网络安全

安全技巧（七）

小未 主编

目　录

2001 年回顾：部分主流杀毒软件点评

随着电脑病毒、黑客程序的肆意猖獗，人们电脑网络安全意识的普及和提高，杀毒软件市场出现了空前的热胀，不管是个人用户，还是单位用户，都在不得已的情况下至少备有一个较新的杀毒软件和一个防火墙产品，有的为了更放心在电脑中安装了好几个同类产品，以保护自己的电脑及资源不被病毒破坏。加上现在正版软件的价格总体上在向盗版靠拢（前一段时间正版“金山毒霸”才买 5 元钱一份，与盗版一样），各用户为了更加放心一般来说是选择了正版杀毒软件，所以正版杀毒软件市场也出现前所未有的好景气。

这带动许多软件开发商开始向杀毒软件进行周边辐射，开发出新的品牌杀毒软件，如金山软件公司的“金山毒霸”、洪恩软件公司的“洪恩盾牌”等。面对如此眼花缭乱的杀毒软件市场，不要说是新用户，就是电脑高手也会在这纷纷嚷嚷的杀毒软件广告中迷失方向，无所适从。下面我就对 2001 年的部分主流杀毒软件作一下横向综合对比，希望能对各位用户在选择杀毒软件时起到抛砖引玉的作用。

一、北京新江民科技公司的 KV3000

相信绝大多数电脑用户都对“KV”系列的杀毒软件有过耳闻，甚至一直用在今天。它们就是北京江民新科技有限公司的产品，从 KV300 系列到 KV300+系列，再发展到今天的 KV3000 系列。KVW3000 是基于 Windows 95/98/NT/2000 平台上的纯 32 位反病毒软件，同时它

提供了 WIN98 的 DOS 模式下的软件盘版，是 KV 系列软件中的一个新的系列产品，它一改过去用字母来表示版本号，如过去的 KV300M、KV300N 等，现在是用通常的数字作为版本号，如我所用的是 4.12 版。

<一>、主要特点及优点

江民公司的 KV 系列杀毒软件给我一直以来的印象就是界面非常朴素，就是到了现在的 KV3000 系列也不例外，这与当前各主流杀毒软件非常华丽、漂亮的界面大相径庭，它的主界面如下图 1 所示（4.12 版）

图 1

这是 KV3000 系列在 Windows 环境中的主界面，它在 WIN98 系统 DOS 模式下的界面与我们原来看到的 KV300 系列 DOS 下的界面差不多。它的主要特点及优点如下：

1、KV3000 系列软件可以搜寻和清除的病毒数较

多，达 1 万种以上，包括文件型病毒、引导区病毒、特洛伊木马、黑客程序、网络蠕虫等，特别是对清除一些较早出现的病毒，DOS 下的病毒、CIH 病毒、修复因 CIH 病毒损坏的硬盘方面有特殊效果；

2、KV3000 系列软件可以识别多种压缩软件，如 ZIP、ARJ、CAB、LZH、RAR 等，也可以识别多种可执行程序的压缩格式，如 PKLITE、LZEXE、WWPACK、ASPACK、UPX 等，让那些隐藏极深的病毒也不得不原形毕漏，这比原来的 KV300 系列软件有明显的加强。

3、KV3000 软件可搜寻到夹带在 Email 中的病毒，同时支持 FoxMail、OutLook 和 Netscape 等常见的 Email 软件生成的信箱格式，但功能不强，不能实现自动查杀，更不能实现金山毒霸所说的“空中拦截”。

4、可以提供安全病毒清除（就是在清除前提醒用户，由用户作出选择）和系统灾难恢复功能，可以为用户提供备份和恢复硬盘主引导记录（MBR）和 C 盘引导扇区（Boot），菜单选项如图 2 和图 3 所示。

