实验 5　火绒安全软件的使用

视频讲解

5.1　实验目的及要求

5.1.1　实验目的

通过实验操作掌握火绒安全软件的安装与基本功能的使用，对安全防御软件原理有一定的了解。能够熟练使用火绒安全软件实现常用的访问控制功能。

5.1.2　实验要求

根据教材中介绍的火绒安全软件的功能和步骤完成实验，在掌握基本功能的基础上，实现日常访问控制，给出实验总结报告。

5.1.3　软件介绍

火绒安全软件是针对互联网 PC 终端设计的安全软件，该软件与 Microsoft 公司合作，适用于 Windows XP、Windows VISTA、Windows 7、Windows 8、Windows 8.1、Windows 10、Windows Server(2003 sp1 及以上)的消费者防病毒软件。

火绒安全软件主要针对杀、防、管、控这几方面进行功能设计，主要有病毒查杀、防护中心、访问控制、安全工具 4 部分功能。由拥有连续 15 年以上网络安全经验的专业团队研发打造而成，特别针对国内安全趋势，自主研发拥有全套自主知识产权的反病毒底层核心技术。

火绒安全软件基于目前 PC 用户的真实应用环境和安全威胁而设计，除了拥有强大的自主知识产权的反病毒引擎等核心底层技术之外，更考虑到目前互联网环境下，用户所面临的各种威胁和困境，有效地帮助用户解决病毒、木马、流氓软件、恶意网站、黑客侵害等安全问题，追求“强悍的性能、轻巧的体量”，让用户能够“安全、方便、自主地使用自己的计算机”。

5.2　基础功能介绍与操作

5.2.1　软件安装流程

(1) 前往火绒官方网站下载软件安装包，网址为 https://www.huorong.cn/。

(2) 运行下载好的安装包。

(3) 选择极速安装,等待安装完成即可(可以根据需要更改安装目录)。软件安装完成后将自动打开运行。火绒安全软件主界面如图 5.1 所示,非常简洁清晰。

图 5.1 火绒安全软件主界面

5.2.2 病毒查杀

火绒病毒查杀能主动扫描在计算机中已存在的病毒和木马威胁。当用户选择了需要查杀的目标,火绒安全软件将通过自主研发的反病毒引擎高效扫描目标文件,及时发现病毒、木马,并帮助用户有效处理并清除相关威胁。

第 1 步:启动扫描。有 3 种模式供用户选择:快速查杀模式是病毒文件通常会感染计算机系统敏感位置,针对这些敏感位置进行快速查杀,用时较少,推荐日常使用;全盘查杀模式是针对计算机所有磁盘位置进行查杀,用时较长,推荐定期使用或发现计算机中毒后进行全面排查;自定义查杀模式是可以指定磁盘中的任意位置进行病毒扫描,完全自主操作,有针对性地进行扫描查杀,推荐在遇到无法确定部分文件安全时使用。查杀模式选择如图 5.2 所示。

第 2 步:发现威胁。当火绒安全软件在扫描中发现病毒时,会实时显示发现风险项的个数,可通过“查看详情”命令(见图 5.3)实时查看当前已发现的风险项。单击“退出详情”按钮即可返回病毒扫描页面。

第 3 步:处理威胁。当扫描到威胁后,火绒安全软件提供病毒处理方式的选择。

- 立即处理:对所选择的风险项进行隔离处理。
- 全部忽略:对扫描出的风险项不做处理。

将威胁文件处理完毕后,提示扫描完成,展示扫描概况,在上一步处理的威胁添加至“隔离区”,如图 5.4 所示。

图 5.2　查杀模式选择

图 5.3　查看风险项

火绒安全软件会将扫描后清除的风险项文件经过加密后备份至“隔离区”，以便特殊需要时，可以主动从隔离区中重新找回被清除的风险项文件。以后在首页的下拉菜单中可找到隔离区，如图 5.5 所示。

