、内容颠倒、写入时间空白、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,也是病毒经常攻击的目标。病毒额外地占用和消耗系统的内存资源,可以导致一些程序受阻,甚至无法正常运行。

病毒攻击内存的方式有占用大量内存、改变内存总量、禁止分配内存、蚕食内存。

4. 干扰系统运行

病毒会干扰系统的正常运行,以此达到自己的破坏行为。其一般表现为不执行命令、干扰内部命令的执行、虚假报警、打不开文件、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。在时钟中载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。

6. 攻击磁盘

攻击磁盘数据、不写盘、写操作变读操作、写盘时丢字节。

7. 扰乱屏幕显示

病毒扰乱屏幕显示一般表现为字符跌落、环绕、倒置、显示前一屏、光标下跌、滚屏、抖动、乱写、吃字符等。

8. 键盘

病毒干扰键盘操作，主要表现为响铃、封锁键盘、换字、抹掉缓存区字符、重复、输入紊乱等。

9. 喇叭

许多病毒运行时，会使计算机的喇叭发出响声。有的病毒作者让病毒演奏旋律优美的世界名曲，在高雅的曲调中抹掉人们的信息财富。其一般表现为演奏的曲子、警笛声、炸弹的噪声、鸣叫、咔咔声、嘀嗒声等。

10. 攻击 CMOS

在机器的 CMOS 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，并具有校验和。有的病毒激活时，能够对 CMOS 进行写入动作，破坏系统 CMOS 中的数据。

11. 干扰打印机

假报警、间断性打印、更换字符。

5.4.2　如何有效防御计算机病毒

怎样有效地防御计算机病毒呢？建议在自己的计算机上做好以下操作：

- 在计算机上安装杀毒软件和防火墙软件，本章以 Symantec Endpoint Protection（端点保护）为例；
- 及时升级杀毒软件，尤其在病毒盛行期间或者病毒突发的非常时期，这样做可以保证计算机受到持续地保护；
- 使用流行病毒专杀工具；
- 开启杀毒软件的实时监控中心功能，系统启动后立即启用计算机监控功能，防止病毒侵入计算机。
- 定期全面扫描一次系统（建议个人计算机每周一次，服务器每天深夜全面扫描一次系统）；

- 复制任何文件到本机时,建议使用杀毒软件右键查杀功能进行专门查杀;
- 以纯文本方式阅读信件,不要轻易打开电子邮件附件;
- 从互联网下载任何文件时,请检查该网站是否具有安全认证;
- 请勿访问某些可能含有恶意脚本或者蠕虫病毒的网站,建议启用杀毒软件网页监控功能;
- 及时获得反病毒预报警示;
- 建议使用 Windows Update 更新操作系统,或者使用杀毒软件系统漏洞扫描工具及时下载并安装补丁程序;
- 使用防火墙软件,防止黑客程序侵入计算机。

5.4.3 如何降低由病毒破坏所引起的损失

- 定期备份硬盘数据,万一发生硬盘数据损坏或丢失,可使用杀毒软件的硬盘数据备份功能恢复数据;
- 可以通过邮件、电话、传真等方式与杀毒软件的客户服务中心联系,由他们的技术中心提供专业的服务,尽量减少由病毒破坏造成的损失。

5.4.4 计算机病毒相关法律法规

为了保护计算机信息系统的安全,促进计算机的应用和发展,保障社会主义现代化建设的顺利进行,制定了《中华人民共和国计算机信息系统安全保护条例》。

为了加强对计算机病毒的预防和治理,保护计算机信息系统安全,保障计算机的应用与发展,根据《中华人民共和国计算机信息系统安全保护条例》的规定,制定了《计算机病毒防治管理办法》。

为了加强计算机信息系统安全专用产品的管理,保证安全专用产品的安全功能,维护计算机信息系统的安全,根据《中华人民共和国计算机信息系统安全保护条例》第十六条的规定,制定了《计算机信息系统安全专用产品检测和销售许可证管理办法》。

5.5 常见病毒的查杀

5.5.1 CIH 病毒的查杀

CIH 病毒最早于 1998 年 6 月初在台湾被发现,它是由一位名叫陈盈豪(Chen Ing Halu)的台湾大学生所编写的,由于其名字第一个字母分别为 C、I、H,"CIH 病毒"名称的由此得来。CIH 病毒的载体是一个名为"ICQ 中文 Ch_at 模块"的工具,并以热门盗版光盘游戏如"古墓奇兵"或 Windows 95/98 为媒介,经互联网各网站互相转载,使其迅速传播。目前传播的主要途径是 Internet 和电子邮件。

CIH 病毒属文件型病毒,它主要感染 Windows 95/98 系统下的 EXE 文件,当一个染毒的 EXE 文件被执行时,CIH 病毒驻留内存,当其他程序被访问时对它们进行感染。其发展过程经历了 v1.0,v1.1、v1.2、v1.3、v1.4 总共 5 个版本,目前较为流行的是 v1.2 版本,在此

期间，同时产生了不下十个变种，但是没有流行起来的迹象。

CIH 病毒属恶性病毒，当其发作条件成熟时，将破坏硬盘数据，同时有可能破坏 BIOS 程序，其发作特征是：某些主板上的 Flash ROM 中的 BIOS 信息将被清除。

瑞星公司提供了针对硬盘的 CIH 病毒修复工具，可以到相关的网站上下载此修复工具。瑞星公司提供的修复程序只是针对 CIH 病毒破坏的硬盘进行修复，对于正常的硬盘不要使用此程序处理。此程序不保证修复所有硬盘数据，也不能保证修复后的数据是完全正确的，只是尽可能修复用户数据。此程序只修复第一块硬盘，如果有多块硬盘，可将其他硬盘摘下，一块一块地对其进行修复。

修复的操作步骤如下。

(1) 该软件包括两个程序：ANTICIH.EXE 和 RAV.REC，这两个文件必须复制到磁盘的同一路径下。

(2) 用无毒的磁盘启动计算机。

(3) 执行 ANTICIH.EXE，该程序将对硬盘进行扫描，以获得有关数据。

(4) 扫描完成后，程序将提示如下：

```
Hard disk scanned result:
SIZE CYLS HEAD SECTOR
XXXX XXXX XXXX XXXX
Partition: C: D:
Drive C: FAT32
Recover partition table (Y/N)?
```

注意：SIZE 是硬盘的大小，以 MB 为单位；CYLS 是硬盘柱面数，HEAD 是硬盘的磁头数，SECTOR 是每道扇区数。对于大于 8GB 的硬盘，只显示硬盘大小。Partition 是找到的分区；Drive C：是说明 C 盘的格式，是 FAT16 或 FAT32。

以上提示信息针对不同硬盘显示不一样，此时确认是否要修复主引导记录，要修复则按 Y 键，否则按 N 键，本程序将退出。如果按了 Y 键，此程序将修复主引导记录，程序进一步提示：

```
Recover drive C: (Y/N)?
```

如果修复 C 盘，则按 Y 键，否则按 N 键，程序将退出。

如果 C 盘是 FAT16，而且破坏比较严重，修复过程可能需要很长时间，请耐心等待。修复完成后，应重启系统。

5.5.2　宏病毒的查杀

宏病毒是一种寄存在文档或模板的宏中的计算机病毒。一旦打开这样的文档，其中的宏就会被执行，于是宏病毒就会被激活，转移到计算机上，并驻留在 Normal 模板上。从此以后，所有自动保存的文档都会感染上这种宏病毒，而且如果其他用户打开了感染病毒的文档，宏病毒又会转移到他的计算机上。目前发现的几种主要宏病毒有 Wazzu、Concept、13 号病毒、Nuclear、July.killer(又名“七月杀手”)。

有些宏病毒对用户进行骚扰，但不破坏系统，比如说有一种宏病毒在每月的 13 日发作

时显示出5个数字连乘的心算数学题；有些宏病毒或使打印中途中断或打印出混乱信息，如Nuclear、Kompu等属此类；有些宏病毒将文档中的部分字符、文本进行替换；但也有些宏病毒极具破坏性，如MDMA.A，这种病毒既感染中文版Word，又感染英文版Word，发作时间是每月的1日。此病毒在不同的Windows平台上有不同的破坏性表现，轻则删除帮助文件，重则删除硬盘中的所有文件；另外还有一种双栖复合型宏病毒，发作可使计算机瘫痪。

1. 宏病毒的预防

(1) 将常用的Word模板文件改为只读属性，可防止Word系统被感染；DOS下的autoexec.bat和config.sys文件最好也都设为只读属性文件。

(2) 因为宏病毒是通过自动执行宏的方式来激活、进行传染破坏的，所以只要将自动执行宏功能禁止掉，即使有宏病毒存在，但无法被激活，也无法发作传染、破坏，这样就起到了防毒的效果。

2. 宏病毒的制作以及查杀实例

下面简单的制作一个宏病毒让大家对实际存在的宏病毒有一个了解，其具体制作步骤如下。

(1) 打开Word文字处理软件，在窗口菜单栏中选择“插入”→“对象”选项，在弹出的“对象”对话框中选择“对象类型”列表的“包”选项，单击“确定”按钮，如图5.1所示。