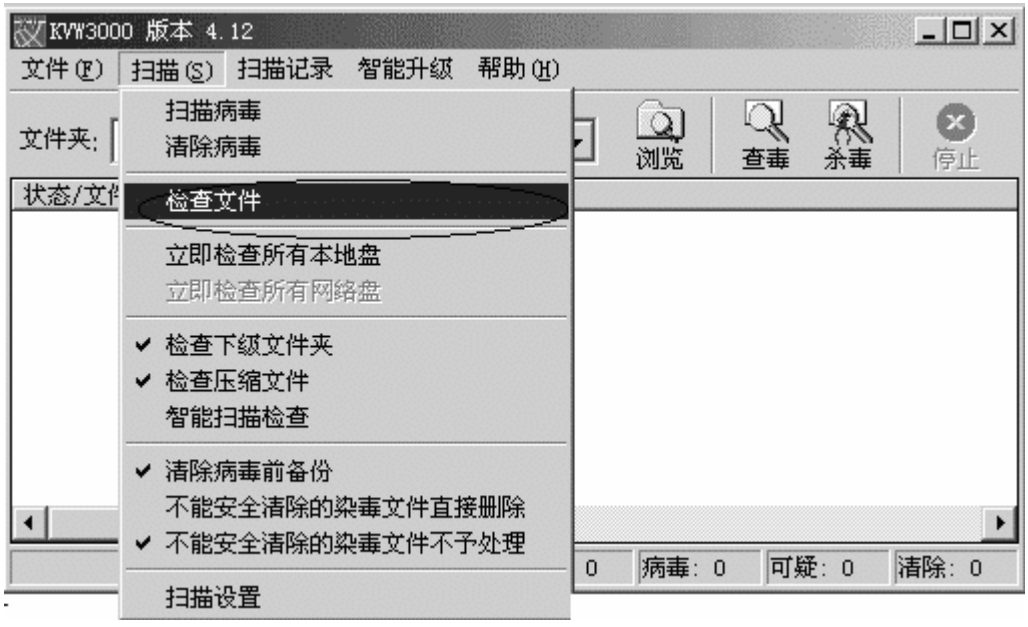

图 2

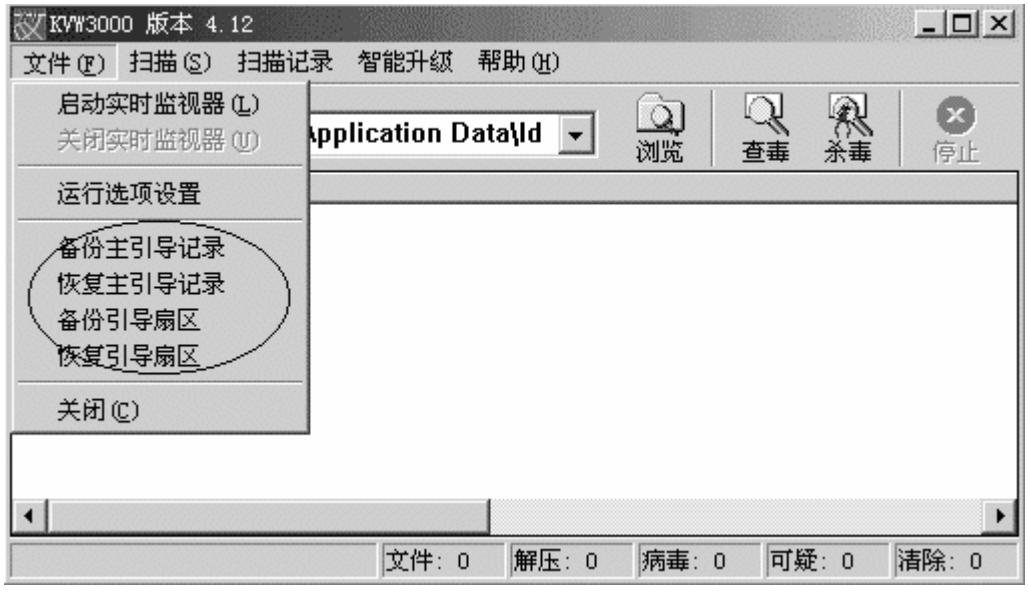

图 3

5、可以对单个文件进行扫描，按如图 4 **菜单所示进**

行。

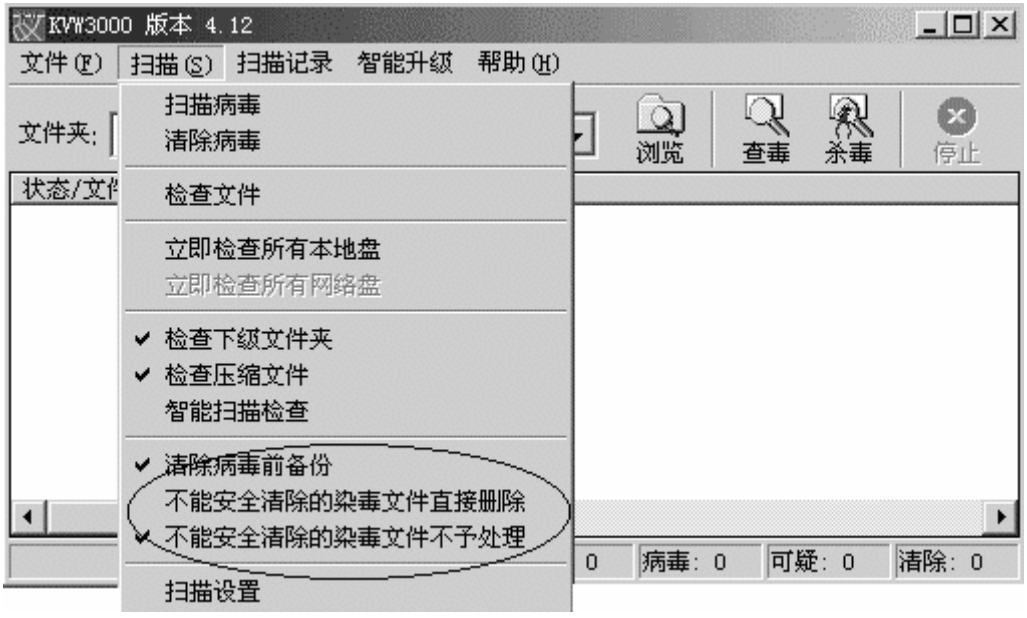

图 4

<二>主要不足之处

KV3000 系列虽然是江民科技这样的老牌杀毒软件开发商开发的最新系列软件，版本也一直在不断更新，但我总觉还有许多不那么令人满意的地方。主要体现在以下几个方面（仅属个人看法，下同）：

1、界面过于老土

虽然我们用软件不是主要在乎其外观界面是否美观，但人总是追求美的一面，有漂亮的外观总好过没有，就象人也一样，也与当今所有软件市场背道而驰，就连微软件都在这方面特别注重（不管它的那一个软件）！

2、占用系统资源太多

我用 KV3000 最为直觉的感觉就是占用系统资源太多，使用它时我的鼠标只能进行慢动作了。后来我的内

存加到了 192M，用了它之后再打开 OUTLOOK 还是显得有点慢了，不光我有这样的感觉，其他朋友都有！

3、功能不是很全面

在功能方面我始终认为江民公司的 KV 系列一直以来没有什么太大的改变，如在 E-mail 邮件病毒跟踪、OFFICE 宏病毒扫描方面比起其它杀毒软件在此方面表现有些原始。