第 4 步：可将确认安全的文件或网址添加到“信任区”。信任区可以添加文件、文件夹与网址。受信任的项目将不被认为包含风险，也不会被病毒查杀以及病毒防护的各项功能

图 5.4　扫描处理结果

检测。也可以在信任区中对已有的项目取消信任。可以在首页的下拉菜单中找到信任区，如图 5.6 所示。

图 5.5　隔离区

图 5.6　信任区

可以选择将需要信任的文件添加至信任区；或者将需要信任的文件夹添加至信任区，如图 5.7 所示。

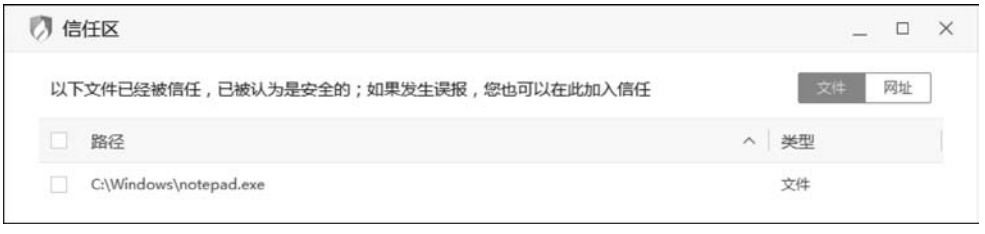

图 5.7　添加至信任区

5.2.3 防护中心

火绒防护中心一共有四大安全模块，包含 21 类安全防护内容。当发现威胁动作触发所设定的防护项目时，火绒安全软件将拦截威胁，帮助计算机避免受到侵害。

1. 病毒防护

病毒防护是针对计算机病毒设计的病毒实时防护系统，包含文件实时监控、恶意行为监控、U 盘保护、下载保护、邮件监控、Web 扫描 6 项安全防护内容，如图 5.8 所示。

图 5.8 病毒防护

1）文件实时监控

将在文件执行、修改或打开时检测文件是否安全，及时拦截病毒程序。在不影响计算机正常使用的情况下，实时保护计算机不受病毒侵害。当有威胁触发了“文件实时监控”时，火绒将自动清除病毒，并弹出提示窗口，如图 5.9 所示。

图 5.9 自动清除病毒提示窗口

2) 恶意行为监控

通过监控程序运行过程中是否存在恶意操作判断程序是否安全,极大提升计算机反病毒能力。当有威胁触发了“恶意行为监控”时,火绒将弹出提示窗口,如图 5.10 所示。可根据需要选择相应的处理方式。

图 5.10　发现病毒提示窗口

3) U 盘保护

在 U 盘插入计算机时对其根目录进行快速扫描,及时发现并阻止安全风险,避免病毒通过 U 盘进入用户的计算机。同时,移动存储设备也会自动纳入文件实时监控等其他监控功能保护范围,全方位保护计算机的安全。

4) 下载保护

在使用浏览器、下载软件、即时通信软件进行文件下载时对文件进行病毒扫描,保护计算机安全。

5) 邮件监控

对所有接收的邮件进行扫描,当发现风险时,将自动打包风险邮件至隔离区,并发送一封火绒已处理的回复邮件。对于发送的邮件,若发现邮件中包含病毒,火绒将直接终止邮件发送,并自动清除病毒邮件至隔离区,防止病毒传播。邮件监控目前仅支持邮件客户端收发的邮件,但不会对邮件客户端做出任何修改。

6) Web 扫描

当有应用程序与网站服务器进行通信时,Web 扫描功能会检测网站服务器返回的数据,并及时阻止其中的恶意代码运行。

2. 系统防护

系统防护模块用于防护计算机系统不被恶意程序侵害。系统防护包含系统加固、应用加固、软件安装拦截、摄像头保护、浏览器保护、联网控制 6 项安全防护内容,如图 5.11 所示。

图 5.11　系统防护

1）系统加固

根据火绒安全软件提供的安全加固策略，当程序对特定系统资源操作时提醒用户可能存在的安全风险。当有威胁动作触发“系统加固”时，会出“系统加固”对话框，如图 5.12 所示，可以根据需要选择对这个动作的处理方式。