图5.1 Word的“对象”对话框

(2) 在如图5.2所示的“对象包装程序”窗口中，选择菜单栏中的“编辑”→“命令行”命令，在弹出的“命令行”对话框窗口中输入“ping -t localhost -l 60000”，完成单击“确定”按钮。那么这条命令只是在永久地ping自己的计算机，并且每次发出的ping包都是60 000字节，如此就会形成一个DoS攻击。黑客们编写的宏病毒往往比这个更加厉害，比如格式化硬盘的命令等。

(3) 在如图5.2所示的“对象包装程序”窗口中，单击“插入图标”按钮，为该命令行选个有诱惑力的图标，在关闭“对象包装程序”窗口后，此时在文档的相关位置出现了一个和命令关联的图标，如图5.3所示，这样一个宏病毒就做成功了。

图 5.2　对象包装程序对话框

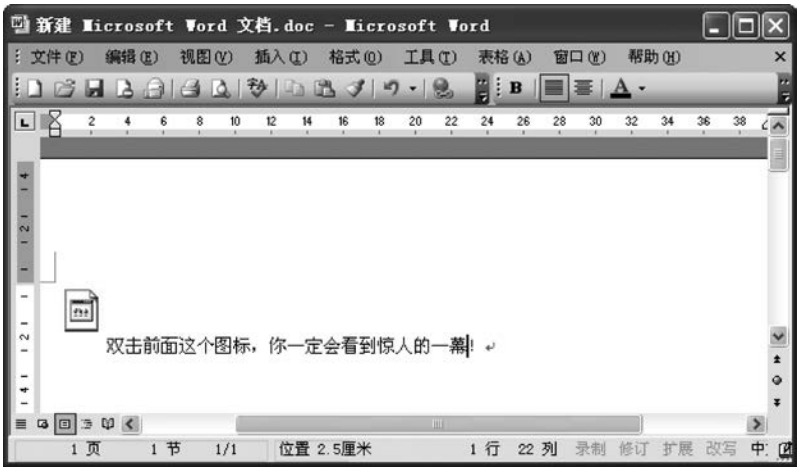

图 5.3　Word 中的宏病毒

真正的宏病毒不是这样制作的，真正的病毒会和宏指令如 FileOpen、FileSave、FileSaveAs 和 FilePrint 等命令相关联，其内编写了具有瘫痪系统，感染每一个 Word 文件的代码，并可以自动保存为“模板”文件，只要打开一次染毒的 Word 文件，则以后所有的 Word 文件都会被感染，看起来再正常不过的一个正规文档文件，很可能就暗藏着宏病毒。

刚才制作的宏病毒运行后的结果如图 5.4～图 5.6 所示。

图 5.4　Word 中的宏病毒运行结果 1

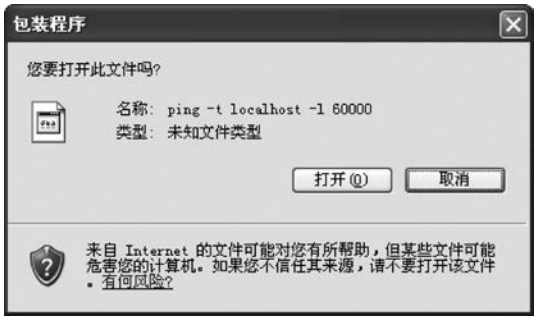

图 5.5　Word 中的宏病毒运行结果 2

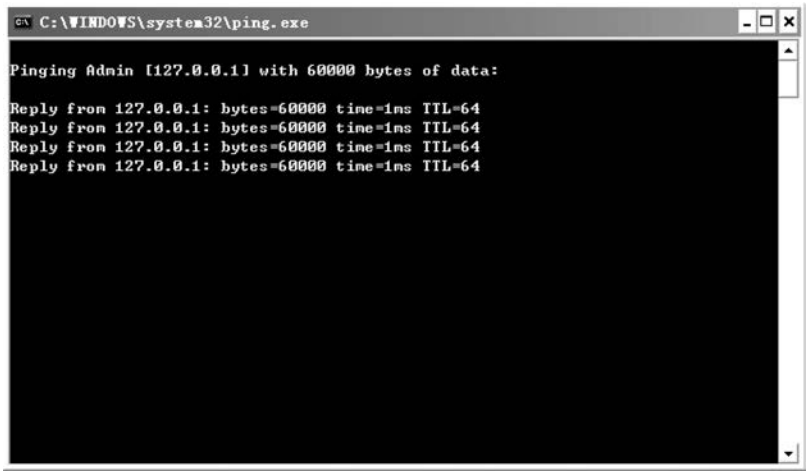

图 5.6　Word 中的宏病毒运行结果 3

3. 宏病毒的清除

(1) 手工：以 Word 为例，最简单的就是禁止 Word 执行宏指令，方法是：在 Word 窗口的菜单栏中选择“工具”→“宏”→“安全性”选项，在弹出的如图 5.7 的所示的对话框中将其安全性设为“高”，这样，未经系统签署的宏指令将会被 Word 禁止执行，这样就不利于宏病毒的运行。

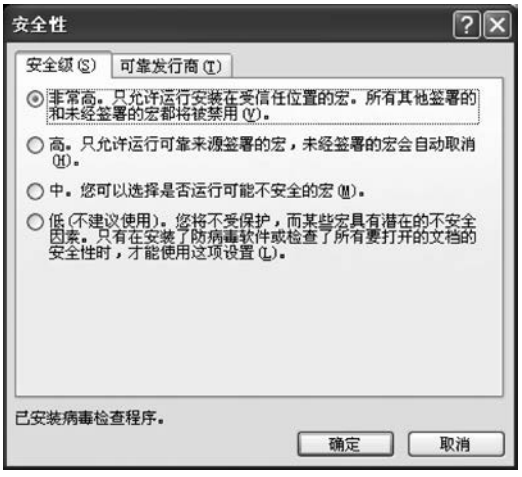

图 5.7　“安全性”对话框

(2) 使用专业杀毒软件：目前杀毒软件公司都具备清除宏病毒的能力，当然也只能对已知的宏病毒进行检查和清除，对于新出现的病毒或病毒的变种则可能不能正常地清除，或者将会破坏文件的完整性，此时建议还是手工清理。

5.5.3　蠕虫病毒的查杀

蠕虫病毒和一般的计算机病毒有着很大的区别，对于它，现在还没有一个成套的理论体

系，但是一般认为，蠕虫病毒是一种通过网络传播的恶性病毒，它除具有病毒的一些共性外，同时具有自己的一些特征，如不利用文件寄生（有的只存在于内存中）、对网络造成拒绝服务，以及与黑客技术相结合等。蠕虫病毒主要的破坏方式是大量的复制自身，然后在网络中传播，严重地占用有限的网络资源，最终引起整个网络的瘫痪，使用户不能通过网络进行正常的工作。每一次蠕虫病毒的爆发都会给全球经济造成巨大的损失，因此它的危害性是十分巨大的；有一些蠕虫病毒还具有更改用户文件、将用户文件自动当附件转发的功能，更是严重地危害到用户的系统安全。

1. 蠕虫病毒常见的传播方式

（1）利用系统漏洞传播——蠕虫病毒利用计算机系统的设计缺陷，通过网络主动地将自己扩散出去。

（2）利用电子邮件传播——蠕虫病毒将自己隐藏在电子邮件中，随电子邮件扩散到整个网络中。这也是个人计算机被感染的主要途径。

2. 蠕虫病毒感染的对象

蠕虫病毒一般不寄生在别的程序中，而多作为一个独立的程序存在，它感染的对象是全网络中所有的计算机，并且这种感染是主动进行的，所以总是让人防不胜防。在现今全球网络高度发达的情况下，一种蠕虫病毒在几个小时之内蔓延全球并不是什么困难的事情。

现在流行的蠕虫病毒主要有尼姆达、红色代码、冲击波、震荡波、求职信以及 2007 年流行的熊猫烧香。本书以冲击波（Worm. Blaster）和熊猫烧香为例来讲解蠕虫病毒的危害以及如何清除。

3. 冲击波病毒的介绍

病毒运行时会不停地利用 IP 扫描技术寻找网络上系统为 Windows 2000 或 Windows XP 的计算机，找到后就利用 DCOM RPC 缓冲区漏洞攻击该系统，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，使系统操作异常、不停重启，甚至导致系统崩溃，如图 5.8 所示。另外，该病毒还会对微软的一个升级网站进行拒绝服务攻击，导致该网站堵塞，使用户无法通过该网站升级系统，该病毒还会使被攻击的系统丧失更新该漏洞补丁的能力。

图 5.8　冲击波病毒的症状

4. 冲击波病毒的防范与查杀

（1）用户可以先进入微软网站，下载相应的系统补丁，给系统打上补丁，每个 Windows 都有相应的版本，下面是一个 Windows XP 32 位版本的下载补丁地址：

```
http://microsoft.com/downloads/details.aspx?FamilyId=2354406C.C5B6.44AC.9532.
3DE40F69C074&displaylang=en
```