4、它提供的加密启动软盘太容易损坏，损坏后需到经销商那些花钱去换，比较麻烦！

二、北京冠群金辰软件公司的 KILL98 5.0

KILL 系列也是老用户耳熟能详的老牌杀毒软件系列，但是近几年我总觉北京冠群金辰在此方面的投入不是很多，不光表现在广告投入，就是在版本升级方面都明显跟不上时代的步伐了，这不，它现在用回了几年前的 KILL98 系列。KILL98 5.0 的主界面如下图 5 所示

图 5

它是一个 WIN9X 系统下的杀毒软件，但 KILL 系列也有相应的 NT、WIN2K 系统版本，下面就 KILL98 5.0 这个版本的 KILL 软件作一下说明。

<一>、主要特点及优点

虽然 KILL 系列软件目前在某些方面跟不上市场的步伐，但毕竟是老牌的合资公司的产品，不是有“瘦死的骆驼比马大“这样一句古话吗，它的存在当然也有它存在的理由，也有它的特点和过人之处，主要表现在如下几个方面：

1、可以同进对文件或文件夹进行扫描，不象 KV30

00 一样扫描文件夹和扫描文件需用不同的途径来达到，比较方便。

2、各项主要功能在主界面中以按钮的形式列示出来，非常直观，让用户一看就知道该软件主要有些有途，参见上图 5。

3、可以为用户创建系统急救盘，以防用户不小心在清除病毒时误删了一些文件而引起系统不能正常启动，则可用系统急救盘对系统进行恢复，KILL98 5.0 为我们提供了创建急救盘的向导，向导主界面见图 6。

