第二章　系统安全防护工具

计算机网络普及和迅猛发展，为用户工作和生活带来无限方便和快捷。然而，病毒互联网化趋势已经凸显，各种盗号木马、恶意病毒、浏览器插件、网站与系统漏洞层出不穷，这些隐藏在用户身边陷阱时时刻刻威胁着计算机安全。

第二章　系统安全防护工具

2.1　计算机病毒与木马

《中华人民共和国计算机信息系统安全保护条例》明确指出：“计算机病毒，是指编制或者在计算机程序中插入破坏计算机功效或者毁坏数据，影响计算机使用，并能自我复制一组计算机指令或者程序代码。”

木马，英文叫做“Trojan house”，其名称取自希腊神话特洛伊战争中著名“木马记”，它是一个含有伪装潜伏功效一段程序。这类程序从表面上看与其它程序没有什么特殊地方，但主要经过与其它文件捆绑，或伪装成系统文件来到达隐藏自己，窃取用户信息目标。

第二章　系统安全防护工具

2.2　计算机病毒、木马特点分析

1．病毒制作机械化

伴随病毒制作分工不停细化，再加上病毒制作工具泛滥，病毒制作者开始按照病毒制造流程制作病毒，由此病毒制造显示出机械化特征。

病毒制作机械化特征，一定程度上得益于制作门槛低和制作工具泛滥。病毒制作者不需要具备任何专业技术知识，只需要依据自己对病毒需求，在对应病毒制作工具中勾选或定制一些功效，便能够轻松生成病毒。

2．病毒制造模块化、专业化

病毒制造者按功效模块进行外包生产或采购技术更为先进功效模块，使得组合起来病毒各个方面都含有很强专业性，这对用户造成极大危害。

3．病毒互联网化

造成病毒数量井喷式暴发最主要原因，是病毒已经互联网化。其实病毒本身在技术上没有本质进步，但病毒制作者充分利用了高效便捷互联网，搭建整合了一个产业链条，使得运作效率大幅提升。

第二章　系统安全防护工具

2.3　病毒防治工具——瑞星全功效安全软件

2.3.1　知识拓展

1．云安全计划

云安全计划就是要将整个互联网变成一个巨大杀毒软件，参加者越多，每个参加者越安全，整个互联网越安全。

2．网页挂马

黑客在某个网页中嵌入一段能够自动下载木马恶意代码，从而利用该代码实施木马植入行为。

第二章　系统安全防护工具

2.3.2　瑞星全功效安全软件安装

2.3.3　瑞星全功效安全软件使用方法

1．开启

正确安装结束后，瑞星会跟随系统自动开启，并在后台保护用户系统。

瑞星全功效安全软件主界面

第二章　系统安全防护工具

2．手动查杀病毒

① 开启瑞星全功效安全软件，单击“杀毒”标签页.

② 在界面左侧“查杀目标”中，勾选需要查杀盘符或文件夹.

③ 在界面右侧，设置当软件发觉病毒时操作反应。

④ 最终单击“开始杀毒”按钮.

⑤ 查杀结束后，扫描结果将自动保留，用户能够经过历史统计来查看以往查杀病毒结果。

手动查杀

查杀过程

第二章　系统安全防护工具

3．空闲时段查杀

① 开启瑞星全功效安全软件，单击“杀毒”标签页.

② 在“杀毒”标签页单击“查杀设置”按钮，此时弹出“设置”对话框。

③ 在“设置”对话框左侧选择“查杀设置”→“空闲时段查杀”选项.

④ 单击“添加”按钮，在弹出对话框中填写相关信息。

⑤ 最终单击“确定”按钮，应用全部设置。

空闲时段查杀

第二章　系统安全防护工具

4．后台查杀与端点续杀

5．智能主动防御

6．病毒隔离区

智能主动防御

病毒隔离区

第二章　系统安全防护工具

2.3.4　瑞星全功效安全软件基本设置

1．自定义白名单

2．云安全设置

① 在软件主界面菜单栏中执行“设置”→“详细设置”命令。

② 在弹出对话框左侧树型目录中选择“其它设置”→“云安全”选项。

③ 勾选“加入瑞星云安全计划”复选框，输入邮箱地址，即可加入云安全计划。

云安全设置