图 5.12 “系统加固”对话框

2）应用加固

通过对容易被恶意代码攻击的软件进行行为限制，防止这些软件被恶意代码利用。

3）软件安装拦截

火绒安全软件会根据用户举报，将曾有过未经允许安装到用户计算机行为的软件，加入安装拦截列表中，在其他用户安装相同软件时进行弹窗提示。

4）摄像头保护

在有任意计算机软件要启用用户的摄像头时弹窗提示，用户可以根据需要选择是否允许程序启用摄像头。

5）浏览器保护

能保护浏览器主页与搜索引擎不被随意篡改。此外，在用户访问电商网站与银行官网等网站时，自动进入网购保护模式，阻止支付页面被篡改等支付风险，为浏览器提供更全面的保护。

6）联网控制

当用户需要阻止某程序联网，或者希望自行管控计算机中所有程序是否联网时，用户可以通过联网控制功能很好地管控计算机程序的联网行为。该功能默认不启用，开启后，每当有程序进行联网时，联网控制都会弹窗提示，因此建议根据需要决定是否开启此功能。在联网控制弹窗中，用户可以根据需要选择对这个动作的处理方式。

3. 网络防护

主要保护计算机在使用过程中对网络危险行为的防御。网络防护包含网络入侵拦截、对外攻击拦截、僵尸网络防护、暴破攻击防护、Web 服务保护、恶意网址拦截 6 项安全防护内容，如图 5.13 所示。

1）网络入侵拦截

当黑客通过远程系统漏洞攻击计算机时，网络入侵拦截能强力阻止攻击行为，保护受攻击的终端，有效降低系统面临的风险。当发现有网络入侵行为时，火绒将自动阻止，并通过托盘消息通知用户。

2）对外攻击拦截

对外攻击拦截与网络入侵拦截技术原理一致（都是通过识别漏洞攻击数据包），但是侧重于拦截本机对其他计算机的攻击行为。当发现用户的计算机有对外攻击行为时，火绒安全软件将自动阻止，并通过托盘消息通知用户。

图 5.13　网络保护界面

3) 僵尸网络防护

检测网络传输的数据包中是否包含远程控制代码,通过中断这些数据包传输以避免用户的计算机被黑客远程控制。当发现有僵尸网络行为时,火绒安全软件将自动阻止,并通过托盘消息通知用户。

4) 暴破攻击防护

不法分子常常通过暴力破解登录密码等其他密码破解攻击获取密码进行远程登录。一旦远程登录进入主机,用户可以操作主机允许的任何事情。当有发现计算机受到密码破解攻击时,火绒安全软件将阻止攻击行为,并通过托盘消息通知用户。

5) Web 服务保护

阻止针对 Web 服务相关的软件的漏洞攻击行为。当发现计算机受到入侵时,火绒安全软件将记录攻击行为,并通过托盘消息通知用户。

6) 恶意网址拦截

可以在用户访问网站时自动分辨即将访问的网站是否存在恶意风险。如果存在风险,将拦截访问行为,并告知用户,避免用户的计算机受到侵害。

4. 高级防护

高级防护中的详细内容,用户可在“防护中心”→“高级防护”中查看,如图 5.14 所示。

1) 自定义防护

自定义防护通过设置自定义防护规则能精准控制各项软件的执行,精准保护用户不希望修改的文件、注册表等。有能力的用户可以通过自行编写防护规则,个性化增强计算机防护能力。

图 5.14　高级防护

2）IP 黑名单

当用户的计算机有不受欢迎的 IP 访问时，用户可以将这些 IP 加入黑名单中，以阻止这些 IP 的访问。当发现有 IP 黑名单中地址的请求数据包时，火绒安全软件将直接丢弃，并通过托盘消息通知用户。

3）IP 协议控制

有一定计算机基础的用户在访问网络的时候，若需要控制访问的具体动作，火绒安全软件提供了协议控制，具体是在 IP 协议层控制数据包进站、出站行为，并且针对这些行为做规则化地控制。