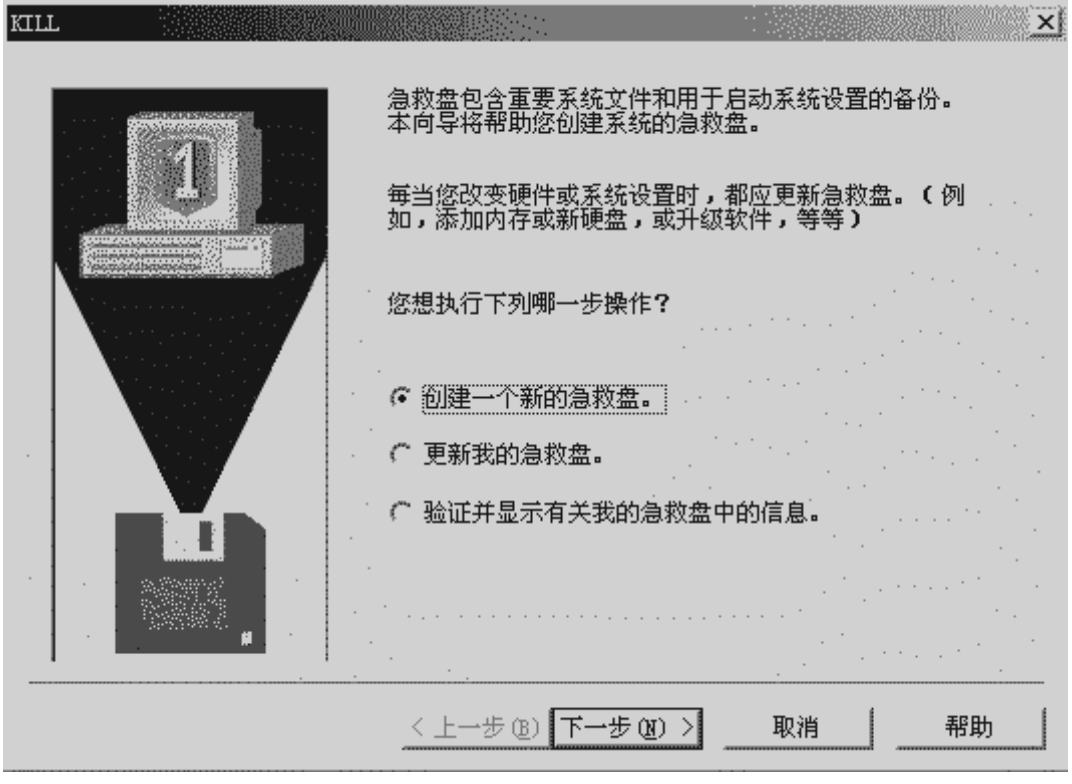

图 6

4、KILL98 5.0 同样为我们准备了详尽的扫描设置选项，但它更为可取的是为了防止别出心裁对自己的设

置进行随便改动，它为用户提供了密码保护功能，如图 7 所示

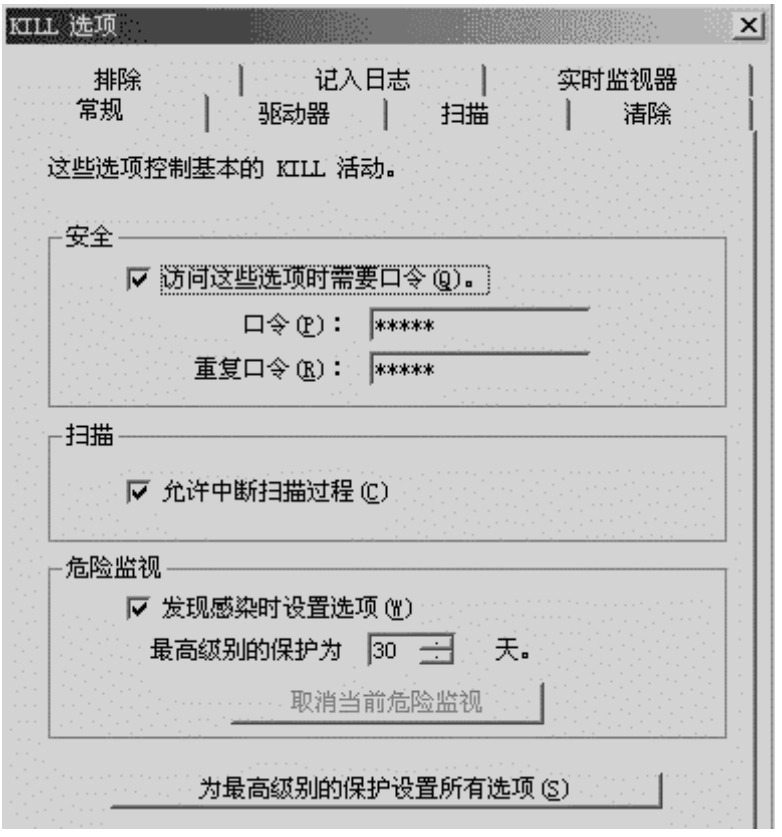

图 7

别人要进入设置选项则先要输入相应的密码才可。

5、可以由用户自由设置不扫描文件的类别、文件夹和文件，大大地增加了扫描的灵活性，在相当多的时候提高了扫描的速度，设置主界面如图 8 所示。