(2) 病毒运行时会建立一个名为 BILLY 的互斥量,使病毒自身不重复进入内存,并且病毒在内存中建立一个名为 msblast 的进程,用户可以用任务管理器将该病毒进程终止。

(3) 病毒运行时会将自身复制为%systemdir%\msblast.exe,用户可以手动删除该病毒文件。

注意:%Windir%是一个变量,它指的是操作系统安装目录,默认是"C:\Windows"或"c:\Winnt",也可以是用户在安装操作系统时指定的其他目录。%systemdir%是一个变量,它指的是操作系统安装目录中的系统目录,默认是"C:\Windows\system"或"c:\Winnt\system32"。

(4) 病毒会修改注册表的 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 项,在其中加入"windows auto update"="msblast.exe"进行自启动,用户可以手工清除该键值。

(5) 病毒会用到 135、4444、69 等端口,用户可以使用 Windows 防火墙软件将这些端口禁止,或者使用"TCP/IP 筛选"功能禁止这些端口。

(6) 也可以使用瑞星专杀工具来进行查杀,图 5.9 就是一款 RPC 漏洞蠕虫专用查杀工具。

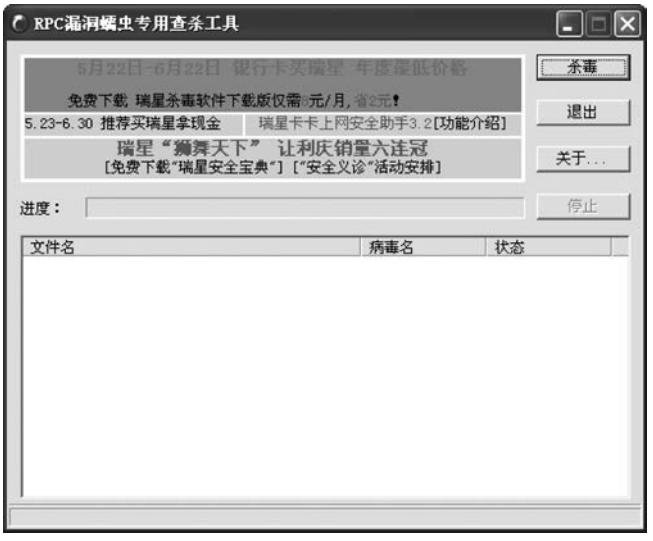

图 5.9 RPC 漏洞蠕虫专用查杀工具

5. 熊猫烧香病毒

熊猫烧香(Worm.Nimaya)又称武汉男生或者尼姆亚,是一种蠕虫病毒。它是一个由 Delphi 编程工具编写的程序,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,IE 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

功能来运行，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。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。这是中国近些年来发生的比较严重的一次蠕虫病毒，影响很大，也造成了很大的损失，图 5.10 列出了被熊猫烧香病毒感染后的文件图标。

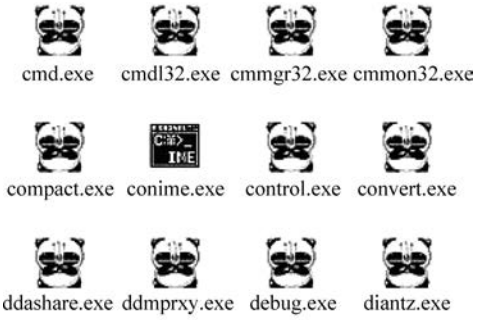

图 5.10　被熊猫烧香病毒感染后的文件图标

6. 熊猫烧香病毒的防范

（1）安装杀毒软件，并在上网时打开网页实时监控。

（2）网站管理员应该更改机器密码，以防止病毒通过局域网传播。

（3）当 QQ、UC 的漏洞已经被该病毒利用时，用户应该去相应的官方网站打好最新补丁。

（4）该病毒会利用 IE 浏览器的漏洞进行攻击，因此用户应该给 IE 打好所有的补丁。如果必要的话，用户可以暂时换用 Firefox、Opera 等比较安全的浏览器。