5.2.4　访问控制

当有访客使用用户的计算机时，用户可以使用上网时间、程序执行控制、网站内容控制、设备使用控制这些功能对访客的行为进行限制。

1. 密码保护

开启访问控制的各项功能后，虽然已经可以限制计算机的使用，但是功能开关仍可被随意修改，同时，火绒安全软件仍可被人为关闭或卸载。此时用户可通过设置密码来解决。在“访问控制”页面中单击“密码保护”链接，进入安全设置页面，设置密码保护，如图 5.15 所示。

1）设置密码

打开“设置”页面，在“常规设置”→“基础设置”中勾选“开启密码保护”复选框，如图 5.16 所示，弹出“密码设置”对话框。需要注意的是，如果用户忘记密码，火绒安全软件将无法为用户找回之前的密码，请务必牢记用户设置的密码。当用户在密码保护的范围中进行任意操作时，均会弹出输入密码的对话框，要求输入设置的密码才能进行相应操作。

图 5.15　设置密码保护

图 5.16　密码设置页面

2）修改密码和保护范围

在启用密码保护后，需要修改密码或修改密码保护范围时，可在“常规设置”→“基础设置”中单击“密码设置”按钮，再次打开密码设置页面，进行修改密码或保护范围。

3）关闭密码保护

只需取消勾选“开启密码保护”复选框，即可关闭密码保护。

2. 上网时段控制

根据用户设定的上网时间对计算机联网功能进行控制。如图 5.17 所示，当前提供两种限制方式：控制上网时段和控制累计时间。控制上网时段以一星期(一周)为周期，对可上网时间段进行限制，管控每天可上网的时间。控制累计时间对工作日(周一至周五)和周末(周六、周日)的累计上网时长进行限制，管控每天总上网时间。当发生流量变化时，就记为正在上网时间。超出限定上网时间时，将弹窗提示并断网，用户仍可单击“详情”链接或打开

火绒安全软件解除上网时段控制。

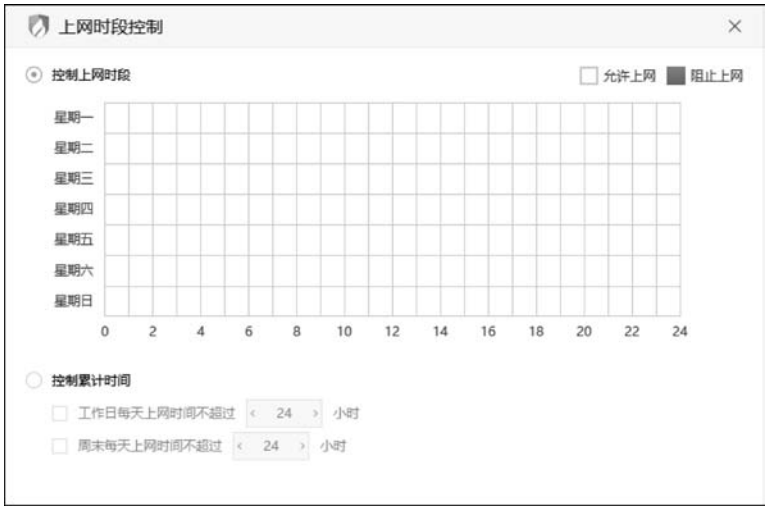

图 5.17　上网时段控制

3. 网站内容控制

可以限制计算机访问指定网址，达到屏蔽某些网站的目的，限制访客访问不受用户信任的网站。除了火绒安全软件内置的 6 项常用的基础规则，还可根据需要添加其他需要屏蔽的网址。用户可以自定义当前规则名称，填写要拦截的网址。多个网址通过换行区分，每行为一个网址。网址支持通配符 *，如 www. *. com 表示 www 开头，以 com 结尾的所有网站都禁止访问。保存此规则，当计算机访问受限网站时，火绒安全软件将拦截访问，并在浏览器中显示拦截提示，如图 5.18 所示。