图 8

6、**提供了非常自由的定时扫描功能，它比** KV3000 **的“ 定时扫描 ”设置精确许多，对比图** 9 **和图** 10。

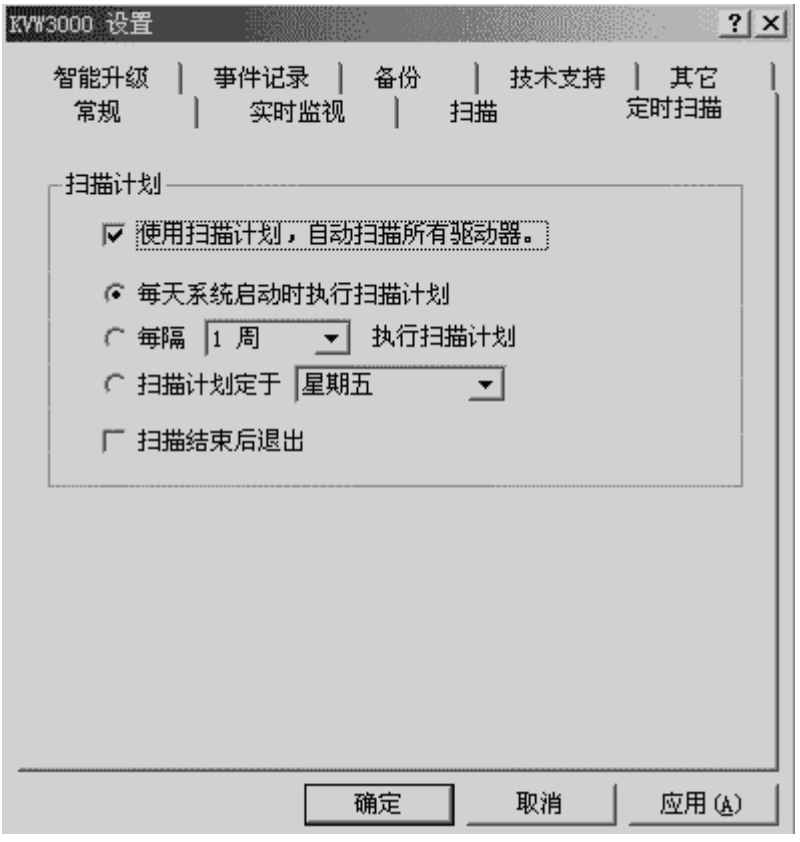
KVW3000 设置
智能升级
事件记录
备份
技术支持
其它
常规
实时监视
扫描
定时扫描
扫描计划
使用扫描计划，自动扫描所有驱动器。
每天系统启动时执行扫描计划
每隔 1 周 执行扫描计划
扫描计划定于 星期五
扫描结束后退出
确定
取消
应用 (A)