7. 熊猫烧香病毒的清除

如果中了熊猫烧香病毒，可以采取以下步骤来对它来进行清除。

（1）断开网络。

（2）结束病毒进程%System%\FuckJacks.exe。

（3）删除病毒文件%System%\FuckJacks.exe。

（4）在分区盘符上右击，在弹出的快捷菜单中选择“打开”选项进入分区根目录，删除根目录下的两个文件：X:\autorun.inf 和 X:\setup.exe。

（5）在注册表中删除病毒创建的启动项：

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
"FuckJacks" = " % System % \FuckJacks.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"svohost" = " % System % \FuckJacks.exe"
```

（6）修复或重新安装反病毒软件。

（7）使用反病毒软件或专杀工具进行全盘扫描，清除恢复被感染的.exe 文件。图 5.11 为瑞星公司的熊猫烧香专杀工具。

图 5.11　熊猫烧香专杀工具

5.5.4　WannaCry 勒索病毒的查杀

1. WannaCry 勒索病毒介绍

WannaCry 勒索病毒是一种利用美国国家安全局的“永恒之蓝”(EternalBlue)漏洞,通过互联网对全球运行 Microsoft Windows 操作系统的计算机进行攻击的加密型勒索病毒,它是蠕虫病毒。该病毒利用 AES-128(高级加密标准)和 RSA 算法(非对称加密演算法)恶意加密用户文件以勒索比特币,其加密流程如图 5.12 所示。

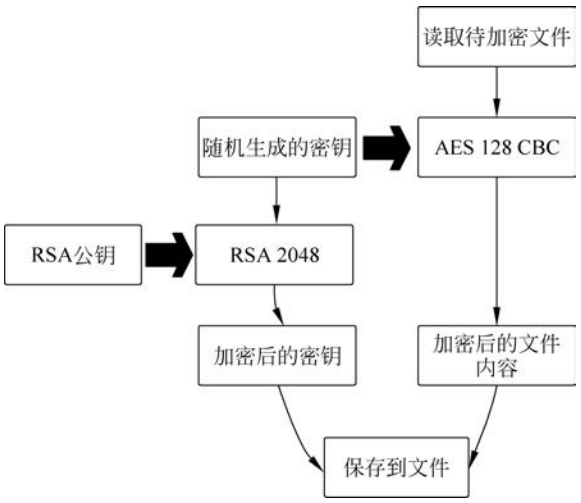

图 5.12　加密流程

2017 年 5 月初,WannaCry 勒索病毒全球大爆发,至少 150 个国家 30 万名用户中病毒,造成的损失高达 80 亿美元,已经影响到金融、能源、医疗等众多行业,造成严重的危机管理问题。中国部分 Windows 操作系统用户遭受感染,校园网用户首当其冲,受害严重,大量实

验室数据和毕业设计被锁定加密。部分大型企业的应用系统和数据库文件被加密后，无法正常工作。WannaCry 勒索病毒是自熊猫烧香病毒以来影响力最大的病毒之一。

微软早在 2017 年 3 月 14 日就推送了更新，封堵了漏洞。没有及时下载这个补丁的 Windows 主机就很可能被感染，如图 5.13 所示，遭受感染后桌面被替换。直到目前为止，没有证据显示攻击者是有目标地进行攻击。还在运行已被微软淘汰的 Windows XP 的主机则非常危险，因为微软早已不对 Windows XP 提供安全更新与支持。但由于此次事件的严重性，微软事后已为部分已经淘汰的系统发布了漏洞修复补丁，Windows XP、Windows Server 2003 和 Windows 8 用户都可从微软官方网站下载修复补丁。但部分腾讯电脑管家用户因补丁遭到屏蔽而未能接受到安全更新，事后据官方回应，部分第三方修改系统安装补丁后可能致使蓝屏、系统异常，因此有部分用户补丁被屏蔽。

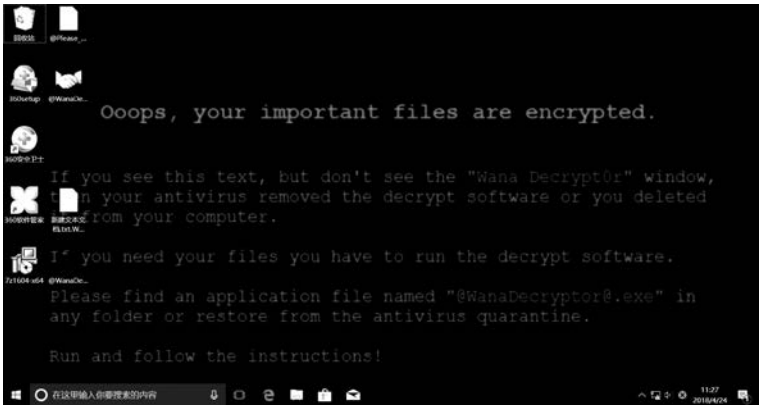

图 5.13　遭受感染后桌面被替换

被 WannaCry 勒索病毒入侵后，用户主机系统内几乎所有类型的文件都将被加密，加密文件的扩展名被统一重命名为.WNCRY，并会在桌面弹出勒索对话框，要求受害者支付 300～600 美元等值的比特币，且赎金金额还会随着时间的推移而增加。如图 5.14 所示，如果单击对话框下方的 Decrypt 按钮，就会弹出如图 5.15 所示的 Decrypt 界面，可以恢复部分已加密的文档。该病毒触发后产生的文件如图 5.16 所示。

2. WannaCry 勒索病毒的防范

若想有效防御此蠕虫病毒的攻击，首先应立即部署微软安全公告 MS17-010 中所涉及的所有安全更新。Windows XP、Windows Server 2003 以及 Windows 8 应根据微软的用户指导安装更新。

当不具备条件安装安全更新，且没有与 Windows XP（同期或更早期 Windows）主机共享的需求时，应当根据微软安全公告 MS17-010 中的变通办法，禁用 SMBv1 协议，以免遭受攻击。虽然利用 Windows 防火墙阻止 TCP 445 端口也具备一定程度的防护效果，但这会导致 Windows 共享完全停止工作，并且可能会影响其他应用程序的运行，应当按照微软公司提供的变通办法来应对威胁。

2017 年 5 月该病毒第一次大规模传播时，署名为 MalwareTech 的英国安全研究员在当时的病毒中发现了一个未注册的域名，主因是病毒内建有传播开关（Kill Switch），会向该域名发

图 5.14　WannaCry 勒索病毒界面

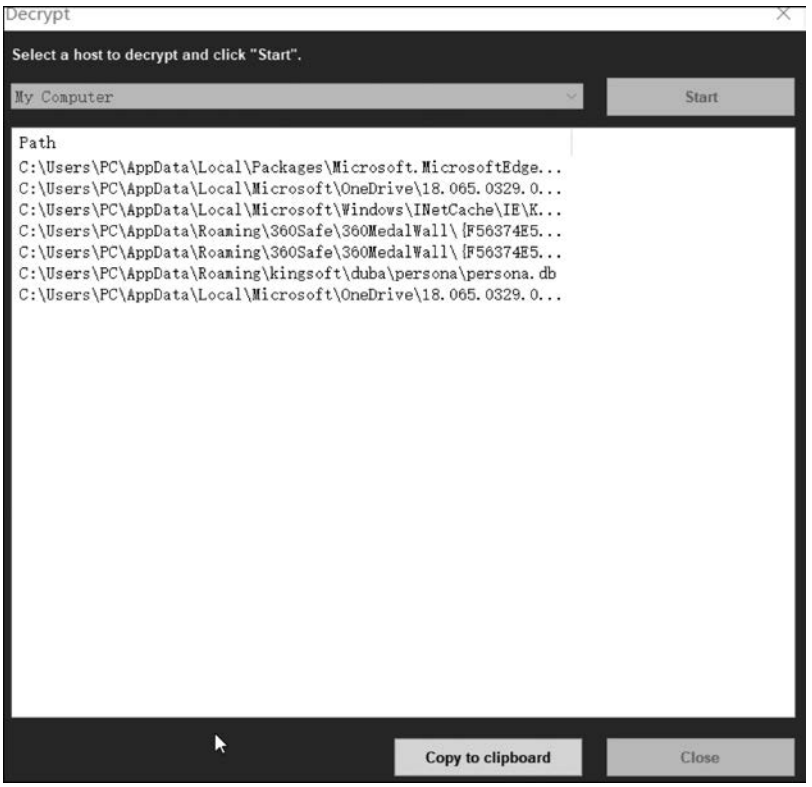

图 5.15　Decrypt 界面

出 DNS 请求,用于测试病毒是否处于防毒软件的虚拟运作环境中。由于该域名并没有设置 DNS,因此正常情况是不会有响应的。若有响应就说明处于虚拟环境下,病毒会停止传播以防被防毒软件清除。这名安全研究员花费 8.29 英镑注册域名后发现每秒收到上千次请求。在

名称	修改日期	类型	大小
msg	2018/4/24 11:21	文件夹	
@Please_Read_Me@	2018/4/24 11:20	文本文档	1 KB
@WanaDecryptor@	2017/5/12 2:22	应用程序	240 KB
00000000.eky	2018/4/24 11:20	EKY 文件	0 KB