图 5.18　拦截网址提示

4. 程序执行控制

在访客使用用户计算机的过程中，若用户希望限制访客使用用户的部分软件，此时可开启程序执行控制，以限制某个或某类程序在计算机中的使用，如图 5.19 所示。

当执行受限制程序时，火绒安全软件将弹窗提示用户，并阻止程序执行。单击“详情”链接会打开火绒的程序执行控制页面，若用户已设置密码，还会弹出输入密码提示窗口。

5. U 盘使用控制

提供了阻挡不被信任的 U 盘接入计算机的功能。当开启 U 盘使用控制功能后，接入的

图 5.19　程序执行控制

U 盘需添加信任,未信任的 U 盘将不能使用。选中需要信任的设备,单击“添加信任”按钮,U 盘即可正常连接使用。信任的设备在下一次连接计算机时无须再次确认,可直接连接。当接入的 U 盘不在信任列表内时,火绒安全软件将弹出阻止窗口。单击“详情”链接会打开 U 盘使用控制页面,若用户已设置密码,还会弹出输入密码提示窗口。

5.2.5　安全工具

火绒安全软件除了在病毒防护与系统安全方面为用户保驾护航,同时还提供了 15 种安全工具,帮助用户更方便地使用和管理计算机。此外,火绒还专门为有一定计算机基础的用户提供了一个强大的系统管理工具——火绒剑,如图 5.20 所示。

图 5.20　安全工具

1. 系统工具

1）漏洞修复

漏洞可能导致用户的计算机被他人入侵利用。微软公司和其他软件公司会不定期地针对 Windows 操作系统以及在 Windows 操作系统上运行的其他应用发布相应的补丁程序，漏洞修复能第一时间获取补丁相关信息，及时修复已发现的漏洞。

扫描发现问题后，火绒会默认勾选“高危漏洞补丁”复选框；功能漏洞补丁一般不容易导致计算机的安全风险，因此不会自动为用户勾选，建议有经验的用户选择性修复；不建议安装的补丁在安装后可能会导致用户软件异常或系统崩溃，默认不会勾选，建议用户在非必要时不要修复。单击“一键修复”按钮将开始下载并安装已勾选的漏洞补丁，如图 5.21 所示。

图 5.21　漏洞补丁

“补丁管理”在漏洞修复首页右下角，在“补丁管理”中的项目将不予以扫描显示。用户如需解除此状态，可在“补丁管理”列表中选中需要解除忽略的项目并单击“取消忽略”按钮。

漏洞较多或漏洞补丁较大时常常需要很长的下载时间与安装时间。用户可在正在修复的页面中选择“后台修复”，将漏洞修复切换至后台并提示用户。在系统托盘中可找到“漏洞修复”图标。

2）系统修复

能修复因为木马病毒篡改、软件的错误设置等原因导致的各类计算机系统异常、不稳定等问题，以保证系统安全稳定地运行。进入“系统修复”主页，单击“扫描”按钮开始扫描排查系统问题。

扫描完成并发现问题后，会显示扫描完成页面，用户可根据自己的需要勾选需要修复的项目，火绒默认只为用户勾选推荐修复项。单击“立即修复”按钮进行系统修复，用户等待修复完成即可。“忽略区”在系统修复首页右下角，在忽略区中的项目将不予以扫描显示。用户如需解除忽略状态，可在“忽略区”列表中勾选该项并单击“取消忽略”按钮。

3）弹窗拦截

很多计算机软件在使用的过程中会通过弹窗的形式推送资讯、广告甚至是一些其他软件，这些行为非常影响计算机的正常使用。火绒采用多种拦截形式自主、有效地拦截弹窗。弹窗拦截开启后，会自动扫描出用户计算机软件中出现的广告弹窗，并开始自动拦截。用户也可手动关闭某些不想被拦截的弹窗。

4）垃圾清理

火绒安全软件提供了垃圾清理工具，清理不必要的系统垃圾、缓存文件、无效注册表等，

节省计算机使用空间。打开垃圾清理页面后,单击“开始扫描”按钮即可开始扫描计算机垃圾。

扫描发现系统垃圾后,火绒会为用户智能勾选推荐清理的垃圾,用户可根据需要勾选或取消勾选。勾选完毕后单击“一键清理”按钮等待垃圾清理自动完成即可。在“软件设置”页面中勾选“开机自动扫描”和“自动清理,无需弹窗提醒”复选框,根据需要选择清理大小和扫描周期,火绒安全软件会根据设置的扫描周期自动进行扫描、清理工作。