图 9

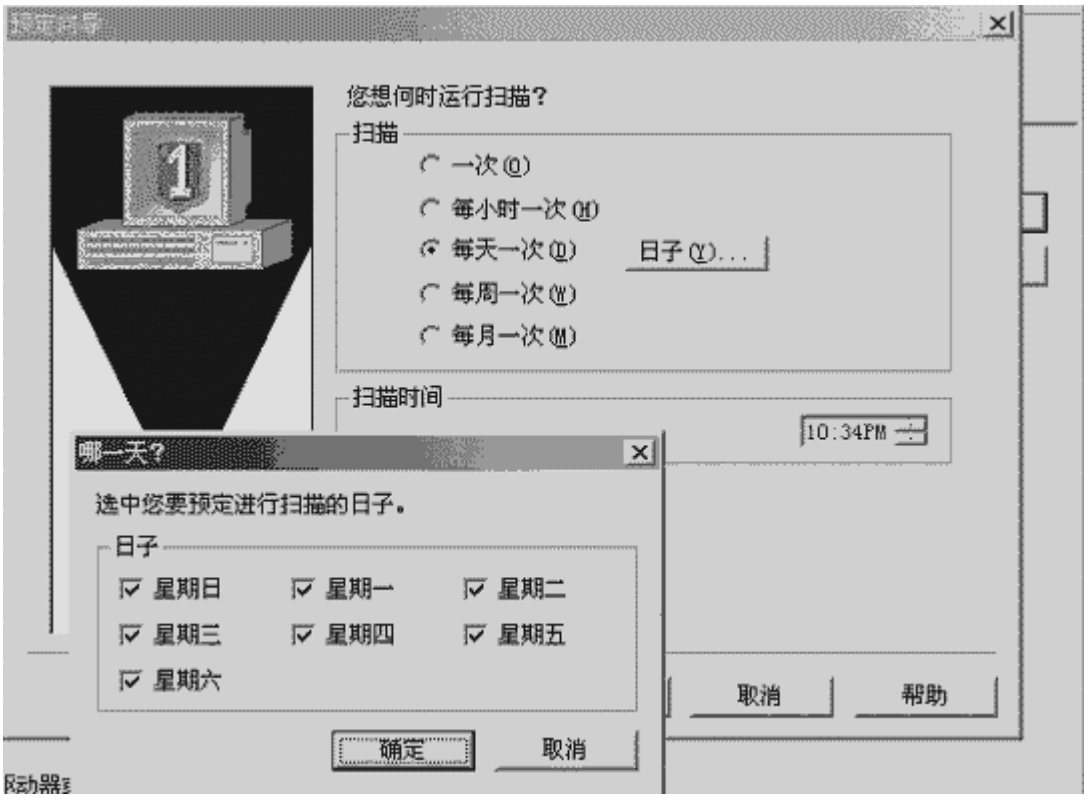

图 10

<二>、主要不足之处

KILL **系列软件也是我用得最多的一个软件，最早用它不知从那一年开始，直到现在的** KILL98 5.0**，它主要不足之处表现在如下几个方面：**

1、扫描速度较慢，全面查杀一个大容量硬盘所花时间近一个小时，用户难到等待；

2、也象 KV3000 **一样，版本虽然升了一次又一次，但新技术方面没有什么多大突破，只不过在病毒库方面进行添加；**

3、界面也较老土，这不知是不是老牌产品的通病，KILL **系列产品的主界面基本上没有什么改变。**

4、扫描功能不全面，比如对邮件病毒、OFFICE 宏病毒方面有所欠缺。

三、诺顿公司的 Norton Antirus 系列

诺顿公司的 Norton Antirus 系列相信新老用户都并不陌生，在杀毒软件市场享有相当高的盛名，特别是在外资或合资企业中，因为它是一个洋品牌，它是由美国 Symantec 公司的产品，在 2001 年它的主要产品有 Norton Antirus 2001 和 Norton Antirus 2002，作为一个非常出名的洋品牌，在国内软件价格竞争如此激烈的今天仍能占稳江山，Symantec 公司肯定有它过人之外，的确如此，经过我对 Norton Antirus 2001 试用一段时间后深有感触，下面我就仅就 Norton Antirus 2001 来谈谈它的主要特点及优点。