00000000.pky	2018/4/24 11:20	PKY 文件	1 KB
00000000.res	2018/4/24 11:24	RES 文件	1 KB
156361524540038.bat.WNCRY	2018/4/24 11:20	WNCRY 文件	1 KB
b.wnry	2017/5/11 20:13	WNRY 文件	1,407 KB
c.wnry	2018/4/24 11:22	WNRY 文件	1 KB
f.wnry	2018/4/24 11:21	WNRY 文件	1 KB
r.wnry	2017/5/11 15:59	WNRY 文件	1 KB
s.wnry	2017/5/9 16:58	WNRY 文件	2,968 KB
t.wnry	2017/5/12 2:22	WNRY 文件	65 KB
taskdl	2017/5/12 2:22	应用程序	20 KB
taskse	2017/5/12 2:22	应用程序	20 KB
u.wnry	2017/5/12 2:22	WNRY 文件	240 KB
wcry	2017/5/13 2:21	应用程序	3,432 KB

图 5.16　WannaCry 勒索病毒触发后产生的文件

该域名被注册后，部分计算机可能仍会被感染，但 WannaCry 的这一版本不会继续传播了 。

然而需要注意的是，在部分网络环境下，例如一些局域网、内部网，或是需要透过代理服务器才能访问互联网的网络，此域名仍可能无法正常连接。另外，现已有报道称该病毒出现了新的变种，一些变种在加密与勒索时并不检查这一域名。

3. 使用 360 安全卫士查杀 WannaCry 勒索病毒

在“360 安全卫士”界面中选择“木马杀毒”页面，选择“全盘扫描”选项开始扫描。在扫描的过程中会提示有问题的危险项，如图 5.17 所示。

图 5.17　360 安全卫士查杀 WannaCry 勒索病毒

扫描病毒结果如图 5.18 所示,发现一个危险项 Worm.Win32.WannaCrypt.J,单击“一键处理”按钮或“立即处理”按钮即可清除病毒;也可以单击病毒查看病毒详情,如图 5.19 所示。

图 5.18 360 安全卫士扫描病毒结果

图 5.19 查看病毒详情

4. 被 WannaCry 勒索病毒感染后的文件恢复

该病毒会读取源文件并生成加密档，直接对源文件进行删除操作。2017 年 5 月 19 日，安全研究人员 Adrien Guinet 发现病毒用来加密的 Windows API 存在的缺陷，在非新版操作系统(Windows 10)中，所用私钥会暂时留在内存中而不会被立即清除。他开发并开源了一个名为 Wannakey 的工具，Wannakey 是专用于 Windows XP 系统的勒索病毒文件恢复工具，前提是该计算机在感染病毒后并未重启，且私钥所在内存还未被覆盖。后有开发者基于此原理开发了名为 wanakiwi 的软件，使恢复过程更加自动化，并确认该方法适用于运行 Windows XP 至 Windows 7 时期的多款 Windows 操作系统。一些安全厂商也基于此原理或软件开发并提供了图形化工具，图 5.20 是 360 安全卫士的功能大全。

图 5.20　360 安全卫士的功能大全

5. 使用 360 安全卫士恢复被 WannaCry 勒索病毒感染的文件

360 安全卫士提供了一个应对这种病毒的工具，在如图 5.20 所示的 360 安全卫士的功能大全界面的“数据安全”下，有一个工具能够恢复被 WannaCry 勒索病毒加密的文件，这个工具称为“WannaCry 勒索病毒文件恢复 V2”，如图 5.21 所示。

打开“WannaCry 勒索病毒文件恢复 V2”，单击“扫描”按钮后扫描全盘被 WannaCry 勒索病毒加密的文件，等待扫描结果，如图 5.22 所示。

扫描完成后选择目录，并单击“确定”按钮，即可将恢复的文件存储在该文件目录，如图 5.23 和图 5.24 所示。

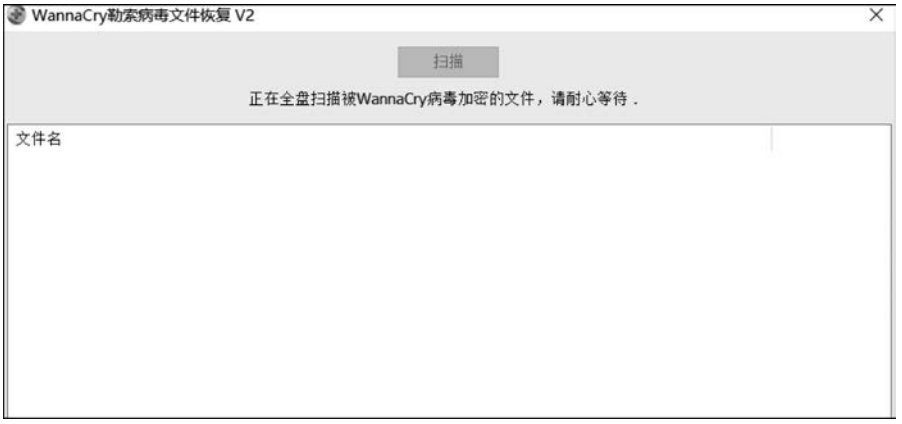

图 5.21　WannaCry 勒索病毒文件恢复 V2

图 5.22　扫描结果

图 5.23　选择恢复文件

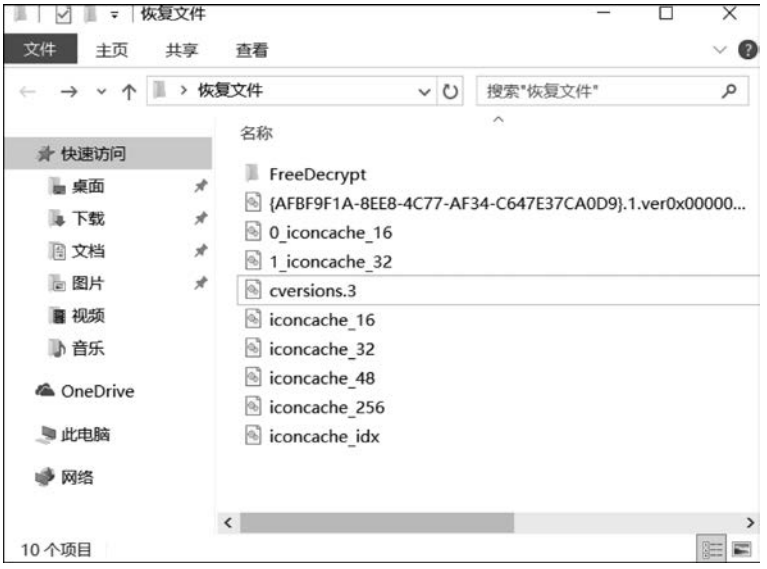

图 5.24　已恢复的文件

5.6　部署企业版杀毒软件

5.6.1　企业版杀毒软件概述

防病毒是网络安全中的重中之重。网络中个别客户端感染病毒后，在极短的时间内就可能感染整个网络，造成网络服务中断或瘫痪，所以局域网的防病毒工作非常重要。最常用的方法就是在网络中部署企业版杀毒软件，比如 Symantec AntiVirus、趋势科技与瑞星的网络版杀毒软件等。本节重点讲解 Symantec 公司推出的新一代企业版网络安全防护产品，Symantec Endpoint Protection(端点保护)。它将 Symantec AntiVirus 与高级威胁防御功能相结合，可以为笔记本电脑、台式机和服务器提供安全防护能力。它在一个代理和管理控制台中无缝集成了基本安全技术，不仅提高了防护能力，而且还有助于降低总拥有成本。Symantec Endpoint Protection 服务器端在安装过程中至少需要 12GB 的硬盘空间，如果空间不足，将导致失败。

1. 主要功能

- 无缝集成一些基本技术，如防病毒与反间谍软件、防火墙、入侵防御和设备控制。
- 只需要一个代理，通过一个管理控制台即可进行管理。
- 由端点安全领域的市场领导者提供无可匹敌的端点防护。
- 无须对每个端点额外部署软件即可立即进行 NAC(网络接入控制)升级。

2. 主要优势

- 阻截恶意软件，如病毒、蠕虫、特洛伊木马、间谍软件、恶意软件、bot、0day 威胁和 rootkit。