5) 启动项管理

可以通过管理计算机开机启动项目,允许必要启动,禁止无用启动,使计算机达到最佳使用状态。用户可在“启动项管理”首页中通过禁用或开启控制软件的自启动,管理用户的启动项。

6) 文件粉碎

在用户使用计算机过程中,有部分文件无法通过常规删除;或部分文件需要彻底删除,防止被技术手段恢复,这时就需要对文件进行彻底粉碎。火绒安全软件为用户提供更安全的粉碎方式,保护用户的个人隐私。打开“文件粉碎”页面,用户可通过拖动目标文件/文件夹或单击页面右下方的“添加文件”“添加目录”按钮选择需要粉碎的文件或文件夹。

7) 右键管理

火绒安全软件提供了针对右键菜单管理的小工具,方便用户隐藏右键菜单中不需要的功能。打开“右键管理”页面后,用户可将不希望在右键菜单中显示的命令关闭,将需要显示的命令开启。右键管理一共可以管理文件右键菜单、桌面右键菜单、IE 右键菜单 3 个区域。

2. 网络工具

1) 断网修复

在计算机日常的使用过程中,有时会遇到突然断网的情况。断网修复能为用户检查出断网原因并自动修复出现的问题,为用户恢复网络通畅。在发现问题后,单击“立即修复”按钮,等待网络修复完成即可。若用户有不想修复的项目,可在问题列表中忽略修复此项目。

2) 流量监控

当很多程序都在利用网络下载/上传数据时,会造成访问缓慢的情况,通过流量监控可以更好地控制上网的程序,查看使用网络情况,防止网络阻塞。当需要限制某程序网络传输速度时,打开“流量监控”页面,单击对应的“操作”按钮,选择“限制网速”,打开“限制网速”窗口。如需查看流量使用历史,单击页面右上角的“历史流量”按钮,如图 5.22 所示,进入流量监控历史页面。在这里可以查看程序上传和下载的总流量,同时依然可通过单击程序右侧的“操作”按钮进行流量控制。

若想查看程序当前的连接状况,可以进入“连接详情”窗口。在“连接详情”窗口中,火绒安全软件提供了关闭连接和右键复制数据项的功能。火绒还为用户提供了便捷查看流量的方式,通过流量悬浮窗可以查看当前流量使用状态。

3) 修改 HOST 文件

火绒安全软件为有一定计算机基础的用户提供了修改 HOST 文件的工具。当有些网站用户不想访问,或者有的网站访问不到时,通过修改 HOST 文件就可以把域名指向的 IP 地址修改成希望指向的 IP 地址,达到想要的效果。单击“修改 HOST 文件”按钮能一键打开 HOST 文件,方便快捷地修改 HOST 文件。

图 5.22　流量监控历史页面

3. 高级工具

1）火绒剑

火绒剑是为专业分析人员提供的分析工具，方便其分析软件动作，查找问题。

2）专杀工具

专杀工具主要用于解决部分顽固木马病毒。这类顽固木马病毒运行后，不仅难以清除，而且会阻止安全软件正常安装。因此，需要专杀工具使用针对性的技术手段进行处理。目前专杀工具需要单独下载，用户可在火绒论坛中下载程序安装后使用。

5.3　进阶功能使用

火绒安全软件为有一定计算机知识背景的用户提供了可以手动自由控制杀毒软件以及计算机的方式，用户可以通过调整火绒安全软件的设置，达到自己想要实现的防护效果，更加精准地保护用户的计算机。

5.3.1　病毒查杀

1. 信任风险文件

在风险项中若含有用户信任的文件，用户不想文件被清除，同时又不想被反复扫描出来，可单击该文件的“详情”链接，在弹出的“风险详情”对话框中单击“信任文件”按钮将该文件添加至信任列表。