1、这个品牌是一个洋品牌，以前多为英文版，但 Symantec 公司为了抢占中国客户，在近两年所开发的软件中多数都进行了汉化，满足了中国市场的需求。它的病毒库较大，可以查杀 47554 种病毒，属较大的一种。

2、它的界面开始进行了较大的改观，不再是原来灰白单一的格调，另外各主要界面都采用了类似微软件的资源管理器的格局，非常直观、明了，它的主界面如图 11 所示。

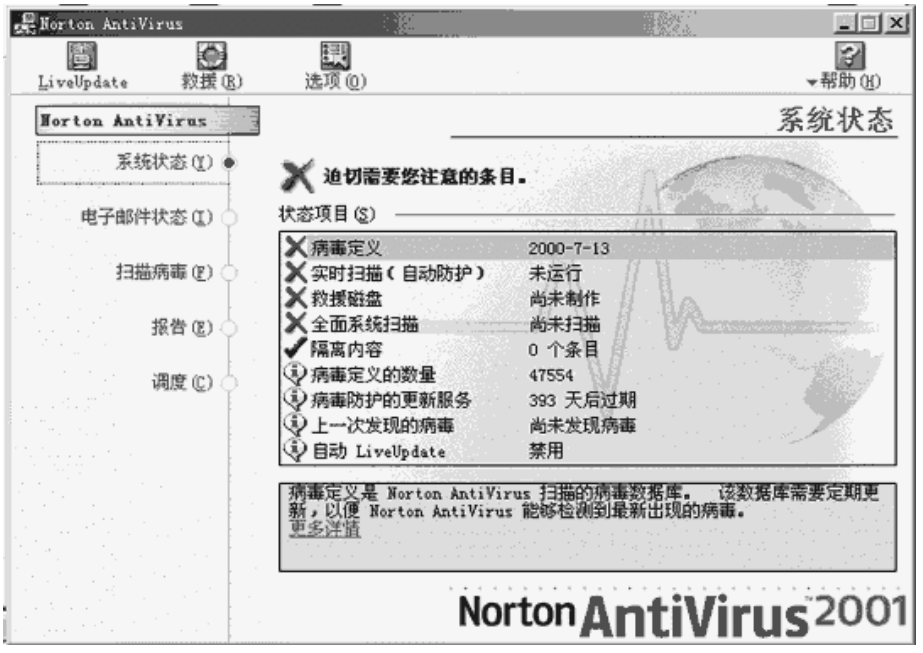

图 11

3、在这个版本中它成功地引入了疫苗新技术，如在你的硬盘经过扫描后，确定没有感染病毒，Norton Anti Virus 会为引导记录接种疫苗，确保它们不会被病毒感染。接种疫苗后，Norton AntiVirus 将在一个专门用于存储疫苗数据的特定文件中记录它的重要信息（类似于取指纹），在以后的扫描中，只需比较当前的指纹和它所存储的指纹，如果出现了任何变化，都会向你发出警报，因为这说明可能出现了病毒。作为 Norton AntiVirus 安装的组成部分，引导记录自动接种疫苗。

4、Norton AntiVirus 具有自动防护功能，就是在用户使用可执行文件、文档和文档模板文件时，它自动对这些文件进行扫描，并可对 WORD 的宏病毒进行自动扫描。除了可以检查文件中已知的病毒外，自动防护还可

以利用 Bloodhound 技术并对具有病毒特征的活动进行监视，这样可以确保未知的病毒也不能感染你的计算机，更不能在正常操作过程中破坏你的数据。

5、Norton AntiVirus 具有高成功率地检测未知病毒能力，Norton AntiVirus 是利用高级的启发式技术——Bloodhound，可检测未知病毒和宏病毒。Bloodhound 隔离且查找文件的各种逻辑区域，且为类似病毒活动习性分析程序逻辑。除此之外，Norton AntiVirus 可通过监视病毒典型的活动特征来检测病毒。当发现可疑病毒时，Norton AntiVirus 将阻止病毒继续活动，从而保护你的电脑。

6、具有启动扫描功能，它能在每次启动计算机时自动执行的特殊扫描，这种扫描会查找可能感染重要文件和启动记录的病毒。

7、可以为系统设置多种个性化的自动扫描计划，在 Norton AntiVirus 就叫做设置扫描调度计度，如图 12 所示。