- 防止安全违规事件的发生,从而降低管理开销。
- 降低保障端点安全的总拥有成本。

新一代 Symantec 安全防护产品主要包括 Symantec Endpoint Protection 和 Symantec Network Access Control(端点安全访问控制)两种。每一种功能都可以提供强大的 Symantec Endpoint Protection Manager(端点保护管理),以帮助管理员快速完成网络安全的统一部署和管理。


课业任务 5-1

课业任务 5-1

WYL 公司采用 Symantec Endpoint Protection 作为安全防护解决方案,网络管理员需要在一台安装 Windows Server 2019 操作系统的计算机上安装 Symantec Endpoint Protection 服务器端软件,然后对其管理的所有客户端进行部署。

下面通过 5.6.2～5.6.5 节分别来讲解服务器端与客户端的安装与部署,完成课业任务 5-1。

5.6.2 安装 Symantec Endpoint Protection Manager

(1) 插入安装光盘,双击光盘根目录下的 Setup.exe 文件,启动安装程序,显示如图 5.25 所示的"Symantec Endpoint Protection 安装程序"窗口。

图 5.25 "Symantec Endpoint Protection 安装程序"窗口

(2) 在图 5.25 所示的窗口中,单击"安装 Symantec Endpoint Protection Manager"按钮,启动 Symantec Endpoint Protection Manager 安装向导,显示如图 5.26 所示的 Symantec Endpoint Protection Manager 安装向导。

(3) 在图 5.26 所示的对话框中,单击"下一步"按钮,显示如图 5.27 所示的"授权许可协议"对话框,选择"我接受该授权许可协议中的条款"单选按钮。

(4) 图 5.27 所示的对话框中,单击"下一步"按钮,显示如图 5.28 所示的"目录文件夹"对话框,单击"更改"按钮可以重新选择安装目录,建议接受默认安装路径。

图 5.26　Symantec Endpoint Protection Manager 安装向导

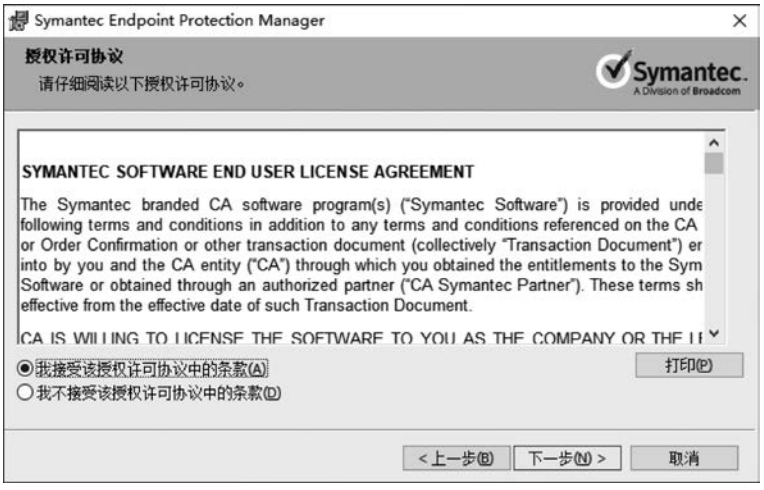

图 5.27　“授权许可协议”对话框

图 5.28　“目录文件夹”对话框

(5) 在图 5.28 所示的对话框中,单击“下一步”按钮,显示如图 5.29 所示的“准备安装程序”对话框,提示安装向导已经准备就绪。

图 5.29 “准备安装程序”对话框

(6) 在图 5.29 所示的对话框中,单击“安装”按钮,即开始安装,需要等待几分钟时间,完成后会再次显示如图 5.30 所示的“管理服务器和控制台安装摘要”对话框。

图 5.30 “管理服务器和控制台安装摘要”对话框

(7) 在图 5.30 所示的对话框中,已经完成 Symantec Endpoint Protection Manager 的安装部分,单击“下一步”按钮将进入 Symantec Endpoint Protection Manager 的“管理服务器配置向导”部分。

5.6.3 配置 Symantec Endpoint Protection Manager

安装 Symantec Endpoint Protection Manager 后,还应该配置 Symantec Endpoint Protection Manager,包括创建服务器组,设置站点名称、管理员密码、客户端安装方式以及制作客户端安装包等,其具体操作步骤如下:

(1) 在图 5.30 所示的对话框中,完成 Symantec Endpoint Protection Manager 的安装部分后,单击“下一步”按钮进入 Symantec Endpoint Protection Manager 的“管理服务器配置向导”部分。默认显示如图 5.31 所示的“管理服务器配置向导”对话框。此处提供“适用于新安装的默认配置(不到 500 个客户端)”和“适用于新安装的自定义配置(超过 500 个客户端,或者自定义设置)”两种配置类型。二者的区别在于“适用于新安装的默认配置(不到 500 个客户端)”是指小于 500 个客户端的情况,并且使用嵌入式数据库,而“适用于新安装的自定义配置(超过 500 个客户端,或者自定义设置)”是指大于 500 个客户端的情况,同时可以使用 Microsoft SQL 数据库。本任务因为企业规模不大,所以选择“适用于新安装的默认配置(不到 500 个客户端)”单选按钮。

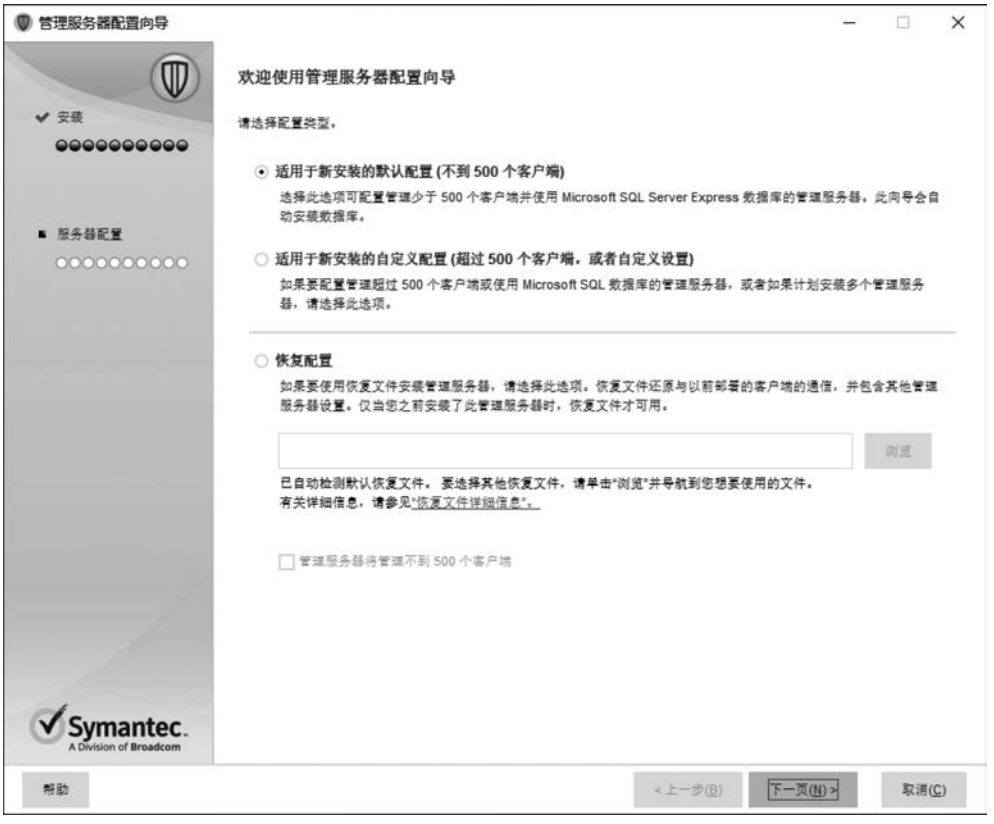

图 5.31　管理服务器配置向导

(2) 在图 5.31 所示的对话框中,单击“下一步”按钮,显示如图 5.32 所示的“创建系统管理员账户”对话框,配置登录 Symantec Endpoint Protection Manager 的用户名与密码和管理员电子邮件地址。

(3) 在图 5.32 所示的对话框中,可以勾选“使用指定的电子邮件服务器”复选框,显示如图 5.33 所示的配置企业电子邮件服务器对话框,设置自己企业的电子邮件 SMTP 服务器。

(4) 在图 5.33 所示的对话框中,单击“下一步”按钮,显示如图 5.34 所示的“合作伙伴信息(可选)”对话框,如果许可证由合作伙伴管理,可输入对应的联系人信息。

图 5.32　创建用户名与密码

图 5.33　配置企业电子邮件服务器对话框