用户仍可再次单击已信任文件的“详情”按钮，单击“取消信任”按钮，继续查杀该风险文件。

2. 调整查杀设置

打开“安全设置”页面，可在“常规设置”→“查杀设置”中调整病毒查杀的相关配置，如扫描压缩包大小、排除扫描某些扩展名文件、修改病毒处理方式等。

5.3.2 防护中心

1. 病毒防护

可以通过对病毒防护模块的设置达到自己想要的防护效果。

1) 文件实时监控设置说明

通过设置可以调整文件实时监控所产生作用的形式,根据个人需要调整扫描时机、排除文件、处理病毒方式、清除病毒备份隔离区、查杀引擎等内容,防止已经隐藏在计算机中的病毒对计算机造成伤害。

2) 恶意行为监控设置说明

通过设置可以调整恶意行为监控发现威胁动作时是否自动处理,处理病毒与清除病毒后备份隔离区等设置项目。生成若干常见文件格式的随机文件,病毒防护系统增强勒索病毒防护,使用这些随机文件诱捕勒索病毒,达到增强防护的目的。

图 5.23 U 盘修复弹窗提示

3) U 盘保护设置说明

通过设置可以管理 U 盘保护的模式。调整自动扫描、病毒处理方式等内容,防止病毒通过 U 盘感染用户的计算机。

4) U 盘修复功能

主要为用户解决清除部分 U 盘病毒后的两类遗留问题。一类是篡改 autorun 文件的病毒,在查杀后可能会在 U 盘中遗留无效的 autorun .inf 文件;另一类是部分病毒会隐藏用户正常文件,释放伪装文件,诱导用户传播病毒,当火绒查杀了这类病毒后会清除病毒生成的伪装文件,但是会导致部分用户误以为杀毒软件把正常文件删除了。通过 U 盘修复可删除无效的 autorun. inf 文件,检索 U 盘根目录下的隐藏文件与目录,引导用户进行修复操作。当 U 盘接入时发现可修复项目,弹窗提示如图 5.23 所示。

5) 下载保护设置说明

通过设置可以管理下载保护的生效方式,用户可以根据自己的需要对下载内容进行有针对性的查杀,防止病毒通过互联网下载文件感染用户的计算机。

6) 邮件监控设置说明

通过设置可以管理邮件监控的生效方式,用户可以根据自己的需要对发送、接收邮件进行有针对性的查杀,防止病毒通过邮件附件感染用户的计算机。

7) Web 扫描设置说明

通过设置可以管理 Web 扫描的病毒处理方式,防止病毒通过用户访问的网站感染用户的计算机。

2. 系统防护

可以通过对系统防护模块的设置,配置相应规则,控制计算机中的程序对系统的修改与调整,达到对系统防护的效果。

1）系统加固设置说明

通过设置可以管理系统加固的生效方式，火绒针对计算机系统进行规则内置，用户可以根据自己的需要调整防护项目，防止计算机的各项系统设置被恶意程序篡改。

在基础防护中针对文件防护、注册表防护、执行防护的防护项目进行修改调整。默认配置了相应规则，用户可根据需要自行调整，勾选需要启动的防护项目，选择对应的生效方式即可。

自动防护：部分程序为了达到持续篡改系统某些配置的目的，会反复执行相同操作，为了不反复弹窗提示拦截信息，影响日常使用，火绒提供了自动防护功能，用户可以选择记住操作，减少相同弹窗提示。同时，火绒开放了自主添加自动处理项目的功能，方便用户自由管控。

自动添加：当危险行为触发系统加固的生效方式为弹窗提示的规则时，会弹窗提示，勾选“记住本次操作”复选框，就会自动添加规则到“自动处理”列表中，下次遇到相同问题，则采取相同方式处理。

2）应用加固设置说明

勾选“应用加固”，代表该防护规则开启，后面的图标为用户计算机中对应安装的应用程序，程序卸载后，对应图标消失。

3）软件安装拦截设置说明

在软件安装拦截设置中修改规则列表中程序的安装行为，此外，还能自动阻止可识别软件的安装行为。在发现存在软件安装行为时会弹窗提示，当勾选“记住本次操作，下次自动理”复选框时，会自动添加一条对应规则至列表中。