(5) 在图 5.34 所示的对话框中,单击“下一步”按钮,等待系统自动安装 SQL Server 2017 并自动完成数据库创建,如图 5.35 所示。完成数据库部署之后,显示如图 5.36 所示的“已完成配置”对话框,完成 Symantec Endpoint Protection Manager 的配置。

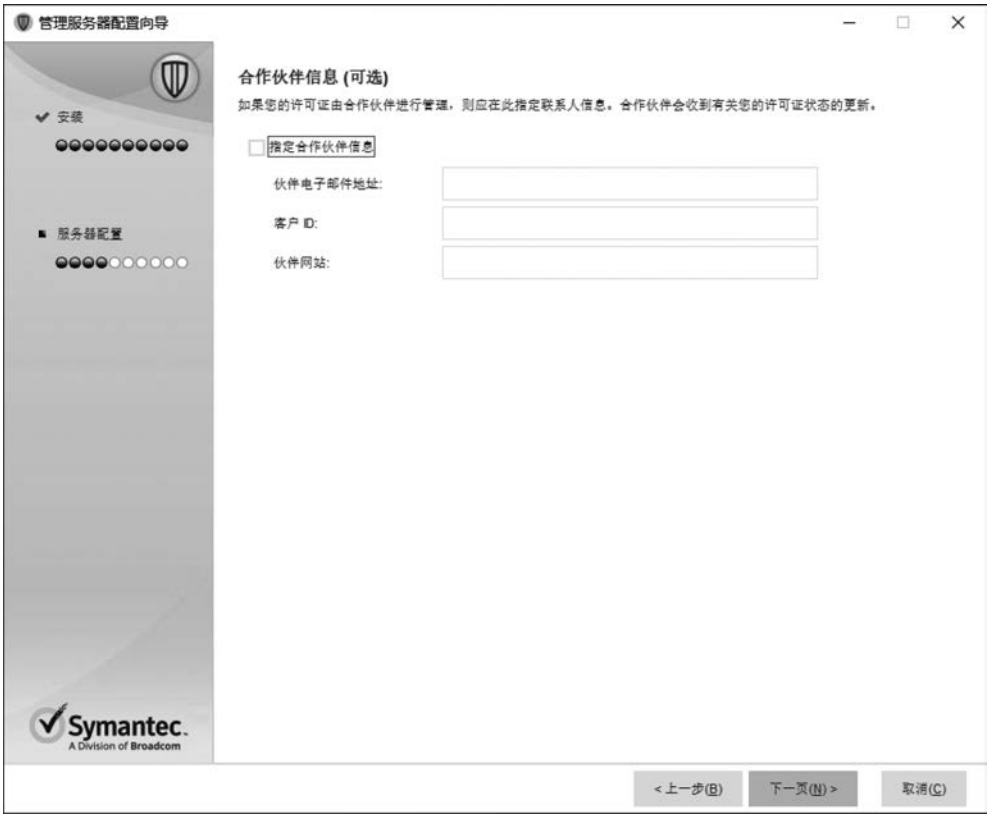

图 5.34　“合作伙伴信息(可选)”对话框

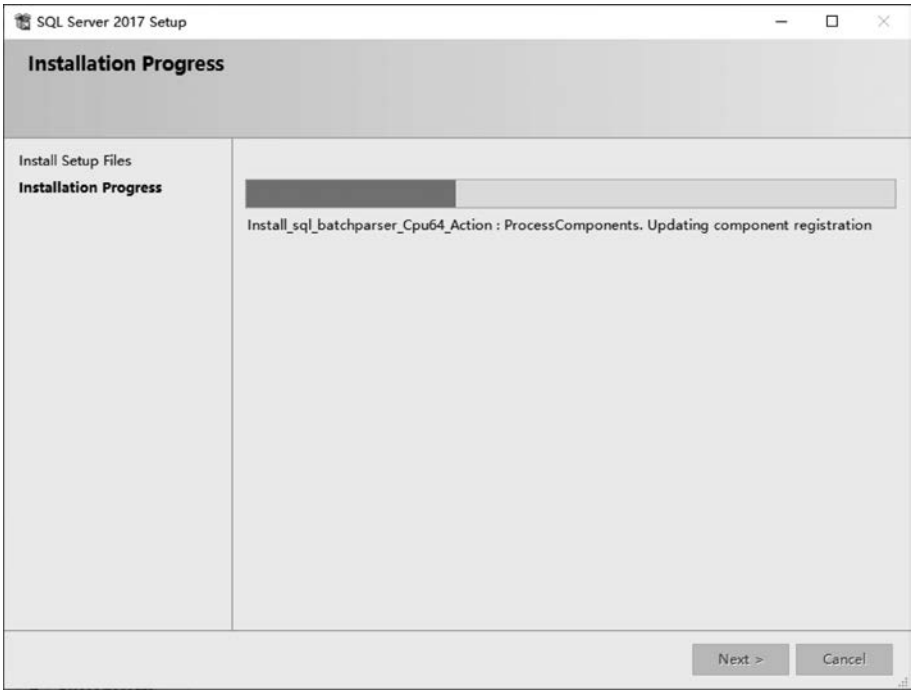

图 5.35　Symantec Endpoint Protection Manager 自动部署 SQL Server 2017

图 5.36 "已完成配置"对话框

5.6.4 客户端本地安装部署

下面介绍客户端的本地安装部署。可以打开 Symantec Endpoint Protection 管理平台开始部署，也可以在浏览器中打开 Symantec Endpoint Protection Web，如图 5.37 所示。

图 5.37 开始部署

(1) 在图 5.37 所示的对话框中，右击"客户端"选项，在弹出的快捷菜单中选择"安装客户端"选项，显示如图 5.38 所示的"选择部署类型"对话框。

(2) 在图 5.38 所示的对话框中，单击"下一步"按钮，显示如图 5.39 所示的"选择组并安装功能集"对话框，可根据需要选择客户端的系统版本(支持 Windows、Mac OS、Linux 客户端，通常情况下保持默认即可)。确认选项无误后单击"下一步"按钮。

(3) 在图 5.39 所示的对话框中，可根据需要选择软件包得安装方式，支持直接生成安装包、通过远程部署准备 Windows 客户端。通过远程安装时，需要启用并启动远程注册表服务，禁用注册表项 LocalAccountTokenFilterPolicy，禁用或删除 Windows Defender 并禁

图 5.38　"选择部署类型"对话框

图 5.39　指定软件包安装方式

用 UAC 远程限制(通常情况下保持默认使用"保存软件包"即可，如图 5.40 所示)。单击"下一步"按钮，显示如图 5.41 所示的"指定软件包的类型"对话框，通常情况下保持默认即可。

(4) 在图 5.41 所示的对话框中，单击"下一步"按钮，显示如图 5.42 所示的"准备保存软件包"对话框，确认将在目标计算机中安装列表中的客户端功能。

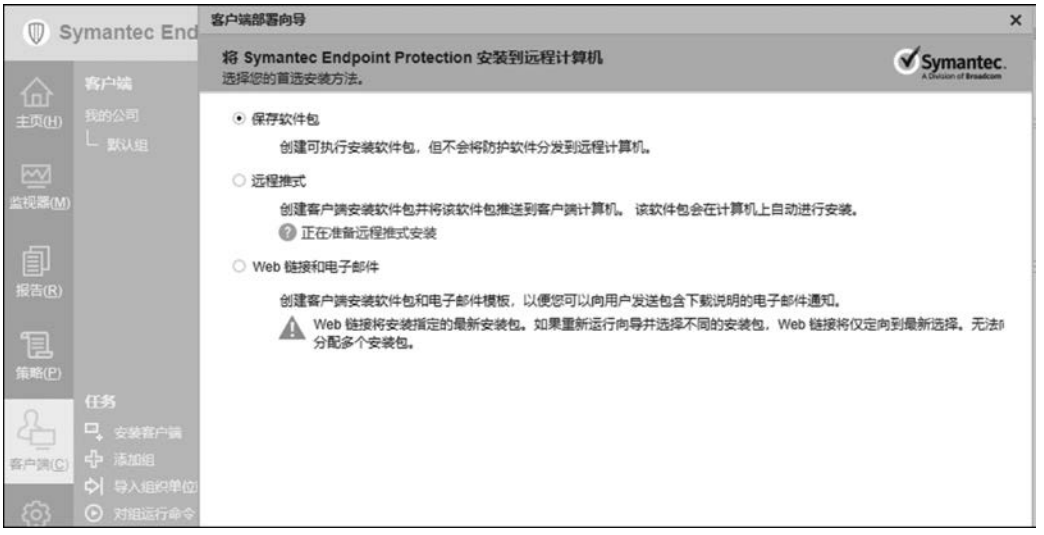

图 5.40 保存软件包

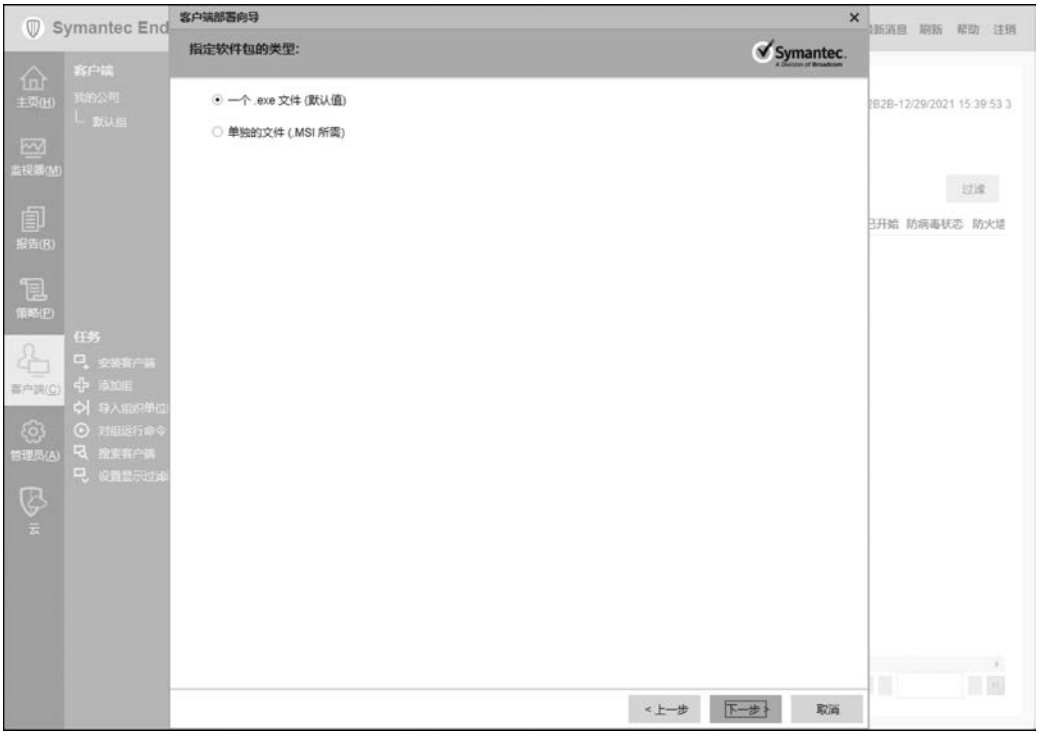

图 5.41 “指定软件包的类型”对话框

(5) 在图 5.42 所示的对话框中,单击“下一步”按钮,显示“正在创建安装文件”对话框,等待几分钟时间后,会显示“成功”对话框。

(6) 如图 5.43 所示,完成“客户端部署向导”对话框,默认情况下将自动下载根据前面设定产生的 Symantec Endpoint Protection Manager 客户端。

图 5.42　"准备保存软件包"对话框

图 5.43　自动下载 Symantec Endpoint Protection Manager 客户端

5.6.5　客户端的远程安装部署

可以打开 Symantec Endpoint Protection 管理平台开始部署，也可以在浏览器中打开 Symantec Endpoint Protection Web，如图 5.44 所示。

(1) 在图 5.44 所示的对话框中，右击左侧的"客户端"选项，在弹出的快捷菜单中选择"安装客户端"选项，如图 5.45 所示。

(2) 在图 5.45 所示的对话框中，根据需要选择客户端的系统安装软件包(支持 Windows、Mac OS、Linux 客户端，通常情况下保持默认即可)。确认选项无误后单击"下一步"按钮。

图 5.44 "欢迎使用客户端部署向导"对话框

图 5.45 安装客户端操作

(3) 在图 5.46 所示的对话框中,可根据需要选择软件包的安装方式,支持直接生成安装包、通过远程部署准备 Windows 客户端。通过远程安装时,需要启用并启动远程注册表服务,禁用注册表项 LocalAccountTokenFilterPolicy,禁用或删除 Windows Defender 并禁用 UAC 远程限制(通常情况下保持默认使用"保存软件包"即可,本案例使用"远程推式"),单击"下一步"按钮,继续安装。

(4) 在图 5.47 所示的对话框中,安装器会自动扫描当前局域网内的所有计算机,如果目标计算机和当前服务器在同一域内,则不需要额外操作,否则需要提供每一台设备的权限,并且打开远程管理服务。如果需要安装的客户端没显示在列表内,可以在如图 5.48 所示的"搜索网络"对话框中,手动指定目标计算机的 IP 地址。

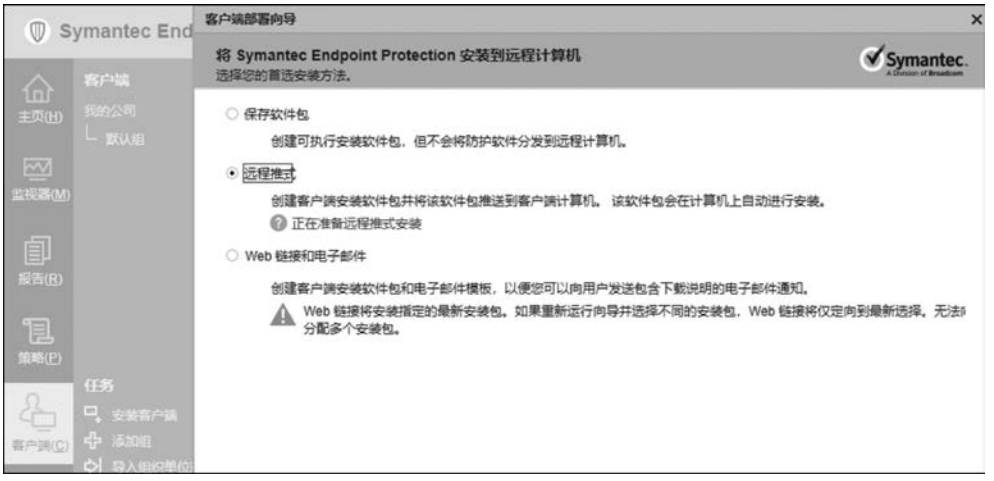

图 5.46　指定软件包安装方式

图 5.47　选择需要安装的计算机

(5) 在图 5.48 所示的对话框中，单击“确定”按钮，出现如图 5.49 中的提示：“管理服务器无法与远程计算机通信。确保以下任一条件得到满足：Windows Remote Registry 服务在客户端计算机上正运行输入正确的管理员凭据，以在目标计算机上验证客户端。”单击“确定”按钮。

(6) 本课业任务对 WinRM 使用 QuickConfig 进行快速配置。如图 5.50 所示，输入 WinRM QuickConfig，然后输入 Y 进行确认。

(7) 如图 5.51 所示，单击“此电脑”，选择任务栏中的“计算机”→“系统”→“管理”选项。