弹出安装拦截提示弹窗时，不会区分软件的安装形式，无论是正常安装还是通过捆绑、推广、静默或其他方式安装，都会统一提示用户软件安装拦截，并非对软件安装包进行报毒，即使选择“阻止”也不会删除软件安装包，用户还可以再次执行，重新安装。

4）摄像头防护设置说明

可在摄像头防护设置中调整规则列表中程序的启动摄像头权限。在发现软件需要启动摄像头时默认弹窗提示，当勾选“记住本次操作，下次自动处理”复选框时，会自动添加一条对应规则至列表中。

5）联网控制设置说明

可在联网控制设置中调整列表中程序的联网行为、添加新的程序联网规则以及调整当前联网控制触发时机。当“联网设置”中选择“询问我”（默认选项）时，每当有联网控制以外的程序发送联网请求，联网控制会弹窗提示，可根据需要选择对这个动作的处理方式。也可勾选“记住本次操作”复选框后选择允许/阻止，添加一条允许/阻止联网的规则到列表中。仍可在联网控制列表中修改或删除此规则。

3. 网络防护

1）入侵拦截设置说明

可在设置中调整当发生黑客入侵或其他网络入侵行为时需要进行的操作。

2）对外攻击拦截设置说明

可在设置中调整当本机发生对外攻击行为时需要进行的操作。

3）僵尸网络防护设置说明

可在设置中调整当计算机被非法远程控制时需要进行的操作。

4) Web 服务保护设置说明

可在设置中调整当黑客对安装了服务器软件的计算机发起攻击,入侵用户计算机的服务器软件时需要进行的操作。

5) 远程登录防护设置说明

当发现计算机受到密码破解攻击时,用户可以在“防护设置”中调整需要进行的操作。同时,也可以添加信任规则,允许指定 IP 发起的远程登录行为。

6) 恶意网址拦截设置说明

可在设置中调整需要拦截的网址类型,同时还能自定义添加需要拦截的网站。

4. 高级防护

1) 自定义防护设置说明

用户可在“自定义防护”设置中添加自定义防护规则,以及查看并管理所有用户创建的自定义规则。“自定义防护”设置中包含自定义规则和自动处理两部分内容。单击“自定义规则”标签页,如图 5.24 所示,进入自定义规则页面。

图 5.24　自定义规则设置

2) IP 黑名单设置说明

可在 IP 黑名单设置中管理黑名单中的所有 IP,同时还支持规则的导出与导入,方便用户的操作。

3) IP 协议控制设置说明

IP 协议控制是在 IP 协议层控制数据包进站、出站行为,并且针对这些行为做规则化的控制。用户可以根据自己的需要选择启用,同时用户也可以自己编写 IP 协议规则。通过设置可以管理 IP 协议控制的相关规则。

5. 管理设置

当用户需要恢复设置的默认状态或是将规则设置导出并在另一台计算机上运行时,管理设置就能很好地满足用户的需求,如图 5.25 所示。

1) 恢复默认设置

将恢复用户在火绒中修改的所有设置为默认状态,单击“恢复默认设置”命令后弹出恢复默认设置提示窗口。单击“确定”按钮则恢复默认设置,单击“取消”按钮或关闭弹窗则不恢复默认设置。

图 5.25　管理设置

2）导出设置

导出当前设置，单击“导出设置”命令后选择保存位置，单击“确定”按钮，等待导出完成即可。

3）导入设置

单击“导入设置”命令后选择需要导入的规则，单击“确定”按钮等待规则导入完成，即可导入设置。

6. 安全日志

安全日志是安全杀毒软件的一项基础功能，用户可以利用安全日志查看一段时间内计算机的安全情况，也可以根据安全日志分析计算机遇到的问题，如图 5.26 所示。

图 5.26　安全日志

以上详细介绍了火绒安全软件各项功能的使用方法,不管是家庭用户还是专业人员,火绒都能提供合适的病毒防护模式,全方位保护计算机安全。通过对火绒安全软件的学习,可以熟悉这类软件的共同特性。

实验思考题

1. 防护中心有哪些功能?
2. 病毒查杀主要有哪几种模式?
3. 访问控制有哪些设置?
4. 安全工具有哪些设置?
5. 在安全日志中可以查看什么信息?