(8) 在如图 5.52 所示的“计算机管理”窗口中，找到 Remote Registry 并选择启动该服务(该服务默认为禁用状态)，如图 5.53 所示。

(9) 在图 5.53 中，单击“应用”按钮，启动 Remote Registry 服务并设置为自动运行，如图 5.54 所示。图 5.55 所示为启动远程部署工作完成。

图 5.48　手动指定目标计算机的 IP 地址

图 5.49　WinRM 服务未运行

图 5.50　WinRM QuickConfig 快速配置

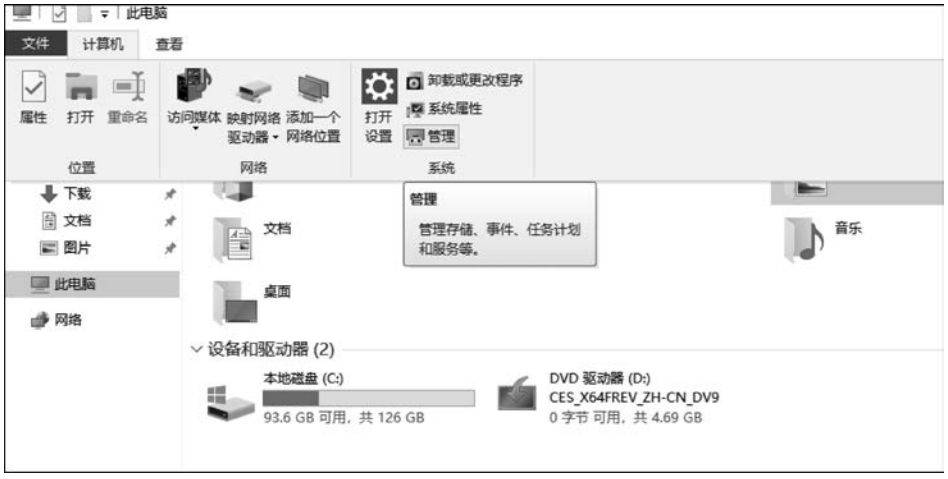

图 5.51　打开服务器管理器

图 5.52　找到 Remote Registry 服务

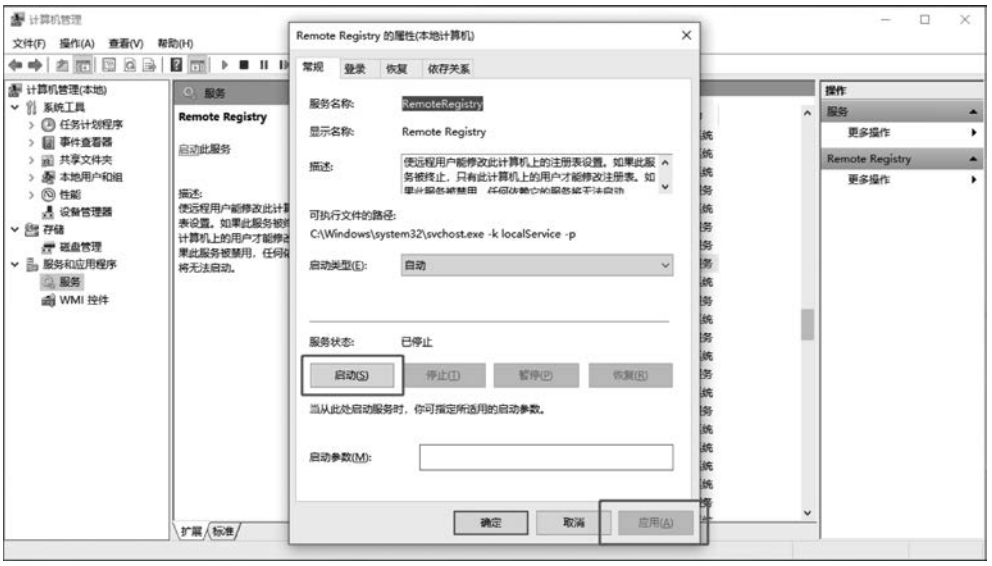

图 5.53　启动 Remote Registry 服务

图 5.54　启动 Remote Registry 服务并设置为自动运行

图 5.55　启动远程部署工作完成

至此,管理服务器上的远程部署工作完成,客户端将开始自动安装,安装完成后将提示用户是否立即重新启动计算机。

5.6.6　设置病毒和间谍软件防护策略


课业任务 5-2

课业任务 5-2

原本设定在凌晨 00:30 的病毒扫描,由于大部分员工都会在下班时关机,WYL 公司管理员决定把原有的扫描策略改成在中午休息时间,在比较少员工使用计算机时进行病毒扫描,并且限制杀毒时间最长不大于 2 小时。

具体操作步骤如下所示。

(1) 在图 5.56 所示的界面中,单击左侧“任务”下的“添加病毒和间谍软件防护策略”选项,显示如图 5.57 所示的“病毒和间谍软件防护策略”,本任务选择“调度扫描”下的“管理员定义的扫描”选项。

(2) 在图 5.57 所示的界面中,单击列表中的“每日调度扫描”,然后选择下方的“编辑”选项,显示如图 5.58 所示的“编辑调度扫描”对话框。

(3) 在图 5.58 所示的界面中,填写任务的说明,然后在下方的“扫描类型”下拉菜单中选择“活动扫描”选项后,选择“调度”选项卡,如图 5.59 所示。

(4) 在图 5.59 所示的界面中,选择执行任务的时间,为了避免影响下午工作正常使用计算机,取消勾选“错过的扫描调度”下的“在以下时间内重试扫描”复选框。完成全部设置后单击“确定”按钮保存所做的更改。

图 5.56　设置病毒和间谍软件防护策略 1

图 5.57　设置病毒和间谍软件防护策略 2

(5) 在图 5.60 所示的界面中，单击“是”按钮，对刚才设置的策略进行分配。

(6) 在图 5.61 所示的界面中，勾选“我的公司”复选框，然后单击“分配”按钮，并且单击“是”按钮确认对已设置的策略进行分配。

5.6.7　升级病毒库

杀毒软件是根据提取的病毒特征来确定文件是否是病毒程序的，升级病毒库是不断地更新能够识别的病毒库特征，增强杀毒软件与系统应用程序之间的兼容性。通常情况下，非受管客户端每天从 Symantec LiveUpdate 站点下载病毒库。在新一代 Symantec 安全防御系统中，新增了 LiveUpdate 管理服务器，主要为大型网络提供客户端病毒库升级管理。

图 5.58　“编辑调度扫描”对话框

图 5.59　编辑调度时间

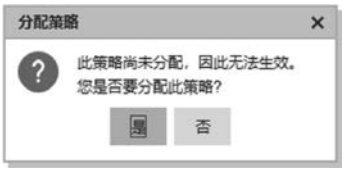

图 5.60　分配病毒和间谍软件防护策略

图 5.61　选择分配策略的组或者位置

练习题

1. 单项选择题

(1) 计算机病毒是(　　)。

A. 编制有错误的计算机程序

B. 设计不完善的计算机程序

C. 已被破坏的计算机程序

D. 以危害系统为目的的特殊的计算机程序

(2) 以下关于计算机病毒的特征说法正确的是(　　)。

A. 计算机病毒只具有破坏性,没有其他特征

B. 计算机病毒具有破坏性,不具有传染性

C. 破坏性和传染性是计算机病毒的两大主要特征

D. 计算机病毒只具有传染性,不具有破坏性

(3) 计算机病毒是一段可运行的程序,它一般(　　)保存在磁盘中。

A. 作为一个文件　　B. 作为一段数据

C. 不作为单独文件　　D. 作为一段资料

(4) 下列措施中,(　　)不是减少病毒的传染和造成的损失的好办法。

A. 重要的文件要及时、定期备份,使备份能反映出系统的最新状态

B. 外来的文件要经过病毒检测才能使用,不要使用盗版软件

C. 不与外界进行任何交流,所有软件都自行开发

D. 定期用抗病毒软件对系统进行查毒、杀毒

(5) 下列说法中,正确的有(　　)。

A. 计算机病毒是磁盘发霉后产生的一种会破坏计算机的微生物

B. 计算机病毒是患有传染病的操作者传染给计算机,影响计算机正常运行

C. 计算机病毒是有故障的计算机自己产生的、可以影响计算机正常运行的程序

D. 计算机病毒是人为制造出来的、干扰计算机正常工作的程序

(6) 计算机病毒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。此特征为计算机病毒的(　　)。

A. 潜伏性　　B. 传染性　　C. 欺骗性　　D. 持久性

(7) 计算机病毒的主要危害有(　　)。

A. 损坏计算机的外观　　B. 干扰计算机的正常运行

C. 影响操作者的健康　　D. 使计算机腐烂

2. 填空题

(1) Office 中的 Word、Excel、PowerPoint、Viso 等很容易感染(　　)病毒。

(2) (　　)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。

(3) 冲击波和震荡波都是属于(　　)病毒。